[TLP: GREEN]

Major Malware Threat Intelligence Report For Bangladesh Context

Report Period: Jan - Sep, 2020

Published: October, 2020

BGD e-GOV CIRT

Bangladesh e-Government Computer Incident Response Team

Table of Contents

About this Report

The goal of this report is to provide actionable intelligence regarding threat actors and the malware or other tools they use for reconnaissance, delivery, exploitation, and so forth in order for security operations teams to be empowered to more quickly detect and respond to this specific threat. This information is also intended so that security operations teams can utilize the intelligence in this report in order to set up preventative measures for their IT asset/network/system/cyber resources.

This threat intelligence report is based on analysis from the BGD e-GOV CIRT team in which we examine TOP malware families specific for Bangladesh context for the period of January,2020 to September,2020. The malware families which is listed in this report ware detected by BGD e-GOV CIRT's analysis from its various trusted sources.

Top Malware family in Bangladesh (period of January,2020 to September,2020) are:

- AZORult
- KPOT Stealer
- Oski Stealer
- FormBookFormgrabber
- Loki PWS
- Nexus Stealer
- TrickBot
- Kinsing Malware
- Outlaw hacking group cryptocurrency miners

Advanced Persistent Threat (APT) threats in Bangladesh:

- Lazarus
- Silence
- OceanLotus

General Definition

Malware (malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network (by contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug). A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware.

Trojan horses

A Trojan horse is a harmful program that misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it. A Trojan horse usually carries a hidden destructive function that is activated when the application is started.

Stealer

A stealer is a Trojan that gathers information from a system. The most common form of stealers are those that gather logon information, like usernames and passwords, and then send the information to another system either via email or over a network. Other stealers, called keyloggers, log user keystrokes which may reveal sensitive information.

Info stealer

An information stealer (or info stealer) is a Trojan that is designed to gather information from a system. The most common form of info stealer gathers login information, like usernames and passwords, which it sends to another system either via email or over a network. Other common information stealers, such as keyloggers, are designed to log user keystrokes which may reveal sensitive information.

Cryptomining malware

Cryptomining malware, or cryptocurrency mining malware or simply cryptojacking, is a relatively new term that refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission.

Indicator of compromise (IOC)

Indicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

Typical IoCs are virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control servers.

Command and Control (CnC) Server

A command-and-control (C&C) server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network. Many campaigns have been found using cloud-based services, such as webmail and file-sharing services, as C&C servers to blend in with normal traffic and avoid detection.

Dropper

A dropper is a kind of Trojan that has been designed to "install" some sort of malware (virus, backdoor, etc.) to a target system. The malware code can be contained within the dropper (single-stage) in such a way as to avoid detection by virus scanners or the dropper may download the malware to the target machine once activated (two stage).

Backdoor

A backdoor is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device. Backdoors are most often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems. From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information.

Bot

Malware bots are used to gain total control over a computer.

Remote access Trojan (RAT)

A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet.

DDoS

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Spyware:

Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.

Advanced persistent threat (APT)

An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

The whole purpose of an APT attack is to gain ongoing access to the system. Hackers achieve this in a series of stages.

Stage One: Gain Access

Like a burglar forcing open a door with a crowbar, cybercriminals usually gain entry through a network, an infected file, junk email, or an app vulnerability to insert malware into a target network.

Stage Two: Establish a Foothold

Cybercriminals implant malware that allows the creation of a network of backdoors and tunnels used to move around in systems undetected. The malware often employs techniques like rewriting code to help hackers cover their tracks.

Stage Three: Deepen Access

Once inside, hackers use techniques such as password cracking to gain access to administrator rights so they can control more of the system and get even greater levels of access.

Stage Four: Move Laterally

Deeper inside the system with administrator rights, hackers can move around at will. They can also attempt to access other servers and other secure parts of the network.

Stage Five: Look, Learn, and Remain

From inside the system, hackers gain a full understanding of how it works and its vulnerabilities, allowing them to harvest the information they want at will.

Hackers can attempt to keep this process running — possibly indefinitely — or withdraw once they accomplish a specific goal. They often leave a back door open to access the system again in the future.

Ref: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Network signatures/Rules

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity. Rules are a different methodology for performing detection, which bring the advantage malware detection. Developing a rule requires an acute understanding of how the vulnerability actually works.

Threat level: High

indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems

Threat level: Medium

indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.

Malware: AZORult

AZORult

AZORult stealer is known since 2016 when it appeared on underground market. This malware is able to steal passwords from popular browsers and dat files of popular crypto wallets.

Platform: Windows

Threat level: High

Category: Trojan

General information

- Stealing of passwords from browsers, email clients, FTP-clients, IM-clients: Chrome, Mozilla Firefox, Opera, Yandex Browser, Comodo Dragon, Internet Explorer, Microsoft Edge, Outlook, Thunderbird, Amigo, Pidgin, PSI, PSI + and others.
- Stealing of cookies files, data from autocomplete forms in browsers Chrome, Mozilla Firefox, Opera, Yandex Browser, Comodo Dragon, Amigo, etc.
- Stealing of banking cards data from Chrome-like browsers.
- Collecting of dat files from popular crypto wallets (bitcoin, litecoin, etc.)
- Collecting files of Skype and files from victim's desktop
- Collecting of information about victim's system (ip/comp/user, list of processes, list of applications, etc.)

Indicators of Compromise (IOCs)

CnC:

43.255.154.108
185.9.147.100
205.185.121.209
103.28.15.220
141.8.195.34
103.211.216.223
209.99.16.206
142.44.131.27
91.243.80.164:80
93.170.105.132
89.108.99.79
91.243.81.212
5.8.88.106
162.244.35.55
91.243.80.23
homeearlybird.com

sijuki.com
lulaaura.top
driverscontroller.com
lacdowronfor.com
http://baliseconsulting.com
hadsparmirat.com
rombutcading.ru

MD5

59953C7BF6FD0D9AF52A483C5F993B66
3163ABA93A0292A4BB27AA52DB27C300
c8996ffafc353f1b14f2cada218f8fa5
2fe90a1d114ed4c91fdcfb5e4bbcf60d
d722759dab276601ce5a6071e282b6c4
5E876524A4BCF406D9B53FA90FE97327
E56D3607E99F3F51A8BD18267D8FC15C
19A1DDDA720F8F444BA81B1E070903F9
6081ED3388C8261E85ED1735EEFC16BE
58FBBD895301937014BA1880284DF58D
B1F988B550C4DB1411BA36773227E248
3FCB889CE9066DD811A79C811B36BF56
FDA0D12ADFB59256B3B655CFB011624F
E829B268494D6A5D53EA91803A018853
9b30f8ac97733dac0fa5a02530f2b94c
07ce7152dcb4ba99c9b05c4a959be577
f76849218adceb805e702a45b85c907c
ad3c82241cdac455de215fd0b37ac4cb
0AC55B5056364CDAC63AAF05F9D7F654
2bfe8198144d16a2bf62740a69f3816f
ed3368dbd10ed6ef74d6b65b1f35ef67
0ac55b5056364cdac63aaf05f9d7f654
60fd7028eba3bb029c0631680ff135a1
ed95fb42855312fd61fb65fb29fb77f1
b8e6efb23e79aa5889360d70f494695c;
29ed79ca7b1778274d76c7ef0304efb5
5ddac41b063bc265854f053fb026475f
f32bd9317b8dc700e899aacc554a3b50
d444350e4ea6e10285865d02982d28ee
7ff25aad4b48a2eca4237755735c158a

Network signatures

AZORult CnC Beacon

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult CnC Beacon"; flow:established,to_server; content:"POST"; http_method; content:".php|20|HTTP/1.1|0d 0a|User-"; fast_pattern; content:"MSIE"; http_user_agent; pcre:"/^J[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; http_content_len; byte_test:0,<,150,0,string,dec; http_header_names; content:!"Referer"; content:"|0d 0a|User-Agent|0d 0a|Host|0d 0a|Content-Length|0d 0a|"; pcre:"/^(?:Cache-Control|Pragma)\r\n\r\n$/R"; classtype:backdoor; target:src_ip; sid:1002985; rev:1; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin gib, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6;)

AZORult Variant.4 Checkin M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.4 Checkin M2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|4a 2f fb|"; fast_pattern; http_client_body; content:"|2f fb|"; http_client_body; depth:11; content:!"Referer"; http_header; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,0ac55b5056364cdac63aaf05f9d7f654; reference:url,twitter.com/James_inthe_box/status/1020522733984100352?s=03; classtype:trojan-activity; target:src_ip; sid:2025885; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_07_23, malware_family AZORult, updated_at 2018_07_23;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:from_server,established; tls_cert_subject; content:"CN=linddiederich462.pw"; nocase; fast_pattern; isdataat:!1,relative; tls_cert_issuer; content:"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:trojan-activity; target:dest_ip; sid:2027799; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_08_05, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-07

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-07"; flow:established,to_client; tls_cert_subject; content:"CN=mailfueler.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,c189cdadd96c148e64912c55c5129d3e; classtype:trojan-activity; target:dest_ip; sid:2028652; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03"; flow:established,to_client; tls_cert_subject; content:"CN=worldmasterclass.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,fe9caf2568d7bbf2bb0e20b8e7dc8971; reference:md5,c5a460fd87ffd50c114fffa684688d01; classtype:trojan-activity; target:dest_ip; sid:2028653; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03"; flow:established,to_client; tls_cert_subject; content:"CN=worldmasterclass.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,fe9caf2568d7bbf2bb0e20b8e7dc8971; reference:md5,c5a460fd87ffd50c114fffa684688d01; classtype:trojan-activity; target:dest_ip; sid:2028653; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03"; flow:established,to_client; tls_cert_subject; content:"CN=corpcougar.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,73fad17f8054d01488c3ddd67e355bf1; reference:md5,a25591dbf57ac687e2a03f94dcccc35a; classtype:trojan-activity; target:dest_ip; sid:2028654; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-02"; flow:established,to_client; tls_cert_subject; content:"CN=adityebirla.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,61b34d02bb09e5a547251a625ce81f9c; reference:md5,cab127c5b8582c1e3ea8860a239a060b; classtype:trojan-activity; target:dest_ip; sid:2028655; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-01

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-01"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, OU=PositiveSSL, CN=www.livdecor.pt"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,7baca517af0b93bd3f94910c7b8f10db; reference:md5,efb4951e11baf306f5680a041c214e5b; classtype:trojan-activity; target:dest_ip; sid:2028656; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-09-30

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-09-30"; flow:established,to_client; tls_cert_subject; content:"CN=flozzy.uk"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,6a333c3f54d7fb6efb276cf6e33315c0; reference:md5,ab578cff6c06157aadd5f324a3413973; classtype:trojan-activity; target:dest_ip; sid:2028657; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult Cnc Server) 2019-09-27

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult Cnc Server) 2019-09-27"; flow:established,to_client; tls_cert_subject; content:"CN=evershinebd.net"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,c93a2d16dd0cf8dd3afa5ecba111e7c4; reference:md5,23aff33025681263adcdcb480d0e9a95; classtype:trojan-activity; target:dest_ip; sid:2028658; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC) 2019-11-18

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-11-18"; flow:established,to_client; tls_cert_subject; content:"CN=solvents.ru"; isdataat:!1,relative; fast_pattern; tls_cert_issuer; content:"C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority"; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,e54cbf645b0840c0dd1f212f42cd47fd; classtype:backdoor; target:dest_ip; sid:2029001; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_11_18, malware_family AZORult, performance_impact Low, updated_at 2019_11_18;)

AZORult v3.3 Server Response M1

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.3 Server Response M1"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|3f 36 90|"; depth:6; content:"|3f 7a cd 3d 69 c0 3d|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029136; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.3 Server Response M2

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.3 Server Response M2"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|3f 36 90|"; depth:6; content:"|69 81 60 6b 92 6d 6b|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029137; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.3 Server Response M3

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.3 Server Response M3"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|3f 36 90|"; depth:6; content:"|92 2c 36 90 3f 3b 90|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029138; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.2 Server Response M1

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.2 Server Response M1"; flow:established,to_client; content:"200"; http_stat_code; file_data;

content:"|31 69 f6|"; depth:6; content:"|31 25 ab 33 36 a6 33|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029139; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.2 Server Response M2

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.2 Server Response M2"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|31 69 f6|"; depth:6; content:"|36 e7 6e 34 f4 63 34|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029140; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08"; flow:established,to_client; tls_cert_subject; content:"CN=superlatinradio.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,ce879fb552e7740bb2e940c65746aad2; classtype:trojan-activity; target:dest_ip; sid:2028672; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_11, malware_family AZORult, performance_impact Low, updated_at 2019_10_11;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08"; flow:established,to_client; tls_cert_subject; content:"CN=corpcougar.in"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,f7a490fcf756f9ddbaedc2441fbc3c0c; classtype:trojan-activity; target:dest_ip; sid:2028673; rev:1; metadata:affected_product

Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_11, performance_impact Low, updated_at 2019_10_11;)

Observed Malicious SSL Cert (AZORult CnC Server) in SNI 2019-09-27

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) in SNI 2019-09-27"; flow:established,to_server; tls_sni; content:"techxim.com"; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,5c4e395fc545b5e0c03f960a4145f4ea; classtype:trojan-activity; target:src_ip; sid:2028659; rev:1; metadata:attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Moderate, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08"; flow:established,to_client; tls_cert_subject; content:"CN=cloudcitytechnologies.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,9a23881abe27dc70ca42597a1e1de354; classtype:trojan-activity; target:dest_ip; sid:2028894; rev:1; metadata:attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_22, malware_family AZORult, performance_impact Low, updated_at 2019_10_22;)

AZORult Variant.2 Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.2 Checkin"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"CWC^@GUSGP"; http_client_body; depth:10; fast_pattern; http_content_type; content:"image/jpeg"; depth:10; http_header_names; content:!"Accept|0d 0a|"; content:!"User-Agent|0d 0a|"; content:!"Referer|0d 0a|"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,b8e6efb23e79aa5889360d70f494695c; classtype:backdoor; target:src_ip; sid:2826206; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_02, malware_family Stealer, performance_impact Moderate, updated_at 2020_03_06;)

AZORult Variant.2 Checkin m2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.2 Checkin m2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"~~~~~~~~~~|3a 20|~~~~~"; fast_pattern; http_header; http_content_type; content:"image/jpeg"; depth:10; http_header_names; content:!"Accept|0d 0a|"; content:!"User-Agent|0d 0a|"; content:!"Referer|0d 0a|"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,b8e6efb23e79aa5889360d70f494695c; classtype:backdoor; target:src_ip; sid:2826232; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_03, performance_impact Moderate, updated_at 2020_03_06;)

AZORult Variant.2 Checkin m3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.2 Checkin m3"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; http_start; content:".php HTTP/1.0|0d 0a|Host"; fast_pattern; http_content_type; content:"image/jpeg"; depth:10; http_header_names; content:!"Accept|0d 0a|"; content:!"User-Agent|0d 0a|"; content:!"Referer|0d 0a|"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,b8e6efb23e79aa5889360d70f494695c; reference:md5,29ed79ca7b1778274d76c7ef0304efb5; classtype:backdoor; target:src_ip; sid:2826361; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_10, malware_family Stealer, malware_family AZORult, performance_impact Moderate, updated_at 2020_03_02;)

AZORult v3.2 Server Response M3

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.2 Server Response M3"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|31 69 f6|"; depth:6; content:"|f4 22 69 f6 31 64 f6|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029141; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult Variant.3 Checkin M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.3 Checkin M1"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|99 4c 42 9d 4f 51 c3|"; http_client_body; depth:7; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,ed95fb42855312fd61fb65fb29fb77f1; classtype:trojan-activity; target:src_ip; sid:2829890; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_03_06, malware_family AZORult, performance_impact Low, updated_at 2018_05_30;)

AZORult Variant.3 Checkin M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.3 Checkin M2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|8c 4c 46 91 5b 42 9a 48 42 9f 14|"; http_client_body; depth:11; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,60fd7028eba3bb029c0631680ff135a1; classtype:trojan-activity; target:src_ip; sid:2831079; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_05_30, malware_family Stealer, malware_family AZORult, updated_at 2018_05_30;)

AZORult Variant.4 XORed Download

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult Variant.4 XORed Download"; flow:established,to_client; file_data; content:"|31 69 f6|"; depth:3; fast_pattern; pcre:"/(?:\x31\x25\xab\x33|\x36\xe7\x6e\x34|\xf4\x22\x69\xf6)/RQs"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; classtype:trojan-activity; target:dest_ip; sid:2831936; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_07_23, malware_family AZORult, updated_at 2018_07_23;)

AZORult Variant.5 Checkin M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.5 Checkin M1"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|26 66 96 26 66 9d 47 14 ef 26 66 98 26 66 99 46|"; http_client_body; depth:20; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,aebb382b54e1521ad1309f66d29a1d1c; classtype:trojan-activity; target:src_ip; sid:2833315; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, updated_at 2018_10_29;)

AZORult Variant.5 Checkin M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.5 Checkin M2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|41 10 8b 30 64 8b 30 66 8b 30 62 8b 30 61 8b 30 62 ed|"; http_client_body; depth:20; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,aebb382b54e1521ad1309f66d29a1d1c; classtype:trojan-activity; target:src_ip; sid:2833316; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, updated_at 2018_10_29;)

AZORult Variant.5 Checkin Response

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult Variant.5 Checkin Response"; flow:established,to_client; file_data; content:"</n><d>"; content:"</d>|0d 0a 30 0d 0a 0d 0a|"; distance:0; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,aebb382b54e1521ad1309f66d29a1d1c; classtype:trojan-activity; target:dest_ip; sid:2833317; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, updated_at 2019_09_28;)

Observed DNS Query to known AZOrult Domain

alert dns $HOME_NET any -> any any (msg:"Observed DNS Query to known AZOrult Domain"; dns_query; content:"makak.bit"; nocase; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,78800a47adadaa3a56e533dd7abf957e; classtype:backdoor; target:src_ip; sid:2834136; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_12_28, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

AZORult CnC Beacon M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult CnC Beacon M2"; flow:established,to_server; content:"POST"; http_method; content:"MSIE"; http_user_agent; content:!"/connect.php"; http_uri; content:!"pq.f.360.cn"; http_host; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; http_start; content:"POST|20 2f 20|HTTP/1.1|0d 0a|User-Agent|3a 20|Mozilla/"; fast_pattern; depth:37; http_content_len; byte_test:0,<,150,0,string,dec; http_header_names; content:!"Referer"; content:"|0d 0a|User-Agent|0d 0a|Host|0d 0a|Content-Length|0d 0a|Cache-Control|0d 0a 0d 0a|"; depth:53; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,111665920191e273002cf649070a7766; classtype:backdoor; target:src_ip; sid:2834334; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag Stealer, signature_severity Major, created_at 2019_01_10, malware_family AZORult, performance_impact Low, updated_at 2019_01_11;)

Azorult++ Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Azorult++ Checkin"; flow:established,to_server; content:"POST"; http_method; urilen:1; content:"|00 00 00|"; http_client_body; depth:3; content:"Content-Length|3a 20|25|0d 0a|"; http_header; fast_pattern; http_header_names; content:"|0d 0a|Content-Type|0d 0a|Host|0d 0a|Content-Length|0d 0a|Connection|0d 0a|"; content:!"Referer"; content:!"User-Agent"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,fe8938f0baaf90516a90610f6e210484; reference:url,securelist.com/azorult-analysis-history/89922/; classtype:backdoor; target:src_ip; sid:2835638; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,

deployment Perimeter, signature_severity Major, created_at 2019_03_29, malware_family AZORult, updated_at 2019_03_29;)

AZORult Geolocation Lookup (set)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Geolocation Lookup (set)"; flow:established,to_server; xbits:set,ETPro.AzoRult.GeoCheck,track ip_src,expire 5; noalert; content: "GET"; http_method; content:"/geoip"; http_uri; depth:6; isdataat:!1,relative; content:"api.ip.sb"; http_host; depth:9; isdataat:!1,relative; content:"Mozilla/5.0|20 28|Windows NT 10.0|3b 20|Win64|3b 20|x64|29 20|AppleWebKit/537.36|20 28|KHTML, like Gecko|29 20|Chrome/72.0.3626.121 Safari/537.36"; http_user_agent; depth:115; isdataat:!1,relative; content:"|0d 0a 0d 0a|"; isdataat:!1,relative; http_header_names; content:"|0d 0a|Content-Type|0d 0a|User-Agent|0d 0a|Host|0d 0a|"; http_content_type; content:"application/x-www-form-urlencoded"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,3a13ecf4f8ee02027cf77396bc130c53; reference:md5,fa633db0e584a35350b84560d6ea29df; reference:md5,a703ba86d3692fb59c41efc88ba98c8e; classtype:backdoor; target:src_ip; sid:2836768; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Minor, created_at 2019_06_10, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

AZORult Geolocation Lookup

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Geolocation Lookup"; flow:established,to_server; xbits:isset,ETPro.AzoRult.GeoCheck,track ip_src; content: "GET"; http_method; content:"/json"; http_uri; depth:6; isdataat:!1,relative; content:"freegeoip.app"; http_host; depth:13; isdataat:!1,relative; content:"Mozilla/5.0|20 28|Windows NT 10.0|3b 20|Win64|3b 20|x64|29 20|AppleWebKit/537.36|20 28|KHTML, like Gecko|29 20|Chrome/72.0.3626.121 Safari/537.36"; http_user_agent; depth:115; isdataat:!1,relative; content:"|0d 0a 0d 0a|"; isdataat:!1,relative; http_header_names; content:"|0d 0a|Content-Type|0d 0a|User-Agent|0d 0a|Host|0d 0a|"; http_content_type; content:"application/x-www-form-urlencoded"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,3a13ecf4f8ee02027cf77396bc130c53; reference:md5,fa633db0e584a35350b84560d6ea29df; reference:md5,a703ba86d3692fb59c41efc88ba98c8e; classtype:backdoor; target:src_ip; sid:2836769; rev:2; metadata:affected_product

Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_06_10, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=techxim.com"; nocase; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,dc6c83c65e091e3f572d6870a4d3b382; classtype:backdoor; target:dest_ip; sid:2838487; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_09_17, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

AZORult CnC Beacon M3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult CnC Beacon M3"; flow:established,to_server; content:"POST"; http_method; content:" MSIE "; http_user_agent; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; http_content_len; byte_test:0,<,150,0,string,dec; http_header_names; content:!"Referer"; content:"|0d 0a|Host|0d 0a|User-Agent|0d 0a|Content-Length|0d 0a|"; depth:36; http_start; content:".php|20|HTTP/1.1|0d 0a|Host|3a|"; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,73964217600c6a83da1110ed4df85217; classtype:backdoor; target:src_ip; sid:2834335; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag Stealer, signature_severity Major, created_at 2019_01_10, malware_family AZORult, performance_impact Low, updated_at 2020_02_12;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-28

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-28"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, CN=dicey.biz"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,76fe84b3901f697927de568f5a0dbb0f; classtype:backdoor;

target:dest_ip; sid:2839137; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_28, malware_family AZORult, performance_impact Low, updated_at 2019_10_28;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-22

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-22"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, CN=derek-heath.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,6867022e6454cc381c6e156466e53a9e; classtype:backdoor; target:dest_ip; sid:2839138; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_28, malware_family AZORult, performance_impact Low, updated_at 2019_10_28;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=azo.icf-fx.kz"; nocase; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,678988bffec50b92a0150e0ed0ea9c24; classtype:backdoor; target:dest_ip; sid:2833327; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, performance_impact Moderate, updated_at 2019_09_28;)

Observed Malicious SSL Cert (AZORult CnC) 2019-11-18

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-11-18"; flow:established,to_client; tls_cert_subject; content:"CN=gemateknindoperkasa.co.id"; isdataat:!1,relative; fast_pattern; tls_cert_issuer; content:"C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority"; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,3289edad56299b031de6e6a35e93969b; classtype:backdoor; target:dest_ip; sid:2839482; rev:2; metadata:affected_product

Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_11_18, performance_impact Moderate, updated_at 2019_11_18;)

Observed AZORult Domain in TLS SNI

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"Observed AZORult Domain in TLS SNI"; flow:established,to_server; tls_sni; content:"1d9f0a85.ngrok.io"; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,5ebe08ea8d7c4f043cd0e94711b0ff7f; classtype:backdoor; target:src_ip; sid:2839694; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_02, malware_family AZORult, performance_impact Low, updated_at 2019_12_02;)

Observed Malicious SSL Cert (AZORult CnC) 2019-12-19

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-12-19"; flow:established,to_client; tls_cert_subject; content:"CN=belco-in.com"; depth:15; isdataat:!1,relative; fast_pattern; reference:md5,5306317feffae1f5d2290229e931b624; classtype:backdoor; target:dest_ip; sid:2840027; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_12_19, malware_family AZORult, performance_impact Low, updated_at 2019_12_19;)

Observed Malicious SSL Cert (AZORult CnC) 2019-12-27

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-12-27"; flow:established,to_client; tls_cert_subject; content:"CN=nsabeau.com.my"; depth:17; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,8390e6ceb68f2bd717d83849c4c0e535; classtype:backdoor; target:dest_ip; sid:2840141; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_12_27, malware_family AZORult, performance_impact Low, updated_at 2019_12_27;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-02"; flow:established,to_client; tls_cert_subject; content:"CN=a-vnet.com"; depth:13; isdataat:!1,relative; fast_pattern; reference:md5,8323181d5829755580d379cde3c7aaea; classtype:backdoor; target:dest_ip; sid:2840227; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_02, malware_family AZORult, performance_impact Low, updated_at 2020_01_02;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-02"; flow:established,to_client; tls_cert_subject; content:"CN=aearthlink.net"; depth:17; isdataat:!1,relative; fast_pattern; reference:md5,2ddd176ca5b852ba366642447cddde39; classtype:backdoor; target:dest_ip; sid:2840228; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_02, malware_family AZORult, performance_impact Low, updated_at 2020_01_02;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-02"; flow:established,to_client; tls_cert_subject; content:"CN=ezvuer.com"; depth:13; isdataat:!1,relative; fast_pattern; reference:md5,bf716722b130148297047ab18fbb0342; classtype:backdoor; target:dest_ip; sid:2840229; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_02, malware_family AZORult, performance_impact Low, updated_at 2020_01_02;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=syndicatemechines.com"; depth:24; isdataat:!1,relative; fast_pattern; reference:md5,b1382375eafb605ab7bbf304fadfed64; classtype:backdoor; target:dest_ip; sid:2840357; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_09, malware_family AZORult, performance_impact Low, updated_at 2020_01_09;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=nsabeau.com.my"; depth:17; isdataat:!1,relative; fast_pattern; reference:md5,8390e6ceb68f2bd717d83849c4c0e535; classtype:backdoor; target:dest_ip; sid:2840114; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_12_26, malware_family AZORult, performance_impact Low, updated_at 2019_12_26;)

Observed Malicious SSL Cert (AZORult CnC) 2019-12-05

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-12-05"; flow:established,to_client; tls_cert_subject; content:"CN=cbn-cargo.co.id"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2839784; rev:2; metadata:attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_06, malware_family AZORult, performance_impact Low, updated_at 2019_12_06;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-10

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-10"; flow:established,to_client; tls_cert_subject; content:"CN=syndicatemechines.com"; depth:24; isdataat:!1,relative; fast_pattern; reference:md5,276add022cac0382c552364a9f0793e0; classtype:backdoor;

target:dest_ip; sid:2840391; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_10, malware_family AZORult, performance_impact Low, updated_at 2020_01_10;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-13

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-13"; flow:established,to_client; tls_cert_subject; content:"CN=nenkel.com"; depth:13; isdataat:!1,relative; fast_pattern; reference:md5,c0ab2bcae5b3e3567fa5654ae4b0fdf2; classtype:backdoor; target:dest_ip; sid:2840417; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_13, malware_family AZORult, performance_impact Low, updated_at 2020_01_13;)

Malware: KPOT Stealer

KPOT Stealer

In July 2018 advertisement about selling if «KPOT Stealer» has been published on underground forums. This malware is able to steal passwords from different browsers, messengers, crypto wallets, FTP and other programs. It also has functions to make screenshots of victim's display and function of loader which allows to infect victim's PC with other malware.

Platform: Windows

Threat level: High

Category: Stealer

General information

- Stealing of passwords, auto filling forms, cookies, masked CC from Chromium-Based and Mozilla-Based browsers. It is realized using recursion.
- Collection of passwords from Internet Explorer (versions 6-11)
- Collections of credentials from jabber clients – psi, psi+, pidgin
- Collection of credentials from outlook, rdp
- Collections of crypto wallets data from wallet.dat, namecoin, monero, bytecoin, electrum, ethereum
- Collection of skype correspondence in format: time – sender— receiver – message
- Grabbing of Telegram session
- Grabbing of Discord session
- Grabbing of Battle.Net session
- Grabbing of passwords in VPN: EarthVPN, NordVPN
- Collection of Steam data: ssfn, config.vdf, loginusers.vdf
- Collection of FTP: FileZilla, WinSCP, TotalCommander, WsFtp
- Collection of wininet cookies in netscape format
- Makes screenshots of victim's display in png format
- Function of files' grabbing-Collects information about victim's system – screen resolution, keyboard layout, video card, the name and number of processor cores, current LOCAL time and time zone, OS version including os edition, number of RAM, IP-address.
- Function of loader – file is recorded into memory. If «resident» is chosen, file will be recorded into Temp, path to the file in PEB will be changed so that your file can be installed by copying itself wherever it is needed. If file is 32 bit, loadup will be in

current process; if file is 64 bit and OS is 64-bit, cmd.exe will be launched and file will be injected using wow64ext.

- Function of self-deleting-Bypassing of firewall on the base of com-interface of Internet Explorer.

Network signatures

KPOT Stealer Check-In

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Check-In"; flow:established,to_server; content:"POST"; http_method; content:"bot_id="; depth:7; nocase; http_client_body; fast_pattern; content:"&x64="; nocase; distance:0; http_client_body; content:"&is_admin="; nocase; distance:0; http_client_body; content:"&IL="; nocase; distance:0; http_client_body; content:"&os_version="; nocase; distance:0; http_client_body; content:!"Referer"; http_header; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,7586034a638b95ddd51b60e5b9f4a2b2; classtype:trojan-activity; target:src_ip; sid:2832358; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_08_28, updated_at 2018_08_28;)

KPOT Stealer Exfiltration

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Exfiltration"; flow:established,to_server; content:"POST"; http_method; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|zip_file|22 3b 20|filename=|22|"; http_client_body; content:".cab|22 0d 0a|Content-Type|3a 20|vnd.ms-cab-compressed|0d 0a|"; http_client_body; distance:0; content:"sysInfo.txt"; http_client_body; distance:0; nocase; http_content_type; content:"multipart/form-data|3b 20|boundary=0xd3adc0d3"; nocase; fast_pattern; depth:40; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,7586034a638b95ddd51b60e5b9f4a2b2; classtype:trojan-activity; target:src_ip; sid:2832359; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_08_28, updated_at 2019_09_28;)

KPOT Stealer Exfiltration M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Exfiltration M2"; flow:established,to_server; content:"POST"; http_method; content:"/gate.php";

http_uri; fast_pattern; isdataat:!1,relative; content:"-stream|0d 0a|Content-Encoding|3a 20|binary|0d 0a|Host"; http_header; http_header_names; content:!"User-Agent"; content:!"Referer"; content:!"Accept"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,bba015562893c9367325057b5e725dae; classtype:trojan-activity; target:src_ip; sid:2832753; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_09_24, malware_family Stealer, malware_family KPOT, updated_at 2019_09_28;)

KPOT Stealer Variant CnC Activity

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Variant CnC Activity"; flow:established,to_server; content:"POST"; http_method; content:"/gate.php"; http_uri; isdataat:!1,relative; fast_pattern; http_content_len; byte_test:0,>,1500,0,string,dec; http_header_names; content:"|0d 0a|Host|0d 0a|Content-Length|0d 0a|Connection|0d 0a|Cache-Control|0d 0a 0d 0a|"; depth:53; content:!"User-Agent"; content:!"Accept"; content:!"Referer"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; reference:md5,d88dd410ac0d4317a493b30442899d16; classtype:trojan-activity; target:src_ip; sid:2834774; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_02_07, malware_family KPOT, performance_impact Moderate, updated_at 2019_09_28;)

SSL/TLS Certificate Observed (KPOT)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSL/TLS Certificate Observed (KPOT)"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, OU=PositiveSSL, CN=chrisovunhie.pw"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; classtype:trojan-activity; target:dest_ip; sid:2836202; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag KPOT, signature_severity Major, created_at 2019_05_02, updated_at 2019_05_02;)

Observed Malicious SSL Cert (KPOT CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (KPOT CnC)"; flow:from_server,established; tls_cert_subject; content:"CN=krtk.icu"; nocase; fast_pattern; isdataat:!1,relative; tls_cert_issuer; content:"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id

f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; classtype:trojan-activity; target:dest_ip; sid:2836970; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_06_21, malware_family KPOT, performance_impact Low, updated_at 2019_09_28;)

KPOT Stealer Exfiltration M3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Exfiltration M3"; flow:established,to_server; content:"POST"; http_method; content:"/conf.php"; http_uri; fast_pattern; isdataat:!1,relative; content:"-stream|0d 0a|Content-Encoding|3a 20|binary|0d 0a|Host"; http_header; http_header_names; content:!"User-Agent"; content:!"Referer"; content:!"Accept"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,a0cfe711cd721ca486a49e31081b4e02; classtype:trojan-activity; target:src_ip; sid:2837753; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_07_30, malware_family KPOT, performance_impact Moderate, updated_at 2019_09_28;)

Win32/KPOT Stealer Initial CnC Activity M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32/KPOT Stealer Initial CnC Activity M1"; flow:established,to_server; content:"GET"; http_method; content:"/gate.php"; http_uri; isdataat:!1,relative; fast_pattern; http_content_type; content:"application/x-www-form-urlencoded"; depth:33; isdataat:!1,relative; http_header_names; content:"|0d 0a|Connection|0d 0a|Content-Type|0d 0a|Host|0d 0a 0d 0a|"; depth:36; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; reference:md5,7e3ae5d4db2e8c55dc4de98843489e78; classtype:trojan-activity; target:src_ip; sid:2838467; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_09_16, malware_family KPOT_Stealer, performance_impact Moderate, updated_at 2019_09_28;)

Win32/KPOT Stealer Initial CnC Activity M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32/KPOT Stealer Initial CnC Activity M2"; flow:established,to_server; content:"GET"; http_method; content:"/conf.php"; http_uri; isdataat:!1,relative; http_content_type; content:"application/x-www-form-urlencoded"; depth:33; isdataat:!1,relative; http_header_names; content:"|0d 0a|Connection|0d 0a|Content-Type|0d 0a|Host|0d 0a

0d 0a|"; depth:36; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; reference:md5,7e3ae5d4db2e8c55dc4de98843489e78; classtype:trojan-activity; target:src_ip; sid:2838468; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_09_16, malware_family KPOT_Stealer, performance_impact Moderate, updated_at 2019_09_28;)

Malware: Oski Stealer

Oski Stealer

Oski Stealer is a malware which is advertised on undergrounds forums by oski_seller seller since July 2019. Malware is written in C/C ++. Oski uses man-in-the-browser (MitB) attacks by hooking the browser processes using DLL injection for extracting credentials. Some of the features are: extracting browser credentials and cryptocurrency wallet passwords.

Platform: Windows

Threat level: High

Category: Info stealer

General information

- Non-resident Loader
- Data collection from Browsers (Passwords, Credit Cards, Cookies, Form AutoComplete, View History, Download History, Search Engine History):
- Chromium browsers
- Google Chrome
- Mozilla Firefox
- Opera
- Internet Explorer
- Microsoft Edge
- Amigo
- BlackHawk
- Comodo
- CentBrowser
- Cyberfox
- Epic Privacy Browser
- IceCat
- Kometa
- KMeleon
- Maxthon5
- Nichrome
- Orbitum
- Pale Moon
- Torch
- TorBro
- Uran
- QIPSurf
- Waterfox
- Sputnik

- Vivaldi

Steals following cryptocurrency wallets:

1. BitcoinCore
2. Ethereum
3. Electrum
4. ElectrumLTC
5. Exodus
6. Jaxx
7. ZCash
8. ElectronCash
9. Anoncoin
10. BBQCoin
11. MultiDoge
12. DashCore
13. InfiniteCoin
14. Litecoin
15. DevCoin
16. DigitalCoin
17. FrankoCoin
18. FlorinCoin
19. FreiCoin
20. GoldCoin
21. IxCoin
22. IOCoin
23. MegaCoin
24. MinCoin
25. NameCoin
26. PrimeCoin
27. TerraCoin
28. YACoin

- Collecting following information about Sytem:

1. Windows version
2. Username
3. PC name
4. Machine ID
5. GUID
6. Processor model
7. Video card model
8. Display resolution

9. RAM
10. Local time
11. Time Zone

Network signatures

Win32/Oski Stealer Data Exfil

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32/Oski Stealer Data Exfil"; flow:established,to_server; content:"POST"; http_method; content:".zip|22 0d 0a|"; http_client_body; content:"|0d 0a|PK"; http_client_body; distance:0; content:"screenshot.jpg"; http_client_body; distance:0; http_content_type; content:"multipart/form-data|3b 20|boundary=1BEF0A57BE110FD467A"; depth:49; isdataat:!1,relative; fast_pattern; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family Oski Stealer, rule_origin etpro, former_category MALWARE; reference:md5,6c8357280b50bb1808ec77b0292eb22b; classtype:trojan-activity; target:src_ip; sid:2029236; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2020_01_08, malware_family Oski, updated_at 2020_01_08;)

Malware: FormBookFormgrabber

FormBookFormgrabber

Formgrabber of "FormBook" has begun to be on sale at underground forum since February, 2016. It is intended for compromise data which victim input from browsers, e-mail clients, FTP and services of instant exchange of messages.

Platform: Windows

Threat level: Medium

Category: Trojan

General information

FormBook can be classified as inforstealer malware that collects passwords, logins, installs formgrabber, FTP credentials, messengers credentials and emails data. It began to be sold in the beginning of 2016. The malware injects into legitimate processes and installs keyboard hooks to log all pressed buttons, steal exchange buffer and intercept HTTP sessions.

- log pressed keyboard buttons
- intecept and extract data from HTTP/HTTPS/SPDY/HTTP2 requests
- extract data from Internet browsers and email clients
- make screenshots
- selfupdate
- selfremove
- execute shell commands
- steal cookies
- reboot system
- shutdown system
- Ring3 rootkit
- it reads Windows' ntdll.dll module from disk into memory

If the malware is running with elevated privileges, it can copy payload to one of the following directories:

%ProgramFiles%

%CommonProgramFiles%

If running with normal privileges, it can copy to one of the following directories:

%USERPROFILE%

%APPDATA%

%TEMP%

Browsers hooks look for following substrings in HTTP requests:

- pass
- token
- email
- login
- signin
- account
- persistent

Malware uses RC4 encrypted and Base64 encoded HTTP POST requests to C&C.

Following commands could be received from CnC:

- update
- downlaod and execute
- selfremove
- execute via ShellExecute API
- clear cookies
- reboot OS
- shutdown OS
- collect passwords and create screenshot
- download and extract ZIP archive

Network signatures

Win32.Trojan Formbook Checkin

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan Formbook
Checkin"; flow:established,to_server; content:"GET"; http_method;
content:!"Referer|3a|"; nocase; http_header; content:!"User-Agent|3a|"; nocase;
http_header; content:!"Accept"; nocase; http_header; content:"/?"; http_uri;
fast_pattern; pcre:"/\/\?[a-zA-Z0-9\-_]+=[a-zA-Z0-9_+/=]*(&.+)?$/U"; content:"|00 00
00 00 00 00|"; isdataat:!1,relative; threshold:type limit, track by_src, seconds 360,
count 1; reference:md5,36d5927e1992190368cb34dd1ce19658;
reference:md5,0b658062652f4f4f8829cc131861a764;
reference:md5,39c6f6d426252499caf2042ebaa21751; classtype:backdoor;
target:src_ip; sid:1002098; rev:4; metadata:cnc 1, severity 5, malware_family
FormBookFormgrabber, malware_family Formbook, ti_malware_name
FormBookFormgrabber, rule_origin gib, ti_malware_id
8eee3e23fc03c10c1d3527bea862fc18541db8b4;)
```

Formbook 0.3 Checkin

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Formbook 0.3 Checkin";
flow:to_server,established; content:"POST"; http_method; content:"Mozilla";
```

http_user_agent; depth:7; content:"dat="; depth:4; http_client_body; nocase; fast_pattern; pcre:"/^[a-z0-9_\/+-]{1000}/PRi"; metadata:cnc 1, severity 5, malware_family FormBookFormgrabber, malware_family Formbook, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,6886a2ebbde724f156a8f8dc17a6639c; classtype:backdoor; target:src_ip; sid:2024436; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_06_29, malware_family Password_Stealer, updated_at 2017_11_07;)

Formbook Stealer Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Formbook Stealer Checkin"; flow:to_server,established; content:"GET"; http_method; content:"/?id="; http_uri; pcre:"/^(?:[A-Za-z0-9/+]{4})*(?:[A-Za-z0-9/+]{2}==|[A-Za-z0-9/+]{3}=|[A-Za-z0-9/+]{4})/URi"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent|0d 0a|"; content:!"Accept"; metadata:cnc 1, severity 5, malware_family FormBookFormgrabber, malware_family Formbook, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,72c511b5b12f8bcc1dc706a77a0e9bd0; classtype:backdoor; target:src_ip; sid:2827594; rev:6; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_08_18, performance_impact Moderate, updated_at 2020_03_02;)

FormBook CnC Checkin (POST)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"FormBook CnC Checkin (POST)"; flow:established,to_server; content:"POST"; http_method; content:!"."; http_uri; content:!"?"; http_uri; content:!"&"; http_uri; content:"="; within:15; http_client_body; pcre:/^[a-z0-9\(_~-]{1000,}/PRi"; http_content_len; byte_test:0,>,400,0,string,dec; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_accept_enc; content:"gzip, deflate"; depth:13; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a|Content-Length|0d 0a|"; depth:36; fast_pattern; metadata:cnc 0, severity 3, malware_family FormBookFormgrabber, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; target:src_ip; sid:2829004; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,

deployment Perimeter, signature_severity Major, created_at 2017_12_20, malware_family Formbook, performance_impact Moderate, updated_at 2019_09_28;)

FormBook CnC Checkin (GET)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"FormBook CnC Checkin (GET)"; flow:established,to_server; content:"GET"; http_method; content:"/?"; http_uri; pcre:"/^[A-Za-z0-9_-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))&[A-Za-z0-9-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))(?:&sql=\d*)?$/RU"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a 0d 0a|"; depth:22; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family FormBookFormgrabber, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; target:src_ip; sid:2829000; rev:7; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_12_19, malware_family Formbook, performance_impact Moderate, updated_at 2019_09_28;)

Malware: Loki PWS

Loki PWS

Loki PWS (Password Stealer, aka Loki Bot, Loki-Bot, LokiBot) is a Trojan designed to steal authentication data and cookies saved in browsers. In addition, the malware can steal logins/passwords from Cryptocoin wallet, email clients, FTP clients, VNC clients, Poker clients. It has file grabber, keylogger, VNC, Proxy, form grabber (FF, Chrome, IE, Edge, and Opera) and resident loader modules. Loki PWS sends stolen information to the C&C server via HTTP POST. The Trojan was written in C++ and works with following versions of Windows: XP, Vista, 7, 8, 8.1, 10 and Linux. Loki PWS first appeared on underground forums in 2015. A seller is known as «carter» and «lokistov». The seller disappeared after Loki v2 release in 2017. Presumably, Loki PWS Control panel was leaked in 2016. A cracked version of the Loki PWS has become widespread by the end of the 2017. 10.10.2018 on the underground forum exploit.in carter published an announcement about the sale of new versions Loki Bot v2.1. An actor wasn't active on forums until appearance of Loki Bot v2.1.

Platform: Windows

Threat level: High

Category: Trojan

General information

The malware can steal logins/passwords which were saved in following browsers:

- Internet Explorer
- Mozilla Firefox (x32+x64)
- Google Chrome
- K-Meleon
- Comodo Dragon
- Comodo IceDragon
- SeaMonkey
- Opera
- Safari
- CoolNovo
- Rambler Nichrome
- RockMelt
- Baidu Spark
- Chromium
- Titan Browser
- Torch Browser
- Browser

- Epic Privacy Browser
- Sleipnir Browser
- Vivaldi
- Coowon Browser
- Superbird Browser
- Chromodo Browser
- Mustan Browser
- 360 Browser
- Cyberfox (x32+x64)
- Pale Moon
- Maxthon browser
- Citrio Browser
- Chrome Canary
- Waterfox
- Orbitum
- Iridium
- SlimBrowser
- Brave
- Kometa
- Avant Browser
- Uran
- Dooble
- Sputnik

the Trojan can steal logins/passwords from email clients:

- Outlook (2003-2013)
- Mozilla Thunderbird
- Foxmail
- Pocomail
- Incredimail
- Gmail Notifier Pro
- SNetz Mailer
- Checkmail
- Opera Mail
- FossaMail
- MailSpeaker
- yMail
- Trojita
- TrulyMail
- Claws Mail
- The Bat!
- Mailbird

- TouchMail

The author noted that Trojan also can work with following FTP/VNC clients

- Total Commander
- FlashFXP
- FileZilla
- FAR Manager
- CyberDuck
- Bitvise
- NovaFTP
- NetDrive
- NppFTP
- FTPShell
- SherrodFTP
- MyFTP
- FTPBox
- FtpInfo
- Lines FTP
- FullSync
- Nexus File
- JaSFtp
- FTP Now
- Xftp
- Easy FTP
- GoFTP
- NETFile
- Blaze Ftp
- Staff-FTP
- DeluxeFTP
- ALFTP
- FTPGetter
- WS_FTP
- AbleFTp
- Automize
- RealVNC
- TightVNC
- Syncovery
- mSecure Wallet
- SmartFTP
- FreshFTP
- BitKinex
- UltraFXP

- FTP Rush
- Vandyk SecureFX
- OdinSecure FTP Expert
- Fling
- ClassicFTP
- Maxthon browser
- Kitty(login+private key)
- WinSCP
- Remmina RDP
- WinFTP
- 32Bit FTP
- FTP Navigator
- Core FTP
- CrossFTP
- FTP Voyager
- FireFTP
- CuteFTP
- JSCAPE

Supported password managers:

- EnPass
- KeePass
- 1Password
- AI RoboForm

The malware has module for stealing logins and passwords from cryptocoin wallets

- Bitcoin
- Litecoin
- MultiBit
- Electrum-BTC
- Electrum-LTC
- Armoryc
- Namecoin
- Ufasoft
- PPCoin
- Blockchain
- Ixcoin
- Feathercoin
- NovaCoin
- Primecoin
- Terracoin
- Devcoin

- Digitalcoin
- Anoncoin
- Worldcoin
- Quarkcoin
- Infinitecoin
- DogeCoin
- AsicCoin
- LottoCoin
- DarkCoin
- BitShares
- MultiDoge
- Monacoin
- BitcoinDark
- Unobtanium
- Paycoin
- Copay
- Monero
- Ethereum
- Electron Cash (Bitcoin Cash)
- Bitcoin Knots
- Green Address
- mSIGNA
- Bither
- Exodus
- WinZec (Zcash)

Network signatures

Win32.Spyware_LokiBot Sending data (Fareit/Pony)

```
alert http $HOME_NET any -> any any (msg:"Win32.Spyware_LokiBot Sending data
(Fareit/Pony)"; flow:established,to_server; content:"POST"; http_method;
content:!"Referer|3A|"; nocase; http_header; content:!"Accept-"; nocase; http_header;
content:".php HTTP/1.0"; content:"(Charon|3B| Inferno)"; http_user_agent;
content:"Content-Key|3A 20|"; threshold:type limit, track by_src, seconds 360, count 1;
reference:md5,1019d4a79c0c66070800b827026bb83c;
reference:md5,565d6e2f8ed24de7c3d36b9c277c4cf9;
reference:md5,99f29c4b4ef7f494c525018212662d97; classtype:backdoor;
target:src_ip; sid:1001732; rev:2; metadata:cnc 0, severity 5, malware_family Loki PWS,
ti_malware_name Loki PWS, rule_origin gib, ti_malware_id
b50509a8a6bfdf5f510b38040b3a38fb311447f2;)
```

Loki Bot Cryptocurrency Wallet Exfiltration Detected

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Loki Bot Cryptocurrency Wallet Exfiltration Detected"; flow:established,to_server; content:"POST"; http_method; content:"(Charon|3b 20|Inferno)"; http_user_agent; content:"|00 26 00|"; offset:1; depth:3; http_client_body; pcre:"/^[\x00-\x01]\x00.\x00{3}/PR"; metadata:cnc 0, severity 5, malware_family Loki PWS, ti_malware_name Loki PWS, rule_origin etpro, ti_malware_id b50509a8a6bfdf5f510b38040b3a38fb311447f2, former_category TROJAN; classtype:backdoor; target:src_ip; sid:2024311; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_17, malware_family lokibot, updated_at 2018_04_13;)

Loki Bot Keylogger Data Exfiltration Detected M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Loki Bot Keylogger Data Exfiltration Detected M1"; flow:established,to_server; content:"POST"; http_method; content:"(Charon|3b 20|Inferno)"; http_user_agent; content:"|00 2b 00|"; offset:1; depth:3; http_client_body; pcre:"/^[\x00-\x01]\x00.\x00[\x00-\x01]\x00.\x00.{4}\x01\x00.\x00{3}.{48}\x05\x00{3}/PR"; metadata:cnc 0, severity 5, malware_family Loki PWS, ti_malware_name Loki PWS, rule_origin etpro, ti_malware_id b50509a8a6bfdf5f510b38040b3a38fb311447f2, former_category TROJAN; classtype:backdoor; target:src_ip; sid:2024315; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_17, malware_family lokibot, updated_at 2018_04_13;)

Malware:Nexus Stealer

Nexus Stealer

Nexus Stealer is a malware which is advertised on undergrounds forums by nexusMP seller since January 2020. Malware is written in C/C ++.

Platform: Windows

Threat level: High

Category: Info stealer

General information

- Data collection of all Chromium browsers (Passwords, Credit Cards, Cookies, Form AutoComplete, View History, Download History, Search Engine History) Includes data from Chrome Browser and browsers with non-standard data location.
- Collecting all .dat of files (recursion) of cryptocurrency wallets, and also collecting cold purses: Anoncoin, Bitcoin, Bitpay, Coinomi, DashCore, devcoin, Eidoo, Electrum, Electrum-NMC, Exodus, Feathercoin, Fetch, FLO, Franko, Freicoin, GoldCoin (GLD), Guarda, I0coin, iXcoin, Jaxx, Litecoin, Luckycoin, MegaCoin, Mincoin, Monero, MyCrypto, NovaCoin, Peercoin, Primecoin, Quarkcoin, TerracoinCore, Worldcoin, Yacoin, Zetacoin.
- Collecting 2FA Sessions - Authenticator (Authy)
- Collecting all Telegram sessions
- Collect all Discord sessions
- Collect all Steam sessions
- Jabber Client Census
- Collect all profiles FileZilla
- Collect all profiles WinSCP
- Collect all profiles TotalCommander
- Collecting credentials WindowsSecureVault
- IE, Edge credential collection
- Collect all Pidgin accounts
- Collecting all PSI, PSI accounts
- Collecting sessions of VPN clients
- Collection of sessions and authorization data OpenVPN
- Collecting Steam Details
- Collecting profile data WiFi
- Collecting profiles from Credmanager
- Collect system information, screenshots, and location data (useful for spot client processing)
- Grabber of files

- Ability to filter CIS-Logi (LPG), protection against repetition
- Loader module with flexible parameters, ability to specify multiple files and multiple filters
- A separate and convenient search page, with the ability to sort by a large number of criteria, including cookies and passwords, to automate the search for the required data.
- Ability to change skin in one click,
- View log data without downloading (passwords, PC information)
- The automated installation of the panel
- Intuitive and at the same time beautiful admin panel. Ability to sort logs by custom templates (Presets), ability to create/edit/delete templates.
- The ability to download or remove all logs directly in the panel (in one click)!
- Smart filtering of fresh logs
- Geostatistical information on home page

Network signatures

Nexus Stealer CnC Data Exfil

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Nexus Stealer CnC Data Exfil"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; isdataat:!1,relative; content:!"Mozilla"; http_user_agent; content:"{"; depth:1; http_client_body; content:"|7e 3b 5e 3b|Windows|20|"; distance:0; http_client_body; within:50; fast_pattern; content:"|7e 3b 5e 3b|"; distance:0; http_client_body; content:"|7e 3b 5e 3b|"; distance:0; http_client_body; content:"|7e 3b 5e 3b|"; distance:0; http_client_body; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family Nexus Stealer, rule_origin etpro, former_category MALWARE; reference:md5,8bd8582155ef003b8a24d341d75f1d7f; classtype:trojan-activity; target:src_ip; sid:2029298; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2020_01_21, malware_family Nexus, updated_at 2020_02_19;)

Malware: TrickBot

TrickBot is banking trojan first appeared in middle 2016. TrickBot is Dyre successor and has strong code similarities to the Dyre trojan. In the beggining the trojan attacks Australian and Canadian banks.

Platform: Windows

Threat level: High

Category: Trojan

General information

In the first half of 2016, Trickbot was first noticed in attacks on clients of banks. Trickbot is a banking trojan using similar techniques as Dyre. After launch of the loader – "TrickLoader", the body of the trojan is installed in the victim's system. This is loaded from the host controlled by the attackers along with additional modules that are then subsequently launched. Amongst these, are modules for collection and distribution of PC system information, data intercepted from browsers, information from email clients, functionality for network spreading, form-grabbers as well as browser inject functionality.

Network signatures

Trickbot SSL certificate detected

```
alert tls any any -> $HOME_NET any (msg:"Trickbot SSL certificate detected";
flow:established,from_server; content:"|55 04 0a|"; content:"|16|Ubiquiti Networks
Inc."; distance:1; within:23; content:"|55 04 0b|"; distance:0; content:"|11|Technical
Support"; distance:1; within:18; content:"|55 04 03|"; distance:0; content:"UBNT-";
distance:1; within:6; target:src_ip; classtype:banking-trojan;
reference:md5,87dfea7f85a960bbc92b0adbf124a072; sid:1002270; rev:2;
metadata:severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae,
ti_malware_name TrickBot, malware_family TrickBot, rule_origin gib;)
```

Win32.Trojan_Trickbot Sending IE history

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan_Trickbot
Sending IE history"; target:src_ip; flow:established,to_server; content:"POST";
http_method; content:!"Referer|3a|"; nocase; http_header; content:"Connection|3a|
close"; nocase; http_header; content:"boundary=---------"; http_header; fast_pattern;
pcre:"/boundary=-{9}[A-Z]{16}\x0d\x0a/"; pcre:"/\/[\x20-\x7e]+?\.[0-9A-F]{32}\/U";
reference:md5,6ace098066b82cd4e6ad5bbdc9954b0d;
```

reference:md5,1a3d01fce1c387a2075f1de6a462a871; classtype:banking-trojan; reference:md5,155106c45d76d566051cc65f77df2e55; sid:1002028; rev:1; metadata:severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin gib;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)"; target:dest_ip; flow:established,from_server; content:"|09 00 e7 1f b0 eb b2 ae 21 70|"; fast_pattern; content:"|55 04 0a|"; distance:0; content:"|13|Default Company Ltd"; distance:1; within:20; reference:url,sslbl.abuse.ch; classtype:banking-trojan; sid:2023541; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_11_22, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_11_22, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN TrickBot IP Check

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN TrickBot IP Check"; target:src_ip; flow:to_server,established; content:"GET"; http_method; content:"User-Agent|3a 20|Mozilla/5.0 (Windows NT 10.0|3b 20|WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36|0d 0a|Host|3a 20|ipinfo.io|0d 0a|"; http_header; depth:141; fast_pattern:121,20; content:!"Referer|3a|"; http_header; content:!"Accept"; http_header; threshold:type both, track by_src, count 1, seconds 5; reference:md5,770db932ec1807de570be1727e5ced09; classtype:banking-trojan; sid:2827992; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_09_18, deployment Perimeter, former_category TROJAN, performance_impact Moderate, signature_severity Major, updated_at 2020_08_12, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN Malicious SSL certificate detected (TrickBot C2)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Malicious SSL certificate detected (TrickBot C2)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0c|421ho4241.ru"; distance:1; within:13; classtype:banking-trojan; sid:2828428; rev:2; metadata:affected_product

Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_26, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2017_10_26, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN Trickbot SSL Certificate Detected

alert tls $EXTERNAL_NET 447 -> $HOME_NET any (msg:"TROJAN Trickbot SSL Certificate Detected"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|13|sd-97597.dedibox.fr"; fast_pattern; distance:1; within:20; reference:md5,3d55d71c3f0655837694ea125687e479; reference:url,sslbl.abuse.ch/intel/cf31d2f8e419d76517b0bc6c3ead1f246b950a42; classtype:banking-trojan; sid:2830188; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_03_29, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, updated_at 2018_03_29, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN Trickbot Payload Request

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Trickbot Payload Request"; target:src_ip; flow:to_server,established; content:"GET"; http_method; pcre:"/^\/(?:kas|ser|mac)[0-9]+\.png$/Ui"; http_start; content:".png HTTP/1.1|0d 0a|Host|3a 20|"; fast_pattern; http_header_names; content:!"Accept"; content:!"Referer|0d 0a|"; content:!"User-Agent|0d 0a|"; reference:md5,2c6cd25a31fe097ee7532422fc8eedc8; classtype:banking-trojan; sid:2024901; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_23, deployment Perimeter, former_category TROJAN, signature_severity Major, tag Trickbot, updated_at 2020_03_04, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

Trickbot Known C&C IP

alert tcp $HOME_NET any -> [200.119.45.140, 107.181.175.122, 79.143.31.94, 186.47.40.234, 181.129.93.226, 190.152.4.210, 107.173.42.177, 82.118.22.87, 195.123.213.186, 195.123.246.69, 51.254.69.233, 195.123.240.36, 195.161.114.131,

192.210.132.15, 168.235.102.16, 164.132.138.134, 23.94.93.106, 190.154.203.218, 189.80.134.122, 125.99.253.34, 191.37.181.152, 187.58.56.26, 146.196.122.167, 177.103.240.149, 131.196.184.141, 103.84.238.3, 190.152.4.210, 202.4.169.178, 36.89.85.103, 103.117.172.206, 45.237.240.178] 443 (msg:"Trickbot Known C&C IP"; reference:md5, 0cc0cbe936aadd2ba70dc0c8a901493b; reference:url, https://brica.de/alerts/alert/public/1274175/trickbot-is-using-google-docs-to-trick-proofpoints-gateway/; reference:url, https://feodotracker.abuse.ch/browse/host/107.173.42.177/; reference:url, https://feodotracker.abuse.ch/browse/host/82.118.22.87/; reference:url, https://feodotracker.abuse.ch/browse/host/195.123.213.186/; reference:url, https://feodotracker.abuse.ch/browse/host/195.123.246.69/; reference:url, https://feodotracker.abuse.ch/browse/host/51.254.69.233/; reference:url, https://otx.alienvault.com/indicator/ip/195.123.240.36; reference:url, https://feodotracker.abuse.ch/browse/host/195.161.114.131/; reference:url, https://feodotracker.abuse.ch/browse/host/192.210.132.15/; reference:url, https://feodotracker.abuse.ch/browse/host/168.235.102.16/; reference:url, https://feodotracker.abuse.ch/browse/host/164.132.138.134/; reference:url, https://feodotracker.abuse.ch/browse/host/23.94.93.106/; reference:url, https://feodotracker.abuse.ch/browse/host/190.154.203.218/; reference:url, https://feodotracker.abuse.ch/browse/host/189.80.134.122/; reference:url, https://feodotracker.abuse.ch/browse/host/125.99.253.34/; reference:url, https://feodotracker.abuse.ch/browse/host/191.37.181.152/; reference:url, https://feodotracker.abuse.ch/browse/host/187.58.56.26/; reference:url, https://feodotracker.abuse.ch/browse/host/146.196.122.167/; reference:url, https://feodotracker.abuse.ch/browse/host/177.103.240.149/; reference:url, https://feodotracker.abuse.ch/browse/host/131.196.184.141/; reference:url, https://feodotracker.abuse.ch/browse/host/103.117.232.198/; reference:url, https://feodotracker.abuse.ch/browse/host/103.84.238.3/; reference:url, https://feodotracker.abuse.ch/browse/host/190.152.4.210/; reference:url, https://feodotracker.abuse.ch/browse/host/202.4.169.178/; reference:url, https://feodotracker.abuse.ch/browse/host/36.89.85.103/; reference:url, https://feodotracker.abuse.ch/browse/host/103.117.172.206/; reference:url, https://feodotracker.abuse.ch/browse/host/45.237.240.178/; target:src_ip; classtype:banking-trojan; sid:1003029; rev:1; metadata:cnc 1, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin gib;)

Malware: Kinsing

Kinsing Malware

In this attack, the attackers exploit a misconfigured Docker API port to run an Ubuntu container with the kinsing malicious malware, which in turn runs a cryptominer and then attempts to spread the malware to other containers and hosts.

Platform: Linux

Threat level: Medium

Category: Cryptominer

General information

- Disabled security measures and cleared log
- Downloaded and ran the shell script every minute using crontab
- Halted and deleted files related to numerous applications like other malware and cryptominers
- Installed and ran the Kinsing malware
- Killed other malicious Docker containers and deleted their image
- Looked for other commands running and cron; if found, it deletes all cron jobs including its own.

Indicators of Compromise (IOCs)

http://142.44.191.122/d.sh

http://142.44.191.122/kinsing/

http://142.44.191.122/al.sh

http://142.44.191.122/cron.sh

http://142.44.191.122/

http://142.44.191.122/kinsing

http://142.44.191.122/ex.sh

http://185.92.74.42/w.sh

http://185.92.74.42/d.sh

http://217.12.221.244/

http://217.12.221.24/d.sh

http://217.12.221.244/kinsing

http://217.12.221.244/j.sh

http://217.12.221.244/t.sh

http://217.12.221.244/spr.sh

http://217.12.221.244/spre.sh

http://217.12.221.244/p.sh

http://217.12.221.244/Application.jar

http://217.12.221.244/f.sh

http://www.traffclick.ru/

http://www.mechta-dachnika-tut.ru/

http://www.rus-wintrillions-com.ru/

http://rus-wintrillions-com.ru/

http://stroitelnye-jekologicheskie-materialy2016.ru

45.10.88.102

91.215.169.111

193.33.87.219

MD5:

kinsing - 0d3b26a8c65cf25356399cc5936a7210

kinsing - 6bffa50350be7234071814181277ae79

kinsing - c4be7a3abc9f180d997dbb93937926ad

kdevtmpfsi - d9011709dd3da2649ed30bf2be52b99e

Malware: Outlaw hacking group cryptocurrency miners

Outlaw hacking group cryptocurrency miners

Outlaw Hacking Group's Botnet download Monero miner script named dota3.tar.gz.

The shell script downloads, extracts, and executes the miner payload. The extracted TAR file contains folders with scripts and the miner and backdoor components.

Platform: Linux

Threat level: Medium

Category: Cryptominer

General information

The Shellbot disguises itself as a process named rsync, commonly the binary seen on many Unix- and Linux-based systems to automatically run for backup and synchronization. This allows the malicious activity to evade detection.

File named "tsm32" and "tsm64" is responsible for propagating the miner and backdoor via SSH brute force, and capable of sending remote commands to download and execute the malware. Another file named as ".satan" is a shell script that installs the backdoor malware as a service.

In Linux, files that start with a period are hidden.

Download masscan tar file and unzip the masscan and scan the connected network subnet excluding private IP. The scan result was kept in a text file named input.txt for delete it.

Indicators of Compromise (IOCs)

146.185.171.227:443

5.255.86.129:3333

54.37.70.249/.satan

54.37.70.249/rp

http://54.37.70.249/.x15cache

http://54.37.70.249/dota2.tar.gz

http://54.37.70.249/fiatlux-1.0.0.apk

http://mage.ignorelist.com/dota.tar.gz

mage.ignorelist.com

zergbase.mooo.com

SHA256

rsync	0d71a39bbd666b5898c7121be63310e9fbc15ba16ad388011f38676a14e27809
ps	bb1c41a8b9df7535e66cf5be695e2d14e97096c4ddb2281ede49b5264de2df59
cron	4efec3c7b33fd857bf8ef38e767ac203167d842fdecbeee29e30e044f7c6e33d
anacron	66b79ebfe61b5baa5ed4effb2f459a865076acf889747dc82058ee24233411e2
tsm32	0191cf8ce2fbee0a69211826852338ff0ede2b5c65ae10a2b05dd34f675e3bae
tsm64	085d864f7f06f8f2eb840b32bdac7a9544153281ea563ef92623f3d0d6810e87

Advanced Persistent Threat (APT): Lazarus

The cybercrime group Lazarus (also known as Dark Seoul Gang/HIDDEN COBRA/Guardians of Peace), which has North Korean roots, is behind the so many major attacks.

Originally a criminal group, the group has now been designated as an advanced persistent threat due to intended nature, threat, and wide array of methods used when conducting an operation.

Malware List of Lazarus APT:

a. Manuscrypt

Manuscrypt is a RAT-type Trojan that can receive commands sent by the actors responsible from the C&C server to the victim's computer via double proxies. Usually, a Trojan hits the victim's computer using other Lazarus malware or after the user visits a compromised website.

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Other Name: FALLCHILL

General information

The Trojan collects basic system information and sends it to C&C:

- Operating system version
- Processor information
- System name
- Local IP address information
- Unique generated ID
- MAC address

Manuscrypt has the following built-in features for remote operations, providing different capabilities on the victim's system:

- retrieve information about all installed drives, including drive type and free disk space;
- create, run and terminate a new process and its main thread;
- search, read, write, move and execute files;
- get and change the timestamps of files or directories;
- change the current directory for the process or file; and

- remove the Trojan and artefacts associated with malware from the infected system

Indicators of Compromise (IOCs)

CnC:
112.217.108.138
211.192.239.232
https://www.elite4print.com/admin/order/batchPdfs.asp
222.239.223.156
https://tpddata.com/flash/gcoin2.swf
tpddata.com
104.243.41.186
https://tpddata.com/flash/gcoin4.swf
http://www.pakteb.com/include/left.php
http://www.nuokejs.com/contactus/about.php
http://www.qdbazaar.com/include/footer.php
www.pakteb.com
www.nuokejs.com
www.qdbazaar.com
104.221.134.28
104.195.1.39
104.31.74.89
https://sfacor.com/upload/profile_2.dmg
sfacor.com
78.128.92.133
https://sfacor.com/upload/profile_4.dmg
https://wifispeedcheck.net/upload/conf3.dat
wifispeedcheck.net
192.99.34.204
https://wifispeedcheck.net/upload/conf6.dat
https://tpddata.com/skins/skin-8.thm
https://tpddata.com/skins/skin-6.thm
https://www.anlway.com/include/arc.search.class.php
https://www.apshenyihl.com/include/arc.speclist.class.php
https://www.ap8898.com/include/arc.search.class.php
http://www.paulkaren.com/synthpop/main.asp
http://www.shieldonline.co.za/sitemap.asp
http://ansetech.co.kr/smarteditor/common.asp
http://mileage.krb.co.kr/common/db_conf.asp
http://www.51up.com/ace/main.asp
http://www.33cow.com/include/control.php
www.anlway.com
www.apshenyihl.com
www.ap8898.com
www.paulkaren.com
www.shieldonline.co.za

ansetech.co.kr
mileage.krb.co.kr
www.51up.com
www.33cow.com
107.165.165.35
104.222.238.212
108.61.91.60
196.38.160.213
106.10.79.34
211.48.76.36
112.126.67.80
https://itaddnet.com/res/prof3.db
https://www.daslibs.com/res/prof3.db
itaddnet.com
www.daslibs.com
https://itaddnet.com/res/prof6.db
https://www.daslibs.com/res/prof6.db
http://www.yich.co.kr/jbcgi/edit/tmp/notice_20112030837572332.png
www.yich.co.kr
222.231.2.43
http://www.marmarademo.com/include/extend.php
http://www.97nb.net/include/arc.sglistview.php
www.marmarademo.com
www.97nb.net
103.238.227.72
http://www.jscw.co.kr/jbcgi/edit/tmp/notice_201002191504537620.gif
www.jscw.co.kr
222.231.2.179
falcancoin.io
http://www.530hr.com/data/common.php
www.530hr.com
23.107.38.5
http://www.028xmz.com/include/common.php
www.028xmz.com
45.34.66.30
http://168wangpi.com/include/charset.php
168wangpi.com
http://hypnosmd.com/include/top.php
hypnosmd.com
64.90.49.224
http://0756rz.com/include/left.php
0756rz.com
http://51xz8.com/include/top.php
51xz8.com
23.244.213.174
http://168va.com/include/data/left.php
168va.com

http://1996hengyou.com/include/dialog/left.php
1996hengyou.com
160.124.191.80
https://www.naviilibs.com/video/battle32.avi
www.naviilibs.com
198.54.116.51
https://www.naviilibs.com/video/battle64.avi
http://10vs.net/include/left.php
10vs.net
182.56.5.227
222.122.31.115
66.99.86.8
210.61.8.12
62.215.99.90
111.207.78.204
181.119.19.56
184.107.209.2
59.90.93.97
80.91.118.45
81.0.213.173
98.101.211.162
125.212.132.222
175.100.189.174
181.119.19.118
181.119.19.141
181.119.19.196
181.119.19.5
181.119.19.50
181.119.19.54
181.119.19.58
181.119.19.74
190.105.225.232
41.92.208.194
41.92.208.196
41.92.208.197
209.183.21.222
190.82.74.66
190.82.86.164
119.10.74.66
122.114.89.131
122.114.94.26
139.217.27.203
221.208.194.72
221.235.53.229
77.78.100.101
62.243.45.227
117.232.100.154

59.90.93.138
125.160.213.239
27.123.221.66
36.71.90.4
191.233.33.177
200.57.90.108
5.79.99.169
203.160.191.116
196.25.89.30
82.223.213.115
82.223.73.81
91.116.139.195
195.74.38.115
210.202.40.35
104.192.193.149
173.0.129.65
173.0.129.83
191.234.40.112
199.167.100.46
208.180.64.10
208.78.33.70
208.78.33.82
216.163.20.178
50.62.168.157
64.29.144.201
66.175.41.191
66.232.121.65
66.242.128.11
66.242.128.12
66.242.128.13
66.242.128.134
66.242.128.140
66.242.128.158
66.242.128.162
66.242.128.163
66.242.128.164
66.242.128.170
66.242.128.173
66.242.128.179
66.242.128.181
66.242.128.185
66.242.128.186
66.242.128.223
71.125.1.130
71.125.1.132
71.125.1.133
71.125.1.138

72.167.53.183
75.103.110.134
96.65.90.58
98.101.211.140
98.101.211.170
98.101.211.251
98.113.84.130
98.159.16.132
197.211.212.14

MD5:

633BD738AE63B6CE9C2A48CBDDD15406
34c2ac6daa44116713f882694b6b41e8
24906e88a757cb535eb17e6c190f371f
3005f1308e4519477ac25d7bbf054899
68fa29a40f64c9594cc3dbe8649f9ebc
d2de01858417fa3b580b3a95857847d5
a5e08dae67549fa790f0efef56813bb4
5e60ff179d6e4af28f91f70f45b72038
22f8d2a0c8d9b54a553fca1b2393b266
35e38d023b253c0cd9bd3e16afc362a7
72fe869aa394ef0a62bb8324857770dd
86d3c1b354ce696e454c42d8dc6df1b7
5182e7a2037717f2f9bbf6ba298c48fb
fcbe4b5a31c37751c561d12b8fc48ca4
a1f98a72f8bff1ce60246363af673c2d
a7c804b62ae93d708478949f498342f9
86685ec8c3c717aa2a9702e2c9dec379
aeee54a81032a6321a39566f96c822f5
b054a7382adf6b774b15f52d971f3799
e1ed584a672cab33af29114576ad6cce
d8484469587756ce0d10a09027044808
667cf9e8ec1dac7812f92bd77af702a1
361c2c5be75439dda958daa6032cab49
d08986b22d2371419dfcdf4abdb821b5
3d0355ff78dcc979b3f83a679b6ba794
aa7f506b0c30d76557c82dba45116ccc
eb6275a24d047e3be05c2b4e5f50703d
a6d1424e1c33ac7a95eb5b92b923c511
912f87392a889070dbb1097a82ccd93f
778a7ed1aa3ce2d8eb719765cac3c166
307797746dabfa55a13d879d1f112aa5
3b1f4d1d0d7a40b449244b8a9e1649ae
c6801f90aaa11ce81c9b66450e002972
12c786c490366727cf7279fc141921d8
df7328f9f6fbab00c63e6c398c961502
cea52553aed83e408702ad7c03f287c7

425dfb5944dab3b3adbffe5128f4cf29
278833c6f56ce1f82c368e623bf8ae96
1f04ca0504ba5e5d721eed5575bc19ef
e19d79fa3d5b70d116a7ec76735bda53
233ad743dd26c959fa735ffbaa456c05
169c4843fe4d114e8d10d84da7cf7d5f
1c53e7269fe9d84c6df0a25ba59b822c
77b50bb476a85a7aa30c962a389838aa
6ab301fc3296e1ceb140bf5d294894c5
ef9db20ab0eebf0b7c55af4ec0b7bced
3229a6cea658b1b3ca5ca9ad7b40d8d4
10b28da8eefac62ce282154f273b3e34
60294c426865b38fde7c5031afc4e453
ca67f84d5a4ac1459934128442c53b03
bfb41bc0c3856aa0a81a5256b7b8da51
f5a4235ef02f34d547f71aa5434d9bb4
9722bc9e0efb4214116066d1ff14094c
00b0cfb59b088b247c97c8fed383c115
aa7924157b77dd1ff749d474f3062f90
1216da2b3d6e64075e8434be1058de06
e48fe20eb1f5a5887f2ac631fed9ed63

SHA-256:
380b76590d3e878d73bc7964fe225a2721218dcda7ed9c571b433af07a8b1107
380b76590d3e878d73bc7964fe225a2721218dcda7ed9c571b433af07a8b1107

Network Signatures

N/A

b. CuriousLoadert

Loader used by hackers from Lazarus. Discovered as part of the attack in October 2019, however, the first sample dates back to December 2018.

Platform: N/A

Threat level: Middle

Category: Loader

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
84b8af33a6181ac13fa5529d08500fc7
11fdc0be9d85b4ff1faf5ca33cc272ed
5e60ff179d6e4af28f91f70f45b72038
2b02465b65024336a9e15d7f34c1f5d9
f6d6f3580160cd29b285edf7d0c647ce
14d79cd918b4f610c1a6d43cadeeff7b
c0a8483b836efdbae190cc069129d5c3

Network Signatures

N/A

c. SvcRAT

Platform: N/A

Threat level: High

Category: remote-access-trojan

General information

Indicators of Compromise (IOCs)

CnC:
23.95.229.119
107.175.59.21
192.3.31.12
66.154.103.104
107.174.25.127
172.245.156.203
https://151.106.27.234:443
151.106.27.234
162.255.119.153
162.255.119.34

MD5:
08b6891f3320c653d69dfd5d0694c69a
947fa11d132caea04e6c13e6150d48e0
932a845b27d5fb9ec78638a839ba5fb1
7f6263ccd71f05e5d3a7ca694ae513ad
8bd120acee67839d73ff6b1fea81b37a
7a372a2f85e9d2b6a3aebb63d8884080
c744a0435bce2fdcc6b05737321f8559
293b4729b8a619a2a2d2a2529e494925

6bd3ff14323c72bccbee75908cbaa899
04c640a5ff10f139738981372cbeb676
51b4527a31e5f4d89d0fed1c18b3199d
79e6d1e84be8742131b95cb94b94b4f5

Network Signatures

N/A

d. RATv3.ps

RATv3.ps - is a PowerShell remote access tool (RAT) or backdoor having the functionality to run commands, manipulate files, upload/download files from a C2 server, manipulate running processes, collect system information and manipulate the Windows registry.

Platform: N/A

Threat level: N/A

Category: Backdoor, remote-access-trojan

Other Name: PowerBrace

General information

- It communicates over TLS with a custom protocol using XOR encoding. Minor obfuscation occurs throughout the script, which makes it slightly more difficult to analyse. The script uses several light forms of obfuscation. Function names and variable names are replaced with non-descriptive names, and strings are stored as base64 encoded Unicode.
- This malware collects various operating system information and sends it to the C2 server. The collected data includes:

  - Internal IP address
  - Computer name
  - Username
  - OS version
  - OS architecture
  - Proxy status
  - Proxy server
  - Script path
  - Last boot time
  - OS caption
  - OS language
  - OS country code
  - Primary C2 address and port
  - Secondary C2 address and port
  - 32/64 bit system

Indicators of Compromise (IOCs)

CnC:

MD5:

b093a18d8de93a39f8d2cdc0fda06265

Network Signatures

N/A

e. Linux.Dacls

Linux.Dacls is a malicious remote-control software for OC Linux used by the Lazarus group.

Platform: Linux

Threat level: High

Category: remote-access-trojan

General information

- Its functions are modular, the C2 protocol uses two-layer TLS and RC4 encryption, the configuration file uses AES encryption and supports the dynamic update of C2 instructions. Linux.Dacls is compiled directly in the Bot program. It was found that Linux has 6 plugins: execution commands, file management, process management, test network access, C2 connection agent, network scan.
- The main functions of Linux.Dacls Bot include: execute commands, file management, process management, test network access, C2 connection agent, network scanning module

Indicators of Compromise (IOCs)

CnC:

162.241.217.135
www.areac-agr.com
http://www.areac-agr.com/cms/wp-content/uploads/2015/12/ldata.dat

MD5:

80c0efb9e129f7f9b05a783df6959812
859e7e9a11b37d355955f85b9a305fec

Network Signatures

N/A

f. MAC.Dacls

MAC.Dacls is a malicious remote-control software for macOS used by the Lazarus group.

Platform: macOS

Threat level: Middle

Category: remote-access-trojan

General information

Indicators of Compromise (IOCs)

CnC:
81f8f0526740b55fe484c42126cd8396
f05437d510287448325bac98a1378de1
b19984c67baee3b9274fe7d9a9073fa2
024e28cb5e42eb0fe813ac9892eb7cbe
MD5:
67.43.239.146
185.62.58.207

Network Signatures
N/A

g. Win32.Dacls

Win32.Dacls is malicious remote-control software for Windows which was used by Lazarus.

Platform: Windows

Threat level: High

Category: remote-access-trojan

General information

Its functions are modular, the C2 Protocol uses two-layer TLS and RC4 encryption, the configuration file uses AES encryption and supports dynamic updating of C2 instructions. Plug-in module Win32.Dacls is dynamically loaded via a remote URL.

Indicators of Compromise (IOCs)

CnC:
162.241.217.135
www.areac-agr.com
http://www.areac-agr.com/cms/wp-content/uploads/2015/12/rdata.dat
68.168.123.86
172.93.184.62

104.232.71.7
23.227.199.69

MD5:
44f15f1657a64423cb49ea317ce0c631
bea49839390e4f1eb3cb38d0fcaf897e
6a066cf853fe51e3398ef773d016a4a8
228998f29864603fd4966cadd0be77fc
da50a7a05abffb806f4a60c461521f41
ec05817e19039c2f6cc2c021e2ea0016
8910bdaaa6d3d40e9f60523d3a34f914

Network Signatures

TROJAN Possible DACLS RAT CnC (Log Server Reporting)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Possible DACLS RAT CnC (Log Server Reporting)"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"log=save&session_id="; http_client_body; depth:20; fast_pattern; content:"&value="; distance:0; http_client_body; pcre:"/^log=save&session_id=[^&]+&value=[^&]+$/P"; reference:url,blog.netlab.360.com/dacls-the-dual-platform-rat-en/; classtype:trojan-activity; sid:2029879; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_04_10, deployment Perimeter, former_category MALWARE, signature_severity Major, updated_at 2020_04_10, severity 3, ti_malware_id c75434dd3df9e41547cf58adb15fe91008f60740, ti_malware_name Win32.Dacls, malware_family Win32.Dacls, rule_origin etpro;)

h. VHD Ransomware

This crypto ransomware encrypts user data with AES-256 ECB + RSA-2048 and then demands a BTC ransom to get the files back.

Platform: N/A

Threat level: Low

Category: Ransomware

Other Names: N/A

General information

- The activity of this crypto-ransomware occurred in the second half of March 2020. Date stamp: March 19, 2020. It is aimed at English-speaking users, which does not prevent its distribution around the world.
- The ransom note is called: **HowToDecrypt.txt**
- Email addresses used:
  - johndoe2020@meet-me.live
  - johndoe2020@airmailhub.com
  - miclejaps@msgden[.]net
  - stevenjoker@msgden.net
- An extension is added to encrypted files: .vhd
- Experts note 2 features of this program:
  - The ransomware uses Mersenne Twister as a source of randomness, but unfortunately for the victims the RNG is reseeded every time new data is consumed.
  - VHD implements a mechanism to resume operations if the encryption process is interrupted. For files larger than 16MB, the ransomware stores the current cryptographic materials on the hard drive, in clear text. This information is not deleted securely afterwards, which implies there may be a chance to recover some of the files.

Indicators of Compromise (IOCs)

CnC:

MD5:
6D12547772B57A6DA2B25D2188451983
D0806C9D8BCEA0BD47D80FA004744D7D
DD00A8610BB84B54E99AE8099DB1FC20
CCC6026ACF7EADADA9ADACCAB70CA4D6
EFD4A87E7C5DCBB64B7313A13B4B1012

Network Signatures
N/A

i. PowerRatankba

PowerRatankba is a powerShell-based malware variant of «Ratankba», which used as a first stage reconnaissance tool and for the deployment of further stage implants on targets that are deemed interesting by the actor.

Platform: Windows

Threat level: High

Category: atm-malware

Other Names: Recon.PS

General information

Indicators of Compromise (IOCs)

CnC:

https://ecombox.store/tbl_add.php
ecombox.store
104.227.146.249
https://ecombox.store/tbl_add.php?action=bgetpsc
https://ecombox.store/tbl_add.php?action=cgetpsa
bodyshoppechiropractic.com
166.62.112.193
http://dreamlabs.net/dreamlabs.net
http://dreamlabs.net/logos.gif
https://dreamlabs.net/index.php?act=getps1
https://ecombox.store/tbl_add.php
https://bodyshoppechiropractic.com/tbl_add.php
http://51.255.219.82/files/download/falconcoin.zip
http://51.255.219.82/theme.gif
http://51.255.219.82/files/download/falconcoin.pdf
51.255.219.82
144.217.51.246
158.69.57.135
201.139.226.67
92.222.106.229
180.235.133.121
23.227.196.117

MD5:

79d09d46fd66085587afca579557bc89
50ca734bfba54ed33af469537b5e22c1
17f0f148f53968effcb42230518aeb67
8b51170fc6ecbea6b8496c8a8a8e4f1a
df934e2d23507a7f413580eae11bb7dc
34404a3fb9804977c6ab86cb991fb130
f34b72471a205c4eee5221ab9a349c55
636f8bd214d092ae3feb547599b4935e
eb30a58da33f1caca3a01e1467d6661c
c9ed87e9f99c631cda368f6f329ee27e
3c2f5ff382b0ec132101e92f72256490
a8b14ca96830d3b1d4d2f70b92d2d186
cb29db3900204071323a940c2a9434b8

9cee042ba1e447baf13eaeb9305f7280
5ad8143d954ebd5de6be0a40e0f65732
2025d91c1cdd33db576b2c90ef4067c7
563db5fc71da5f3bfc216aa3ec52f074
1f7897b041a812f96f1925138ea38c46
911de8d67af652a87415f8c0a30688b2
1507e7a741367745425e0530e23768e6
cb52c013f7af0219d45953bae663c9a2
18a451d70f96a1335623b385f0993bcc
9216b29114fb6713ef228370cbfe4045

SHA-256:
20d94f7d8ee2c4367443a930370d5685789762b1d11794810dc0ac6c626ad78e
41f155f039448edb42c3a566e7b8e150829b97d83109c0c394d199cdcfd20f9b
20f7e342a5f3224cab8f0439e2ba02bb051cd3e1afcd603142a60ac8af9699ba
db8163d054a35522d0dec35743cfd2c9872e0eb446467b573a79f84d61761471
3cd0689b2bae5109caedeb2cf9dd4b3a975ab277fadbbb26065e489565470a5c
b265a5d984c4654ac0b25ddcf8048d0aabc28e36d3e2439d1c08468842857f46
1768f2e9cea5f8c97007c6f822531c1c9043c151187c54ebfb289980ff63d666
99ad06cca4910c62e8d6b68801c6122137cf8458083bb58cbc767eebc220180d
f7f2dd674532056c0d67ef1fb7c8ae8dd0484768604b551ee9b6c4405008fe6b
d844777dcafcde8622b9472b6cd442c50c3747579868a53a505ef2f5a4f0e26a

Network Signatures
N/A

j. PowerTask

Backdoor of Lazarus group which was uploaded to VirusTotal on 29/03/2019 from Nigeria.

Platform: Windows

Threat level: High

Category: Backdoor

Other Names: N/A

General information

- Researched file "stage.ps1" was uploaded to VirusTotal on 29.03.2019 from Nigeria. This file is a PowerShell script. It has following functions:
  - Checks presence of connection with specified network node
  - Updates configuration parameters
  - Executes commands in Windows CLI
  - Creates new processes
  - Launches PowerShell commands
  - Deletes itself

- File doesn't contain C&C address. Executed commands are read by the script from the file. The name of the file is transmitted during the launch of the script. Based on these facts we may assume that other tool is used for communication with C&C. On the moment we didn't detect it.

Indicators of Compromise (IOCs)

CnC:

MD5:
ee664c219e8cf9a3ef6f9b7eb56f3c18
ae4e5917e3b4cf2e7c2457f411b66343
e186e60ab803d23d1cdf39c313cb34a4
c9b3b6bdc0cbb09f1ca5d4caab8bea9f

Network Signatures
N/A

k. HOPLIGHT

On infected systems, the malware collects information about the target's device and sends the data to a remote server. It can also receive commands from its command and control (C&C) server and execute various operations on infected hosts.

Platform:N/A

Threat level: Middle

Category: Backdoor

Other Names: N/A

General information

- HOPLIGHT can:
  - Read, write, and move files
  - Enumerate system drives
  - Create and terminate processes
  - Inject code into running processes
  - Create, start, and stop services
  - Modify registry settings
  - Connect to a remote host
  - Upload and download files
- The malware also uses a built-in proxy application to mask its communications with the remote command-and-control (C&C) server.

- The proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors.

Indicators of Compromise (IOCs)

CnC:

117.239.241.2
217.117.4.110
195.158.234.60
210.137.6.37
119.18.230.253
221.138.17.152

MD5:

3dbd47cc12c2b7406726154e2e95a403
2a791769aa73ac757f210f8546125b57
2ff1688fe866ec2871169197f9d46936
170a55f7c0448f1741e60b01dcec9cfb
e4ed26d5e2a84cc5e48d285e4ea898c0
23e27e5482e3f55bf828dab885569033
5c3898ac7670da30cf0b22075f3e8ed6
c5dc53a540abe95e02008a04a0d56d6c

Network Signatures

N/A

l. BISTROMATH

It is a full-featured Remote Access Trojan (RAT).

Platform: N/A

Threat level: Middle

Category: remote-access-trojan

General information

Indicators of Compromise (IOCs)

CnC:

159.100.250.231

MD5:

83833f8dbdd6ecf3a1212f5d1fc3d9dd

Network Signatures

N/A

m. SLICKSHOES

It is a dropper that decodes and drops the embedded file.

Platform: N/A

Threat level: Middle

Category: Dropper

General information

Indicators of Compromise (IOCs)

CnC:
188.165.37.168
MD5:
cca9fbb11c194fc53015185b741887a8
Network Signatures
N/A

n. CROWDEDFLOUNDER

Malware, which is designed to unpack and execute a Remote Access Trojan (RAT) binary in memory

Platform: Windows

Threat level: Middle

Category: Trojan,remote-access-trojan

General information

- This sample (MD5: f2b9d1cb2c4b1cd11a8682755bcc52fa) a Themida packed 32-bit Windows executable, which is designed to unpack and execute a Remote Access Trojan (RAT) binary in memory. This application is designed to accept arguments during execution or can be installed as a service with command line arguments. It is designed to listen as a proxy for incoming connections containing commands or can connect to a remote server to receive commands.

- When executed, the application is designed to open the Windows Firewall on the victim's machine to allow for incoming and outgoing connections from the victim system. The firewall is modified using a (netsh firewall add portopening) command.
- The following command line arguments are utilized to control the RAT functionality:
  -p: You can use the -p command line argument to force the malware to listen on a specific port. Example: malware.exe -p 8888
  -h: You can use the -h CLI to force the malware to connect to a remote host and port. Example: malware.exe -h <url_string>:8888

- The RAT uses a rotating exclusive or (XOR) cryptographic algorithm to secure its data transfers and command-and-control (C2) sessions. The malware is designed to accept instructions from the remote server to perform the following functions:

- Download and upload files
- Execute secondary payloads
- Execute shell commands
- Terminate running processes
- Delete files
- Search files
- Set file attributes
- Collect device information from installed storage devices (disk free space and their type)
- List running processes information
- Collect and send information about the victim's system
- Securely download malicious DLLs and inject them into remote processes

Indicators of Compromise (IOCs)
CnC:

MD5:
f2b9d1cb2c4b1cd11a8682755bcc52fa
Network Signatures
N/A

o. HOTCROISSANT

This is the full-featured implant for reconnaissance, uploading/dowloading files and executing commands

Platform: N/A

Threat level: Middle

Category: Trojan

General information

- Sample (MD5: 062e9cd9cdcabc928fc6186c3921e945), detected by experts, is a full-featured beaconing implant. his sample performs a custom XOR network encoding and is capable of many features including conducting system surveys, file upload/download, process and command execution, and performing screen captures.
- The sample performs dynamic DLL importing and API lookups using LoadLibrary and GetProcAddress on obfuscated strings in an attempt to hide it's usage of network functions. However, only a small number of API calls are obfuscated this way, and their selection is not consistent through the sample.
- The sample obfuscates strings used for API lookups as well as the strings used during the network handshake using a simple Byte xor with 0x0f.

- The sample attempts to connect to a hardcoded C2 IP and then immediately sends it's Victim Info. It then listens for commands from the C2 and returns the results. Network communications are first zipped and then encoded with a custom xor algorithm.

Indicators of Compromise (IOCs)

CnC:
94.177.123.138

MD5:
062e9cd9cdcabc928fc6186c3921e945

Network Signatures
N/A

p. ARTFULPIE

An implant that performs downloading and in-memory loading and execution of a DLL from a hardcoded URL

Platform: N/A

Threat level: Middle

Category: Loader

General information

- An implant (MD5: 2d92116440edef4190279a043af6794b) that performs downloading and in-memory loading and execution of a DLL from a hardcoded URL.
- Downloads the hardcoded URL hxxp[:]//193[.]56[.]28[.]103:88/xampp/thinkmeter[.]dll into memory using the user-agent string: "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)".
- Loads the .dll into its own address space manually (fully in memory).
- Calls the .dll's entry-point.

Indicators of Compromise (IOCs)

CnC:
193.56.28.103

MD5:
2d92116440edef4190279a043af6794b

Network Signatures
N/A

q. BUFFETLINE

A tool, which is used for uploading/downloading, deleting and executing files, accessing the Windows command-line interface, creating and process completion

Platform: Windows

Threat level: Middle

Category: Trojan

General information

- A sample (MD5: 11cb4f1cdd9370162d67945059f70d0d) is a full-featured beaconing implant. This sample uses PolarSSL for session authentication, but then utilizes a FakeTLS scheme for network encoding using a modified RC4 algorithm. It has the capability to download, upload, delete, and execute files; enable Windows CLI access; create and terminate processes; and perform target system enumeration.
- The sample performs dynamic DLL importing and API lookups using LoadLibrary and GetProcAddress on obfuscated strings in an attempt to hide it's usage of network functions.
- The sample obfuscates strings used for API lookups as well as the strings used during the network handshake using a modified RC4 algorithm. A Python 3 script to decrypt the obfuscated strings is given below. Note: The hardcoded command and control (C2) IP's are not obfuscated, but appear in plaintext within the executable.
- The sample attempts to perform a PolarSSL handshake to initiate a connection to each of these hardcoded C2 IPs using TLS version 1.1. It uses the PolarSSL server_name extension with the Server Name set to «!Q@W#E$R%T^Y&U*I(O)P».
- After the TLS authentication is completed this particular sample does NOT use the session key that is generated via TLS. Instead, it uses a FakeTLS scheme, where a 'fake' TLS packet header is prepended to the packet data which is encrypted with custom xor encryption scheme
- After the TLS authentication, the sample performs a handshake with the C&C, where hardcoded 32 Byte strings are exchanged, as well as a Victim ID and the Victim Internal IP. After this exchange, the implant sends it's Victim Information, and then waits for tasking from the C&C.

Indicators of Compromise (IOCs)

CnC:

107.6.12.135
210.202.40.35

MD5:

11cb4f1cdd9370162d67945059f70d0d

Network Signatures

N/A

r. KEYMARBLE

Trojan such as Remote Access Trojan (RAT), which is used to attack hackers from the group Lazarus

Platform: Windows

Threat level: Middle

Category: Trojan

General information

- This RAT uses a customized XOR cryptographic algorithm to secure its data transfers and command-and-control (C2) sessions. It is designed to accept instructions from the remote server to perform the following functions:
  - Download and upload files
  - Execute secondary payloads
  - Execute shell commands
  - Terminate running processes
  - Delete files
  - Search files
  - Set file attributes
  - Create registry entries for storing data:(HKEY_CURRENT_USER\SOFTWARE\Microsoft\WABE\DataPath)
  - Collect device information from installed storage devices (disk free space and their type)
  - List running processes information
  - Capture screenshots
  - Collect and send information about the victim's system (operating system, CPU, MAC address, computer name, language settings, list of disk devices and their type, time elapsed since the system was started, and unique identifier of the victim's system)

Indicators of Compromise (IOCs)

CnC:
222.143.21.13
104.194.160.69
100.43.153.60
http://37.238.135.70/img/anan.jpg
37.238.135.70
194.45.8.41
104.194.160.59

MD5:
1ce252b7bf2bca58266ae89d79c19144

50bc6970fd8a8594bad6c64dd8b80a01
3e925fb44f6d408e9f0f52cc8f0be2b4
d8e51f1b9f78785ed7449145b705b2e4
b1091ee2a5af5e9f9aa0b9e57ab4cc41
cf6fb91589af0951f34bad0785bec4c1
dc3fff0873c3e8e853f6c5e01aa94fcf
6526e4b8c5dd407382300497f974be37
704d491c155aad996f16377a35732cb4

SHA-1:
7C55572E8573D08F3A69FB15B7FEF10DF1A8CB33
E7FDEAB60AA4203EA0FF24506B3FC666FBFF759F
18EA298684308E50E3AE6BB66D7321A5CE664C8E
8826D4EDBB00F0A45C23567B16BEED2CE18B1B6A

Network Signatures
N/A

s. Dtrack

This spyware was created by the Lazarus group and is being used to upload and download files to victims' systems, record key strokes and conduct other actions typical of a malicious remote administration tool (RAT).

Platform: N/A

Threat level: High

Category: Backdoor, remote-access-trojan

General information

A list of features is provided in the table below.

- upload a file to the victim's computer
- make target file persistent with auto execution on the victim's host start
- download a file from the victim's computer
- dump all disk volume data and upload it to a host controlled by criminals
- dump a chosen disk volume and upload it to a host controlled by criminals
- dump a chosen folder and upload it to a host controlled by criminals
- set a new interval timeout value between new command checks
- exit and remove the persistence and the binary itself
- default execute a process on the victim's host

Indicators of Compromise (IOCs)

CnC:

http://www.totalmateria.net/wp/profile2.php
www.totalmateria.net
http://www.materialindia.in/wp/wp-main/gallery/profile2.php
www.materialindia.in
http://10.0.3.254/software.php
10.0.3.254
http://katawaku.jp/bbs/data/theme/profile2.php
http://10.44.0.2/openldap/scripts/profile.php
10.44.0.2
http://gamestoyshop.us/ocart2/catalog/demo/provision.php
gamestoyshop.us
51.91.7.156
http://newshoesfasion.com/oscom/private/identity.php
newshoesfasion.com
158.69.114.83
http://heromessi.com/wp-public/career/car_add.php
heromessi.com
http://hawai-tour.com/wp/wp-imgs/luxury/scenes/view.php
hawai-tour.com
http://www.trendshow.xyz/wp/wp-admin/control/
www.trendshow.xyz
http://eshopt.freeoda.com/phpBB3/phpbb/php/config/
eshopt.freeoda.com
10.6.139.114
http://www.trendshow.xyz/wp/wp-template/

MD5:

f84de0a584ae7e02fb0ffe679f96db8d
3a3bad366916aa3198fd1f76f3c29f24
8f360227e7ee415ff509c2e443370e56
8fa49304e4de43c4b36f3e584752ffa9
80c98421cb53136f6f1bcde66c6a37e6
37362c2aa8742e22480892bd181093af
ebb52f45ff1483e82ff3258b7f086571
b9c6bfcf59c8240f4909e2fc163d79e0
2ebb3e170dfeda090c6f94ea81bdc155
68509263aff6f44a5c2ce28c23f5672b
15db4ca9c33afdd667577ac57ccb1ce3
b133080935dc01e3b8ec3e2410e52945
a03a344484300687992152c5f1bd2fea

Network Signatures

N/A

t. Dtrack.Stealer

The application code is based on the source code of Dtrack.Backdoor. The "1007" command of the Trojan Dtrack.Backdoor dumps all disk volume data to a file and uploads it to a host controlled by criminals. The stealer performs the similar actions.

Platform: N/A

Threat level: Middle

Category: Infostealer

Indicators of Compromise (IOCs)

CnC:
172.22.22.156
10.2.114.1
172.22.22.5
10.2.4.1
10.2.114.9
http://10.2.114.9/cgibin/lib/dbc/func.php

MD5:
4f8091a5513659b2980cb53578d3f798
a1d103ae93c8b7cba0ea5b03d0bd2d9d

Network Signatures
N/A

u. BADCALL

BADCALL is composed of three separate files, the first two are Windows executables designed to disable the firewall (by modifying a registry key) and transform infected systems into proxy servers. They, too, disguise malicious C2 communications as encrypted HTTPS traffic, but in actuality they encrypt their activity using a rudimentary cipher (XOR/ADD and SUB/XOR, respectively). The third file is an Android Package Kit (APK) file designed to run on Android platforms as a fully functioning Remote Access Tool (RAT).

Platform: Android

Threat level: Middle

Category: remote-access-trojan

General information

The Trojan has the following functions of a backdoor:

- Record the microphone
- Capture from the camera
- Upload, execute, and manipulate local files
- Download remote files
- Record GPS information
- Read contact information
- Observe SMS or MMS messages
- Record web browsing history and bookmarks
- Scan and capture WiFi information

Indicators of Compromise (IOCs)

CnC:

MD5:
12cc14bbbc421275c3c6145bfa186dff
150cc194e43a661288a43a422212dc3e
3ad421c887aee54527b22844baeabbfe
763f0e57113d5855bafafc03c15f5b8f
d93b6a5c04d392fc8ed30375be17beb4

Network Signatures
N/A

v. Electricfish

Electricfish is a malware variant that targets Windows systems and is used by the advanced persistent threat Lazarus Group, attributed to North Korea. The malware contained a custom protocol that permits traffic to be funneled between source IP and destination IP addresses, allowing traffic to travel through proxies to outside a victim network, bypassing authentication requirements. This can be used by attackers to covertly exfiltrate data and stay hidden in the network.

Platform: Windows

Threat level: N/A

Category: tunneling-tool

Indicators of Compromise (IOCs)

CnC:

MD5:
df934e2d23507a7f413580eae11bb7dc
41030182de3899cded5531fb0dad5a78
f9ced93b94c8c8a8c0de20028300e11d
8d9123cd2648020292b5c35edc9ae22e
fa51d3b55296436ad91099bc6fb13c9f
63440d2ba41916c5cb9f0f91f4c82b5a
ee54ae8df7b969c4fd6ffda465eeddd4
0ba6bb2ad05d86207b5303657e3f6874
22082079ab45ccc256e73b3a7fd54791

Network Signatures

TROJAN Win32/ElectricFish Authentication Packet Observed

alert tcp $HOME_NET any -> any any (msg:"TROJAN Win32/ElectricFish Authentication Packet Observed"; target:src_ip; flow:established,to_server; content:"aaaabbbbccccdddd|00 00 00 00 00 00 00 00|"; depth:24; fast_pattern; content:"|00 00 04 00 00 00|"; distance:2; within:6; reference:url,www.us-cert.gov/ncas/analysis-reports/AR19-129A; classtype:trojan-activity; sid:2027340; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, created_at 2019_05_09, deployment Perimeter, deployment Internal, former_category TROJAN, performance_impact Low, signature_severity Major, tag APT, tag T1090, tag connection_proxy, updated_at 2019_05_09, severity 3, ti_malware_id b44769790886c8833ba893d8927ff6c79108a51c, ti_malware_name Electricfish, malware_family Electricfish, rule_origin etpro;)

w. RATv3.ps

RATv3.ps - is a PowerShell remote access tool (RAT) or backdoor having the functionality to run commands, manipulate files, upload/download files from a C2 server, manipulate running processes, collect system information and manipulate the Windows registry.

Platform: Windows

Threat level: High

Category: Backdoor, remote-access-trojan

General information

It communicates over TLS with a custom protocol using XOR encoding. Minor obfuscation occurs throughout the script, which makes it slightly more difficult to analyse. The script uses several light forms of obfuscation. Function names and variable names are replaced with non-descriptive names, and strings are stored as base64 encoded Unicode.

This malware collects various operating system information and sends it to the C2 server. The collected data includes:

- Internal IP address
- Computer name
- Username
- OS version
- OS architecture
- Proxy status
- Proxy server
- Script path
- Last boot time
- OS caption
- OS language
- OS country code
- Primary C2 address and port
- Secondary C2 address and port
- 32/64 bit system

Indicators of Compromise (IOCs)
CnC:

MD5:
b12325a1e6379b213d35def383da2986
aff88674d2869f79f9c6d5ecf5fc2d63
1e2795f69e07e430d9e5641d3c07f41e
3be75036010f1f2102b6ce09a9299bca
b88d4d72fdabfc040ac7fb768bf72dcd
7c651d115109fd8f35fddfc44fd24518

25376ea6ae0903084c45bf9c57bd6e4f
8a41520c89dce75a345ab20ee352fef0

Network Signatures

N/A

x. Rising Sun

this is a full-featured modular backdoor that conducts reconnaissance on the victim's network.

Platform: N/A

Threat level: High

Category: Backdoor

General information

It was found that Rising Sun is based on the Duuzer Trojan family, which also belongs to cybercriminals from the Lazarus group.

The Rising Sun has 14 backdoor options:

- Execute commands
- Get disk information
- Disc type
- Total bytes on disk
- Total free bytes on disk
- Name of the specified volume
- Run a process from a binary Windows
- Get information about processes
- End the process
- Get file time
- Read file
- Clear process memory
- Burn file to disk
- Delete file
- Getting more information about files in a directory
- Connect to IP address
- Change file attributes

Indicators of Compromise (IOCs)

CnC:

MD5:

f3bd9e1c01f2145eb475a98c87f94a25

Network Signatures
N/A

y. KillDisk

KillDisk is a hard drive eraser software for secure formatting of hard drives without any possibility of following data recovery.

Platform: N/A

Threat level: N/A

Category: Trojan, wiper

Indicators of Compromise (IOCs)

CnC:

MD5:
c1831baa5505f5a557380e0ab3f60f48
571de903333a6951b8875a73f6cf99c5
ffb72166c7f715be6fa23cbbd3111bde
02ba51012af4fb59f3742e21dab90b80

Network Signatures
N/A

z. PowerSpritz

PowerSpritz is a Windows executable that hides both its valid payload and malicious PowerShell command using a custom implementation of the now rarely used Spritz encryption algorithm.

Platform: N/A

Threat level: N/A

Category: dropper

General information

Indicators of Compromise (IOCs)

CnC:
https://doc-00-64-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/39cbphg8k5qve4q5rr6nonee1bueiu8o/1499428800000/13030420262846080952/*/0B63J1WTZC49hX1JnZUo4Y1pnRG8?e=download
https://drive.google.com/uc?export=download&id=0B63J1WTZC49hdDR0clR3cFpITVE

http://201.211.183.215:8080/update.php?t=Skype&r=update
http://122.248.34.23/Index.php?t=SkypeSetup&r=mail_new
http://122.248.34.23/Index.php?t=Telegram&r=1.1.9
http://dogecoin.deaftone.com:8080/mainls.cs
dogecoin.deaftone.com
http://macintosh.linkpc.net:8080/mainls.cs
macintosh.linkpc.net
http://skype.2.vu/1
104.236.48.227
telegramupdate.2.vu
skypeupdate.2.vu
http://skypeupdate.2.vu/1

MD5:
26466867557f84dd4784845280da1f27

SHA-256:
cbebafb2f4d77967ffb1a74aac09633b5af616046f31dddf899019ba78a55411
9ca3e56dcb2d1b92e88a0d09d8cab2207ee6d1f55bada744ef81e8b8cf155453
5a162898a38601e41d538f067eaf81d6a038268bc52a86cf13c2e43ca2487c07

Network Signatures
N/A

aa. Joanap

Joanap is a fully functional RAT that can receive multiple commands that can be set remotely from a management server. Joanap usually infects the system as a file downloaded by other malware that users unknowingly downloaded either when visiting sites compromised by hackers or when opening malicious email attachments. Joanap gives cybercriminals the ability to expand data, load and run additional payloads, initialize proxy connections on a compromised Windows device, manage files and processes, create and delete directories, and manage nodes.

Platform: N/A

Threat level: N/A

Category: remote-access-trojan

General information

Indicators of Compromise (IOCs)

CnC:
110.164.115.177

118.102.187.188
118.70.143.38
119.15.245.179
122.55.13.34
168.144.197.98
189.114.147.186
196.44.250.231
201.222.66.25
60.251.197.122
62.135.122.53
62.150.4.42
62.87.153.243
63.131.248.197
63.149.164.98
64.71.162.61
66.210.47.247
69.15.198.186
72.156.127.210
75.145.139.249
78.38.221.4
80.191.114.136
81.130.210.66
81.83.10.138
83.211.229.42
92.253.102.217
92.47.141.99
93.62.0.22
94.28.57.110
96.39.78.157

MD5:
298775B04A166FF4B8FBD3609E716945
4613f51087f01715bf9132c704aea2c2
fd59af723b7a4044ab41f1b2a33350d6
074dc6c0fa12cadbc016b8b5b5b7b7c5
27a3498690d6e86f45229acd2ebc0510
7a83c6cd46984a84c40d77e9acff28bc
1d8f0e2375f6bc1e045fa2f25cd4f7e0
304cea78b53d8baaa2748c7b0bce5dd0
a1ad82988af5d5b2c4003c42a81dda17

SHA-256:
29b8c57226b70fc7e095bb8bed4611d923f0bcefc661ebae5182168613b497f8

66d44e2bc7495662d068051c5a687d17c7e95c8f04acb0f06248b34cd255cd25
fae77c173815b561ad02d8994d0e789337a04d9966dd27a372fd9055f1ac58b1
c1c56c7eb2f6b406df908ae822a6ea936f9cc63010ee3c206186f356f2d1aa94
4c5b8c3e0369eb738686c8a111dfe460e26eb3700837c941ea2e9afd3255981e
113d705d7736c707e06fb37ac328080b3976838d0a7b021fd5fb299896c22c7c
1a6c3e5643d7e22554ac0a543c87a2897ea4ea5a07bc080943a310a391e20713
0b860af58a9d2d7607f09022aa69508b0966a1cc8d953d3995a5fe07f8fabcac
5d73d14525ced5bdf16181f70f4d931b9c942c1ae16e318517d1cd53f4cd6ea9
c34ad273d836b2f058bbd73ea9958d272bd63f4119dacacc310bf38646ff567b
500c713aa82a11c4c33e9617cad4241fcef85661930e4986c205233759a55ae8
5f5acf76a991c1ca33855a96ec0ac77092f2909e0344657fe3acf0b2419d1eea
c6d96be46ce3d616e0cb36d53c4fade7e954e74bfd2e34f9f15c4df58fc732d2
d558bb63ed9f613d51badd8fea7e8ea5921a9e31925cd163ec0412e0d999df58
006e0cc29697db70b2d4319f320aa0e52f78bf876646f687aa313e8ba04e6992
2d9edf45988614f002b71899740d724008e9a808efad00fa79760b31e0a08073
3d2a7ea04d2247b49e2dcad63a179ae6a47237eddbfd354082f1417a63e9696e
ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
f4113e30d50e0afc4fa610a3181169bb03f6766aea633ed8c0c0d1639dfc5b29
08203b4ddc9571418b2631ebbc50bea57a00eadf4d4c28bd882ee8e831577a19
a3992ed9a4273de53950fc55e5b56cc5b1327ffee59b1cea9e45679adc84d008
575028bbfd1c3aaff27967c9971176ae7038902f1a67d70def55ae8456e6166d
428cf6ec1a4c947b51ec099a656f575ce42f67737ee53f3afc3068a25adb4c0d
f53e3e0b3c524471b1f064aabd0f782802abb4e29534a1b61a6b25ad8ec30e79

Network Signatures

N/A

bb. Brambul

Brambul is a malicious SMB worm for 32-bit Windows that functions as a dynamic library service file or portable executable file that is frequently downloaded and installed on the victim's network by droppers. When executed, the malware attempts to contact victim systems and IP addresses on the local subnets of the victims. If successful, the application tries to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching a brute force attack using a list of available passwords. In addition, the malware generates random IP addresses for further attacks.

Platform: N/A

Threat level: N/A

Category: remote-access-trojan

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
e86c2f4fc88918246bf697b6a404c3ea
1c532fad2c60636654d4c778cfe10408
1db2dced6dfa04ed75b246ff2784046a
3844ec6ec70347913bd1156f8cd159b8
40878869de3fc5f23e14bc3f76541263
95a5f91931723a65dcd4a3937546da34
99d9f156c73bd69d5df1a1fe1b08c544
a1ad82988af5d5b2c4003c42a81dda17
ca4c2009bf7ff17d556cc095a4ce06dd
f273d1283364625f986050bdf7dec8bb

Network Signatures
N/A

cc. BrowserPasswordDump

Browser Password Dump is the free command-line (cmd.exe) version of Browser Password Decryptor. This shady tool serves the purpose of recovering passwords from popular web browsers through cmd.exe.

Platform: Windows

Threat level: N/A

Category: N/A

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
e74047ca6798423e47096c77efb0ca1d

Network Signatures
N/A

dd. HARDRAIN

HARDRAIN is composed three malicious executable files. The first two are 32-bit, Windows-based dynamic link library (DLL) executables, which configure the Windows Firewall to allow incoming connections, thus allowing machines to function as proxies. Illicit communications

are masked as HTTPS sessions by leveraging public certificates sourced from legitimate Internet services. In reality, however, the traffic is actually encrypted using an unidentified algorithm. Accompanying these two DLL files is an Android-based Executable Linkable Format (ELF) file that connects to hard-coded Internet Protocol (IP) addresses and acts as a RAT program.

Platform: Android

Threat level: Middle

Category: remote-access-trojan

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
9ce9a0b3876aacbf0e8023c97fd0a21d
8b98bdf2c6a299e1fde217889af54845
24f61120946ddac5e1d15cd64c48b7e6

Network Signatures
N/A

ee. Gh0st

Gh0st is a well-known Chinese RAT used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth. Gh0st presumably was made by. C.Rufus Security Team, source code is publicly available since 2011.

Platform: Windows

Threat level: High

Category: RAT

Other Name: Ghost, Gh0st RAT

General information

Gh0st is a well-known Chinese RAT used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth. Gh0st presumably was made by. C.Rufus Security Team, source code is publicly available since 2011.

Indicators of Compromise (IOCs)

CnC:
http://180.235.133.235/img.gif
http://180.235.133.121/images/img.gif

MD5:

Network Signatures

Win32.Trojan.PCRat/Gh0st Beacon

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan.PCRat/Gh0st Beacon"; target:src_ip; flow:established,to_server; content:"greater!"; depth:8; threshold:type limit, track by_src, seconds 360, count 1; classtype:backdoor; reference:md5,44e65266280b6ab1832dc1bc24ea5a40; sid:1002066; rev:1; metadata:severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin gib;)

TROJAN [CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN [CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon"; target:src_ip; flow:established, to_server; content:"Adobe"; depth:5; content:"|e0 00 00 00 78 9c|"; distance:4; within:15; reference:url,blog.crowdstrike.com/whois-anchor-panda/index.html; classtype:backdoor; sid:2016656; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2013_03_22, deployment Perimeter, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, malware_family Panda, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 23

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 23"; target:src_ip; flow:to_server,established; dsize:>11; content:"|78 9c|"; offset:8; byte_jump:4,-18,relative,little,from_beginning, post_offset 1; isdataat:!2,relative; pcre:"/^.{8}[\x20-\x7e]+?.{2}\x78\x9c/s"; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; reference:md5,db1c4342f617798bcb2ba5655d32bf67; classtype:backdoor; sid:2018075; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_02_05, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Gh0st_Apple Checkin

alert http $HOME_NET any -> $EXTERNAL_NET 110 (msg:"TROJAN Gh0st_Apple Checkin"; target:src_ip; flow:to_server,established; content:"GET"; http_method; content:".gif?pid"; fast_pattern; content:"&v="; content:"Mozilla/4.0("; http_user_agent; reference:url,contagiodump.blogspot.com.br/2013/09/sandbox-miming-cve-2012-0158-in-mhtml.html; reference:md5,82644661f6639c9fcb021ad197b565f7; classtype:backdoor; sid:2017412; rev:8; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2013_09_03, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Gh0st Trojan CnC 2

alert tcp $HOME_NET any -> $EXTERNAL_NET !25 (msg:"TROJAN Gh0st Trojan CnC 2"; target:src_ip; flow:established,to_server; dsize:<250; content:"Gh0st"; offset:8; depth:5; classtype:backdoor; sid:2017505; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2013_09_20, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12 SET

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12 SET"; target:src_ip; flow:to_server,established; dsize:8; content:"|00 00|"; offset:2; depth:2; content:"|00 00|"; distance:2; within:2; flowbits:set,ET.gh0stFmly; flowbits:noalert; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; reference:md5,3b1abb60bafbab204aeddf8acdf58ac9; classtype:backdoor; sid:2017935; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_01_06, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01,

severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 15

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 15"; target:src_ip; flow:to_server,established; dsize:>11; content:"FWKJGH"; offset:8; depth:6; byte_jump:4,0,little,from_beginning,post_offset 5; isdataat:!2,relative; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; reference:md5,edd8c8009fc1ce2991eef6069ae6bf82; classtype:backdoor; sid:2017974; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_01_16, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 17

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 17"; target:src_ip; flow:to_server,established; dsize:>11; content:"AngeL"; depth:5; byte_jump:4,0,relative,little,from_beginning,post_offset -1; isdataat:!2,relative; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; classtype:backdoor; sid:2018007; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_01_23, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server"; target:src_ip; flow:established,to_server; dsize:100<>300; content:"Gh0st"; depth:5; reference:url,www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; reference:url,www.symantec.com/connect/blogs/inside-back-door-attack; classtype:backdoor; sid:2013214; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2011_07_06, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 5

alert tcp $HOME_NET any -> $EXTERNAL_NET [!5800] (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 5"; target:src_ip; flow:to_server,established; dsize:>11; content:"|78 9c|"; fast_pattern; byte_jump:4,0,little,post_offset 1; isdataat:!2,relative; byte_extract:4,0,compressed_size,little; byte_test:4,>,compressed_size,4,little; pcre:"/^.{8}[\x20-\x7e]+?[\x00]*?\x78\x9c/s"; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; classtype:backdoor; sid:2017876; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2013_12_17, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2019_10_07, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

ff. WannaCry

WannaCry, originally named as WanaCrypt, having aliases of Wana Crypt0r and Wana Decrypt0r, is a ransomware wormon Microsoft Windows (can be run on Linux via WINE) that uses two NSA-leaked tools that has wreaked havoc in airports, banks, universities, hospitals and many other facilities. It has spread to some 150 countries worldwide, mainly Russia, Ukraine, and India. .

Platform: Windows

Threat level: High

Category: Ransomware

General information

On 12/05/2017, 2017 widespread use of ransomware WannaCry Cryptor that affects Microsoft Windows systems was observed. This ransomware has the behaviour of a worm and was spreader using exploit ETERNALBLUE. It scanned network and infected each vulnerable machine. Thus, great number of systems were infected in 11 countries during two hours: Russia, Great Britain, USA, China, Spain, Italy, Vietnam, Taiwan. Big corporations and companies were affected. The threat actor is asking for $ 300 in Bitcoins to restore access to the files.

Security researches @MalwareTechBlog and Darien Huss (Proofpoint) established that the switch was hardcoded into the malware in case the creator wanted to stop it spreading. This involved a very long nonsensical domain name that the malware makes a request to – just as if it was looking up any website – and if the request comes back and shows that the domain is live, the kill switch takes effect and the malware stops spreading. This domain was unregistered, so researcher registered it in himself and stop spreading.

In addition, on 12/05/2017 Microsoft released patch for unsupported systems to fix this vulnerability.

Indicators of Compromise (IOCs)

CnC:
85.248.227.164
194.109.206.212
217.79.190.25
204.11.50.131
95.183.48.12
171.25.193.9
195.154.164.243
131.188.40.189
5.9.159.14
199.254.238.52
178.16.208.57
128.31.0.39
163.172.35.247
154.35.175.225
iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

104.17.37.137
104.17.38.137
104.17.39.137
104.17.40.137
104.17.41.137
212.51.134.123
5.199.142.236
197.231.221.221
149.202.160.69
46.101.166.19
91.121.65.179
2.3.69.209
146.0.32.144
50.7.161.218
87.101.243.252
184.74.243.67
203.69.210.247

MD5:
6f0338af379659a5155b3d2a4f1a1e92
3bc855bfadfea71a445080ba72b26c1c
f27cf59b00dacdd266ad7894a1df0894

Network Signatures

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:ransomware; sid:2024298; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2019_10_07, severity 5, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3"; target:src_ip; flow:established,to_server; content:"ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf"; http_header; fast_pattern; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:ransomware; sid:2024300; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2019_10_07, severity 5, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024299; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18, severity 3, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024301; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18, severity 3, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 5

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 5"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024302; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18, severity 3, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN Possible WannaCry DNS Lookup 1

alert dns $HOME_NET any -> any any (msg:"TROJAN Possible WannaCry DNS Lookup 1"; target:src_ip; dns_query; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; depth:41; nocase; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:ransomware; sid:2024291; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_12, deployment Perimeter, former_category TROJAN, signature_severity Critical, tag Ransomware, updated_at 2020_08_20, severity 5, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

gg. DoublePulsar

DoublePulsar is a backdoor developed by Equation Group (Presumably, this group is part of ANB) that was leaked by The Shadow Brokers in early 2017. DoublePulsar can be classified as a "stager" - an implant that first gets on the infected device and serves to install other implants.

Platform: N/A

Threat level: High

Category: Backdoor

General information

Indicators of Compromise (IOCs)

CnC:

MD5:

Network Signatures

EXPLOIT Possible DOUBLEPULSAR Beacon Response

alert smb $HOME_NET any -> any any (msg:"EXPLOIT Possible DOUBLEPULSAR Beacon Response"; target:src_ip; flow:from_server,established; content:"|00 00 00 23 ff|SMB2|02 00 00 c0 98 07 c0 00 00|"; depth:18; content:"|00 00 00 08 ff fe 00 08|"; distance:8; within:8; fast_pattern; pcre:"/^[\x50-\x59]/R"; content:"|00 00 00|"; distance:1; within:3; isdataat:!1,relative; classtype:ek-activity; sid:2024216; rev:1; metadata:attack_target SMB_Server, created_at 2017_04_17, deployment Internal, former_category EXPLOIT, signature_severity Critical, updated_at 2019_09_28, severity 3, ti_malware_id c7c12af404eff6f639799e6b103044f1aa0d7357, ti_malware_name DoublePulsar, malware_family DoublePulsar, rule_origin etpro;)

EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication

alert tcp any any -> $HOME_NET 445 (msg:"EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication"; target:src_ip; flow:to_server, established; content:"|FF|SMB2|00 00 00 00|"; depth:9; offset:4; byte_test:2,!=,0x0000,52,relative,little; pcre:"/^.{52}(?:\x04|\x09|\x0A|\x0B|\x0C|\x0E|\x11)\x00/R"; reference:url,github.com/ptresearch/AttackDetection; classtype:attempted-admin; sid:2024766; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target SMB_Server, created_at 2017_09_25, deployment Internet, former_category EXPLOIT, performance_impact Low, signature_severity Major, updated_at 2017_09_28, severity 1, ti_malware_id c7c12af404eff6f639799e6b103044f1aa0d7357, ti_malware_name DoublePulsar, malware_family DoublePulsar, rule_origin etpro;)

hh.Volgmer

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, Lazarus Group (aka Hidden Cobra) actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries. It is a Destover-related backdoor and has several capabilities including: gathering system information, updating service registry keys, downloading and uploading files, executing commands, terminating processes, and listing directories. Also, a botnet controller functionality was discovered in one of the known samples. The malware communicates with its C&C server either through a custom binary protocol via TCP port 8080 or 8088 or by implementing Secure Socket Layer (SSL) encryption.

Platform: Windows

Threat level: High

Category: Backdoor

General information

Gather system information
Update service registry keys
Download and upload files
Execute commands
Terminate processes
List directories
Control botnets

Successful network intrusion could result in the following impacts:

Temporary or permanent loss of sensitive or proprietary information,
Disruption to regular operations,
Financial losses incurred to restore systems and files, and
Potential harm to an organization's reputation.

Indicators of Compromise (IOCs)

CnC:

103.16.223.35
113.28.244.194
116.48.145.179
186.116.9.20
186.149.198.172
195.28.91.232
195.97.97.148
199.15.234.120
200.42.69.133
203.131.222.99
210.187.87.181
83.231.204.157
84.232.224.218
89.190.188.42
199.68.196.125
103.27.164.42
112.133.214.38
114.79.141.59
115.115.174.67
115.178.96.66
115.249.29.78
117.211.164.245
117.218.84.197
117.239.102.132
117.239.144.203
117.240.190.226
117.247.63.127
117.247.8.239
118.67.237.124
125.17.79.35
125.18.9.228
14.102.46.3
14.139.125.214
14.141.129.116

180.211.97.186
182.156.76.122
182.72.113.90
182.73.165.58
182.73.245.46
182.74.42.194
182.77.61.231
183.82.199.174
183.82.33.102
203.110.91.252
116.90.226.67
113.203.238.98
115.186.133.195
182.176.121.244
182.187.139.132
37.216.67.155
84.235.85.86
103.241.106.15
203.118.42.155
58.185.197.210
61.91.47.142
185.134.98.141
109.68.120.179
85.132.123.50
80.95.219.72
88.201.64.185
103.10.55.35
45.124.169.36
222.44.80.138
61.153.146.207
41.131.164.156
82.129.240.148
82.201.131.124
31.146.82.22
103.27.164.10
203.196.136.60
203.88.138.79
43.249.216.6
45.118.34.215
139.255.62.10
128.65.184.131
128.65.187.94
178.248.41.117

185.113.149.239
185.115.164.86
185.46.218.77
213.207.209.36
217.218.90.124
217.219.193.158
217.219.202.199
37.235.21.166
37.98.114.90
78.38.114.15
78.38.182.242
78.39.125.67
80.191.171.32
85.185.30.195
85.9.74.159
89.165.119.105
91.106.77.7
91.98.112.196
91.98.126.92
91.98.36.66
94.183.177.90
95.38.16.188
27.114.187.37
123.231.112.147
222.165.146.86
122.146.157.141
140.136.205.209
110.77.137.38
118.175.22.10
125.25.206.15
203.147.10.65
58.82.155.98
117.239.214.162
12.217.8.82
123.176.38.17
123.176.38.175
134.121.41.45
190.210.39.16
200.42.69.13
206.123.66.136
206.163.230.170
212.33.200.86
213.207.142.82

220.128.131.251
24.242.176.130
41.21.201.101
64.3.218.243
78.93.190.70
89.122.121.230
200.87.126.116
194.224.95.20
121.170.194.185
222.236.46.5

MD5:

2D2B88AE9F7E5B49B728AD7A1D220E84
9A5FA5C5F3915B2297A1C379BE9979F0
BA8C717088A00999F08984408D0C5288
1B8AD5872662A03F4EC08F6750C89ABC
E034BA76BEB43B04D2CA6785AA76F007
EB9DB98914207815D763E2E5CFBE96B9
143cb4f16dcfc16a02812718acd32c8f
1ecd83ee7e4cfc8fed7ceb998e75b996
35f9cfe5110471a82e330d904c97466a
5dd1ccc8fb2a5615bf5656721339efed
81180bf9c7b282c6b8411f8f315bc422
e3d03829cbec1a8cca56c6ae730ba9a8

SHA-256:

37dd416ae6052369ae8373730a9189aefd6d9eb410e0017259846d10ac06bff5
87db427b1b44641d8c13be0ba0a2b2f354493578562326d335edfeb998c12802
e40a46e95ef792cf20d5c14a9ad0b3a95c6252f96654f392b4bc6180565b7b11
53e9bca505652ef23477e105e6985102a45d9a14e5316d140752df6f3ef43d2d
8fcd303e22b84d7d61768d4efa5308577a09cc45697f7f54be4e528bbb39435b
6dae368eecbcc10266bba32776c40d9ffa5b50d7f6199a9b6c31d40dfe7877d1
b987f7e6467704029c7784e9beb9ad3aa6e1375a661dc10b5f3d11c6a8fc1ef2
1d0999ba3217cbdb0cc85403ef75587f747556a97dee7c2616e28866db932a0d
9f177a6fb4ea5af876ef8a0bf954e37544917d9aaba04680a29303f24ca5c72c
78af649d3d6a932bcf53cfe384ce6bf9441f4d19084692b26b7e28b41f7a91bd
5d617f408622afc94b1ca4c21b0b9c3b17074d0fcd3763ee366ab8b073fc63e9
fee0081df5ca6a21953f3a633f2f64b7c0701977623d3a4ec36fff282ffe73b9
c5946116f648e346b293e2e86c24511a215ebe6db51073599bba3e523fb0d0a8
eab55bded6438cd7b8a82d6447a09bba078ded33049fca22d616a74bb2cad08f
ff2eb800ff16745fc13c216ff6d5cc2de99466244393f67ab6ea6f8189ae01dd
1ee75106a9113b116c54e7a5954950065b809e0bb4dd0a91dc76f778508c7954
f71d67659baf0569143874d5d1c5a4d655c7d296b2e86be1b8f931c2335c0cd3
96721e13bae587c75618566111675dec2d61f9f5d16e173e69bb42ad7cb2dd8a

Network Signatures

Possible Volgmer User-Agent

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible Volgmer User-Agent"; target:src_ip; flow:established,to_server; content:"Mozillar/"; http_user_agent; depth:9; classtype:backdoor; reference:url,https://www.us-cert.gov/ncas/alerts/TA17-318B; sid:1002080; rev:1; metadata:severity 5, ti_malware_id faece0aa10e65d5804c138704c65c4ed54e144df, ti_malware_name Volgmer, malware_family Volgmer, rule_origin gib;)

ii. FASTCash

This malware in turn intercepts fraudulent Lazarus cash withdrawal requests and sends fake approval responses, allowing the attackers to steal cash from ATMs.

Platform: ATM, Windows

Threat level: High

Category: atm-malware

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
b3efec620885e6cf5b60f72e66d908a9
b66be2f7c046205b01453951c161e6cc
46b318bbb72ee68c9d9183d78e79fb5a
d790997dd950bb39229dc5bd3c2047ff
a2b1a45a242cee03fab0bedb2e460587

Network Signatures

N/A

jj. Duuzer

Duuzer is a backdoor Trojan. After installing Duuzer, cybercriminals have the following capabilities:

- Gathering information about the system and disks
- Create, number and end processes
- Access, download, modify and delete files
- Change temporary file attributes
- Execute commands.

Platform: N/A

Threat level: N/A

Category: Backdoor

General information
Indicators of Compromise (IOCs)
CnC:

MD5:
1205c4bd5d02782cc4e66dfa3fef749c
92d618db54690c6ae193f07a31d92098
3e6be312a28b2633c8849d3e95e487b5
41a6d7c944bd84329bd31bb07f83150a
7343f81a0e42ebf283415da7b3da253f
73471f41319468ab207b8d5b33b0b4be
84a3f8941bb4bf15ba28090f8bc0faec
b04fabf3a7a710aafe5bc2d899c0fc2b
e04792e8e0959e66499bfacb2a76802b
3a963e1de08c9920c1dfe923bd4594ff
51b3e2c7a8ad29f296365972c8452621
5f05a8f1e545457dbd42fe1329f79452
91e5a64826f75f74a5ae123abdf7cef5
9749a4b538022e2602945523192964ad
9ca7ec51a98c2b16fd7d9a985877a4ba
bb6cbebd4ffd642d437afc605c32eca0
fb4caaaf1ac1df378d05111d810a833e
4b2d221deb0c8042780376cb565532f8
cd7a72be9c16c2ece1140bc461d6226d
f032712aa20da98a1bbad7ae5d998767
f940a21971820a2fcf8433c28be1e967
71cdcc903f94f56c758121d0b442690f
0f844300318446a70c022f9487475490
Network Signatures

N/A

kk. Destover

Destover is a trojan that has dropper, backdoor and wiper functions. Destover's destructive payload is produced using igfxtrayex.exe.

- Delete all files on stationary and remote drives
- Change the partition table
- Install additional modules
- Connect to multiple IP addresses on ports 8080 and 8000.

Platform: N/A

Threat level: N/A

Category: Backdoor

Indicators of Compromise (IOCs)

CnC:
88.53.215.64
217.96.33.164
203.131.222.102
101.76.99.183
112.206.230.54
124.47.73.194
165.138.120.35
175.45.4.158
177.189.204.214
187.176.34.40
202.182.50.211
208.105.226.235
209.237.95.19
211.76.87.252
213.42.82.243
31.210.53.11
59.125.119.135
59.125.62.35
61.91.100.211
62.141.29.175
65.117.146.5
71.40.211.3
85.112.29.106
91.183.41.5

93.157.14.154
1.202.129.201
110.78.165.32
113.10.158.4
124.81.92.85
140.134.23.140
196.36.64.50
199.83.230.236
201.22.95.127
202.9.100.206
185.20.218.28
103.233.121.22
187.111.14.62
187.54.39.210
200.202.169.103
202.152.17.116
203.131.210.247
206.248.59.124
37.34.176.14
94.199.145.55
110.77.140.155
113.160.112.125
114.143.184.19
148.238.251.30
161.139.39.234
161.246.14.35
175.111.4.4
177.0.154.88
177.19.132.216
177.52.193.198
184.173.254.54
185.30.198.1
185.81.99.17
186.167.17.115
194.165.149.51
196.202.33.106
200.87.126.117
201.163.208.37
202.39.254.231
203.113.122.163
203.115.13.105
203.170.66.206
210.211.124.229

223.255.129.230
31.210.54.14
37.148.208.67
37.58.148.34
41.21.201.107
41.76.46.182
5.22.140.93
62.0.79.45
67.229.173.226
78.38.114.213
87.101.243.246
90.80.152.49
203.132.205.250
59.90.208.171
201.25.189.114
91.183.71.18
184.20.197.204
208.87.77.153
201.216.206.49
87.101.243.252
208.69.30.151
69.54.32.30

MD5:
d1c27ee7ce18675974edf42d4eea25c6
760c35a80d758f032d02cf4db12d3e55
e1864a55d5ccb76af4bf7a0ae16279ba
b80aa583591eaf758fd95ab4ea7afe39
2618dd3e5c59ca851f03df12c0cab3b8

SHA-256:
e0066ddc9e6f62e687994a05027e3eaa02f6f3ad6d71d16986b757413f2fb71c
9ec83d39d160bf3ea4d829fa8d771d37b4f20bec3a68452dfc9283d72cee24f8
10d3ab45077f01675a814b189d0ac8a157be5d9f1805caa2c707eecbb2cbf9ac
33207f4969529ad367909e72e0f9d0a63c4d1db412e41b05a93a7184ec212af1
389ee412499fd90ef136e84d5b34ce516bda9295fa418019921356f35eb2d037
e0ce1f4b9ca61747467cee56307f9ea15dd6935f399837806f775e9b4f40e9ca
54ab7e41e64eb769b02b855504c656eaaff08b3f46d241cb369346504a372b4f
47830371f6f3d90d6a9fbe39e7f8d43a2e126090457448d0542fcbec4982afd6
83e507104ead804855d07bc836af4990542d1eac5ac2a8ce86f985d082199f6f
d94ceade521452864ae8daae9d6b202a79d4761f755c7c769ec4e103c7c3127d
bebf6266e765f7a0eefcde7c51507cc9f6e3b5d5b82a001660454e4e84f6e032
4166f6637b3b11f69cccbeb775f9ee6987a5a30475c54db189b837ee3fbbf0d1
eeb146ebbc3f144f5a6156d07322a696eead9c4895a9a6f94212d24056acd41c

6959af7786a58dd1f06d5463d5ba472396214d9005fce8559d534533712a9121
68006e20a2f37609ffd0b244af30397e18df07483001150bcc685a9861e43d44
d8fedef123b3d386f0917f11db9fae0956ffe5b16a9aaad8805f72309437d066
2368ee0e0001599b7789d8199c7b19f362a87925118ae054309d85f960d982ec
6e3db4da27f12eaba005217eba7cd9133bc258c97fe44605d12e20a556775009
98abfcc9a0213156933ccd9cb0b85dc51f50e498dbfdec62f6a66dc0660d4d92
d36f79df9a289d01cbb89852b2612fd22273d65b3579410df8b5259b49808a39
696ff9dda1ce759e8ff6dd96b04c75d232e10fe03809ba8abac7317f477f7cf5
7501c95647cef0c56e20c6d6a55de3d23f428e8878a05a603a0b37ea987a74e2
3c3d2ab255daa9482fd64f89c06cdbfff3b2931e5e8e66004f93509b72cf1cc7
7d9631a62ae275c58e7ad2a3e5e4c4eac22cff46c077410ad628be6c38dd5e08
ca4b4a3011947735a614a3dc43b67000d3a8deefb3fffa95b48f1d13032f2aea
31a76629115688e2675188d6f671beacfe930794d41cf73438426cc3e01cebae
7cea18dce8eb565264cc37bfa4dea03e87660b5cea725e36b472bafdcfe05ab1
757cd920d844fdcb04582a89b55f62b9a3e9bf73804abf94c9a9e15d06030b93
8a4f000049ad2a6c4eeac823c087b1c6e68c58b241c70341821cceccdf0f2d17
0654d112c17793c7a0026688cee569e780b989a9eb509585a977efd326dc2873
453d8bd3e2069bc50703eb4c5d278aad02304d4dc5d804ad2ec00b2343feb7a4
1f689996439db60970f4185f9cfc09f59bfe92650ba09bda38c7b1074c3e497b
029f93b7b7012777ee9fb2878d9c03b7fc68afad0b52cdc89b28a7ea501a0365
5831e614d79f3259fd48cfd5cd3c7e8e2c00491107d2c7d327970945afcb577d
6b70aa88c3610528730e5fb877415bc06a16f15373c131284d5649214cd2e96b
9b4c90ca8906e9fea63c9ea7a725db5fc66e1ca6c2a20bec2e8c1749b0000af5
b0cfaab0140f3ea9802dc6ed25bf208a2720fb590733966b7a3e9264a93a4e66
b3c0b7e355bee34cdb73d0bbdb1ba1b61797c035db31f0c82b19f9aa6a7abcc7
36844e66e5f4d802595909e2cbe90a96ad27da6b254af143b6611ab9ee85a13e
4efeea9eeae3d668897206eeccb1444d542ea537ca5c2787f13dd5dadd0e6aaa
5b28c86d7e581e52328942b35ece0d0875585fbb4e29378666d1af5be7f56b46
66df7660ddae300b1fcf1098b698868dd6f52db5fcf679fc37a396d28613e66b
72008e5f6aab8d58e4c8041cde20ee8a4d208c81e2b3770dbae247b86eb98afe
822a7be0e520bb490386ad456db01f26c0f69711b4ac61ba2cb892d5780fe38f
899ff9489dde2c5f49d6835625353bfe5ea8ca3195ca01362987a9d4bdac162d
8b50d7d93565aab87c21e42af04230a63cd076d19f8b83b063ef0f61d510adc7
90d8643e7e52f095ed59ed739167421e45958984c4c9186c4a025e2fd2be668b
ac27cfa2f2a0d3d66fea709d7ebb54a3a85bf5134d1b20c49e07a21b6df6255a
c5be570095471bef850282c5aaf9772f5baa23c633fe8612df41f6d1ebe4b565
ce0e43c2b9cb130cd36f1bc5897db2960d310c6e3382e81abfa9a3f2e3b781d7
facb32efc05bc8c4f3cb3baa6824db0f7effc56c02dbc52c33bafe242a1def77
763d1cb589146dd44e082060053ffbf5040830c79be004f848a9593d6be124ac
02d1d4e7acd9d3ec22588d89aed31c9a9d55547ef74fa3749659b610893f5405
47181c973a8a69740b710a420ea8f6bf82ce8a613134a8b080b64ce26bb5db93
e187811826b2c33b8b06bd2392be94a49d068da7f703ae060ee4faffde22c2fe
2811fdceb8a8aa03bbf59c0b01a43bd1f2aee675a8f20d38194258046987e5fa
39e53ba6984782a06188dc5797571897f336a58b8d36020e380aa6cd8f1c40a2
530a0f370f6f3b78c853d1e1a6e7105f6a0f814746d8a165c4c694a40c7ad09a
7a2a740d60bd082c1b50ab915ef86cc689ba3a25c35ac12b24e21aa118593959
eaea45f8bfb3d8ea39833d9dcdb77222365e601264575e66546910efe97cba99

ee49322ed9fb43a9a743b54cc6f0da22da1d6bc58e87be07fd2efe5e26c3ef8a
ef07d6a3eb4a0047248c845be3da3282c208ede9508a48dbb8128eacc0550edf
477ca3e7353938f75032d04e232eb2c298f06f95328bca1a34fce1d8c9d12023
5a69bce8196b048f8b98f48c8f4950c8b059c43577e35d4af5f26c624140377c
89b25f9a454240a3f52de9bf6f9a829d2b4af04a7d9e9f4136f920f7e372909b
a01bd92c02c9ef7c4785d8bf61ecff734e990b255bba8e22d4513f35f370fd14
b93793e3f9e0919641df0759d64d760aa3fdea9c7f6d15c47b13ecd87d48e6a9
d589043a6f460855445e35154c5a0ff9dbc8ee9e159ae880e38ca00ea2b9a94f
92cc25e9a87765586e05a8246f7edb43df1695d2350ed921df403bdec12ad889
f2a14c5ef6669d1eb08fababb47a4b13f68ec8847511d4c90cdca507b42a5cf3
520778a12e34808bd5cf7b3bdf7ce491781654b240d315a3a4d7eff50341fb18
e55fff05de6f2d5d714d4c0fa90e37ef59a5ec4d90fdf2d24d1cb55e8509b065
e506987c5936380e7fe0eb1625efe48b431b942f61f5d8cf59655dc6a9afc212
2477f5e6620461b9146b32a9b49def593755ac9788fc4beeee81bf248aa2e92a
f69747d654acc33299324e1da7d58a0c8a4bd2de464ec817ad201452a9fa4b54
44884565800eebf41185861133710b4a42a99d80b6a74436bf788c0e210b9f50
2f629c3c65c286c7f55929e3d0148722c768c730a7d172802afe4496c0abd683
b5e1740312b734fb70a011b6fe52c5504c526a4cccb55e154177abe21b1441c9
0e162a2f07454d65eaed0c69e6c91dd10d29bdb27e0b3b181211057661683812
a53e33c77ecb6c650ee022a1311e7d642d902d07dd519758f899476dbaae3e49
c95eaedaafd8041bb0fea414b4ebc0f893f54cdec0f52978be13f7835737de2a
da255866246689572474d13d3408c954b17d4cc969c45d6f45827799e97ed116
8465138c0638244adc514b2722fcb60b2a26a8756aa7d97f150e9bdc77e337cc
77a32726af6205d27999b9a564dd7b020dc0a8f697a81a8f597b971140e28976
794b5e8e98e3f0c436515d37212621486f23b57a2c945c189594c5bf88821228
c248da81ba83d9e6947c4bff3921b1830abda35fed3847effe6387deb5b8ddbb
fba0b8bdc1be44d100ac31b864830fcc9d056f1f5ab5486384e09bd088256dd0
c3f5e30b10733c2dfab2fd143ca55344345cc25e42fbb27e2c582ba086fe3326

Network Signatures

N/A

II. Koredos

Trojan.Koredos / DDoS-KSig / DeltaAlfa Trojan.Koredos is a Trojan horse that attempts to carry out DDoS attacks and encrypts data files found on the infected computer.

Platform: N/A

Threat level: N/A

Category: DDoS

Other Name: Trojan.Koredos, DDoS-KSig, DeltaAlfa

Indicators of Compromise (IOCs)

CnC:

MD5:

0a21b996e1f875d740034d250b878884
c963b7ad7c7aefbe6d2ac14bed316cb8
a63f4c213e2ae4d6caa85382b65182c8

Network Signatures

N/A

mm. KorDllBot

It is a family of small/medium size trojans that usually are configured to be installed as services.

Platform: N/A

Threat level: N/A

Category: Backdoor

Other Name: Redobot

General information

KorDllbot is a family of small/medium size trojans that usually are configured to be installed as services.
Samples can vary a great deal in functionality - from just listening on a port and accepting commands, to harvesting data, to actively spreading over SMB. This functionality seems almost modular, using different encryption and encoding methods and different C&C command words.

Common capability seen in the KorDllbot family is:

- Get bot status
- List logical drives
- List directory
- Change directory
- Get process list
- Kill process
- Execute file
- Delete file
- Change file time
- Execute shell command
- Download file
- Upload file
- Get volume serial number
- Get file attributes

Indicators of Compromise (IOCs)

CnC:

MD5:

SHA-256:

87bae4517ff40d9a8800ba4d2fa8d2f9df3c2e224e97c4b3c162688f2b0d832e
fd95e095658314c9815df6a97558897cb344255bd54d03c965fa4cbd16d7bafd
82169a2d8f15680c93e1436687538afa01d6a2ecfe7a7cb613817c64a1a82342
792b484ac94f0baefc7e016895373ba92c2927e3463f62adb701ddbe4c90604c
162d6223c1c1219ca81a77e60e6b776058517272fe7cac828a3f64dcacd87811
56e0b1794a588e330e32a10813cdc9904e472c55f17dd6c8de341aeaf837d077
c16a66c1d8e681e962f03728411230fe7c618b7294c143422005785d3a724ec4
57b4c2e71f46fe3e7811a80d19200700c15dd358bdf9d9fdf61f1c9a669f7b4b
2d9edf45988614f002b71899740d724008e9a808efad00fa79760b31e0a08073
006e0cc29697db70b2d4319f320aa0e52f78bf876646f687aa313e8ba04e6992
dda136bc51670e57a4b2f091f83ab7b44291a9323d5483abd9e91b78221e027f
163571bd56001963c4dcb0650bb17fa23ba23a5237c21f2401f4e894dfe4f50d
3d2a7ea04d2247b49e2dcad63a179ae6a47237eddbfd354082f1417a63e9696e
ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
6e8a2329567cdbbba68460ccb97209867d7508983cb638662b33bfe90d0134d4
af7b53ce584b83085488e1190e1458948eaf767631f766e446354d0d5523e9d0
69300a42e055f68a8057192077fbbef3be5b66514ea9ca258b077c5c7e9417a9
e0cd4eb8108dab716f3c2e94e6c0079051bfe9c7c2ed4fcbfdd16b4dd1c18d4d
96c35225dc4cac65cc43a6cc6cdcce3d13b3bda286c8c65cad5f2879f696ad2a
29355f6d4341089b36834b4a941ef96b3bf758a4fe35fbb401cc4e74b9b1c90f
9e226a5eb4de19fcb3f7ecc3abcf52ea22a1f1a42a08dd104f5f7a00164e074e
041605e498bb41b07d2d43003152cc2a992e7e2ade7a47ee9aef2570bdb16d94
82fe3a8f2248643505e8de1977b734f97eb38225e6d3df6ea8f906430514b4f5
08203b4ddc9571418b2631ebbc50bea57a00eadf4d4c28bd882ee8e831577a19
8e3c3398353931c513c32330c07f65b6ee6f62fc7a56edac7cbe4edb1bf4c74e
bb4204dd059849848e9492523ce32520bf37cb80974320c0ca71f3b79e83f462
2f8c448bb05ed1218e638c61bb56ebb953b962ed5e065b08fa03cfcf6f6a1c68
f98c67c4cf9b02acaabb555664a0d9d648a1e43f681f9bf234af066d5451be8d
1226d3635c1a216be9316c9dfa97f103c79ed4c44397e5e675d3b1e37786bf31
c5baece9978649659220af2681a3a43b83f8ae47afdd3862185d1fec7735a7d2
a4b982d4e7137d7d3687f3127e6d5c2a8b2be1f53daeebce9175461c7e6a53cd
9bcecd6afa54eb4f343b7eb82a86ceee189cc10bc91fa83f8cdc98cc5aaef117
b7f2595dd62d1174ce6e5ddf43bf2b42f7001c7a4ec3c4cbe3359e30c674ed83
b039383a19e3da74a5a631dfe4e505020a5c5799578187e4ccc016c22872b246
f4a06dd6ebfd0805d445f45ce33d7bba4a33c561111c39a347024069a78169e9
3acaea01fd79484d5a72c72e1b9c2fbf391145fb1533c17a8a83e897d8777f82
81067f057d523fdcddf7df1da39a7c3614c45f6bff6bd387274c049244efda3b
218ee208323dc38ebc7f63dba73fac5541b53d7ce1858131fa3bfd434003091d
73edc54abb3d6b8df6bd1e4a77c373314cbe99a660c8c6eea770673063f55503
6d5d706f5356e087f5961ba2ed808c51876d15c2e09eb081618767b36b1d012f

7a538c3eed1f01b62a19226750c1369e4e9210b1331d5829ca91fe2b69087f06
6059cb08489170aea77caf0940131e5765b153a593e76d93a0f244e89ddb9e90
e97a8909349a072ed945899fbe276fc27e9c5847bc578b0abccf017da3fd680c
c4852ddba88e5c53a8711c4c7540b7ac98dac6b9e31d10dd999a81a4f0e117c3
3ebb3d8292a1aa5dc81b028beeefdec0f0448516d6225b336ee37d550ab8c3ab
87e68055959328d857b287e797896d9a96695b69ed300a843eee73319427b3b3
94e14a85a2046b40842f6c898c5f6c3200de3d89c178a9a9f9a639c1d3de9ee9
cd8c729da299b29618819afeef8b2a79451e6c3d35dea3769ef638c649c69001
9d9889585f1a4048a3955d3a9cead2f426a509afaeacad27540382cc3266f0fa
888844c040be9d0fc3dab00dd004aa9e8619f939aff2eba21e4f48ca20e13784
d7044a35e76543a03cd343d71652c7bbd9a28e246d7f3a43f4a2e75cd0ef7366
50974c15a546e961fbee8653e5725960a77b79e0f7c8eadf3b6d35ba3a46dd57
bfb5fa2a09ac60efcc0e9f05e781bd22cae0b8f6ba356d7819285f073845a0eb
9bc8fe605a4ad852894801271efd771da688d707b9fbe208106917a0796bbfdc
7b171a160cb2a17f87ca6a4a1c62b4cd9e718f987b7278d3effe0614b5b51be4
0a27acaaebc7db0878239b40ab9d2feff13888839c05a03348fc09b78de6ced5

Network Signatures

N/A

Advanced Persistent Threat (APT): Silence

Silence APT, a Russian-speaking cybercriminal group, known for targeting financial organizations primarily in former Soviet states and neighboring countries is now aggressively targeting banks in more than 30 countries across America, Europe, Africa, and Asia including : Kyrgyzstan, Armenia, Georgia, Serbia, Germany, Latvia, Czech Republic, Romania, Kenya, Israel, Cyprus, Greece, Turkey, Taiwan, Saudi Arabia, Malaysia, **Bangladesh,** Switzerland, Vietnam, Austria, Uzbekistan, Great Britain, Hong Kong, and others.

Silence uses phishing as their infection vector. The threat actor's emails usually contain a picture or a link without a malicious payload and are sent out to a huge recipient database of up to 85,000 users.

Silence has made a number of changes to their toolset with one goal: to complicate detection by security tools. In particular, they changed their encryption alphabets, string encryption, and commands for the bot and the main module. In addition, the actor has completely rewritten TrueBot loader, the first-stage module, on which the success of the group's entire attack depends. The hackers also started using Ivoke, a fileless loader, and EDA agent, both written in PowerShell. Silence has also made a move to including fileless modules in their arsenal, albeit much later than other APT groups, suggesting that the group is still playing catch-up compared to other cybercriminal groups.

Malware List of Silence APT:

a. Silence Backdoor

Platform: Windows

Threat level: High

Category: Backdoor

Other Name: Silence.MainModule

General information

Indicators of Compromise (IOCs)

CnC:

195.123.246.126
37.120.145.253
185.29.10.13
185.236.76.216
167.99.43.101
185.70.184.32
counterstat.pw

counterstat.club
185.161.208.9
151.248.115.41
193.124.18.72
185.154.52.83
185.154.52.142
185.29.9.41
zaometallniva.ru
1mliked.ru
185.20.187.89
http://185.161.208.61/index.php?xy=1
http://185.29.10.117/index.php

MD5:

363df0b3c8b7b390573d3a9f09953feb
800060b75675493f2df6d9e0f81474fd
E81CD10C838F5A268944AAF50B1BB3B5
0512D025AD198A94E16D03EF31F790EF
ff411742f5e8b970d27bef660349b559
fd133e977471a76de8a22ccb0d9815b2
8b437da524c25d03ab33d7d78d2d6a77
afdfe8c799aa76420622d370416a72be
39537145ce7f01aa8b8c27f9fd40eaa2
7EAF9BBD855C6A124E2EE962BF2DB735
c4f18d40b17e506f42f72b8ff111a614
F1954B7034582DA44D3F6A160F0A9322

Network Signatures

N/A

b. Silence.ProxyBot

The program is designed to access isolated segments of the network via an intermediate node

Platform: N/A

Threat level: N/A

Category: Bot

Indicators of Compromise (IOCs)

CnC:

91.92.136.193
79.141.168.114
45.84.0.201

185.29.10.13
167.99.43.101
185.70.184.32
counterstat.pw
counterstat.club
185.20.187.89
84.38.134.103
http://185.161.208.61/run.exe
46.183.221.89

MD5:

ce04972114bbd5844aa2f63d83cdd333
3f5372c2776e5cc8aec8a7107f49cf8a
f1f73008183d1b161f25b62a76cd2513
043b383e895a26848bef90abb8da2216
1136c47332daa275d2ecc179a0bf4c0c
BEBB2DE1C051B4E847EE6501D118D522
2fe01a04d6beef14555b2cf9a717615c
b33cd8d369a7167351c69fe57bae0bb1
50565c4b80f41d2e7eb989cd24082aab
88cb1babb591381054001a7a588f7a28

Network Signatures

N/A

c. APT.Silence.EDA.ps1

Platform: N/A

Threat level: High

Category: remote-access-trojan

General information

This program is intended for remote management of compromised system via DNS protocol and processes following modules: changing the address of the management server, downloading the file from the network, sending a local file to the management server, executing commands in the cmd.exe, collecting system information, rebooting and turning off the system, traffic tunneling.

Indicators of Compromise (IOCs)

CnC:

91.92.136.193
79.141.168.114
45.84.0.201

167.99.43.101
counterstat.pw
counterstat.club

MD5:

ce04972114bbd5844aa2f63d83cdd333
3f5372c2776e5cc8aec8a7107f49cf8a
f1f73008183d1b161f25b62a76cd2513
043b383e895a26848bef90abb8da2216
1136c47332daa275d2ecc179a0bf4c0c
9812a3436f917af18a7f93a2c71dc846
dcba65555652431c8d3cd773bf873118

Network Signatures

N/A

d. Truebot (Silence's loader)

Loader for backdoor of Silence group, was first detected end of 2017.

Platform: Windows

Threat level: High

Category: Loader

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

185.70.186.149
151.248.115.41
193.124.18.72
185.154.52.83
185.154.52.142
185.29.9.41
zaometallniva.ru
1mliked.ru
84.38.133.22
itablex.com
213.183.63.227
185.70.187.188
http://185.70.187.188/inf/getsi.php
http://185.70.187.188/inf/logs/logpc.php
217.160.233.141
185.244.131.68

http://basch.eu/administrator/components/com_admin/sql/updates/mysql/exe.exe
http://185.244.131.68/z/get.php
185.175.58.136
http://185.175.58.136/gif/gifupload.php
http://146.0.77.112/a/logs/logpc.php
146.0.77.112
http://146.0.77.112/a/getsi.php
http://146.0.72.139/flk
146.0.72.139
http://5.39.218.204/ks
5.39.218.204
http://5.8.88.254/HUYfhwuiGYUR/opensource.php/name=?
fpbank.ru
http://91.243.80.200/yre
91.243.80.200
5.8.88.254
http://144.217.14.173/file.exe
http://137.74.224.142/z/get.php

MD5:

7441cca252b7a2da481ddf2c70eed727
b2ad4409323147b63e370745e5209996
8cc6d41f5be9144093a2ff8a5c3b32a3
65f673a77c93c4a2c9db34b3704279e2
edf59a111cce8ea1d09a2b4e8febdfdf
e2e1035f382c397d64303e345876a9db
5127fff71a4251e3c62c420a4de57010
f1a4e74e72390ef98c23f19589d3c7cd
81f3e843b26d254ae58c44d778c7ee5b
13cc98fcb654ac83cda6d3ec9946fa9b
C2A00949DDACFED9ED2EF83A8CB44780
97599e2edc7e7025d5c2a7d7a81dac47
C2F1AF367576FFA39182864044769E42
404d69c8b74d375522b9afe90072a1f4
43eda1810677afe6791dd7a33eb3d83c
7d3614df9409da3933637f09587af28c
15d097a50718f2e7251433ea65401588
a58a830dce460e91217328bdefb25cbe
9b037ead562c789620a167af85d32f72
c6c84da4f27103db4ff593f4d4f45d95

Network Signatures

Win32.Trojan_YU Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan_YU Checkin"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".php?name="; http_uri; fast_pattern; pcre:"/\.php\?name=[0-9a-f]+ HTTP\/1\.1\x0d\x0aHost\: ([0-9]{1,3}\.){3}[0-9]{1,3}\x0d\x0a\x0d\x0a$/"; threshold:type limit, track by_src, count 1, seconds 360; classtype:apt-trojan; reference:md5,9b037ead562c789620a167af85d32f72; sid:1001404; rev:1; metadata:severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin gib;)

TrueBot (Silence APT) CnC activity 1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TrueBot (Silence APT) CnC activity 1"; flow:established,to_server; content:".php?xy=1"; http_uri; isdataat:!1,relative; fast_pattern; content:"User-Agent|3a 20 0d 0a 0d 0a|"; target:src_ip; classtype:apt-trojan; reference:md5,c4f18d40b17e506f42f72b8ff111a614; sid:1002195; rev:1; metadata:severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin gib;)

TROJAN TrueBot/Silence.Downloader CnC Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN TrueBot/Silence.Downloader CnC Checkin"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; isdataat:!1,relative; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|file|22 3b 20|filename=|22|C|3a 5c|"; http_client_body; content:".DAT|22 3b 0d 0a|"; http_client_body; distance:0; content:"|0d 0a|Host Name|3a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20|"; http_client_body; distance:0; content:"|0d 0a|OS Name|3a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20|"; http_client_body; distance:0; content:"|0d 0a|OS Version|3a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20|"; http_client_body; distance:0; http_header_names; content:!"Referer"; content:!"User-Agent"; content:!"Accept"; reference:md5,c2a00949ddacfed9ed2ef83a8cb44780; classtype:apt-trojan; sid:2026559; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_10_29, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin etpro;)

TROJAN TrueBot/Silence.Downloader Keep-Alive

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN TrueBot/Silence.Downloader Keep-Alive"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".php?dns="; http_uri; fast_pattern; pcre:"/^[a-f0-9]{8}$/RUs"; http_header_names; content:"|0d 0a|Host|0d 0a 0d 0a|"; depth:10; isdataat:!1,relative; reference:md5,c2a00949ddacfed9ed2ef83a8cb44780; classtype:apt-trojan; sid:2026560; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_10_29, deployment Perimeter, former_category TROJAN, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin etpro;)

TrueBot (Silence APT) CnC activity 2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TrueBot (Silence APT) CnC activity 2"; flow:established,to_server; content:".php?xy=2&axy="; http_uri; target:src_ip; classtype:apt-trojan; reference:md5,c4f18d40b17e506f42f72b8ff111a614; sid:1002196; rev:1; metadata:severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin gib;)

e. FlawedAmmyy

It is malicious program for remote control, based on leaked source codes of legitimate utility Ammyy Admin. After infection, it allows full access to threat actors: opportunity to remote entering to the system, to restart it, process commands and upload any files. In addition, it has function of remote desktop. It was discovered in 2016. In August 2018 there were malicious email sendings with this malware to banks.

Platform: Windows

Threat level: High

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

http://n57u[.]com/inform
195.123.224.99
http://g78k.com/set
51.254.167.115
http://g50e[.]com/security
http://g50e[.]com/benat.exe
31.202.132.13
http://r48t[.]com/input

54.36.91.25
http://f67i[.]com/con
81.4.101.187
185.99.132.12

MD5:

b2f2ce77063476ef9c8ebb3c63fad402
a471555caf8dbb9d30fac3014172515f
73964f92d3e5e142047574afa78726e3
627ae12b487dfacad66d4ff3bf8a5134
0906ab6a9ed0fa8f173d6800f8957f4a
919c8bd911850741522fedf362effca3
92feb5c5358835e80dd1f62ef6ebc475
aa0a5f274d4c612b6fdfb91f66aef94f
65713d26cf111eb64de1aa524bbecb2b
5fdeaa5e62fabc9933352efe016f1565
bacd1120ad0918b81d98de9b9acb69ce
85e1828d863004ff681f2908297c7fee
1094ec2f32abc7780f0856928cb0c261

Network Signatures

RAT.FlawedAmmyy CnC communication

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"RAT.FlawedAmmyy CnC communication"; flow:established,to_server; content:"id="; content:"&os="; distance:0; content:"&priv="; distance:0; content:"&cred="; distance:0; content:"&pcname="; distance:0; content:"&avname="; distance:0; content:"&build_time="; distance:0; content:"&card="; distance:0; target:src_ip; classtype:backdoor; reference:md5,b2f2ce77063476ef9c8ebb3c63fad402; sid:1002344; rev:1; metadata:severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin gib;)

TROJAN Win32/FlawedAmmyy RAT Reporting System Details

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/FlawedAmmyy RAT Reporting System Details"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|2e|php"; http_uri; isdataat:!1,relative; content:"Host|20|Name|3a 20 20 20 20 20|"; http_client_body;

depth:17; fast_pattern; content:"OS|20|Name|3a 20 20 20 20|"; http_client_body; distance:0; content:"OS|20|Version|3a 20 20 20 20|"; http_client_body; distance:0; reference:md5,d334c877fb1adc37fd68bf2b40275d7e; reference:md5,cf1e4eb6325ed0d9969bddac56eeda58; classtype:backdoor; sid:2837164; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_07_01, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag RAT, updated_at 2019_09_28, severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin etpro;)

TROJAN Win32/FlawedAmmyy RAT Reporting Loader Results

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/FlawedAmmyy RAT Reporting Loader Results"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|2e|php"; http_uri; isdataat:!1,relative; content:"running loader|0d 0a|"; http_client_body; depth:16; fast_pattern; content:"exiting loader"; http_client_body; distance:0; reference:md5,d334c877fb1adc37fd68bf2b40275d7e; reference:md5,cf1e4eb6325ed0d9969bddac56eeda58; classtype:backdoor; sid:2837165; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_07_01, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag RAT, updated_at 2019_09_28, severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin etpro;)

TROJAN Win32/FlawedAmmyy RAT Reporting Installed Software

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/FlawedAmmyy RAT Reporting Installed Software"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|2e|php"; http_uri; isdataat:!1,relative; content:"|ff fe 4e 00 61 00 6d 00 65 00 20 00 20 00 20 00|"; http_client_body; depth:16; fast_pattern; content:"|56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 20 00 20 00 20|"; http_client_body; distance:0; reference:md5,d334c877fb1adc37fd68bf2b40275d7e; reference:md5,cf1e4eb6325ed0d9969bddac56eeda58; classtype:backdoor; sid:2837166; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_07_01, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag RAT, updated_at

2019_09_28, severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin etpro;)

f. Ammyy Admin

Ammyy Admin - is a free remote desktop sharing and PC remote control software that can be used for remote administration, remote office arrangement, remote support or distant education purposes. It was developed by russian company Ammyy Group.

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

http://31.207.45.85/d.dat
31.207.45.85
http://185.179.188.185/ldr.exe
185.179.188.185

MD5:

7af426e0952b13ef158a4220e25df1ae
e71819cf79b1d5627acd9ac9aec6a4bc

Network Signatures

POLICY RemoteAdmin Win32.Ammyy.z Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"POLICY RemoteAdmin Win32.Ammyy.z Checkin"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:!"User-Agent|3a| "; http_header; content:"v="; depth:2; http_client_body; content:"&d="; distance:3; within:3; http_client_body; pcre:"/^v=\d\.\d&d=[a-zA-Z0-9-/]+?$/P"; reference:md5,da83a04e05d95f8b68b4bd2198de2097; classtype:trojan-activity; sid:2806289; rev:10; metadata:created_at 2013_04_23, updated_at 2020_06_09, severity 3, ti_malware_id 6ddc5de6cfaf12b1adb729a4f26e0358efe648a0, ti_malware_name Ammyy Admin, malware_family Ammyy Admin, rule_origin etpro;)

g. Atmosphere

Atmosphere is a software created by Silence group for controlling the ATM dispenser. It was first discovered in October 2017. It allows to get information on the content of ATM cassettes and to issue cash. Another version of Atmosphere discovered in April 2018. There were minor differences compared to the previous versions, but it was clear that the developer went a long way to debug the program and that he eventually got rid of the unnecessary functions and enhanced the program's sustainability. For example, this version didn't process commands from the PIN pad.

Platform: ATM

Threat level: High

Category: atm-malware

Indicators of Compromise (IOCs)

CnC:

MD5:

44f15f1657a64423cb49ea317ce0c631

Network Signatures

h. Smoke Bot

Smoke bot is malware with functions of loader and form grabber. This malware is known since 2011.

Platform: ATM

Threat level: High

Category: atm-malware

Other Names: Sharik, Dofoil, Smoke Loader

Indicators of Compromise (IOCs)

CnC:

MD5:

44f15f1657a64423cb49ea317ce0c631

Network Signatures

TROJAN Smokeloader getgrab Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getgrab Command"; target:src_ip; flow:established,to_server; content:"cmd=getgrab"; http_uri; classtype:backdoor; sid:2014009; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smokeloader getproxy Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getproxy Command"; target:src_ip; flow:established,to_server; content:"cmd=getproxy&login="; http_uri; classtype:backdoor; sid:2014010; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smokeloader getsock Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getsock Command"; target:src_ip; flow:established,to_server; content:"cmd=getsocks&login="; http_uri; classtype:backdoor; sid:2014011; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smokeloader getload Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getload Command"; target:src_ip; flow:established,to_server; content:"cmd=getload&login="; http_uri; reference:url,sophosnews.files.wordpress.com/2013/07/sophosszappanosplugxrevisitedintroducingsmoaler-rev1.pdf; reference:url,symantec.com/security_response/writeup.jsp?docid=2011-100515-1838-99&tabid=2; classtype:backdoor; sid:2014012; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smoke Loader Checkin r=gate

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smoke Loader Checkin r=gate"; target:src_ip; flow:established,to_server; content:".php?r=gate&"; http_uri; content:"&group="; http_uri; distance:0;

content:"&debug="; http_uri; distance:0; content:"5.0 (Windows|3b| U|3b| MSIE 9"; http_header; reference:md5,7ef1e61d9b394a972516cc453bf0ec06; classtype:trojan-activity; sid:2014728; rev:6; metadata:created_at 2012_05_09, former_category MALWARE, updated_at 2020_05_13, severity 3, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smoke Loader C2 Response

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Smoke Loader C2 Response"; target:dest_ip; flow:established,from_server; content:"Content-Length|3a| 4|0d 0a|"; http_header; file_data; content:"Smk"; depth:3; fast_pattern; pcre:"/^\d+[\r\n]*?$/Rs"; classtype:trojan-activity; sid:2015835; rev:7; metadata:created_at 2012_10_22, former_category MALWARE, updated_at 2012_10_22, severity 3, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN SmokeBot grab data plaintext

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN SmokeBot grab data plaintext"; target:src_ip; flow:established,to_server; content:"cmd=grab&data="; fast_pattern; http_client_body; content:"&login="; http_client_body; classtype:trojan-activity; sid:2016011; rev:5; metadata:created_at 2012_12_07, updated_at 2020_09_17, severity 3, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

Smoke Loader domain +uri

alert http any any -> any any (msg:"Smoke Loader domain +uri"; target:src_ip; flow:from_client; content:"GET"; http_method; pcre:"/\.php\?act\=([^&]*)\&file\=/I"; nocase; content:!"www.tumcivil.com"; classtype:backdoor; http_host; sid:1000429; rev:2; metadata:severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin gib;)

TROJAN SmokeLoader - Init 0x

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN SmokeLoader - Init 0x"; target:dest_ip; flow:established,to_client; content:"Init|3a| 0x"; http_header; classtype:backdoor; sid:2016088; rev:2; metadata:created_at 2012_12_21, updated_at 2020_04_22, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

SMOKE LOADER

alert http any any -> any any (msg:"SMOKE LOADER"; target:src_ip; flow:from_client; content:"index.php?cmd=getgrab"; classtype:general-suspicious; http_uri; sid:1000412; rev:1; metadata:severity 2, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin gib;)

TROJAN Sharik/Smoke CnC Beacon 2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Sharik/Smoke CnC Beacon 2"; target:src_ip; flow:established,to_server; urilen:1; content:"POST"; http_method; content:!"Accept"; http_header; content:!"Referer|3a|"; http_header; content:"Cache-Control|3a 20|no-cache|0d 0a|Pragma|3a 20|no-cache|0d 0a|Content-Type|3a 20|application/x-www-form-urlencoded|0d 0a|User-Agent|3a 20|"; depth:104; http_header; fast_pattern:76,20; content:"Connection|3a 20|Keep-Alive|0d 0a|Content-Length|3a 20|"; distance:0; http_header; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; pcre:"/User-Agent\x3a[^\r\n]+(?:MSIE|rv\x3a)[^\r\n]+\r\nConnection\x3a\x20Keep-Alive\r\nContent-Length\x3a\x20\d+\r\nHost\x3a[^\r\n]+\r\n(?:\r\n)?$/Hm"; reference:md5,789ee114125a6e1db363b505a643c03d; classtype:backdoor; sid:2021631; rev:2; metadata:created_at 2015_08_14, former_category MALWARE, updated_at 2020_05_29, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Sharik/Smoke Loader Receiving Payload

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Sharik/Smoke Loader Receiving Payload"; target:dest_ip; flow:established,from_server; content:"404"; http_stat_code; file_data; content:"|00|"; distance:1; within:1; content:"|00|MZ"; distance:1; within:3; content:"This program must be run under Win32"; distance:0; fast_pattern; reference:md5,65c7426b056482fcda962a7a14e86601; classtype:backdoor; sid:2023567; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_11_30, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2020_08_03, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;

i. Silence's ATM malware

Malware for ATM cashing out used by Silence group

Platform: Windows

Threat level: High

Category: atm-malware

Other Names: ATMRod

Indicators of Compromise (IOCs)

CnC:

http://149.56.131.140:443/microsoft
http://149.56.131.140:443/win

MD5:

B3ABB10CC8F4CBB454992B95064A9006
14863087695D0F4B40F480FD18D061A4
79E61313FEBE5C67D168CFC3C88CD743
4107F2756EDB33AF1F79B1DCE3D2FD77
86EA1F46DF745A30577F02FC24E266FF
6743F474E3A6A02BC1CCC5373E5EBBFA
DDB276DBFBCE7A9E19FEECC2C453733D

Network Signatures

N/A

j. Silence.SurveillanceModule

A module for spying on users. It used for secretly taking screenshots and proceeded to investigate the operator's work via a pseudo-video stream

Platform: Windows

Threat level: High

Category: Spyware

Other Names: N/A

General information

- Silence.SurveillanceModule a module for secretly taking screenshots and proceeded to investigate the operator's work via a pseudo-video stream.

Indicators of Compromise (IOCs)

CnC:

MD5:

242b471bae5ef9b4de8019781e553b85
d7491ed06a7f19a2983774fd50d65fb2

Network Signatures
N/A

k. Perl IRC DDoS bot

This bot is a Perl script designed to run on Linux OS. Its functionality includes retrieving information about the infected machine, executing shell commands (cmd), sending emails, downloading files, scanning ports and carrying out DDoS attacks.

Platform: Linux

Threat level: Middle

Category: DDoS

Other Names: N/A

Indicators of Compromise (IOCs)

CnC:

http://92.222.68.32/bot.pl
http://92.222.68.32/wolf/

MD5:

081ee959cbe6bc7dde7a6d13168e4fb4
ee650c800d2eedd471ed59aa9435e55f
aa9c31883b3d8e493efad2f983908be3

Network Signatures
N/A

l. Kikothac

Kikothac is a Trojan horse that opens a back door on the compromised computer and downloads potentially malicious files.

Platform: Windows

Threat level: Middle

Category: Backdoor

General information

Indicators of Compromise (IOCs)

CnC:

46.183.221.89
193.169.245.89
185.29.9.45

MD5:

9628d7ce2dd26c188e04378d10fb8ef3
0074d8c3183e2b62b85a2b9f71d4ccd8
440b21958ad0e51795796d3c1a72f7b3

Network Signatures

N/A

Advanced Persistent Threat (APT): OceanLotus

Group OceanLotus began active operations in late 2009.Among the objects of the attacks noted: government agencies, organizations for the protection of human rights, media, companies in the oil industry, research institutes, enterprises of marine industry, retail, hospitality, banking, it companies, companies involved in information security, individuals and activists. Various researchers noted the long-term nature of the group's campaigns, the active phase is preceded by a long period of preparation. OceanLotus is interested in cyber espionage, intelligence, and intellectual property theft. Along with phishing mailings disseminated by e-mail addresses of potential victims, OceanLotus also conduct a spa attack, an attack supported compromise of a large range of legitimate sites. alternative aliases: APT32, APT-C-00, SeaLotus, cobalt Kitty. throughout its activities, the criminal group used the subsequent vulnerabilities:

During its activities, the criminal group used the following vulnerabilities:

• CVE-2016-7255

• CVE-2017-11882

• CVE-2017-8759

• CVE-2017-0199

Malware List of OceanLotus APT:

a. Cobalt Strike

"Cobalt Strike" is a framework that offers a range of methods for conducting attacks, including delivery and control of malware on the victim's computer. Connection with the "Cobalt Strike" server is conducted through creation of hidden channels via DNS, HTTP, HTTPS protocols to avoid detection.

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Other Name: Framwork

General information

This program is in open sale for $3500 USD at https://www.cobaltstrike.com, and a trial version is available for 21 days.
In addition to these instances of sales, some versions of "Cobalt Strike" are available on underground forums.

"Cobalt Strike" is a framework that offers a range of methods for conducting attacks, including delivery and control of malware on the victim's computer. Connection with the "Cobalt Strike" server is conducted through creation of hidden channels via DNS, HTTP, HTTPS protocols to avoid detection. The payload can carry out the following commands:

- Receive system information (OS, hardware, list of processes, computer name, etc.)
- Receive information on the network
- Execute commands in shell
- Download and launch .exe files
- Launch programs for copying of logins and passwords from Windows memory using the exploit in the lsass.exe process (using "mimikatz")
- Bypass Windows (UAC) user account management
- Make copies of hash passwords for Windows
- Gain remote access via VNC protocols with the ability to intervene in current Windows processes
- Provide access to file system
- Scan ports
- Take print screens
- Log keystrokes from specific processes
- Launch a SOCKS proxy server on a specified port, which allows tunnelling of traffic to other applications using DNS, HTTP, HTTPS protocols to avoid detection.
- Provide VPN server functionality
- Provide access to infected computer using «psexec»;
- Change file timestamp attributes

Of the most well-known criminal groups which targeted Russian banks (Corkow, Anunak, Buhtrap, Lurk) only Anunak has used "Cobalt Strike".

Indicators of Compromise (IOCs)

CnC:
cdn.redirectme.net
137.74.181.105
http://www.hkbytes.info/resource/image.jpg
www.hkbytes.info
http://27.102.102.139/lcpd/index.jpg
27.102.102.139
https://27.102.102.139/oEcE
http://www.hkbytes.info/logo.gif

MD5:
DFBF9CC304E36C0B67DB02AAA062297B
AD43D67ED35472D4D6541D9C555F05DB
8ADFD63DE516FCB142EA443FD5AB3B95
045451fa238a75305cc26ac982472367

SHA-256:

Network Signatures

Cobalt Strike http related X-Malware EICAR header

alert http any any -> any any (msg:"Cobalt Strike http related X-Malware EICAR header"; target:dest_ip; content:"X-Malware"; http_header; content:"EICAR-STANDARD-ANTIVIRUS-TEST-FILE"; http_header; within:64; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1000829; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Strike reported domain name (host4.marketshigh.com)

alert http any any -> any any (msg:"Cobalt Strike reported domain name (host4.marketshigh.com)"; target:src_ip; flow:established,to_server; content:"host4.marketshigh.com"; http_host; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1001420; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt-related DNS Lookup (host4.marketshigh.com)

alert udp any any -> any 53 (msg:"Cobalt-related DNS Lookup (host4.marketshigh.com)"; target:src_ip; flow:from_client; content:"|05|host4|0b|marketshigh|03|com|00|"; nocase; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1001421; rev:1; metadata:severity 5, ti_threatactor_id c509eac2111b5bd8b67314feb259572255c6f6cc, ti_threatactor_name Cobalt, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (wecloud.biz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (wecloud.biz)"; target:src_ip; flow:from_client; content:"|07|wecloud|03|biz|00|"; classtype:apt-trojan; nocase; sid:1001650; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (mail.maincdn.biz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (mail.maincdn.biz)"; target:src_ip; flow:from_client; content:"|04|mail|07|maincdn|03|biz|00|"; classtype:apt-trojan; nocase; sid:1001651; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (document.com.kz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (document.com.kz)"; target:src_ip; flow:from_client; content:"|08|document|03|com|02|kz|00|"; classtype:apt-trojan; nocase; sid:1001652; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Strike reported IP address

alert tcp $HOME_NET any -> [92.63.111.201,192.52.167.228,89.33.64.134,45.32.165.110,37.1.207.202,176.9.99.134,46.21.147.63,86.105.1.116] !445 (msg:"Cobalt Strike reported IP address"; target:src_ip; threshold:type limit, track by_src, seconds 30, count 1; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1001419; rev:2; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Win32.Trojan.Dropper Downloading Cobalt Strike Beacon

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan.Dropper Downloading Cobalt Strike Beacon"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:!"Referer|3a|"; nocase; http_header; content:!"Accept-Language|3a|"; nocase; http_header; content:"%20?id="; http_raw_uri; fast_pattern; pcre:"/\/%20\?id=\d*&act=\d*$/I"; classtype:apt-trojan; reference:md5,7edca868c6c52a9f7b24892dc361e444; sid:1001493; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (address-in.kz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (address-in.kz)"; target:src_ip; flow:from_client; content:"|0a|address-in|02|kz|00|"; classtype:apt-trojan; nocase; sid:1001790; rev:1; metadata:severity 5, ti_malware_id

b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS Response with payload

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"Cobalt Backdoor JS Response with payload"; target:dest_ip; flow:established,to_client; flowbits:isset,GIB.cobalt.backdoor.js.payload; file_data; content:"<package"; depth:8; content:"<component id="; distance:0; content:"<registration"; distance:0; content:"progid="; distance:0; content:"classid="; distance:0; content:"<script language=|22|JScript|22|"; distance:0; classtype:apt-trojan; reference:md5,bd07b04e008093a40f60e48b903c59cf; sid:1001728; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

TROJAN Cobalt Strike Exfiltration

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Cobalt Strike Exfiltration"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|43 6f 62 61 6c 74 20 53 74 72 69 6b 65 20 42 65 61 63 6f 6e 29|"; fast_pattern; http_user_agent; isdataat:!1,relative; http_header_names; content:!"Referer"; classtype:apt-trojan; sid:2025636; rev:1; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2018_07_03, deployment Perimeter, former_category TROJAN, signature_severity Major, updated_at 2020_09_16, severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin etpro;)

TROJAN CopyKittens Cobalt Strike DNS Lookup (cloudflare-analyse . com)

alert dns $HOME_NET any -> any any (msg:"TROJAN CopyKittens Cobalt Strike DNS Lookup (cloudflare-analyse . com)"; target:src_ip; dns_query; content:"cloudflare.analyse.com"; depth:22; nocase; isdataat:!1,relative; fast_pattern; threshold:type limit, track by_src, count 1, seconds 60; reference:url,www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf; reference:md5,752240cddda5acb5e8d026cef82e2b54; classtype:apt-trojan; sid:2024497; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_07_25, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_09_17, severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin etpro;)

b. METALJACK

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Other Name: Framwork

General information

Indicators of Compromise (IOCs)

CnC:
vitlescaux.com
141.98.212.23
MD5:
a4808a329b071a1a37b8d03b1305b0cb

SHA-256:

Network Signatures
N/A

c. KerrDown

The loader used by the OceanLotus group since March 2018.

Platform: N/A

Threat level: N/A

Category: N/A

Other Name: downloader

General information

Indicators of Compromise (IOCs)

CnC:
vitlescaux.com
141.98.212.23
account.dvrdns.org
https://outlook.updateoffices.net/vean32.png
88.150.138.114
https://cortanasyn.com/kirr64.png
cortanasyn.com
https://syn.servebbs.com/kuss32.gif
syn.servebbs.com

MD5:

6875F307D95790CA25C1DA542EA736A8
8D42D9FD3A4D32BC0474D07052CE8984
05b5707d79ca0aee269eb1b02db75b19
8ac2841fbb960a36739a958783ad1694
0a5e5a9a77e64d4fdd987ef7ae66fbe3
d279e98e77d895dc5a981bb8312a5918
3b36fb3a8cf15b0c5a288329e357e916
8ccfd46a24d3bcbee934af91dda8483d
a91e0c32ea93465b80d1bab41193ea4f
d568d10f3e66b89159abf402b31a37b8
f198ab61bc0bf8e5ae8c237d93c7b95d
cab262b84dbd319f3df84f221e5c451f
9bcd0b2590c53e4c0ed5614b127c6ba7
ac5f18f1c20901472d4708bd06a2d191
85dc4f704ee017844e84b42d4b17a1c3
50c6e221e5cd4f41973f3d6779ae1c4c
f5ad93917cd5b119f82b52a0d62f4a93
d6955b482cb67558e2152f6cdd0a2c91
77390c852addc3581d14acf06991982e
4973d4d95b17150153fddc07bbdb6575
49e969a9312ee2ae639002716276073f
6aa22d6c51ea5abe9a9af3a3fb51721b
b75bf1c32bcbe5dfd9261dd558b63277
611f35b485bf2b79db911842bb9d4e8f
c9093362a83b0e7672a161fd9ef9498a
305d992821740a9cbbda9b3a2b50a67c
c28abdfe45590af0ef5c4e7a96d4b979
bf040c081ad1b051fdf3e8ba458d3a9c
751c735585fdff7cb1bf2ae2f281393c
6c2a8612c6511df2876bdb124c33d3e1
1211dea7b68129d48513662e546c6e21
a406626173132c8bd6fe52672deacbe7
e04594ba7e2c63d4f48d92cc99246cce
43c03994e843164625794f4ac727811e
7338852de96796d7f733123f04dd1ae9
6b8fc8c9fe4f4ef90b2fcbcc0d24cfc9
4bdada3dea9b6bb14418e584c1b6af08
2f1f8142d479a1daf3cbd404c7c22f9f
c3bb2b1eabfb34181a9a052e4f06397c
7a6ba3e26c86f3366f544f4553c9d00a
4e7e56be0fdea72564ba761916897895
7df61bc3a146fcf56fe1bbd3c26ea8c0
d40b4277e0d417e2e0cff47458ddd62d

b1990e19efaf88206f7bffe9df0d9419
3c04352c5230b8cbaa12f262dc01d335
d65287550672dac1a89b804c90e7accf
9a10292157ac3748212fb77769873f6c
2756b2f6ba5bcf811c8baced5e98b79f
f3551be56b9f72374787442453bf0428
a530410bca453c93b65d0de465c428e4
c78fd680494b505525d706c285d5ebce
f42611ac0ea2c66d9f27ae14706c1b00
518f52aabd9a059d181bfe864097091e
3a869e8a7b7022082d5a8661ed2fb602
865a7e3cd87b5bc5feec9d61313f2944
760024b35e51a06dcde2128843b1bfdb
ce0afd0b440e25267a96e181d3d9ec5a
546bb6ef89bebfb053999777f6930d7e
38f9655c72474b6c97dc9db9b3609677
9972111cc944d20c9b315fd56eb3a177
0f877ad5464fcbb12e1c019adf7065cc

SHA-256:
5cda7d8294a8804d09108359dd2d96cdf4fdcf22ec9c00f0182d005afff76743

Network Signatures
N/A

d. OceanLotus.Denis

Denis is a simple backdoor developed by the OceanLotus Group, well observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.

Platform: Windows

Threat level: Middle

Category: Backdoor

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:
udt.sophiahoule.com
ourkekwiciver.com
dieordaunt.com
straliaenollma.xyz
andreagahuvrauvin.com
byronorenstein.com

stienollmache.xyz
Andreagbridge.Com
illagedrivestralia.Xyz
http://dload01.s3.amazonaws.com/b89fdbf4-9f80-11e7-abc4-2209cec278b6b50a/FirefoxInstaller.exe
nasahlaes.com
jeffreyue.com
rackerasr.com
urnage.com
maerferd.com
harinarach.com
eoneorbin.com
74.119.239.234
tsworthoa.com
orinneamoure.com
lbertussbau.com
arinaurna.com
icmannaws.com
avidsontre.com
aulolloy.com

MD5:

a8ff3e6abe26c4ce72267154ca604ce3
c7931fa4c144c1c4dc19ad4c41c1e17f
56b5a96b8582b32ad50d6b6d9e980ce7
DD8B36F8F967A26314820C35632FA0D0
F3551BE56B9F72374787442453BF0428
655C536462944D0F3C9FCF4EC19D2015
6AA3115FA1F3ADB8F0539E93D2CF21CA
DDD161A6BB63CA46E8CB0663587920FE
74731674920C51668C36CC3C16F30553
b612735909c41fb7a47e9c12fd1b6cfc
b123f9151c5e7057f061f3e03c1e8416
9453f31cdb02533d509948cc4fd0c44f
4282c6633122dce395de35c05159282d
eb2b52ed27346962c4b7b26df51ebafa
62944e26b36b1dcace429ae26ba66164
fcd7227891271a65b729a27de962c0cb
58d2907361f6414742dcc5071ca20980
1fa011e6a692ee95452c626e61b5263a
627e3ff5659b9a0ab9dc4b283c3288dd
d592b06f9d112c8650091166c19ea05a
88152846c45924d5706a11523942c82b
05bc07fc6265e6affa8478118c02942a

SHA-256:

Network Signatures
N/A

e. OceanLotus.masOS.Backdoor

It was discovered in November 2014. The Trojan was disguised as an Adobe Flash update and was used to attack macOS users by the OceanLotus APT group. The Trojan allows an attacker to manipulate the file system: transfer commands for execution via the command line; download files at a specific URL; modify files (as well as delete, move, copy); terminate processes. The components of the Trojan itself are encrypted, which complicates its analysis; in addition, the malware makes changes to the security settings of the Internet browser, thereby allowing attackers to download arbitrary files without the user's knowledge. The malware also checks for a running virtual environment and reads the OS version.

Platform: Mac

Threat level: N/A

Category: Backdoor

Other Name: N/A

General information

Indicators of Compromise (IOCs)
CnC:
web.dalalepredaa.com
rio.imbandaad.com
web.dalalepredaa.com
5.135.199.9

MD5:
06334cb14c1512bf2794af8dae5ab357
a76be0181705809898d5d7d9aed86ee8
da71b64e77ad45bab56cf71ecd4f55d4
306d3ed0a7c899b5ef9d0e3c91f05193
9831a7bfcf595351206a2ea5679fa65e

SHA-256:

Network Signatures
N/A

f. WINDSHIELD

A malicious program used by the group since 2014. Features WINDSHIELD communication via TCP; 4 C2 servers and 6 configured ports - a pair is chosen at random; manipulation of the

registry / file system; collecting information about the values of the registry, username and computer; termination of processes; loading additional modules.

Platform: N/A

Threat level: N/A

Category: Backdoor

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
7a81a6fdaee15162a3a231751bdd0259
189a078150b12baff608fc18af4bb837
5bcf16810c7ef5bce3023d0bbefb4391
79D06DD20768FD8CD4A043833C1F2D4B
Network Signatures
N/A

g. Denes

A dropper used by the OceanLotus group to install other malicious components and programs.

Platform: N/A

Threat level: N/A

Category: dropper

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
49a2e438309e219fa4d9c51dfb7ffcb1
96b971c9ac868c8d9ae98618b9a9bddc
88152846c45924d5706a11523942c82b
d592b06f9d112c8650091166c19ea05a

Network Signatures

N/A

h. OceanLotus.SteganoLoader

Loader used since September 2018 by the OceanLotus group. The downloader combines steganography and Dll Side-loading techniques, which allows you to download malware using legitimate software along with .png images.

Platform: N/A

Threat level: N/A

Category: Loader, APT

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
c55f1145ecc9ea52b2872a99a3f04eb4
bbeba6edfea62c34ab92a60e86fd7ce7
ec52a11625bdb4aad3740ff8cc6d8c0f
1675afb65f32c7b148f5d8acbeed2acc
43b57414a07f69aa87ad3ec85fb06b6d
f6c672a15b2c5101279a6420f8d4ecc7
71f512da26deeeceb7e41fbb6a5e3267
08c984ac6b0e0a291f16d0c249310a14
SHA-256:
a2719f203c3e8dcdcc714dd3c1b60a4cbb5f7d7296dbb88b2a756d85bf0e9c1e

Network Signatures
N/A

i. Downloader

A program that can install malicious components and programs. The dropper can be either another malicious program or legitimate software infected with malicious code.

Platform: N/A

Threat level: N/A

Category: Trojan

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:

ourkekwiciver.com
dieordaunt.com
straliaenollma.xyz
andreagahuvrauvin.com
byronorenstein.com
stienollmache.xyz
Andreagbridge.Com
illagedrivestralia.Xyz
164.132.45.67
192.34.109.173
http://defprocindia.com/register.doc
defprocindia.com
162.255.119.117
http://www.oxfam.org/en/invitation<https://drive/google/com/file/s/0B7fMhZc0wl0OeTJpZmViQXU4YVE/edit?usp=sharing
www.oxfam.org
151.236.216.85
tripadvisor.dyndns.info
62.75.204.91
neuro.dyndns-at-home.com
foursquare.dyndns.tv
wowwiki.dynalias.net
yelp.webhop.org
179.43.134.61

MD5:

b123f9151c5e7057f061f3e03c1e8416
9453f31cdb02533d509948cc4fd0c44f
4282c6633122dce395de35c05159282d
3dfc49add45ad35a7c6e21054a53a351
a3d09d969df1742a7cc9511f07e9b44b
6ecb19b51d50af36179c870f3504c623
109cd896f8e13f925584dbbad400b338
A08b9a984b28e520cbde839d83db2d14
877ecaa43243f6b57745f72278965467
87d108b2763ce08d3f611f7d240597ec
5f69999d8f1fa69b57b6e14ab4730edd
75a00fcede0b91793a19295a8b9a7060
cd74dd88322431441fb1088ac7dd6715
e3e99f6d1333ca76a80ba2899a4e2587
02AE075DA4FB2A6D38CE06F8F40E397E
B10F93CDBCDF43D4C5C5770872E239F4
fd4e2b72bbd5f0f27eb5788cc6a7dedd

da71b64e77ad45bab56cf71ecd4f55d4
9831a7bfcf595351206a2ea5679fa65e
d1233d34fcbd643b8c03c026dc4b2e7e
af170750a8228c9e5f21bfc35fc67721
6e667d6c9e527ada1a3284aa333d954d
616d32151c907fdd4e718bde2163cc40
1a60715c51da0caa8a5ebff6fdc9d472

SHA-256:
2fa7ad4736e2bb1d50cbaec625c776cdb6fce0b8eb66035df32764d5a2a18013

Network Signatures
N/A

j. OceanLotus.Backdoor

The backdoor that the OceanLotus group has been using since May 2017. Backdoor features: system fingerprint; setting the session identifier; creating a process and getting the result of execution; getting information from a file or registry key and calculating MD5; creating / deleting / moving directories / files; creating an entry in the registry or a stream in memory; file system search; creating a list of logical drives; install and run the program; switch to HTTP; reboot; setting / retrieving environment variables; running shellcode in a new thread.

Platform: N/A

Threat level: N/A

Category: Trojan

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:
tephens.com
traveroyce.com

MD5:
B10F93CDBCDF43D4C5C5770872E239F4
72A5AD375401F33A5079CAEE18884C9D
79D06DD20768FD8CD4A043833C1F2D4B
EC505565E4CB5A22BFD3F63E4AD83FF3
93da064e3fc4422c63fecca93ee1b157
a7f98d3b7b7e2a7d1c194c2f26045618
96b971c9ac868c8d9ae98618b9a9bddc

SHA-256:

Network Signatures
N/A

k. PhantomLance

PhantomLance is a malicious program for the Android operating system. This malware able to collect confidential information from the victim's device. To do this, the malware can obtain root rights on the device, and thus gain the ability to transmit geolocation data, a call log, SMS messages, a list of installed applications, and full information about the infected device to its operators. At the same time, its functionality can be expanded at any time by loading additional modules from the C&C server.

Platform: N/A

Threat level: N/A

Category: Backdoor

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:

MD5:
2e06bbc26611305b28b40349a600f95c
b1990e19efaf88206f7bffe9df0d9419
7048d56d923e049ca7f3d97fb5ba9812
e648a2cc826707aec33208408b882e31
3285ae59877c6241200f784b62531694
8d5c64fdaae76bb74831c0543a7865c3
6bf9b834d841b13348851f2dc033773e
0d5c03da348dce513bf575545493f3e3
0e7c2adda3bc65242a365ef72b91f3a8
a795f662d10040728e916e1fd7570c1d
d23472f47833049034011cad68958b46
8b35b3956078fc28e5709c5439e4dcb0
af44bb0dd464680395230ade0d6414cd
65d399e6a77acf7e63ba771877f96f8e
79f06cb9281177a51278b2a33090c867
b107c35b4ca3e549bdf102de918749ba
83cd59e3ed1ba15f7a8cadfe9183e156
c399d93146f3d12feb32da23b75304ba
83c423c36ecda310375e8a1f4348a35e

94a3ca93f1500b5bd7fd020569e46589
54777021c34b0aed226145fde8424991
872a3dd2cd5e01633b57fa5b9ac4648d
243e2c6433815f2ecc204ada4821e7d6
a330456d7ca25c88060dc158049f3298
a097b8d49386c8aab0bb38bbfdf315b2
7285f44fa75c3c7a27bbb4870fc0cdca
b4706f171cf98742413d642b6ae728dc
8008bedaaebc1284b1b834c5fd9a7a71
0e7b59b601a1c7ecd6f2f54b5cd8416a

SHA-256:

Network Signatures

N/A

I. OceanLotus.Encryptor

OceanLotus Encryptor - First discovered in February 2014. The Trojan is an executable file masquerading as JPG or Word files. To bypass security systems, the program, by filling with random characters, increases the file size, which leads to the fact that the file becomes too large for uploading to cloud systems for their subsequent analysis. The Trojan is also capable of detecting the virtual environment and, in case of a positive result, stops further execution.

Platform: N/A

Threat level: N/A

Category: Trojan

Other Name: N/A

General information

Indicators of Compromise (IOCs)

CnC:

active.soariz.com
193.169.244.73

MD5:

0529b1d393f405bc2b2b33709dd57153
d39edc7922054a0f14a5b000a28e3329
d1233d34fcbd643b8c03c026dc4b2e7e
41bced8c65c5822d43cadad7d1dc49fd

SHA-256:

Network Signatures

N/A