NCCIC NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER | US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Analysis Report (MAR) - 10135536-B

2017-12-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government - referred to by the U.S. Government as BANKSHOT. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov/hiddencobra.

FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation. DHS and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity.

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Users or administrators should flag activity associated with the malware, report the activity to the DHS National Cybersecurity and Communications Integration Center (NCCIC) or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.

This report provides analysis of seven (7) malicious executable files. Five (5) of these files are proxy applications that all use a similar cipher algorithm to mask traffic between the malware and the remote operator. Additionally, two of the five proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors. The remaining two (2) executables are remote access tools (RATs), providing remote users with the ability to run various commands on an infected system. One of these RATs uses a cipher and the OpenSSL library to add a layer of encryption to communications between the infected system and its command and control (C2) server; this RAT may have been used to install the proxy servers onto compromised systems.

The following YARA signature can be used to detect the proxy servers and RATs:

```
rule Unauthorized_Proxy_Server_RAT
{
meta:
  Author="US-CERT Code Analysis Team"
  Incident="10135536"
  MD5_1 = "C74E289AD927E81D2A1A56BC73E394AB"
  MD5_2 = "2950E3741D7AF69E0CA0C5013ABC4209"
  Info="Detects Proxy Server RAT"
  super_rule = 1

strings:
  $s0 = {8A043132C288043125FF00000003C299F73D40404900A14440490003D0413BCF72DE5E5FC3}
  $s1 = {8A04318844241432C28804318B44241425FF00000003C299F73D40404900A14440490003D0413BCF72D65E5FC3}
  $s2 = {8A04318844241432C28804318B44241425FF00000003C299F73D5C394100A16039410003D0413BCF72D65E5FC3}
  $s3 = {8A043132C288043125FF00000003C299F73D5C394100A16039410003D0413BCF72DE5E5FC3}
  $s4 = {B91A7900008A140780F29A8810404975F4}
  $s5 = {399FE192769F839DCE9F2A9D2C9EAD9CEB9FD19CA59F7E9F539CEF9F029F969C6C9E5C9D949FC99F}
  $s6 = {8A04318844241432C28804318B44241425FF00000003C299F73D40600910A14460091003D0413BCF72D65E5FC3}
```

```
$s7 = {3C5C75208A41014184C074183C72740C3C7474083C6274043C2275088A41014184C075DC}
$s8 = {8B063D9534120077353D59341200722E668B4604663DE8037F24}
$s9 = {8BC88B74241CC1E1052BC88B7C2418C1E1048B5C241403C88D04888B4C242083F9018944240C7523}
$s10 = {8B063D9034120077353D59341200722E668B4604663DE8037F246685C0}
$s11 = {30110FB60148FFC102C20FBEC09941F7F94103D249FFC875E7}
$s12 = {448BE8B84FECC44E41F7EDC1FA038BCAC1E91F03D16BD21A442BEA4183C541}
$s13 = {8A0A80F9627C2380F9797F1E80F9647C0A80F96D7F0580C10BEB0D80F96F7C0A80F9787F05}

condition:
any of them
}
```

Files

Processed	7 0137f688436c468d43b3e50878ec1a1f (0137F688436C468D43B3E50878EC1A1F) 114d8db4843748d79861b49343c8b7ca (114D8DB4843748D79861B49343C8B7CA) 2950e3741d7af69e0ca0c5013abc4209 (2950E3741D7AF69E0CA0C5013ABC4209) 964b291ad9bafa471da3f80fb262dbe7 (964B291AD9BAFA471DA3F80FB262DBE7) 9e4d9edb07c348b10863d89b6bb08141 (9E4D9EDB07C348B10863D89B6BB08141) c74e289ad927e81d2a1a56bc73e394ab (C74E289AD927E81D2A1A56BC73E394AB) fc9e40100d8dfae2df0f30a3414f50ec (FC9E40100D8DFAE2DF0F30A3414F50EC)

Files

C74E289AD927E81D2A1A56BC73E394AB

Details

Name	C74E289AD927E81D2A1A56BC73E394AB
Size	675840
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	c74e289ad927e81d2a1a56bc73e394ab
SHA1	771f7d69a476d5b0b7c942bdc21e86691dabba89
ssdeep	12288:NxZ0n+1OzKZDK+xgYDUWfVUBXfJFzLlrpoqR:a+EzUfVUNfPz9poq
Entropy	6.65567602919

Antivirus

K7	Trojan (700000041)
Cyren	W32/Heuristic-KPP!Eldorado
VirusBlokAda	BScope.Trojan.Agent

PE Information

Compiled	2016-06-21T05:56:00Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	f4c5b7ebe0ffb8c5d5632877552f2e23	4096	0.649735689975
.text	d2cf27a072c85308a12b834aa3150af0	442368	6.63294155589
.rdata	bc433c07b82c684a09d26e014c0cefdb	159744	6.13100276138
.data	1cfe81260eb717a1b917d7b3d1349851	69632	4.94697538055

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Description

This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations. When executed, the malware binds to the victim system and listens to activity on port 110. Static analysis of this application indicates that its primary purpose is to force a compromised system to function as a proxy server for Internet connections. This capability enables an operator to securely access the Internet through the compromised host. Data to and from the victim system is encoded to prevent identification of the proxy sessions by firewalls or network analysis devices.

Analysis of the cipher algorithm indicates it uses a four-byte key. When the compromised system operating as a proxy server receives an initial connection from the operator, it expects to receive the four-byte key. The malware accepts six additional bytes, which is decoded by using the cipher and the previously received four bytes. The malware verifies the first four bytes received from the operator are between the values 00123459h and 00123490h. If the first four bytes do not fall between these values, the malware terminates the session with the operator. If the first four of these six bytes are between the specified values, the malware accepts the additional data. From the previous six bytes of data, the fifth and sixth byte are used to make up a double word value, which is used to identify the size of the data the malware expects to arrive next. If the double word value is larger than 1,000 bytes, the malware will terminate the connection. Analysis indicates this is a safety mechanism built into the software to protect it from buffer or heap sprays.

FC9E40100D8DFAE2DF0F30A3414F50EC

Details

Name	FC9E40100D8DFAE2DF0F30A3414F50EC
Size	684032
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	fc9e40100d8dfae2df0f30a3414f50ec
SHA1	566243e09a3d19828c243c799f638ae34469d967
ssdeep	12288:DlvM82yKa7LYlSZJMmHsf82mdQIQYlFph:ziQi82gQH4ph
Entropy	6.62263634126

Antivirus

Cyren	W32/Heuristic-KPP!Eldorado
VirusBlokAda	BScope.Trojan.Agent

PE Information

Compiled	2016-04-24T01:55:11Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	a679879146f59c7ba1b29ff42851a5ed	4096	0.627951249971
.text	d25e32c2f4c243f8b0fb537b73c6f07c	442368	6.65458990149
.rdata	b94f8f257f9ebfb122acf253691a713e	159744	6.13277165525
.data	4dfa17c0b8e612b8d4db9cea10b5a3d7	77824	4.54069669695

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Description

This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations. When executed, the malware binds to the victim system and listens to activity on port 110. Static analysis indicates the malware's primary purpose is to force a previously compromised server to function as a proxy server. This file is similar in design and functionality to the file C74E289AD927E81D2A1A56BC73E394AB.

0137F688436C468D43B3E50878EC1A1F

Details

Name	0137F688436C468D43B3E50878EC1A1F
Size	737280
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	0137f688436c468d43b3e50878ec1a1f
SHA1	f4088bca25fd9ee78119458bfb300721266ecbcb
ssdeep	6144:MMYkRFxwXGv6d64L6G0kyU/CyS9fNe4fDDxCtMOhYr437HimZ508poBBanFq8StJ:VXv6d0lJWfD8BCiv48HepV8gdU0z
Entropy	6.59562883528

Antivirus

F-secure	Gen:Trojan.Heur.LP.Tu4@aqf3yp
BitDefender	Gen:Trojan.Heur.LP.Tu4@aqf3yp
Emsisoft	Gen:Trojan.Heur.LP.Tu4@aqf3yp (B)

PE Information

Compiled	2016-05-20T07:15:22Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	e385ce08c1c7b68edfc2150f3682b256	4096	0.771172194608
.text	fc14f0c7ff263b01c27ac84ff16072e6	462848	6.59870923197
.rdata	a5166df020ef131fd115707cf8e284ce	147456	5.90353775299
.data	5271c65208ed70fad30077524f371ed8	77824	4.90723221684
.rsrc	620f0b67a91f7f74151bc5be745b7110	4096	0.0
.reloc	3dfc4d44b2b523659f00d8945225bc60	40960	5.73692004764

Packers

Name	Version	Entry Point
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

Description

This artifact is a malicious Windows dynamic-link library (DLL) and is similar in design and functionality to the file C74E289AD927E81D2A1A56BC73E394AB. The primary difference is that this file is a Windows DLL instead of a Windows executable.

Static analysis indicates this application uses the OpenSSL library to add an additional layer of encryption over the traffic between the operator and the proxy malware. The malware accepts four bytes of data, used as an argument to the Win32 API, setsockopt. When executed, this proxy binds to the victim system and listens to activity on port 1030.

114D8DB4843748D79861B49343C8B7CA

Details

Name	114D8DB4843748D79861B49343C8B7CA
Size	159744
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	114d8db4843748d79861b49343c8b7ca
SHA1	bbf1ff28e84766ad27683cc9078d16f0493cdbab
ssdeep	1536:q17RHwAbgW3yPEzf77thIovuczbJ4YNiDIovuczbJ4YNibIovuczbJ4YNi:trNsz3t2oPz+n0oPz+nsoPz+n
Entropy	6.83923058232

Antivirus

F-secure	Gen:Variant.Graftor.373993
Cyren	W32/Heuristic-KPP!Eldorado
VirusBlokAda	BScope.Trojan.Agent
BitDefender	Gen:Variant.Graftor.373993
Emsisoft	Gen:Variant.Graftor.373993 (B)

PE Information

Compiled	2016-03-01T00:21:03Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	1ce8e90ffa2199ff32be8b977e9a441b	4096	0.650753707439
.text	caef1f2015675da6b139275b4c7c86d3	40960	6.45414824189
.rdata	62a4ecd0721de04fc52f5fcef933ee44	4096	4.88154271504
.data	941009d7534325e92b5a0183b05aec00	106496	6.93256592914
.rsrc	f0a1309490c5ee84dedc04b035c45cd0	4096	0.231410143047

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) 114D8DB4843748D79861B49343C8B7CA (114d8)	Characterized_By	(S) Figure 1: Hidden Cobra communication flow

Description

This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations. When executed, the malware binds to the victim system and listens to port 1058. Static analysis of this application indicates that its primary purpose is to force a compromised server to function as a proxy server for Internet connections.

This file is similar in design and functionality to the file C74E289AD927E81D2A1A56BC73E394AB, but with the additional capability of providing what appear to be proxied SSL encrypted sessions using public certificates from well-known, legitimate internet services. When communicating with its C2, the malware attempts to disguise traffic by generating a false TLS handshake using a public certificate from one of the sites listed below. Note: the malware does not communicate with any of the servers listed:

--Begin Public Websites--

myservice.xbox.com
uk.yahoo.com
web.whatsapp.com

www[.]apple.com
www[.]baidu.com
www[.]bing.com
www[.]bitcoin.org
www[.]comodo.com
www[.]debian.org
www[.]dropbox.com
www[.]facebook.com
www[.]github.com
www[.]google.com
www[.]lenovo.com
www[.]microsoft.com
www[.]paypal.com
www[.]tumblr.com
www[.]twitter.com
www[.]wetransfer.com
www[.]wikipedia.org

--End Public Websites--

Static analysis reveals this malware contains an embedded XOR-encoded block of data that is 31,002 bytes in size. The malware decodes this block by XORing it with the value "9Ah". Analysis of this decoded block indicates it contains public SSL encryption certificates for the sites listed above. Strings of interest from the decoded data are displayed below:

--Strings of Interest--

com1
microsoft1
corp1
redmond1
MSIT Machine Auth CA 20
130322100818Z
150322100818Z0
myservice.xbox.com0

Ohttp[:]//mscrl.microsoft.com/pki/mscorp/crl/MSIT%20Machine%20Auth%20CA%202(1).crl
Mhttp[:]//crl.microsoft.com/pki/mscorp/crl/MSIT%20Machine%20Auth%20CA%202(1).crl
8http[:]//corppki/crl/MSIT%20Machine%20Auth%20CA%202(1).crl0
Ihttp[:]//www[.]microsoft.com/pki/mscorp/MSIT%20Machine%20Auth%20CA%202(1).crt0D
8http[:]//corppki/aia/MSIT%20Machine%20Auth%20CA%202(1).crt0?

VeriSign, Inc.1
VeriSign Trust Network1;09
2Terms of use at https[:]//www[.]verisign.com/rpa (c)101/0-
&VeriSign Class 3 Secure Server CA - G30
140924000000Z
150925235959Z0
US1
California1
Sunnyvale1
Yahoo Inc.1
Information Technology1
www[.]yahoo.com0
DigiCert Inc1'0%
DigiCert SHA2 Secure Server CA0
130802000000Z
160805120000Z0l1
US1
California1
Santa Clara1
WhatsApp, Inc.1
web.whatsapp.com0
_xC,aa
gu(
_:mz%`
WpG0UXI
&P9s
web.whatsapp.com
w1.web.whatsapp.com

w2.web.whatsapp.com
w3.web.whatsapp.com
w4.web.whatsapp.com
w5.web.whatsapp.com
w6.web.whatsapp.com
w7.web.whatsapp.com
w8.web.whatsapp.com
w9.web.whatsapp.com
w10.web.whatsapp.com0
Symantec Corporation1
Symantec Trust Network1(0&
Symantec Class 3 EV SSL CA - G30
141219000000Z
16041623595 9Z0
US1
California1
Private Organization1
C0806592
US1
950141
California1
Cupertino1
1 Infinite Loop1
Apple Inc.1%0#
Internet Services for Akamai1
www[.]apple.com0
VeriSign, Inc.1
VeriSign Trust Network1;09
2Terms of use at https[:]//www[.]verisign.com/rpa (c)101/0-
&VeriSign Class 3 Secure Server CA - G30
140609000000Z
1506092359 59Z0
CN1
beijing1
beijing1907
0BeiJing Baidu Netcom Science Technology Co., Ltd1%0#
service operation department1
Washington1
Redmond1
Microsoft Corporation1
Microsoft IT1
Microsoft IT SSL SHA20
141212193042Z
16121119304 2Z0
www[.]bing.com0
GeoTrust Inc.1 0
RapidSSL SHA256 CA - G30
141210012651Z
17011021182 4Z0
GT03479942110/
(See www[.]rapidssl.com/resources/cps (c)141/0-
&Domain Control Validated - RapidSSL(R)1
www[.]bitcoin.org0
Greater Manchester1
Salford1
COMODO CA Limited1402
+COMODO Extended Validation Secure Server CA0
131212000000Z
1512122359 59Z0
38301381
US1
Delaware1
Private Organization1
US1
070131
NJ1
Clifton1
Suite 1001
1255 Broad St.1

Comodo Group Inc.1
COMODO EV SSL1
COMODO EV SGC SSL1
www[.]comodo.com0
Paris1
Paris1
Gandi1 0
Gandi Standard SSL CA 20
141217000000Z
151231235959Z0U1!0
Domain Control Validated1
Gandi Standard SSL1
debian.org0
DigiCert Inc1
www[.]digicert.com1402
+DigiCert SHA2 Extended Validation Server CA0
141024000000Z
16102812000Z0
Private Organization1
US1
Delaware1
43482961
185 Berry St STE 4001
941071
US1
California1
San Francisco1
Dropbox, Inc1
www[.]dropbox.com0

--End Strings of Interest--

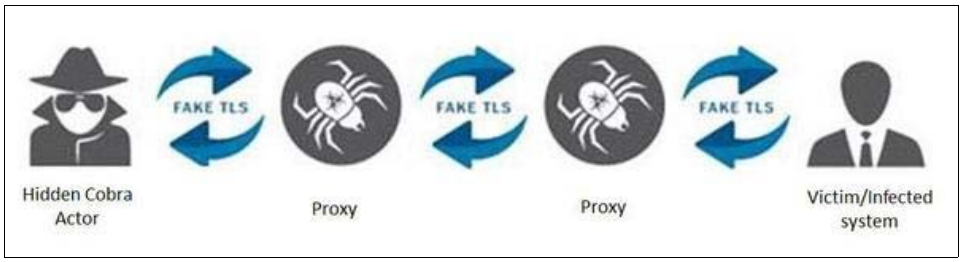
This malware uses a cipher and authentication method similar to that used by C74E289AD927E81D2A1A56BC73E394AB for encrypting network communication between itself and a remote operator.

The cipher and communication method, coupled with the malware's ability to create falsified TLS handshake traffic, allows the operator to disguise network connections and obfuscate network traffic sent to and from a remote system.

See Figure 1 below for an illustration of the malware's communication flow using this proxy software.

Screenshots

- **Figure 1: Hidden Cobra communication flow**



9E4D9EDB07C348B10863D89B6BB08141

Details

Name	9E4D9EDB07C348B10863D89B6BB08141
Size	114688
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	9e4d9edb07c348b10863d89b6bb08141
SHA1	65122e5129fc74d6b5ebafcc3376abae0145bc14
ssdeep	1536:fwO0XhTH/oB3ALcqmr3+vycketJIovuczbJ4YNiS:v6Z1VC3+vycketeoPz+nS
Entropy	6.05304069999

Antivirus

F-secure	Gen:Trojan.Heur.LP.hu4@aKqgOsli
BitDefender	Gen:Trojan.Heur.LP.hu4@aKqgOsli
Emsisoft	Gen:Trojan.Heur.LP.hu4@aKqgOsli (B)

PE Information

Compiled	2016-04-24T02:27:29Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	f82e3e0c1cadda61be2ed2885911bd3d	4096	0.724408322087
.text	c3349c549162ffa3b8148d564efdfd0e	45056	6.55964269599
.rdata	6e90fb74568b471c2699f72b7cae68dc	8192	3.30149343314
.data	0e0f176e5767c4f278df968c7364e815	45056	6.22326236797
.rsrc	6c330d24bbac0cdc751eb2033a2ab6c7	4096	0.231505445665
.reloc	5b8468fde2fdd44adf4eba4d955fa265	8192	3.21012791926

Packers

Name	Version	Entry Point
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

Description

This artifact is a malicious Windows DLL and is similar in design and functionality to the file 114D8DB4843748D79861B49343C8B7CA. The malware also contains 31,002 bytes of XOR-encoded public SSL certificates for public Internet service providers. The public SSL certificates stored within this application are identical to those stored within 114D8DB4843748D79861B49343C8B7CA. It decodes the public SSL certificates via an XOR with the value "9Ah".

2950E3741D7AF69E0CA0C5013ABC4209

Details

Name	2950E3741D7AF69E0CA0C5013ABC4209
Size	827904
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	2950e3741d7af69e0ca0c5013abc4209
SHA1	af9db3ed2605572e9897d71086308873045be47b
ssdeep	12288:Aq/TlttbCSvbcEk8NJ7WIf/sI5xxcSZ/pbEzF87mc+BHFtLMBmLlBpyovNh2M4Ks:Aq7lttbE8JHy87D+9FtMmpyRKWF
Entropy	6.79960385183

Antivirus

F-secure	Trojan.Inject.RO
VirusBlokAda	BScope.Trojan.Agent
Ahnlab	Trojan/Win32.Akdoor

PE Information

Compiled	2016-06-22T04:13:36Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	cfc3f97af184f52c091a175eda4587b8	1024	2.71795432504
.text	51e2667d68017283e27efb2950932c58	539648	6.70314771616
.rdata	15e68b7d71ae9401600fbf50c1f37e66	175104	6.18962071273
.data	aa336c62ce0214b5ffe1d41d93d6e99b	66560	5.25915313943
.rsrc	f77d3025527d202bbe572f5791d038d3	1024	4.79504070454
.reloc	ceb5df2b67157dbc6b6aac93c8524f3d	44544	5.79343910767

Packers

Name	Version	Entry Point

Microsoft Visual C++ DLL *sign by CodeRipper	NA	NA

Description

The artifact is a malicious Windows DLL application and was identified as a RAT, disguised as an installer for a generic security application. When the file installs, the malware will expect the "SYSTEM\\CurrentControlSet\\Control\\LSA = Security Packages" registry key to be configured properly before loading the DLL onto the operating system as a security package. Analysis suggests an external loader application was used to load this DLL.

The malware searches the system for configuration data by checking for the presence of the registry key "SOFTWARE\\Microsoft\\Qnuimh = DataPath". If the registry key is not found, the malware attempts to read a file named "system32\\msncf.dat" to access the configuration data. If neither the registry key or .dat file are found, the malware's main thread does not execute.

Static analysis of the main thread reveals it is designed to provide C2 of the infected system to a remote operator. This file uses a cipher and authentication method similar to that of files C74E289AD927E81D2A1A56BC73E394AB and 114D8DB4843748D79861B49343C8B7CA.

The malware uses the OpenSSL library to provide an additional layer of SSL encryption to the communications between the operator and malware. This SSL encryption is used in addition to the cipher. The RAT provides the ability to exfiltrate and upload files to and from the compromised system and terminate processes. It also provides the ability to upload and execute secondary payloads. The OpenSSL library and XOR cipher will protect the data uploaded and exfiltrated by the RAT. No hard coded C2s were found in the DLL. However, a common Domain Generation Algorithm was identified, indicating the malware dynamically generates a domain from the current date and time.

964B291AD9BAFA471DA3F80FB262DBE7

Details

Name	964B291AD9BAFA471DA3F80FB262DBE7
Size	95232
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	964b291ad9bafa471da3f80fb262dbe7
SHA1	350778fc552918dddf84ea3a4c956e9996afe0d5
ssdeep	1536:wMfUQwrWeCIpgfAkbU/cnIIytNvMv5K9gnaCrq+gNvw1hqBgOleTNjw2pS9:wMsQLIp6bU/cn7eI49lCrq/pwOBgOle8
Entropy	6.10686715126

Antivirus

nProtect	Trojan/W64.Agent.95232
McAfee	Trojan-FLDA!964B291AD9BA
ClamAV	Win.Trojan.Agent-6319549-0
Ahnlab	Trojan/Win64.Dllbot
Quick Heal	Trojan.Generic

PE Information

Compiled	2014-03-04T09:43:53Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	ab32b3c672765e57e0892dc1f046728a	1024	2.72686979002
.text	4aef9d49dc3fe0af76cecb93904875c0	65024	6.26878660906
.rdata	720f2fd596b0523ad6da7864337a3e3a	15360	5.47919921082
.data	03e0ab7f93b56899460fda790387d7c1	8192	4.15642395322
.pdata	324652d914c29aa7a7081d418add47dc	3584	4.70286078328
.rsrc	f5391c0baa8c69ab8fc159089099c8c4	1536	4.39600332665
.reloc	2de998d058c83ca559bc6a4b4b4d40b6	512	1.93486789339

Description

This artifact is a malicious 64-bit DLL. This DLL was installed as a service, with an export "ServiceMain". The installer for this file was not included in the submission. This file contains obfuscated API names and is designed to listen for commands and access requests from a remote server.

When executed, the malware verifies if it is running as a service and attempts to read the following files:

--Begin files--

"%system32%\msncf.dat"
"%AppData%\Local\Temp\~DFB3090EB172633EA.TMP"

--End files--

The files were not part of the submission.

The malware is designed to load or write data into the following registry key:

--Begin key--

hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\\Microsoft\\Pniumj"
ValueName = "DataPath"

--End key--

The data the malware attempts to load or write was not included in the submission.

The malware is designed to listen for commands or access requests from a remote server. This backdoor allows for the following remote operations:

--Begin operations--

Mimic Timestamp
Execute Shell Command
Change Listening Port and proxy
Gather system information
Upload files Install configuration in the registry
Create, start, and terminate a new process and its primary thread
Search, read, write, move, download, and execute files
Delete all artifacts associated with the malware from the infected system
Send Status
Retrieves information about all installed disk, including the disk type and the amount of free space on the disk

--End operations--

Relationship Summary

(F) 114D8DB4843748D79861B49343C8B7CA (114d8)	Characterized_By	(S) Figure 1: Hidden Cobra communication flow
(S) Figure 1: Hidden Cobra communication flow	Characterizes	(F) 114D8DB4843748D79861B49343C8B7CA (114d8)

Mitigation Recommendations

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- 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.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- 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 thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MAR? A Malware Analysis Report (MAR) is intended to provide detailed code analysis and insight into specific tactics, techniques, and procedures (TTPs) observed in the malware.

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 US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

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

US-CERT 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 US-CERT's homepage at www.us-cert.gov.

TLP:WHITE