





# Malware Analysis Report (MAR) - 10135536-F

# 2018-02-05

# **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 <a href="http://www.us-cert.gov/tlp/">http://www.us-cert.gov/tlp/</a>.

# **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 – commonly known as HARDRAIN. 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 three (3) malicious executable files. The first two (2) files are 32-bit Windows executables that function as Proxy servers and implement a "Fake TLS" method similar to the behavior described in a previously published NCCIC report, MAR-10135536-B. The third file is an Executable Linkable Format (ELF) file designed to run on Android platforms as a fully functioning Remote Access Tool (RAT).

#### **Files**

#### Processed

3

3dae0dc356c2b217a452b477c4b1db06 (3DAE0DC356C2B217A452B477C4B1DB06) 746cfecfd348b0751ce36c8f504d2c76 (746CFECFD348B0751CE36C8F504D2C76) 9ce9a0b3876aacbf0e8023c97fd0a21d (9CE9A0B3876AACBF0E8023C97FD0A21D)

TLP:WHITE

US-CERT MAR-10135536-F 1 of 10

# **Files**

# 3DAE0DC356C2B217A452B477C4B1DB06

Details	
Name	3DAE0DC356C2B217A452B477C4B1DB06
Size	336073
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	3dae0dc356c2b217a452b477c4b1db06
SHA1	4efb9c09d7bffb2f64fc6fe2519ea85378756195
ssdeep	3072: jUdidTaC07z IQt9xSx1pYxHvQY06emquSYttxlxep0xnC: jyi1XCzcbpYdvQ2e9g3kp01C
Entropy	6.65226708818

		us

McAfee	BackDoor-FCIV!3DAE0DC356C2
К7	Trojan ( 004be70e1 )
Symantec	Heur.AdvML.B
BitDefender	Gen:Variant.Graftor.185553
Microsoft Security Essentials	Backdoor:Win32/Escad.A!dha
Emsisoft	Gen:Variant.Graftor.185553 (B)
Avira	TR/Agent.cjav
Ahnlab	Backdoor/Win32.Akdoor
ESET	a variant of Win32/NukeSped.M trojan
NANOAV	Trojan.Win32.Agent.ebiijz
Vir.IT eXplorer	Backdoor.Win32.Generic.AIVO
AVG	BackDoor.Generic19.AIVO

#### PE Information

2016-01-29T09:21:46Z Compiled

PE Sections	
Name	

Name	MD5	Raw Size	Entropy
(header)	e14dca360e273ca75c52a4446cd39897	4096	0.672591739631
.text	076cdf2a2c0b721f0259de10578505a1	49152	6.41338619924
.rdata	4a6af2b49d08dd42374deda5564c24ef	8192	3.293891672
.data	c797dda9277ee1d5469683527955d77a	110592	6.78785911234
.reloc	fbefbe53b3d0ca62b2134f249d249774	8192	3.46819043887

# **Packers**

Name	Version	<b>Entry Point</b>
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

# Description

This artifact (original name: ProxyDII.dll) is a malicious PE32 DLL designed to open the Windows Firewall on the victim's machine to allow incoming connections and force the compromised system to function as a proxy server.

The proxy sessions are disguised to appear as encrypted TLS/SSL sessions by using public SSL certificates obtained from well-known, legitimate Internet services. The legitimate certificates are contained within the malware. However, the traffic between the operator and the proxy server is encrypted using an unidentified cipher. This "fake TLS" behavior is similar to behavior described in an earlier NCCIC malware report, MAR-10135536-B. Strings of interest extracted from these public SSL certificates are displayed below. Note: the malware does not communicate with any of the servers listed:

--Begin SSL CERT Strings--

www[.]dropbox.com support.dropbox.com live.dropbox.com

**TLP:WHITE** 

opensource.dropbox.com linux.dropbox.com texter.dropbox.com0 n0l04 .http[:]//crl3.digicert.com/sha2-ev-server-g1.cr 04 .http[:]//crl4.digicert.com/sha2-ev-server-g1.cr 0B ;0907 0\*0( https[:]//www[.]digicert.com/CPS0 |0z0\$ http[:]//ocsp.digicert.com0R Fhttp[:]//cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt0 DigiCert Inc1 www[.]digicert.com1%0# DigiCert High Assurance CA-30 140828000000Z 151028120000Z0a1 US1 CA1 Menlo Park1 Facebook, Inc.1 \*.facebook.com0Y0 **I**\*% %1\N K03 \*.facebook.com facebook.com \*.fbsbx.com \*.fbcdn.net \*.xx.fbcdn.net \*.xy.fbcdn.net fb.com \*.fb.com \*.facebookcorewwwi.onion facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion \*.m.facebook.com \*.messenger.com messenger.com0 Z0X0\* \$http[:]//crl3.digicert.com/ca3-g29.crl0\* \$http[:]//crl4.digicert.com/ca3-g29.crl0B www[.]digicert.com1402 +DigiCert SHA2 Extended Validation Server CA0 140408000000Z 160412120000Z0 Private Organization1 US1 Delaware1 51575501 548 4th Street1 941071 US1 California1 San Francisco1 GitHub, Inc.1 github.com0 MoC +m8 6V! Mx\$ f%i ;rnO tev ,Ob

**TLP:WHITE** 

github.com

www[.]github.com0

n0l04

.http[:]//crl3.digicert.com/sha2-ev-server-g1.cr 04

.http[:]//crl4.digicert.com/sha2-ev-server-g1.cr 0B

;0907

0\*0(

https[:]//www[.]digicert.com/CPS0

|0z0\$

http[:]//ocsp.digicert.com0R

Google Inc1%0#

Google Internet Authority G20

150211124702Z

150512000000Z0f1

US1

California1

Mountain View1

Google Inc1

\*.google.com0Y0

Fqi

yl|x \*.google.com

\*.android.com

\*.appengine.google.com

\*.cloud.google.com

\*.google-analytics.com

\*.google.ca

\*.google.cl

\*.google.co.in

\*.google.co.jp

\*.google.co.uk

\*.google.com.ar

\*.google.com.au

\*.google.com.br

\*.google.com.co

\*.google.com.mx

\*.google.com.tr

\*.google.com.vn

\*.google.de

\*.google.es

\*.google.fr

\*.google.hu

\*.google.it

\*.google.nl

\*.google.pl

\*.google.pt

\*.googleadapis.com

\*.googleapis.cn

\*.googlecommerce.com

\*.googlevideo.com

\*.gstatic.cn

\*.gstatic.com

\*.gvt1.com

\*.gvt2.com

\*.metric.gstatic.com

\*.urchin.com

\*.url.google.com

\*.youtube-nocookie.com

'.youtube.com

\*.youtubeeducation.com

\*.ytimg.com

android.com

g.co

goo.gl

google-analytics.com

google.com

googlecommerce.com

urchin.com

youtu.be

**TLP:WHITE** 

youtube.com youtubeeducation.com0 \0Z0+ http[:]//pki.google.com/GIAG2.crt0+ http[:]//clients1.google.com/ocsp0 )0'0% http[:]//pki.google.com/GIAG2.cr 0

-- End SSL CERT Strings--

When executed, the malware checks and attempts to read data from the configuration data file "c\_1990.nls" if installed on the victim system. The configuration data file was not available for analysis. Static analysis indicates that the configuration data contains the C2 address the malware used for network connection.

The malware is designed to generate crafted TLS sessions (fake TLS communication mechanism). The malware utilized the following command to open the Windows Firewall on the victim's machine in order to allow incoming connections.

--Begin netsh firewall command--

"cmd.exe /c netsh firewall add portopening TCP 443 "adp""

-- End netsh firewall command--

#### 746CFECFD348B0751CE36C8F504D2C76

Details	
Name	746CFECFD348B0751CE36C8F504D2C76
Size	180224
Туре	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	746cfecfd348b0751ce36c8f504d2c76
SHA1	4d51a6f714fac3013142a3ff28f294e4ccd6eb6d
ssdeep	1536:jHI+dvKd59GTnI+Dj0v7/OoMrQtKYUwnZ7hUOrYUwnZ7hUOLpnYUwnZ7hUONv:jUdidTaC07zIQt9xSx1pYxHv
Entropy	6.61189736378

Ar		

Symantec BitDefender Gen:Variant.Graftor.185553 Backdoor:Win32/Escad.A!dha Gen:Variant.Graftor.185553 (B) BDS/Escad.180224 Backdoor/Win32.Akdoor a variant of Win32/NukeSped.M trojan Backdoor.Win32.Agent AVG BackDoor.Generic19.AIVO  Trojan.Win32.Agent BackDoor.Generic19.AIVO	McAfee	BackDoor-FCIV!746CFECFD348
BitDefender Microsoft Security Essentials Emsisoft Avira Ahnlab ESET Vir.IT eXplorer Ikarus  Gen:Variant.Graftor.185553 Backdoor:Win32/Escad.Aldha Gen:Variant.Graftor.185553 (B) BDS/Escad.180224 Backdoor/Win32.Akdoor a variant of Win32/NukeSped.M trojan Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	К7	Trojan ( 004be70e1 )
Microsoft Security Essentials Emsisoft Avira Ahnlab ESET Vir.IT explorer Ikarus Backdoor:Win32/Escad.A!dha Gen:Variant.Graftor.185553 (B) BDS/Escad.180224 Backdoor/Win32.Akdoor a variant of Win32/NukeSped.M trojan Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	Symantec	Heur.AdvML.C
Emsisoft Avira BDS/Escad.180224 Backdoor/Win32.Akdoor a variant of Win32/NukeSped.M trojan Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	BitDefender	Gen:Variant.Graftor.185553
Avira Ahnlab BDS/Escad.180224 Backdoor/Win32.Akdoor a variant of Win32/NukeSped.M trojan Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	Microsoft Security Essentials	Backdoor:Win32/Escad.A!dha
Ahnlab Backdoor/Win32.Akdoor a variant of Win32/NukeSped.M trojan Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	Emsisoft	Gen:Variant.Graftor.185553 (B)
ESET a variant of Win32/NukeSped.M trojan  Vir.IT eXplorer Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	Avira	BDS/Escad.180224
Vir.IT eXplorer Backdoor.Win32.Generic.AIVO Trojan.Win32.Agent	Ahnlab	Backdoor/Win32.Akdoor
Ikarus Trojan.Win32.Agent	ESET	a variant of Win32/NukeSped.M trojan
1,11	Vir.IT eXplorer	Backdoor.Win32.Generic.AIVO
AVG BackDoor,Generic19,AIVO	Ikarus	Trojan.Win32.Agent
	AVG	BackDoor.Generic19.AIVO

# PE Information

**Compiled** 2016-01-29T09:21:46Z

PE Sections			
Name	MD5	Raw Size	Entropy
(header)	e14dca360e273ca75c52a4446cd39897	4096	0.672591739631
.text	076cdf2a2c0b721f0259de10578505a1	49152	6.41338619924
.rdata	4a6af2b49d08dd42374deda5564c24ef	8192	3.293891672
.data	c797dda9277ee1d5469683527955d77a	110592	6.78785911234
.reloc	fbefbe53b3d0ca62b2134f249d249774	8192	3.46819043887

**TLP:WHITE** 

5 of 10

US-CERT MAR-10135536-F

Packers		
Name	Version	<b>Entry Point</b>
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

# Description

This artifact (original name: ProxyDll.dll) is a malicious PE32 DLL designed to open the Windows Firewall on the victim's machine to allow incoming connections and force the compromised system to function as a proxy server. This binary and the file 3DAE0DC356C2B217A452B477C4B1DB06 function similarly. Static analysis indicates this application is designed to bind and listen on port 443.

Connections to the malware are designed to appear to be encrypted within a TLS/SSL session. Analysis indicates the malware is not designed to actually setup a valid TLS/SSL session with the operator but mimic such a connection using embedded SSL CERTS from public internet service providers (ISP). However, traffic between the operator and the proxy server is encrypted using an unidentified cipher. Importantly, this malware comes hard-coded with multiple public SSL certificates from public ISPs which it utilizes for the fake TLS sessions. Strings of interest extracted from these public SSL certificates are displayed below:

# --Begin SSL CERT Strings--

US1

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

mok#n

www[.]yahoo.com

yahoo.com

hsrd.yahoo.com

us.yahoo.com

fr.yahoo.com

uk.yahoo.com

za.yahoo.com

ie.yahoo.com

it.yahoo.com es.yahoo.com

de.yahoo.com

ca.yahoo.com

qc.yahoo.com

br.yahoo.com

ro.yahoo.com

se.yahoo.com

be.yahoo.com

fr-be.yahoo.com

ar.yahoo.com mx.yahoo.com

cl.yahoo.com

co.yahoo.com

ve.yahoo.com

espanol.yahoo.com

pe.yahoo.com

in.yahoo.com

sg.yahoo.com

id.yahoo.com

malaysia.yahoo.com

ph.yahoo.com

vn.yahoo.com

maktoob.yahoo.com

en-maktoob.yahoo.com

**TLP:WHITE** 

US-CERT MAR-10135536-F 6 of 10

ca.my.yahoo.com gr.yahoo.com att.yahoo.com au.yahoo.com nz.yahoo.com tw.yahoo.com hk.yahoo.com brb.yahoo.com my.yahoo.com add.my.yahoo.com espanol.att.yahoo.com frontier.yahoo.com verizon.yahoo.com ca.rogers.yahoo.com fr-ca.rogers.yahoo.com tatadocomo.yahoo.com tikona.yahoo.com ideanetsetter.yahoo.com mtsindia.yahoo.com smartfren.yahoo.com0 ^0\0Z 60L0# https[:]//d.symcb.com/cps0% https[:]//d.symcb.com/rpa0 \$0"0 http[:]//sd.symcb.com/sd.crl0W K010 http[:]//sd.symcd.com0& http[:]//sd.symcb.com/sd.crt0 US1 DigiCert Inc1'0% DigiCert SHA2 Secure Server CA0 130802000000Z 160805120000Z0I1 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 )http[:]//crl3.digicert.com/ssca-sha2-g3.crl0/ )http[:]//crl4.digicert.com/ssca-sha2-g3.crl0B ;0907 0\*0( https[:]//www[.]digicert.com/CPS0| p0n0\$ http[:]//ocsp.digicert.com0F  $: http[:] /\!/ cacerts. digicert.com/DigiCertSHA2SecureServerCA.crt0$ 

**TLP:WHITE** 

Symantec Corporation1 Symantec Trust Network1(0& Symantec Class 3 EV SSL CA - G30 141219000000Z 160416235959Z0 US1 California1 Private Organization1 C08065921 US1 950141 California1 Cupertino1 1 Infinite Loop1 Apple Inc.1%0# Internet Services for Akamai1 www[.]apple.com0 j>e9 dtn 9J;P GZU{Rd 5Cv ?DA amZ www[.]apple.com ssl.apple.com0 \_0]0[ 0L0# https[:]//d.symcb.com/cps0% https[:]//d.symcb.com/rpa0 j0+ \$0"0 http[:]//sr.symcb.com/sr.crl0W K010 http[:]//sr.symcd.com0& http[:]//sr.symcb.com/sr.crt0 US1 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 150609235959Z0 CN1 beijing1 beijing1907 0BeiJing Baidu Netcom Science Technology Co., Ltd1%0# service operation department1 \*.baidu.com0 G`A 6http[:]//mscrl.microsoft.com/pki/mscorp/crl/msitwww2.crl 4http[:]//crl.microsoft.com/pki/mscorp/crl/msitwww2.crl0p d0b0< Ohttp[:]//www[.]microsoft.com/pki/mscorp/msitwww2.crt0" http[:]//ocsp.msocsp.com0 G0E0C 0604 (http[:]//www[.]microsoft.com/pki/mscorp/cps www[.]bing.com bing.com \*.platform.bing.com \*.bing.com ieonline.microsoft.com \*.windowssearch.com cn.ieonline.microsoft.com \*.origin.bing.com \*.mm.bing.net \*.api.bing.com ecn.dev.virtualearth.net

**TLP:WHITE** 

\*.cn.bing.net

- \*.cn.bing.com
- \*.ssl.bing.com
- \*.appex.bing.com
- \*.platform.cn.bing.com ssl-api.bing.com
- ssl-api.bing.net
- \*.api.bing.net
- \*.bingapis.com

www[.]bingsandbox.com

bingsandbox.com0

-- End SSL CERT Strings--

#### 9CE9A0B3876AACBF0E8023C97FD0A21D

Details	
Name	9CE9A0B3876AACBF0E8023C97FD0A21D
Size	21812
Type	ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV)
MD5	9ce9a0b3876aacbf0e8023c97fd0a21d
SHA1	f4fac6fea1a947e3bf9ea499450ccf0c370ef5dd
ssdeep	384:M1JPX/pAibVDSBV55oXy8KQvKvCT1bo0Z:MpvhA4SCKQS41bh
Entropy	6.13535106368

# **Antivirus**

Symantec	Backdoor.Trojan
Sophos	Andr/Spy-ANK
Ahnlab	Linux/Backdoor.21812
ESET	a variant of Android/NukeSped.A trojan
lkarus	Backdoor AndroidOS BlockBuster

#### Description

This artifact is a malicious ELF ARM executable designed to connect to hard-coded Internet Protocol (IP) addresses. Static analysis indicates this ELF binary, designed to run on Android platforms, is a fully functioning Remote Access Tool.

The malware contains references to the following non-malicious domains.

--Begin list of non-malicious domains--

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 list of non-malicious domains--

The following YARA signature may be utilized to uniquely identify this RAT variant.

--Begin YARA Signature--

**TLP:WHITE** 

```
rule Hidden_Cobra_ELF_Android_BD{
meta:
description = "Will Identify Hidden Cobra Android RAT"
author = "DHS/NCCIC"
date = "2018/01/23"
hash0 = "9CE9A0B3876AACBF0E8023C97FD0A21D"

strings:
$s0 = {2F646174612F73797374656D2F646E7363642E6462}
$s1 = {13171BFCFC1F23FC27FCFC0B2F2BFC3BFCFCFC0E3336}

condition:
all of them
}
--End YARA Signature--
```

# **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: <a href="https://forms.us-cert.gov/ncsd-feedback/">https://forms.us-cert.gov/ncsd-feedback/</a>

#### **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 <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a>.

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: <u>submit@malware.us-cert.gov</u>
- 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 <a href="https://www.us-cert.gov">www.us-cert.gov</a>.

**TLP:WHITE** 

US-CERT MAR-10135536-F 10 of 10