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**

<table>
<thead>
<tr>
<th>Files Processed</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3dae0dc356c2b217a4f2b477c4b1db06 (3DAE0DC356C2B217A4F2B477C4B1DB06)</td>
<td></td>
</tr>
<tr>
<td>746cfecfd348b0751ce36c8f504d2c76 (746CFECEFDF348B0751CE36C8F504D2C76)</td>
<td></td>
</tr>
<tr>
<td>9ce9a0b3876aacf0e8023c97fd0a21d (9CE9A0B3876AACBF0E8023C97FD0A21D)</td>
<td></td>
</tr>
</tbody>
</table>
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.

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
www.github.com
n0l04
;0907
0*0{
https://www.digicert.com/CPS0
|020$ http://ocsp.digicert.com

Google Inc1%0#
Google Internet Authority G20
150211124702Z
150512000000Z01
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
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.

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

```
--End netsh firewall command--
```

### Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>MD5</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>746CFECFD348B0751CE36C8F504D2C76</td>
<td>180224</td>
<td>PE32 executable (DLL) (console) Intel 80386, for MS Windows</td>
<td>746cfecfd348b0751ce36c8f504d2c76</td>
<td>4d51a6f714fac3013142a3f28f294e4ccd6eb6d</td>
</tr>
<tr>
<td>ssdeep</td>
<td></td>
<td></td>
<td>1536:jHl+dvKd59STnl+Dj0v7/OoMrQtKUYUwnZ7hUOrYUwnZ7hUOLpnYUwnZ7hUONv:jUdidTaC07zIQt9xSx1pYxHv</td>
<td></td>
</tr>
<tr>
<td>Entropy</td>
<td></td>
<td></td>
<td>6.6189736378</td>
<td></td>
</tr>
</tbody>
</table>

### Antivirus

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee</td>
<td>BackDoor-FCIV/746CFECFD348</td>
</tr>
<tr>
<td>K7</td>
<td>Trojan ( 004be70e1 )</td>
</tr>
<tr>
<td>Symantec</td>
<td>Heur.AdvMLC</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Gen:Variant.Graftor.185553</td>
</tr>
<tr>
<td>Microsoft Security Essentials</td>
<td>Backdoor:Win32/Modena</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>Gen:Variant.Graftor.185553 (B)</td>
</tr>
<tr>
<td>Avira</td>
<td>BDS/Scad.180224</td>
</tr>
<tr>
<td>Ahnlab</td>
<td>Backdoor/Win32.Akdoor</td>
</tr>
<tr>
<td>ESET</td>
<td>a variant of Win32/NukeSped.M trojan</td>
</tr>
<tr>
<td>Vir.IT eXplorer</td>
<td>Backdoor.Win32.Generic.AIWO</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>Trojan.Win32.Agent</td>
</tr>
<tr>
<td>AVG</td>
<td>BackDoor.Generic19.AIWO</td>
</tr>
</tbody>
</table>

### PE Information

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

### PE Sections

<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>Raw Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(.header)</td>
<td>e14dca360e273ca75c52a4446cd39897</td>
<td>4096</td>
<td>0.672591739631</td>
</tr>
<tr>
<td>.text</td>
<td>076cfd2a2c0b72f0259de10578505a1</td>
<td>49152</td>
<td>6.41338619924</td>
</tr>
<tr>
<td>.rdata</td>
<td>4a6af2bf49d08dd4234d4d9556a6c3d85e</td>
<td>8192</td>
<td>3.293891672</td>
</tr>
<tr>
<td>.data</td>
<td>c797dada2977ee1d5469638527955d77a</td>
<td>110592</td>
<td>6.78785911234</td>
</tr>
<tr>
<td>.reloc</td>
<td>fbefbe53b3d0ca62b2134f249d2497774</td>
<td>8192</td>
<td>3.46819043887</td>
</tr>
</tbody>
</table>
Packers

Name | Version | Entry Point
--- | --- | ---
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 3DAE0DC356C2B217DA52B477C4B1DB06 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.com
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
da.yahoo.com
br.yahoo.com
qc.yahoo.com
se.yahoo.com
be.yahoo.com
fr-be.yahoo.com
ar.yahoo.com
mx.yahoo.com
dl.yahoo.com
cr.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
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
carogers.yahoo.com
fr-ca.rogers.yahoo.com
tatadocomo.yahoo.com
tikona.yahoo.com
ideanetsetter.yahoo.com
mtsindia.yahoo.com
smartfren.yahoo.com
^0/0Z
60L0#
https[:\]//d.symcb.com/cps0%
https[:\]//d.symcb.com/rpa0
$0^0
http[:\]//sd.symcb.com/sd.crl0W
K0I0
http[:\]//sd.symcd.com0&
http[:\]//sd.symcb.com/sd.crt0

US1
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
d0b0/
)http[:\]//crl3.digicert.com/ssca-sha2-g3.crl0/
)http[:\]//crl4.digicert.com/ssca-sha2-g3.crt0B
;0907
0^0(https[:\]//www[.]digicert.com/CPS0|
p0n0$
http[:\]//ocsp.digicert.com0F
:http[:\]//cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt0

Symantec Corporation1
Symantec Trust Network10&
Symantec Class 3 EV SSL CA - G30
9CE9A0B3876AAACBF0E8023C97FD0A21D

## Details

<table>
<thead>
<tr>
<th>Name</th>
<th>9CE9A0B3876AAACBF0E8023C97FD0A21D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>21812</td>
</tr>
<tr>
<td>Type</td>
<td>ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV)</td>
</tr>
<tr>
<td>MD5</td>
<td>9ce9a0b3876aacbf0e8023c97fd0a21d</td>
</tr>
<tr>
<td>SHA1</td>
<td>f4fac6fea1a94f3bf9e499450cc0c370ef5dd</td>
</tr>
<tr>
<td>ssdeep</td>
<td>384:M1LPX/pAbpVDBSV55oXY4KqV5CT1bo0Z:MrVh4a4SCKQS41bh</td>
</tr>
<tr>
<td>Entropy</td>
<td>6.13535106368</td>
</tr>
</tbody>
</table>

## Antivirus

<table>
<thead>
<tr>
<th>Symantec</th>
<th>Backdoor.Trojan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sophos</td>
<td>Andr/Spy-ANK</td>
</tr>
<tr>
<td>Ahnlab</td>
<td>Linux/Backdoor.21812</td>
</tr>
<tr>
<td>ESET</td>
<td>a variant of Android/NukeSped.A trojan</td>
</tr>
<tr>
<td>Ikarus</td>
<td>Backdoor.AndroidOS.BlockBuster</td>
</tr>
</tbody>
</table>

## 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--
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.