MAR-10135536-21 – North Korean Tunneling Tool: ELECTRICFISH | CISA

Published: 2019-05-14 · Archived: 2026-04-05 13:50:25 UTC

Notification

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between DHS and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified a malware variant used by the North Korean government. This malware has been identified 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 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 and report the activity to the Cybersecurity and Infrastructure Security Agency (CISA) or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.

This report provides analysis of one 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 (1)

a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb (a1260fd3e9221d1bc5b9ece6e7a5a9...)

Findings

a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb

Details

Name	a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb
Size	1422336 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8d9123cd2648020292b5c35edc9ae22e

SHA1	0939363ff55d914e92635e5f693099fb28047602
SHA256	a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb
SHA512	646697e3d5146e05a221183f6c9f00f5eb38400ef9a2f83bfd0fcf2f8af1a7efff99c0a3486740c745ce6cf0939c4f0678cb818cbbff8ed2b2
ssdeep	24576:HsO8RKL6OLnWZGFbHq0aMow5Q3gkD/74tU3hYPgP5IyrMsEOhVRpxHkADUHEPbzJ:0KjKHMbO3pkoBIyIstVRpxH
Entropy	6.703195

Antivirus

BitDefender	Gen:Variant.Ursu.349885Unclassified
Emsisoft	Gen:Variant.Ursu.349885 (B)

Yara Rules

No matches found.

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

Process List

Process	PID	PPID
lsass.exe	488	(384)
a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb.exe	3052	(3024)

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 command-line arguments allowing it to be configured with a destination IP address and port, a source IP address and port, a proxy IP address and port, and a user name and password, which can be utilized to authenticate with a proxy server. 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.

--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--

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--
61616161626262626363636364646464000000000000000002B6E0000040000009210
--End Authentication Packet Sent to Destination System--

Screenshots

Figure 1 - Screenshot of the malware authenticating with the proxy server configured at command prompt.

Figure 2 - Screenshot of the malware building the authentication packet that will be sent to the destination system. It must begin with the static value "aaaa" for it to be accepted by the utility.

Figure 3 - Screenshot of the malware evaluating a received authentication packet.

Figure 4 - Screenshot of the malware system authentication packet to the source/destination system.

Figure 5 - Screenshot of the authentication packet sent to the source/destination system during analysis. The malware will attempt to tunnel traffic between the source and destination systems specified in the command prompt.

Figure 6 - Screenshot of the malware generating two-bytes of random data which will be included in the authentication packet sent to the source/destination systems.

Figure 7 - Screenshot of the authentication packet sent to "source" system with lab environment. Malware will attempt to tunnel traffic between the source and destination systems specified at command prompt.

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 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.
