MAR-10271944-2.v1 – North Korean Trojan: ARTFULPIE

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of ar 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 foreseeab accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distribut 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 Department of Homeland Security (DHS), the Federal Bureau of Inve the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Trojan malware variants used by the N government. This malware variant has been identified as ARTFULPIE. The U.S. Government refers to malicious cyber activity by the North Korea 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 activi

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Use should flag activity associated with the malware and report the activity to the Cybersecurity and Infrastructure Security Agency (CISA) or the FBI C (CyWatch), and give the activity the highest priority for enhanced mitigation.

This report looks at an implant that performs downloading and in-memory loading and execution of a DLL from a hardcoded url.
For a downloadable copy of IOCs, see MAR-10271944-2.v1.stix.

Submitted Files (1)

606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c (mega.exe.exe)

IPs (1)

193.56.28.103

Findings

606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c

Tags

downloadertrojan

Details

Name	mega.exe.exe
Size	83968 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	2d92116440edef4190279a043af6794b

SHA1	eb2eb432445b3dcf6483e7d5f670acb94a8bab70
SHA256	606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c
SHA512	ef849cb69d785bdcef98127abed65e0acc749f9748753d04105818e68ec5e37e068f8c4a7146b5238c5a6bf75712b198935c356b0fe0bb
ssdeep	1536:FNtzOnGK/pmGC4ISgyCOkaPeFAuf+jXQ1JsWODjgncdw1DCaAqGgo:FNqpmGC7S1rJPQAFXKqDjgWwBCaAq3o
Entropy	6.334481

Antivirus

Avira	HEUR/AGEN.1031247
ByteHero	Trojan.Win32.Heur.098
Symantec	Heur.AdvML.B

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-06-14 05:41:48-04:00
Import Hash	8079a02c54cad285e36d60589737d1e3

PE Sections

MD5	Name	Raw Size	Entropy
33371b670b629e6e418f34546c9b5eda	header	1024	2.672349
d7c48cf554eae1f467a10903d05d84fc	.text	51712	6.635530
4b19a4f766cd6f95bd6b36fab052c916	.rdata	24064	4.908608
9ccfa1efb02e96faf15883c5d135e6f9	.data	2560	1.986341
c970c10a1e848ee974b87923ecbe6a2f	.rsrc	512	4.706155
51b1d3e64f81f0cc54f348474457a1d4	.reloc	4096	6.403055

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

606c6000f3... Connected_To 193.56.28.103

Description

The sample is a downloader/loader that performs the following steps:

Downloads the hardcoded URL hxxp[:]//193[.]56[.]28[.]103:88/xampp/thinkmeter[.]dll into memory using the user-agent string: "Mozilla/5.0 (compa
Windows NT 6.1; Trident/5.0)".

Loads the .dll into its own address space manually (fully in memory).

Calls the .dll's entry-point.
193.56.28.103

Tags

command-and-control

URLs

193.56.28.103:88/xampp/thinkmeter.dll

Ports

88 TCP

Relationships

193.56.28.103	Connected_From	606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c

Relationship Summary

606c6000f3...	Connected_To	193.56.28.103
193.56.28.103	Connected_From	606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organizatio 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 unl
- 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
- 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) Specia **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

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

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 mos will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regar desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manua 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 shoul CISA at 1-888-282-0870 or soc@us-cert.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 ph Reporting forms can be found on CISA's homepage at www.us-cert.gov.

Revisions

February 14, 2020: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.