MAR-10265965-2.v1 – North Korean Trojan: SLICKSHOES

us-cert.gov/ncas/analysis-reports/ar20-045b

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 SLICKSHOES. The U.S. Government refers to malicious cyber activity by the North Kor 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 ((CyWatch), and give the activity the highest priority for enhanced mitigation.

This sample is a Themida-packed dropper that decodes and drops a file "C:\Windows\Web\taskenc.exe" which is a Themida-packed beaconing ir beaconing implant does not execute the dropped file nor does it schedule any tasks to run the malware. The dropped beaconing implant uses an encoding algorithm and is capable of many features including conducting system surveys, file upload/download, process and command executior captures.
For a downloadable copy of IOCs, see MAR-10265965-2.v1.stix.

Submitted Files (1)

fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac (CCA9FBB11C194FC53015185B741887...)

IPs (1)

188.165.37.168

Findings

fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac

Tags

emotettrojan

Details

Name	CCA9FBB11C194FC53015185B741887A8
Size	3133440 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	cca9fbb11c194fc53015185b741887a8
SHA1	9e7bf03a607558dafe146907db28d77fda81be22
SHA256	fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac
SHA512	a1d1747dbc96c14b45f345679c0f7ba38186458f4992eecf382dd0af6391b4224c1b487431d681f5ffd052839f2901bc6203ea81c3235efc
ssdeep	49152:bbcROoCHuumCvGyQwNr6Ljvhg1J/4fxcBhmdSP8sWNRy8kLn3o1Dn:jVHaaGyQG6npcJ4xcD5d2Ry8kDo
Entropy	7.968879

Antivirus

Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.Casdet
Avira	TR/Crypt.TPM.Gen
BitDefender	Gen:Variant.Barys.1619

ClamAV	Win.Trojan.Agent-7376504-0
Cyren	W32/Trojan.QBAU-3559
ESET	a variant of Win32/Packed.Themida.AOO trojan
Emsisoft	Gen:Variant.Barys.1619 (B)
Ikarus	Trojan.Win32.Themida
K7	Trojan (0040f4ef1)
McAfee	Trojan-Themida
Microsoft Security Essentials	Trojan:Win32/Emotet
NANOAV	Trojan.Win32.TPM.ggaakh
Sophos	Troj/Agent-BCXR
Symantec	Trojan Horse
VirusBlokAda	Trojan.Wacatac
Zillya!	Trojan.Themida.Win32.3185

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-02-26 20:08:54-05:00
Import Hash	baa93d47220682c04d92f7797d9224ce

PE Sections

MD5	Name	Raw Size	Entropy
0de0ceb73fba415dc20a730f628429a6	header	4096	0.816628
74520bd2f6bb3211bd82b6f9547ff207		1572864	7.979303
32762b0a8ae1347aebaba811505cadcf	.rsrc	49152	4.290489
79cf217f58f3178dafbfe532c01ef5c4	.idata	512	1.308723
f0347e7e1ac9efb817c55b3ba9e5bf2d		512	0.264678
4fb94c6713c62a51c1b230a2bc033fac	suylcrzz	1505792	7.954736
81610ae95a418f6ef9ef042b37a26c4a	ajqluhke	512	3.110274

Relationships

fdb87add07...	Connected_To	188.165.37.168

Description

This sample is a Themida-packed dropper that decodes and drops an embedded file (MD5: B57DB76CC1C0175C4F18EA059D9E2AB2 / SHA25
7250ccf4fad4d83d087a03d0dd67d1c00bf6cb8e7fa718140507a9d5ffa50b54) to C:\Windows\Web\taskenc.exe. This dropper does not execute the
create any auto-run keys or scheduled tasks to execute it.

The dropped file (taskenc.exe) is a Themida-packed beaconing implant with RAT functionality. The implant beacons to a hardcoded IP (188.165.3
hardcoded TCP port 80 every 60 seconds. The initial beacon contains the string “ApolloZeus” as well as victim information, including OS version,
address. All traffic, including the beacon, is encoded with an indigenous encoding algorithm. Due to the way the implant decodes the hardcoded s
place in memory, the first beacon contains the string in plaintext, the second beacon will contain the string encoded, and so on. This is probably u
oversight by the developers.

--Begin Packet Format--
[8 Bytes data length][2Byte Opcode][data]
--End Packet Format--

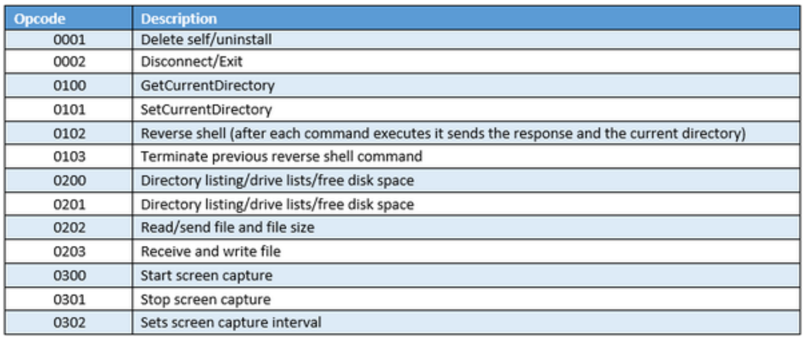
--Begin Victim Information--
OS Version
User name
IP address
--End Victim Information--

A Python3 script for decoding the traffic is displayed below:

```
--Begin Python3 Script--
def decode(enc):
dec = b”
key1 = 0x49;
key2 = 0x1310a024;
key3 = 0xa323da32;

for e in enc:
   dec += chr((ord(e) ^ key3 ^ key1) & 0xff)
   tmp1 = key3 >> 8
   key1 = (key2>>0x10) & (key2>>8) & key2 ^ (key3>>0x10) & tmp1 ^ key3 & key1 ^ (key3>>0x18);
   tmp2 = key3 * 2 ^ key3;
   key3 = key2 << 0x18 | key3 >> 8;
   key2 = (tmp2 & 0x1fe) << 0x16 | key2 >> 8;
return dec
--End Python3 Script--
```

Screenshots



Opcode	Description
0001	Delete self/uninstall
0002	Disconnect/Exit
0100	GetCurrentDirectory
0101	SetCurrentDirectory
0102	Reverse shell (after each command executes it sends the response and the current directory)
0103	Terminate previous reverse shell command
0200	Directory listing/drive lists/free disk space
0201	Directory listing/drive lists/free disk space
0202	Read/send file and file size
0203	Receive and write file
0300	Start screen capture
0301	Stop screen capture
0302	Sets screen capture interval

Figure 1 - Implant Functionality.

188.165.37.168

Ports

80 TCP

Relationships

188.165.37.168	Connected_From	fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac

Description

Hardcoded C2 address used in implant.

Relationship Summary

fdb87add07...	Connected_To	188.165.37.168
188.165.37.168	Connected_From	fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac

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
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 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

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

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