MAR-10288834-2.v1 – North Korean Trojan: TAINTEDSCRIBE | CISA

Published: 2020-05-12 · Archived: 2026-04-06 00:20:11 UTC

Notification

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 Trojan malware variants used by the North Korean government. This malware variant has been identified as TAINTEDSCRIBE. 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, 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 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 looks at a full-featured beaconing implant and its command modules. These samples uses FakeTLS for session authentication and for network encryption utilizing a Linear Feedback Shift Register (LFSR) algorithm. The main executable disguises itself as Microsoft's Narrator. It downloads its command execution module from a command and control (C2) server and then has the capability to download, upload, delete, and execute files; enable Windows CLI access; create and terminate processes; and perform target system enumeration.

For a downloadable copy of IOCs, see MAR-10288834-2.v1.stix.

Submitted Files (3)

106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438 (Narrator.exe)

19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35 (EngineDll.dll)

2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf (EngineDll.dll)

IPs (1)

211.192.239.232

Findings

106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438

Tags

trojan

Details

Name	Narrator.exe
Size	286720 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	24906e88a757cb535eb17e6c190f371f
SHA1	bda6c036fe34dda6aea7797551c7853a9891de96
SHA256	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
SHA512	b02f86d8261875c9eaf2ee9d491bc7a5ed3227c90854060078598a7425b58d096398315144517a9daec6cb3542fe901af434b597692963de
ssdeep	3072:qKhnf91e3YGs53EeY9eDUSGPGrdj+MieMUgUo2n6/rZDS35bb3tiWh6f9FKi4Z+J:xWvsN/Y9eDpjnieMB2BFtQFgZKUV
Entropy	6.553050

Antivirus

AegisLab	Trojan.Win32.Generic.mmcn
Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.Wacatac
Avira	TR/RedCap.ihekz
BitDefender	Trojan.GenericKD.32212178
Cyren	W32/Agent.XH.gen!Eldorado
ESET	a variant of Win32/NukeSped.CO trojan
Emsisoft	Trojan.GenericKD.32212178 (B)
NANOAV	Trojan.Win32.NukeSped.fuwevb
VirusBlokAda	BScope.Trojan.Win64.AllStars
Zillya!	Trojan.Generic.Win32.918308

YARA Rules

- rule CISA_3P_10135536_36 : lfsrPolynomials_handshakeBytes
  {
    meta:
      Author = "CISA Trusted Third Party"
      Incident = "10135536"
      Date = "2019-12-20"
      Actor = "Hidden Cobra"
      Category = "n/a"
      Family = "n/a"
      Description = "Detects LFSR polynomials used for FakeTLS comms and the bytes exchanged after the FakeTLS handshake"
      MD5_1 = "24906e88a757cb535eb17e6c190f371f"
      SHA256_1 = "106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438"
    strings:
      $p1 = { 01 23 45 67 }
      $p2 = { 89 AB CD EF }
      $p3 = { FE DC BA 98 }
      $p4 = { 76 54 32 10 }
      $h1 = { 44 33 22 11 }
      $h2 = { 45 33 22 11 }
    condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-07-31 21:47:58-04:00
Import Hash	8222381c21809ba71801ba1e0290adcc
Company Name	Microsoft Corporation
File Description	Screen Reader
Internal Name	SR.exe
Legal Copyright	© Microsoft Corporation. All rights reserved.
Original Filename	SR.exe
Product Name	Microsoft® Windows® Operating System
Product Version	6.3.9600.17415

PE Sections

MD5	Name	Raw Size	Entropy
05cafd41e93a7bd6aa578e957e7c0b4f	header	1024	2.508565
a6c7082567c2424071bfda7ab3bd8095	.text	144384	6.231730
edd9ce426d2be22871091e1c979b8f94	.rdata	37376	4.515794
3a129f29c07cc0ec4bb30fc7b4fb51e5	.data	4608	2.451992
0674e93d57aa4e7727acc7bdbc37bb36	.rsrc	86016	7.119585
978e1e848b291daef77e403a94cf8497	.reloc	13312	4.524800

Relationships

106d915db6...	Downloaded	2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf
106d915db6...	Downloaded	19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35
106d915db6...	Connected_To	211.192.239.232

Description

This file is the main implant executable. For persistence, when executed the malware copies itself into the current user's Startup folder as "Narrator.exe". The malware can have 5 hard-corded callback IP addresses/Ports. However, only 2 IP addresses are set, both to 211.192.239.232:8443. It will randomly pick one of the 5 IP addresses and attempt to connect to it. If it fails, it will wait 60 seconds and then try another IP address.

It performs the connection and authentication, then it attempts to download an additional module (3005f1308e4519477ac25d7bbf054899 or 68fa29a40f64c9594cc3dbe8649f9ebc) from the C2, which it loads and uses for command processing.

The modules export a function, CreateFileProcEx or CreateFileEx. The function is called by this sample with a number of arguments, including a handle to the active connection socket.

The malware utilizes a "FakeTLS" scheme in an attempt to obfuscate its network communications. It picks a random URL from a list (Figure 1) to use in the TLS certificate. The sample and the C2 externally appear to perform a standard TLS authentication, however, most of the fields used are filled with random data sourced from rand().

Once the FakeTLS handshake is complete, all further packets use a FakeTLS header, followed by LFSR encrypted data.

--Begin packet structure--
17 03 01 <2 Byte data length> <LFSR encrypted data>
--End packet structure--

After the TLS authentication, the sample performs a handshake with the C2 (outlined in Figure 2). After this exchange, the implant sends the Victim Info (outlined in Figure 3), and then waits for tasking from the C2.

Screenshots

Figure 1 - List of certificate URLs used in the TLS certificate.

Figure 2 - Table of the session structure.

Figure 3 - Table of the victim information structure.

Figure 4 - The implant contains the commands displayed in the table.

2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf

Tags

trojan

Details

Name	EngineDll.dll
Size	166400 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	3005f1308e4519477ac25d7bbf054899
SHA1	0cf64de7a635f5760c4684c18a6ad2983a2c0f73
SHA256	2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf
SHA512	77b0b20002ab4a175941a81e309ac6771295abee45497ae507d43fcef237dc7f614bac1e9f97086ef22892db5ef895075c63e467347b08d7e
ssdeep	3072:jdouAxXKBsOmN7OslJyOmg/wMFOpYop4vdxZdXYGeJavqL:jd3kCsOM5/YY3d9z
Entropy	6.511161

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-02-19 08:23:40-05:00
Import Hash	f56b60ba203f4772b5f87e061b59670a

PE Sections

MD5	Name	Raw Size	Entropy
9ba90552855e9e8b3cfbcec483e4b036	header	1024	2.654189
8244acedace09a0d354fd56aaf0c0f40	.text	123904	6.641205

MD5	Name	Raw Size	Entropy
84e6930849c4126353e3367f2431b941	.rdata	25600	5.215729
7403e6dd1ea8fd928cb704a43a82d773	.data	6144	3.443058
9a33838895830247744985365b8b2948	.rsrc	512	5.115767
7c956dfb879b86c9d57c3e783f4ab241	.reloc	9216	5.177068

Packers/Compilers/Cryptors

Microsoft Visual C++ DLL *sign by CodeRipper

Relationships

2057c0cf46...	Downloaded_By	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
2057c0cf46...	Downloaded_By	211.192.239.232

Description

This file and 68FA29A40F64C9594CC3DBE8649F9EBC appear identical in functionality, except for the exported function name. Narrator.exe (24906E88A757CB535EB17E6C190F371F) looks for the exported function name CreateFileEx.

19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35

Tags

trojan

Details

Name	EngineDll.dll
Size	166400 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	68fa29a40f64c9594cc3dbe8649f9ebc
SHA1	b24f6c60fa4ac76ffc11c2fcee961694aeb2141b
SHA256	19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35
SHA512	ffca587964d68e3bea67b4add649b06d768457bf49e2db0708996835f0d9da95cc79bcb6640220053632e993fe545e8ca4cd50309bf0d769
ssdeep	3072:VovrXpvEgEOtXOssvdAeL7Mz81dYFQbEPWgtXJtLNh1jUV46mG:VUDpNyD77YF/+gtHLRj7G
Entropy	6.512934

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-02-05 21:20:52-05:00
Import Hash	b100cffd23b28dfc257c5feeb1e89eb9

PE Sections

MD5	Name	Raw Size	Entropy
35b77733290c275ff61e476e1491ed7a	header	1024	2.620308
6a8fcc80d3b556c366b9915ca084df91	.text	123904	6.638987
52890df518ebf2eeba3c08102c595dc1	.rdata	25600	5.207715
f73aec76a9c7a7f6bc0e0dbce1dd57b0	.data	6144	3.442575
9a33838895830247744985365b8b2948	.rsrc	512	5.115767
6f67f8a4390a007724e02090e947d315	.reloc	9216	5.186683

Packers/Compilers/Cryptors

Microsoft Visual C++ DLL *sign by CodeRipper

Relationships

19f9a9f7a0...	Downloaded_By	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
19f9a9f7a0...	Downloaded_By	211.192.239.232

Description

This file and 3005F1308E4519477AC25D7BBF054899 appear identical in functionality, except for the exported function name. Narrator.exe (24906E88A757CB535EB17E6C190F371F) looks for the exported function name CreateFileProcEx.

211.192.239.232

Tags

command-and-control

Ports

- 8443 TCP

Relationships

211.192.239.232	Connected_From	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
211.192.239.232	Downloaded	2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf
211.192.239.232	Downloaded	19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35

Description

Narrator.exe (24906E88A757CB535EB17E6C190F371F) attempts to download payload from the IP address.

Relationship Summary

106d915db6...	Downloaded	2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf
106d915db6...	Downloaded	19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35
106d915db6...	Connected_To	211.192.239.232
2057c0cf46...	Downloaded_By	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
2057c0cf46...	Downloaded_By	211.192.239.232
19f9a9f7a0...	Downloaded_By	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
19f9a9f7a0...	Downloaded_By	211.192.239.232

211.192.239.232	Connected_From	106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438
211.192.239.232	Downloaded	2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf
211.192.239.232	Downloaded	19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35

Mitigation

The following Snort rule can be used to detect the FakeTLS LFSR encrypted handshake packets:

// Detects the FakeTLS LFSR encrypted handshake packets
// 17 03 01 00 18 + lfsr_encoded([44-45] 33 22 11 00 00 00 00)

alert tcp any any -> any any (msg:"Malware Detected"; pcre:" /\x17\x03\x01\x00\x18.\x26\xa5\xbb\xf1\x4f\x33\xcb/"; rev:1; sid:99999999;)

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.
