MAR-10265965-3.v1 – North Korean Trojan: CROWDEDFLOUNDER | CISA

Published: 2020-02-14 · Archived: 2026-04-05 16:50:12 UTC

Notification

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between 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 CROWDEDFLOUNDER. 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 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 analyzes a Themida packed 32-bit Windows executable, which is designed to unpack and execute a Remote Access Trojan (RAT) binary in memory. This application is designed to accept arguments during execution or can be installed as a service with command line arguments. It is designed to listen as a proxy for incoming connections containing commands or can connect to a remote server to receive commands.

For a downloadable copy of IOCs, see MAR-10265965-3.v1.stix.

Submitted Files (1)

a2a77cefd2faa17e18843d74a8ad155a061a13da9bd548ded6437ef855c14442 (F2B9D1CB2C4B1CD11A8682755BCC52...)

Findings

a2a77cefd2faa17e18843d74a8ad155a061a13da9bd548ded6437ef855c14442

Tags

trojan

Details

Name	F2B9D1CB2C4B1CD11A8682755BCC52FA
Size	1658880 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	f2b9d1cb2c4b1cd11a8682755bcc52fa

SHA1	579884fad55207b54e4c2fe2644290211baec8b5
SHA256	a2a77cefd2faa17e18843d74a8ad155a061a13da9bd548ded6437ef855c14442
SHA512	b047a4275f0fa7c0025945800acbffb5be1d327160a135c6ba8ff54352be603cbb47fff71f180ab1a915229778b7a883ed19e1d6a954ab824
ssdeep	24576:darngxIJfX2+8mGrvs5pdUIPv3eAUW/Y8w9ejjERAjYrNFtI937sTR7R5NwrzD:da7gx2B81gdVXvfAnHRFtIl7k7RPwr
Entropy	7.958686

Antivirus

Ahnlab	Trojan/Win32.Xpacked
Antiy	Trojan/Win32.BlueNoroff
Avira	TR/Crypt.TPM.Gen
BitDefender	Trojan.GenericKD.41987817
ClamAV	Win.Trojan.Agent-7376505-0
Cyren	W32/Trojan.SXNN-1599
ESET	Win32/NukeSped.CL trojan
Emsisoft	Trojan.GenericKD.41987817 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0040f4ef1)
McAfee	Trojan-NukeSped.a
Microsoft Security Essentials	Trojan:Win32/Thcsim
NANOAV	Trojan.Win32.BlueNoroff.ggbrdv
NetGate	Trojan.Win32.Malware
Sophos	Troj/Agent-BCXR
Symantec	Trojan Horse
TrendMicro	TROJ_THCSIM.A
TrendMicro House Call	TROJ_THCSIM.A
VirusBlokAda	BScope.TrojanPSW.Predator
Zillya!	Trojan.NukeSped.Win32.184

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-02-20 05:45:37-05:00
Import Hash	baa93d47220682c04d92f7797d9224ce

PE Sections

MD5	Name	Raw Size	Entropy
a7295799f336e3a6e8b61fe4f93e2251	header	4096	0.812374
2db23f163210140d797f67ed1ec1f08e		156160	7.983767
d41d8cd98f00b204e9800998ecf8427e	.rsrc	0	0.000000
efcb51d4d8a55d441d194e80899bb2b0	.idata	512	1.308723
d5443c2d2f51ba6c31a5fc9c35af7a2f		512	0.240445
8eea01ecbee2f6234d68b27d4e05585a	htusmqub	1497088	7.954958
6b71d93792bb677f0a09dbe70e6df1a2	ijybpcqb	512	3.636986

Description

This application is a Themida packed 32-bit Windows executable, which is designed to unpack and execute a RAT binary in memory. This application is designed to accept arguments during execution or can be installed as a service with command line arguments. When executed, the application is designed to open the Windows Firewall on the victim's machine to allow for incoming and outgoing connections from the victim system. The firewall is modified using a "netsh firewall add portopening" command (Figure 2). Static analysis indicates this malware may be utilized to listen as a proxy for incoming connections containing commands or can connect to a remote server to receive commands. The following command line arguments are utilized to control the RAT functionality:

--Begin RAT command line arguments--

-p: You can use the -p command line argument to force the malware to listen on a specific port. Example: malware.exe -p 8888

-h: You can use the -h CLI to force the malware to connect to a remote host and port. Example: malware.exe -h <url_string>:8888

Note: <url_string> can be either a fully qualified domain name or an Internet Protocol (IP) address.

--End RAT command line arguments--

The RAT uses a rotating exclusive or (XOR) cryptographic algorithm to secure its data transfers and command-and-control (C2) sessions (Figure 1). The malware is designed to accept instructions from the remote server to perform the following functions:

--Begin functions performed by the malware--
Download and upload files
Execute secondary payloads
Execute shell commands
Terminate running processes
Delete files
Search files
Set file attributes
Collect device information from installed storage devices (disk free space and their type)
List running processes information
Collect and send information about the victim's system
Securely download malicious DLLs and inject them into remote processes
--End functions performed by the malware--

The -h argument is utilized to force the RAT to connect to a C2 server and the CURL library (Version 7.49.1) will be used for data transfers. Note: A rotating XOR cipher will be used to secure all C2 traffic sent and received from the external C2 server. Although the malware appears to expect a numeric IP address with the -h argument, it will also accept a string Uniform Resource Locator (URL) value. If a URL string is provided (i.e. domain.com) the malware will then query this address using the Win32 API getaddrinfo(). If this call succeeds, an IP address will be returned and the malware will attempt to connect to that IP address. If the call to getaddrinfo() fails the malware will hash this domain using the MD5 hashing algorithm, resulting in a 16 byte hash value. The malware will then take bytes 4 through 8 of this hash value and XOR them with a four byte value. The resultant four byte value will then be treated as a numeric IP address. The malware will then attempt to connect to this newly generated IP address. Note: all of the command line executables referenced within this

product generate and connect to an IP address generated from the provided URL string if the call to getaddrinfo() against the provided URL fails.

Screenshots

Figure 1 - XOR based cipher utilized by RAT to secure traffic between itself and the operator/C2 server.

Figure 2 - Malware loading the command to open the firewall.

Figure 3 - This structure is utilized to parse the proxy port or remote C2 server from the command line arguments.

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.