FBI FLASH

FEDERAL BUREAU OF INVESTIGATION ♦ CYBER DIVISION

28 Oct 2021

FLASH Number

CU-000154-MW

Tactics, Techniques, and Indicators of Compromise Associated with Hello Kitty/FiveHands Ransomware

Summary

The FBI first observed Hello Kitty/FiveHands ransomware in January 2021. Hello Kitty/FiveHands actors aggressively apply pressure to victims typically using the double extortion technique. In some cases, if the victim does not respond quickly or does not pay the ransom, the threat actors will launch a Distributed Denial of Service (DDoS) attack on the victim company's public facing website. Hello Kitty/FiveHands actors demand varying ransom payments in Bitcoin (BTC) that appear tailored to each victim, commensurate with their assessed ability to pay it. If no ransom is paid, the threat actors will post victim data to the Babuk site (payload.bin) or sell it to a third-party data broker.

Technical Details

Hello Kitty/FiveHands ransomware uses compromised credentials or known vulnerabilities in SonicWall products (CVE-2021-20016, CVE-2021-20021, CVE-2021-20022, CVE-2021-20023). Once inside the network, the threat actor will use publicly available penetration tool suites such as Cobalt Strike, Mandiant's Commando, or PowerShell Empire preloaded with publicly available tools like Bloodhound and Mimikatz to map the network and escalate privileges before exfiltration and encryption.

Indicators

The following indicators were leveraged by threat actors during Hello Kitty/FiveHands ransomware compromises:

Tools	
Filename	**SHA-256**
Rclone.exe	53ae3567a34097f29011d752f1d3afab8f92beb36a8d6a5df5c1d4b12edc1703
Mimikatz.exe	3e02e94e3ecb5d77415c25ee7ecece24953b4d7bd21bf9f9e3413ffbdad472d2
Advanced_IP_Scanner_2.5.3850.exe	87bfb05057f215659cc801750118900145f8a22fa93ac4c6e1bfd81aa98b0a55
Netscan.exe	a710f573f73c163d54c95b4175706329db3ed89cd9337c583d0bb24b6a384789
RouterScan.exe	18229920a45130f00539405fecab500d8010ef93856e1c5bcabf5aa5532b3311
MEGAClient.exe	9a4acb3112a52fcc58b221b12fa5e90f068247ac3f8990ff2b4bf7e20ed5b4e1
pCloud.exe	6ce1ab4f45c78a102197258acd2da446902dad2031825c93d875660c90df27c4
psexec.c	3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

PAExec.exe	19ce4f92e7a7b1a812ee2efa834733279ddf1052e123cf36bb77443197a0ed5f
my15.ps1 (Warprism)	3b90d9fad35a45a738c6b2830896168c99014474de17984411be61b25acf6db5
grabff.exe	7d57e0ba8b36ec221b16807ce4e13a1125d53922fa50c3827a5ebd6811736ffd
grbachrome.exe	374a98a083fc04f30b86718a9fe7a5a61d1afc22b93222a89d2b752b5da1df7e
spoolsv.exe	88a2d5cbb7ae903f8208b4a831e8ca6fb5ccb6717d4ea158ce792436aa2b9a4d
9e63911b5b7e63023708125418d6d4d5.virus	59f5320b70ef8c51be409aec486366c76f6dff2730b0ab227ffd1607a4ba9b54
rfusclient.exe	a9226978b33d0bca5b6a216b98dc25558458c28fea11d1ffc650cab1527dc5d0
s3browser-9-5-3.exe	5f312e137beb1ce75f8fdf03a59e1b3cba3dc57ccc16e48daee3ee52c08fa149

SombRAT – SHA- 256
61e286c62e556ac79b01c17357176e58efb67d86c5d17407e128094c3151f7f9
99baffcd7a6b939b72c99af7c1e88523a50053ab966a079d9bf268aff884426e
fdc2de095390ec046dc3f398a47a38670282bdc2ef76dd7fc1195ac4ee0421a8
71c97ea6d14f4a6da86d51d07ea284447cc486488b9637f9c1de0ba42054c6f2
ccacf4658ae778d02e4e55cd161b5a0772eb8b8eee62fed34e2d8f11db2cc4bc
15df17be2f97295b0d8d66e434e2949850c8edc2a8edddf9b30b2b638b20612b
e09ead5b6ac9ec9203b9fb6c9152ba451498bb291478a69ac71ff6c36c468f9e

HelloKitty/Five Hands Ransomware	
ionline.exe	02a08b994265901a649f1bcf6772bc06df2eb51eb09906af9fd0f4a8103e9851

f568229e696c0e82abb35ec73d162d5e.virus	c2498845ed4b287fd0f95528926c8ee620ef0cbb5b27865b2007d6379ffe4323
dc007e71085297883ca68a919e37687427b7e6db0c24ca014c148f226d8dd98f.bin	dc007e71085297883ca68a919e37687427b7e6db0c24ca014c148f226d8dd98f
947e357bfdfe411be6c97af6559fd1cdc5c9d6f5cea122bf174d124ee03d2de8.bin	947e357bfdfe411be6c97af6559fd1cdc5c9d6f5cea122bf174d124ee03d2de8
ef614b456ca4eaa8156a895f450577600ad41bd553b4512ae6abf3fb8b5eb04e.bin	ef614b456ca4eaa8156a895f450577600ad41bd553b4512ae6abf3fb8b5eb04e
bade05a30aba181ffbe4325c1ba6c76ef9e02cbe41a4190bd3671152c51c4a7b.bin	bade05a30aba181ffbe4325c1ba6c76ef9e02cbe41a4190bd3671152c51c4a7
52dace403e8f9b4f7ea20c0c3565fa11b6953b404a7d49d63af237a57b36fd2a.bin	52dace403e8f9b4f7ea20c0c3565fa11b6953b404a7d49d63af237a57b36fd2a
a147945635d5bd0fa832c9b55bc3ebcea7a7787e8f89b98a44279f8eddda2a77.bin	a147945635d5bd0fa832c9b55bc3ebcea7a7787e8f89b98a44279f8eddda2a77
0e5f7737704c8f25b2b8157561be54a463057cd4d79c7e016c30a1cf6590a85c.bin	0e5f7737704c8f25b2b8157561be54a463057cd4d79c7e016c30a1cf6590a85c
servmanger.exe	7be901c5f7ffeb8f99e4f5813c259d0227335680380ed06df03fb836a041cb06
Hi_Kitty_2.exe	501487b025f25ddf1ca32deb57a2b4db43ccf6635c1edc74b9cff54ce0e5bcfe
ag.exe	9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0
3ae7bedf236d4e53a33f3a3e1e80eae2d93e91b1988da2f7fcb8fde5dcc3a0e9.bin	3ae7bedf236d4e53a33f3a3e1e80eae2d93e91b1988da2f7fcb8fde5dcc3a0e9
10887d13dba1f83ef34e047455a04416d25a83079a7f3798ce3483e0526e3768.bin	10887d13dba1f83ef34e047455a04416d25a83079a7f3798ce3483e0526e3768
Outlook.exe	e94064401b54c399d3f844fdf08f880cb8c5d74c34de9dc28733dd22dabba678

Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, or fund illicit activities. Paying the ransom also does not guarantee a victim's files will be recovered. However, the FBI understands when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decides to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators and analysts with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks.

The FBI may seek the following information:

- Recovered executable files
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- IP addresses identified as malicious or suspicious
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom
- Post-incident forensic reports

Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure all data is not accessible for modification or deletion from the system where the data resides.

- Use two-factor authentication with strong passwords, including for remote access services.
- Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords and settings, if applicable.
- Keep computers, devices, and applications patched and up-to-date.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Review the following additional resources:
    - CISA's analysis report and malware analysis report on FiveHands ransomware provide analysis of a threat actor's tactics, techniques, and procedures used in a successful cyberattack; indicators of compromise; and recommended mitigations to protect against, detect, and respond to potential FiveHands ransomware attacks.
    - The joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity provides additional guidance when hunting or investigating a network and common mistakes to avoid in incident handling.
    - The Cybersecurity and Infrastructure Security Agency-Multi-State Information Sharing & Analysis Center Joint Ransomware Guide covers additional best practices and ways to prevent, protect, and respond to a ransomware attack.
    - StopRansomware.gov is the US Government's official one-stop location for resources to tackle ransomware more effectively.

If your organization is impacted by a ransomware incident, the FBI and CISA recommend the following actions:

- **Isolate the infected system.** Remove the infected system from all networks, and disable the computer's networking capabilities, including wireless and Bluetooth. Ensure all shared and networked drives are disconnected, whether wired or wireless.
- **Turn off other computers and devices.** Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any additional computers or devices that share a network with the infected computer(s), even if they have not been fully encrypted by ransomware. If possible, collect and secure all infected and potentially infected computers and

devices in a central location, making sure to clearly label any computers that have been encrypted. Powering-off and segregating infected computers and computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists.

- **Secure your backups.** Ensure that your backup data is offline and secured. If possible, scan your backup data with an antivirus program to check that it is free of malware.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.