FBI FLASH

FEDERAL BUREAU OF INVESTIGATION ♦ CYBER DIVISION

19 April 2022

FLASH Number

CU-000167-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

BlackCat/ALPHV Ransomware Indicators of Compromise

Summary

This FLASH is part of a series of FBI reports to disseminate known indicators of compromise (IOCs) and tactics, techniques and procedures (TTPs) associated with ransomware variants identified through FBI investigations. As of March 2022, BlackCat/ALPHV ransomware as a service (RaaS) had compromised at least 60 entities worldwide and is the first ransomware group to do so successfully using RUST, considered to be a more secure programming language that offers improved performance and reliable concurrent processing. BlackCat-affiliated threat actors typically request ransom payments of several million dollars in Bitcoin and Monero but have accepted ransom payments below the initial ransom demand amount. Many of the developers and money launderers for BlackCat/ALPHV are linked to Darkside/Blackmatter, indicating they have extensive networks and experience with ransomware operations.

Technical Details

BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system. Once the malware establishes access, it compromises Active Directory user and administrator accounts. The malware uses Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware. Initial deployment of the malware leverages PowerShell scripts, in conjunction with Cobalt Strike, and disables security features within the victim's network. BlackCat/ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise.

BlackCat/ALPHV steals victim data prior to the execution of the ransomware, including from cloud providers where company or client data was stored.

The actors leverage Windows scripting to deploy ransomware and to compromise additional hosts. For example, the following batch and PowerShell scripts were observed:

- `start.bat` - launches the ransomware executable with required arguments
- `est.bat` - copies the ransomware to other locations
- `drag-and-drop-target.bat` - launches the ransomware executable for the MySQL Server
- `run.bat` – executes a callout command to an external server using SSH - file names may change depending on the company and systems affected
- `Runs1.ps1` – PowerShell script to disable McAfee

Indicators

The following are characteristics of compromise by BlackCat/ALPHV, as of mid-February 2022:

PowerShell Scripts	
Filename	**MD5 Hash**
amd - Copy.ps1	861738dd15eb7fb50568f0e39a69e107
ipscan.ps1	9f60dd752e7692a2f5c758de4eab3e6f
Run1.ps1	09bc47d7bc5e40d40d9729cec5e39d73
Additional PowerShell Filenames	
[###].ps1	CME.ps1
[#].ps1	Run1.ps1
mim.ps1	[##].ps1
psexec.ps1	Systems.ps1
System.ps1	

Batch Scripts	
Filename	**MD5 Hash**
CheckVuln.bat	f5ef5142f044b94ac5010fd883c09aa7
Create-share-RunAsAdmin.bat	84e3b5fe3863d25bb72e25b10760e861
LPE-Exploit-RunAsUser.bat	9f2309285e8a8471fce7330fcade8619
RCE-Exploit-RunAsUser.bat	6c6c46bdac6713c94debbd454d34efd9
est.bat	e7ee8ea6fb7530d1d904cdb2d9745899
runav.bat	815bb1b0c5f0f35f064c55a1b640fca5

Executables and DLLs	
Filename	**MD5 Hash**
http_x64.exe	6c2874169fdfb30846fe7ffe34635bdb
spider.dll	20855475d20d252dda21287264a6d860
spider_32.dll	82db4c04f5dcda3bfcd75357adf98228
powershell.dll	fcf3a6eeb9f836315954dae03459716d
rpcdump.exe	91625f7f5d590534949ebe08cc728380
Filename	**SHA1 Hash**
mimikatz.exe	d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
run.exe	4831c1b113df21360ef68c450b5fca278d08fae2
zakrep_plink.exe	fce13da5592e9e120777d82d27e06ed2b44918cf
beacon.exe	3f85f03d33b9fe25bcfac611182da4ab7f06a442
win1999.exe	37178dfaccbc371a04133d26a55127cf4d4382f8
[compromised company].exe	1b2a30776df64fbd7299bd588e21573891dcecbe
Additional Observed Filenames	
test.exe	xxx.exe
Mim.exe	xxxw.exe
crackmapexec.exe	Services.exe
plink.exe	Systems.exe
PsExec64.exe	

BlackCat Ransomware SHA256 Hashes:
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
80dd44226f60ba5403745ba9d18490eb8ca12dbc9be0a317dd2b692ec041da28

C2 IPs:			
89.44.9.243	142.234.157.246	45.134.20.66	185.220.102.253
37.120.238.58	152.89.247.207	198.144.121.93	89.163.252.230
45.153.160.140	23.106.223.97	139.60.161.161	146.0.77.15
94.232.41.155			

Information Requested:

The FBI is seeking any information that can be shared, to include IP logs showing callbacks from foreign IP addresses, Bitcoin or Monero addresses and transaction IDs, communications with the threat actors, the decryptor file, and/or a benign sample of an encrypted file.

Recommended Mitigations:

The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to promptly report ransomware incidents to your local FBI field office. Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized “actions” (for example: review the steps each scheduled task is expected to perform).
- Review antivirus logs for indications they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.

- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

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.