FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 AUG 2021

Alert Number
CU-000149-MW

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact www.fbi.gov/contact-us/field-offices

**Note: By reporting any related information to the FBI, 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.*

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

This FLASH has been released **TLP: WHITE**. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with OnePercent Group Ransomware

Summary

The FBI has learned of a cyber-criminal group who self identifies as the "OnePercent Group" and who have used Cobalt Strike to perpetuate ransomware attacks against US companies since November 2020. OnePercent Group actors compromise victims through a phishing email in which an attachment is opened by the user. The attachment's macros infect the system with the IcedID[1] banking trojan. IcedID downloads additional software to include Cobalt Strike. Cobalt Strike moves laterally in the network, primarily with PowerShell remoting.

OnePercent Group actors encrypt the data and exfiltrate it from the victims' systems. The actors contact the victims via telephone and email, threatening to release the stolen data through The Onion Router (TOR) network and clearnet, unless a ransom is paid in virtual currency. OnePercent Group actors' extortion tactics always begin with a warning and progress from a partial leak of data to a full leak of all the victim's exfiltrated data. The extortion/data leak typically follows these steps:

[1] IcedID can also be delivered using TA551 (also known as Shathak and GoldCabin).

- **Leak Warning:** After initially gaining access to a victim network, OnePercent Group actors leave a ransom note stating the data has been encrypted and exfiltrated. The note states the victim needs to contact the OnePercent Group actors on TOR or the victim data will be leaked. If the victim does not make prompt communication within a week of infection, the OnePercent Group actors follow up with emails and phone calls to the victim stating the data will be leaked.

- **One Percent Leak:** If the victim does not pay the ransom quickly, the OnePercent Group actors threaten to release a portion of the stolen data to various clearnet websites.

- **Full Leak:** If the ransom is not paid in full after the "one percent leak", OnePercent Group actors threaten to sell the stolen data to the Sodinokibi Group[2] to publish at an auction.

Ransom Note Details and TOR Website

OnePercent Group ransom notes are uniquely named and provide a link to the TOR website, which victims must access by downloading and using a TOR browser. This website is used to communicate the ransom amount, provide technical support, and negotiate with the victims via an online chat functionality. The victims are instructed to pay the ransom to a Bitcoin address, and advised that a decryption key will be provided in 24-48 hours after payment.

Details
Onion Domain: 5mvifa3xq5m7sou3xzaajfz7h6eserp5fnkwotohns5pgbb5oxty3zad.onion
BTC Address: bc1qds0yly3fn608gtm332gag029munvlute2wxktn

File Names and Tools used by Attackers

The following applications are leveraged by OnePercent actors to compromise victims. While some of these applications support legitimate purposes, they can also be used by threat actors to aid in system compromise or exploration of a victim company's enterprise network:

[2] Sodinokibi is a Russia-based ransomware-as-a-service group.

- AWS S3 cloud
- IcedID
- Cobalt Strike
- Powershell
- Rclone
- Mimikatz
- SharpKatz
- BetterSafetyKatz
- SharpSploit

Technical Details

OnePercent Group actors gain unauthorized access to victim networks through phishing emails with a malicious zip file attachment. The zip file includes a Microsoft Word or Excel document that contains malicious macros that allow the actors to subsequently infect the victim's system with the banking Trojan IcedID. The actors use IcedID to install and execute the software Cobalt Strike on the victim's network to move laterally to other systems within the environment through PowerShell remoting. The actors use rclone for data exfiltration from the victim's network. The actors have been observed within the victim's network for approximately one month prior to deployment of the ransomware.

Once the ransomware is successfully deployed, the victim will start to receive phone calls through spoofed phone numbers with ransom demands and are provided a ProtonMail email address for further communication. The actors will persistently demand to speak with a victim company's designated negotiator or otherwise threaten to publish the stolen data. When a victim company does not respond, the actors send subsequent threats to publish the victim company's stolen data via the same ProtonMail email address.

The FBI identified the following indicators of compromise (IOCs) that we assess are likely associated with this activity.

Indicators	
File Extension of Encrypted Files:	The file extension presents itself as a random 8 character string. .dZCqciAv is an example of an extension seen by a victim company.

File Name of Ransom Note	[8 character random string]-readme.txt This readme file will share the same random characters as the encrypted files. .dZCqciAv-readme.txt is an example seen by a victim company
Observed Malware Filename:	%TEMP%\Temp1_request.zip\[FILENAME].doc %PROGRAMDATA%\vexby.txt
TOR URL:	http://5mvifa3xq5m7sou3xzaajfz7h6eserp5fnkwotohns5pgbb5oxty3zad.onion

Email Addresses Provided by OnePercent Group Threat Actors	
1percentransom@protonmail.com	1percentransomware@protonmail.com

IPs and Domains			
157.245.239.187	31.187.64.199	206.189.227.145	167.71.224.39
80.82.67.221	138.197.179.153	134.209.203.30	nix1.xyz
golddisco.top	delokijio.pw	june85.cyou	intensemisha.cyou
biggarderoub.cyou	d30qpb9e10re4o.cloudfront.net		

Recommended Mitigations

Due to the attackers in question utilizing the rclone program, it is recommended that affected organizations be aware of the following hashes associated with rclone:

Rclone File Hashes	
SHA256 Rclone.exe (64 bit)	ECA9FAC6848545FF9386176773810F96323FEFF0D575C4B6E1C55F8DB842E7FE
SHA1 Rclone.exe (64 bit)	C00CFB456FC6AF0376FBEA877B742594C443DF97
SHA256 Rclone.exe (32 bit)	E70ED531C8A12E7ECCE83223D7B9AA1895110DC140EDF85AFC31C8C5CD580116
SHA1 Rclone.exe (32 bit)	A1D985E13C07EDDFA2721B14F7C9F869B0D733C9
TOR URL:	http://5mvifa3xq5m7sou3xzaajfz7h6eserp5fnkwotohns5pgbb5oxty3zad. onion

- Back-up critical data offline.
- Ensure administrators are not using "Admin Approval" mode.
- Implement Microsoft LAPS, if possible.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device. This information should not be accessible from the compromised network.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the original data resides.
- Keep computers, devices, and applications patched and up-to-date.
- Consider adding an email banner to emails received from outside your organization.
- 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.
- Implement network segmentation.
- Use multi-factor authentication with strong passphrases.

Additional Resources

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomeware.gov is the U.S. Government's new, official one-stop location for resources to tackle ransomware more effectively.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. 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.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Administrative Note

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

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only.