FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

28 JULY 2020

Alert Number

MI-000130-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact your local **Cyber Task Force**

Local Field Offices: https://www.fbi.gov/contact-us/field-offices

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 product 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 Associated with Netwalker Ransomware

Summary

As of June 2020, the FBI has received notifications of Netwalker ransomware attacks on U.S. and foreign government organizations, education entities, private companies, and health agencies by unidentified cyber actors. Netwalker became widely recognized in March 2020, after intrusions on an Australian transportation and logistics company and a U.S. public health organization. Cyber actors using Netwalker have since taken advantage of the COVID-19 pandemic to compromise an increasing number of unsuspecting victims.

Technical Details

Following a successful intrusion, Netwalker encrypts all connected Windows-based devices and data, rendering critical files, databases, and applications inaccessible to users. When executed, Netwalker deploys an embedded configuration that includes a ransom note, ransom note file names, and various configuration options.

In March 2020, actors using Netwalker began exploiting COVID-19 fears by luring unsuspecting victims with pandemic related phishing e-mails. Specifically, Netwalker spread through a Visual Basic Scripting (VBS) script attached to COVID-19 phishing e-mails that executed the payload once opened.

In April 2020, actors using Netwalker began gaining unauthorized access to victim networks by exploiting unpatched Virtual Private Network (VPN) appliances, vulnerable user interface components in web applications, or weak passwords used for Remote Desktop Protocol connections.

Two of the most common vulnerabilities exploited by actors using Netwalker are Pulse Secure VPN (CVE-2019-11510) and Telerik UI (CVE-2019-18935). Once an actor has infiltrated a network with Netwalker, a combination of malicious programs may be executed to harvest administrator credentials, steal valuable data, and encrypt user files. In order to encrypt the user files on a victim network, the actors typically launch a malicious PowerShell script embedded with the Netwalker ransomware executable.

Actors using Netwalker have previously uploaded stolen data to the cloud storage and file sharing service, MEGA.NZ (MEGA), by uploading the data through the MEGA website or by installing the MEGA client application directly on a victim's computer. In June 2020, actors transitioned from uploading and releasing stolen data on MEGA to uploading the stolen data to another file sharing service: website.dropmefiles.com.

Confirmed Indicators		
Email Addresses:		
2hamlampampom@cock.li	galgalgalgalk@tutanota.com	johprohnpo@cock.li
cancandecan@tutanota.com	galgalgalgawk@tutanota.com	kavariusing@tutanota.com
eeaammzzyy@cock.li	hamlampampom@cock.li	kazkavkovkiz@cock.li
eeaammzzyy@tuta.io	hariliuios@tutanota.com	kkeessnnkkaa@cock.li
eeeooppaaaxxx@tuta.io	hhaaxxhhaaxx@tuta.io	kkkwwwsvvv@cock.li
knoocknoo@cock.li	pabpabtab@tuta.io	sevenoneone@cock.li
kokbiglock@cock.li	repairdb@seznam.cz	sevenonone@cock.li
kokoklock@cock.li	rrrkkktttaaa@cock.li	

MD5 Hashes:	
258ed03a6e4d9012f8102c635a5e3dcd	73de5babf166f28dc81d6c2faa369379
3d6203df53fcaa16d71add5f47bdd060	7a1288c7be386c99fad964dbd068964f
5b80cbbdcb697c0b8ec26e6cf0ff305c	993b73d6490bc5a7e23e02210b317247
27304b246c7d5b4e149124d5f93c5b01	8fbc17d634009cb1ce261b5b3b2f2ecb
59881abed688ceba3d67c2ff22076ad8	6a64553da499c1d9a64d97f4de3882f5

SHA-256 Hashes:
8f834966a06f34682b78e1644c47ab488b394b80109ddea39fc9a29ed0d56a0c
58e923ff158fb5aecd293b7a0e0d305296110b83c6e270786edcc4fea1c8404c
8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160
9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967
ad8d379a4431cabd079a1c34add903451e11f06652fe28d3f3edb6c469c43893
de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d

SHA1 Hashes:	
655352e00c7e478c3fed38bc6f407982dec3768d	a3bc2a30318f9bd2b51cb57e2022996e7f15c69e
6fd314af34409e945504e166eb8cd88127c1070e	e393a9ecf0d0a8babaa5efcc34f10577aff1cad1
Malicious Files and Executables:	

qeSw.exe	pw.exe	Invoke-Mimikatz.ps1	mimikatzN.exe
CORONAVIRUS_COVID-19.vbs	wce.exe	Invoke-mimikittenz.ps1	mimikatz.exe
t.exe	pwdump7.exe	dl.exe	rz.ps1

Tor Onion URLs:
rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdq3did.onion

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, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that 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 have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

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 data is not accessible for modification or deletion from the system where the data resides.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Use two-factor authentication with strong passwords.
- Keep computers, devices, and applications patched and up-to-date.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's Internet Crime Complaint Center (IC3). Field office contacts can be identified at https://www.fbi.gov/contact-us/field-offices. Contact IC3 at www.ic3.gov. 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, TLP:WHITE information may be distributed without restriction.

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.