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](mailto:2hamlampampom@cock.li)
- [cancandecan@tutanota.com](mailto:cancandecan@tutanota.com)
- [eeammmzzyy@cock.li](mailto:eeammmzzyy@cock.li)
- [eeammmzzyy@tuta.io](mailto:eeammmzzyy@tuta.io)
- [knoocknoo@cock.li](mailto:knoocknoo@cock.li)
- [kokbiglock@cock.li](mailto:kokbiglock@cock.li)
- [repairdb@seznam.cz](mailto:repairdb@seznam.cz)

**MD5 Hashes:**

- 258ed03a6e4d9012f8102c635a5e3dcd
- 3d6203df53fcaa1ed71add5f47bdd906
- 5b80cbdbcb697cb88ec2666cf0ff305c
- 27304b2467d5b4e149124d5f93c5b01
- 59881abed688ceba3d67c2ff22076ad8

**SHA-256 Hashes:**

- 8f834966a06f34682b78e1644c47ab488b394b08199d6ea39fca9a29ed0d56a0c
- 8639825239d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160
- 9f90275b5dc40ce43ef2a7c7d1aebcbdb244ef6b169aaffb599ebc40368967
- 8f834966a06f34682b78e1644c47ab488b394b08199d6ea39fca9a29ed0d56a0c
- 8639825239d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160

**SHA1 Hashes:**

- 8f834966a06f34682b78e1644c47ab488b394b08199d6ea39fca9a29ed0d56a0c
- 8639825239d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160

**SHA256 Hashes:**

- 8f834966a06f34682b78e1644c47ab488b394b08199d6ea39fca9a29ed0d56a0c
- 8639825239d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160
- 9f90275b5dc40ce43ef2a7c7d1aebcbdb244ef6b169aaffb599ebc40368967
- 8f834966a06f34682b78e1644c47ab488b394b08199d6ea39fca9a29ed0d56a0c
- 8639825239d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160

**SHA1 Hashes:**

- 655352e00c7e478c3fed38bc6f407982dec3768d
- a3bc2a30318f9bd2b51cb57e2022996e7f15c69e
Malicious Files and Executables:

<table>
<thead>
<tr>
<th>Malicious Files</th>
<th>Executables</th>
</tr>
</thead>
<tbody>
<tr>
<td>qeSw.exe</td>
<td>pw.exe</td>
</tr>
<tr>
<td>Invoke-Mimikatz.ps1</td>
<td>mimikatzN.exe</td>
</tr>
<tr>
<td>CORONAVIRUS_COVID-19.vbs</td>
<td>wce.exe</td>
</tr>
<tr>
<td>Invoke-mimikittenz.ps1</td>
<td>mimikatz.exe</td>
</tr>
<tr>
<td>t.exe</td>
<td>pwdump7.exe</td>
</tr>
<tr>
<td>dl.exe</td>
<td>rz.ps1</td>
</tr>
</tbody>
</table>

Tor Onion URLs:

- rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
- pb36hu4sp16cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzjdq3did.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. 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 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.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. Press inquiries should be directed to the FBI’s National Press Office at npo@ic.fbi.gov or (202) 324-3691.

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. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.