FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 MAY 2021

Alert Number

MU-000146-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact

FBI CYWATCH immediately.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, 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 and the Department of Energy.

This FLASH has been released TLP:GREEN: Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Indicators of Compromise Associated with Darkside Ransomware

Summary

In May 2021, the FBI received notification that the ransomware variant Darkside had infected a critical infrastructure company in the United States. The FBI has been investigating Darkside since October 2020. Darkside is a ransomware-as-a-service (RaaS) variant, in which criminal affiliates conduct the attacks and the proceeds are shared with the ransomware developer(s). Darkside has impacted numerous organizations across various sectors including manufacturing, legal, insurance, healthcare, and energy.

Technical Details

After Darkside actors gain access to a victim's network, they not only deploy the Darkside ransomware to encrypt data, but also exfiltrate victim data and then threaten to publish the data to further pressure the victims into paying the ransom demand. This is a double extortion trend.

Darkside actors are encouraged by the ransomware developers to use Monero[1] in their demands, as cyber actors believe that cryptocurrency provides additional anonymity and security. Darkside affiliates use an administrative panel over The Onion Router (TOR) to access communications with the victims and manage administration of the ransomware. The Darkside website includes a landing page with possible victims and descriptions of data taken, as well as a "Press Releases" tab. According to a 27 January 2021 post about rules for using Darkside, affiliates are not allowed to attack the funeral services industry, hospitals, nursing homes, and companies that distribute the COVID-19 vaccine.

Darkside Encryption

Darkside can encrypt files on fixed and removable hardware as well as network devices. Darkside encrypts files using Salsa20 encryption with an RSA-1024 public key and affiliates can use Darkside in both Windows and Linux environments.

Indicators of Compromise

The indicators of compromise that have been observed in samples of Darkside ransomware are listed in Appendix A.

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 and analysts with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks. The FBI is seeking any of the following information that you determine you can legally share, including:

- Recovered executable files

[1] Monero cryptocurrency was released in 2014 and uses various privacy-enhancing technologies to provide users with greater anonymity compared to more traditional cryptocurrencies such as Bitcoin.

- Complete phishing email files with headers
- Live memory (RAM) capture
- Malware samples
- Network and Host Based Log files
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount and if the ransom was paid
- Virtual Currency wallets used by the attackers
- Virtual Currency wallets used to pay the ransom (if applicable)
- Tor sites used to contact the attackers
- Names of any other malware identified on your system
- Copies of any communications with attackers
- Document use of .icu domains for C2
- Identification of website or forum where data was leaked

Recommended Mitigations

- Backup data regularly, keep offline backups, and verify integrity of backup process.
- Keep software updated. Install software patches so that attackers can't take advantage of known problems or vulnerabilities.
- Use two-factor authentication and strong passwords.
- Audit logs for all remote connection protocols.
- Audit logs to ensure all new accounts were intentionally created.
- Scan for open or listening ports, and disable SMBv1.
- Consider disabling RDP if it is not being used.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Monitor Active Directory and local administrators group changes.
- Maintain only the most up-to-date version of PowerShell and uninstall older versions.

- Enable PowerShell logging and monitor for unusual commands, especially execution of Base64 encoded PowerShell.
- Turn off the option to automatically download attachments. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and disable it.

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-offices. CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@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@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked TLP:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

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.