JOINT CYBERSECURITY ADVISORY

TLP:WHITE

Product ID: AA21-131A

May 11, 2021

Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks

SUMMARY

Callout Box: *This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques*.

The Cybersecurity and Information Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are aware of a ransomware attack affecting a critical infrastructure (CI) entity—a pipeline company—in the United States. Malicious cyber actors deployed Darkside ransomware against the pipeline company's information technology (IT) network.[1] At this time, there is no indication that the entity's operational technology (OT) networks have been directly affected by the ransomware.

CISA and FBI urge CI asset owners and operators to adopt a heightened state of awareness and implement the recommendations listed in the Mitigations section of this Joint Cybersecurity Advisory, including implementing robust network segmentation between IT and OT networks; regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections. These mitigations will help CI owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if impacted by ransomware.

- **(Updated May 19, 2021):** Click here for a STIX package of indicators of compromise (IOCs). **Note:** These IOCs were shared with critical infrastructure partners and network defenders on May 10, 2021. The applications listed in the IOCs were leveraged by the threat actors during the course of a compromise. Some of these applications might appear within an organization's enterprise to support legitimate purposes; however, these applications can be used by threat actors to aid in malicious exploitation of an organization's enterprise. CISA and FBI recommend removing any application not deemed necessary for day-to-day operations.

Contact Information

Victims of ransomware should report it immediately to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office. To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

TECHNICAL DETAILS

After gaining initial access to the pipeline company's network, Darkside actors deployed Darkside ransomware against the company's IT network. In response to the cyberattack, the company proactively disconnected certain OT systems to ensure the safety of the OT systems.[2] At this time, there are no indications that the threat actor moved laterally to OT systems.

Darkside is ransomware-as-a-service (RaaS). The Darkside group develops ransomware used by cybercriminal actors and receives a share of the proceeds. According to open-source reporting, since August 2020, Darkside actors have been targeting multiple large, high-revenue organizations, resulting in the encryption and theft of sensitive data. The Darkside group has publicly stated that they prefer to target organizations that can afford to pay large ransoms instead of hospitals, schools, non-profits, and governments.[3],[4]

According to open-source reporting, Darkside actors have previously been observed gaining initial access through phishing and exploiting remotely accessible accounts and systems and Virtual Desktop Infrastructure (VDI) (*Phishing* [T1566], *Exploit Public-Facing Application* [T1190], *External Remote Services* [T1133]).[5],[6] Darkside actors have also been observed using Remote Desktop Protocol (RDP) to maintain *Persistence* [TA0003].[7]

After gaining access, Darkside actors deploy Darkside ransomware to encrypt and steal sensitive data (*Data Encrypted for Impact* [T1486]). The actors then threaten to publicly release the data if the ransom is not paid.[8],[9] The Darkside ransomware uses Salsa20 and RSA encryption.[10]

Darkside actors primarily use The Onion Router (TOR) for *Command and Control (C2)* [TA0011] (*Proxy: Multi-hop Proxy* [1090.003]).[11],[12] The actors have also been observed using Cobalt Strike for C2.[13]

MITIGATIONS

CISA and FBI urge CI owners and operators to apply the following mitigations to reduce the risk of compromise by ransomware attacks.

- **Require multi-factor authentication** for remote access to OT and IT networks.
- **Enable strong spam filters to prevent phishing emails from reaching end users**. Filter emails containing executable files from reaching end users.
- **Implement a user training program and simulated attacks for spearphishing** to discourage users from visiting malicious websites or opening malicious attachments and re-enforce the appropriate user responses to spearphishing emails.
- **Filter network traffic** to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL blocklists and/or allowlists.
- **Update software**, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.

- **Limit access to resources over networks, especially by restricting RDP**. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multi-factor authentication.

CISA and FBI urge CI owners and operators to apply the following mitigations now to reduce the risk of severe business degradation should their CI entity fall victim to a ransomware attack in the future.

- **Implement and ensure robust network segmentation between IT and OT networks** to limit the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- **Organize OT assets into logical zones** by taking into account criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit industrial control system (ICS) protocols from traversing the IT network.
- **Identify OT and IT network inter-dependencies and develop workarounds or manual controls** to ensure ICS networks can be isolated if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans such as manual controls so that safety critical functions can be maintained during a cyber incident.
- **Regularly test manual controls** so that critical functions can be kept running if ICS or OT networks need to be taken offline.
- **Implement regular data backup procedures** on both the IT and OT networks. Backup procedures should be conducted on a frequent, regular basis. The data backup procedures should also address the following best practices:
  - **Ensure that backups are regularly tested**.
  - **Store your backups separately**. Backups should be isolated from network connections that could enable the spread of ransomware. It is important that backups be maintained offline as many ransomware variants attempt to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems to its previous state. Best practice is to store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive. (See the Software Engineering Institute's page on ransomware.)
  - **Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt**. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - **Retain backup hardware** to rebuild systems in the event rebuilding the primary system is not preferred. Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - **Store source code or executables**. It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.

- **Ensure user and process accounts are limited through account use policies, user account control, and privileged account management.** Organize access rights based on the principles of least privilege and separation of duties.
- **Set antivirus/antimalware programs to conduct regular scans** of IT network assets using up-to-date signatures. Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- **Implement unauthorized execution prevention** by:
  - **Disabling macro scripts from Microsoft Office files** transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
  - **Implementing application allowlisting**, which only allows systems to execute programs known and permitted by security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs, including the `AppData/LocalAppData` folder.
- **Monitor and/or block inbound connections from Tor exit nodes and other anonymization services** to IP addresses and ports for which external connections are not expected (i.e., other than VPN gateways, mail ports, web ports). For more guidance, refer to Joint Cybersecurity Advisory AA20-183A: Defending Against Malicious Cyber Activity Originating from Tor.
- **Deploy signatures to detect and/or block inbound connection from Cobalt Strike servers** and other post exploitation tools.

If your organization is impacted by a ransomware incident, CISA and FBI recommend the following actions:

- **Isolate the infected system**. Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected, whether wired or wireless.
- **Turn off other computers and devices**. Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware. If possible, collect and secure all infected and potentially infected computers and devices in a central location, making sure to clearly label any computers that have been encrypted. Powering-off and segregating infected computers and computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists. (See Before You Connect a New Computer to the Internet for tips on how to make a computer more secure before you reconnect it to a network.)
- **Secure your backups**. Ensure that your backup data is offline and secure. If possible, scan your backup data with an antivirus program to check that it is free of malware.
- Refer to Joint Cybersecurity Advisory: AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity for more best practices on incident response.

Note: CISA and the FBI do 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.

CISA offers a range of no-cost cyber hygiene services to help CI organizations assess, identify and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

RESOURCES

- CISA and MS-ISAC: Joint Ransomware Guide
- CISA: Ransomware page
- CISA Tip: Protecting Against Ransomware
- CISA: CISA Ransomware One-Pager and Technical Document
- CISA Insights: Ransomware Outbreak
- CISA: Pipeline Cybersecurity Initiative
- CISA Webinar: Combating Ransomware
- CISA: Cybersecurity Practices for Industrial Control Systems
- FBI: Incidents of Ransomware on the Rise
- National Security Agency (NSA): Stop Malicious Cyber Activity Against Connected Operational Technology
- Department of Energy: Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model
- Transportation Security Agency: Pipeline Security Guidelines
- National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity
- NIST: Ransomware Protection and Response
- NIST: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events
- NIST: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
- NIST: Data Integrity: Recovering from Ransomware and Other Destructive Events
- NIST: Guide to Industrial Control Systems (ICS) Security
- Software Engineering Institute: Ransomware: Best Practices for Prevention and Response

REFERENCES

[1] Colonial Pipeline Media Statement on Pipeline Disruption: https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

[2] Ibid: https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

[3] SonicWall: Darkside Ransomware Targets Large Corporations. Charges up to $2M: https://securitynews.sonicwall.com/xmlpost/darkside-ransomware-targets-large-corporations-charges-up-to-2m/

[4] Varonis: Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign: https://www.varonis.com/blog/darkside-ransomware/

[5] BankInfo Security: FBI: DarkSide Ransomware Used in Colonial Pipeline Attack: https://www.bankinfosecurity.com/fbi-darkside-ransomware-used-in-colonial-pipeline-attack-a-16555

[6] Varonis: Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign: https://www.varonis.com/blog/darkside-ransomware/

[7] Ibid. https://www.varonis.com/blog/darkside-ransomware/

[8] SonicWall: Darkside Ransomware Targets Large Corporations. Charges up to $2M: https://securitynews.sonicwall.com/xmlpost/darkside-ransomware-targets-large-corporations-charges-up-to-2m/

[9] Varonis: Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign: https://www.varonis.com/blog/darkside-ransomware/

[10] McAfee: Threat Landscape Dashboard DarkSide – Ransomware: https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.darkside-ransomware.html

[11] SonicWall: Darkside Ransomware Targets Large Corporations. Charges up to $2M: https://securitynews.sonicwall.com/xmlpost/darkside-ransomware-targets-large-corporations-charges-up-to-2m/

[12] Varonis: Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign: https://www.varonis.com/blog/darkside-ransomware/

[13] McAfee: Threat Landscape Dashboard DarkSide – Ransomware: https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.darkside-ransomware.html