



TLP:CLEAR

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

07 November 2023

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients 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 PIN was coordinated with DHS/CISA.

PIN Number

20231107-001

This PIN has been released **TLP:CLEAR**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Ransomware Actors Continue to Gain Access through Third Parties and Legitimate System Tools

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification to highlight ransomware initial access trends and encourage organizations to implement the recommendations in the "Mitigations" section to reduce the likelihood and impact of ransomware incidents.

Threat

As of July 2023, the FBI noted several trends emerging or continuing across the ransomware environment and is releasing this notification for industry awareness. New trends included ransomware actors exploiting vulnerabilities in vendor-controlled remote access to casino servers, and companies victimized through legitimate system management tools to elevate network permissions.

TLP:CLEAR

- The FBI continues to track reporting of third-party vendors and services as an attack vector for ransomware incidents. Between 2022 and 2023, the FBI noted ransomware attacks compromising casinos through third-party gaming vendors. The attacks frequently targeted small and tribal casinos, encrypting servers and the personally identifying information (PII) of employees and patrons.
- As of June 2023, the Silent Ransom Group (SRG), also called Luna Moth, conducted callback-phishing data theft and extortion attacks by sending victims a phone number in a phishing attempt, usually relating to pending charges on the victims' account. Once the victims called the provided phone number, malicious actors directed them to join a legitimate system management tool via a link provided in a follow-up email. The threat actors then used the management tools to install other legitimate system management tools that can be repurposed for malicious activity. The actors then compromised local files and the network shared drives, exfiltrated victim data, and extorted the companies.

Mitigations

The FBI recommends organizations take the steps below to improve their organization's security posture in response to these new activity trends. The FBI recommends organizations establish and maintain strong liaison relationships with the FBI Field Office in their region. The location and contact information for FBI Field Offices can be located at www.fbi.gov/contact-us/field-offices. Through these partnerships, the FBI can assist with identifying vulnerabilities and mitigating potential threat activity. The FBI further recommends organizations review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a cyber incident.

The FBI and recommends network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by ransomware:

Preparing for Cyber Incidents -

- **Maintain offline backups of data**, and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and that backup data will be accessible when it is needed.
- **Ensure all backup data is encrypted, immutable** (that is, cannot be altered or deleted), and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.
- **Review the security posture of third-party vendors and those interconnected with your organization.** Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

- **Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs** under an established security policy.
- **Document and monitor external remote connections.** Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (that is, a hard drive, other storage device, or the cloud).

Identity and Access Management -

- **Require all accounts** with password logins (for example, service account, admin accounts, and domain admin accounts) **to comply** with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.
 - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
 - Store passwords in hashed format using industry-recognized password managers;
 - Add password user “salts” to shared login credentials;
 - Avoid reusing passwords;
 - Implement multiple failed login attempt account lockouts;
 - Disable password “hints”;
 - Refrain from requiring password changes more frequently than once per year unless a password is known or suspected to be compromised. **Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password “patterns” cyber criminals can easily decipher.
 - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

Protective Controls and Architecture -

- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Secure and closely monitor** remote desktop protocol (RDP) use.
 - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.

Vulnerability and Configuration Management -

- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should prioritize patching of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog.
- **Disable unused ports.**
- **Consider adding an email banner to emails** received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Ensure devices are properly configured and that security features are enabled.**
- **Disable ports and protocols that are not being used** for a business purpose (such as RDP Transmission Control Protocol Port 3389).
- **Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB** (such as SMB version 1). Threat actors use SMB to propagate malware across organizations.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or ic3.gov. 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, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

U.S. Joint Ransomware Task Force (JRTF)

The JRTF, co-chaired by CISA and FBI, is an interagency, collaborative effort to combat the growing threat of ransomware attacks. The JRTF was launched in response to a series of high-profile ransomware attacks on U.S. critical infrastructure and government agencies.

The JRTF:

- Coordinates and streamlines the US Government's response to ransomware attacks and facilitates information sharing and collaboration between government agencies and private sector partners.
- Ensures operational coordination for activities such as developing and sharing best practices for preventing and responding to ransomware attacks, conducting joint investigations and operations against ransomware threat actors, and providing guidance and resources to organizations that have been victimized by ransomware.
- Represents a significant step forward in enabling unity of effort across the US Government's efforts to address the growing threat of ransomware attacks.

For more info on JRTF, see www.cisa.gov/joint-ransomware-task-force.

Administrative Note

This product is marked **TLP:CLEAR**. Subject to standard copyright rules, the information in this product may be shared without restriction.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: <https://www.ic3.gov/PIFSurvey>

