JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

Product ID: AA21-243A

August 31, 2021

Ransomware Awareness for Holidays and Weekends

SUMMARY

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months. The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

Immediate Actions You Can Take Now to Protect Against Ransomware

- Make an offline backup of your data.
- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

THREAT OVERVIEW

Recent Holiday Targeting

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of

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, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. 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. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

ransomware, as network defenders and IT support of victim organizations are at limited capacity for an extended time.

- In May 2021, leading into Mother's Day weekend, malicious cyber actors deployed DarkSide ransomware against the IT network of a U.S.-based critical infrastructure entity in the Energy Sector, resulting in a week-long suspension of operations. After DarkSide actors gained access to the victim's network, they deployed ransomware to encrypt victim data and—as a secondary form of extortion—exfiltrated the data before threatening to publish it to further pressure victims into paying the ransom demand.
- In May 2021, over the Memorial Day weekend, a critical infrastructure entity in the Food and Agricultural Sector suffered a Sodinokibi/REvil ransomware attack affecting U.S. and Australian meat production facilities, resulting in a complete production stoppage.
- In July 2021, during the Fourth of July holiday weekend, Sodinokibi/REvil ransomware actors attacked a U.S.-based critical infrastructure entity in the IT Sector and implementations of their remote monitoring and management tool, affecting hundreds of organizations—including multiple managed service providers and their customers.

Ransomware Trends

The FBI's Internet Crime Complaint Center (IC3), which provides the public with a trustworthy source for reporting information on cyber incidents, received 791,790 complaints for all types of Internet crime—a record number—from the American public in 2020, with reported losses exceeding $4.1 billion. This represents a 69 percent increase in total complaints from 2019. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020, representing a 20 percent increase in the number of incidents, and a 225 percent increase in ransom demands. From January to July 31, 2021, the IC3 has received 2,084 ransomware complaints with over $16.8M in losses, a 62 percent increase in reporting and 20 percent increase in reported losses compared to the same time frame in 2020.[1] The following ransomware variants have been the most frequently reported to FBI in attacks over the last month.

- Conti
- PYSA
- LockBit
- RansomEXX/Defray777
- Zeppelin
- Crysis/Dharma/Phobos

The destructive impact of ransomware continues to evolve beyond encryption of IT assets. Cyber criminals have increasingly targeted large, lucrative organizations and providers of critical services with the expectation of higher value ransoms and increased likelihood of payments. Cyber criminals have also increasingly coupled initial encryption of data with a secondary form of extortion, in which they threaten to publicly name affected victims and release sensitive or proprietary data exfiltrated

[1] This number includes only those victims who have provided information to IC3.

before encryption, to further encourage payment of ransom. (See CISA's Fact Sheet: Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches.) Malicious actors have also added tactics, such as encrypting or deleting system backups—making restoration and recovery more difficult or infeasible for impacted organizations.

Although cyber criminals use a variety of techniques to infect victims with ransomware, the two most prevalent initial access vectors are phishing and brute forcing unsecured remote desktop protocol (RDP) endpoints. Additional common means of initial infection include deployment of precursor or dropper malware; exploitation of software or operating system vulnerabilities; exploitation of managed service providers with access to customer networks; and the use of valid, stolen credentials, such as those purchased on the dark web. Precursor malware enables cyber actors to conduct reconnaissance on victim networks, steal credentials, escalate privileges, exfiltrate information, move laterally on the victim network, and obfuscate command-and-control communications. Cyber actors use this access to:

- Evaluate a victim's ability to pay a ransom.
- Evaluate a victim's incentive to pay a ransom to:
    - Regain access to their data and/or
    - Avoid having their sensitive or proprietary data publicly leaked.
- Gather information for follow-on attacks before deploying ransomware on the victim network.

THREAT HUNTING

The FBI and CISA suggest organizations engage in preemptive threat hunting on their networks. Threat hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack. Threat actors can be present on a victim network long before they lock down a system, alerting the victim to the ransomware attack. Threat actors often search through a network to find and compromise the most critical or lucrative targets. Many will exfiltrate large amounts of data. Threat hunting encompasses the following elements of understanding the IT environment by developing a baseline through a behavior-based analytics approach, evaluating data logs, and installing automated alerting systems.

- **Understand the IT environment's routine activity and architecture by establishing a baseline.** By implementing a behavior-based analytics approach, an organization can better assess user, endpoint, and network activity patterns. This approach can help an organization remain alert on deviations from normal activity and detect anomalies. Understanding when users log in to the network—and from what location—can assist in identifying anomalies. Understanding the baseline environment—including the normal internal and external traffic—can also help in detecting anomalies. Suspicious traffic patterns are usually the first indicators of a network incident but cannot be detected without establishing a baseline for the corporate network.
- **Review data logs.** Understand what standard performance looks like in comparison to suspicious or anomalous activity. Things to look for include:
    - Numerous failed file modifications,

  - Increased CPU and disk activity,
  - Inability to access certain files, and
  - Unusual network communications.
- **Employ intrusion prevention systems and automated security alerting systems**—such as security information event management software, intrusion detection systems, and endpoint detection and response.
- **Deploy honeytokens** and alert on their usage to detect lateral movement.

Indicators of suspicious activity that threat hunters should look for include:

- Unusual inbound and outbound network traffic,
- Compromise of administrator privileges or escalation of the permissions on an account,
- Theft of login and password credentials,
- Substantial increase in database read volume,
- Geographical irregularities in access and log in patterns,
- Attempted user activity during anomalous logon times,
- Attempts to access folders on a server that are not linked to the HTML within the pages of the web server, and
- Baseline deviations in the type of outbound encrypted traffic since advanced persistent threat actors frequently encrypt exfiltration.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for additional guidance on hunting or investigating a network, and for common mistakes in incident handling. Also review the Ransomware Response Checklist in the CISA-MS-ISAC Joint Ransomware Guide.

Cyber Hygiene Services

CISA offers a range of no-cost cyber hygiene services—including vulnerability scanning and ransomware readiness assessments—to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats. By taking advantage of these services, organizations of any size will receive recommendations on ways to reduce their risk and mitigate attack vectors.

RANSOMWARE BEST PRACTICES

The FBI and CISA strongly discourage paying a ransom to criminal actors. Payment does not guarantee files will be recovered, nor does it ensure protection from future breaches. Payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of malware, and/or fund illicit activities. Regardless of whether you or your organization decide to pay the ransom, the FBI and CISA urge you to report ransomware incidents to CISA, a local FBI field office, or by filing a report with IC3 at IC3.gov. Doing so provides the U.S. Government with critical information needed to help victims, track ransomware attackers, hold attackers accountable under U.S. law, and share information to prevent future attacks.

Information Requested

Upon receiving an incident report, the FBI or CISA may seek forensic artifacts, to the extent that affected entities determine such information can be legally shared, including:

- Recovered executable file(s),
- Live memory (RAM) capture,
- Images of infected systems,
- Malware samples, and
- Ransom note.

RECOMMENDED MITIGATIONS

The FBI and CISA highly recommend organizations continuously and actively monitor for ransomware threats over holidays and weekends.[2] Additionally, the FBI and CISA recommend identifying IT security employees to be available and "on call" during these times, in the event of a ransomware attack. The FBI and CISA also suggest applying the following network best practices to reduce the risk and impact of compromise.

Make an offline backup of your data.

- Make and maintain offline, encrypted backups of data and regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete or encrypt accessible backups.
- Review your organization's backup schedule to take into account the risk of a possible disruption to backup processes during weekends or holidays.

Do not click on suspicious links.

- Implement a user training program and phishing exercises to raise awareness among users about the risks involved in visiting malicious websites or opening malicious attachments and to reinforce the appropriate user response to phishing and spearphishing emails.

If you use RDP—or other potentially risky services—secure and monitor.

- Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA. If RDP must be available externally, it should be authenticated via VPN.
- Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts, log RDP login attempts, and disable unused remote access/RDP ports.
- Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).

[2] FBI and CISA highly recommend IT security personnel subscribe to CISA cybersecurity publications—and regularly visit the FBI Internet Crime Complaint (ic3.gov)—for the latest alerts.

- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations.
- 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.
- Open document readers in protected viewing modes to help prevent active content from running.

Update your OS and software; scan for vulnerabilities.

- Upgrade software and operating systems that are no longer supported by vendors to currently supported versions. Regularly patch and update software to the latest available versions. Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which network assets and zones should participate in the patch management program.
- Automatically update antivirus and anti-malware solutions and conduct regular virus and malware scans.
- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices. (See the Cyber Hygiene Services section above for more information on CISA's free services.)

Use strong passwords.

- Ensure strong passwords and challenge responses. Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access.

Use multi-factor authentication.

- Require multi-factor authentication (MFA) for all services to the extent possible, particularly for remote access, virtual private networks, and accounts that access critical systems.

Secure your network(s): implement segmentation, filter traffic, and scan ports.

- Implement network segmentation with multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- 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.
- Scan network for open and listening ports and close those that are unnecessary.

- For companies with employees working remotely, secure home networks—including computing, entertainment, and Internet of Things devices—to prevent a cyberattack; use separate devices for separate activities; and do not exchange home and work content.

Secure your user accounts.

- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties.
- Regularly audit logs to ensure new accounts are legitimate users.

Have an incident response plan.

- Create, maintain, and exercise a basic cyber incident response plan that:
  - Includes procedures for response and notification in a ransomware incident and
  - Plans for the possibility of critical systems being inaccessible for a period of time.

  Note: for help with developing your plan, review available incident response guidance, such as the Public Power Cyber Incident Response Playbook and the Ransomware Response Checklist in the CISA-MS-ISAC Joint Ransomware Guide.

If your organization is impacted by a ransomware incident, the FBI and CISA 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 share 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 from computers that have not been fully encrypted may allow for the recovery of partially encrypted files by specialists.
- 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.

ADDITIONAL RESOURCES

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the U.S. Government's new, official one-stop location for resources to tackle ransomware more effectively. Additional resources include:

- CISA Insights: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses

- CISA: Cyber Essentials
- NIST SP 800-83 Rev. 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security