Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends

Original release date: November 22, 2021

As Americans prepare to hit the highways and airports this Thanksgiving holiday, CISA and the Federal Bureau of Investigation (FBI) are reminding critical infrastructure partners that malicious cyber actors aren't making the same holiday plans as you. Recent history tells us that this could be a time when these persistent cyber actors halfway across the world are looking for ways—big and small—to disrupt the critical networks and systems belonging to organizations, businesses, and critical infrastructure.

There are actions that executives, leaders, and workers in any organization can take proactively to protect themselves against cyberattacks, including possible ransomware attacks, during the upcoming holiday season—a time during which offices are often closed, and employees are home with their friends and families. Although neither CISA nor the FBI currently have identified any specific threats, recent 2021 trends show malicious cyber actors launching serious and impactful ransomware attacks during holidays and weekends, including Independence Day and Mother's Day weekends.

CISA and the FBI strongly urge all entities–especially critical infrastructure partners–to examine their current cybersecurity posture and implement best practices and mitigations to manage the risk posed by cyber threats. Specifically, CISA and the FBI urge users and organizations to take the following actions to protect themselves from becoming the next victim:

- Identify IT security employees for weekends and holidays who would be available to surge during these times in the event of an incident or ransomware attack.
- Implement multi-factor authentication for remote access and administrative accounts.
- Mandate strong passwords and ensure they are not reused across multiple accounts.
- If you use remote desktop protocol (RDP) or any other potentially risky service, ensure it is secure and monitored.
- Remind employees not to click on suspicious links, and conduct exercises to raise awareness.

Additionally, CISA and the FBI recommend maintaining vigilance against the multiple techniques cybercriminals use to gain access to networks, including:

- Phishing scams, such as unsolicited emails posing as charitable organizations.
- Fraudulent sites spoofing reputable businesses—it is possible malicious actors will target sites often visited by users doing their holiday shopping online.
- Unencrypted financial transactions.

Finally—to reduce the risk of severe business/functional degradation should your organization fall victim to a ransomware attack—review and, if needed, update your incident response and communication plans. These plans should list actions to take—and contacts to reach out to—should your organization be impacted by a ransomware incident. Note: for assistance, review available incident response guidance, such as the Ransomware Response Checklist in the CISA-MS-ISAC Joint Ransomware Guide, the Public Power Cyber Incident Response Playbook, and the new Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

CISA and the FBI urge users and organizations to take these actions immediately to protect themselves against this threat. For a comprehensive overview, see the joint Cybersecurity Advisory Ransomware Awareness for Holidays and Weekends. For more information and resources on protecting against and responding to ransomware, visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.