ANALYSIS REPORT

AR21-134A NUMBER

May 14, 2021 DATE

Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise

SUMMARY

Since December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) has been responding to a significant cyber incident. An advanced persistent threat (APT) actor added malicious code to multiple versions of SolarWinds Orion and, in some instances, leveraged it for initial access to enterprise networks of multiple U.S. government agencies, critical infrastructure entities, and private sector organizations. Once inside the network, the threat actor bypassed multi-factor authentication (MFA) and moved laterally to Microsoft Cloud systems by compromising federated identity solutions. **Note:** On April 15, 2021, the U.S. Government attributed this activity to the Russian Foreign Intelligence Service (SVR). See the statement from the White House for additional details.

For more information and resources on this activity, refer to us-cert.cisa.gov/remediating-apt-compromised-networks. For more information on CISA's response to this activity, refer to cisa.gov/supply-chain-compromise.

CISA has provided this guidance to federal agencies with networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity—CISA Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations labels these as Category 3 agencies. This guidance is intended to support Category 3 agencies in crafting their eviction plans in accordance with ED 21-01: Supplemental Direction Version 4 placeholder]. **Note**: agencies should refer to CISA Alert AA20-352A for guidance on determining if they are Category 3. CISA is aware of other initial access vectors; agencies should not assume they are not compromised by this APT actor solely because they have never used affected versions of SolarWinds Orion. Those agencies should investigate to confirm they have not observed related threat actor tactics, techniques, and procedures (TTPs). CISA recommends any agency that detects related activity review this guidance as well as CISA Alert AA20-352A, and contact CISA for further assistance.

Although this guidance is tailored to federal agencies, CISA encourages critical infrastructure entities; state, local, territorial, and tribal government organizations; and private sector organizations to review and apply it, as appropriate.

The steps provided in this guidance are resource-intensive and highly complex and will require the enterprise network to be disconnected from the internet for 3–5 days. In order to have fully informed senior-level support, CISA recommends that agency senior leadership conduct planning sessions throughout this process to understand the resources needed and any potential disruption in business operations. CISA encourages agency leadership to review CISA Insights: SolarWinds and AD/M365 Compromise Risk Decisions for Leaders for more information.

By taking steps to evict this adversary from compromised on-premises and cloud environments, agencies will position themselves for long-term actions to build more secure, resilient networks.

DESCRIPTION

> ***Important:*** *Category 3 organizations should use out-of-band communications for all mitigation and remediation communications and documentation, i.e., do not use any compromised systems to internally or externally communicate remediation plans or actions.*

Remediation plans for dealing with malicious compromises are necessarily unique to every organization, and success requires careful consideration. There are three phases for evicting the actor:

- **Phase 1: Pre-Eviction**. Actions to detect and identify APT activity and prepare the network for eviction. **Note**: for the purposes of this guidance, a network is defined as any computer network with hosts that share either a logical trust or any account credentials with affected versions of SolarWinds Orion.
- **Phase 2: Eviction**. Actions to remove the APT actor from on-premises and cloud environments. This phase includes rebuilding devices and systems.
- **Phase 3: Post-Eviction**. Actions to ensure eviction was successful and the network has good cyber posture.

Conducting eachstep in this guidance is necessary to fully evict the adversary from Category 3 networks. **Failure to perform comprehensive and thorough remediation activity will expose enterprise networks and cloud environments to substantial risk for long-term undetected APT activity**, and compromised organizations will risk further loss of sensitive data and erosion of public trust in their networks.

Although this guidance provides a level of detail that describes actions to be completed, it does not describe how these actions should be completed. To successfully evict the threat actor, these actions need to be conducted in the order specified. Additionally, this guidance clearly notes caveats and provides references to help agencies develop their plan.

Pre-Eviction Phase

1. **Define the true scope** by identifying trust boundaries (including between Active Directory [AD] forests and domains) and determining the enterprise assets to which this guidance applies (i.e., determine what assets are within the trust boundary).
    a. For example, the organization needs to determine the identity provider (IdP) sources (such as Okta, Microsoft Active Directory Federation Services [ADFS],

Duo) that it uses to issue single-sign on (SSO) credentials and it needs to identify assets that rely on the SSO credentials to allow access (i.e., what controlled data sources are accessible via that credential).

2. **Investigate suspicious account activity** associated with your SolarWinds servers, especially service accounts used by SolarWinds Orion. Additionally, enumerate and investigate any credentials stored or used on the SolarWinds server, including network administration and device credentials. This can be conducted, for example, using a transitive mapping of all potentially compromised credentials to the systems that those credentials accessed. If—as a Category 3 agency—you cannot confirm that all your credential activity is benign, you should proceed as if the highest administrative level of credentials on your affected SolarWinds server has been compromised. In many cases, the adversary may have had this access for months. Refer to the following resources for more information.
    a. FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
    b. CISA Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

3. **Investigate potential Security Assertion Markup Language (SAML) abuse** in your environment. Refer to the following resources.
    a. CISA Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
    b. National Security Agency: Detecting Abuse of Authentication Mechanisms
    c. FireEye: Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452
    d. Microsoft: Understanding "Solorigate's Identity IOCs - for Identity Vendors and their customers

    Note: if the adversary has compromised administrative level credentials in an environment—or if your organization has identified SAML abuse in the environment— simply mitigating individual issues, systems, servers, or specific user accounts will likely not lead to the adversary's removal from the network. In such cases, organizations should consider the entire identity trust boundary compromised. In the event of a total identity compromise, successful remediation requires a full reconstitution of identity and trust services. Because this threat actor is among the most capable, in many cases, a full rebuild of the environment is the safest action. For many organizations, remediation from this level of compromise may necessitate engaging third-party assistance.

4. **Scope the intrusion**.
    a. Look for the artifacts from known TTPs associated with this activity. Refer to SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures for TTPs and corresponding detection artifacts. Prioritize these by biggest value for the investment

(e.g., prioritize these by techniques or technologies that cover multiple tactics or that provide visibility into shared data sources). After identifying the TTPs for which your organization has security controls to detect/stop/mitigate, you can make risk-based decisions on how to address visibility and protection strategies for the remaining MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)-based paths.

b. Audit all network device configurations stored or managed on the SolarWinds monitoring server for signs of unauthorized or malicious configuration changes. Organizations should audit the current network device running configuration and any local configurations that could be loaded at boot time.
c. Assess the current endpoint telemetry collection level and configure endpoint forensics and detection solutions for aggressive collection; prioritize this by value of asset and account.

5. **Harden the enterprise attack surface.**
    a. Review and validate perimeter firewall rulesets. Remove all allow rules for which the organization does not have a clearly defined, understood, and documented need. "Deny all" statements that identify necessary connections and allow them as exceptions are the standard for perimeter devices.
        i. Reduce the number of systems that are able to access the internet directly. **Note:** this action may require analysis by network engineers with fundamental knowledge of (1) how network data communicates through agency trust boundaries and (2) the IP routing in the enterprise.
            - For example, domain controllers should never be used for—or capable of— browsing the internet (Microsoft's analysis of domain controllers identified that privileged users often use Internet Explorer to browse the intranet or internet).
            - For more information on designing networks where critical or security-related appliances and servers do not have access to the internet, refer to the United Kingdom's National Cyber Security Centre (NCSC): Security Architecture Anti Patterns.
        ii. Reduce the number of egress ports at the enterprise perimeter. This requires a review of all perimeter firewall rulesets (rulesets may differ among firewalls).
    b. Implement host-based firewalls to make the work of moving laterally more challenging for the adversary, disrupting the ability to move from compromised workstations to domain resources. Consider blocking or closely monitoring workstation-to-workstation communications as much as possible, using Privileged Access Workstations (PAWs) and servers for administrative functions. Firewalls and endpoint detection and response functions may have similar capability, but both need to feature (1) filtering of allowed connections and (2) visibility/detection for connections.
    c. Close and/or monitor high-risk ports (e.g., Remote Desktop Protocol [RDP], Server Message Block [SMB], File Transfer Protocol [FTP], Trivial File Transfer

Protocol [TFTP], Secure Shell [SSH], and WebDAV).

d. Carefully employ application execution control (allowlisting), especially for systems providing remote access to the enterprise.
e. Enforce enterprise Domain Name System (DNS) resolution for all systems. Do not allow internal systems to directly access internet DNS servers.
f. Ensure that all endpoints that will need to be updated are powered on for as long as possible during the eviction phase. **Note**: this action is necessary for all vital changes to AD to be pushed to all systems in the environment prior to reconnection and also to verify that all systems are rebooted. This action is especially tricky given that many user endpoints are not connected 24/7 due to remote work. Organizations may want to look at "jailing" systems that connect in this way into minimal virtual local area networks (VLANs) until they can be verified to have received and implemented updates and any other mitigations (endpoint detection and response [EDR] agents, patches, antivirus definitions, specific scans, etc.) decided on by the organization.
g. Agencies using Microsoft Defender for Endpoint or Microsoft 365 Defender should refer to Microsoft: Use attack surface reduction rules to prevent malware infection for more information on hardening the enterprise attack surface.

6. **Identify federation model for on-premises resources to cloud trust relationship and identify adversary activity in Microsoft 365 (M365)/Azure environment.**
    a. Identify the Source Anchor for Azure AD Connect in the current Azure Tenant, if used (this is required in order to sever the connection and restore later).
    b. Run Sparrow or similar tools to identify permission and credential changes to applications and service principals. Identify overly permissive applications, unusual credentials in applications, or modifications to federation trust settings. Refer to CISA Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments for more information.
    c. Review M365 tenant configuration and perform a cloud security assessment for administrative accounts and applications. Specifically, review all accounts with privileged access and each application to determine if the rights and credentials are as intended and still necessary.
        i. This assessment should include shared trusts or identity relationships with third-party cloud service providers (CSPs) in which the identity is a resident on the CSP's tenant but is also capable of performing actions in the organization's M365 environment.

Eviction Phase

Note: to effectively evict the APT action, the following steps should be completed fully and in the order listed.. These steps may affect operations of critical business functions. CISA recommends agencies conduct a thorough risk assessment prior to starting eviction so that potential impacts on critical business functions are documented and understood. Given that these steps are complex, CISA also encourages agencies to use third-party help to support eviction efforts if needed.

1. **Sever the enterprise network from the internet**.

    Note: this step requires the agency to understand its internal and external connections. When making the decision to sever internet access, knowledge of connections must be

combined with care to avoid disrupting critical functions.

2. **Reset the Kerberos Ticket Granting Ticket account (krbtgt)**.

   Note: krbtgt must be reset twice; the second time after the first has finished. The resets may take a long time to propagate fully on large AD environments. For more information, refer to Microsoft guidance: AD Forest Recovery - Resetting the krbtgt password.

3. **Eradicate known malware/backdoors/implants discovered during pre-eviction steps**.

   Note: this can be done while waiting for the krbtgt resets to complete.

4. **Apply network device mitigations** identified in CISA Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organization.

   For network devices managed by the SolarWinds monitoring server, the running firmware/software should be checked against known good hash values from the network vendor. CISA recommends that, if possible, organizations re-upload known good firmware/software to managed network devices and perform a reboot.

   Note: be sure to wait until after krbtgt reset completes to avoid interrupting the reset.

5. **Unenroll any suspicious MFA tokens.** Audit all MFA tokens configured in your environment, especially those used for remote access. Unenroll any tokens that cannot be accounted for or are suspicious.

6. **Rebuild and reimage systems**.

   Note: agencies should do an impact assessment for endpoints to determine if they need to be reimaged. An agency should identify (1) credentials observed on compromised machines as at risk and (2) any subsequent system accessed from the corresponding accounts as compromised. Consider:

   a. Was the endpoint altered by a known malicious actor action? If yes, reimage the system.
   b. Was data on the endpoint accessed but the endpoint shows no sign of being altered? If yes, you may not need to reimage the system.

7. **Regain control of the AD and ADFS,** by instituting Local Administrator Password Solution (LAPS), PAWs, and modified administrative accounts.
   a. Re-establish control of the ecosystem items that were most easily manipulated by the attacker. Start with the “lowest hanging fruit,” i.e., items that are low risk to operations, low administrative overhead, that do not require new skill sets to control. These actions block the most frequently used attack methods on a network. Refer to the Microsoft and Center for Internet Security joint presentation Critical Hygiene for Preventing Major Breaches for more information on prioritizing controls with the

largest return on investment.

i. Audit the privilege levels of accounts that were utilized on affected SolarWinds Orion servers. Consider only granting the minimal rights and accounts needed to function, following Just Enough Administration (JEA) principles. (Refer to Microsoft: Just Enough Administration for more information.)
ii. Ensure there are unique and distinct administrative accounts for each set of administrative tasks. Enforce the principle of least privilege. Remove all accounts that are unnecessary; remove privileges not expressly required by an account's function or role. Institute a group policy that disables remote interactive logins and use Domain Protected Users Group.
iii. Enforce MFA for all administrative accounts and functions.
iv. Create and establish PAWs for administrative accounts and mandate use for administrative functions (AD Administrators first, at minimum).
v. Enable unique local administrative accounts (e.g., LAPS) and a management function for those accounts. (**Note:** For LAPS, if the endpoints are cloned, each individual endpoint's local administrative account password needs to be changed afterward to enforce uniqueness.)

8. **Rotate all the Secrets**.
   a. Rotate secrets associated with remote access MFA token generation.
   b. Reset passwords for:
      i. All AD accounts with elevated privileges (such as administrators)
      ii. All AD service accounts
      iii. Directory Services Restore Mode (DSRM) account on domain controllers
      iv. All AD accounts
      v. Accounts with suspicious activity or whose credentials existed on compromised systems, such as affected SolarWinds servers
      vi. Any account where Smartcard/Personal Identity Verification (PIV) is not enforced (which are on an exception or similar exemption)

          Note: the New Technology LAN Manager (NTLM) hashes of smartcard/PIV-enabled accounts can be used in pass-the-hash attacks and should be refreshed regularly. For more information, including guidance and scripts on rolling over these hashes, refer to the National Security Agency (NSA) Information Assurance Advisory: Long-Lived Hashes for AD Smartcard Required Accounts, NSA Cyber's GitHub page on Pass the-Hash Guidance, and Microsoft: Passwordless Strategy.

      vii. All AD user accounts
      viii. All Windows local administrative accounts (including those that are renamed, especially those not managed by LAPS in environment)
      ix. Non-AD application privileged accounts (e.g., elevated accounts on systems that are not joined to AD; some high value assets (HVAs) may fall into this category)
      x. Network device administrative accounts
      xi. Non-AD HVA user accounts

c. Change all credentials being used to manage network devices, including keys and strings used to secure network device functions (Simple Network Management Protocol [SNMP] strings/user credentials, IPsec/IKE preshared keys, routing secrets, TACACS/RADIUS secrets, RSA keys/certificates, etc.). Monitor for failed logins resulting from these resets.

9. **Sever Azure environment from on-premises, and conduct M365/Azure remediation**.
    a. Evaluate IdP sources. Harden SSO features. (See FireEye's white paper, Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452). Turn on advanced logging and establish a privileged access management (PAM) baseline (expected privileged account state) for cloud environments.
    b. Harden the Azure AD Connect Service. (See Trimarc Security's post, Securing Microsoft Azure AD Connect.)
    c. Review and adjust federation trust relationships. **Note:** Microsoft recommends severing federation trusts between on-premises networks and the cloud; organizations should migrate to an external IdP or use Azure AD to manage users and, if the latter, users should be "mastered" from Azure AD. Revoke unauthorized or unnecessary federation trusts if maintaining a federated identity solution. (CISA recommends avoiding federated enterprise environments whenever possible.) For more information review the following resources.
        - Microsoft: Protecting Microsoft 365 from on-premises attacks
        - CrowdStrike: CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory
    d. Fully isolate your M365 admin accounts. Activities in this step include, but are not limited to (1) creating cloud-only administrators, controlled appropriately with role based access control (RBAC) and MFA, and (2) monitoring, in an automated fashion, any changes to the established baseline or unusual use. See the following resources for more information (**Note:** CISA will be releasing guidance on cloud remediation and hardening following dissemination of this guidance).
        - Microsoft: Advice for incident responders on recovery from systemic identity compromises
        - Microsoft: Protecting Microsoft 365 from on-premises attacks
    e. After remediating privileged identities (step d), revoke all existing M365 tokens.
    f. Double check to ensure no on-premises accounts have administrative privileges in M365.
    g. Review and sanitize (i.e., remove unwelcome actions) compromised mailboxes using industry standard tooling and service portal manual review.
    h. Review, and adjust accordingly, Tenant settings and configurations. Use publicly available or open-source tools such as CrowdStrike Reporting Tool for Azure (CRT) and Hawk to review Tenant settings. Refer to CISA Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.
    i. Use tools—such as Sparrow or Azure AD Investigator—to review existing Azure

applications. Remediate applications that have been compromised. Refer to CISA Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.

j. Perform IdP review and eviction.

10. **Clear DNS cache** on all servers, workstations, and non-Windows systems.
    a. Reduce the "Domain member: Maximum machine account password age" in Group Policy to 2–3 days during eviction; it can be set back to the default 30 days after eviction is complete. This will hasten the resetting of the Computer object passwords. For more information, refer to Microsoft: Machine Account Password Process.
    b. Reboot all servers and workstations, especially those joined to the AD.

11. **Verify eviction steps have been properly completed**.
    a. Have all the tasks above been completed on all applicable systems and accounts? **Note:** CISA highly recommends implementing a process to verify you have completed each task.
    b. Have the endpoints that were not completely mitigated been removed from network communication, pending their completion?
    c. Have you applied all critical and high patches to the endpoints that lack them, especially any that needed re-imaging?
    d. Have you added enhanced visibility and monitoring capabilities for cloud environments—such as telemetry for cloud environments—into existing agency security information and event management (SIEM) technology?
    e. Have you implemented monitoring capability for highly privileged cloud identities and Service Principals?

POST EVICTION

1. **Report to your senior leadership completed pre-eviction and eviction actions** as well as those remaining to be completed; provide leadership an assessment of the risk remaining, including assumed residual risk.
2. **Reconnect to the internet**. **Note:** the decision to reconnect to the internet depends on senior leadership's confidence in the actions taken. It is possible—depending on the environment—that new information discovered during pre-eviction and eviction steps could add additional eviction tasks.
3. **Create an actionable and accountable plan for integrating the next 60 days of Active Directory privilege credential baselining guidance** (i.e., completing the next step). **Note:** this next step has high overhead and will likely disrupt business operations; agencies must have a plan for testing breaks associated with the changes to administrative control schemes and will need to alter their policies and procedures to accommodate these disruptions.
4. **Establish and control baseline mechanisms for administrators**.

Note: this step should be completed over the next 60 days. *While completing this task, agencies should move on to the next step*.

    a. Implement PAWs for remaining administrative accounts.

b. Perform additional hardening of administrative accounts.
    i. Implement Credential Guard. (Refer to Microsoft: Manage Windows Defender Credential Guard for more information.)
        1. Introducing Credential Guard as an endpoint tool can be challenging for organizations due to hardware restrictions, but the impact on privileged identity credential management is significant. Chief information security officers (CISOs) should prioritize identity-focused solutions for immediate action.
    ii. Restrict RDP usage to an exclusive list of necessary administrators and from only dedicated administrative workstations (such as PAWs) and identified necessary alternative locations. RDP access should be judiciously and carefully scoped and monitored.
    iii. Establish time bound and temporal escalated Domain Privileges (require second factor for elevation and that access expires).
c. Implement JEA for domain controller access and maintenance.
d. Harden/reduce attack surface of domain controllers. Remove connection to the internet whenever possible, and remove all unnecessary protocols, services, and accounts (in accordance with the principle of least functionality). Consider implementing Windows Server Core for all domain controllers.

5. **Integrate detection mechanisms** that focus on endpoints and changes to privileged identity sources. Solutions include pervasive use of endpoint security (such as the Microsoft Defender Suite of services, including Endpoint and Identity) as well as high value identity monitoring solutions. The view of user behavior should be unified across all platforms and behavioral analytics should be enabled. **Note:** behavioral analytics (with an understanding of what traditional administrative activity consists of, and what tools are used for it) combined with frequency analysis of activity is often the only avenue for network defenders to detect anomalous activity.
6. **Report to CISA**. Post-eviction, all Category 3 agencies should report to CISA actions taken, any actions left incomplete, and their assessments of the residual risk. Following dissemination of this guidance, CISA will release a checklist to the Homeland Security Information Network (HSIN) for agencies to use to complete the steps in this guidance. Agencies should fill out and submit the checklist to CISA.
7. **Maintain vigilance**. In the hours, days, and weeks after the network's internet connection is restored, the agency's detection capability will be important in verifying that all threat actor activity within the enterprise has stopped. Extended vigilance is necessary because this threat actor has demonstrated extreme patience with follow-on activity.
    a. Agencies should ensure their security operations center (SOC) has capabilities for enhanced visibility and monitoring of enterprise network and cloud environments. Refer to SolarWinds and Active Directory/M365 Compromise: Detecting APT Activity from Known Tactics, Techniques, and Procedures for known TTPs that agencies should look out for as part of network and environment monitoring.
    b. Configure endpoint forensics and detection solutions for aggressive collection; prioritize this by value of asset and account.

FREQUENTLY ASKED QUESTIONS

Does my organization have to complete all the steps in this eviction guidance?

In accordance with ED 21-01: Supplemental Direction Version 4, agencies with networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity, such as binary beaconing to `avsvmcloud[.]com` and secondary command and control (C2) activity to a separate domain or IP address, must execute and complete the pre-eviction phase of this guidance. Agencies that find additional adversarial activities must execute and complete the eviction and post eviction phases of this guidance. Conducting all of the steps in this guidance is necessary to fully evict the adversary from applicable networks. Failure to perform comprehensive and thorough remediation activity will expose enterprise networks and cloud environments to substantial risk for long-term undetected APT activity.

Is there a time limit to completing the eviction activities?

In accordance with ED 21-01: Supplemental Direction Version 4, agencies subject to the requirements must complete the applicable phases in this eviction guidance by July 16, 2021, or within 90 days of discovery of follow-on threat activity after issuance of ED 21-01 Supplemental Direction Version 4.

Given that severing the enterprise network from the internet will have significant operational impact, does the organization need to take *all* its endpoints offline?

If the affected organization can authoritatively and comprehensively identify compromised internet-connected endpoints, identities, and systems and is able to take those offline without affecting uncompromised or non-internet connected systems, then the agency does not need to disconnect non-compromised endpoints or non-internet-connected systems. This will still disrupt C2 activities while allowing the agency to keep as much of the system up as possible. **Note**: access to environments with pervasively compromised credentials will frequently appear to be standard user activity, as it will use “native” services and identities.

Will CISA provide agencies new TTPs in the event of a reinfection?

Refer to SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures for reinfection TTPs and corresponding detection artifacts.

Will CISA provide architectural recommendations for future rebuilds?

This current guidance is tailored to provide short-term remediation steps for agencies to evict this adversary from compromised on-premises and cloud environments and protect networks against additional compromise. CISA will be releasing long-term enterprise architecture and security operations guidance that incorporates updated credential/access management, monitoring, and detection guidance for a more secure, resilient federal enterprise.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at:

- Phone: (888) 282-0870
- Email: central@cisa.gov