Volt Typhoon State-Sponsored Threat Actors Targeting Critical Infrastructure

Threat Bulletins | TLP:WHITE | Alert ID : 2d926381 | Mar 22, 2024, 12:48 PM

Health-ISAC is disseminating this alert out of an abundance of caution influenced by risks and associated security implications stemming from the posturing of targeted cyber attacks against critical infrastructure. Attacks on water and wastewater systems have the potential to disrupt clean and safe drinking water, imposing significant costs on healthcare providers.

Specifically, state-sponsored threat actor activity associated with the People's Republic of China (PRC) has been observed in cyberattacks against water systems. Threat actors are increasingly targeting critical infrastructure, seeking to disrupt essential services to inflict cascading impacts. Specific guidance for securing water and wastewater systems is available for critical infrastructure defenders around the globe.

On March 19, 2024, the Environmental Protection Agency (EPA) shared a letter discussing the urgent need to safeguard critical infrastructure against cyber threats. Specifically, the EPA emphasized drinking water and wastewater systems are critical resources, but many systems have not adopted important cybersecurity practices to thwart potential cyberattacks.

On February 7, 2024, Health-ISAC shared an alert titled People's Republic of China (PRC) State-Sponsored Actors Compromise and Maintain Access to Critical Infrastructure, which focuses explicitly on attacks from Volt Typhoon. The alert includes a link to guidance for identifying and mitigating living off-the-land techniques commonly used by Volt Typhoon. Critical infrastructure organizations around the globe are encouraged to consider this guidance while securing healthcare sector infrastructure from attacks.

Recommendations

Critical infrastructure defenders are encouraged to ensure the following mitigation measures are implemented:

- Implement multifactor authentication for access to the operational technology (OT) network whenever applicable.
- If you require remote access, implement a firewall and/or virtual private network (VPN) to control network access. A VPN or gateway device can enable multifactor authentication for remote access even if the system does not support multifactor authentication.
- Create strong backups of the logic and configurations of systems to enable fast recovery. Familiarize yourself with factory resets and backup deployment as preparation in the event of ransomware activity.
- Keep systems updated with the latest versions by the manufacturer.
- Confirm third-party vendors are applying applicable countermeasures to mitigate exposure of systems and all installed equipment.

Please also review the attached resources for additional insight and mitigation guidance.

Reference | References

CISA ICS Medical Advisory
CISA ICS Medical Advisory
CISA ICS Medical Advisory
epa
epa
CNN Money
Bleeping Computer
Security Week

Tags

Volt Typhoon, People's Republic of China, PRC

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org

PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS

SUMMARY

This fact sheet provides an overview for executive leaders on the urgent risk posed by People's Republic of China (PRC) state-sponsored cyber actors known as "Volt Typhoon." CISA—along with the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and other U.S. government and international partners[1]—released a major advisory on Feb. 7, 2024, in which the U.S. authoring agencies warned cybersecurity defenders that Volt Typhoon has been pre-positioning themselves on U.S. critical infrastructure organizations' networks to enable **disruption or destruction of critical services** in the event of increased geopolitical tensions and/or military conflict with the United States and its allies. This is a critical business risk for every organization in the United States and allied countries.[2]

The advisory provides detailed information related to the groups' activity and describes how the group has successfully compromised U.S. organizations, especially in the Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors.[3] The authoring organizations urge critical infrastructure owners and operators to review the advisory for defensive actions against this threat and its potential impacts to national security.

CISA and partners[4] are releasing this fact sheet to provide leaders of critical infrastructure entities with guidance to help prioritize the protection of critical infrastructure and functions. The authoring agencies urge leaders to recognize cyber risk as a core business risk. This recognition is both necessary for good governance and fundamental to national security.

[1] U.S. Department of Energy (DOE), U.S. Environmental Protection Agency (EPA), U.S. Transportation Security Administration (TSA), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Communications Security Establishment's (CSE's) Canadian Centre for Cyber Security (CCCS), United Kingdom National Cyber Security Centre (NCSC-UK), and New Zealand National Cyber Security Centre (NCSC-NZ)

[2] CCCS assesses that Canada would likely be affected as well, due to cross-border integration. ASD's ACSC and NCSC-NZ assess Australian and New Zealand critical infrastructure, respectively, could be vulnerable to similar activity from PRC state-sponsored actors.

[3] See Critical Infrastructure Sectors | CISA for descriptions of critical infrastructure sectors.

[4] NSA, FBI, DOE, EPA, TSA, U.S. Department of the Treasury, ASD's ACSC, CCCS, NCSC-UK, and NCSC-NZ

ACTIONS FOR LEADERS

Make Informed and Proactive Resourcing Decisions

Empower cybersecurity teams to make informed resourcing decisions to better detect and defend against Volt Typhoon and other malicious cyber activity. As a first step, organizations should use intelligence-informed prioritization tools, such as the Cybersecurity Performance Goals (CPGs) or derived guidance from an SRMA. The CPGs help leaders make strategic investments in a limited number of essential actions with high-impact security outcomes. Second, empower and resource cybersecurity teams so they can:

- **Effectively apply detection and hardening best practices** contained in Identifying and Mitigating Living off the Land Techniques and PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Volt Typhoon does not rely on malware to maintain access to networks and conduct their activity. Rather, they use built-in functions of a system. This technique, known as "living off the land," enables them to easily evade detection. To protect against living off the land, organizations need a comprehensive and multifaceted approach, as described in these joint products.

> Key best practices for your cybersecurity teams includes **ensuring logging, including for access and security, is turned on for applications and systems and logs are stored in a central system**. Robust logging is necessary for detecting and mitigating living off the land. Ask your IT teams which logs they maintain as certain logs reveal commands (referenced in the CSA) used by Volt Typhoon actors. If your IT teams do not have the relevant logs, ask which resources they may need to effectively detect compromise.

- **Receive continuous cybersecurity training and skill development** that is relevant to the threat environment. Continuous training ensures that staff have the capabilities needed to defend their unique environments and maintain good cyber hygiene.
- **Develop comprehensive information security plans and conduct regular tabletop exercises**.
    - Leaders should ensure personnel from all business sections, including executive leadership, are involved in development of the plan, sign off on it, and are aware of their roles and responsibilities. Ensuring comprehensive and tested plans are in place and approved enables cybersecurity teams to make appropriate risk-informed decisions.
    - Refresh and test plans on an appropriate basis, and test OT systems and manual mode.

For smaller organizations without their own in-house cybersecurity teams, leaders should obtain managed security services that can carry out this guidance to maintain sufficient cybersecurity posture.

Secure Your Supply Chain

Ensure effective risk management policies are in place to minimize the likelihood of damage resulting from a compromise.

- **Establish strong vendor risk management** processes to evaluate and monitor third-party risks, ensuring that suppliers and partners adhere to strict security standards and any foreign ownership, control, or influence (FOCI) are clearly identified and managed, including consideration of, for example, the U.S. Department of Commerce Entities List and Unverified List.
- **Ensure those responsible for procurement:**
    - **Exercise due diligence** when selecting software, devices, cloud service providers (CSPs), and managed service providers (MSPs).
        - **Use guidance including the secure by design principles to help inform vendor selection** to reduce the availability of attack pathways threat actors can leverage. Follow best practices for supply chain risk management and only source from reputable vendors.
        - **Ensure that the vendor has a patching plan** in place that supports your organization and that you can also support.

- **Identify and limit usage of any products** that break the principle of least privilege, do not clearly enumerate needed access, or require disabling antivirus tools.
- **Select vendors** that enable interoperability as a best practice for resilience and to avoid vendor lock-in.

As a leader, advocate for vendors to deliver secure and resilient systems and support staff efforts to integrate Secure by Design principles into procurement/vendor contracting processes, including mechanisms for ensuring compliance and patching. Additionally, direct software development teams to integrate the Secure Software Development Framework (SSDF) throughout your existing practices. Visit our webpage for more on Secure by Design.

Drive a Cybersecurity Culture

Ensure performance management outcomes are aligned to the cyber goals of the organization by:

- **Encouraging collaboration between IT, OT, cloud, cybersecurity, supply chain, and business units** to align security measures with business objectives and risk management strategies.
- **Championing organizational cybersecurity risk assessments and audits** to identify vulnerabilities and gaps in the security posture.
- **Engaging with external cybersecurity experts and advisors for independent assessments** and guidance tailored to your organization and performing GAP analysis on findings.
- **Increasing awareness of social engineering tactics** and facilitating a culture which encourages incident reporting.[5]

INCIDENT RESPONSE

If your organization is impacted by an incident or suspected incident:

- Implement your cyber incident response plan. See the joint cybersecurity advisory by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom on Technical Approaches to Uncovering and Remediating Malicious Activity for incident response best practices.
- Review and update your cyber incident response plans on a regular basis.
- Report incidents or anomalous activity immediately to an authoring agency (see the Contact Information section).
- Consider entering into a proactive retainer agreement with a reputable third-party cybersecurity organization to provide subject matter expertise and incident response services.

CONTACT INFORMATION

U.S. Organizations

- CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870 or your local FBI field office. 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. CISA provides timely situational awareness and enables coordination with Sector Risk Management Agencies such as EPA, TSA, and Treasury.
- For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
- Entities subject to regulatory requirements should follow established reporting requirements, as appropriate.

Australian Organizations

Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

[5] Avoiding Social Engineering and Phishing Attacks | CISA; Social engineering – ITSAP.00.166 - Canadian Centre for Cyber Security; https://www.cyber.gc.ca/en/guidance/how-protect-your-organization-insider-threats-itsap10003-0

Canadian Organizations

Report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand Organizations

Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom Organizations

Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

RESOURCES

- Refer to CISA's Logging Made Easy page for free centralized log management solutions.
- Refer to CISA's Cyber Essentials for additional recommendations on managing cybersecurity risks.
- See CCCS's Cyber Hygiene publication for best practices for your organization.
- See Questions Every CEO Should Ask About Cyber Risks for additional best practices to help companies understand their risks and prepare for cyber threats.
- See CISA Director Jen Easterly's opening statement on Volt Typhoon before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party.
- See CISA's Recommended Cybersecurity Best Practices for Industrial Control Systems for more guidance specific to organizations supporting U.S. critical infrastructure.
- See CISA's Cyber Resilience Review webpage for more information on CISA's no-cost, non-technical assessment to help organizations evaluate their operational resilience and cybersecurity practices.
- See CISA's Fact Sheet Rising Ransomware Threats to Operational Technology Assets for more information on reducing the vulnerability to severe business degradation if affected by malicious cyber activity. Although tailored to ransomware, the Fact Sheet has applicable guidance for other cyber threats.
- See EPA Cybersecurity for the Water Sector | US EPA for free cybersecurity assessments, training, funding and additional resources tailored to support drinking water and wastewater entities.

ACKNOWLEDGEMENTS

Cisco Talos, NTT Corporation, Google, Mandiant, and Sophos contributed to this fact sheet.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

TLP:CLEAR

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

JOINT GUIDANCE:

Identifying and Mitigating Living Off the Land Techniques

Publication: February 7, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Department of Energy
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE)
United Kingdom National Cyber Security Centre
New Zealand National Cyber Security Centre

TLP:CLEAR

Summary

This guide, authored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and the following agencies (hereafter referred to as the authoring agencies), provides information on common living off the land (LOTL) techniques and common gaps in cyber defense capabilities.

- U.S. Department of Energy (DOE)
- U.S. Environmental Protection Agency (EPA)
- U.S. Transportation Security Administration (TSA)
- Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- New Zealand National Cyber Security Centre (NCSC-NZ)

The joint guide for network defenders focuses on how to mitigate identified gaps and to detect and hunt for LOTL activity. The information in this joint guide is derived from a previously published joint advisory; incident response engagements undertaken by several of the authoring agencies; red team assessments by several of the authoring agencies using LOTL for undetected, persistent access; and collaborative efforts with industry.

The authoring agencies have observed cyber threat actors, including the People's Republic of China (PRC) [1],[2] and Russian Federation [3] state-sponsored actors, leveraging LOTL techniques to compromise and maintain persistent access to critical infrastructure organizations. The authoring agencies are releasing this joint guide for network defenders (including threat hunters) as the malicious use of LOTL techniques is increasingly emerging in the broader cyber threat environment.

Cyber threat actors leveraging LOTL abuse native tools and processes on systems, often using "living off the land binaries." They use LOTL in multiple IT environments, including on-premises, cloud, hybrid, Windows, Linux, and macOS environments. LOTL enables threat actors to conduct their operations discreetly as they can camouflage activity with typical system and network behavior, potentially circumventing basic endpoint security capabilities.

LOTL is particularly effective because:

- Many organizations lack effective security and network management practices (such as established baselines) that support detection of malicious LOTL activity—this makes it difficult for network defenders to discern legitimate behavior from malicious behavior and conduct behavioral analytics, anomaly detection, and proactive hunting.
- There is a general lack of conventional indicators of compromise (IOCs) associated with the activity, complicating network defenders' efforts to identify, track, and categorize malicious behavior.

- It enables cyber threat actors to avoid investing in developing and deploying custom tools.

Even for organizations adopting best practices, distinguishing malicious LOTL activity from legitimate behavior is challenging because network defenders often:

- Operate in silos separate from IT teams and their operational workflows;
- Rely predominantly on untuned endpoint detection and response (EDR) systems, which may not alert to LOTL activity, and discrete IOCs that attackers can alter or obfuscate to avoid detection;
- Maintain default logging configurations, which do not comprehensively log indicators of LOTL techniques or sufficiently detailed information to differentiate malicious activity from legitimate IT administrative activity; and
- Have difficulty in identifying a relatively small volume of malicious activity within large volumes of log data.

The authoring agencies strongly urge critical infrastructure organizations to apply the following *prioritized* best practices and detection guidance to hunt for potential LOTL activity. These recommendations are part of a multifaceted cybersecurity strategy that enables effective data correlation and analysis. There is no foolproof solution to fully prevent or detect LOTL activity, but by applying these best practices organizations can best position themselves for more effective detection and mitigation.

Detection Best Practices:

1. Implement detailed logging and aggregate logs in an out-of-band, centralized location that is write-once, read-many to avoid the risk of attackers modifying or erasing logs.
2. Establish and continuously maintain baselines of network, user, administrative, and application activity and least privilege restrictions.
3. Build or acquire automation (such as machine learning models) to continually review all logs to compare current activities against established behavioral baselines and alert on specified anomalies.
4. Reduce alert noise by fine-tuning via priority (urgency and severity) and continuously review detections based on trending activity.
5. Leverage user and entity behavior analytics (UEBA).

Hardening Best Practices:

1. Apply and consult vendor-recommended guidance for security hardening.
2. Implement application allowlisting and monitor use of common LOLBins.
3. Enhance IT and OT network segmentation and monitoring.
4. Implement authentication and authorization controls for all human-to-software and software-to-software interactions regardless of network location.

For details and additional recommendations, see the Best Practice Recommendations and Detection and Hunting Recommendations sections. If LOTL activity is identified, defenders

should report the activity to the relevant agencies, as applicable, and apply the remediation guidance in this guide.

Additionally, this guide provides recommendations for software manufacturers to reduce the prevalence of exploitable flaws in software that enable LOTL. In many cases, software defects or unsecure default configurations allow cyber threat actors to carry out malicious cyber activity using LOTL techniques. The authoring agencies strongly encourage software manufacturers to take ownership of their customers' security outcomes by applying the secure by design recommendations in this guide and in CISA's joint secure by design guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.

Technology manufacturers can reduce the effectiveness of LOTL techniques by producing products that are secure by design, including by:

- Disabling or removing unnecessary protocols by default.
- Limiting network reachability to the extent feasible.
- Limiting processes and programs running with elevated privileges.
- Enabling phishing-resistant MFA as a default feature.
- Providing high-quality secure logging at no additional charge beyond processing and storage costs.
- Eliminating default passwords and credentials when installing software.
- Limiting or removing dynamic code execution.

Table of Contents

Introduction

The authoring agencies are releasing this joint guide to warn network defenders that cyber threat actors, including PRC [1],[2] and Russian Federation [3] state-sponsored actors, are leveraging living off the land (LOTL) techniques to compromise and maintain persistence in critical infrastructure organizations.

This guide provides information for network defenders—including threat hunters—on LOTL, network defense weaknesses that enable actors to use LOTL undetected, and detection guidance. The information and guidance are derived from:

- A previously published joint advisory.
- Authoring agency incident response engagements, including a recent CISA incident response engagement where cyber threat actors had persistent, long-term access to the victim's environment and compromised the domain controller (DC). The actors used LOTL techniques throughout the intrusion.
- Authoring agency red team assessments, including CISA red team assessments of Federal Civilian Executive Branch (FCEB) networks and, upon the request of the network owner, of non-federal networks. (CISA's red teams frequently use publicly known LOTL techniques for execution, persistence, lateral movement, discovery, and credential access with network defenders rarely detecting their activity.)
- Collaborative efforts with interagency and industry experts in cybersecurity and incident response.

Living off the Land

LOTL involves the abuse of native tools and processes on systems, especially living off the land binaries, often referred to as LOLBins, to blend in with normal system activities and operate discreetly with a lower likelihood of being detected or blocked because these tools are already deployed and trusted in the environment. Cyber threat actors effectively use LOTL across multiple environments, including in on-premises, cloud, hybrid, Windows, Linux, and macOS environments, in part because it enables the ability to avoid investing in the development and deployment of custom tools.

Authoring agency incident response teams predominantly observe cyber threat actors leverage LOTL in Windows environments due to the operating system's widespread use in corporate and enterprise settings. In Windows environments, cyber threat actors use native tools, services, and features, relying on the fact that these components are ubiquitous and generally trusted.

In macOS environments, LOTL is also referred to as "living off the orchard." Malicious actors exploit native scripting environments, built-in tools, system configurations, and binaries referred to as "LOOBins." In hybrid environments, cyber threat actors are increasingly

exploiting both physical and cloud-based systems by leveraging sophisticated LOTL techniques. See Appendix A: LOTL in macOS and Hybrid for more information on LOOBins.

For more information on LOLBins known to be used maliciously, see Appendix C: Known LOLBins Used Maliciously and the following resources:

- LOLBAS project's GitHub repository Living Off The Land Binaries, Scripts and Libraries.
- For a list of Unix binaries that can be used in LOTL, see gtfobins.github.io.
- For a list of macOS LOLBins that can be used in LOTL, see loobins.io.
- For a list of Windows Living Off the Land Drivers, see loldrivers.io.

In addition to LOLBins, cyber threat actors similarly use third-party remote access software, e.g., remote monitoring and management, endpoint configuration management, EDR, patch management, mobile device management systems, and database management tools. These tools, some of which are meant to administer and protect domains, come with a built-in functionality that can run commands on all client hosts in the network, including sensitive hosts like domain controllers. By necessity, these tools have high privileges necessary for target system administration. See Appendix B: Third-Party Tools for LOTL for more information.

Network Defense Weaknesses

LOTL is an effective technique because many organizations do not implement security best practice capabilities that support detection of malicious activity. CISA's red teams frequently leverage LOTL for undetected, persistent access. These red team assessments demonstrate how an adversary could achieve full domain compromise with little to no investment in tooling. In many of these instances, CISA's red teams found that the assessed organization lacked security baselines, allowing LOLBins to execute and leaving analysts unable to identify anomalous activity. In other cases, organizations did not appropriately tune their detection tools to reduce alert noise, leading to an unmanageable level of alerts to sift through and action. Automated systems such as ongoing management functions using service accounts and vulnerability scanners frequently perform highly privileged, possibly suspicious actions that drown analysts in log events if not appropriately categorized.

Even in cases where organizations with more mature cyber postures have applied best practices, distinguishing malicious LOTL activity from legitimate behavior is challenging because LOTL allows actors to blend in with normal system and network activities.

- LOLBins are used legitimately by IT administrators, and, as such, have trusted attributes (such as file hashes or digital signatures). This can mislead network defenders into thinking they are safe for all users. System administrators should identify responsible and permitted usage of LOLBins and enforce that as policy.
- A common misconception is that because a program is a legitimate IT administrative tool, it is safe to allow globally. Blanket "allow" policies for common LOLBins expand

the attack surface. System administrators should restrict “allow” policies, limit log on usage and attempted usage, and create alerts for behaviors that deviate from allowed usage.

- For example, CISA’s red teams often find LOLBins accessible to all users, even standard users. CISA’s red teams also encounter overly broad exceptions for the PsExec tool because administrators regularly use it for their job duties. Malicious actors often leverage the lack of restrictions to move laterally without detection.

This issue is exacerbated by insufficient defensive postures and detection capabilities. In many cases, authoring agency red teams and incident response teams frequently find that network defenders:

- Operate in silos that separate security practitioners from IT teams and their operational workflows.
  - By operating in silos, network defenders are unable to create a baseline of user behavior (normal and privileged).
  - Lack of open communication and collaboration mechanisms between security practitioners and IT teams also increases time to remediate vulnerabilities or investigate abnormal behavior. In large organizations, investigations may take several months, during which cyber threat actors expand their access.
  - Silos may also negatively affect business-based (resource) decisions; for example, CISA’s red teams has observed leaders making decisions based on business risk due to legacy systems or insecure software without sufficient consideration of assessments presented by their own security teams. This can lead to easily exploitable systems remaining on the assessed network.
- Rely predominantly on untuned EDR systems and discrete IOCs.
  - LOTL may avoid triggering EDR products. EDR vendors may assume that LOLBins are "safe” or administrators worried about EDR blocking their tools request standard configurations to allow LOLBins.
  - Threat actors can easily modify known IOCs, such as filenames and command line arguments, or modify content to change the hash. Cyber threat actors bypass conventional, “known-bad" detections by modifying common IOCs such as filenames, file paths, and command and control destinations. State-sponsored actors exploit alternative syntax in command line arguments or command line arguments using environment variables.[1] For example, `ntdsutil snapshot “activate instance ntds” create quit quit` is also effective when it is shorted to `ntdsutil snapshot “ac i ntds” create quit quit`.
- Maintain default logging configurations that lack nuanced, extensive, and centralized logging.
  - Default logging configurations will not capture all activity. Every network is unique with regards to benign activity and files. Relying on default configurations and vendor assurances is never enough to fully defend networks. Regular testing and

validation of active configurations is essential to proactive defense. In addition, legacy systems or specialty software (such as Unix-based hosts and infrastructure devices such as routers) rarely come with advanced logging functionality.
    - Many applications, even when properly configured, produce logs that require additional processing before they can be useful to network defenders.
    - Some vendor-provided logs are only available to customer organizations at an extra charge. Unfortunately, some malicious activity can only be identified via "enhanced" logging (see joint CSA Enhanced Monitoring to Detect APT Activity Targeting Outlook Online). Organizations who do not pay for enhanced logging may, therefore, be unable to detect certain malicious activity. Note: In line with Secure by Design principles, CISA strongly urges software manufacturers to view enhanced logging, beyond actual processing and storage costs, as a basic necessity for network security and include it in all service levels. This way all organizations, particularly those least resourced, can detect and respond to intrusions. See the Secure by Design section for more information.
- Have broad allowlisting policies for internet protocol (IP) address ranges owned by hosting and cloud providers.
    - It is important to consider that these IP ranges are accessible to any organization renting IP space from the vendor, including malicious actors. Identify and prioritize essential IP ranges for organizational operations, apply selective restrictions on others, and routinely review and update allowlists for adaptability and security against emerging threats. Monitor network traffic patterns to identify deviations from normal activity.

Network defenders should ensure adequate protections are in place for macOS devices; there are often misconceptions about the inherent security of macOS.

- macOS lacks standardized and widely promoted system hardening guidance compared to other operating systems. This lack of emphasis on hardening practices can lead to macOS systems being deployed with default settings, which may not be optimized for security. Cyber professionals often overlook the need for comprehensive hardening guidelines that address macOS-specific security configurations and best practices. For additional guidance, see NCSC-UK's Device Security Guidance and GitHub's macOS Security Compliance Project.
- There is a prevalent belief that macOS devices are 'safe' due to their design and built-in security features. This presumption of safety can lead to underestimating the potential risks and vulnerabilities associated with macOS. As a result, security measures that are standard in other environments, such as regular security assessments, high-fidelity logs, and application allowlisting, might be deprioritized or ignored in macOS environments.
- In mixed-OS environments, it is common for Windows devices to outnumber the macOS devices. This dynamic can cause system administrators to prioritize Windows

over macOS when hunting threats. IT and security teams tend to overlook or pay less attention to macOS due to its lower representation in some environments, potentially leaving these systems more vulnerable to intrusions.

These factors often contribute to a complacency in devoting adequate resources for the security management of macOS devices. This includes allocating budget and time for implementing advanced security measures like EDR and investing in security tools specific to macOS.

Best Practice Recommendations

LOTL detection requires organizations undertake contextual analyses of multiple data sources to identify command executions, file interactions, privilege escalations, and other network activities that differ from normal administrative actions. Implementing these recommendations depends on each organization's risk landscape and resource capabilities. However, establishing and maintaining an infrastructure that collects and organizes data for defenders is essential for detecting LOTL techniques.

> These recommendations are not foolproof but are part of a multi-faceted and comprehensive approach to mitigating LOTL cyber threats.
>
> Although prioritized, organizations should implement as many as possible because their effectiveness lies in their combined implementation, which will enable effective data correlation and analysis.

The authoring agencies strongly encourage network defenders implement the following *prioritized detection and hardening* recommendations to enable behavior analytics, anomaly detection, and proactive hunting.

Detection

1. **Implement comprehensive (i.e., large coverage) and verbose (i.e., detailed) logging and aggregate logs** in an out-of-band, centralized location where adversaries cannot tamper with them, to enable behavior analytics, anomaly detection, and proactive hunting. In addition, implementing centralized logging allows defenders to maintain longer log histories.
    a. **Enable comprehensive logging for all security-related events**, including shell activities, system calls, and audit trails on all platforms. Additionally, defenders should prioritize logs and data sources that are more likely to detect malicious LOTL activity and tools. **Note:** Default logging configurations rarely capture all needed events. This may require purchasing enhanced logging capabilities because some malicious activity can only be identified via enhanced logging. As part of CISA's Secure by Design campaign, CISA urges software manufacturers to provide high-quality audit logs to customers at no extra charge or provide logs that do not require customers to make additional configurations. See the Secure by Design section of this guide for more information. For additional recommendations on log management, see NIST SP 800-92 Rev. 1: Cybersecurity Log Management Planning Guide.
        i. For cloud environments:
            1) Ensure that logging is enabled for all control plane operations, including API calls and end user logins, through services like Amazon Web Services CloudTrail, Azure Activity Log, and Google Cloud Audit Logs. Configure

these logs to capture read and write activities, administrative changes, and authentication logs.

2) Configure logging policies for all cloud services available in the organization's environment, even if they are not actively being used. Cyber threat actors may take advantage of unused services or regions that are not actively monitored to avoid detection.

b. **Enable verbose logging for security-related events,** including command lines, PowerShell activity, and WMI event tracing to gain visibility into tool usage within the environment. Additionally, EDR may be able to collect and centralize logs.
   i. For Microsoft environments, **enable specific Microsoft server roles that have optional advanced logging features**, such as advanced Microsoft IIS event logging. These features can help identify and may be required to detect certain attack vectors. For example, IIS module web shells can be difficult to detect if these logs are not enabled. For more information, see Microsoft's IIS modules: The evolution of web shells and how to detect them.
   ii. For cloud-specific configurations, **enable detailed logging for network gateways and load balancers to track ingress and egress traffic**, and configure log exports from cloud storage services to a SIEM or centralized logging server like Amazon S3 CloudTrail data events (or S3 access logs) or Azure Blob Storage logging to monitor data access patterns.
   iii. For macOS systems, **enable verbose logging for Terminal commands**, AppleScript activities, and access to key binaries like `curl`, `osascript`, and `launchctl`.

c. **Consider using security information and event management solution (SIEM) tools** for log aggregation and management. SIEM tools collect event log data from a range of sources, facilitating network defenders with the ability to identify activity that deviates from baselines. Log aggregation is critical because some cyber threat actors are known to clear or modify local system event logs. Additionally, the majority of network infrastructure devices available on the market today have traditionally limited, local storage capabilities. Implementing centralized logging can ensure that the logs do not roll over as quickly, affording network defenders a decently maintainable log history that can be correlated across logged events from multiple systems.

d. **Regularly audit log integrity and alerting efficiency.** Routinely verify that events are correctly logged, securely relayed to a centralized repository, and reliably trigger alerts. This is critical, as software and firmware updates, configuration adjustments, or system alterations can affect event logging and forwarding. This can potentially undermine log accuracy and alert efficacy.

2. **Establish and continuously maintain a baseline of installed tools and software**, account behavior, and network traffic. This way, network defenders can identify potential outliers, which may indicate malicious activity.

a. Leverage **the aggregated logs/SIEM** to baseline account behavior, normally used tools, service meshes, network traffic, system intercommunications, and other items as applicable.
b. **Enhance network monitoring, log retention, and threat hunting to identify prolonged adversary presence.** Extending log storage, fine-tuning anomaly detection, and deepening threat hunting tactics can help uncover threat actors leveraging LOTL techniques over immediate and extended dwell periods.
c. **Select a minimal subset of administrative tools to use in the network**, configure them with extensive logging, and block or alert on all others. Apply corresponding restrictions to network logons. This reduces the ambient noise that defenders must sift through and provides more detail for observed behavior.
d. **Clearly baseline the behavior of privileged accounts.** Establish what tools admins typically use, the commands they execute, their active timeframes, and the specific devices they interact with. Modify network logon policies to limit unnecessary access paths based on this well-defined profile of legitimate activity. Behavioral baselines should also include the sequence of use. For example, there is typically a default series of applications that run when a user logs on. However, the sequence of applications at other times of day may indicate suspicious activity depending on the baseline, especially if apps are calling to other apps.
    i. **Use Privileged Access Workstations (PAWs)** for administrative accounts and mandate use for administrative functions. In Windows environments, at minimum, use PAWs for Active Directory (AD) administrators first. For more information, see Microsoft's Securing Device as Part of the Privileged Access Story.
e. **Clearly define the behavior of automated tools and systems** (e.g., applications and services using service accounts and network scanners). Their usage should be predictably bounded by time of day, source/destination hosts, and user account(s) that can be affected by an automated service. These accounts are targets for threat actors because they frequently have additional, unnecessary privileges and do not utilize multi-factor authentication (MFA).
f. **Create an inventory of existing configurations, policies, and installed software** on each host. If the host does not require a specific piece of software, uninstall it to limit the tools available to cyber threat actors. EDR tools are uniquely suited to this role.
g. **Place additional scrutiny on at-risk hosts**, such as public-facing servers in a DMZ. Cyber threat actors who obtain an initial foothold through exploitation of internet-facing services frequently rely on LOLBins for initial execution, reconnaissance, and deployment of secondary payloads.
h. **Track and record what infrastructure has been swept**, if there are any open issues, and continuously log what is considered high-risk to proactively prioritize efforts.

i. **Establish a baseline for LOLBins and monitor changes.** Understand which LOLBins attackers are abusing and understand the specifics of normal use of those binaries in the environment. For example, a particular LOLBin may be used, but always with a specific command-line or user. Assess whether alerts can be created if those LOLBins are used outside of the baseline and investigate observed executions.

j. For cloud environments:
   i. **Architect cloud environments to ensure proper separation of enclaves** using subnet or security group tools. This may enable additional logs within the environment and provide more insight. Ensure backups of environment to include infrastructure as code are in place. This can be used to compare changes to environment.

3. **Use automation to continually review all logs and increase the efficiency of hunting activities.** Compare current activities against established behavioral baselines, paying particular attention to privileged accounts and critical assets like domain controllers. As new strategies for hunting are identified, leverage automation and ensure staff are properly trained on its use.
   a. In Linux environments, **regularly audit `cron jobs` and `systemd` timers for unexpected entries**. Implementing file integrity monitoring on critical configuration files such as `/etc/crontab`, `/etc/cron.*/*`, and `systemd` unit files may alert defenders to unauthorized modifications. Look for unexpected or unfamiliar entries, especially those invoking scripts or binaries not part of standard system maintenance tasks.
   b. For macOS, **conduct routine checks of PLIST files and macOS scheduled tasks** (using `launchd`). Look for unauthorized or modified entries that could indicate persistence mechanisms.
   c. For Windows, regularly audit the Windows Registry for changes to auto-start locations, such as `Run` and `RunOnce` keys, and other areas often used for persistence. Implement file integrity monitoring on these keys. Additionally, create detections for scheduled tasks that run at unusual times, execute uncommon scripts or binaries, or have been recently modified without authorization.
   d. In cloud environments, **monitor for unusual API calls**, especially those involving changes to security groups, configuration of cloud resources, or access to sensitive data. This can be done using cloud-native tools.
      i. **Investigate any unusual account behavior**, such as out-of-hours logins, concurrent sign-ins from geographically disparate locations, and internal network enumeration.
   e. **Consider leveraging machine learning based anomaly detection capabilities** within cloud provider security services for enhanced log analysis. These services process log data from multiple sources in real time beyond the scope of traditional methods, employing machine learning to detect anomalous patterns

and behaviors indicative of malicious activity. Focus on irregular API call patterns, unusual cloud storage access, and atypical network traffic.

4. **Reduce alert noise.** Refine monitoring tools and alerting mechanisms to differentiate between typical administrative actions and potential threat behavior. Additionally, correlate remote authentication activities to identify anomalies and outliers, thus focusing on alerts that most likely indicate suspicious activities.
   a. **Avoid overly broad detection rules** such as `CommandLine=*` or `Filepath=C:\...\*`. This applies to inclusion and exclusion rules.
   b. **Coordinate with IT teams to reduce the prevalence of allowed administrative tools and logon types available in the network.** Consider the host, its intended purpose, and the user associated with the activity. For example, a typical business user will never open a command prompt or run ipconfig. A backend server, administered via secure shell (SSH) or a hypertext transfer protocol (HTTPS) interface, should not need RDP enabled. User accounts with domain administrator privileges should never log into anything except domain controllers.
   c. Disable and alert on the installation and use of remote access tools that your organization does not require.
   d. **Consider implementing a threat detection maturity model** to develop, implement, test, and tune alerting mechanisms enabled within network and host intrusion detection systems or SIEM. Consider implementing a standardized naming convention for alerts that includes the alert maturity level and MITRE ATT&CK phase to allow faster incident response triage. As alerts are tuned, their maturity should be updated to reflect the stability of the rule ultimately building reliable robust detections.
5. **Leverage user and entity behavior analytics (UEBA)** to analyze and correlate activities across multiple data sources, to identify potential security incidents that may be missed by traditional tools, and to profile and monitor user behavior, detecting insider threats or compromised accounts.

Hardening

1. Apply hardening guidance.
   a. **Strengthen software and system configurations** based on vendor-provided or industry, sector, or government (e.g., U.S. National Institute of Standards and Technology [NIST]) hardening guidance to reduce the attack surface. Do not rely on default configurations for software and devices that may be insecure. Note: As part of CISA's Secure by Design campaign, CISA urges software manufacturers to prioritize secure by default configurations to eliminate the need for customer implementation of hardening guidelines. See the Secure by Design section of this guide for more information.

i. For Windows, **apply security updates and patches provided by Microsoft**. For comprehensive hardening guidelines, follow Microsoft's Windows Security Baselines Guide or CIS Benchmarks. Harden services that are often targets of exploitation, like SMB and RDP, and disable any superfluous services and features.
ii. In Linux systems, **check what binary permissions are set to**. See CIS's Red Hat Enterprise Linux Benchmarks.
iii. For macOS, **regularly update to the latest version and apply all security patches**. Use macOS's built-in security features, including Gatekeeper, XProtect, and FileVault. Adhere to the guidelines set forth by GitHub's macOS Security Compliance Project. Implement application allowlisting and leverage the built-in firewall to control network access.
iv. Organizations with Microsoft cloud infrastructure, see CISA's Microsoft 365 security configuration baseline guides, which provide minimum viable secure configuration baselines for Microsoft Defender for Office 365, Azure Active Directory, Exchange Online, OneDrive for Business, Power BI, Power Platform, SharePoint Online, and Teams. For additional guidance, see the Australian Signals Directorate's Blueprint for Secure Cloud.
v. Organizations with Google cloud infrastructure, see CISA's Google Workspace security configuration baseline guides, which provide minimum viable secure configuration baselines for Groups for Business, Gmail, Google Calendar, Google Chat, Google Common Controls, Google Classroom, Google Drive and Docs, Google Meet, and Google Sites.

b. **Adopt** hardening **measures that are universally applicable**, such as minimizing running services, applying principles of least privilege, and securing network communications. For additional recommendations, see CISA's Cross-Sector Cybersecurity Performance Goals.
c. **Secure critical assets** by applying vendor hardening measures. For example, for Microsoft Tier 0/critical assets, such as Active Directory Federation Services (ADFS) and Active Directory Certificate Services (ADCS), apply guidance from Microsoft's Security Documentation: Enterprise Access Model. Critical assets include cross-platform infrastructure components like identity providers, directory services, mobile device management (MDM), and cloud management consoles. Securing these assets means not only hardening their configurations, but also limiting the applications and services that can be used or accessed by them. This will reduce their exposure and place stringent restrictions on all accounts that have administrative access to the assets.
d. **Use administrative tools that do not cache credentials on the remote host.** If a threat actor compromises a host with cached credentials, the actor can often find and reuse those credentials to gain access to other hosts and services.

2. **Implement application allowlisting** to constrain the execution environment and configure allowlisting for business roles. This strategy channels all user and administrative activity through a narrow path that is easier to monitor, enhancing the effectiveness of behavioral analytics and reducing the volume of alerts to those that are most pertinent. For additional recommendations, see CISA's Technical Approaches to Uncovering and Remediating Malicious Activity.
    a. For macOS, configure Gatekeeper settings to prevent the execution of unsigned or unauthorized applications and monitor for attempts to bypass these settings.
    b. For Windows, **employ AppLocker and Windows Defender Application Control for robust application allowlisting**. These mechanisms facilitate stringent regulation of executable files, scripts, MSI files, DLLs, and packaged app formats. Administrators can enforce security policies by crafting rules centered on file attributes like name, version, publisher, and path.
3. **Enhance network segmentation and monitoring** to limit lateral movement possibilities for threat actors. Abnormal network behavior may indicate the presence of a threat actor that evaded host-based detections, possibly via LOTL techniques. Properly implementing and managing network segmentation ensures that users only have access to the minimum number of applications and services to perform their daily duties. When a cyber threat actor compromises legitimate credentials, having appropriate network segmentation limits the "blast radius" of accessible systems.
    a. **Use network traffic analysis tools to monitor inter-segment traffic**, focusing on unusual patterns or communications to sensitive segments.
    b. **Strategically place network sensors and network traffic parsers** at critical points in the network infrastructure, such as intersections between different network segments, external gateways/virtual private networks (VPNs), and demilitarized zones (DMZs). Ensure these sensors have deep packet inspection capabilities to facilitate comprehensive traffic analysis.
    c. **Employ network traffic metadata parsers** (e.g. Zeek, [formerly Bro]) for efficient parsing and analysis of network traffic, enabling the identification of suspicious patterns and anomalies indicative of LOTL activities. Also, consider integrating open source network intrusion detection systems (NIDS) (e.g. Snort, Suricata) to improve LOTL threat detection.
    Note: As a longer-term strategy, the authoring agencies strongly recommend organizations implement zero trust architectures. Implementing zero trust principles will ensure that binaries, and the accounts that use them, not automatically trusted. Additionally, their use should be restricted and examined to confirm trustworthy behavior. For more information, see CISA's Zero Trust Maturity Model.
4. Implement authentication controls:
    a. Enforce phishing-resistant multi-factor authentication (MFA) across all systems, especially for privileged accounts.

b. **Deploy a robust privileged access management (PAM) solution** with just-in-time access, restricting elevated access to specific needs and timeframes. Utilize time-based PAM controls, including time-of-day and day-based access, and complement with role-based access control (RBAC) for tailored access based on job requirements. This ensures that elevated access is granted only when required and for a limited duration, minimizing the window of opportunity for abuse or exploitation of privileged credentials.
c. For cloud environments, **enforce strict identity and credential access management (ICAM) policies**, ensuring minimal privileges for each user and service account. Regularly audit ICAM configurations for overly permissive roles and rectify them. Additionally, consider creating RBAC IDs with associated cloud master IDs and securely storing these offline. Ensure access keys are rotated or have expiration dates.
d. For macOS and Unix, **regularly review the `sudoers` file for misconfigurations** that might allow privilege escalation. Ensure it adheres to the principle of least privilege.

Additionally, the authoring agencies recommend network defenders apply the following to better position themselves to mitigate LOTL techniques:

- **Exercise due diligence** when selecting software, devices, cloud service providers, and managed service providers. Select vendors with secure by design principles in place to reduce the availability of LOLBins that threat actors can leverage.
  - Hold vendors accountable for their software's default configurations and requirements. Be wary of products that break the principle of least privilege, do not clearly enumerate needed access (e.g., overly broad firewall rules rather than specific TCP ports), or require disabling antivirus tools.
  - Follow best practices for supply chain risk management and only source from reputable vendors.
- **Audit remote access software and their configurations** on devices on your network to identify currently used and/or authorized remote access software.
  - Consider reducing remote access software on systems by choosing one solution and a backup solution. This will help network defenders identify potential anomalous activity; for example, if there is activity from unapproved remote access solutions.
  - Apply best practices for remote access software from the joint Guide to Securing Remote Access Software.
- **Limit exposure of defensive configurations.** Malicious actors may read defensive configurations and adjust their tradecraft if the information is available. For example, Sysmon rules—what is or is not being logged—are available by default in a globally readable registry key and can be parsed with Sysmon.exe.

    - Audit attempts to read the configuration, disable the monitoring software, or tamper with log artifacts.
- Restrict outbound internet connectivity.
    - Back-end servers (especially databases, domain controllers, etc.) do not need internet access. Restricting it, by default, prevents many initial payloads—especially those used in supply chain compromises.
        - For servers or applications that require internet egress, restrict and monitor outbound connectivity to only essential egress destinations.
    - Many essential services, including EDR, are now cloud-connected. Ensure that services have what they need but do not provide overly broad access (e.g., allow certain domains/IPs needed for services rather than allowlisting the entire service provider).
    - Look for raw connections to IP addresses without corresponding DNS requests.

Detection and Hunting Recommendations

General

The authoring agencies strongly recommend network defenders routinely review and compare the behavior of automated tools and systems, configurations, and software installed on hosts, logs, and other items in their baseline to identify potential malicious activity. These recommendations are not foolproof, instead they are guidelines for how to use logs as part of a multifaceted approach.

Application, Security, and System Event Logs

Review application, security, and system event logs, focusing on Windows Extensible Storage Engine Technology (ESENT) Application Logs. Certain ESENT Application Log event IDs (`216`, `325`, `326`, and `327`) may indicate actors copying `NTDS.dit`. See joint advisory PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure for more information, including examples of ESENT and other key log indicators that should be investigated.

Network Logs

LOTL network artifacts are significantly harder to detect and capture than host artifacts. Network defenders can find host artifacts, unless the threat actor deletes them, without making configuration changes to the system. However, network artifacts require that network defenders configure and setup logs appropriately for detection. Additionally, network artifacts for LOTL activity are largely transient because they are derived from network traffic. If there are no sensors in place to capture the traffic, then there will be no way to see the LOTL activity from a network perspective.

There is rarely a single indicator of LOTL activity, presenting one of many challenges encountered when attempting to detect this activity as it occurs. Rather, it is a collection of possible indicators that paints a bigger picture of the behavior of network traffic.

Some ways of discovering potential LOTL activity and their indicators may include the following:

- Review blocked access attempts in firewall logs. In a properly segmented network, denied (disallowed) traffic can be an indicator of compromise. Network discovery and mapping attempts (especially from inside of the network originating from one or more hosts) may also be an indicator. Care should be taken to ensure that this is not normal behavior associated with many different network management tools. Rather than defining thresholds of behavior, any abnormal traffic, such as the following, should be investigated.
  - LDAP requests to a DC from non-domain joined Linux hosts in separate enclaves.
  - SMB requests across geographic sites or logical network segments, such as a user accessing fileservers unrelated to their work role.
  - Database access requests from a user workstation to a backend database server. Only the frontend server should be talking to the database server.

If legitimate applications are making those requests, consider factoring that into your baseline noise levels.

- In addition to logs from dedicated network devices, examine logs from services like Sysmon, IIS, and other network services on host machines. These logs can provide insight into web server interactions, file transfer protocol (FTP) transactions, and other network activities managed by the host. Aligning this data with network device logs can reveal discrepancies or anomalies indicative of malicious network behavior, such as unusual external access attempts or data exfiltration activities. It is important to remember that network-focused logs on host machines can offer valuable context and details not captured by traditional network devices.
- Combine network traffic logs with host-based logs to include additional information, such as user account and process. Compare the destination with on-network artifacts as mismatched information could indicate malicious traffic. For example:
  - Traffic through port `88`. Few processes (such as `lsass.exe`) should be talking to Kerberos via port `88`.
  - Remote access traffic, such as RMM update service, going to an unrelated, but legitimate appearing site.

Authentication Logs

- **Adopt a robust strategy for separation of privileges**, which is crucial for identifying LOTL techniques through authentication logs. Restrict domain administrator accounts so they can only log into domain controllers, thereby minimizing credential

exposure and risk of compromise. For other administrative roles, utilize PAWs in conjunction with bastion hosts as controlled and predictable jump points to enforce standardized login procedures. These bastion hosts, in tandem with PAWs, are especially critical in industrial control system (ICS) environments. They serve as secure, monitored gateways that reinforce network segmentation by allowing access to critical devices solely from designated network zones. Implement multifactor authentication as an added layer of protection.

- **Compare the activity with normal user behavior**. Unusual behaviors include odd login hours, access that conflicts with expected work schedules or planned holiday breaks, rapid succession or high volume of access attempts followed by a successful login, unusual access paths, concurrent sign-ins from multiple geographic locations, and instances of impossible time travel.

Sysmon/Host-based Logs

- Use established baselines of running tools and activity to identify abnormal or potentially malicious behavior.
- Rely on privileged (more secure) logs that are less likely to be tampered with by an adversary during initial exploitation. For example, Linux `.bash_history` files can be modified by nonprivileged users, but system-level `auditd` logs would be inaccessible.
- In Windows environments, Sysmon logs provide visibility into system activities, offering a detailed record of process creations, network connections, registry modifications, cryptographic hashes, and more. This granular information empowers security teams to hunt for and detect malicious use of legitimate tools and system utilities. For more information, see Microsoft's Sysmon's Configuration Guidance.
- For most Microsoft utilities, use `OriginalFileName` to identify renamed files, for example `net.exe` to `net2.exe`, which may indicate malicious activity (for most utilities, the original file names are in the PE header with the on-disk filename).
- Implement detection techniques in Windows environments to identify malicious use of command-line and scripting utilities, particularly those leveraging Alternate Data Streams (ADS). Configure Sysmon to log command-line activity with a focus on detecting commands that indicate ADS exploitation. This involves monitoring for specific command-line arguments or syntax used to interact with ADS, such as the use of `>` or `:` operators in `cmd.exe` or PowerShell scripts. For example, look for patterns like `type file.txt > file.txt:hidden.exe` or PowerShell `-command "&{Get-Content file.txt -Stream hidden}"`. These patterns are indicative of attempts to execute or interact with hidden payloads within New Technology File System (NTFS) streams.
- Develop targeted detection strategies for high obfuscation techniques in command-line interfaces (CLI) and scripting utilities, such as `cmd.exe`, in Windows environments. Enhance Sysmon configurations to log and scrutinize command-line

executions, paying special attention to patterns indicative of obfuscation. This includes detecting extensive use of escape characters, concatenation of commands, excessive use of environment variables, or the employment of Base64 encoding. For instance, monitor for `cmd.exe` executions containing unusual sequences like `^`, `%%`, or `&`, or PowerShell commands encoded in Base64, as in `powershell.exe -EncodedCommand [Base64String]`. Such obfuscation methods are often used by cyber threat actors to bypass security monitoring tools and execute malicious payloads without detection. Integrate these Sysmon logs with analytics in SIEM systems to automate the detection process.

- Monitor for suspicious process chains, such as Microsoft Office documents initiating scripting processes. Focus on tracking process creations, especially when Office applications like Word or Excel spawn `cmd.exe`, PowerShell, `wscript.exe`, or `cscript.exe`. This is a red flag, as it is uncommon for these applications to launch such scripting processes. Additionally, pay attention to these processes if they begin to execute unusual commands (e.g., whoami, net, and query, which are atypical for regular Office operations). The isolated execution of these commands might not signal an alert, but their launch from an Office application is anomalous and warrants investigation. Establish baselines for normal parent-child process activities to effectively spot deviations. Integrating Sysmon logs with SIEM systems, and applying correlation rules, helps pinpoint advanced attack scenarios involving Office applications as conduits for script-based exploitation and reconnaissance.
- Compare user account and normal behavior. Normal, non-technical users will typically never open a command prompt and run ipconfig. A compromised user account, on the other hand, might.
- On Linux machines, enable `Auditd` or Sysmon for Linux logging and send the logs to an SIEM platform—this can greatly improve an organization's ability to identify anomalous activity. `Auditd` logging is easily customizable, giving organizations the ability to monitor for specific commands, command syntax, or file/directory changes. Configuring alerting for unapproved changes or uncommon commands helps to identify potentially malicious activity. Pay special attention to unexpected process trees, such as a text editor like Vim or Gedit initiating network tools like `curl` or SSH. Use tools like SELinux or AppArmor for additional monitoring and enforcement of standard application behavior.
- For macOS, utilize tools like Santa, an open source binary authorization system, to monitor process executions. Focus on detecting abnormal spawning of processes by applications typically used for productivity, such as Pages or Numbers, which might initiate scripting utilities like bash, zsh, or Python. Monitor for executions of uncommon shell commands or scripts from these applications, as this behavior is rare in standard operations.

Review Configurations

- Review existing host configurations against a known baseline of installed software and expected behavior. This can catch IOCs that may not get reverted through regular group policy updates, such as installed software, firewall changes, or updates to core files (e.g., Hosts file that helps with DNS resolution).
  - Cyber threat actors can bypass standard event logs for registering services and scheduled tasks purely by writing to the registry since this does not create standard system events. See Scheduled Task Tampering | WithSecure™ Labs for more information.
- Regular system inventory audits can catch adversary behavior that event logs missed, either because the wrong events were captured, or the activity happened before logging changes were deployed.

Tailored Detection Examples

Understanding the context of LOTL activities is crucial for accurate detection and response, so this section includes tailored detection guidance from real-word examples—specifically `ntdsutil.exe` and `psexec.exe`, which are frequently used by state-sponsored advanced persistent threat (APT) actors in compromised environments. The authoring agencies strongly recommend network defenders apply the following guidance to detect potential use of these LOLBins.

NTDSUtil.exe

Given `ntdsutil.exe`'s ability to create snapshots of the Active Directory database, `ntdsutil.exe` is a priority target in LOTL tactics due to the access it provides to sensitive user data and system configurations.

A hallmark TTP used by a state-sponsored APT group includes creating a volume shadow copy followed by the dumping of the `ntds.dit` file, involving both `vssadmin.exe` and `ntdsutil.exe`. The actors initiate the process by creating a volume shadow copy of the system drive using a command such as `vssadmin.exe Create Shadow /for=C:`. This step establishes a snapshot of the system's state, including the Active Directory database. Subsequently, `ntdsutil.exe` is employed with the command sequence `ntdsutil snapshot “activate instance ntds” create quit quit` to interact with this shadow copy. The actors then access the shadow copy to extract the `ntds.dit` file from the `\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[X]\Windows\NTDS` directory. This orchestrated sequence is designed to extract sensitive credentials, such as hashed passwords, from the Active Directory, leading to a full domain compromise. The successful execution of this technique provides the APT actors with escalated privileges, facilitates lateral movement across the network, and enables their persistent access to critical systems and data.

Taking the specific example of the `ntdsutil snapshot "activate instance ntds" create quit quit` command, which creates a snapshot of the Active Directory database, multiple log sources can be leveraged to build a comprehensive context around this activity. Additionally, network defenders should consider that many commands can be shortened, and detection should account for this. For example, `ntdsutil snapshot "ac i ntds" create quit quit` command will also work. This approach is vital for distinguishing between legitimate administrative use and potential malicious exploitation. The following logs may add context and aid in detecting this activity:

- Command-line and process creation logs: Security logs with Event ID `4688` and Sysmon logs with Event ID `1` provide visibility into the execution of the `ntdsutil` command. These logs record the command-line arguments used, offering the first layer of insight. In a typical enterprise environment, the use of `ntdsutil` for snapshot creation might not be a regular occurrence and could signal unusual activity.
- File creation and access logs: Sysmon's Event ID `11` logs file creation events. The creation of a snapshot using `ntdsutil` involves generating specific files, which can be captured in these logs. Additionally, security logs with Event ID `4663`, which records attempts to access objects, can indicate access to sensitive files like `NTDS.dit`, providing further context to the snapshot creation process.
- Privilege use logs: Event ID `4673` in the security logs indicates the use of privileged services. The execution of `ntdsutil` requires elevated privileges, and monitoring for such privilege escalation can be a key indicator of potential misuse, especially when correlated with the execution of the command.
- Network activity and authentication logs: Alongside these logs, network activity logs can provide context about any concurrent remote connections or data transfers, which might indicate data exfiltration attempts post snapshot creation. Authentication logs can also be crucial in determining who executed the `ntdsutil` command and whether the account used aligns with typical administrative behavior.

In this real-world example, if an organization were to rigorously implement and follow best practice recommendations (listed above), the outcome of APT activity could be mitigated. Through strict network segmentation and the enforcement of principles of least privilege, an organization could restrict the threat actor's ability to move laterally across the network. Even if high-level credentials are extracted, segmentation could limit the actor's reach to isolated network segments. Additionally, robust privileged access management would ensure that elevated access is granted sparingly and monitored closely, making it challenging for a cyber threat actor to misuse stolen credentials. Application allowlisting would further prevent unauthorized software execution, reducing the risk of additional administrative tools being deployed. However, these measures are most effective when combined with vigilant monitoring, rapid incident response, and a continuous reassessment of network access controls and configurations.

PSExec.exe

`PSExec.exe` is part of the Microsoft PsTools suite and a common tool in LOTL tactics due to its ability to remotely execute commands across networked systems, often with elevated `SYSTEM` privileges. Understanding the context of LOTL activities is also crucial when it comes to tools like `PSExec.exe`, commonly used for remote administration and execution of processes.

State-sponsored actors have used the following `PSExec.exe` command to run one-off commands, such as this attempt to remove port proxy configurations on a remote host:

- `"C:\pstools\psexec.exe" {REDACTED} -s cmd /c "cmd.exe /c netsh interface portproxy delete v4tov4 listenaddress=0.0.0.0 listenport=9999"`[1]).

To effectively detect and contextualize such use of `PSExec.exe`, network defenders can rely on various logs:

- Command-line and process creation logs: Security logs with Event ID `4688` and Sysmon logs with Event ID `1` offer crucial insights into the execution of `PSExec.exe` and any associated commands, such as `Netsh`. These logs capture the command line used, providing essential information about the nature and intent of the process.
- Privilege use and explicit credential logs: Security logs with Event ID `4672` record instances of special privileges being assigned to new logons. This is particularly pertinent when PSExec is run with the `-s` switch, which executes the command with `SYSTEM` privileges. Additionally, Event ID `4648` in the security logs may capture instances of explicit credential use, which occurs when PSExec is executed with specific user credentials.
- Sysmon logs: Sysmon's Event ID 3 is instrumental for logging network connections, which are indicative of remote execution, a central component of PSExec's functionality. These logs can provide valuable information about the network interaction during the PSExec operation. Event IDs `12`, `13`, and `14` (Registry Events) will capture any changes made to the registry as a result of the `Netsh` command. In this specific instance, the logs would likely show deletion events (Event ID `14`) for registry keys associated with the port proxy configuration. The keys affected would typically be within paths like `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4`.
- Windows registry audit logs: Windows registry audit logs (if enabled) would record modifications made to the registry keys related to the port proxy settings. Given the specific `Netsh` command used, the logs would indicate the deletion of entries under the `v4tov4` key which manage port proxy settings for listen address `0.0.0.0` and listen port `9999`. The logs would include details such as the timestamp of the change,

the account under which the change was made (likely the `SYSTEM` account in this case, due to the switch in PSExec), and the specific registry values that were altered or deleted.

- Network and Firewall Logs: For network traffic analysis, specifically SMB traffic, which is characteristic of PSExec use, network device logs are crucial. Network defenders can identify connections to administrative shares (like the share) and other IPC traffic typically over TCP port . Firewall logs on the target system, if local firewall logging is enabled, can also provide insights into changes to the system's network configuration. These logs might reflect alterations in port proxy settings or changes to firewall state or rules, corresponding to the time of command execution.

Remediation

If compromise is detected, organizations should implement the following immediate, defensive countermeasures:

1. **Investigate to determine the highest privilege level account that the threat actor had or has access to.**
   a. **If the threat actor has control of an administrative account, such as Windows Active Directory Domain Admin, reset credentials of privileged and non-privileged accounts within the trust boundary of each compromised account.**
      i. Force password resets, and revoke and issue new certificates for all accounts/devices.
      ii. In Windows environments:
         1. If it is suspected that actors gained access to the DC/AD, then the passwords for all local accounts—such as `Guest`, `HelpAssistant`, `DefaultAccount`, `System`, `Administrator`, and `kbrtgt`—should be reset. It is essential that the password for the `kbrtgt` account is reset as this account is responsible for handling Kerberos ticket requests, as well as encrypting and signing them. The `kbrtgt` account should be reset twice (as the account has a two-password history). The first account reset for the `kbrtgt` needs to be allowed to replicate prior to the second reset to avoid any issues. See CISA's Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise for more information. Although tailored to FCEB agencies compromised in the 2020 SolarWinds Orion supply chain compromise, the steps are applicable to organizations with Windows AD compromise.
         2. If it is suspected that the `ntds.dit` file has been exfiltrated, then all domain user passwords will need to be reset.
         3. Review access policies to temporarily revoke privileges/access for affected accounts/devices. If alerting the cyber threat actor needs to be avoided

(e.g., for intelligence purposes), then privileges can be reduced for affected accounts/devices to "contain" them.

b. **Reset the relevant account credentials or access keys if the investigation finds the threat actor's access is limited to non-elevated permissions.**
   i. Monitor related accounts, especially administrative accounts, for any further signs of unauthorized access.

2. **Audit all network appliance and edge device configurations with indicators of malicious activity for signs of unauthorized or malicious configuration changes.** Organizations should ensure they audit the current network device running configuration and any local configurations that could be loaded at boot time. If configuration changes are identified:
   a. Change all credentials being used to manage network devices, to include keys and strings used to secure network device functions (SNMP strings/user credentials, IPsec/IKE pre-shared keys, routing secrets, TACACS/RADIUS secrets, RSA keys/certificates, etc.).
   b. Update all firmware and software to the latest version.
3. Report the compromise to an authoring agency as applicable.
   a. **US organizations:** To report suspicious or criminal activity related to information found in this joint guide, contact:
      i. CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870 or Your local FBI field office. 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.
      ii. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
      iii. For transportation entities regulated by TSA, report to CISA Central in accordance with the requirements found in applicable Security Directives, Security Programs, or TSA Order.
      iv. Entities required to report incidents to DOE should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov.
      v. Water and Wastewater Systems Sector organizations, contact the EPA Water Infrastructure and Cyber Resilience Division at watercyberta@epa.gov to voluntarily provide situational awareness.
   b. **Australian organizations:** Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.
   c. **Canadian organizations:** Report incidents by emailing CCCS at contact@cyber.gc.ca.
   d. **New Zealand organizations:** Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

e. **United Kingdom organizations:** Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

4. For organizations with cloud or hybrid environments, apply best practices for identity and credential access management.
5. **Minimize and control use of remote access tools and protocols** by applying best practices from joint Guide to Securing Remote Access Software and joint Cybersecurity Information Sheet: Keeping PowerShell: Security Measures to Use and Embrace.

For more information on incident response and remediation, see:

- Joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity. This advisory provides incident response best practices.
- CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to U.S. Federal Civilian Executive Branch (FCEB) agencies, the playbooks are applicable to all organizations. The incident response playbook provides procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents.

Secure by Design: Recommendations for Software Manufacturers

The above Best Practice Recommendations and Detection Recommendations sections apply to critical infrastructure organizations with on-premises or hybrid environments. Insecure software allows threat actors to leverage flaws to enable LOTL techniques and the responsibility should not solely be on the end user. CISA urges software manufacturers to implement the following to reduce the prevalence of weak default configurations and passwords, recognize the need for low or no-cost enhanced logging, and other exploitable issues identified in this guide.

- **Minimize attack surfaces that can be leveraged by cyber threat actors using LOTL techniques.** Disable unnecessary protocols by default, limit the number of processes and programs running with escalated privileges, and take other steps to limit the ability for cyber threat actors to leverage native functionality to conduct intrusions.
- **Embed security into product architecture** throughout the entire software development lifecycle (SDLC).
- **Mandate MFA, ideally phishing-resistant MFA**, for privileged users and make MFA a default, rather than opt-in, feature.
- **Provide high-quality logging for platforms and applications at no additional charge.** Cloud services should commit to generating and storing security-related logs at no additional charge. On-premises products should likewise generate security-related logs at no additional charge.

- **Track and reduce "hardening guide" size.** Reduce the size of "hardening guides" that are included with products and strive to ensure that the size shrinks over time as new versions of the software are released. Integrate components of the "hardening guide" as the default configuration of the product.
- **Consider the user experience consequences of security settings.** Each new setting increases the cognitive burden on end users and should be assessed in conjunction with the business benefit it derives. Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default. When configuration is necessary, the default option should be broadly secure against common threats.
- **Remove default passwords.** Default passwords should be removed entirely or, where necessary, passwords should be generated or set on first install then rotated on a periodic basis.
- **Remove or limit dynamic code execution.** Dynamic code execution allows products to be more versatile but is an extremely vulnerable attack surface, which can be exploited with hard to detect IOCs.
- **Remove hard-coded credentials.** Applications and scripts that contain hard-coded plaintext credentials allow malicious actors to leverage the credentials to easily access resources and expand their access in a network.

These mitigations align with tactics provided in the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. CISA urges software manufacturers to take ownership of improving the security outcomes of their customers by applying these and other secure by design tactics. By using secure by design principles, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing security software and logs, monitoring, and making routine updates.

For more information on secure by design, see CISA: Secure by Design, Australian Signals Directorate: Secure by Design, and Secure by Design Principles: UK Government Security.

Resources

CISA: Logging Made Easy Tool
NSA, CISA, NCSC-NZ, and NCSC-UK: Keeping PowerShell: Security Measures to Use and Embrace
NSA and CISA: Kubernetes Hardening Guide
Microsoft: Applications that can bypass WDAC and how to block them

References

[1] CISA: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

[2] CISA: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
[3] Mandiant: Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology
[4] MITRE: Unsecured Credentials: Cloud Instance Metadata API
[5] MITRE: Event Triggered Execution
[6] MITRE: Automated Exfiltration: Traffic Duplication
[7] CISA: Scattered Spider
[8] Microsoft: cmd.exe
[9] Microsoft: Windows Management Instrumentation
[10] WMIC: WMI command-line utility
[11] Microsoft: What is PowerShell?
[12] MITRE: System Binary Proxy Execution: Mshta
[13] Man7: sh(1p)
[14] GNU: Bash Reference Manual
[15] Die.Net: csh(1)
[16] Zsh.org
[17] Stanford: vi
[18] Vim.org
[19] Man7: curl(1)
[20] Man7: tar(1)
[21] Microsoft: Controlling a Service Using SC
[22] Microsoft: Use the at command to schedule tasks
[23] Microsoft: New-Service
[24] Microsoft: Win32_Service class
[25] Microsoft: PsTools
[26] Microsoft: PsExec v2.43
[27] MITRE: PsExec
[28] Microsoft: Ntdsutil
[29] Microsoft: reg commands
[30] Microsoft: Detecting and Preventing LSASS Credential Dumping Attacks
[31] Man7: cat(1)
[32] Man7: less(1)
[33] Man7: more(1)
[34] Man7: head(1)
[35] Man7: tail(1)
[36] Man7: sudo(8)
[37] Die.net: gpg(1)
[38] Microsoft: Net.exe
[39] Microsoft: Dsquery
[40] Microsoft: Get-ADUser

[41] Microsoft: Ldifde
[42] Microsoft: ipconfig
[43] Microsoft: Dnscmd
[44] Microsoft: nslookup
[45] Die.net: nslookup(1)
[46] Die.net: dig(1)
[47] Man7: ifconfig(8)
[48] Man7: ip(8)
[49] Microsoft: dir
[50] Man7: ls(1)
[51] Microsoft: Get-ChildItem
[52] Microsoft: netstat
[53] Man7: netstat(8)
[54] Microsoft: Get-NetTCPConnection
[55] Microsoft: tasklist
[56] Microsoft: Get-Process
[57] Microsoft: whoami
[58] Man7: whoami(1)
[59] Man7: id(1)
[60] Man7: uname(1)
[61] Die.net: procinfo(8)
[62] Man7: lscpu(1)
[63] Microsoft: Understanding the Remote Desktop Protocol (RDP)
[64] Virtual Network Computing from ORL: VNC Documentation
[65] Microsoft: Windows Remote Management
[66] OpenSSH: Manual Pages
[67] Man7: ssh(1)
[68] Man7: scp(1)
[69] Man7: iptables(8)
[70] Debian: NFT

Disclaimer

The information in this report is being provided “as is” for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

Acknowledgements

The following organizations contributed to this guide:

- Amazon Web Services (AWS)
- Energy industry representatives, through the DOE CESER Energy Threat Analysis Center (ETAC) pilot.
- Nippon Telegraph and Telephone (NTT)

Version History

Feb. 7, 2024: Initial version.

Appendix A: LOTL in WIndows, Linux, MacOS, and Hybrid Environments

Windows

Some common LOLBins cyber threat actors use in Windows (on-premises and hybrid) environments are `wmic.exe`, `ntdsutil.exe`, `Netsh`, `cmd.exe`, PowerShell for execution. For example:

- In one confirmed compromise, CISA observed the use of `ntdsutil.exe` in a potentially unauthorized manner on DCs. In one event, the `ntds.dit` file was moved from its original location to another within the `HarddiskVolumeShadowCopy` directory.
- In another event, CISA observed potential data exfiltration activities, including execution of WMIC, creation of temporary directories, initiation of the Volume Shadow Copy process, and mounting of the `ntds.dit` database. Modifications were made to the `MountPoints2\CPC` registry keys for three user accounts, suggesting cyber threat actors attempted to hide indications of data exfiltration.
- CISA observed the threat actors use the `Netsh` command to create a portProxy registry modification on compromised devices. Specifically, the modification was added to the registry key `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\PortProxy\v4tov4\cp\0.0.0.0/49275 | {redacted IP address}/8443`. This registry setting caused inbound traffic on port `49275` to be forwarded to a suspected threat actor command and control server on port `8443`.

Linux

Some common LOLBins cyber threat actors use in Linux environments are `curl`, `systemctl`, `systemd`, and python. For example, cyber threat actors:

- Use scripting environments like Python to gain interactive shell access, generate a reverse shell, transfer files, or to run custom scripts on compromised devices.
- Use SSH credentials or certificates to move laterally blending in with normal administrator activities, taking advantage of trusted relationships between Linux hosts.
- Exploit software with elevated permissions or elevated cronjobs to escalate privileges or maintain persistence.
- Exploit binaries `Suid Bit` set to escalate privileges or access secured system files.

macOS

- Malicious actors are known to use the following LOTL techniques in macOS environments.

- Scripting Environment and Tool Exploitation in macOS: Cyber threat actors exploit macOS's native scripting languages and built-in tools for malicious purposes. They utilize AppleScript and Bash to automate tasks, control applications, and execute commands, often manipulating AppleScript to interact with legitimate applications for data exfiltration or system manipulation. Additionally, they abuse built-in tools like `osascript` for executing AppleScripts and JavaScripts, `launchctl` for managing daemons and agents, and `curl` for file transfers, thus leveraging macOS's inherent functionalities for nefarious activities.
- Manipulating Property List (PLIST) files for persistence: Cyber threat actors may modify PLIST files to automatically execute malicious payloads during system startup or user login.
- Escalating privileges via misconfigured `sudoers`: Cyber threat actors may exploit `sudoers` misconfigurations that allow executing commands as a superuser without a password, enabling them to gain elevated access.
- Bypassing Gatekeeper for malware execution: Cyber threat actors may bypass Gatekeeper by leveraging trusted developer certificates or modifying system settings to allow execution from unidentified developers.

Cloud Environments

Some LOTL techniques malicious actors are known to use in cloud environments include:

- Abuse of native cloud instance metadata services (IMDS): The IMDS API can be queried (without authentication) from cloud instances to obtain a variety of useful information, including credentials that applications use to interact with other cloud services. Cyber threat actors who gain access to virtual instances may attempt to query the IMDS API to obtain credentials and gain further access to cloud resources [4].
- Achieve persistence through scheduled tasks: Cloud automation services can be used by cyber threat actors to achieve persistence in the environment by creating or modifying an event trigger to run malicious scripts whenever the event occurs. Cyber threat actors may also use this technique to escalate privileges by taking advantage of the fact that these automated actions can be configured to run under a different account than the user (such as a service account, which may have more privileges than the cyber threat actor) [5].
- Achieve persistence using service accounts: Service accounts are commonly used to provide applications with access to cloud resources that they need to communicate with. As these accounts are typically used for applications, they lack additional protection, such as MFA, that are frequently required for user accounts. Threat actors can target these accounts to achieve persistent access to the cloud tenant rather than having to continually bypass MFA protections on user accounts even with compromised credentials.

- Traffic Mirroring using application gateways: Cloud vendors typically offer traffic mirroring services for duplicating and forwarding traffic for analysis by network defenders. Cyber threat actors can leverage these services to exfiltrate traffic [6].
- Misuse of Cloud Service Providers (CSPs) CLI Tools: CLI tools provided by CSPs, such as AWS CLI and Azure CLI, are accessible within cloud environments. CLI tools can be misused for unauthorized activities on cloud resources, including data exfiltration and establishing persistent threats.

Hybrid Environments

- Malicious actors are known to use the following LOTL techniques in hybrid environments. **Note:** Organizations with hybrid environments should review Windows and Linux content as applicable.
- Exploitation of Identity Federation Systems: Hybrid environments frequently employ Active Directory Federation Services (ADFS) for identity management across both on-premises and cloud platforms. Threat actors target ADFS to compromise and manipulate federation tokens and impersonate legitimate users or entities. This allows threat actors to gain unauthorized access to a multitude of resources.
- Token manipulation and replay attacks: In hybrid environments, threat actors exploit the inherent trust between on-premises identity providers and cloud services. They achieve this by acquiring or fabricating federation tokens, such as Security Assertion Markup Language (SAML) tokens. This tactic effectively circumvents security measures reliant on traditional credential-based verification.
- LOLBins in hybrid environments: Windows LOLBins like PowerShell and `cmd.exe` are used to manipulate both on-premises and cloud systems. **Note:** Detecting their misuse is tougher in these environments due to less segmentation compared to standalone cloud or on-premises systems.
- Misuse of cloud service providers' (CSPs) CLI Tools: CLI tools provided by CSPs, such as AWS CLI and Azure CLI, are accessible within hybrid environments. CLI tools can be misused for unauthorized activities on cloud resources, including data exfiltration and establishing persistent threats.
- Targeting of hybrid cloud management platforms: Platforms that oversee both on-premises and cloud resources are potential intrusion vectors. Threat actors can exploit these platforms to gain comprehensive insights into the hybrid infrastructure, modify configurations, or deploy malicious elements.

Appendix B: Third-Party Tools for LOTL

Cyber threat actors use deployed software/remote access software, including the following, for LOTL:

- **Mobile device management systems.** Mobile device management (MDM) systems are attractive targets for threat actors because they provide elevated access to thousands of mobile devices.
- **Remote monitoring and management/system center configuration management (SCCM).** RMM software has significant capabilities to monitor or operate devices and systems as well as attain heightened permissions, making it an attractive tool for cyber threat actors to maintain persistence and move laterally on compromised networks.
- **Patch management systems.** Patch management systems provide access to thousands of systems.
- **EDR:** Cyber threat actors leverage common EDR tools installed on the victim networks to take advantage of the tools' remote-shell capabilities.[7]
- **VM management tools:** Cyber threat actors target vital virtualization management tools to exploit VM infrastructures. They use these platforms to commandeer VMs, execute commands, facilitate lateral network movement, and access sensitive data.
- **Database management tools:** Cyber threat actors can target database management tools to execute SQL commands, extract sensitive data, or manipulate database entries.
- **Network management systems:** Network management systems offer broad visibility and control over network devices and are prime targets. The compromise of these systems can lead to a cyber threat actor's ability to monitor network traffic, alter configurations, and potentially disrupt network operations, exploiting the very tools used to ensure network stability and security.
- **Identify and access management systems (IAM).** IAM systems, which are central to managing network user identities and access, are frequently targeted by cyber threat actors for their critical role in network access control.
- **IT service management (ITSM).** Cyber threat actors can manipulate IT service management (ITSM) platforms, exploiting these systems to alter tickets, workflows, and trigger automated actions for malicious purposes.
- For more information, see joint Guide to Securing Remote Access Software.

Appendix C: Known Lolbins Used Maliciously

Note: This guide uses the MITRE ATT&CK for Enterprise framework, version 14. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

See Table 1—Table 5 for known LOLBins used maliciously and the associated MITRE ATT&CK tactic and technique. Many LOLBins below demonstrate the multitude of techniques available for adversaries to achieve the same goal.

As these tools are used by administrators for legitimate functions, network defenders should not block or limit their use indiscriminately. Instead, network defenders should follow guidance in this guide to identify potential malicious use based on behavior. In some cases, alternate command-line arguments are also available, and network defenders should account for other options (see `net.exe`'s `/dom` and `/domain` flags or `ntdsutil.exe`'s `i` and `ifm` flags).

***Table 1: LOLBins Used for Execution** [TA0002]*

LOLBin	Environment	Use	MITRE ATT&CK Technique
`cmd.exe`, `wmic.exe`, `powershell.exe`, `Mshta.exe`	Windows	`cmd.exe` is a command-line interface for Windows operating systems (OSs).[8] Windows Management Instrumentation (WMI) is used to manage data and operations on Windows-based operating systems, and `wmic.exe`, which is deprecated, provides a command-line interface for WMI.[9],[10] PowerShell is a scripting language and command line tool for Windows OSs.[11] `Mshta.exe` executes Microsoft HTML Applications (HTA) files, which are standalone applications that execute with models and technologies of Internet Explorer outside of the browser.[12]	Command and Scripting Interpreter [T1059] System Binary Proxy Execution: Mshta [T1218.005] Windows Management Instrumentation [T1047]

LOLBin	Environment	Use	MITRE ATT&CK Technique
		Cyber threat actors can use these tools to tweak command line arguments, obfuscate parent-child process relationships, orphan child processes, and even run code on other hosts. Actors can also use some of these to execute secondary payloads.	
sh, bash, csh, and zsh	Unix	Unix shells like sh,[13] bash,[14] csh,[15] and zsh[16] are ubiquitous command line interpreters installed on most Linux and macOS systems. Cyber threat actors can abuse these shells as LOLBins to carry out malicious operations.	Command and Scripting Interpreter [T1059]
perl, python, and ruby	Windows or Unix	perl, python, ruby, and other scripting interpreters are commonly present on Windows and Unix systems and are often possess excessive permissions. Cyber threat actors can use these scripting interpreters to perform arbitrary code execution.	Command and Scripting Interpreter [T1059]
vim, vi, `curl`, and tar	Unix	The vim text editor has a --cmd flag which can be used to run Python or shell commands.[17] Similarly, the vi binary can be made to execute commands with `:!` followed by the command.[18] The curl command has an option --exec that allows executing scripts or binaries after downloading files.[19] The tar utility can be tricked into arbitrary code execution by passing special crafted archives or spawning an interactive shell by using the --checkpoint-action=exec flag.[20]	Command and Scripting Interpreter [T1059]

LOLBin	Environment	Use	MITRE ATT&CK Technique
		Cyber threat actors can abuse these utilities as LOLBins to carry out malicious activity.	
`Sc.exe`, `at.exe`, PowerShell's New-Service command, Win32_Service WMI Class	Windows	These LOLBins are used to create, modify, and/or execute services. `Sc.exe` is a command line utility for controlling services.[21] `at.exe` is a command line utility used to schedule tasks.[22] PowerShell New-Service can creates new services.[23] Win32_Service is a WMI class that represents services on hosts running Windows OSs.[24] Cyber threat actors can use these tools to create services and move laterally.	System Services: Service Execution [T1569.002]
`PsExec.exe`	Windows	`PsExec.exe`, part of the PsTools suite, remotely executes processes. `PsExec.exe` can launch interactive command-prompts on remote systems and remote-enabling tools like IpConfig.[25],[26] Cyber threat actors commonly use PsExec.exe for service execution, remote account creation, and lateral movement.[27]	System Services: Service Execution [T1569.002]

***Table 2: LOLBins Used for Credential Access** [TA0006]*

LOLBin	Environment	Use	MITRE ATT&CK Technique
`Ntdsutil.exe`	Windows	`Ntdsutil.exe` is a command-line tool for Windows OSs. It is used for management of Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).[28]	OS Credential Dumping: NTDS [T1003.003]

LOLBin	Environment	Use	MITRE ATT&CK Technique
		Cyber threat actors can use Ntdsutil.exe to obtain credentials by exfiltrating copies of ntds.dit from domain controllers (DCs). ntds.dit is the main Active Directory (AD) database file and, by default, is stored at `%SystemRoot%\NTDS\ntds.dit`. This file contains information about users, groups, group memberships, and password hashes for all users in the domain.	
`reg.exe`	Windows	`reg.exe` is used to perform operations on registry subkey information and values in registry entries.[29] Cyber threat actors can export the SAM and SYSTEM registry hives to search for locally cached credentials.	Unsecured Credentials: Credentials in Registry [T1552.002]
`lsass.exe`	Windows	`Lsass.exe` stores cached credentials in memory while users are logged in to facilitate single sign-on to network resources. Since `lsass.exe` runs at a high privilege level, cyber threat actors utilize memory injection tools like Procdump and Mimikatz to extract credential data out of lsass.exe.[30]	OS Credential Dumping: LSASS Memory [T1003.001]
sudo, cat, less, more, head, tail, vi, and vim	Unix	Since many configurations and credentials are stored as files on Unix-based systems threat actors are increasingly leveraging ubiquitous Unix utilities that can read files to uncover credentials stored on compromised systems. Commands like cat,[31] less,[32] more,[33] head,[34] and tail [35] when invoked on files containing secrets such as hashed passwords, private keys, API tokens, or database connection strings could enable the cyber threat	OS Credential Dumping: /etc/passwd and /etc/shadow [T1003.008] Unsecured Credentials [T1552.001]

LOLBin	Environment	Use	MITRE ATT&CK Technique
		actor to covertly steal these credentials for further exploitation. Similarly, standard text editors like vi and vim may allow cyber threat actors to access the contents of sensitive files. Finally, utilities like sudo can be used to elevate privileges to dump credential files as a superuser.[36]	
gpg	Unix	The gpg binary may contain decrypted credentials or keys if improperly secured.[37]	Unsecured Credentials [T1552.001]

***Table 3: LOLBins Used for Discovery** [TA0007]*

LOLBin	Environment	Use	MITRE ATT&CK Technique
`net.exe`, `dsquery.exe`, PowerShell's GET-AD* cmdlets, `ldifde.exe`	Windows	`net.exe` can query Active Directory, manage running services, list shares, among other items.[38] Dsquery is a Windows OS command-line tool for querying the Active Directory.[39] PowerShell's GET-AD* cmdlets gets user objects from the Active Directory.[40] `ldifde.exe` is a Windows command line-tool that creates, modifies, and deletes directory objects.[41] Cyber threat actors use these for Lightweight Activity Directory (LDAP) queries to enumerate domain users and groups. Executables like dsquery.exe and ldifde.exe may not be present on all systems; they are only installed alongside certain roles (such as domain controllers) or outdated operating systems. Backwards	Account Discovery: Domain Account [T1078.002]

LOLBin	Environment	Use	MITRE ATT&CK Technique
		compatibility allows adversaries to upload and run these legitimate Microsoft tools in a semi-LOTL fashion.	
`ipconfig.exe`, `dnscmd.exe`, `nslookup.exe`, nslookup, and dig	Windows or Unix	`ipconfig.exe` can dump the system's cached DNS records as well as current network configuration. [42] `dnscmd.exe` is a command-line interface for managing DNS servers.[43] The `nslookup.exe` in Windows or nslookup binary in Unix displays DNS information.[44],[45] The dig binary can be used to interrogate DNS servers. [46] Cyber threat actors can use these to enumerate the internal domain name system (DNS).	System Network Configuration Discovery [T1016]
ifconfig, ip	Unix	The ifconfig [47] and ip [48] binaries are common network configuration utilities in Unix and Linux systems that can be used to view and configure network interfaces. Cyber threat actors can use ifconfig or ip to enumerate system network information or modify network configurations.	System Network Configuration Discovery [T1016]
cmd.exe /c dir, PowerShell's Get-ChildItem cmdlet, and ls	Windows or Unix	cmd.exe /c dir, the ls binary, and PowerShell's Get-ChildItem all display a list of a directory's files and subdirectories.[49],[50],[51] Cyber threat actors can use these LOLBins to enumerate files on disk and internal Server Message Block (SMB) servers.	File and Directory Discovery [T1083]

LOLBin	Environment	Use	MITRE ATT&CK Technique
netstat.exe, PowerShell's Get-NetTCPConnection cmdlet, and netstat	Windows or Unix	The netstat.exe in Windows or netstat binary in Unix lists active TCP connections, ports on which the host is listening, and the IP routing table.[52],[53] The Get-NetTCPConnection cmdlet can get current TCP connections.[54] Cyber threat actors can use these LOLBins to enumerate local network connections, including active Transmission Control Protocol (TCP) connections.	System Network Connections Discovery [T1049]
Tasklist.exe, PowerShell's Get-Process cmdlet, and ps	Windows or Unix	The Tasklist.exe in Windows or the ps binary in Unix lists currently running processes.[55] PowerShell's Get-Process cmdlet gets the processes running.[56] Cyber threat actors can use these LOLBins to enumerate software, services, and processes on a compromised system.	Software Discovery [T1518] System Service Discovery [T1007] Process Discovery [T1057]
Whoami.exe, whoami, id	Windows or Unix	The Whoami.exe displays user, groups, and privileges information for the user who is currently logged on to the local Windows host.[57] The whoami binary in Unix can show the username for the currently logged on user.[58] The id binary in Unix can show the user and group information for a specified user or current process.[59] Malicious actors can use these binaries to identify primary or common users of compromised systems.	System Owner/User Discovery [T1033]
systeminfo.exe	Windows	Systeminfo.exe can be used to gather information about the compromised system's operating system.	System Information Discovery [T1082]

LOLBin	Environment	Use	MITRE ATT&CK Technique
		Cyber threat actors can use systeminfo.exe to enumerate local system information.	
uname, lscpu, procinfo	Unix	The uname binary (commonly used with the -a flag) prints system information like kernel version and hardware architecture.[60] The procinfo and lscpu binaries print system and CPU information. [61],[62] Cyber threat actors can use these binaries to enumerate local system information.	System Information Discovery [T1082]

Table 4: LOLBins Used for Lateral Movement

LOLBin	Environment	Use	MITRE ATT&CK Technique
RDP, VNC, WinRM	Windows or Unix	Actors may use Remote Desktop Protocol (RDP) [63], Virtual Network Computing (VNC) [64], and WinRM [65] with valid accounts to remotely interact with hosts. This activity produces different log artifacts than other types of logins.	Remote Services: Remote Desktop Protocol [T1021.001] Remote Services: VNC [T1021.005] Remote Services: Windows Remote Management [T1021.006]
Secure Shell (SSH), Secure Copy (SCP)	Windows or Unix	Secure Shell (SSH) is used to securely log in to Windows or Unix systems via a command-line interface, and malicious actors can use SSH to move laterally.[66] [67] Secure Copy	Application Layer Protocol [T1071] Remote Services: SSH [T1021.004]

		(SCP) is an encrypted file transfer protocol that utilizes SFTP and SSH to transfer data.[68] CISA red teams frequently use SSH to move laterally through compromised networks after acquiring SSH private keys for privileged service accounts. Threat actors could use these LOLBins to remotely access compromised systems, exfiltrate data, or move laterally.	

Table 5: LOLBins Used for Command and Control

LOLBin	Environment	Use	MITRE ATT&CK Technique
`Netsh`, Netsh interface portproxy	Windows	`Netsh` is a built-in Windows command line scripting utility that can display or modify the network settings of a host, including the Windows Firewall. Netsh interface portproxy enables port forwarding on hosts.	Proxy [T1090] Impair Defenses: Disable or Modify [T1562.001] System Firewall [T1562.004]
Ldifde.exe, certutil.exe	Windows	Malicious actors can use these LOLBins to allow threat actors to upload, download, and obfuscate files on disk.	Ingress Tool Transfer [T1105] Exfiltration over Web Service [T1567]
iptables, nftables	Linux	The iptables [69] and nftables [70] binaries allow system administrators to configure the IP packet filter rules of the Linux firewalls. Malicious actors can use iptables to redirect traffic from Linux-based hosts.	Proxy [T1090]

LOLBin	Environment	Use	MITRE ATT&CK Technique
Secure Shell (SSH), Secure Copy (SCP)	Windows or Unix	SSH is used to securely log in to Windows or Unix systems via a command-line interface. [66] [67] Secure Copy (SCP) is an encrypted file transfer protocol that utilizes SFTP and SSH to transfer data.[68] Malicious actors can use the –L, -R, -D flags to create encrypted proxy tunnels (either point-point or dynamic). Threat actors could use these LOLBins to remotely access compromised systems, exfiltrate data, or move laterally.	Application Layer Protocol [T1071] Remote Services: SSH [T1021.004]