JOINT CYBERSECURITY ADVISORY

Technical Approaches to Uncovering and Remediating Malicious Activity

AR20-245A

September 1, 2020

ACSC Australian Cyber Security Centre

certnz

National Cyber Security Centre
a part of GCHQ

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

CONTENTS

Overview..2
Key Takeaways 2
Description..3
Recommended Artifact and Information Collection 3
Host-Based Artifacts.............................3
Network-Based Artifacts........................4
Common Mistakes in Incident Handling ..5
Recommended Investigation and Remediation Processes 6
General Mitigation Guidance 6
General Recommendations and Best Practices Prior to an Incident................9
Additional Best Practices 13
Resources 13

OVERVIEW

This joint advisory is the result of a collaborative research effort by the cybersecurity authorities of five nations: Australia, Canada, New Zealand, the United Kingdom, and the United States.[1] It highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices. The purpose of this report is to enhance incident response among partners and network administrators along with serving as a playbook for incident investigation.

Key Takeaways

When addressing potential incidents and applying best practice incident response procedures:

- ✓ First, collect and remove for further analysis:
  - Relevant artifacts,
  - Logs, and
  - Data.

- ✓ Next, implement mitigation steps that avoid tipping off the adversary that their presence in the network has been discovered.

- ✓ Finally, consider soliciting incident response support from a third-party IT security organization to:
  - Provide subject matter expertise and technical support to the incident response,
  - Ensure that the actor is eradicated from the network, and
  - Avoid residual issues that could result in follow-up compromises once the incident is closed.

[1] Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), New Zealand CERT NZ, United Kingdom National Cyber Security Centre (UK NCSC), United States Cybersecurity and Infrastructure Security Agency (CISA)

DESCRIPTION

The incident response process requires a variety of technical approaches to uncover malicious activity. Incident responders should consider the following activities.

- **Indicators of Compromise (IOC) Search** – Collect known-bad indicators of compromise from a broad variety of sources, and search for those indicators in network and host artifacts. Assess results for further indications of malicious activity to eliminate false positives.
- **Frequency Analysis** – Leverage large datasets to calculate normal traffic patterns in both network and host systems. Use these predictive algorithms to identify activity that is inconsistent with normal patterns. Variables often considered include timing, source location, destination location, port utilization, protocol adherence, file location, integrity via hash, file size, naming convention, and other attributes.
- **Pattern Analysis** – Analyze data to identify repeating patterns that are indicative of either automated mechanisms (e.g., malware, scripts) or routine human threat actor activity. Filter out the data containing normal activity and evaluate the remaining data to identify suspicious or malicious activity.
- **Anomaly Detection** – Conduct an analyst review (based on the team's knowledge of, and experience with, system administration) of collected artifacts to identify errors. Review unique values for various datasets and research associated data, where appropriate, to find anomalous activity that could be indicative of threat actor activity.

RECOMMENDED ARTIFACT AND INFORMATION COLLECTION

When hunting and/or investigating a network, it is important to review a broad variety of artifacts to identify any suspicious activity that may be related to the incident. Consider collecting and reviewing the following artifacts throughout the investigation.

Host-Based Artifacts

- Running Processes
- Running Services
- Parent-Child Process Trees
- Integrity Hash of Background Executables
- Installed Applications
- Local and Domain Users
- Unusual Authentications
- Non-Standard Formatted Usernames
- Listening Ports and Associated Services
- Domain Name System (DNS) Resolution Settings and Static Routes
- Established and Recent Network Connections
- Run Key and other AutoRun Persistence
- Scheduled Tasks
- Artifacts of Execution (Prefetch and Shimcache)
- Event logs
- Anti-virus detections

Information to Review for Host Analysis

- Identify any process that is not signed and is connecting to the internet looking for beaconing or significant data transfers.
- Collect all PowerShell command line requests looking for Base64-encoded commands to help identify malicious fileless attacks.

- Look for excessive `.RAR`, `7zip`, or `WinZip` processes, especially with suspicious file names, to help discover exfiltration staging (suspicious file names include naming conventions such as, `1.zip`, `2.zip`, etc.).
- Collect all user logins and look for outlier behavior, such as a time of login that is out of the ordinary for the user or a login from an Internet Protocol (IP) address not normally used by the user.
- On Linux/Unix operating systems (OSs) and services, collect all `cron` and `systemd` `/etc/passwd` files looking for unusual accounts and log files, such as accounts that appear to be `system / proc` users but have an interactive shell such as `/bin/bash` rather than `/bin/false/nologin`
- On Microsoft OSs, collect Scheduled Tasks, Group Policy Objects (GPO), and Windows Management Instrumentation (WMI) database storage on hosts of interest looking for malicious persistence.
- Use the Microsoft Windows Sysinternals Autoruns tool, which allows IT security practitioners to view—and, if needed, easily disable—most programs that automatically load onto the system.
- Check the Windows registry and Volume Shadow Copy Service for evidence of intrusion.
- Consider blocking script files like `.js`, `.vbs`, `.zip`, `.7z`, `.sfx` and even Microsoft Office documents or PDFs.
- Collect any scripts or binary ELF files from `/dev/shm/tmp` and `/var/tmp`.
- Kernel modules listed (lsmod) for signs of a rootkit; dmesg command output can show signs of rootkit loading and device attachment amongst other things.
- Archive contents of `/var/log` for all hosts.
- Archive output from journald. These logs are pretty much the same as /var/log; however, they provide some integrity checking and are not as easy to modify. This will eventually replace the /var/log contents for some aspects of the system. Check for additional Secure Shell (SSH) keys added to user's `authorized_keys`.

Network-Based Artifacts

- Anomalous DNS traffic and activity, unexpected DNS resolution servers, unauthorized DNS zone transfers, data exfiltration through DNS, and changes to host files
- Remote Desktop Protocol (RDP), virtual private network (VPN) sessions, SSH terminal connections, and other remote abilities to evaluate for inbound connections, unapproved third-party tools, cleartext information, and unauthorized lateral movement
- Uniform Resource Identifier (URI) strings, user agent strings, and proxy enforcement actions for abusive, suspicious, or malicious website access
- Hypertext Transfer Protocol Secure/Secure Sockets Layer (HTTPS/SSL)
- Unauthorized connections to known threat indicators
- Telnet
- Internet Relay Chat (IRC)
- File Transfer Protocol (FTP)

Information to Review for Network Analysis

- Look for new connections on previously unused ports.
- Look for traffic patterns related to time, frequency, and byte count of the connections.
- Preserve proxy logs. Add in the URI parameters to the event log if possible.
- Disable LLMNR on the corporate network; if unable to disable, collect LLMNR (UDP port 5355) and NetBIOS-NS (UDP port 137).
- Review changes to routing tables, such as weighting, static entries, gateways, and peer relationships.

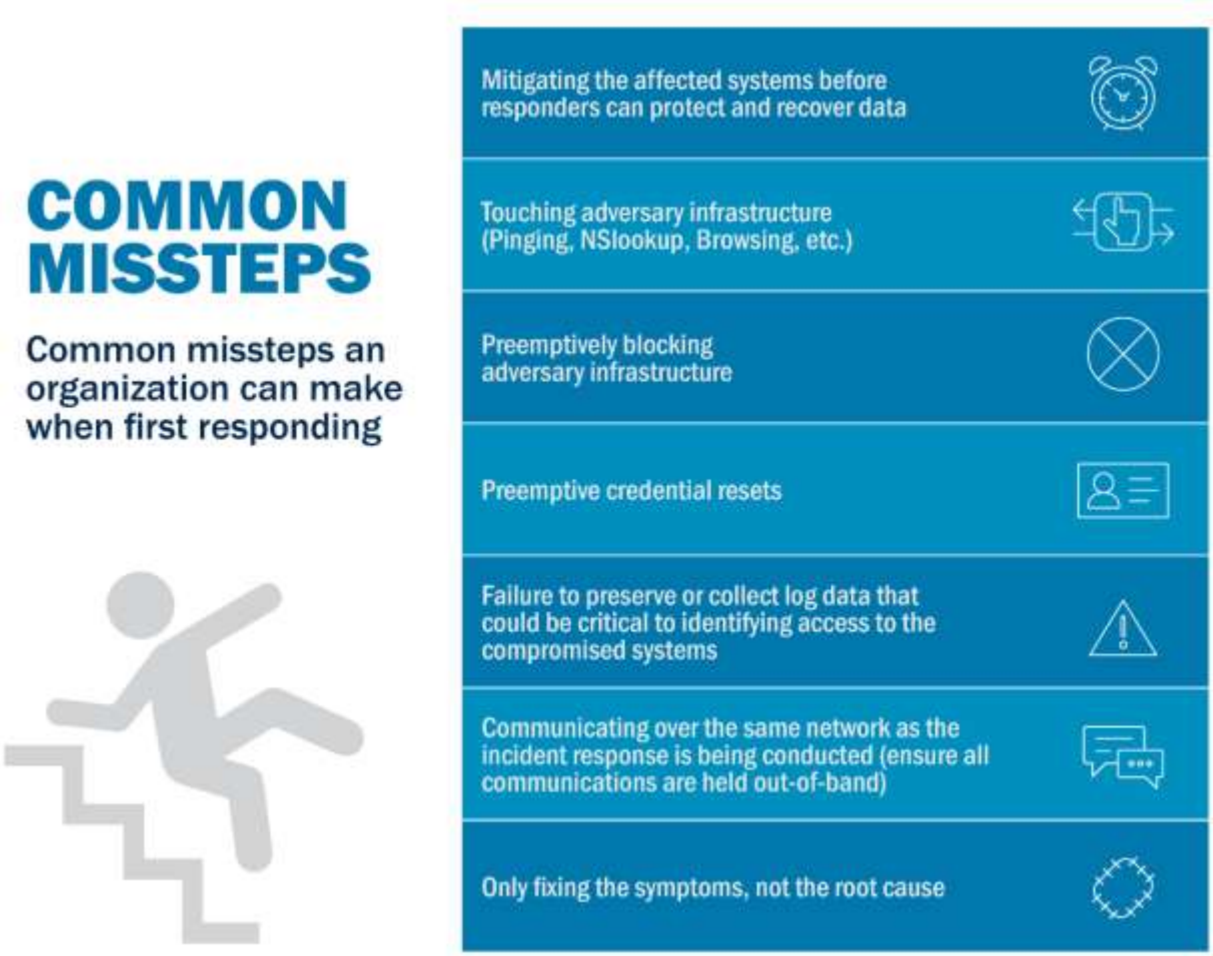
COMMON MISTAKES IN INCIDENT HANDLING

After determining that a system or multiple systems may be compromised, system administrators and/or system owners are often tempted to take immediate actions. Although well intentioned to limit the damage of the compromise, some of those actions have the adverse effect of:

1. Modifying volatile data that could give a sense of what has been done; and
2. Tipping the threat actor that the victim organization is aware of the compromise and forcing the actor to either hide their tracks or take more damaging actions (like detonating ransomware).

Below—and partially listed in figure 1—are actions to avoid taking and some of the consequence of taking such actions.

- **Mitigating the affected systems before responders can protect and recover data**
    - This can cause the loss of volatile data such as memory and other host-based artifacts.
    - The adversary may notice and change their tactics, techniques, and procedures.
- **Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)**
    - These actions can tip off the adversary that they have been detected.
- **Preemptively blocking adversary infrastructure**
    - Network infrastructure is fairly inexpensive. An adversary can easily change to new command and control infrastructure, and you will lose visibility of their activity.
- **Preemptive credential resets**
    - Adversary likely has multiple credentials, or worse, has access to your entire Active Directory.
    - Adversary will use other credentials, create new credentials, or forge tickets.
- **Failure to preserve or collect log data that could be critical to identifying access to the compromised systems**
    - If critical log types are not collected, or are not retained for a sufficient length of time, key information about the incident may not be determinable. Retain log data for at least one year.
- **Communicating over the same network as the incident response is being conducted (ensure all communications are held out-of-band)**
- **Only fixing the symptoms, not the root cause**
    - Playing “whack-a-mole” by blocking an IP address—without taking steps to determine what the binary is and how it got there—leaves the adversary an opportunity to change tactics and retain access to the network.



COMMON MISSTEPS

Common missteps an organization can make when first responding

- Mitigating the affected systems before responders can protect and recover data
- Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)
- Preemptively blocking adversary infrastructure
- Preemptive credential resets
- Failure to preserve or collect log data that could be critical to identifying access to the compromised systems
- Communicating over the same network as the incident response is being conducted (ensure all communications are held out-of-band)
- Only fixing the symptoms, not the root cause

Figure 1: Common missteps to be avoided when responding to an incident

RECOMMENDED INVESTIGATION AND REMEDIATION PROCESSES

The following recommendations and best practices may be helpful during the investigation and remediation process. **Note**: Although this guidance provides best practices to mitigate common attack vectors, organizations should specific to [Client]'s network should tailor mitigations specific to their network.

General Mitigation Guidance

Restrict or Discontinue Use of FTP and Telnet Services

The FTP and Telnet protocols transmit credentials in cleartext, which are susceptible to being intercepted. To mitigate this risk, discontinue FTP and Telnet services by moving to more secure file storage/file transfer and remote access services.

- Evaluate business needs and justifications to host files on alternative Secure File Transfer Protocol (SFTP) or HTTPS-based public sites.
- Use Secure Shell (SSH) for access to remote devices and servers.

Restrict or Discontinue Use of Non-approved VPN Services

- Investigate the business needs and justification for allowing traffic from non-approved VPN services.

- Identify such services across the enterprise and develop measures to add the application and browser plugins that enable non-approved VPN services to the denylist.
- Enhance endpoint monitoring to obtain visibility on devices with non-approved VPN services running. Enhanced endpoint monitoring and detection capabilities would enable an organization's IT security personnel to manage approved software as well as identify and remove any instances of unapproved software.

Shut down or Decommission Unused Services and Systems

- Cyber actors regularly identify servers that are out of date or end of life (EOL) to gain access to a network and perform malicious activities. These present easy and safe locations to maintain persistence on a network.
- Often these services and servers are systems that have begun decommissioning, but the final stage has not been completed by shutting down the system. This means they are still running and vulnerable to compromise.
- Ensuring that decommissioning of systems has been completed or taking appropriate action to remove them from the network limits their susceptibility and reduces the investigative surface to be analyzed.

Quarantine and Reimage Compromised Hosts

Note: proceed with caution to avoid the adverse effects detailed in the Common Mistakes in Incident Handling section above.

- Reimage or remove any compromised systems found on the network.
- Monitor and educate users to be cautious of any downloads from third-party sites or vendors.
- Block the known bad domains and add a web content filtering capability to block malicious sites by category to prevent future compromise.
- Sanitize removable media and investigate network shares accessible by users.
- Improve existing network-based malware detection tools with sandboxing capabilities.

Disable Unnecessary Ports, Protocols, and Services

- Identify and disable ports, protocols, and services not needed for official business to prevent would-be attackers from moving laterally to exploit vulnerabilities. This includes external communications as well as communications between networks.
- Document allowed ports and protocols at the enterprise level.
- Restrict inbound and outbound access to ports and protocols not justified for business use.
- Restrict allowed access list to assets justified by business use.
- Enable a firewall log for inbound and outbound network traffic as well as allowed and denied traffic.

Restrict or Disable Interactive Login for Service Accounts

Service accounts are privileged accounts dedicated to certain services to perform activities related to the service or application without being tied to a single domain user. Given that services tend to be privileged accounts and thereby have administrative privileges, they are often a target for attackers aiming to obtain credentials. Interactive login to a service account not directly tied to an end-user account makes it difficult to identify accountability during cyber incidents.

- Audit the Active Directory (AD) to identify and document active service accounts.
- Restrict use of service accounts using AD group policy.
- Disallow interactive login by adding service account to a group of non-interactive login users.
- Continuously monitor service account activities by enhancing logging.

- Rotate service accounts and apply password best practices without service, degradation, or disruption.

Disable Unnecessary Remote Network Administration Tools

- If an attacker (or malware) gains access to a remote user's computer, steals authentication data (login/password), hijacks an active remote administration session, or successfully attacks a vulnerability in the remote administration tool's software, the attacker (or malware) will gain unrestricted control of the enterprise network environment. Attackers can use compromised hosts as a relay server for reverse connections, which could enable them to connect to these remote administration tools from anywhere.
- Remove all remote administration tools that are not required for day-to-day IT operations. Closely monitor and log events for each remote-control session required by department IT operations.

Manage Unsecure Remote Desktop Services

Allowing unrestricted RDP access can increase opportunities for malicious activity such as on path and Pass-the-Hash (PtH) attacks.

- Implement secure remote desktop gateway solutions.
- Restrict RDP service trust across multiple network zones.
- Implement privileged account monitoring and short time password lease for RDP service use.
- Implement enhanced and continuous monitoring of RDP services by enabling logging and ensure RDP logins are captured in the logs.

Credential Reset and Access Policy Review

Credential resets need to be done to strategically ensure that all the compromised accounts and devices are included and to reduce the likelihood that the attacker is able to adapt in response to this.

- Force password resets; revoke and issue new certificates for affected accounts/devices.
- If it is suspected that the attacker has gained access to the Domain Controller, 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 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.
- If it is suspected that the `ntds.dit` file has been exfiltrated, then all domain user passwords will need to be reset.
- Review access policies to temporarily revoke privileges/access for affected accounts/devices. If it is necessary to not alert the attacker (e.g., for intelligence purposes), then privileges can be reduced for affected accounts/devices to "contain" them.

Patch Vulnerabilities

Attackers frequently exploit software or hardware vulnerabilities to gain access to a targeted system.

- Known vulnerabilities in external facing devices and servers should be patched immediately, starting with the point of compromise, if known.
  - Ensure external-facing devices have not been previously compromised while going through the patching process.
- If the point of compromise (i.e., the specific software, device, server) is known, but how the software, device, or server was exploited is unknown, notify the vendor so they can begin analysis and develop a new patch.

- Follow vendor remediation guidance including the installation of new patches as soon as they become available.

General Recommendations and Best Practices Prior to an Incident

Properly implemented defensive techniques and programs make it more difficult for a threat actor to gain access to a network and remain persistent yet undetected. When an effective defensive program is in place, attackers should encounter complex defensive barriers. Attacker activity should also trigger detection and prevention mechanisms that enable organizations to identify, contain, and respond to the intrusion quickly. There is no single technique, program, or set of defensive techniques or programs that will completely prevent all attacks. The network administrator should adopt and implement multiple defensive techniques and programs in a layered approach to provide a complex barrier to entry, increase the likelihood of detection, and decrease the likelihood of a successful attack. This layered mitigation approach is known as defense-in-depth.

User Education

End users are the frontline security of the organizations. Educating them in security principles as well as actions to take and not take during an incident will increase the organization's resilience and might prevent easily avoidable compromises.

- Educate users to be cautious of any downloads from third-party sites or vendors.
- Train users on recognizing phishing emails. There are several systems and services (free and otherwise) that can be deployed or leveraged.
- Train users on identifying which groups/individuals to contact when they suspect an incident.
- Train users on the actions they can and cannot take if they suspect an incident and why (some users will attempt to remediate and might make things worst).

Allowlisting

- Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
- Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from `PROGRAMFILES`, `PROGRAMFILES(X86)`, and `SYSTEM32`. Disallow all other locations unless an exception is granted.
- Prevent the execution of unauthorized software by using application allowlisting as part of the OS installation and security hardening process.

Account Control

- Decrease a threat actor's ability to access key network resources by implementing the principle of least privilege.
- Limit the ability of a local administrator account to log in from a local interactive session (e.g., Deny access to this computer from the network) and prevent access via an RDP session.
- Remove unnecessary accounts and groups; restrict root access.
- Control and limit local administration; e.g. implementing Just Enough Administration (JEA), just-in-time (JIT) administration, or enforcing PowerShell Constrained Language mode via a User Mode Code Integrity (UMCI) policy.
- Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.

Backups

- Identify what data is essential to keeping operations running; make regular backup copies.
- Test that backups are working to ensure they can restore the data in the event of an incident.

- Create offline backups to help recover from a ransomware attack or from disasters (fire, flooding, etc.).
- Securely store offline backups at an offsite location. If feasible, choose an offsite location that is at a distance from the primary location that would be unaffected in the event of a regional natural disaster.

Workstation Management

- Create and deploy a secure system baseline image to all workstations.
- Mitigate potential exploitation by threat actors by following a normal patching cycle for all OSs, applications, and software, with exceptions for emergency patches.
- Apply asset and patch management processes.
- Reduce the number of cached credentials to one (if a laptop) or zero (if a desktop or fixed asset).

Host-Based Intrusion Detection / Endpoint Detection and Response

- Configure and monitor workstation system logs through a host-based endpoint detection and response platform and firewall.
- Deploy an anti-malware solution on workstations to prevent spyware, adware, and malware as part of the OS security baseline.
    - Ensure that your anti-malware solution remains up to date.
- Monitor antivirus scan results on a regular basis.

Server Management

- Create a secure system baseline image and deploy it to all servers.
- Upgrade or decommission end-of-life non-Windows servers.
- Upgrade or decommission servers running Windows Server 2003 or older versions.
- Implement asset and patch management processes.
- Audit for and disable unnecessary services.

Server Configuration and Logging

- Establish remote server logging and retention.
- Reduce the number of cached credentials to zero.
- Configure and monitor system logs via a centralized security information and event management (SIEM) appliance.
- Add an explicit `DENY` for `%USERPROFILE%`.
- Restrict egress web traffic from servers.
- In Windows environments, use Restricted Admin mode or remote credential guard to further secure remote desktop sessions against pass-the-hash attacks.
- Restrict anonymous shares.
- Limit remote access by only using jump servers for such access.
- On Linux, use SELINUX or AppArmor in enforcing mode and/or turn on audit logging.
- Turn on bash shell logging; ship this and all logs to a remote server.
- Do not allow users to use `su`. Use `Sudo -l` instead.
- Configure automatic updates in `yum` or `apt`.
- Mount `/var/tmp` and `/tmp` as `noexec`.

Change Control

- Create a change control process for all implemented changes.

Network Security

- Implement an intrusion detection system (IDS).
  - Apply continuous monitoring.
  - Send alerts to a SIEM tool.
  - Monitor internal activity (this tool may use the same tap points as the netflow generation tools).
- Employ netflow capture.
  - Set a minimum retention period of 180 days.
  - Capture netflow on all ingress and egress points of network segments, not just at the Managed Trusted Internet Protocol Services or Trusted Internet Connections locations.
- Capture all network traffic
  - Retain captured traffic for a minimum of 24 hours.
  - Capture traffic on all ingress and egress points of the network.
- Use VPN
  - Maintain site-to-site VPN with customers and vendors.
  - Authenticate users utilizing site-to-site VPNs.
  - Use authentication, authorization, and accounting for controlling network access.
  - Require smartcard authentication to an HTTPS page in order to control access. Authentication should also require explicit rostering of permitted smartcard distinguished names to enhance the security posture on both networks participating in the site-to-site VPN.
- Establish appropriate secure tunneling protocol and encryption.
- Strengthen router configuration (e.g., avoid enabling remote management over the internet and using default IP ranges, automatically log out after configuring routers, and use encryption.).
- Turn off Wi-Fi protected setup, enforce the use of strong passwords, and keep router firmware up-to-date.
- Improve firewall security (e.g., enable automatic updates, revise firewall rules as appropriate, implement allowlists, establish packet filtering, enforce the use of strong passwords, encrypt networks).
  - Whenever possible, ensure access to network devices via external or untrusted networks (specifically the internet) is disabled.
- Manage access to the internet (e.g., providing internet access from only devices/accounts that need it, proxying all connections, disabling internet access for privileged/administrator accounts, enabling policies that restrict internet access using a blocklist, a resource allowlist, content type, etc.)
  - Conduct regular vulnerability scans of the internal and external networks and hosted content to identify and mitigate vulnerabilities.
  - Define areas within the network that should be segmented to increase the visibility of lateral movement by a threat and increase the defense-in-depth posture.
  - Develop a process to block traffic to IP addresses and domain names that have been identified as being used to aid previous attacks.
- Evaluate and consider the security configurations of Microsoft Office 365 (O365) and other cloud collaboration service platforms prior to deployment.
  - Use multi-factor authentication. This is the best mitigation technique to protect against credential theft for O365 administrators and users.
  - Protect Global Admins from compromise and use the principle of “Least Privilege.”
  - Enable unified audit logging in the Security and Compliance Center.
  - Enable alerting capabilities.
  - Integrate with organizational SIEM solutions.
  - Disable legacy email protocols, if not required, or limit their use to specific users.

Network Infrastructure Recommendations

- Create a secure system baseline image and deploy it to all networking equipment (e.g., switches, routers, firewalls).
- Remove unnecessary OS files from the internetwork operating system (IOS). This will limit the possible targets of persistence (i.e., files to embed malicious code) if the device is compromised and will align with National Security Agency Network Device Integrity best practices.
- Remove vulnerable IOS OS files (i.e., older iterations) from the device's boot variable (i.e., show boot or show bootvar).
- Update to the latest available operating system for IOS devices.
- On devices with a Secure Sockets Layer VPN enabled, routinely verify customized web objects against the organization's known good files for such VPNs, to ensure the devices remain free of unauthorized modification.
- Ensure that any incident response tools that point to external domains are either removed or updated to point to internal security tools. If this is not done and an external domain to which a tool points expires, a malicious threat actor may register it and start collecting telemetry from the infrastructure.

Host Recommendations

- Implement policies to block workstation-to-workstation RDP connections through a Group Policy Object on Windows, or by a similar mechanism.
- Store system logs of mission critical systems for at least one year within a SIEM tool.
- Review the configuration of application logs to verify that recorded fields will contribute to an incident response investigation.

User Management

- Reduce the number of domain and enterprise administrator accounts.
- Create non-privileged accounts for privileged users and ensure they use the non- privileged accounts for all non-privileged access (e.g., web browsing, email access).
- If possible, use technical methods to detect or prevent browsing by privileged accounts (authentication to web proxies would enable blocking of Domain Administrators).
- Use two-factor authentication (e.g., security tokens for remote access and access to any sensitive data repositories).
- If soft tokens are used, they should not exist on the same device that is requesting remote access (e.g., a laptop) and instead should be on a smartphone, token, or other out-of-band device.
- Create privileged role tracking.
- Create a change control process for all privilege escalations and role changes on user accounts.
- Enable alerts on privilege escalations and role changes.
- Log privileged user changes in the network environment and create an alert for unusual events.
- Establish least privilege controls.
- Implement a security-awareness training program.

Segregate Networks and Functions

Proper network segmentation is a very effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Security architects must consider the overall infrastructure layout, segmentation, and segregation. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders, in the event that they have gained a foothold somewhere inside the network.

Physical Separation of Sensitive Information

Local Area Network (LAN) segments are separated by traditional network devices such as routers. Routers are placed between networks to create boundaries, increase the number of broadcast domains, and effectively filter users' broadcast traffic. These boundaries can be used to contain security breaches by restricting traffic to separate segments and can even shut down segments of the network during an intrusion, restricting adversary access.

Recommendations:

- Implement Principles of Least Privilege and need-to-know when designing network segments.
- Separate sensitive information and security requirements into network segments.
- Apply security recommendations and secure configurations to all network segments and network layers.

Virtual Separation of Sensitive Information

As technologies change, new strategies are developed to improve IT efficiencies and network security controls. Virtual separation is the logical isolation of networks on the same physical network. The same physical segmentation design principles apply to virtual segmentation but no additional hardware is required. Existing technologies can be used to prevent an intruder from breaching other internal network segments.

Recommendations:

- Use Private Virtual LANs to isolate a user from the rest of the broadcast domains.
- Use Virtual Routing and Forwarding (VRF) technology to segment network traffic over multiple routing tables simultaneously on a single router.
- Use VPNs to securely extend a host/network by tunneling through public or private networks.

Additional Best Practices

- Implement a vulnerability assessment and remediation program.
- Encrypt all sensitive data in transit and at rest.
- Create an insider threat program.
- Assign additional personnel to review logging and alerting data.
- Complete independent security (not compliance) audits.
- Create an information sharing program.
- Complete and maintain network and system documentation to aid in timely incident response, including:
  - Network diagrams,
  - Asset owners,
  - Type of asset, and
  - An up-to-date incident response plan.

RESOURCES

- https://www.cisa.gov/insights
- https://www.us-cert.gov/ncas/alerts/TA18-276A
- https://us-cert.cisa.gov/ncas/alerts/aa20-120a
- https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf
- https://www.cyber.gov.au/acsc/view-all-content/publications/preparing-and-responding-cyber-security-incidents
- https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

- https://www.cyber.gov.au/acsc/view-all-content/guidance/managing-cyber-security-incidents
- https://www.ncsc.gov.uk/collection/incident-management
- https://www.ncsc.govt.nz/guidance/incident-management/
- https://cyber.gc.ca/en/publications
- https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
- https://cyber.gc.ca/en/guidance/1-introduction-itsg-22
- https://www.cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38