TLP:WHITE

NCCIC

Targeted Cyber Intrusion Detection and Mitigation Strategies (Update B)

Released:
Wednesday, February 6, 2013 - 19:00

Overview

Sophisticated and targeted cyber intrusions have increased in recent months against owners and operators of industrial control systems across multiple critical infrastructure sectors. ICS-CERT developed the following guidance to provide basic recommendations for owners and operators of critical infrastructure to mitigate the impacts of cyber attacks and enhance their network security posture.

This guidance applies to organizations whose networks have been compromised by a cyber attack as well as to those desiring to improve their network security preparedness to respond to a cyber incident. The guidance is relevant to both enterprise and control system networks, particularly where interconnectivity could allow adversaries to move laterally within and between networks. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to implementing defensive measures to avoid any negative impact to normal operations.

The guidance is organized into several topical areas and provides network administrators with concepts for improving detection of intrusions, preventing lateral movement of threat actors, and controlling access to the various segments of a network. The guidance is in the form of “what” should be done and “why” it is important. The “how” of implementation is the responsibility of each organization and is dependent on individual needs, network topology, and operational requirements.

Guidance and Recommended Practices

The impacts of a cyber intrusion will likely be different for every organization depending on the nature of the compromise and the organization’s capabilities to respond. Each organization must assess its particular situation, identify the criticality of the impacted devices, and develop a prioritized course of action. Unfortunately, a simple and prescriptive remedy that can be applied uniformly to every organization does not exist. However, basic principles and recommendations exist that are essential to maintaining a sound network security posture and that will provide the necessary capabilities to respond to an incident.

Organizations that suspect a compromise should first consider how to preserve forensic data and stop movement of the intruder through the network. While the tendency might be to first find and eliminate the intruder, unless adequate steps are taken to preserve data and prevent lateral movement, the recovery processes will not likely be successful. Also, while disconnecting compromised workstations

TLP:WHITE

from the network is important, unless the data that are essential to identifying the intruder are preserved, future detection will be more challenging. Therefore, the guidance listed in the Preserving Forensic Data and Credential Management sections below should be considered primary actions to help mitigate the spread of compromise through a network.

Also, the need for intrusion detection capabilities cannot be overstated. The ability to detect and identify the source and analyze the extent of a compromise is crucial to rapid incident response, minimizing loss, mitigating exploited weaknesses, and restoring services. Early detection of an incident can limit or even prevent possible damage to control systems and reduces the level of effort required to contain, eradicate, and restore affected systems. Auditing and logging with host-level Domain Name Service (DNS) resolution capabilities are essential for improving detection and determining the depth and breadth of any compromise.

Network segmentation, role-based access control, and application whitelisting are additional concepts discussed in this guidance, which will provide a defensive posture to prevent intruders from moving within a network. These techniques can be more challenging to implement but will provide long-term value.

Preserve Forensic Data

Preserving forensic data is an essential aspect of any incident response plan. The forensic data acquired during the overall incident response process are critical to containing the current intrusion and improving security to defend against the next attack. An organization's network defenders should make note of the following recommendations for retention of essential forensic data:

- Keep detailed notes of all observations, including dates/times, mitigation steps taken/not taken, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.
- Capture a forensic image of the system memory prior to powering down the system.
- When powering down a system, physically pull the plug from the wall rather than gracefully shutting down. Forensic data can be destroyed if the operating system (OS) executes a normal shut down process.
- After shutting down, capture forensic images of the host hard drives.
- Avoid running any antivirus software "after the fact" as the antivirus scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.
- Avoid making any changes to the OS or hardware, including updates and patches, as they might overwrite important information relevant to the analysis. Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts.

When a compromised host is identified, it should be removed from the network for forensic data collection (but not powered off, as noted above). When all available data have been retained from the infected host, the organization should follow established internal policies for recovering the host.

If an organization does not have an adequate incident response plan or the necessary staff to handle a serious cyber incident, it should consult trained forensic investigators to assist with developing a response plan and implementing recovery efforts.

Control system environments have special needs that must be evaluated when establishing a cyber incident response plan. ICS-CERT recommends a review of the CSSP Recommended Practice: Creating Cyber Forensics Plans for Control Systems.[a]

Credential Management

--------- Begin Update B Part 1 of 1 --------

Protecting logon credentials for network hosts is an important consideration when defending a network against lateral movement by an intruder. Attackers trying to compromise those credentials commonly employ tactics such as brute force password hash cracking and a technique referred to as “pass-the-hash.”

Brute force cracking requires the attacker to “guess” the original password by systematically hashing and comparing the results of possible passwords. When a match is found, it indicates a usable password has been identified. The use of “rainbow tables” (large tables of pre-computed hashes) greatly expedites the process. The pass-the-hash technique uses cached password hashes extracted from a victim machine’s memory to gain access to additional machines in the domain.

The following paragraphs describe mitigation techniques to reduce the possible attack vectors for compromising credentials and/or to reduce the network locations where an attacker could use stolen credentials. In addition to this list, Microsoft has also released guidance that discusses methods for protecting user credentials that administrators should consult.[b] Administrators should evaluate each of these techniques and their possible side effects before making any changes to control system networks.

- Proper Permission Management

1. Establish an appropriate privileged account hierarchy for administrative accounts (e.g., Enterprise Administrator, Domain Administrator, help desk accounts). In a proper hierarchal design administrative rights and administrative responsibility are inversely proportional to each other. For example, Domain Administrators (one of the most privileged accounts) should only be used to administer the domain controllers, while a help desk account (an account with several task responsibilities) should have few administrative rights. This design approach should also include decisions about which hosts will allow the accounts and the manner in which the administrator accesses the devices. Exceptions to these policies should be handled through the creation of temporary accounts that are removed after completing the intended task, or through the use of designated management machines that are heavily restricted using ACLs (access control lists) and/or IPSec.[c] These approaches make it more difficult for attackers to compromise the Domain Administrator account, Enterprise Administrator account, domain controller, exchange server, and other high value targets.

1. **Note**: Newer versions of Windows provide greater levels of granularity for assigning privileges, enabling better silos for safeguarding permissions.

2. Carefully consider the risks before granting administrative rights to users on their own machines. The machine is at greater risk of compromise and credentials theft when Web browsing or reading email as an administrator.
3. Restrict the use of the SeDebugPrivilege to those users that actually need it. An attacker can use this privilege to perform DLL injection, a technique used by the majority of the pass-the-hash tools, and by other malware. By default, the entire Administrators group receives this privilege, but it should be more restricted than that. Create a specific Debug user, and assign that account the right to use the privilege via the “run as” command, thereby allowing only temporary privilege escalation.[d]

- Network/System Design and Policies

1. Apply the principle of Internet, DMZ, and intranet zones throughout the network to isolate different trust sectors. A workstation rarely needs to talk to another workstation, or to all the servers. Use infrastructure devices and software to create security zones that group users who need to communicate with each other. This helps to slow or prevent an intruder’s lateral network movement.[e] Use host-based firewalls to restrict incoming connections as another method for impeding unneeded inter-host communication.
2. Exercise caution when using a common baseline image to load company workstations if the machine contains active local user accounts, because all images will share the same password. This is especially risky if the owner has not disabled the local administrator accounts. An attacker could use those common credentials to quickly compromise all the machines loaded with this image. For that reason, IT administrators should consider disabling or removing local machine accounts, or at least ensure that local accounts across the network have unique passwords.[f]
3. Require that all machines be rebooted immediately after being used by a privileged user. The reboot process clears the user’s credentials from memory, a common target of pass-the-hash tools.[g]
4. ICS-CERT also recommends that organizations move away from using LAN Manager (LM) hashes,[h] where possible. LM hashes are inherently weak and can be broken relatively quickly, which allows an adversary to use the actual password instead of relying on a pass-the-hash attack. Not all companies will be able to make this switch because some legacy systems are incompatible. However, system administrators should make every effort to migrate away from those systems to increase their network wide security posture.
    1. **Note**: When performing a global password reset, network managers should simultaneously disable LM hashes to avoid the need for another global password reset when that method of password storage is disabled.
5. Organizations should consider moving to a multi-factor authentication system (e.g., smart cards) or at least ensure users choose complex passwords that change regularly.

--------- End Update B Part 1 of 1 --------

Increase Logging Capabilities

System and network device logs provide valuable records of activities that have occurred. Logs may contain indicators of compromise, command and control (C2) communications, exfiltrated data, remote access logins, and more. The following types of logging should be considered.

- firewall,
- proxy,
- DNS,
- IDS,
- packet captures,
- flow data from routers and switches, and
- host and application logs.

DNS Logging with Host Level Granularity

When implementing increased auditing and logging capabilities, organizations should particularly consider enabling host level DNS resolution. Because most malware uses domain name-based C2 servers (versus hard coded IP based C2), it is essential for network defenders to have full awareness of DNS requests throughout the enterprise. ICS-CERT recommends that organizations deploy host level granularity in DNS logging to give network administrators the ability to identify which internal host (by hostname or IP address) originated a specific DNS request and to identify hosts that have connected to malicious domains. This is one of the best indicators of compromise.

To ensure that all DNS resolutions are captured and logged, network administrators should ensure that all DNS requests go through company DNS servers. In addition, the company servers should only service DNS requests from authorized company hosts.

Logging these data also provides a historical view of when and how the malware has moved through the network after the initial infection. This information helps to determine the full breadth and depth of the compromise.

Retention of logs is essential since sophisticated threat actors tend to maintain a presence for long periods of time and will often lay dormant for many months. If possible, log retention for a year or two would be ideal and will provide the ability to go back and possibly find the time of initial infection and indictors of a compromise.

In most configurations, host-level DNS logging is disabled by default and must be specifically enabled on authorized DNS resolvers. ICS-CERT recommends that organizations evaluate their DNS solution and enable this logging feature.

Audit Network Hosts for Suspicious Files

MD5 hashes are digital fingerprints used to identify files. Changing just one byte in a file will result in a different hash. If an MD5 hash is known to belong to a malicious file, any file with a matching hash should be considered malicious, regardless of the filename.

The ability to perform an enterprise wide host level search for MD5 hashes is a powerful organizational tool for incident response. MD5 hashes are among the key indicators that can be used to identify the presence of an intruder.

Multiple host-based IDS and forensic tools, as well as plug-ins to enterprise configuration management software, offer this functionality.

Network Segmentation

Network segmentation involves separating one large network into smaller functional networks using firewalls, switches, and other similar devices. Effective network segmentation restricts communication between networks and reduces the extent to which an adversary can move across the network.

Organizations should decide which departments, applications, services, and assets should reside on each network segment. Implementation of network segmentation can be a long-term project and should include careful planning, implementation, and regular maintenance.

In an ideal world, the business and control system networks would be physically separated. However, this is not practical in many situations. In practice, firewalls and data diodes are good options for segmenting networks. A data diode allows only one-way communication between network segments and can be used to ensure that network data only flows out of the control systems network. Firewalls allow two-way communication between networks and risks of exposure if the firewall is not well configured.

The network should also include one or more demilitarized zone (DMZ) segments grouped by function such that the attack surface at each segment is minimized. DMZs should include the organization's external services that are exposed to the Internet or any critical systems that are accessed from multiple internal network segments. Firewalls should control communication between DMZs and internal/external hosts.

Strict Role-Based Access Control

Role-based user access control grants or denies access to resources based on job function. Active Directory (AD) implements role-based user access control through group policies. Groups provide logical network segmentation and prevent users from accessing machines that are not necessary for job performance.

Organizations should define the roles and permissions needed for each group to perform its duties. Implementing strict role-based access control allows better auditing and reduces risk by minimizing the privileges associated with each group. In addition, this logical network segmentation makes it harder for an adversary to move laterally through the network after the initial intrusion.

Application Whitelisting

Application whitelisting permits the execution of explicitly allowed (or whitelisted) software and blocks execution of everything else. This eliminates the execution of unknown executables, including malware.

One challenge when using application whitelisting in business networks is managing the constantly changing list of allowed applications. That burden is significantly reduced in control systems environments, because the set of applications that run in those systems is essentially static. ICS-CERT recommends deploying application whitelisting on the control systems and business networks wherever applicable. In particular, application whitelisting could be appropriate for business servers such as mail servers and domain controllers.

Additional Recommended Practices

ICS-CERT recommends that users take the following standard measures to protect themselves from social engineering attacks.

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to *Recognizing and Avoiding Email Scams* for more information on avoiding email scams.
3. Refer to *Avoiding Social Engineering and Phishing Attacks* for more information on social engineering attacks.

ICS-CERT encourages asset owners to take the following additional defensive measures.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Keep software up to date with a patch management plan.[i]
- Develop, review, and maintain an up-to-date incident response plan.[j]
- Keep patches up to date whenever possible.

---

a. Recommended Practice: Creating Cyber Forensics Plans for Control Systems (2008), http://www.us-cert.gov/controlsystems/practices/documents/ForensicsRP.pdf, Web site last accessed January 22, 2013.

b. http://www.microsoft.com/en-us/download/details.aspx?id=36036, Microsoft Download Center “Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques” (3.3 MB), last accessed January 22, 2013.

c. http://www.sans.org/readingroom/whitepapers/testing/pass-the-hash-attack... , Web site accessed on January 22, 2013.

d. http://www.sans.org/readingroom/whitepapers/testing/crack-pass-hash33219, Web site accessed on January 22, 2013.

e. http://www.infoworld.com/d/security-central/isolated-security-zones-yiel..., Web site accessed on January 22, 2013.

f. http://www.nsa.gov/ia/files/vtechrep/ManageableNetworkPlan.pdf, Web site accessed on January 22, 2013.

g. http://www.infoworld.com/d/security-central/isolated-security-zones-yiel..., Web site accessed on January 22, 2013.

h. http://supportmicrosoft.com/kb/299656 “How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases,” Web site last accessed January 22, 2013.

i. Recommended Practice for Patch management of Control Systems, http://ics-cert.us-cert.gov/content/recommended-practices#nogo, Web site last accessed January 22, 2013.

j. Developing an ICS Cybersecurity Incident Response plan, http://ics-cert.us-cert.gov/content/recommended-practices#nogo, Web site last accessed January 22, 2013.