Operating on a Compromised Network

This paper provides guidance for operating a compromised network for some limited period of time until trust can be reestablished, while minimizing information loss and the damage a cyber-adversary can inflict. The guidance ranges from standard network security best practices to actions that are focused specifically on reducing the risk of operating on the compromised network. Although this paper is primarily written for system administrators and end users, information security managers, network owners, and decision makers must be involved in implementing this guidance to ensure the best balance of mission and security.

Networks are complex and diverse, as are the types and severity of threats and attacks against them. Therefore, the guidance below is more generic. Some of the mitigation actions will improve overall security with little to no cost and should be implemented by default. Other mitigations may have major impact on operational usage and require careful thought.

Strike a balance between doing too little and doing too much. Over-reacting to an incident could reduce mission capability or result in a loss of functionality that endangers lives, operations and property; underreacting could expose missions to further compromise.

Assumptions

The following are assumptions for this paper:

- Best effort has been undertaken to detect, prevent and clean any known infections from the network. However, the network is still assumed to be compromised because of what is not known. Confidentiality, integrity, or availability compromises are all assumed to be possible.
- There are activities underway to rebuild and reestablish the necessary trust in the compromised network (e.g. re-imaging/replacement of computing platforms and network fabric) while it is being used.
- There will be some reduction in functionality available to network users, and using the network may be more inconvenient (e.g. use of specific types of removable media may be restricted, certain protocols may not be allowed, and some applications may not be available).

General Guidance

Develop an action plan for operating on the compromised network. The plan should prioritize mitigation actions tailored for the specific network and situation, assign responsibility for each action, and identify plans for overall reestablishment of trust on the network. Do not universally apply all of the mitigation actions below without thorough consideration. Some mitigations may not be able to be implemented in certain situations because they would make the network/system unusable. If possible, test the mitigations on another network first. The following table provides specific mitigation items. Each item is annotated with:

- Importance of implementation categorized as high (H), medium (M), or low (L)
- Whether the mitigation should be considered a standard security practice (SSP) implemented at all times or just used when the network is considered compromised (CSP)
- Whether the mitigation needs to be primarily implemented by an information assurance manager (M), system administrator (SA), or user (U)

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
1.	Establish out of band communications, especially when discussing any activity associated with the compromise or other sensitive topics. Consider using phones or fax on a separate network for the most critical communications instead of e-mail or other communications services on the compromised network. If e-mail communication is necessary, encrypt and digitally sign e-mail if possible.	High	CSP	User
2.	Establish and train dedicated network security teams that are responsible for proactively monitoring, implementing, enforcing, and otherwise working security for the compromised network. Additional help desk staffing will also be necessary to address increased user requests and problems.	High	CSP	M
3.	Immediately inform users of the severity of the threat, the restrictions under which they are operating, the reasons for the added security measures, and the anticipated effect on their mission activities. Clearly identify actions they will be required to take to help reduce risk to mission activities.	High	CSP	M, SA
4.	Follow organizational procedures for dealing with any newly infected machines found on the network. If no procedures exist, disconnect the machine from the network and leave it powered up to preserve memory contents for forensics analysis.	High	SSP	SA
5.	Identify critical assets and remove them from the network (e.g. documentation, source code). These should only be re-introduced after a thorough risk analysis has been performed after the compromise. Strongly consider keeping these critical assets on a physically separated network. At a minimum, utilize a logically separated network to protect the assets.	High	CSP	M, SA

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
6.	Ensure that anti-virus (AV) and anti-spyware software capable of detecting, preventing, and cleaning known malicious code is deployed to all servers and workstations. Update AV signature files on a regular basis. Require that complete scans are regularly scheduled and successfully completed. Consider using multiple vendor products to increase the chances of detecting or preventing new infections.	High	SSP	SA
7.	Leverage threat intelligence clouds (e.g., AV file reputation and DNS reputation services) to obtain protection from the most recent threats before they become available in AV and security product updates.	High	SSP	SA
8.	Force a password change across all networks, preferably just after the detection of the compromise and again after other high importance mitigation actions are implemented. This includes all computer accounts, databases, remote logons to network components, etc. On Windows® systems, accounts with smart cards actually have an associated Windows password hash, which should be flushed and regenerated. Consider implementing a policy for more frequent password changes. Password changes on accounts, such as database accounts that are accessed via applications, must be coordinated with application owners to avoid users of the application being locked out.	High	CSP	SA, User
9.	Apply and use all applicable security configuration guidance from Microsoft and other software vendors for servers and client machines to the greatest extent possible. Use the “High” security settings. Use automated mechanisms (e.g. Microsoft Group Policy or other security configuration tools) to control configurations where possible.	High	SSP, CSP (highest setting)	SA

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
10.	Lock down web browser security settings to “High” security, and disable all JavaScript®, ActiveX® controls, and similar scripting capabilities. Allow such scripts by exception only when it is known that a critical mission function cannot be performed without them. Assess user complaints to determine the need to readjust exceptions	High	SSP, CSP (highest setting)	SA
11.	Ensure all software used on the network is up-to-date on patches and at the most current version as much as possible	High	SSP	SA
12.	Deploy an anti-exploitation tool, such as Microsoft’s Enhanced Mitigation Experience Toolkit (EMET), to protect against common classes of exploitation.	High	SSP	SA
13.	Restrict the usage of and access to administrative accounts on the network. Remove standard users from privileged security groups. Restrict systems that privileged accounts can access. Ensure administrative accounts do not have e-mail or Internet access.	High	SSP	SA
14.	Minimize services and applications being used on the network. Turn off most services unless necessary for mission critical activities, remove unnecessary/unauthorized programs, and disable unneeded interfaces in BIOS®. Use group policy where possible to enforce this	High	SSP	SA
15.	Mark system backups made between the time of the infection and its discovery as high risk, and label with enough information that administrators can recognize the reason for special treatment. If data from these backups is needed, it should be restored using an isolated/standalone network and evaluated and cleaned. These backups must not be destroyed. A new, full set of backups should be performed and marked accordingly for replaced, cleaned or repaired machines.	High	CSP	SA

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
16.	Maintain and actively monitor a centralized logging solution that keeps track of all anomalous and potentially malicious activities on their network. In addition to logging, network packet capture can provide invaluable information to incident responders. Ensure that all relevant devices have logging enabled and aggregated to a Security Information and Event Management (SIEM) system or other centralized monitoring solution.	High	SSP	SA
17.	Implement an SSL/TLS inspection capability to gain full insight into the traffic passing through the network perimeter. Enable the SSL/TLS inspection feature of the organization's web proxy devices. Ideally, all connections should be evaluated to determine whether or not they are permitted by policy and reveal evidence of malicious content. At a minimum, a more fine-grained Internet access policy should be defined to identify which types of traffic would be allowed to pass, which types of traffic would be inspected, and which types of traffic would be blocked.	High	CSP	SA
18.	Implement integrity monitoring to detect changes in files that should not normally change (e.g. operating system files). When possible, use tools that create a trusted baseline of cryptographic hashes that are compared to periodic file snapshots to find/detect changes. The process should also list new files and files which have been deleted	High	SSP	SA
19.	Use secure, authenticated login for remote access to servers, desktops, network devices and other network equipment instead of plain text services such as Telnet and FTP. For devices that cannot support secure login, implement strict IP address restrictions to permit remote access only from a small set of secure local servers.	High	SSP	SA

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
20.	Limit workstation-to-workstation communication to thwart an adversary's ability to move laterally within the network. Microsoft Windows systems can be configured to limit where workstations can communicate on the network via Windows Firewall or Group Policy security settings. Alternately, logical segmentation (e.g. via virtual LANs) can serve to limit communication.	High	SSP	SA
21.	Deploy a host intrusion prevention (HIPS) capability on workstations and servers. More effective than standard signature-based capabilities, HIPS technology focuses on threat behaviors and can better scale to entire sets of intrusion activities.	High	SSP	SA
22.	Implement application whitelisting to allow a limited set of approved programs to run, while all other programs and most malware are blocked from running by default. Use a third-party application (e.g. a host based security application) such as Microsoft's AppLocker® on Windows operating systems.	High	SSP	SA
23.	Restrict and/or limit the use of removable media and devices that connect to USB ports. Ensure that any media used is purchased or acquired only from authorized sources. When possible, use third party software or, for Windows systems, Active Directory® Group Policy to control use of removable media and USB access. Consider treating thumb drives and similar removable media as accountable property and registered to a specific owner for a specific purpose. Scan and clean these devices on a "trusted scanner system" that implements multiple anti-virus (AV) software after each use. Do not allow personal electronic devices (e.g. phones, tablets) to connect via USB, even to charge the devices.	High	SSP	SA, User

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
24.	Revalidate all accounts, including those for users, administrative roles, devices, and automated services. This includes accounts on servers, computers, and routers and other network components, especially where remote login by those accounts is possible. Disable all accounts that cannot be validated.	High	SSP	SA
25.	Use encrypted file storage based on individual user keys (e.g. Public Key Infrastructure - PKI) where possible to limit future loss of data. Move all user data storage from local storage (e.g. C drive) to network storage to minimize storage locations and to ease reimaging/replacement of infected machines. Ensure all such user data is scanned and cleaned	Medium	CSP	SA, User
26.	Ensure that all wireless capabilities are disabled on laptops, routers, etc., or that their need is validated and that they are properly secured. When possible, disable wireless in BIOS or in the operating system instead of in an application. Consider establishing monitoring for unauthorized local wireless access activities.	Medium	CSP	SA
27.	Consider segmenting the network to help isolate critical servers or other platforms. For example, critical mission servers could be firewalled off and controlled to limit access to them. System administration workstations could be isolated in a similar way.	Medium	SSP	SA
28.	Where already available in existing network fabric, use Network Access Control capabilities to enforce configuration level of computer platforms and to detect and prevent connection of unauthorized network devices.	Medium	SSP	SA

Item #	Mitigation Guidance	Implementation Importance (High, Medium, or Low)	Standard Security Practice (SSP) or Compromised Security Practice (CSP)	Implemented by IA Manager (M), System Administrator (SA), and/or User
29.	Restrict remote activity. Access to systems from outside of an enclave should only be allowed from organization owned devices with two-factor authentication through a hardened VPN gateway with split-tunneling prohibited. Implement a Virtual Desktop type system (e.g. Citrix, Terminal Server, Outlook Web Access, etc.) on this VPN gateway to establish security enforcement and monitoring points. If possible, restrict VPN usage to users that require it (e.g. traveling users), and force other users to come into the office to cut down on VPN connection attempts. This allows VPN connections to be analyzed to look for anomalies, such as logins from IP addresses where organization personnel are not physically located.	Medium	SSP, CSP (discontinue use of VPN)	SA
30.	In Windows network environments, closely re-examine all trust relationships for the various Windows domains, particularly those in a “transitive trust” relationship. Consider severing the trust to prevent spread of the compromise to other networks.	Medium	SSP, CSP (severing trust)	SA
31.	Consider creating a Virtual Private Network (VPN) on top of the compromised network for use by the most critical users or missions. As the workstations of critical users are repaired they could be added to this VPN until such time as the entire network has been repaired.	Low	CSP	SA
32.	Require users to power cycle their computers at least weekly, and require that they select “Restart” when they logoff rather than “Logoff” to reduce the persistence of memory based attacks.	Low	CSP	User
33.	Identify security critical registry keys/settings and set Group Policy to audit changes to them. The policy would cause entries in the security event log which could then be reviewed regularly to determine anomalous behavior. This is in addition to AV and HIPS. Perhaps limit this to the most critical machines on the network (e.g. servers, critical users).	Low	CSP	SA

Reestablishing trust in Critical Network Components

Note that the trust re-establishment areas and activities suggested here are not all inclusive. Activities needed to completely clean the network are beyond the scope of this paper.

Reestablish/regain positive control of network management and administration.

Systems used by system administrators for performing administrative functions must be replaced or repaired. Other assets that must be considered for early replacement or repair are as follows:

- Systems performing important network and security management activities such as domain controllers and workstations used for PKI administration
- Workstations used by critical users such as an important senior officials who are more likely to be targeted than average users
- Servers providing critical mission services such as command and control, strategic communications, Active Directory, e-mail, etc.
- Critical network infrastructure components (e.g. certain routers, switches, firewalls)

Replace and/or repair devices

Some critical network assets must be trusted even on a compromised network. Such assets should be replaced or repaired as soon as possible, even if they are not suspected of having been compromised. To replace or repair a device:

- Re-flash the BIOS with a known good configuration. Configure BIOS security/password when available.
- Replace the hard drive for the most critical platforms. Overwriting hard drives using organization approved methods may be acceptable for some less critical platforms.
- Reimage the hard drive. Create a new secure baseline image that includes an operating system and approved applications that are hardened according to security base practice configurations mentioned above.
    - Use the latest versions of operating systems and applications. Windows client operating systems should be at least Windows 7® (for workstations) or Windows Server 2008 R2® (for servers) with the latest service pack. If possible, client machines should be upgraded to Windows 8.1 or later to take advantage of newer security features.
    - Within the image, include best practice security capabilities such as application whitelisting, AV, and anti-exploitation features described above. Establish an automated process to measure and report the systems' state of compliance to the established security baselines on a weekly basis.
- Don't use backups to reimage as these may be infected. Re-imaging must be done off-line (i.e. in a separate provisioning lab, not on the operational network) to reduce the risk of re-infection. Reestablish system backups as necessary based on the reimaged/new machines.

Disclaimer of Endorsement

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov