Compromised Personal Network Indicators and Mitigations

More and more government workers are teleworking, using Government Furnished Equipment (GFE) for official work and connecting them through personal networks. Cybersecurity is a crucial priority for these users to ensure their data and networks remain secure and uncompromised. This includes being able to identify indicators of a network compromise and pursue potential mitigations. This knowledge aids users in safeguarding their personal networks and data.

Personal networks are those used in homes for personal use or telework, such as a home network provided by a residential Internet Service Provider (ISP). These networks usually consist of a router or wireless access points connecting devices to the Internet. They may have computers, mobile devices, gaming systems, or a variety of Internet of Things (IoT) devices connected to them. When setting up these personal networks, implementing proper security from the beginning is crucial.[1] While there is no way to ensure that personal networks will be completely secured from attacks—attackers are persistent and continue to find ways to circumvent security controls—users can still take steps to help prevent future attacks [1].

This document provides guidance to users who have received authorization to connect GFE to personal networks. It describes potential indicators of compromise and mitigation practices that can be used to minimize damage if the network is believed to be compromised. If indicators of compromise, as outlined in this document, are observed, then follow the guidance to mitigate the compromise. Users can apply this guidance to any computers, mobile devices, or IoT devices that they connect to personal networks. The best practices included here are not meant to fully mitigate a compromised network on a large business or corporate scale.

In the event of a suspected compromise, some users of personal networks may prefer to seek expert support in lieu of attempting to mitigate the issue themselves. Forensic expert support typically involves analyzing volatile data in compromised devices. The guidance here includes steps that involve rebooting devices, as well as other steps that could corrupt or destroy volatile data that is crucial to a forensic investigation. **Users who seek expert support should disregard the remainder of this paper and take guidance from the expert.**

Indicators of a personal network compromise

Due to the increasing amount of devices connected to personal networks, indicators of compromise may come in a variety of forms. While recommendations may change as technology evolves, and vulnerabilities and threats continue to develop, users should always be aware of the basic indicators of a compromised network so proper steps can be taken to mitigate or eliminate the threat. The following table lists common indicators that a network may be compromised. The table is not comprehensive, and only lists some of the most obvious signs of compromise. It should also be noted that many of these indicators can also be caused by non-malicious issues.

Table I: Indicators That Personal Networks Could be Compromised

Type of Compromise	Indicators of Compromise	Description of Suspicious Activity
Compromised Router	Router Password Changes	Existing router login credentials that were not changed by the user become ineffective and/or foreign devices are found on the personal network.
	Modified Connectivity	Router/wireless status shows a different router/SSID connected.
Compromised Router or Malware	Browser Redirects	User intends to access a certain site and has been redirected to a different, unintended site. Redirection of banking sites in particular can lead to massive financial theft. This can be done by malware on the device or on the network.

[1] Please refer to "Best Practices for Keeping Your Home Network Secure" for preventative measures that can help all users improve the chances of avoiding network or device compromise.

Type of Compromise	Indicators of Compromise	Description of Suspicious Activity
Malware (e.g. Spyware, Adware, Rootkits)	Devices Functioning Without User Input	Computer cursors begin to move on their own, web cameras and microphones activate without being enabled by the user, or a device turns on by itself.
	False Anti-Virus / Anti-Malware Alerts	Misleading notifications resembling reputable security programs appear on device screens. These often look different from the usual alerts and may appear within web pages (in places where it seems like they do not belong).
	Unexpected Hardware Displays	Camera light/LED is "on" unexpectedly.
	Inactivity Faults	"Off" computer is hot/warm after extended periods of time being turned off. Mobile devices in particular should not normally run hot when not in use.
	Tampered Logs	The website history and/or cache is reset (unrelated to user's manual reset or scheduled reset).
	Malfunctioning Anti-virus or Anti-malware	Anti-virus/anti-malware task manager or registry will not start up, is put in a reduced state, or completely disabled, but not by the user.
	Taxed Memory	The Task Manager shows applications or services with uncharacteristic heavy memory usage.
	Modified Parameters	The clock "time" is reset or appears different from the current time.
	Operation Instability	Periodic device crashes. Devices reboot on their own or during times disassociated from updates.
	Usage Strain	Portable network devices (e.g., laptop, mobile device) hold power for drastically shorter periods of time. This can also be caused by normal battery wear and poor charging practices.
	Phishing Emails[2]	Emails or messages sent to the user claiming to have the person's username, password, or have installed a rootkit or key logger on the device. This can also be an attempt to compromise the user.
	Changed Software Displays	New or different application icons on the screen. This can also be caused by legitimate software updates.
	Unexpected Advertisements	Advertisements appear randomly on device screens without a browser being opened.
Ransomware	Ransomware Messages	Messages appear or completely lock the device and may restrict access to content until the victim pays a specified fee.
	Unexpected File Encryption	Files or folders randomly become encrypted and the user is unable to open them.
Compromised Account	Sharing Exposure	Collaborative or teleconference applications show previous connections different from those initiated by the user.

[2] Phishing emails could also be social engineering attempts to gain access to a device or network.

Type of Compromise	Indicators of Compromise	Description of Suspicious Activity
	Unexpected Login Notifications	Many services provide notifications (e.g. by email or text) when new devices connect to an account on the service. Sometimes they will give the option to block the new device. Pay attention to these notifications and act on them.
	Unintentional Sent Messages[3]	Family, friends, or co-workers receive messages or invitations supposedly from the user but not sent by the user.
	Unusual Displays	"Please update or change password" prompts appear (which may look different from normal prompt).

What to do if you suspect a personal network is compromised

If these indicators lead a user to suspect their personal network is compromised, steps can be taken to mitigate the damage or eliminate the network threat altogether. This section recommends general steps for responding to suspicious activity as well as more aggressive actions that can be taken depending on the severity of the compromise.

Responding to generally suspicious activity

The following are recommended actions—in no particular order—for users to take in response to some common indicators. It is advised that users should seek expert support if they do not have the required skillset to perform the actions.

Compromised Router

- Reboot the device.
- Disable local/remote administration.
- Reset the device to factory settings.
- Update the software/firmware.
- Change passwords on all accounts.
- Enable multi-factor authentication if applicable.

Malware (e.g. Spyware, Adware, Rootkits)

- Disconnect suspected compromised devices from the network.
- Sign into accounts on a separate, trusted device and change all passwords that were used on the compromised device.
- Sign into accounts on a separate, trusted device and sign all unknown or untrusted devices out of online services.
- Run an anti-virus/redirection scan on the device.
- Remove the malware.
- Restore the device to a previously backed up good state.
- Run automatic updates for the operating system and software.

Ransomware

- Do **NOT** pay the ransom.
- Disconnect suspected compromised devices from the network.
- Run an anti-virus/redirection scan on the device.
- Remove the malware if possible.
- Certain ransomware variants have recovery programs or keys available (only use from reputable sources).
- Reset the device to factory settings.
- Restore the device to a previously backed up good state.
- Run automatic updates for the operating system and software.
- Using the service's online portal, sign all untrusted devices out of services such as social media accounts.

[3] In the case of unintentional sent messages, users should check to see if the message came from their actual account or if a duplicate account was created.

- Change all passwords that were used on the compromised device.

Compromised Account

- Change passwords on all accounts.
- Enable multi-factor authentication if applicable.
- Remove social media accounts and applications.
- Reset the device to factory settings.
- If contact list may have been stolen, warn contacts to avoid clicking links that appear to come from the compromised account.

Aggressive eradication of threats on a compromised personal network

The actions recommended in this section are more aggressive: they attempt to eliminate the threat on a device or personal network. If necessary, these steps may be taken if a user has the required knowledge/skillset, as some actions may result in the loss of data or connectivity. It is advised that users should seek expert support if desired.

Disconnect all devices from the network and reset network devices

This should include all computers, mobile devices, routers, access points, and IoT devices connected to the network. Once disconnected, perform a factory reset on all of the network devices to include ISP-supplied devices. If desired, users can acquire personal routers or access points that can be connected to the ISP equipment, as ISP provided equipment may have potentially compromised administrative credentials. By using personal routers or access points, users can add an additional layer of security to the personal network.

Perform a factory reset on previously connected devices

Factory reset all mobile devices, desktops, and laptops. When restoring the devices, only use the original operating system media for desktops and laptops and update them as soon as possible. For mobile devices, perform a full reset to include backup/restore of data.

Immediately change passwords and require a new sign in from all linked devices

This should include all bank, email, social media, wireless access, and administrator router console passwords. This mitigation is crucial as attackers may have acquired user credentials during the compromise. If this is the case, the attackers will still have access to the accounts unless the credentials are changed.

Safeguard personal networks and data

By following the mitigations outlined within this document, users should be able to eradicate and/or minimize the damage caused by a compromised personal network. If suspicious activity continues after performing mitigation steps, users should seek expert advice to assist in further resolving the compromise or other issue.

Works Cited

[1] "Best Practices for Keeping Your Home Network Secure." NSA, 2018. [Online] Available at: https://media.defense.gov/2019/Jul/16/2002158056/-1/-1/0/CSI-BEST-PRACTICES-FOR-KEEPING-HOME-NETWORK-SECURE.PDF

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

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