Eighth Army

CYBERSECURITY BULLETIN Issue 24-01 – November 2023

8th Army G6 Cybersecurity Readiness Campaign Plan Issue: 24-01 Subject: Removable Media and USB Devices Security Awareness Tips and Best Practices

A quarterly bulletin to promote cybersecurity awareness to Eighth Army Users

Cybersecurity Best Practices – Removeable Media and USB Devices

This Quarterly 8A G6 Cybersecurity Culture Campaign bulletin focuses on **"NOT"** connecting unauthorized USB devices to government computers, safety measures and best practices regarding USB devices and removable media.

"Everyday is a battle in the Cyber domain and everyone is important to that fight. Our enemies know that the actions or inactions of our own teammates pose the biggest threat to our warfighting networks. Lapses in cyber hygiene often result in significant loss of productivity, and at worst, compromise information and systems. As cyber threats evolve, we can't take anything for granted. This is our call to action and all of us must do our part in safeguarding digital assets."

- COL Les Thompson, 8A ACoS G6

Cybersecurity Bulletin Issue 24-01, November 2023

What is Removable Media?

Removable media includes flash media, external hard drives, optical discs, and music players. Other mobile computing and portable electronic devices (PEDs), including laptops, tablets, Bluetooth devices, and smartphones, have similar features. Whether flash media or a mobile device, the same rules, protections, dangers, and risks, all detailed below, are applicable.

1. **USB devices are convenient for both users and attackers.** USB drives are inexpensive, readily available, and portable. These characteristics make them popular amongst users for storing and transferring files as well as an appealing attack vector for adversaries.

2. **Malware infection can easily occur.** Attackers can use USB drives to infect computers with malware that can detect when the USB drive is plugged into a computer. The malware then downloads malicious code onto the USB drive and when it is plugged into another computer, the infection spreads. Some attackers have also targeted the supply chain, infecting items such as electronic picture frames and USB drives during production. When users purchase and plug these infected products into their computers, malware is installed.

3. **Data can be easily stolen or lost.** Attackers may use their USB drives to steal information directly. An attacker with physical access to a computer can download information directly onto a USB drive. Even computers that are turned off may be vulnerable because a computer's memory is still active for several minutes without power. If an attacker plugs a USB drive into the computer during that time and quickly reboots the system from the USB drive, they can retrieve the computer's memory, including sensitive data such as passwords, and encryption keys. This attack can be difficult to even detect. Aside from these attack vectors, USB drives are easily lost and stolen. If the data is not backed up, the loss of a USB drive can mean hours of lost work. Finally, on an unencrypted drive, all data is accessible to whoever finds or steals it.

Best Practices in using Removable Media and USB Devices

Implementing and following best practices can help reduce the impact of potential cyber-attacks. Here are some tools and measures to apply and follow to best reduce and avoid catastrophic consequences that may affect your personal or organizational security.

1. **Beware of devices of unknown or questionable origin.** If a device is found at your workplace, give it to the appropriate authorities (your organization's cybersecurity team). Do not plug it into any computer to view the contents or to try to identify the owner.

2. **Ensure your personal PCs and laptops are adequately protected.** Proper configuration such as disabling the Autorun feature can prevent malicious code on an infected USB drive from opening automatically. Additionally, using and maintaining antivirus software, a firewall, and ensuring virus definitions and software updates are current, all make your device less vulnerable to attacks associated with USB devices and removeable media.

3. **Beware when travelling with and using mobile devices in public.** Always maintain visual or physical control of your devices, especially when going through airport security checkpoints. Be aware that information sent over public Wi-Fi connections can be exposed to theft, and the device may be exposed to malware. Utilizing a Virtual Private Network (VPN) can help reduce risks associated with public Wi-Fi. Be careful of information visible on your device when using it in public and never discuss sensitive information in public, even if using a secure device.

4. **Ensure data on Removeable Media, PED, and USB devices is properly safeguarded.** Be sure to lock your device when not in use and to enable automatic screen locking after a period of inactivity. Make sure sensitive data on all devices is encrypted when possible. Also, when possible, ensure your devices are utilizing two-factor authentication such as biometrics or one-time-passwords (OTP).

5. **Exercise caution when using devices that support near field communication (NFC) and be aware of GPS on mobile devices.** NFC is a wireless technology employed on smartphones that enables information exchange when devices are in very close proximity and is commonly used for the transmission of credit card payment information (e.g., contactless payments). Similarly, GPS is often utilized on mobile devices and accessed by many applications that may track your location without your knowledge or consent. It is important to keep devices and apps updated, as well as review application permissions to minimize risks associated with these technologies.

6. **DO NOT PLUG SMARTPHONES INTO ANY WORK COMPUTER.** On government-owned computers, unless explicitly authorized by your organization, NEVER plug in any USB drive, smartphone, or other PED into ANY USB port. This includes USB ports found on workstations, thin clients, docking stations and hubs, and even monitors. Even if only for the purpose of charging a device, and even if no data is transferred, unauthorized USB devices will be detected resulting in a cybersecurity incident that must be thoroughly investigated and officially documented. Do not be the cause of a cybersecurity incident for your organization!

For additional information or for any questions pertaining to Cybersecurity Awareness, please contact our distro on the global:

USARMY Camp Humphreys 8 Army List Cybersecurity Information Request usarmy.humphreys.8-army.list.cybersecurity-information-request@army.mil