Volume #4 - Issue #149
March 2nd, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Evil Maid Attack

The once famous ‘Evil Maid’ is again making a comeback. A security firm, F-Secure has issued a fresh warning about possible evil maid attacks by exploiting Intel’s Active Management Technology and other techniques. The spate of fresh evil maid attacks in the wild were discovered circulating among the public.

Investigations that insecure defaults in Intel’s AMT allow an intruder to completely bypass login credentials in any laptop in 30 seconds, which

lends itself to the “evil maid” scenario. Even a minute of distracting a target from your laptop is enough to enable an attacker to gain access to the target machine.

So what exactly is an evil maid attack and how do you protect your laptop against such attacks? Here is a scenario that explain this type of attack:

Scene I: You are out vacationing or sitting in a restaurant. You suddenly feel the urge to visit nature’s call. Due to urgency, you leave your laptop open because you are confident that laptop is safe as the hard drive is encrypted.

Scene II: An evil maid spots you leaving you leaving your table.

Scene III: The evil maid sneaks up to the laptop and boots it with a compromised bootloader on a USB stick. The evil maid then installs a keylogger to capture your encryption key and shuts the laptop back down.

Scene IV: You come back to your table and boot the laptop. Nothing is amiss and you don’t even recollect leaving your laptop orphaned in coming days.

Scene V: The following morning or the day after, the evil maid comes back and retrieves the encryption key from the database.

The purpose of the attack may be to steal and sell the key or make changes to the laptop’s software right then and there, but whatever the reason for the attack, the laptop has been touched twice by an unauthorized person without an alarm bell going off. The newly found AMT vulnerability aids such attacks though there are numerous other ways a potential hacker can compromise a device, including cold boot attacks, inserting compromised hardware, and loading malware.
To safeguard your laptop and other portable devices from such evil maid attacks you are advised to:

- Never leave devices unattended.
- Always carry with you all small peripherals, such as USB drives.
- Avoid using any unknown peripheral.
- Enable input–output memory management unit (IOMMU) features.
- Adopt full disk encryption.
- Enforce secure boot protection.
- Shut down devices when unattended.

Some attackers are so skilled that they can replace a device with an identical one without the victim knowing it, so you have to extra careful when you leave your laptop or smartphone unattended. Always be aware of what is going on around you and it may save you from some very unfortunate consequences.

This Week's Cyber Alerts:

Alert Issued 3/1/18 **Popular Cache Utility Exploited for Massive DoS Attacks**

Alert Issued 2/27/18 **Mobile Banking Trojans Spread Confusion Worldwide**

Alert Issued 2/26/18 **IRS Warns of Spike in W-2 Phishing Emails**

Alert Issued 2/26/18 **Crooks Launder Money Using Real (and fake) Amazon Ebooks**

Thank you for subscribing to our email and I hope the information we have shared will make your online life a little easier.