Sophisticated Tools From Spyware to Ninja Cable

Attackers don't always need sophisticated James Bond hardware to break into your company. Sometimes a $99 device will do.

Up until just a few years ago, unless you were working as a secret agent, your only chance of seeing spy tools and gadgets was in the movies. These days, it still isn't easy to buy a lipstick pistol or a Bulgarian umbrella, but it has become shockingly easy to legally buy hardware-based cyberattack tools. Although IT security tools have quickly and significantly improved and threat-hunting teams of the leading enterprises have become more professional, cybercriminals are still growing and thriving.

Document leaks, such as the NSA ANT catalog and the US Central Intelligence Agency's Vault 7, released a huge hacking tool arsenal including concepts of operation, drawings, source code, etc., and allowed individuals and specialized companies to join the game. Hardware cyberattack tools that were in the hands of only governments and intelligence agencies are now available for purchase as legitimate penetration-testing tools starting at less than $10.

A recent example of a dangerous tool is the USB Ninja cable, which was introduced earlier this year. The Ninja cable looks like any ordinary and innocent smartphone-charging cable and will charge a smartphone as usual. However, this cable's design and internals are inspired by the leaked NSA Cottonmouth, a USB hardware implant that provides a wireless bridge into a target network as well as the ability to load exploit software onto target PCs. When it was a top-secret weapon in use by the government, the unit price was $20,000. These days, when publicly offered as a pen-testing tool, anyone can buy it for around $99.

Now just imagine a cybercrime organization trying to get into a bank's internal network. Chances of being able to overcome the network security tools such as firewalls, email scanners, etc., are not that high, and every failing attempt will just make the systems and security team more alert. But what if the threat actor could drop some of those cables around the company's HQ lobby? What if a cable is left on the cafeteria table? What if the ATM custodian gets one as a freebie? Probably, this cable will be plugged into a corporate laptop sooner rather than later, just for the sake of charging the phone.

The method of using infected hardware devices as attack vehicles and as invisible doors into sensitive infrastructure is even more attractive because the attacker can jump over air gaps and enter into or steal information from parts of the network that are segregated from the Internet or other parts of the enterprise network.

There is a huge gap in the awareness of IT and security teams between software deployment and usage policies and those that relate to hardware devices. Corporate employees or contractors will never be able to install or use uncontrolled software on an enterprise workstation or laptop. There are not only regulations and processes, but the entire system of authorization levels and user management will block it even if they tried.

On the other hand, in many places, anyone can bring in and connect any uncontrolled gadget or peripheral device directly to the infrastructure. Not only are there no policies in place to define what's allowed and what's forbidden, there isn't even a way for IT teams or risk officers to know and understand the attack surface they're in charge of protecting.

Know the Risk

The good news is that it's possible to address this rapidly growing threat. As always, being aware and understanding the risk is the most important step. This change in mindset is quickly taking hold in the industry — the Center for Internet Security (CIS, a nonprofit with large companies, government agencies, and academic institutions as members) has defined inventory and control of hardware assets as a top priority.

CIS urges organizations to actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.