GET YOUR INDUSTRIAL MEMORY UP TO FORM

Various forms of malware, including the offspring of the Stuxnet worm that was written to hunt for controller hardware, are tailored to transfer via USB drive. Michael Barrett recommends the use of industrial form factor devices in all instances where the use of removable memory is essential to operations

Removable memory devices are used for many applications in the industrial sector. These include the storage and transfer of files, the implementation of software/firmware updates, and for user authentication and controlling access privileges.

The USB drive (memory stick) is the most common form factor; being low-cost, widely available and easy to use. But these conveniences come at a price. There are considerable security concerns around the use of USB sticks. One of these is targeted data theft, and it has been reported in many places how hackers are writing executable programs and placing them on memory drives.

These drives are then left at venues frequented by the employees of the [targeted] company. The program executes automatically as soon as the drive is plugged into a computer. Its purpose: to transfer another program residing on the drive to the computer. That second program will give the hacker remote access to the company's network and, by extension, commercially sensitive data and any IP that exists as software (including programs for controlling drives and automation equipment).

This form of cyber-attack (the first move of which was within the company's firewall) could go undetected for a long time.

KEY POINTS

- ***Data theft programs, ransomware and digital weapons are just some of the dangerous code that can reside on a USB stick***
- ***Industrial removable memory devices are available that have Flash memory inside and communication is via the USB protocol; mechanically they are incompatible with USB***
- ***Anyone wishing to introduce malware into a system via a receptacle intended for a bespoke form factor drive would need the correct device***

LOCKED OUT

Another concern is a cyber-attack through ransomware. Increasingly favoured by cyber-criminals, ransomware prevents users from accessing their files by encrypting them. A key is needed to decrypt the files and sometimes each file is given a unique key, meaning that correctly guessing a key would only unlock one file. Moreover, the malware can lie dormant for a period so that it gets backed up.

The cyber-criminals then request payment in the cryptocurrency Bitcoins, online vouchers or via other methods that provide a high degree of anonymity; this under the practice known as ransomware-as-a-service (RaaS). There is no guarantee that files will be decrypted though, i.e. perpetual blackmail, or you may be asked to make a further payment to remain safe in the future, i.e. a cyber protection racket.

Along with falling foul of phishing emails, visiting a compromised [trusted] website and downloading files and remote desktop access (e.g. someone phones you and talks you through fixing a problem that's allegedly been detected on your PC), ransomware can also make its way on to your PC via memory stick. Indeed, some malware is tailored for transfer specifically by USB stick; a case in point being the 'USB Thief' trojan that collects personal data and made the news a few years ago.

THERE ARE CONSIDERABLE SECURITY CONCERNS AROUND THE USE OF USB STICKS

An even more malicious attack – again designed for USB drives – is one that hunts a network for specific hardware and controller software with the aim of shutting it down and/or driving it in such a way to cause an accident.

The one to mention here is of course Stuxnet, which was effectively a weapon. Spreading through PCs running Windows, Stuxnet hunted for Siemens Step 7 software, which runs on programmable logic controllers (PLCs). The malware provides instructions to the PLCs that will cause damage to hardware and it is believed that power stations were a target, with many of Iran's nuclear centrifuges damaged in 2010. Though Stuxnet is history, its source code has since appeared in other malware.

Data theft programs, ransomware and digital weapons are just some of the dangerous code that can reside on a USB stick. Also, though we think we live in an increasingly cyber-aware world – and most of us simply would not plug a USB stick we found into a computer – the reality is somewhat more disturbing.

For instance, in 2016 Google and two universities in the US conducted a study. They left almost 300 USB sticks infected with a harmless trojan around the universities' campuses. Almost half were picked up and plugged into PCs, at which point the trojans reported in. Of these, only a few were scanned for viruses first. Those looking on the devices were allegedly doing so to see if any of the content would identify the rightful owner. Good Samaritan. Bad consequences. It only takes the careless actions of one person to breach a network.

GO INDUSTRIAL

It is the popularity and availability of devices like USB sticks that make them ideal carriers for malware. On another note, any system with a USB port on its front panel, elsewhere on its enclosure or even inside is vulnerable to attack because data can be stolen, or malware introduced, using a portable computing device and a USB lead.

FURTHER PROTECTION CAN BE AFFORDED THROUGH MOVING AWAY FROM 'USB SILICON'

Accordingly, many industries have banned the use of USB drives. However, such bans need policing/enforcing and some companies have made the possession of a USB drive on company property a sackable offence. Other companies have added physical security devices such as locks to the USB ports of their systems; a practice which also requires policing as there will always be the danger of a platform with unlocked ports being left unattended. Again, it takes just a single infringement to compromise the entire network.

However, as it is the popularity of the USB form factor (for drives and ports) that is the weak link in security. If your operations rely on the use of removable memory devices, the best solution is to 'go industrial'.

Industrial removable memory devices are available that have Flash memory inside and communication is via the USB protocol. Mechanically they are incompatible with USB, so if a drive containing sensitive information were to be lost or stolen it is extremely unlikely the finder would have a receptacle with which to interface with the device. For instance, had industrial removable memory devices, such as Datakey keys or tokens, been left lying around as part of the study on the university campuses, the individuals picking them up would have been unable to access the content – content which would not have been able to escape.

Similarly, anyone wishing to introduce malware into a system via a receptacle intended for a bespoke form factor drive would need the correct device. Unlike USB sticks, industrial removable memory devices and their corresponding receptacles are only available through authorised distributors.

UP A LEVEL

Further protection can be afforded through moving away from 'USB silicon', particularly if there is no need for a large volume of memory. For example, in early 2020 Datakey launched a new line of CryptoAuthentication memory tokens, designed for systems that require 'cyber robust' removable memory devices for applications that include the transfer of passwords (or other data needed for user authentication purposes) or for the physical transfer of security keys, certificates, sensitive data or system configuration files.

At the heart of all devices in this new line is a Microchip CryptoAuthentication high-security hardware IC. Its features include a unique and non-changeable 72bit serial number (set by Microchip), a 512bit one-time programmable (OTP) zone, a random number generator and a SHA-256 hash algorithm for data encryption.

However, and far from wishing to plug products, we cite this purely as an example of how 'security robust' you can make a system requiring removable memory devices.

As a minimum, move away from the USB form factor. It is being targeted too much by cyber-criminals plus there is the constant risk of others reading a lost or stolen drive. For applications requiring extremely high security, look to data encryption technologies that make unauthorised access and cloning virtually impossible.

Michael Barrett is MD of Nexus Industrial Memory
Tel: 01794 732 082