The Evolution of USB Based Microcontroller Attacks in Corporate Espionage

Many organizations still look at corporate espionage and insider threats as something that will not happen to them. They see it as something that other companies need to worry about and naively believe that their employees are all trustworthy and would never act out against the company’s interests. During an economic recession and when companies are downsizing their workforce it behooves organizations to consider their risks and exposures to these types of threats. Now with the emergence of a new type of USB attack it is more difficult than ever to detect inappropriate or malicious employee activity.

Historic Review of USB Devices and Malicious Activity

Traditionally, USB storage devices have been the prevailing culprit for everything from virus infections and malware to data loss and corporate espionage. USB drives are one of the greatest conveniences when we need to move data between systems and individuals and are also the greatest risk for losing data. The small size, large storage capacity and cheap prices of USB storage devices have made them ubiquitous to our daily computer use. While there have been many advances in use and effectiveness of security tools to identify and detect malicious USB devices there are still significant risks associated with them.

The complexity of USB based attacks and their usefulness as a corporate espionage tool has changed significantly over the course of their development. In order to understand the emerging risks associated with this new breed of USB devices and how they can be used as tools in corporate espionage we need to first look at how USB attacks have changed over the years.

Originally, malicious code was placed on a USB storage device with the hopes that an attacker could manipulate or social engineer a weary user into clicking on a file on the device, thus executing the attacker’s code. While this type of attack worked it had significant disadvantages. The attacker was at greater risk of being discovered due to the interaction required between them and the owner of the target computer system. Additionally, any latent evidence of the attack could easily be tired back to the attack should it be discovered at a later date.

The next leap forward came with the emergence of U3 drives. U3 drives provided a significantly more sophisticated attack platform and many advantages from a corporate espionage perspective because of their inherent ability to “autorun” commands and code without requiring the interaction of a person. U3 drives are simply USB mass storage devices with an extra component. U3 drives have a small firmware section on the device that emulates a cdrom drive. The business purpose for this functionality was to take advantage of Microsoft’s Windows autorun functionality that automatically executed commands stored in a special file typically found on the root directory of CDs. From a user’s perspective the autorun functionality of U3 drives was an excellent business tool. It provided the user with a small virtual operating system that would automatically start when the drive was inserted into a computer. The very thing that made U3 drives convenient for users is also what made them so devastating when used for malicious purposes.
Attackers quickly discovered that they could use the autorun functionality to their advantage and developed methods of putting customized firmware on certain brands of U3 drives. Once the ability to implement customized firmware on U3 drives became public an assortment of highly sophisticated attack scripts were created. These types of modified drives are known as “USB switchblades” or “USB Hacksaws” and are easily made. Since Microsoft operating systems prior to Windows XP service pack 3 would automatically execute commands on a U3 drive an attacker could potentially compromise a system or covertly steal data simply by having the USB drive temporarily inserted into a target system.

This method of attack has enjoyed several years of success and is still a viable method today. Many different variations and implementations of this attack are possible and can be easily customized to focus on a specific target or organization. As the severity and potential impact from these types of attacks became more widely known organizations and security vendors started making tools that would detect the use of U3 USB devices. While this attack can still slip past some security monitoring tools most modern versions of operating system have been patched against it and there is significant awareness of it.

The Next Evolution of USB Based Attack

A new evolution to the USB attack arsenal is emerging. While traditional USB attacks can be detected by most antivirus and malware detection software packages and only worked against systems running older versions of the Windows operating system the new evolution is cross platform and significantly more difficult to detect. Enter the world of microcontroller attacks.

Microcontrollers are taking the place of simply USB drives as the next evolution of USB attack tools. Why microcontrollers? Just like traditional computers microcontrollers have developed and evolved over the years and are no longer simply used by electronics hobbyists. Microcontrollers are essentially very small computers able to be used in myriad of implementations and most importantly can easily interact and connect to computers. Modern microcontrollers are very small about the size of a postage stamp and come in a dizzying area of capabilities and function. Many microcontrollers are designed with a specific purpose in mind while others known as “USB Development Boards” are designed specifically to interoperate with computers. USB microcontroller development boards are very low cost, highly adaptable and are easily powered and connected to any regular USB port making them a perfect platform for developing functionality between a computer and the microcontroller.

An emerging capability of these small microcontrollers is the ability to emulate Human Interface Devices (HID). It is this capability that is unique compared to other USB drives and makes them an effective attack platform. HID devices are simply peripherals we connect to our computers to enter information or execute commands. While there are many different types of HID devices the most common are keyboards, mice and joy sticks. These new microcontrollers can act as a HID device and are able to enter commands into the computer. The easiest analogy is to think of the USB microcontroller as a person sitting at the keyboard able to enter keystrokes and
commands whenever it wants. As an attack platform the capability to emulate a keyboard and/or mouse to a computer represents a significant threat.

Unlike traditional USB devices that are connected to a computer, when a keyboard is connected to a computer its drivers are automatically loaded by default often before the operating system even loads. Typically no drivers are even required for common keyboards as they are standardized across most platforms and operating systems.

So what can these microcontrollers really do? What makes them such a threat from a corporate espionage point of view? What makes these microcontroller so much more effective at delivering malicious code or surreptitiously steal information isn’t just the small size and ability to be connected via USB ports, it’s the ease at which sophisticated attacks can be developed and its ability to work on virtually all operating systems and platforms undetected.

The use of a USB microcontroller to emulate a HID device may seem benign on the surface until you consider it from an attacker’s point of view. These devices give an attacker a number of advantages over previously known USB attacks.

No user intervention required - A maliciously programmed USB microcontroller does not require any form of user intervention once it is plugged in a target system. While most USB attacks rely on autorun capabilities a maliciously programmed microcontroller has no such limitations. Once connected to a computer’s USB port the device will run its code instantly or wait until predetermined conditions are met. This gives an attacker significant control over the actions that are taken on a target machine and make it easy to collect sensitive information or documents.

Platform Agnostic – Since a microcontroller can be configured to emulate a keyboard and do not require special software to function, they are operating system independent and easily adapted to work on Macintosh, Linux and most other operating systems with the same degree of effectiveness. A maliciously configured microcontroller can be programmed to look for characteristics of a system it is plugged into such as the apple key on a Mac or the pressing of Ctrl+Alt+Del on a Windows machine and adapt accordingly.

Highly customizable – The use of USB microcontrollers for corporate espionage can be configured to target a wide range of systems or be customized to target a specific organization or a specific type of data. The devices can easily be configured to target and steal only informational assets deemed important by the attacker thereby decreasing the chances of the activity getting noticed by people or security tools.

Difficult to detect – It is the difficulty to detect USB microcontroller attacks that make them such a significant threat if used for corporate espionage. When these microcontrollers are connected to a target computer the system simply sees it as a keyboard and accepts commands as such. Most computers will not even notice or register that a USB microcontroller is connected to the system nor will they notice any signs of performance degradation. In addition the likelihood that a user or software tools will detect activity is extremely low. The computer will diligently perform the requested tasks as if a person is typing the commands. This also makes attacks from a USB Microcontroller extremely difficult to detect from a forensic or repudiation standpoint.
**Practical Example of a USB Microcontroller Attack**

The following is an example that highlights one potential configuration for a USB microcontroller attack:

A disgruntled employee intends to steal sensitive documents and sell them to a competing organization. The documents reside on a manager’s computer and can only be accessed from this one computer. Before the manager arrives at work the employee plugs his maliciously configured USB microcontroller device into an empty USB port on the back of the target computer amongst the tangle of wires. Once the computer is turned on the device starts its program and starts monitoring the activity of computer. The device monitors manager’s activity on the computer and recognizes when there is period of inactivity, such as when the manager leaves their desk for lunch or a meeting. To keep the user logged in the device has the cursor move 1 pixel every few minutes to prevent the screen saver from loading. This activity is invisible to the naked eye, but the computer responds as if a user was moving their mouse minutely. While keeping the user logged in the device issues the keystrokes to begin darkening the screen so commands cannot be seen easily by individuals passing by. Next, searches are executed on attached and network drives for certain file names previously configured by the attacker. Identified files are then uploaded to a remote Internet file web site via the manager’s own web browser. This activity can continue over days or weeks based on the devices configuration. After the employee is comfortable with the files he has retrieved from the manager’s computer he simply removes the USB microcontroller from the back of the computer when time permits.

The above is a simple demonstration of what a USB microcontroller can do. Much more sophisticated attacks are possible based on the complexity of the target environment. It’s important to note that activity performed by the USB microcontroller runs under the context of the person logged into the computer, in the above example it would be the manger. Even a forensic analysis of the computer would conclude the Manager performed the activity. Because of the manner in which USB microcontrollers perform the attack it can completely circumvent the repudiation capabilities of most systems.

Another consideration of USB microcontroller attacks is that they are virtually undetectable with existing security software such as anti-virus and malware detection tools. USB microcontrollers do not typically store executable code rather rely on simple commands to perform the intended actions. In the above example, when the organization detects the leaked documents an immediate investigation would begin with the manager’s computer. Without the telltale signs of a system compromise or malicious devices being plugged into the system the focus of the investigation will shift to the manager who was logged into the computer at the time of the attack.

*What Does the Future Hold? -*
So with this new and emerging tool in the hands of insiders and disgruntled employees what does the future hold? The use of USB microcontrollers is in its infancy and we will see significant growth and changes in this area in the coming years. The complexity USB microcontroller attacks will evolve and quickly overtake traditional USB drive attacks as a prominent attack platform especially in the realm of corporate espionage. While the detection and countermeasures for these types of devices will develop as security professionals become more aware of the risks, it is likely that USB microcontrollers will remain an effective tools used by attackers and insider threats for some time.