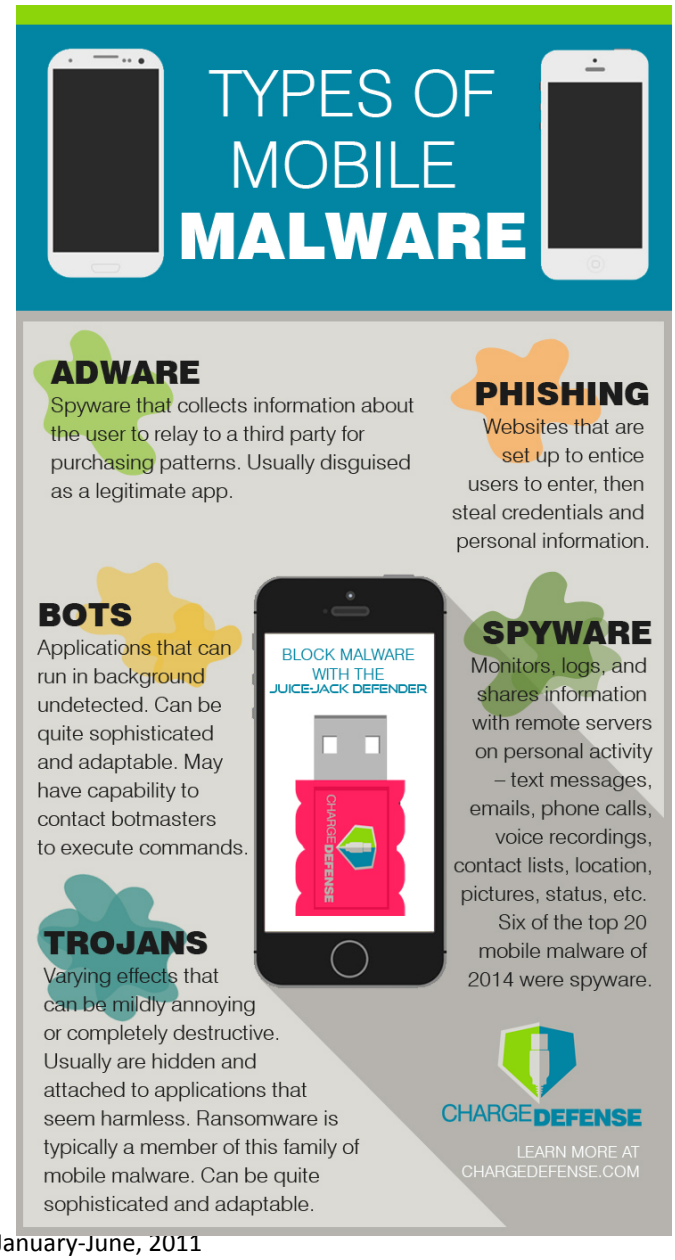
ALERT: SmartPhones – Twice as Dangerous as USB Flash Drives

Every IT professional knows that USB storage devices such as flash drives are notorious for carrying malware and exploiting USB autorun features to expose viruses to corporate enterprises. In fact, a Microsoft study in 2011 on 600 million systems revealed that malware infections via USB storage devices were responsible for 26% of the total infection rate[1], and that rate steadily increases year-to-year. In 2014, Microsoft further showed that 5 out of 10 malware instances are worms spread by USB removable drives.[2] That astounding number of potential infections has led many IT departments to outlaw the use of USB flash drives on enterprise-connected machines. Nevertheless, infection rates through USB continue to climb.



Perhaps a major reason for the increase in and severity of these infections is the pervasive use of smartphones for consumer and business purposes. After all, a smartphone is a USB storage device with a LOT more capability both for good and malicious purposes. Smartphones can not only carry around a virus (along with your personal information), they can also execute the virus on the phone itself, AND they can communicate wirelessly with the cyber criminals that put it there. Yet most people never think twice about plugging their smartphones into any USB port within reach for a quick charge, especially while traveling. It should therefore be said at shouting level: **SMARTPHONES ARE AT LEAST TWICE AS DANGEROUS AS USB FLASH DRIVES!**

Even Hollywood is picking up on the increasing trend in juice-jacking and understands the severity of having your personal information hacked on your smartphone. A recent CBS CSI Cyber episode is centered around a cyber-criminal juice-jacking attack at an airport, exposing thousands of unsuspecting travelers to identity theft. But, juice-jacking is not limited to connecting to unknown charging locations. Personal and corporate enterprise

[1] Microsoft Security Intelligence Report Volume 11, January-June, 2011
[2] Microsoft Security Intelligence Report Volume 17 English, multiple authors, Page 97, January – June 2014

systems are just as likely to be both carriers of juice-jacking viruses as well as victims. The Stuxnet virus that hobbled the Iranian nuclear weapons program in 2010 is a great example of a targeted cyber-terrorism campaign which worked magnificently.

Cyber Terrorists Target Corporate Enterprises via Infected Mobile Devices

In the past couple of years identity thieves and hackers have become even more sophisticated, shifting their attention to mobile devices. Malware applications originally developed for Windows operating systems are rapidly being migrated to attack mobile platforms. A February 2015 report from McAfee showed a 6x increase in mobile malware over a two year period and found that 8% of all mobile devices are infected with 387 new threats every minute, or more than 6 every second."[3] McAfee further reported accelerated mobile infection rates with 17% growth in just the last quarter of 2014.[4] Alcatel-Lucent's Kindsight Security Labs report agrees with this staggering increase in mobile malware, stating growth of 20% in 2013 and another 25% in 2014 with estimates of 18 million infected smartphones and growing quickly.[5] The same report showed a nearly identical percentage growth of infections on fixed networks. The coincidence is interesting and illustrates how cyber criminals are targeting mobile devices to ultimately attack networked systems within corporate enterprises.

To further substantiate the concern of USB devices being used to infiltrate enterprises, the February 2015 McAfee report makes some very disturbing correlations on the recent Sony Pictures Entertainment master boot record wiping attack by North Korea. They state that "this vector of attack [Shellshock] will be the entry point into infrastructures from consumer appliances" (connected devices like USB flash drives and smartphones) to corporate enterprises, and they "expect to see a significant increase in non-Windows malware in 2015."[6]

Although Android and Windows systems are the most common malware targets - nearly equally distributed at 50/50[7] - Apple iOS devices also have recently been targeted and infected by cyber criminals. The Wirelurker virus infected desktop and laptops by posing as a popular game app that used USB ports to infect Apple mobile devices when connected to the infected machine. The mobile virus then stole information from mobile devices and sent it to criminals via wireless means. Apple responded rapidly by posting an operating system fix -but not before reports of hundreds of thousands of people had been infected, via the reactive "closing the barn door after the horse has escaped" process which all too many malware remedies end up following. This wasn't the only major attack against iOS systems; 'Find and Call', discovered in 2012, was the first notable non-jailbreaked iOS trojan which uploaded contact lists to a remote server. Two years later spyware applications XAgent and MadCap were discovered on iOS systems. This malware was directed at political and military employees and intended to perform advanced political espionage. This is not meant to impugn or blame Apple for product flaws; they are a great company with great products and, truth be told, they have much lower

[3] McAfee Labs Threats Report, February 2015
[4] McAfee Labs Threats Report, February 2015
[5] Motive Security Labs malware report H2 2014, Alcatel-Lucent, 2014
[6] McAfee Labs Threats Report, February 2015
[7] Motive Security Labs malware report H2 2014, Alcatel-Lucent, 2014

infection rates than Android devices. However, it shows that no one is immune to mobile viruses. Everyone should be on high alert.

Protect the Enterprise from Cyber Criminals

So, what can IT professionals do to protect their Enterprise from inside threats presented by USB vulnerabilities which are often introduced unintentionally by well-meaning employees? Educating employees on the dangers associated with USB charging is the first step. Implementing security policies and periodic training is a common best practice among most companies large enough to support an IT staff. However, education, training and policies might not prevent an employee with just 5% charge left on their phone from plugging it into a USB port on his work computer. This small and seemingly harmless act can bring down an entire network if lurking malware on the phone can circumvent policies intended to thwart it. Just as bad, it can also expose corporate intellectual property such as research, product plans, employee records, financials, and a host of other information that should never go outside of the corporate network. The majority of USB enterprise security breaches are accidental. Therefore, more comprehensive mitigation strategies should be considered. One such strategy is the USB port blocker, which are inexpensive mechanical plugs that physically prevent the connection of all USB devices.

While this will work in some scenarios, the port blocker comes with an obvious disadvantage: it completely disables the functionality of the USB port, including its ability to charge devices. For the proverbial employee low on smartphone power you'll need to consider a solution that meets their needs as well as your security requirements. It's possible to disable the data synchronization component of a USB port (which is how viruses can spread) while still allowing charging. Some devices and "charge-only" cables allow power-only connections by disconnecting the data lines on the USB port. Unfortunately, this is not a solution for many more sophisticated smartphones, including the Apple phones, as they will not charge in this situation. Other charge-only solutions charge at slow USB 1.0 speeds and may not support all mobile devices (smartphones and tablets) and mobile operating systems (Android, iOS, Blackberry, and Microsoft) or use chips that could potentially be hacked and completely defeat the purpose.

ChargeDefense's Juice-Jack Defender® is the solution that supports all these requirements – it blocks all data transfer between device and charging source, supports all mobile devices and operating systems, supports charging at up to twice the normal USB charging speed and has no chips or memory to execute and store malware.

The bottom line is that the majority of enterprise infections come from inside the company and most of those infections are unintentional. Over ¼ of infections are through USB connections and the trend with hackers and malware developers is to target mobile users. Every smartphone should be considered an infected device when connected to enterprise machines. Simply implementing policies to disallow USB

connections is not 100% effective. A combination of education and training, port blockers, and power-only charging solutions such as the Juice-Jack Defender® is an inexpensive, practical way to keep honest employees from infecting your enterprise and exposing corporate and employee information to the bad guys.

Don’t Get Juice-Jacked!