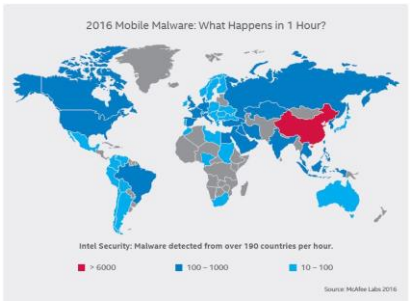
Monthly Newsletter

July 2016 **Mobile Devices and Malware**

In This Issue

Introduction

The past few years have seen a tremendous increase in the use of mobile devices. This is partly due to devices becoming more affordable, but the real reason is convenience. Mobile devices have increased in speed, power and storage space, making them more convenient than carrying around a laptop. This has led to a rise in people using them for online shopping, managing their finances, paying their bills, etc. While this is convenient for users, it also exposes them, and potentially where they work, to multiple threats.



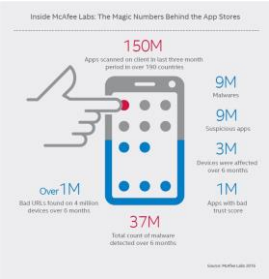
Mobile devices have become so numerous that in the latter half of 2013 there were more mobile devices accessing the internet than traditional computers. Today it is almost impossible to find someone who doesn't have a smartphone. And several people have tablets, smart watches, and/or more than one smart phone. Because of this, mobile devices have become a target for cybercriminals and malware.

What is Malware?

As you may remember from May's newsletter, malware is a compound word derived from combining Malicious and Software. Basically it is a program that has been written to perform a malicious act. Examples of malware are viruses, worms, adware, ransomware, etc. So why does malware work on one computer and not another? The answer to that is because the malware has to be written to work on a specific operating system or computer hardware. That means that the program has to be written to work on a Windows, Mac, Linux, etc. computer.

Are Mobile Devices Vulnerable?

Most people don't realize that smartphones, tablets, smart watches, etc. are nothing more than specialized computers. Even the devices you have in your home such as Smart TVs, refrigerators that keep track of what you have and can order when you get low on something, your home security systems, etc. are just specialized computers and are just as vulnerable to targeted Malware.



On June 29, 2007 the first iPhone was introduced and on October 22, 2008 the first Android phone was introduced. Since then both phones have competed for dominance, and currently hold (approximately) a 99% market share of the cell phone industry. These two types of phones account for the majority of the approximately 207 million cellphones currently in use in the U.S., making them a very desirable target for cybercriminals.

Between 2014 and 2015 there was a 61% rise in mobile malware attacks. Ransomware, bank fraud and Remote Access Tools (RATs) have been just some of the things that have been observed. These phones have been compromised in a variety of ways. Some have been compromised from infected apps from the Apple App Store or from the Android Play Store. Others have been compromised from users clicking on links sent to them or by visiting compromised websites. And still others have been compromised by receiving specially crafted MMS messages (see

Contact Us

Cyber Security

kirk.burns@dps.texas.gov

Stagefright link on the left). Stagefright didn't require any user interaction. All that was required for your phone to be compromised was for the attacker to text you. It was even possible for a vulnerable phone to receive a text, have a RAT implanted, and have all traces of the attack be erased with no interaction from the user while the device is charging on your nightstand.

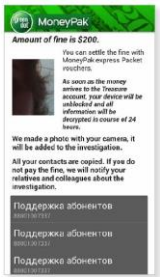
Because of the severity of this problem, both Apple and Android have pulled hundreds of apps from their stores and are routinely pushing out security updates. However, this will not ensure your mobile device is safe.

To give you an idea of how serious this problem is, in 2015 there were 5x more OS X malware than in the previous 5 years combined. There has been a 262% increase in the number of iOS vulnerabilities and 188% increase in Android vulnerabilities since 2011.

Dangers to Businesses

The average U.S. Enterprise Cost of Cybercrime by Industry is:

- $8.6 million for U.S. retail stores
- $12.7 million in communications
- $14.5 million in technology
- $20.8 million in financial services



It is anticipated that there will be 229 million cell phones in use in the U.S. by 2018. Some studies show that as many as 35% of cell phones don't have any security. That means that they don't even have a lock code programmed to prevent unauthorized access. And there are no reliable sources on how many mobile devices have (or don't have) antivirus software installed. This lack of security makes these devices very vulnerable.

Current industry estimates put the number of Internet-connected wearables (another serious danger) around 780 million by 2018. This works out to a wearable device on one of every 10 people on Earth. If we assume that there will be fewer wearables in developing countries, that number is probably closer to one in every four or five people.

Several businesses have started embracing the idea of BYOD (Bring Your Own Device), BYOT (Bring Your Own Technology), BYOP (Bring Your Own Phone) or BYOPC (Bring Your Own PC) in the work environment. It is anticipated that this will become a growing trend for businesses.

Assuming these devices do not meet minimum security standards, this will open up even more vectors of attack to individuals and organizations. Businesses will likely find themselves more vulnerable to insider attacks than they currently are while also having to defend from even more external attacks.

How to Protect Yourself

Just like with your computer, there is no way to ensure your mobile device never gets Malware. But there are somethings that you can do to mitigate the dangers.

1. Never Root or Jailbreak your device
2. Always keep your mobile device updated
3. Only download apps from approved locations (App and Play Stores)
4. Install an Antivirus program on your mobile device and keep it updated
5. Update apps installed on your mobile devices
6. Uninstall apps you no longer use

If you haven't done so already, I highly encourage you to install an antivirus program on all of your mobile devices. Sophos is the antivirus program we use here at DPS. As I mentioned in the March newsletter, the company has provided its program for free for personal use. You can download it for your computers by visiting their website. To install on your mobile device, go to either the App or Play Store and search for Sophos.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber**".

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.