MOBILE MALWARE

and How to Protect Yourself From It

by Cindy Phillips

Malware has been around since 1982 which is when Elk Cloner, an Apple II virus, came to be known as the first virus discovered "in the wild." The Brain Virus, the first PC/MS-DOS virus, arrived in 1986. However, like Elk Cloner (a 15-year-old's practical joke), the Brain Virus's effect was fairly harmless. By comparison, today's malware has a degree from Took U. and if you aren't careful you will be schooled and stuck with tuition fees — forewarned is forearmed.

Desktop malware tactics have successfully migrated to the mobile platform. The classics: pornography, scams, phishing, spam, and malicious apps are still leading malware threats. However, push-button rootkits, common on the desktop platform, haven't yet migrated to the mobile platform. According to Blue Coat Systems' 2013 Mobile Malware Report, malware that can truly break the mobile device security model is still in its infancy.

Today's malware coders and hackers (MCH) are, more often than not, financially or politically motivated; neither motive is mutually exclusive. MCHs are targeting Android, the Google-developed mobile platform, because it's currently the most popular mobile platform. Android's share of the mobile malware pie has grown proportionally with its popularity. In their Third Annual Threat Report (Mar 2012 - Mar 2013), Juniper Network says that 92% of all malware is targeting the Android platform. The other platforms: iOS, Blackberry, and Window Mobile are still seeing their share of mobile malware infections. However, the threat is often cross-platform in nature.

Phishing is the use of legitimate-looking email from a trusted or well-known website in an attempt to gather financial or personal information from recipients. In their white paper, Phishing and Web Security, Webroot says that phishing, after a brief absence, has retaken the throne as the number one web threat. However, this isn't your naive daddy's phishing. Adversity has caused the evolution of phishing: the decreased effectiveness of phishing 1.0 techniques against consumers. Cybercriminals have focused their sights on the business community and evolved their techniques — with growing success.

Phishing 2.0 (Spear Phishing) techniques involve one or more groups and organized, highly targeted, campaigns with stages: (1) profiling, (2) reconnaissance, (3) crafting targeted phishing emails, (4) planting the malware on the victim's computer, and (5) exploiting the breached computer. Phishing 2.0 is directed at businesses of all sizes. It can fool security-savvy users and evade anti-virus and anti-

phishing software. Bank accounts, intellectual property, customer lists — employees with access to this sensitive information are most often targeted by phishing 2.0 techniques.

Another notable nasty is a technique dubbed Water Holing, a counter countermeasure in the phishing 2.0 bag of tricks. Water Holing is another form of targeted attack which yields the same results as a phishing attack. This technique involves compromising a website (known to attract people from a certain company, geographic region, or industry) and setting up a drive-by download.

Drive-by downloads typically involve luring a victim into downloading and executing a malware file; often, via: (1) a clicked-on email attachment, (2) a link in an email which then requests a file download, or (3) clicking a link on a compromised webpage.

There's no shortage of mobile malware on the internet and even more on the way. However, mobile users can take steps to protect their data and their mobile devices. A few ways to protect against mobile malware are:

- Update mobile operating systems (OS). OS updates often contain code patches to update/secure code which hackers can use to penetrate the OS and install malware. Keeping the mobile device's OS updated can better protect it, as well as help prevent successful attacks.
- Install antivirus software to protect mobile devices from malware. When choosing antivirus software, stay on the well-traveled yellow brick road: select only from the well-known mobile antivirus software apps available. Malware masquerading as antivirus software is an old, and still successful, desktop ploy.
- Update desktop OSes and desktop antivirus software. Again, cross-platform malware is still a source for concern. Whether it's a desktop or mobile platform, email is an effective malware attack vector. If similar care isn't taken to secure a desktop computer the backdoor is being left open for malware infection via syncing or other data transfer between a desktop and a mobile device.
- Avoid Sideloading. Sideloading involves turning off the setting which allows software from untrusted sources to be installed on a mobile device. In the case of Android, this is an APK file that wasn't downloaded from Google Play or other well-known Android app site. These files have no 'trusted' signature to verify that they haven't been infected with malware.

The take-away here is that the internet has caused a global evolution on almost every social level. As such, the internet is no longer the sole playground of technical punk pranksters; it hasn't been for some time. Organized crime has also evolved, the evidence is clear.

Organized e-crime — organized crime reloaded — is often military in discipline (if not in fact), globally-networked, dogmatically methodical, ever evolving, and even alluring.

Stay aware, updated, and secured.