January 2015
Feature Article: Mobile Malware: Should I Keep Taking The Tablets?

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Mobile Malware: Should I Keep Taking The Tablets?

David Harley, ESET Senior Research Fellow

A shorter version of this article previously appeared on IT Security UK. However, I've participated in discussions in several forums recently that indicate that whether and how to protect mobile devices is still a question that people find perplexing. Some months ago, I recently came across a comment to one of my blogs – it doesn't matter which, because it didn't actually relate directly to the article it was attached to, but it was a WeLiveSecurity article. The commenter wanted to know whether she needed to install anti-virus onto her tablet, because 'tablets can't get viruses', as her son had told her, and she wondered whether she was being conned by anti-virus companies into buying and filling up her tablet with unnecessary apps for the detection of mobile malware.

It's sometimes difficult to tell troll from truth in blog comments, where anonymity is easy, spam is sometimes quite clever (though by no means always!), and some remarks are made (im-)purely with the attention of causing trouble, but in this case I made a short response. And I got to thinking that at a time when for many people their phone and/or tablet is their main computing experience (outside work, at any rate), maybe there are others in a similar state of confusion, so I tried to expand in a subsequent article on that theme.

Is it true that tablets can't get viruses? "Can't" is a big word, but it's true that mobile devices don't usually get 'real' viruses. But – as Aryeh Goretsky pointed out in a more recent blog on the somewhat related topic of whether there is a need for Linux anti-virus – while there are still occasional sightings of a high-profile Windows virus, self-replicating malware is far from still being the only game in town. Indeed, it long ago declined nearly to vanishing point even on the platforms where viruses once flourished (mostly DOS and Windows), leaving the dinosaurs of my generation as the custodians of knowledge concerning technology that nowadays excites little interest. Unless, of course, you count the occasional journalist wanting to compile yet another '10 viruses that once ruled the earth', or security bloggers waxing nostalgic on the anniversary of some long-gone media virus or worm like Michelangelo or Lovebug.

Non-viral malicious software is a different matter. Depending on what you may understand by the term, of course: clearly, there's a difference in impact between a totally destructive Trojan and joke apps or even mildly irritating adware, though there are instances of adware that's so intrusive that it makes the system it infects unusable. But there are plenty of other types of malware that come somewhere in between those extremes. And while there's no other platform yet that can 'boast' quite as many unique samples of unequivocally malicious software as Windows, there are certainly all too many other examples known to target other platforms – many targeting a programming or scripting environment rather than a hardware platform or OS, so that they may work on more than platform.

The person who posed the question in the comment to my blog didn't say what tablet she uses, but there are many, many examples of Android malware – AV-Test apparently claimed 1.8 million samples at the time of a recent test of Android security suite. It is, I suppose, only fair to mention that opinions vary – well, Google's does – on how much real impact Android malware has.

Some devices and OS versions are, of course, more vulnerable than others. While iOS isn't impregnable, most of what iOS-

targeting malware there is relies on the device being jailbroken. In general, Apple's 'iron hand' approach to app-sandboxing and App Store whitelisting has made iGadgets largely free of unequivocal malware, while making it all but impossible for AV companies to introduce full-strength malware detection software to the platform. On-demand scanners for iOS do exist in a limited sense, but they're focused on Windows and Mac malware rather than the tiny handful of programs that can unequivocally be called iOS badware. This is presumably because there is a theoretical possibility that malware for other platforms to find its way onto a tablet and might even, to quote myself and Lysa Myers: from a paper we presented at Virus Bulletin in 2013, 'use the iGadget as a gateway to vulnerable systems' even though they're not native to iOS and couldn't execute on the iGadget.

We've actually used the term 'heterogeneous malware transmission' for many years to describe this process in the context of other operating systems. Perhaps the most notorious example of this phenomenon is the spread of Microsoft Word macro viruses in the 1990s: while most macro viruses could execute well enough to infect Word documents on vulnerable Mac systems – that is, those systems running a vulnerable version of Word – payloads were, more often than not, Windows-specific, and could not be executed.

So a deluge of infected documents found their way, via people using infectable versions of Word on Macs, onto Windows systems where the payload *could* be executed (unless they were running up-to-date security software). You could certainly argue that heterogeneous isn't strictly the correct term in this instance: there is a difference between operating systems that are simply not binary-compatible, and environments that are shared across operating systems. Word versions for Mac and PC are not binary-compatible: that is, you can't run the same binary as a native application on both platforms. (You can, of course, run Word for Windows in an *emulated* Windows environment on a Mac.) However, Word macros are native to the Word application, not to the underlying operating system. While malicious Word macros are very rare now, in principle those that already exist run under Word rather than the operating system (OS) under which Word runs. So if a similar Word version runs on both Mac and Windows operating systems (as was the case with Word 6.x), there can be a degree of compatibility between macros.

(You may think that the age of macro malware is long gone, but that's not exactly the case. Targeted malware and so-called APTs continue to use documents as a vector, and it's certainly not unknown for untargeted malware to take similar approaches, though it's still the case that higher volumes of specific malware tend to be detected earlier by a wide range of security products.)

It's very common now for applications and application frameworks to be available across a wide range of platforms. While the underlying binary is specific to the operating system/platform on which it runs, the application itself can run code which is to a greater or lesser extent compatible with the same application sitting on a completely different OS and/or hardware. If that code happens to be malicious, it may work across a range of OS/hardware combinations, as long as it doesn't make unsafe assumptions about the OS and hardware underlying the application framework.

If malware is unable to work at all on any platform but the one on which it was originally designed to run, it might still be transmitted via a platform on which it can't be executed, in which case it might be described as 'latent' malware until it reaches an environment in which it can and does execute.

There are two other classes of malware that need to be borne in mind when considering what kind of security software to use (if any) on a platform that isn't generally considered prone to malware attacks:

- Borderline apps that are closer to the 'possibly unwanted' class than to unequivocal malware.
- Malware that can only take hold on a device that has been modified to evade the built-in security of the operating system so as to make it easier and more convenient to run applications that haven't been approved or signed by the manufacturer, such as a jailbroken iGadget.

There are a lot of security apps out there that seem to me to be of doubtful usefulness, but those tend not to be made by the mainstream security vendors. And, of course, there are 'security apps' that are not only useless but also actively malicious, though fortunately these tend not to be available through approved retail channels for long. If you're going to buy a security app – and you may think it's better to be safe than sorry, but that's not a decision I'd want to make for you – I'd suggest that you go for a product by a company with a track record in security programs for other platforms. However, there are actually quite a few free products for mobile devices from mainstream vendors, even though they may have very limited functionality compared to desktop products.

AV-Test has run a number of tests in 2014 focused on protective software for Android:

- http://www.av-test.org/en/news/news-single-view/35-android-protection-apps-put-to-a-6-month-endurance-test/
- http://www.av-test.org/en/news/news-single-view/36-security-apps-for-android-are-put-under-constant-fire/
- http://www.av-test.org/en/news/news-single-view/30-security-apps-for-android-take-on-2200-pieces-of-malware/

AV-Comparatives has also published a comprehensive review of Android security products.

AMTSO has published a decent set of guidelines for anyone aspiring to test mobile products: http://www.amtso.org/released/20140220_AMTSO%20Guidelines%20on%20Mobile.pdf

While it's not uncommon for generalist computer publications to publish comparative reviews of iOS security apps, I haven't seen one yet that I could unreservedly recommend. At present, few mainstream testers are dipping their feet into these murky waters: one significant reason for this is likely to be the difficulty of testing most security apps without using a jailbroken device. This immediately poses a major difficulty, since jailbreaking diverges from the 'average' user's experience of mobile devices, as does using a simulated iOS environment.

ESET Corporate News

ESET Hires New Vice President of Sale

ESET® announced the hiring of a new Vice President of Sales, Gerald C. Choung, former Senior Director of Channel Strategy and Sales for Qualcomm, Inc. (currently Omnitracs). Choung brings more than 20 years of experience in partner and channel development, sales operations and enterprise software sales to ESET.

“We are excited and privileged to have Gerald join our expanding team here at ESET,” said Andrew Lee, CEO of ESET North America. “With internet and data security continuing to move to the forefront, Gerald comes at a perfect time to guide ESET on its upward trajectory.”

As Vice President of Sales for ESET North America, Choung will be responsible for leading the North America Sales Team and providing strategic direction for ESET’s robust partner and distributor network.

ESET Announces New Encryption Capabilities for Channel Partners with DESlock+ for iOS

ESET® announced that its channel partners in North America now have exclusive access to DESlock+ for iOS, an easy-to-use encryption application for devices running on the Apple® mobile platform, through its Technology Alliance partner DESlock+. The technology allows consumer and businesses of all sizes to encrypt and decrypt email, attachments and texts on their iOS devices.

“In today’s cybercrime environment, encryption is an essential part of a layered cyber security approach and companies not utilizing this technology are leaving their customers at risk," said Andrew Lee, CEO of ESET North America. “Encryption is no longer the IT headache it used to be thanks to products like DESlock+, with functionality and settings conveniently managed from a central server. No other product can match DESlock+ for its flexibility and ease of use, so we are thrilled that this product extends protection to iOS users.”

DESlock+ has been a part of the ESET Technology Alliance, an integration partnership, since 2013. DESlock+ provides ESET customers with better protection of company infrastructure, as well as effective encryption on corporate devices.

The Top Ten Threats

1. HTML/Refresh

Previous Ranking: 1
Percentage Detected: 2.77%

HTML/Refresh is a Trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 2.37%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address from which it tries to download several files. The files are then executed and HTTP is used for communication with the C&C to receive new commands. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. Win32/Adware.MultiPlug

Previous Ranking: 3
Percentage Detected: 2.04%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it gets a foothold on the users system might cause applications to display pop-up advertising windows during internet browsing.

4. HTML/ScrInject

Previous Ranking: N/A
Percentage Detected: 1.42%

Generic detection of HTML web pages containing obfuscated scripts or iframe tags that automatically redirect to the malware download.

5. Win32/Sality

Previous Ranking: 5
Percentage Detected: 1.39%

Sality is a polymorphic file infector. When executed registry keys are created or deleted related to security applications in the system and to ensure that the malicious process restarts each time the operating system is rebooted.
It modifies EXE and SCR files and disables services and processes implemented by and associated with security solutions.

More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah.

6. LNK/Agent.AV

Previous Ranking: 8
Percentage Detected: 1.23%

LNK/Agent.AV is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat.

7. Win32/Ramnit

Previous Ranking: 10
Percentage Detected: 1.23%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and also searches htm and html files so as to insert malicious instructions into them. It exploits a vulnerability (CVE-2010-2568) found on the system that allows it to execute arbitrary code. It can be controlled remotely to capture screenshots, send information it has gathered, download files from a remote computer and/or the Internet, and run executable files or shut down/restart the computer.

8. JS/Kryptik.I

Previous Ranking: N/A
Percentage Detected: 1.22%

JS/Kryptik is a generic detection of malicious obfuscated JavaScript code embedded in HTML pages; it usually redirects the browser to a malicious URL or implements a specific exploit.

9. INF/Autorun

Previous Ranking: 7
Percentage Detected: 1.16%

INF/Autorun is a generic detection of versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malware executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malware executable when the infected drive is mounted. The AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes present in an attempt to hide the file from Windows Explorer.

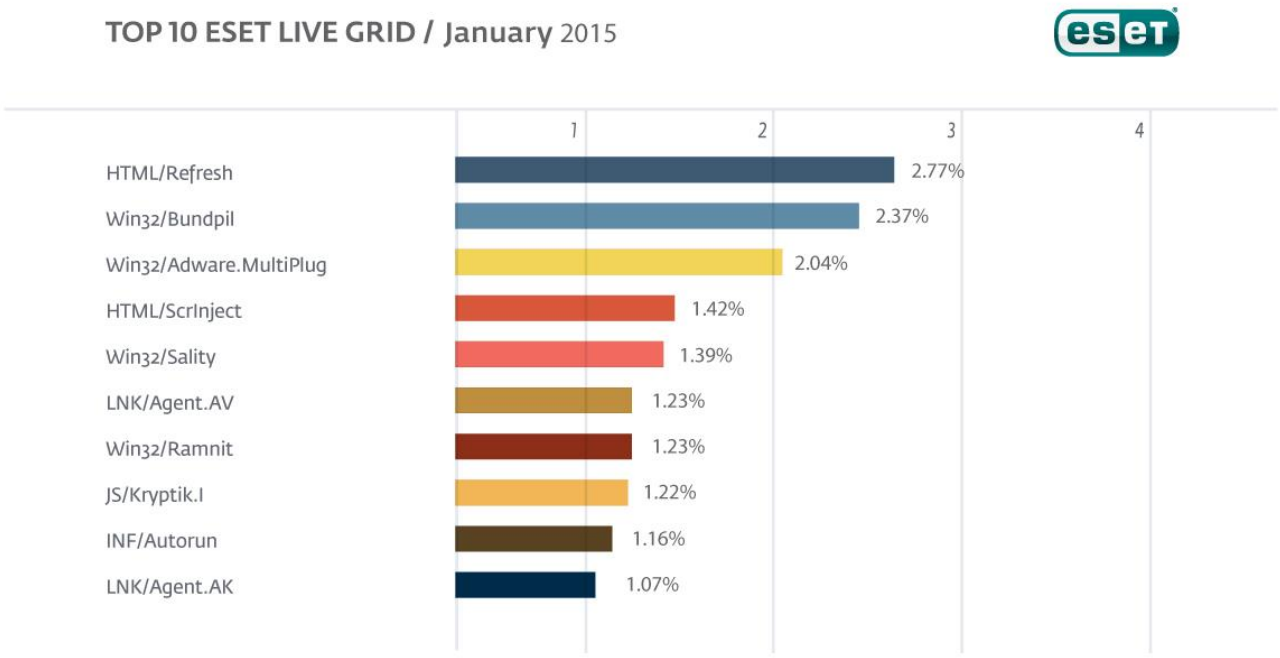
10. LNK/Agent.AK

Previous Ranking: 6
Percentage Detected: 1.07%

LNK/Agent.AK is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat. This vulnerability became known at the time of discovery of Stuxnet, as it was one of four vulnerabilities that were executed by Stuxnet variants.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with 2.77% of the total, was scored by the HTML/Refresh class of treat.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- WeLiveSecurity
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation