June 2014
Feature Article: The Increasingly Strange Case of the Antipodean iOS Ransomware

ENJOY SAFER TECHNOLOGY™

Table of Contents

The Increasingly Strange Case of the Antipodean iOS Ransomware

David Harley, ESET Senior Research Fellow ESET North America
Small Blue-Green World

[This article appeared previously on the Mac Virus website, while a shorter version originally appeared on the ITsecurity web site.]

It's not clear exactly what happened in the mysterious case of the Antipodean iOS 'ransomware' attack – in particular, why the only people affected initially seemed to be in Australia and New Zealand, though there have been subsequent reports of victims in the UK.

There's a good blog/FAQ by Graham Cluley (who has done his usual excellent job of following the story) for Intego here, offering several possible thoughts as to what might have gone wrong, but most of them don't really address the localization issue. The later arrests of two people in Moscow alleged to have carried out a similar attack against Russian iGadget users may shed more light on these events, but at the time of writing, as Thomas Reed has pointed out, there is at present no proven link between the two attacks on very different localities, offering no further answer to the question 'why the Antipodes?'.

The Australian attacks seem to use the "Lost iDevice" feature, and affected Apple devices displayed this message: "Hacked by Oleg Pliss. For unlock device YOU NEED send voucher code by 100 $/eur one of this (Moneypack/Ukash/PaySafeCard) to [email address]"

The Russian attacks seem to have been effected by setting up a phishing site in order to capture iCloud credentials, then using the access thus obtained to lock the devices. However, according to Reed, the message in this case translates to "Your device is locked in relation to the complaint. And can help you unlock it. Check your email!"

My colleague at IT Security, Kevin Townsend, wrote in a recent blog:

The problem with this scam is that there is no malware that Apple can block in the future: it is the business process rather than the device software that is hacked. That means that other hackers can use the same methods again and again in the future – and it is quite likely that there will be other copycat attempts in the future.

It's not impossible that the same parties carried out both attacks using a similar modus operandi based on phishing and social engineering, of course, but I think it's too early to assume that the case is all but closed. It could even turn out that there is in fact some issue that can be addressed by patching or some form of re-engineering, though I've no grounds for suspecting the existence of the kind of vulnerability that Apple has already dismissed as a possibility. Frankly, there just isn't enough information at present. Either way, Kevin is certainly right to stress the importance of taking advantage of the precautionary measures that are currently available.

Irrespective of what part of the world you live in, the most important (hopefully) preventative measure is to enable Apple's 2-factor authentication for Apple ID credentials – as far as I can ascertain, no-one in Australia or New Zealand who'd done this had the Oleg Pliss problem. See Apple's knowledgebase article for details of how to implement it. Essentially, this allows

you to authenticate using a password and a 4-digit PIN (verification code) texted to a trusted device at each login, and also generates a 14-digit recovery in case of emergency. This might also be a good time and reminder to change your AppleID password and ensure that you're not re-using a password that might have been exposed by the compromise of another service.

Apple Australia has also suggested contacting AppleCare or visiting an Apple Store if necessary, and insists that an iCloud breach is not responsible.

Another colleague, Stephen Cobb, observed for WeLiveSecurity:

Regardless of where you live, this incident should serve as a wake-up call to Apple users who have not yet done the following:

- *Turn on Apple's 2-factor authentication for Apple ID credentials.*
- *Establish a backup regime, using one or more of iCloud, iTunes, Time Machine.*
- *Create a strong and unique password for your AppleID.*

While Apple's "walled garden" approach to protecting your devices from bad stuff and bad people is an excellent model, it is we, the Apple users who can sometimes be the weak link. Please take the time to do all three of the above.

For people who *have* been affected, you can try to erase and the device and its passcode using recovery mode. This is how http://support.apple.com/kb/ht1212 describes the procedure for people who haven't synched with iTunes, don't have Find My iPhone set up, or can't restore from iTunes or iCloud backup via their own computer:

- Disconnect all cables and turn off the device.
- Press and hold down the Home button while connecting to iTunes.
- When you do, iTunes should offer to restore the device.

Stephen noted:

Apple Australia has also suggested contacting AppleCare or visiting an Apple Store if necessary. The company has apparently stated that an iCloud breach is not responsible for this rash if incidents. Regardless of which hemisphere you are in, if you get a ransom message on any Apple device I suggest you head straight to the nearest Apple store. Apart from anything, this will help Apple learn more about the problem.

I don't know of an instance where an Australian victim actually paid the ransom demand, but there's no reason to assume that if they had the criminal would actually have restored the victim's access to the affected device(s). It's likely that victims might have paid and yet still had to do what amounts to a factory reset in order to get back the use of their iGadgets. Clearly, some Russian victims did pay up, since the alleged criminals were caught on CCTV withdrawing payments from those victims from an ATM.

Other links:

- Apple Support Communities
- OSX Daily: Forgot an iPhone Passcode? How to Reset the iPhone passcode
- Simon Sharwood for The Register
- International Business Times
- John Leyden for The Register
- Graham Cluley for Intego: Have you been hacked by Oleg Pliss? FAQ for iPhone and iPad users
- Thomas Reed: Russian iCloud hackers arrested
- Charles Arthur for the Guardian: Two confess to Apple iCloud 'ransomware', say Russian authorities
- Kevin Townsend: Two iPhone hackers probably behind the Oleg Pliss attacks arrested in Russia
- Graham Cluley for Intego: Moscow Hacking Duo Confess to Hijacking and Locking Apple Devices
- Ben Grubb for the Sydney Morning Herald: Hackers suspected of holding Apple devices to ransom detained in Russia

ESET Corporate News

ESET Delivers Mid-Year Security Threat Review

ESET recently hosted ESET's Mid-Year Security Threat Review in a free webinar that covered some of the more interesting pieces of malware and threats that occurred during the first six months of the year. It focused on serious new developments, as well as the persistence of numerous older threats that continue to plague our systems.

Included in ESET's review was the latest information on banking Trojans, Bitcoin miners and stealers, Heartbleed SSL vulnerability, Mac and iPhone threats, nation-state malware campaigns and the Windigo campaign. Presenter Aryeh Goretsky, a distinguished researcher at ESET and veteran of the anti-virus malware industry, also discussed the end of Windows XP and the impact it will have on the future of the security landscape.

ESET Announces Start of Cyber Boot Camp 2014

ESET announced the start of the fourth annual Cyber Boot Camp for local high school students, taking place this week at the company's North American headquarters. The camp, hosted by Securing Our eCity and sponsored by ESET; California Coast Credit Union; Computers 2 San Diego Kids; Higgs, Fletcher & Mack, LLP; Mendez Strategy Group; and San Diego Gas & Electric, consists of five days of intense cybersecurity education that combines hands-on experience in a computer lab with presentations from subject matter experts, including a U.S. magistrate judge and members of the FBI's cyber squad.

Nearly two dozen students from Canyon Crest Academy, Westview and Mira Mesa High Schools and numerous volunteers from the local community are participating in this year's camp. In addition to sponsors, cybersecurity experts from the following organizations will be on hand to speak to students during the week-long event: Bridgepoint Education, C.A.T.C.H., FBI, Georgia Tech Research Institute, San Diego Police Department, San Diego Gas & Electric, Verizon and more.

At the heart of the Cyber Boot Camp is a computer lab, known to participants as "The War Room," which enables students to practice both computer defense and system penetration in a safe environment. The lab was created by ESET Security Researcher, Cameron Camp, CISSP, who will be on hand to instruct students throughout the week.

One of this year's highlighted activities features an off-campus visit to the Southern District of California U.S. District Court, where the students will engage with Judge Mitchell D. Dembin as he outlines how the choices they make now will have a profound impact on their future.

During the Cyber Boot Camp and in the future, students will be faced with a life-long decision whether to use their highly honed skill set wearing a "white hat" for the good of the nation and future employers or to slip on the "black hat," where they will have to look over their shoulder for the rest of their life. Judge Dembin is proficient at bringing these choices to light in ways that only a former Assistant U. S. Attorney and current Federal Magistrate can.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 2.59%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address, and it tries to download several files from the address. The files are then executed and the HTTP protocol is used. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

2. JS/Kryptik.I

Previous Ranking: n/a
Percentage Detected: 2.35%

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.

3. LNK/Agent.AK

Previous Ranking: 2
Percentage Detected: 1.91%

LNK/Agent.AK is a link that concatenates commands to run the real or legitimate application/folder and, additionaly runs the threat in the background. It could become the new version of the autorun.inf threat. This vulnerability was known as Stuxnet was discovered, as it was one of four that threat vulnerabilities executed.

4. Win32/Sality

Previous Ranking: 3
Percentage Detected: 1.49%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.
It modifies EXE and SCR files and disables services and process related to security solutions.
More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

5. INF/Autorun

Previous Ranking: 5
Percentage Detected: 1.38%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case.

6. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.2%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This treat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://www.eset.com/threat-center/blog/?cat=145.

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders.

7. Win32/Ramnit

Previous Ranking: 7
Percentage Detected: 1.16%

It is a File infector that executes on every system start. It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.

8. HTML/ScrInject

Previous Ranking: 4
Percentage Detected: 1.06%

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

9. HTML/Iframe

Previous Ranking: n/a

Percentage Detected: 1.04%

Type of infiltration: Virus
HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

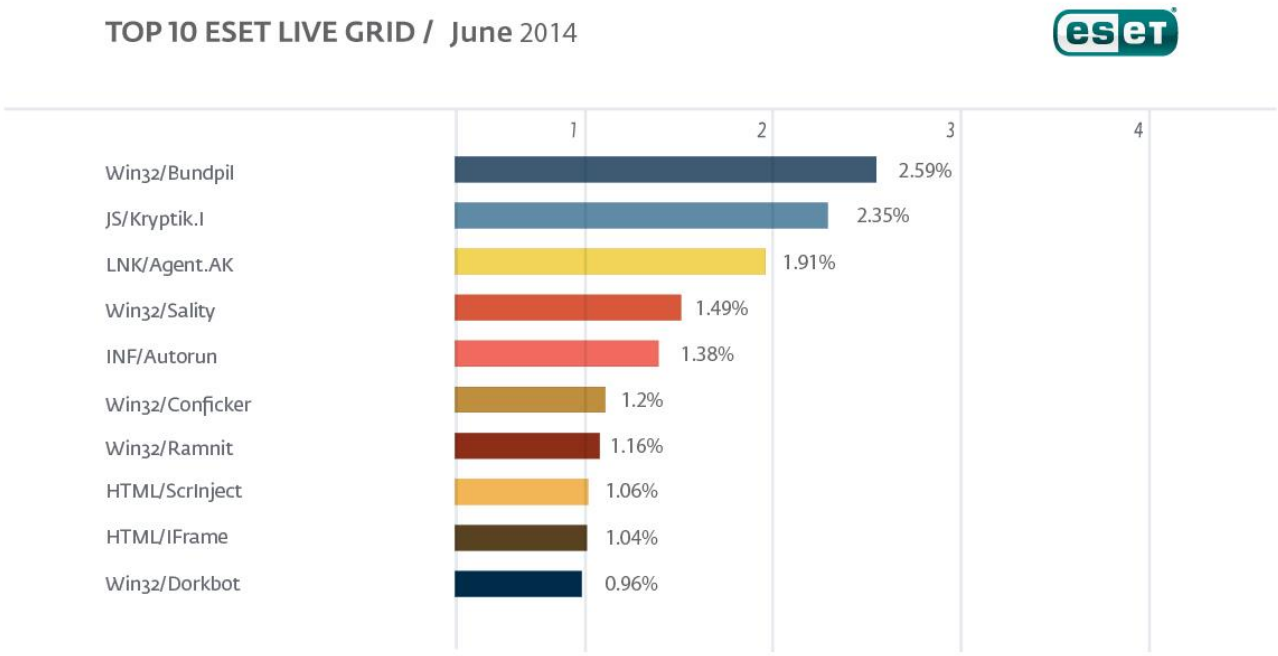
10. Win32/Dorkbot

Previous Ranking: 10
Percentage Detected: 0.96%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX. The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

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 2.59% of the total, was scored by the Win32/Bundpil 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