Threat Radar

April 2013
Feature Article: Spookeasy

eset® ENJOY SAFER TECHNOLOGY™

Table of Contents

Spookeasy

David Harley, ESET Senior Research Fellow

As I blogged recently - SpookSpeak: cryptic, but not cryptographic – a tantalizing note recently went up on the MI5 website (that's the UK's security service, in the unlikely event that you don't regularly visit it).

It warns that people have been contacted by email or by phone by people claiming to be working for the security services, or even from the head of MI5, Sir Jonathan Evans, and making it clear that these are financial scams that have nothing to do with security services or the Director General.

Unfortunately, that's all the warning made clear, and no further information has hit my radar since, but I suppose secrecy is MI5's business. Still, it might have been useful to know more about the type of scam the warning refers to. It could, after all, be anything from a 419 to some form of ransomware, and the ways of recognizing and dealing with those different kinds of scam can be very different. But I have yet to find an actual example.

John Leyden subsequently commented for the Register on the same topic, in MI5 undercover spies: People are falsely claiming to be us (love the subtitle: go and read it!) Leyden referred to that blog and remarked that the warning is more likely to refer to Reveton-like ransomware than to "bogus offers to shift seized assets and the like, the staple of advanced-fee fraud (aka 419 scams)". He's correct, of course, but I had in mind the type of 419 that attempts to extort money by threats of assassination, rather than the "I need you to put £30m of a dead dictator's gold into your Post Office account" type of 419.

In fact, it's actually the use of the Director General's name that makes me think 419: ransomware generally uses the name of an agency to intimidate rather than that of an individual.

There's an amusing variation on the friendly assassin 419 theme noted here - A Deadly 419. Presumably that particular post was meant more as pastiche than a serious threat to extort, but it's based on a sub-class of 419 that has been around for quite a while. Here's part of a more typical example from 2007:

Good day Mr Firstname Lastname ,

I want you to read this message very carefully, and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i have being paid $50,000.00 in advance to terminate you with some reasons listed to me by my employers, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation, Do not contact the police or F.B.I. or try to send a copy of this to them, because if you do i will know, and might be pushed to do what i have being paid to do, beside, this is the first time I turned out to be a betrayer in my job.

Of course, an extortion attempt from 'MI5' might take quite different forms to this assassination scenario: unless Thames House decides to break the habit of a lifetime and release a little more information, who knows ?

I could have told you more about this, but there are some men in black at the door.

ESET at Virus Bulletin

Once again, ESET researchers will be represented at the prestigious Virus Bulletin conference this year. Righard Zwienenberg, representing the Anti-Malware Testing Standards Organization (AMTSO), will present a paper on 'The Realtime Threat List'. Here's the abstract:

Tracking malware threats that users have encountered 'in the wild' has a long history, and is an excellent example of collaboration within the anti-virus industry. For over a decade, the industry has standardized on the WildList, founded by Joe Wells, and currently run by ICSALabs. For many years, this list of active threats has served testers, users, and developers well, but it is not devoid of problems. In particular, the change in the nature of online threats has left the WildList trailing the 'real-time' threat, making it unsuitable for effective 'in-the-wild' testing.

In this presentation we explore the shortcomings of the WildList, and introduce our solution, the Real Time Threat List (RTTL). This list, hosted and sponsored by AMTSO, is based upon Avira's sample sharing system, and is designed to provide a real-time view of threats as they are found in the wild. The list allows for customization of queries to provide testers with information about specific threats in specific regions, as well as several other interesting test scenarios.

The design of the RTTL is such that all AMTSO members can contribute samples to the system. Furthermore, the system lowers the workload for many vendors who already participate in the existing Avira system. As such, we believe it represents a more forward-looking way to track and catalogue in-the-wild threats.

During the talk, we will show the prototype system, and also discuss how we see the system evolving and the new test scenarios that the RTTL enables.

Also, David Harley and Intego's Lysa Myers will present a paper on Mac hacking: the way to better testing? Here's the abstract:

Anti-malware testing on the Windows platform remains highly controversial, even after almost two decades of regular and frequent testing using millions of malware samples. Macs have fewer threats and there are fewer prior tests on which to base a testing methodology, so establishing sound mainstream testing is even trickier. But as both Macs and Mac malware increase in prevalence, the importance of testing the software intended to supplement the internal security of OS X increases too

What features and scenarios make Mac testing so much trickier? We look at the ways in which Apple's intensive work on enhancing OS X security internally with internal detection of known malware has actually driven testers back towards the style of static testing from which Windows testing has moved on. And in what ways might testing a Mac be easier? What can a tester do to make testing more similar to real-world scenarios, and are there things that should reasonably be done that would make a test less realistic yet more fair and accurate? This paper looks to examine the testing scenarios that are unique to Macs and OS X, and offers some possibilities for ways to create a test that is both relevant and fair.

This will be David's 14th Virus Bulletin paper: the others, including several that were written before he started to work with ESET, are available via the Geek Peninsula blog.

Events worldwide April/May

During April, ESET has been present worldwide at the following events:

- April 6th Security Session, at VUT Brno, Czech Republic.
- April 8th HITB EU, in Amsterdam, Netherlands.
- April 11th Infiltrate, in Miami, US.
- April 23th Mobile Rulezz, in Bratislava, Slovakia.
- April 23th Infotrendy 2013, in Bratislava, Slovakia.
- April 23th Infosec UK, in London, UK.
- April 24th APWG Counter-eCrime Operations Summit, In Buenos Aires, Argentina.
- April 25th SYSCAN'13, in Singapore.
- April 27th Android Roadshow 2013, in Kosice, Slovakia.

Furthermore, during May ESET's representatives will be attending to different events such as AMTSO, which will take place from May 14th to the 15th, in Bratislava (Slovakia), where the Real Time Threat List that is going to be launch and demoed.

Likewise, ESET is going to participate in CARO, also in Bratislava and organized by ESET, from May 16th to the 17th, discussing the "what", "when" and "where" of targeted attacks, AV security and APT.

In addition to these activities, ESET will be present at the Interop Conference, the leading business technology event from May 6th to the 10th, in Las Vegas (US).

Finally, on May 24th Robert Lipvosky will participate in PhDays, which features the International information protection CTF contest, and will discuss several topics about hacking activities.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 2.98%

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, as Randy Abrams has suggested in our blog (http://www.eset.com/threat-center/blog/?p=94; http://www.eset.com/threat-center/blog/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. HTML/ScrInject.B

Previous Ranking: 3
Percentage Detected: 2.29%

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

3. Win32/Sality

Previous Ranking: 2
Percentage Detected: 1.82%

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

4. Win32/Dorkbot

Previous Ranking: 5
Percentage Detected: 1.62%

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.

5. HTML/Iframe.B

Previous Ranking: 7
Percentage Detected: 1.48%

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.

6. WIN32/Bundpil

Previous Ranking: 34
Percentage Detected: 1.48%

Win32/Bundpil.A is a worm that spreads via removable media.

7. Win32/Ramnit

Previous Ranking: 5
Percentage Detected: 1.46%

It is a file infector. It's a virus 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/Phishing.LinkedIn.A

Previous Ranking: 18
Percentage Detected: 1.34%

HTML/Phishing.LinkedIn.A is a trojan that redirects the browser to a specific URL location with malicious software.

9. Win32/Conficker

Previous Ranking: 6
Percentage Detected: 1.25%

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 threat 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. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

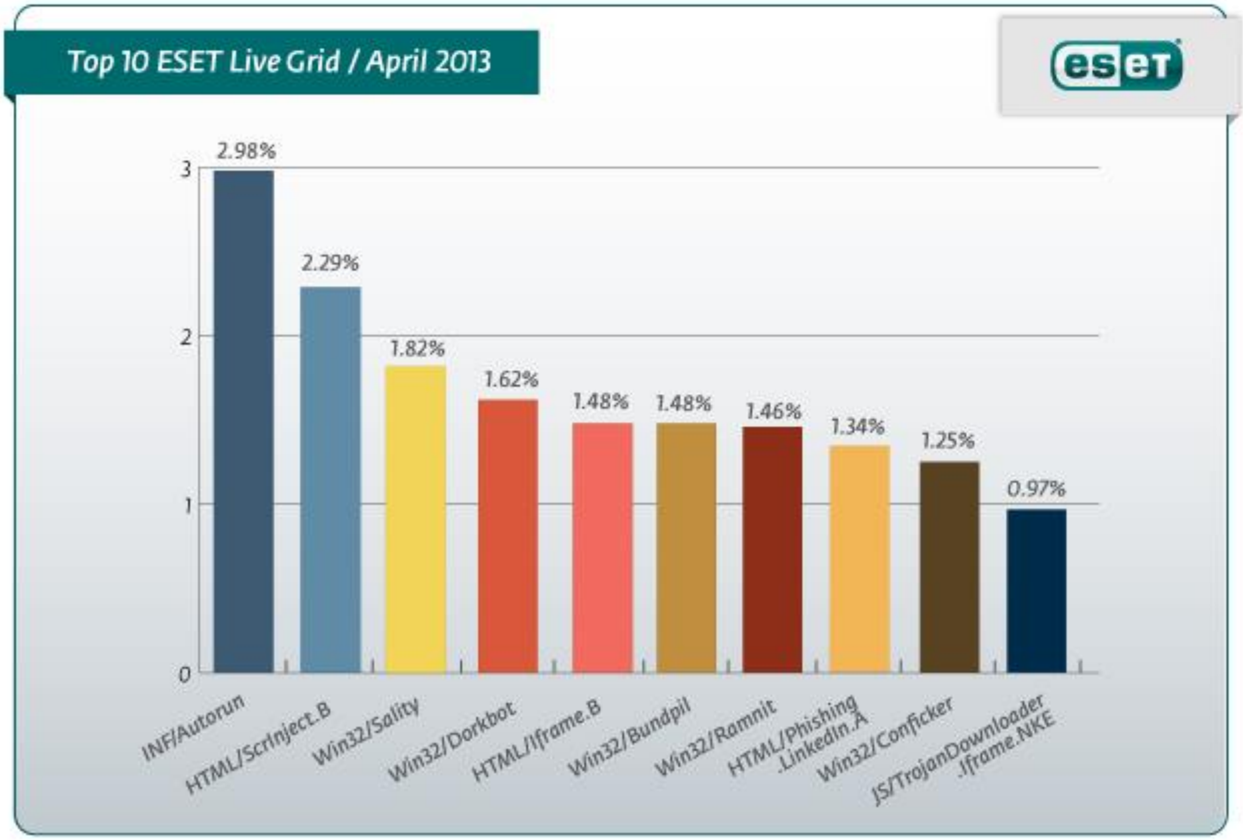
10. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 10
Percentage Detected: 0.97%

It 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.

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 almost 2.98% of the total, was scored by the INF/Autorun 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
- ESET Blog (also available at welivesecurity.com)
- ESET Podcasts
- Independent Benchmark Test Results

Anti-Malware Testing and Evaluation