September 2013
Feature Article: TLDs, Phishing, Business Security and Education

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

TLDs, Phishing, Business Security and Education

David Harley CITP FBCS CISSP ESET Senior Research Fellow

Recently we were asked about the security implications of the new wave of professional Top Level Domains (TLDs), notably .bank. This isn't an issue I've really given much thought to: I only work seven days a week. But it seems to me that the central issue with gTLDs (generic TLDs) like .bank as opposed to specific brand TLDs like .barclays is how much trust you can place in the bona fides of a domain.

Some thought has been put into reducing the risk of trademark infringement and avoiding cybersquatting in terms of brand TLDs, and that has in indirect benefit to the user because it makes phishing somewhat less likely. However, once the domain is approved and launched, how safe it is depends on the good intent and security-awareness of the domain holder.

Very heavy use has been made in recent years of subdomains under TLDs such as .co.cc and .tk to host malicious URLs, as well as TLDs whose core business is to provide subdomains (or sub-subdomains) under their own *.com domain. There's potential here for an expansion of such malicious activity, and I for one am not going to rush to click on any links in any email I receive from {mybank}.bank, let alone such gifts to typosquatting as .comm.

There's recently been a revitalized discussion on Twitter about the much-heralded death of anti-virus. I've been hearing this since about 1994, so it must be going to happen soon. Well, Larry Bridwell and I will be discussing the demise of the industry that pays my bills at the AVAR conference in December, so I won't devote a lot of space to that issue now, but one of the interesting facets of that Twitter threat came out of a blog by Blaze in which he suggests that there is a blame attribution model where various stakeholders – AV vendors, other security vendors, Microsoft, and other application vendors – attribute some blame to one or more of the other players, but all blame the end user.

I agree, that's kind of close to a 'blame the victim' culture like the one that old-school virus writers and new age cybercriminals are both apt to subscribe to. Kurt Wismer points out though that "at the end of the day, no one is expecting the attackers to collectively vanish, so improving things is going to require changes on the part of other players as well, including the users." Improving user awareness across the board – particularly for home users – is a bigger job than I can do justice to in a short article, but how about in the business world? As it happens, that's something else we were asked about recently…

Every kind of business generates and store data that is potentially of interest to cyber criminals, and even the smallest business should assess how valuable or sensitive its data really is, by performing a formal security audit if appropriate. Businesses of any size are also subject to national data protection laws and need to be aware of these and of the penalties for non-compliance.

As part of their risk analysis, businesses (irrespective of their size) need to consider the impact of a security breach on the business, thinking about who or what would be affected and whether the business could continue to trade if a breach was successful. Once it has a clear view of the risks it can then decide how to communicate network security policies to its staff.

The first step is to make sure staff are aware of the risks from cyber-criminals. Although cybercrooks are sometimes very

cunning and sophisticated, their impact can be drastically reduced by some simple preventative measures and education. Good user education is a filter, not a flood: you can't educate effectively by hitting people with 'everything they need to know about security' in one massive hit: it's an ongoing process that focuses on essentials, on teaching the user to extrapolate from one example scenario to others, and reinforcement of core messages over the whole period where the staff member works for the company.

It's essential to create a culture of security awareness where all staff, regardless of level and role, take it for granted that they are part of the solution.

For cyber security efforts to be as successful as should be, everyone needs to know and understand what the organisation's cyber security policies are, how to comply with them through proper use of controls, why compliance is important and the possible consequences of failure to comply (to the company *and* to the individual).

The goal should be the creation of a "security-aware workforce": not a workforce comprised entirely of security gurus, but one where employees are empowered to report risky practices to management. Staff training sessions should make employees aware of such things as email safety, password usage, safe mobile use and the importance of data protection, and an Acceptable Use Policy (AUP) for all staff, including approved web and social media usage. Policies, controls and security education should also take into account data-sharing relationships with partners, vendors and clients. An authoritarian approach to security enforcement with draconian penalties won't suit every environment, but employers should spell out that a breach of security can be very bad news for business and threaten its continued operation. If there are specific disciplinary consequences, they need to be clearly documented so that staff are in no doubt as to their existence.

Education is not a one-time, one-shot process. People forget what they don't use, and have to be reminded and even re-trained. People are better at complying with policies when they understand the rationale behind them. Even assuming that they intend to comply, they're likelier to remember to comply if they understand why they *should* do X and *shouldn't* do Y.

Since education *is* an on-going process, HR can play an important role in ensuring that everyone receives suitable and consistent training in the form most appropriate to their role. IT and HR need to liaise to ensure that people have appropriate training and system privilege levels as they enter the organisation and change roles, and to ensure that they don't retain inappropriate access once they leave.

ESET @ Virus Bulletin Conference

The 23rd Virus Bulletin International Conference - will take place **2-4 October 2013** in Berlin, Germany. You can take a look at the programme here: http://www.virusbtn.com/conference/vb2013/programme

There will be some ESET speakers participating in the event. Here are the abstracts of the presentations:

Andrew Lee

Keynote: Ethics and the AV inudustry in the age of WikiLeaks

The events of the last few years from Bradley Manning to Edward Snowden have brought with them a tranche of new ethical issues. On the one hand the 'old-school' approach is to see malware, detect malware, but it is increasingly likely that in future (if not already) companies will come under pressure from government agencies and perhaps be compelled by law, to avoid detection, disclose data or report on customer activity. Is there a need for a collective response from the industry? Do we all sink or swim alone? What are the issues around trusting sample or vulnerability sharing with companies known to share (or to be compelled to share) such information with governments?

In his keynote address, Andrew Lee aims not to provide all the answers, but to open a wider conversation by examining some of the issues and asking the relevant questions.

Righard Zwienenberg, Richard Ford, Thomas Wegele

The Real Time Threat List

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

Stephen Cobb

What can Big Data Security learn from the AV industry?

The anti-virus industry has several decades of experience sharing threat data between competing vendors, private enterprises, public institutions, and non-governmental organizations. In this paper we examine the history of this pioneering threat data sharing for lessons that can inform the evolution of Big Data Security.

Big Data Security is this year's hot information security concept, a key element of which is using shared threat data, along with internal data, to detect and mitigate threats to information systems. Big Data Security is defined as more than either SIEM or NBA, both of which are characterized as limited visibility solutions. The goal of Big Data Security is full visibility into all aspects of all the data, all the time, so that near real-time

analysis of OSI layers 2 through 7, plus threat data feeds from beyond the enterprise, will produce faster, better threat detection and response.

This goal cannot be achieved without timely access to shared threat data, ranging from malicious code signatures and malicious URLs to whitelists, incident profiles and more. We will determine how the anti-virus industry's experiences may inform the development of Big Data Security in the areas of standards, legal constraints, privacy concerns, logistical challenges, and more.

David Harley and Lysa Myers

Mac hacking: the way to better testing?

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.

Robert Lipovsky, Anton Cherepanov

Last-minute paper: Hassle with Hesperbot: a new, sophisticated and very active banking trojan

In the middle of August 2013 we discovered a trojan horse that was hosted on a domain that passed itself off as belonging to the Czech Postal Service. Looking further into this discovery, we found out that this was a new banking trojan targeting potential victims in the Czech Republic through active malware-spreading campaigns. Later in our research we found similar campaigns and, as a result, active botnets in Turkey and Portugal as well. The perpetrators of the botnets most certainly knew what they were doing and also utilized malicious components designed for mobile phones.

What we found lurking behind the malicious links was not the ubiquitous Zeus or SpyEye however, but a new malware family, which we named Win32/Spy.Hesperbot. Analysis of the threat revealed that we were dealing with a very potent banking trojan which features common functionalities, such as keystroke logging, creation of screenshots and video capture, and setting up a remote proxy, but which also includes some more advanced tricks, such as creating a hidden VNC server on the infected system. And of course the banking trojan feature list wouldn't be complete without network traffic interception and HTML injection capabilities. Win32/Spy.Hesperbot does all this in quite a sophisticated manner and also utilizes the mobile components for Android, Symbian and Blackberry to overcome banks' security through mobile transaction authentication numbers.

The malware implements a unique technique for carrying out man-in-the-middle attacks against users connecting to their

secured online banking websites. This will be described in detail in the presentation. A similar technique was used by the Gataka banking trojan (presented at VB2012 by Jean-Ian Boutin). We will compare and contrast these two dangerous cybercrime tools.

We'll also explain the modus operandi of the scams and give details on the different campaigns that we've discovered. After a higher-level perspective on the functioning of the malware and motives of the attackers, we'll take a deeper look at some of the more sophisticated code that makes Win32/Spy.Hesperbot stand out, including its mobile components.

ESET Corporate News

ESET Reports Major Increase of Dangerous Filecoders

ESET HQ Malware Research Lab is reporting an unusual spike in the activity of Filecoder malware - Trojans that encrypt user files and try to extort a ransom from the victim in exchange for a decrypting software. ESET LiveGrid® technology - the company's cloud-based malware collection system - has shown a rising weekly number of Win32/Filecoder detections by over 200% since July 2013 from average numbers in January - June 2013.

More information:
http://www.welivesecurity.com/2013/09/23/filecoder-holding-your-data-to-ransom/

ESET Protects Mac users with ESET Rootkit Detector

ESET® Rootkit Detector is a new security tool for Mac® OS X that scans for malicious kernel extensions attempting to change operating system behavior by hooking inside the OS. When the rogue kernel extensions hook inside the OS X, they can bypass any security measure thus allowing complete access of system privileges.

ESET Opens Branch in Australia

ESET has opened a branch in Australia, Sydney, helping SMBs to tackle threats as Trojans targeting LinkedIn. Florin Vasile was appointed to the role of Country Manager, Australia, to grow the local business and provide renewed focus on developing the ESET partner program. Mr. Vasile joins ESET from a background of executive positions with leading IT&C companies in multiple countries and continents. According to ESET semi-annual Threat Report in Australia, from January to August 2013, the malware targeting social networks is on rise. The biggest single threats came from the group of malicious software commonly grouped as Trojans. Trojans are typically used by criminals to steal data. According to the report, Trojan activity has been on the rise over the past six months. Small to medium businesses are being targeted in particular, and especially via LinkedIn, a software platform increasingly used by people seeking work opportunities or employers looking to find staff.

ESET Uncovers Advanced Banking Trojan "Hesperbot"

ESET HQ malware research lab has uncovered a new and effective banking trojan which targets online banking users in Europe and Asia. Using very credible-looking spreading campaigns related to trustworthy organizations it lures victims to actually run the malware. Several victims have already been robbed of financial assets because of this newly-revealed threat. Based on LiveGrid® data – ESET's cloud-based malware

collection system – hundreds of infections have been detected in Turkey, dozens in the Czech Republic, United Kingdom and Portugal. This very potent and sophisticated banking malware dubbed Hesperbot is spreading via phishing-like emails and also attempts to infect mobile devices running Android, Symbian and Blackberry.

More information:
http://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/

ESET Tops the Security Software Consumer Satisfaction in Japan for the 3rd Time

ESET has been for the third time in a row announced the leader in Consumer Satisfaction Survey by the Kadokawa ASCII General Research Institute* in Japan. ESET has again obtained the top 88.4 points score which is 13 points higher than the closest competitor, Kaspersky® and more than 10 points higher than Kingsoft®, the winner of the non-paid AV category. ESET security solutions were ranked as the best among paid AV products in several categories, including the Response Speed of Resident Software, Security Performance, Support categories.

More information:
http://www.eset.com/int/about/press/articles/article/eset-tops-the-security-software-consumer-satisfaction-in-japan-for-the-3rd-time/

Events worldwide September/October

During September, ESET has been present in Security Days, which is a set of presentations for primary and highschool students with insights into the latest security trends. This event took place in Donovaly and Kosice (Slovakia), from September 20th to October 3rd.

Also, during October, ESET's representatives will be attending to the following events:

- September 30th – October 4th, Interlop 2013 conference in New York (US).
- October 2nd – 4th, Virus Bulletin Conference in Berlin (Germany).
- October 9th – 10th, Secure 2013 conference in Warsaw (Poland).
- October 11th – 12th, Hacktivity IT Security Festival in Budapest (Hungary).
- October 22nd – 24th, Hack.lu convention in Luxembourg.
- October 24th – 25th, T2 conference in Helsinki (Finland).

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 3.69%

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. INF/Autorun

Previous Ranking: 5
Percentage Detected: 2.08%

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.

3. Win32/Sality

Previous Ranking: 4
Percentage Detected: 2.05%

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. HTML/Iframe

Previous Ranking: 1
Percentage Detected: 1.78%

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.

5. HTML/ScrInject

Previous Ranking: 3
Percentage Detected: 1.73%

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

6. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.59%

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.

7. Win32/Conficker

Previous Ranking: 6
Percentage Detected: 1.58%

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.

8. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.43%

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.

9. Win32/Qhost

Previous Ranking: 9
Percentage Detected: 1.23 %

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.

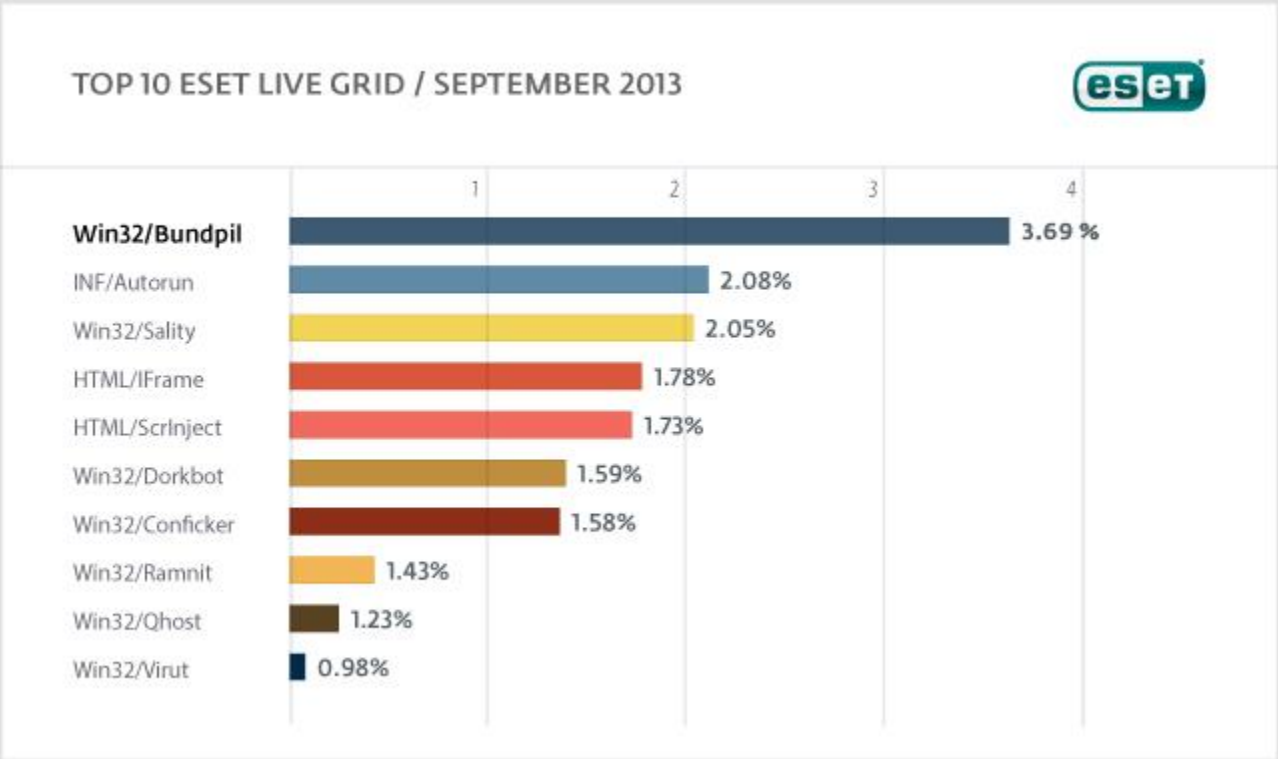
10. Win32/Virut

Previous Ranking: 10
Percentage Detected: 0.98%

Win32/Virut is a polymorphic file infector. It affects files with EXE and SCR extensions, by adding the threat itself to the last section of the files source code. Aditionally, it searches for htm, php and asp files adding to them a malicious iframe. The virus connects to the IRC network. It 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 almost 3.69% 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
- ESET Blog (also available at welivesecurity.com)
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation