August 2015
Feature Article: Grumpy Old Researchers

ENJOY SAFER TECHNOLOGY™

Table of Contents

Grumpy Old Researchers

David Harley, ESET Senior Research Fellow

The US research team was recently asked whether they had any thoughts about what they considered to be the most ridiculous security lingo. (It was actually in connection with a Twitter chat run by NCSA: if you want to hear what else was discussed, search for #ChatSTC.

I suppose after nearly three decades in security it's not surprising that I've become so inured to security jargon that my first thoughts were not particularly security-related:

> *Who wallpapers a desk(top)? Or, come to that, their windows? And why isn't it 'Windows are shutting down'? (Perhaps it should be drawing the curtains? Shuttering down?)*

However, in the ensuing discussion, we found quite a lot of common ground. If only a tendency towards grumpiness, with a tendency to linguistic pedantry that would gladden the heart of Lynne Truss, author of *Eats, Shoots & Leaves: The Zero Tolerance Approach to Punctuation*.

One of our number observed:

> *The names of the threats we protect people against are ridiculous.*
>
> *Virus… as in a biological pathogen?*
>
> *Worm… as in a nematode? Earthworm Jim?*
>
> *Trojan… I'm not even going to go there.*

Another took up a related theme.

> *The questionable use of benign to describe malware that has no malicious (or should I say malign?) payload even though that doesn't stop it being damaging. I'm fully aware of its medical applications, of course, but it's misleading there, too. And it doesn't improve the dubious analogy between computer viruses and biological pathogens to mix them up with other biological phenomena.*

Call of the WildList

A throwaway grumble about zoos and the WildList got me thinking.

What's with the concept of a zoo of viruses? Are we talking about cells in cells, or at any rate in cages? What about the antithetical concept of 'in the wild' (In the Wild, in-the-wild, ItW)? In the heyday of the WildList, it was quite a useful concept, a way of distinguishing malicious programs that were out there and posing a threat to everyday computer users rather than those that were to be found only in zoos (or collections). The collection of malware called WildCore maintained by the WildList Organization is, in the current threatscape, closer to a zoo than it is to anything that lives where the wild things are.

The main reason WildCore is still used in certification testing is that it offers a baseline performance indicator that all detection-oriented security software should be able to handle, being a collection of agreed, verified samples. But most malware isn't static: samples don't generally circulate 'in the wild' for any length of time, whereas ancient boot-sector viruses kept turning up (and thus keeping their place on the list) for years on end. So that process of verification means that in most cases, the samples used in testing have already passed their best-by date.

Best Practice, Worst Practice

One of us remarked:

> *Best practice – who says? Usually someone who's marketing a product or service...*

Others were in agreement:

> *Indeed, I almost always disagree with so-called best practices. They are often a good baseline, but for the experienced techie, there's sure to be a tweak or even a major change that will, at least in that tech's environment, be better than the supposed "best practice." Just call them "Baseline Security Benchmarks" and I'd be happy as a clam, though. Probably.*

Robert Slade, in his 'Dictionary of Information Security', mentions a discussion on the CISSPforum in 2005 that noted that:

> *…"best practice" is never a guarantee or panacea. Other phrases discussed were standard practice (what most people do), essential practice (what should be done as an absolute minimum), and leading practice (what the "best" companies do).*

Cyberdrivel

Here are two very similar opinions on the escalating popularity of the word 'cyber':

- *The use of 'cyber' as a noun. It's bad enough using it as a vague term denoting information technology in general, or networking, as the US military uses it. In the UK, law enforcement has a nasty habit of using it as a vague equivalent to computer crime. Or cybercrime, if you must. Actually, the use of 'cyber' as a prefix, 9 times out of 10.*

- *Someone in some Marketing department somewhere thought "digital" or "computer" or "IT" felt old or overused, so they decided to use cyber in front of anything that had anything to do with a computer, networking, the internet, etc. Brace yourself: the days of the "Cyber" department in a corporation are coming. I shudder at the thought.*

Right as a Trivium

Then there was this point.

> *The answer is trivial.*
>
> *People talk about security issues and obstacles as being trivial meaning "easy to overcome" but that is a highly relative use of the term that "trivializes" the problem and misleads 99% of the audience.*

I must admit to having used 'trivially' in the sense of 'commonplace', which is defensible but could mislead. I probably need to rethink that. ☹

There was also a black mark against 'verbifying of any sort, in Security or elsewhere. Grrrrr.' It took me a moment to think of an example of security verbifying, but I will admit that my hackles do rise at the use of 'leverage' as a verb. Then I remembered seeing the word trojan used as a verb where most of us would probably use Trojanize (or trojanize). Actually, I found it in a chapter I was commissioned to rewrite for a book called *Maximum Security*, and felt honour-bound to mention it, but that doesn't mean I like it. And that's before we even get into the argument (previously referred to above, obliquely) as to whether it's Trojan or trojan when referring to malware. Well, I guess the security industry moved on to this after we got tired of trying to establish universally accepted definitions of worm and virus.

The issue, if you're really this short of something to worry about, is this. Trojan is a 'proper adjective', meaning that it's derived from the proper name Troy, so it's normally capitalized as in Trojan Horse (if you're referring to the one in the Iliad) or Trojan horse more generically. There are those who believe that the use of the term is far enough removed from its original sense when applied to malware – especially when the horse is allowed to bolt for the sake of brevity – to justify the use of the uncapitalized form. There is an argument for this: for example, the diesel in diesel engine derives from the name of its inventor, Rudolf Diesel. I think the process of severance is

established just enough for any of these forms to be considered defensible.

Consider Yourself Assured

Another objection was raised to *Information Assurance* as representing "Information Security."

> *I don't know about you, but in my book, if you give me "security", I feel secure. If you give me "assurance", I think I might be secure, but I also think that more probably you are probably trying to sell me a bill of goods.*
>
> *[I also assert that those who offer "Information Assurance" usually are trying to sell you a bill of goods -- more than those who profess to offer "Information Security", anyway.]*

I have to agree.

In fact, the renaming and redefining of threats and solutions is classic marketspeak: consider, for instance, the use of the term APT (Advanced Persistent Threat) to describe something that may or may not be advanced, but is assumed to be so sophisticated that it defies detection except by certain products that have apparently rendered anti-malware redundant. And don't get me started on signatures.

ESET Corporate News

ESET Launches Free App to Detect Android Stagefright Vulnerability

ESET® announced the availability of a free Android app - ESET Stagefright Detector – which helps users determine if their Android device is affected by the critical Stagefright exploit. The app is available in the Google Play Store now.

First discussed at Black Hat 2015, the Stagefright vulnerability allows attackers to gain control of Android phones via the Stagefright library, an open-source media player used by 95 percent of Android devices. The vulnerability gives attackers access to most of the victim's phone data including email, photos, and personal information by simply sending an MMS (Multimedia Messaging Service) message to the victim's Android smartphone.

ESET StageFright Detector works with Android 4.0 and older versions of the Android operating system. The new ESET app alone cannot repair the vulnerability, however once users activate the app and determine whether their Android smartphone is vulnerable they can click on the "Learn More about Stagefright" icon. This takes users to the ESET Knowledgebase article which provides safety steps to protect their data.

ESET Announces Appointment of Country Manager for Canada

ESET® has announced expansion into the Canadian market with the opening of a Canadian office and the naming of Iva Peric-Lightfoot as Country Manager for Canada. Iva will manage operations of ESET's new Toronto office, with a focus on channel sales, marketing and distribution. The appointment is effective immediately.

With more than 20 years in the technology industry, Iva Peric-Lightfoot has significant experience developing and implementing national and international channel strategies.

Expansion into Toronto, Canada's largest technology hub, will complement the existing ESET research offices in Montreal and position ESET to better meet customer demand across Canada.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 4.86%

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

*.exe

*.vbs

*.pif

*.cmd

*Backup

2. Win32/Qhost

Previous Ranking: N/A
Percentage Detected: 2.25%

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

3. Win32/Adware.MultiPlug

Previous Ranking: 3
Percentage Detected: 1.90%

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. LNK/Agent.AV

Previous Ranking: 5
Percentage Detected: 1.66%

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.

5. HTML/Refresh

Previous Ranking: 9
Percentage Detected: 1.62%

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.

6. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.36%

Sality is a polymorphic file infector. When it is 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

7. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.30%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and searches for htm and html files into which it can insert malicious instructions. 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. LNK/Agent.BS

Previous Ranking: 6
Percentage Detected: 1.29%

LNK/Agent.BS 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.

9. INF/Autorun

Previous Ranking: 10
Percentage Detected: 1.16%

INF/Autorun is a generic detection of multiple malicious versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malicious executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malicious 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.

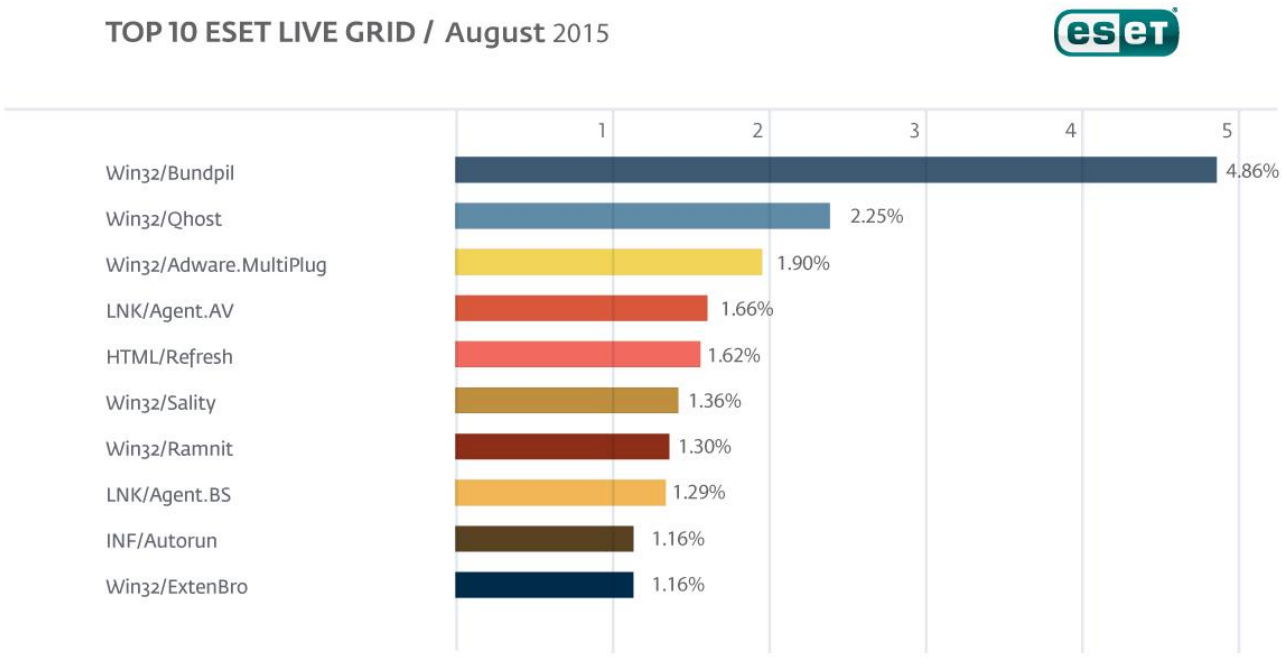
10. Win32/ExtenBro

Previous Ranking: N/A
Percentage Detected: 1.16%

Win32/ExtenBro is a malicious extension for a web browser distributed by Social Networks, and aims to intercept and steal data from the user's activities.

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 4.86% 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