Threat Radar

July 2013
Feature Article: Keyboards and Keywords

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Keyboards and Keywords

David Harley, ESET Senior Research Fellow

A version of this article also appeared on the Anti-Phishing Working Group blog.

The Wikipedia entry for 'error message' includes a number of infamous (and confusing) error messages, though it doesn't include my all-time favourite:

> Keyboard not found! Press any key to continue

And no, that's not an urban legend. While I'm not sure that was the exact wording, I did see more or less that same error message two or three times back in the days when user support was part of my job.

The reason that I was scouring the web for links related to 'error messages' and 'security alerts' is this: I happened across an article on the American Psychological Association web site that told me that Gary Brase (a psychologist) and Eugene Vasserman (a computer security researcher), of Kansas State University, have been given a $150,000 grant for research into developing more effective online alerts. I don't know how many security companies have explored this approach – though I don't believe for a moment that *no* security company has *ever* involved psychologists, focus groups, and ergonomists (amongst others with interest and expertise in aspects of human-computer interaction) in the development of a product and its user interface – but I'm sure we've all seen enough in the way of confusing software-generated alerts to agree that some software could do with a little more attention to the HCI dimension. There is a special place in my heart for the sort of alert that we often see along the lines of 'EICAR test virus not-a-virus detected'.

In fact, while I may be biased – my own academic background was originally in social sciences, computer science being a later add-on – I don't think that computer security that's focused entirely on bits and bytes is ever going to solve the world's problems with cybercrime, cyber-espionage, and all the other cyber-issues du jour. Certainly the kind of security alert that leaves the user wondering "What the heck does that mean? What does the darn thing want me to do?" is failing some kind of usability test.

The APA article includes a couple of examples cited by Brase:

> "Do you want to trust this signed applet?" or "This application's digital signature has an error; do you want to run the application?"

Frankly, I've seen far more confusing examples guaranteed to have the end user running to the nearest wall to bang his head against it. Such as any message that includes an error code or a hex string, or something like 'unknown error scanning file [filename]', or even a blank message box, but these examples do finger an essential problem with security alerts that I'm not sure $150k is going to be enough to fix.

The problem with Brase's examples isn't the wording, it's conceptual. If the algorithm behind the program isn't able to make a reliable determination of the risk, why should we expect the everyday user to be able to? Actually, he might: maybe he knows that a site is (normally) OK, even if he can't be sure that it hasn't been compromised in some way. Software has the disadvantage that it can only deduce intent from the programmatic characteristics of a program, or from automated textual analysis. And while filtering has progressed immeasurably from the days when phrases like 'magna cum laude' or the name Scunthorpe triggered porn detection algorithms all over the globe, there are still many contexts where an informed human being can make a better decision than an email or web filter. But 'informed' people aren't the main target for research like this: rather, Brase states that "Good security alerts should be tailored for all types of users, no matter what their intent," which suggests a wide range of skill/knowledge levels, as well as a wide range of target sites. There's an important point there: I'm in agreement with being in touch with the intent of the user as well as that of the malefactor. In fact, Jeff Debrosse and I wrote a paper a few years ago in which we suggested that security companies could increase their effectiveness by incorporating analysis of the user's behaviour into the software as well as analysis of programmatic behaviour – Malice Through the Looking Glass: Behaviour Analysis for the Next Decade – though I'm not holding my breath waiting for that approach to catch on. It is one way, potentially, of addressing another of Brase's points: i.e. that 'user education has not kept pace with the increasing complexity of Internet transactions.' That, at least, is perfectly true. I'm all for making computers people-literate (the very apposite title of a book by Elaine Weiss).

The logical flaw here, though, is this: improving the *presentation* of security alerts won't make security software (or other software with some security functionality, such as a browser using technology like Google's Safe Browsing, for example) any more capable of discriminating between human motivation than it already is. That's not such a negative comment as it sounds: programmatic filters don't in themselves 'detect' malicious intent, but they do reflect the programmer's understanding of *some* behaviour – programmatic or semantic – characteristic of malicious intent. But malicious behaviour is not a constant, not static. The average security program is a long way from achieving the same discrimination in analysing textual content that a moderately psychologically-aware human being is capable of.

The Google technology is actually a pretty good illustration of the limitations of technology for countering attacks that are primarily social engineering. Google tells us that Safe Browsing currently flags an impressive 10,000 sites per day as malicious, data that it now draws on for its Transparency Report. Yet phishing is considered to be a more effective attack than ever, many years after it first came to prominence as a major threat, though email is no longer its primary entry point, whereas web browsers and web-hosted services such as social media account for a high proportion of phish delivery.

This is by no means a criticism of Safe Browsing, which is a very useful layer of protection for web users (not just Chrome users – the technology is used by Firefox and Safari too), and I applaud their efforts. After all, anti-malware technology isn't capable of detecting 100% of malicious programs and URLs either: if it were, this would be a very different world. For a start, we wouldn't need to pop up any alerts asking users to answer questions they don't understand: we'd simply tell them that the site or application they were trying to access would not be allowed to run, as the app believed it to be malicious.

But here in the real world, we need to bear in mind that there are plenty of malicious sites and other vectors out there – our lab processes several hundred thousand threats per day, and they don't all come from those 10,000 web sites. So while Google's Transparency Report statistics may prove interesting and useful – and no doubt have some PR value – end users should continue to be vigilant and take care in selecting which sites they visit, rather than assuming that they can click where they like because they have protection.

It's not all bad news, though. I've just seen what may be the most inept 419 scam email of all time.

- The sender is one Gen Peter Blay
- The subject line reads “1”
- The body text: well, technically, there is no body text. However, there is a signature: “your retrieve donation”

It’s hard to believe that there is anyone naïve enough to fall for that. Not least because it’s unclear from that what the scam actually is (presumably some form of advance fee fraud, though), let alone what the scammer needs the victim to do in order to execute the scam.

In other contexts, I’d probably write this off as an example of a spammer/scammer test run. In this case, though, I’m in some doubt as to whether he’ll work out how to do a 419 spam run before he expires from starvation. But perhaps I’m doing him an injustice. In that case, Gen Pete, just send the million dollars to me care of the ESET North America office.

ESET Corporate News

ESET has received its 80th VB100 Award and celebrates a record of 10 years consecutive VB100 Awards

At the beginning of July, ESET has celebrated an AV industry record - 10 years of consecutive VB100 awards, as well as its record breaking already 80th VB100 Award from Virus Bulletin, a well-known independent security software testing organization. In both cases, ESET’s NOD32® technology has received more VB100 awards than any other AV software vendor on the market. Passing the “VB100“ certification reflects overall capabilities of both - the tested AV product and the Research and Development Team - in detecting all the so-called “In-the-Wild“ malware and having zero false positives.

The Rise of TOR-based Botnets

In 2013, ESET researchers had already detected TOR-based botnets, however during the summer they have observed a growth in the numbers of malware families starting to use TOR-based communications. In July, ESET researchers Anton Cherepanov, Malware Researcher and Aleksandr Matrosov, Security Intelligence Team Lead, detected two different types of TOR-based botnets based on the malware families Win32/Atrax and Win32/Agent.PTA. Both botnets have form-grabbing functionality for possible further fraud operations.

Events worldwide July/August

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

- July 27th – August 1st BlackHat USA and Defcon, in Las Vegas (US).

Also, during August, ESET’s representatives will be attending to the GamesCom 2013, from August 15th to the 21st in Cologne (Germany), which is Europe’s biggest trade fair for interactive games and entertainment

Furthermore, from August 23rd to the 26th in Telford (UK), Insomnia will take place, which is the biggest gaming festival in the UK.

The Top Ten Threats

1. WIN32/Bundpil

Previous Ranking: 1
Percentage Detected: 3.78%

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. HTML/ScrInject

Previous Ranking: 2
Percentage Detected: 2.30%

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

3. INF/Autorun

Previous Ranking: 3
Percentage Detected: 2.23%

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.

4. Win32/Sality

Previous Ranking: 5
Percentage Detected: 2.18%

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. HTML/Iframe

Previous Ranking: 6
Percentage Detected: 2.04%

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.

6. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.75%

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: 8
Percentage Detected: 1.71%

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. JS/Chromex.FBook

Previous Ranking: n/a
Percentage Detected: 1.55%

JS/Chromex.FBook is a trojan that posts messages to user profiles on Facebook. Depending the variant of the family, the threat could be a malicious Google Chrome or Mozilla Firefox extension/plugin.

9. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.41%

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.

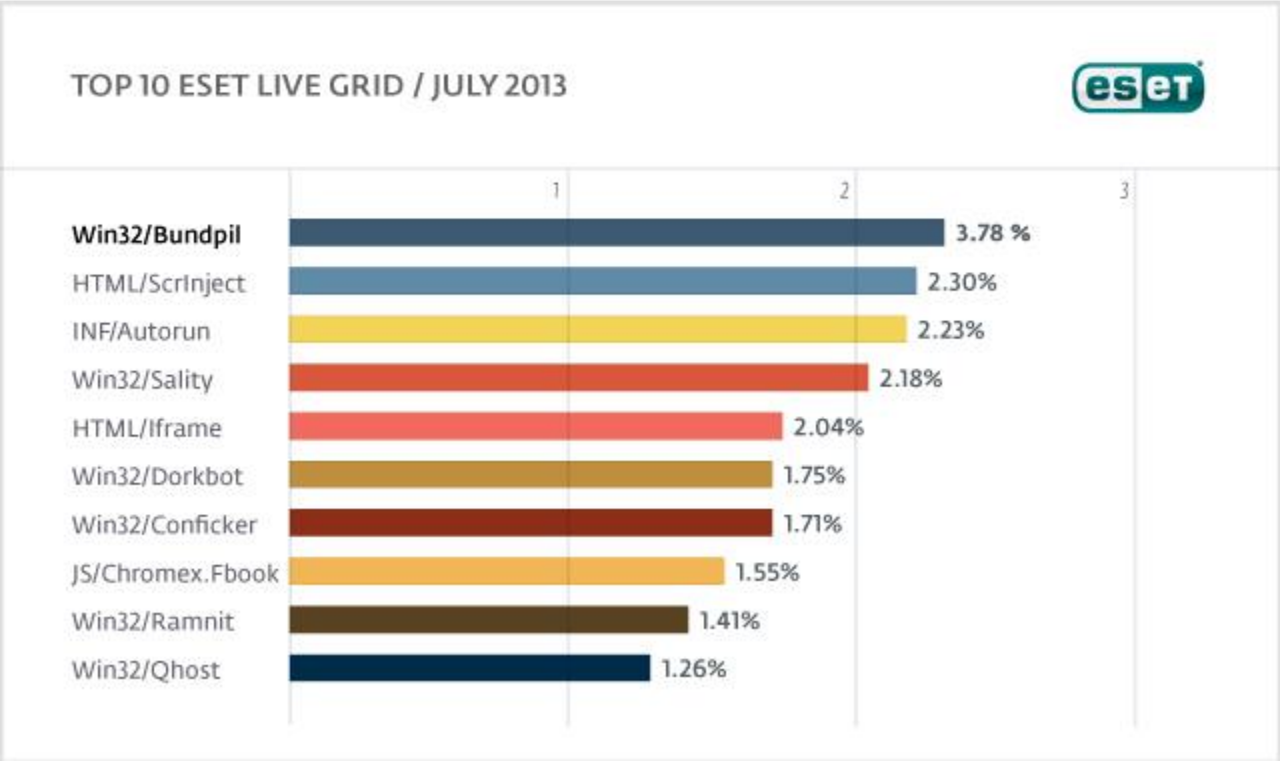
10. Win32/Qhost

Previous Ranking: 10
Percentage Detected: 1.26 %

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.

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 3.78% 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