November 2014
Feature Article: Virus Bulletin and AVAR: a conference paper is for life

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Virus Bulletin and AVAR: a conference paper is for life 3
Support Scams: the gift that goes on taking 4
ESET Corporate News 6
The Top Ten Threats 7
Top Ten Threats at a Glance (graph) 10
About ESET 11
Additional Resources 11

Virus Bulletin and AVAR: a conference paper is for life

David Harley, ESET Senior Research Fellow

In the specialist anti-virus industry – though really there are no major companies that *only* do anti-virus any more – the flurry of conferences that starts to kick in at the end of the summer tends to start winding down with the AVAR (Association of anti-Virus Asia Researchers) International Conference. As 2014 draws to a close, so does the security conference season, for the moment. However, a conference paper is for life, not just Christmas. (Well, I try to keep all mine available, even though some of the earlier ones are mostly only of historical interest).

Since the Virus Bulletin conference in September, Martijn Grooten has published a series of blogs about papers from the conference that have been made available on the VB site, including a paper by Jean-Ian Boutin in which he discusses the commoditization of web injects, and a paper by Eugene Rodionov, Aleksandr Matrosov and myself on the continuing evolution of bootkits.

- VB2014 paper: The evolution of webinjects
- VB2014 paper: Bootkits: past, present & future

The blogs include links to the papers in HTML and PDF formats, and the slide decks, all of which are available on the Virus Bulletin web site, and the videos on VB's YouTube channel, which show the slides as background to the audio from the actual presentation.

A quick link for the Bootkit paper is here (PDF), and for the Bootkit presentation here. The webinjects paper is here (PDF), and the corresponding presentation here. Much more information is given in the Virus Bulletin blog articles. The blog series also includes similar articles linking to other papers and presentations from VB2004.

Meanwhile, there was the AVAR conference in Sydney. This year's conference in Sydney, appropriately called 'Security Down Under', was the 17th AVAR conference. Wow… It hardly seems yesterday since a speaker at a Virus Bulletin conference invited me to join the fledgling organization, though it wasn't till 2003 that I actually got there and presented my first AVAR paper. (As it happens, that was also held in Sydney.) This year, my paper **Lemming Aid and Kool Aid: Helping the Community to help itself through Education** was co-written with ESET Latin America's Sebastian Bortnik, and he did a great job of presenting it at the conference. That paper is now available here, and there'll be a blog or two expanding on the topic shortly.

I don't know if there are any such plans for Peter Kosinar's presentation on **Stealing the internet, one router at a time** or Sébastien Duquette's talk about **Exploitation of CVE-2014-1761 in targeted attack campaigns**, but both were well received, even by our competitors.

However, the presentation voted top of the AVAR pops was Graham Cluley's keynote presentation, on **What 20 years working in the Anti-Virus industry taught me.** Having known Graham pretty much all that time, I was confident that he'd have some interesting reminiscences and insights, and that confidence proved justified. In spite of his indescribable rendition of his AntiVirus Industry Song. But he did promise never to sing it again. (We can but hope).

The same may not be true of the motley crew of slightly more

musical security researchers who couldn't resist getting up to play at the party after the conference: after all, it's become almost traditional to have such an event at the end of meetings in which ESET has had a hand. Here's a sample courtesy of YouTube and AV-Test's Andreas Marx…

Support Scams: the gift that goes on taking

This is an expanded version of an article that originally appeared on the IT Security UK site.

Will no-one rid us of these turbulent tech support scammers with their cold-calling, their misleading advice, fake viruses and fake support package deals? It was back in the early summer of 2010 (it seems much longer!) that I first wrote about a support scammer claiming to represent Microsoft who rang a potential victim…

"…informing him that notification had been received concerning a virus infection on his PC, and offering to help him to install antivirus software."

At that time I was particularly irritated because: "When asked what antivirus software was being offered, the caller claimed that it was ESET's…", and no security company wants to be accused of unethical selling practices.

However, this turned out to be the tip of a very large and ugly iceberg, with a wide range of increasingly sophisticated gambits used to trick the victim into thinking they needed 'help'. A lot of time and effort expended on raising awareness of the issue doesn't seem to have paid much in the way of dividends. However, Kelly Fiveash, for The Register, recently reported that US court SHUTS DOWN 'scammers posing as Microsoft, Facebook support staff': Netizens allegedly duped into paying for bogus tech advice.

The documentation lodged by the Federal Trade Commission in the case of the New York-based company Pairsys Inc. suggests that the scam, if the allegations turn out to be correct, would have been along familiar lines:

"Defendants operate a telemarketing scheme that tricks consumers into spending approximately $149 – $249 to fix non-existent problems with their computers. By exploiting consumers' legitimate concerns about Internet threats like spyware and viruses, Defendants scare consumers into believing that their computers are infected or corrupted. Defendants do not present genuine evidence of the computers being infected or corrupted, and instead present either innocuous system information or messages they have generated in order to scare consumers."

For the moment, the company is "banned from deceptive telemarketing practices, and may not sell or rent their customer lists to any third party. The injunction requires that their websites and telephone numbers must be shut down and disconnected, and their assets be frozen."

And even more recently, the FTC took action again, against two groups of companies alleged to have made $120m from "deceptively marketing computer software and tech support services." The FTC tells us:

According to the FTC's complaints, each scam starts with computer software that purports to enhance the security or performance of consumers' computers. Typically, consumers download a free trial version of software that runs a computer system scan. The defendants' software scan always identifies

numerous errors on consumers' computers, regardless of whether the computer has any performance problems.

However, even if the allegations are proven, they are more effective against company which happens to be in the District Court's backyard. I've seen little evidence that the FTC's efforts have had significant impact in India, where most of the companies associated with support scamming (and other cold-call scams) seem to be concentrated. The FTC *has* actually been having an effect in the US, but there are umpteen scammers to go, and most of them aren't in the US. Though the virtual border between the US and India seems to have become surprisingly porous: Brian Krebs has posted a lengthy article explaining that 'A tech support company based in the United States that outsources its work to India says its brand is being unfairly maligned by -- wait for it.....tech support scammers based in India.' It's not the first time that companies outsourcing tech support – even security companies – have discovered that some call centres have difficulty distinguishing between support and fraud. However, it appears from the Krebs article that the company may not have helped its own case.

A single resources page is not going to solve the tech support scam problem, but I maintain a page of cold-call support scam resources here that includes links to just about every useful article related to the topic that I've ever come across.

ESET Corporate News

ESET to Launch Completely Re-designed, Best-of-Breed Business Security Suite

ESET today announced a significant transformation in its endpoint security products performance and usability. Building on the experience gained from more than 26 years of developing leading security solutions, ESET will introduce a completely re-designed suite of business security products for enterprise applications and small and medium-size businesses (SMBs) in North America later this year.

Today, ESET protects more than 100 million endpoints and actively works with business customers on next-generation technology and threat mitigation strategies. While continuing to offer best-in-class speed and detection, the new ESET business products have been completely reengineered and redesigned to provide the most advanced and easily managed business protection available, thus increasing the strength of internet security and reducing the demands on internal IT resources. The latest offerings from ESET will include industry-leading protection for multiple endpoints, including file servers, email communication, mobile devices and more.

ESET awarded highest score in AV-Comparatives Performance Test

ESET announces award-winning scores for its latest release of ESET Smart Security in the latest AV-Comparatives Performance Test.

Published recently, AV-Comparatives awarded the new version of ESET Smart Security with the Advanced+ Award. Details of the test show that ESET achieved the highest score for performance, outperforming all contenders, including AVG, Avira, BitDefender, F-Secure, Kaspersky, McAfee and Sophos, and Trend Micro.

”During the whole year ESET showed an excellent performance in all of our tests. Not only is ESET very good at protecting the customer, the latest performance test revealed that it has nearly no impact on the speed of the computer,“ said Andreas Clementi, CEO at AV-Comparatives.

ESET wins the Home Anti-Virus Protection award from Dennis Technology Labs

ESET was awarded 100% protection for detection and prevention of internet threats by ESET Smart Security 7 by Dennis Technology Labs in its independent test. This result was the highest protection score awarded to all products within the test, outranking Norton, Kaspersky, Avast, Trend, McAfee, BitDefender, AVG and Microsoft.

We know that our tests really challenge anti-malware products“, said Simon Edwards, Technical Director at Dennis Technology Labs. “This is why it’s quite rare for any one product to do consistently well and obtain high awards over a period of time. ESET Smart Security, in its various versions over the years, has always been very successful in our tests and has managed to achieve the highest protection score in the latest report.”

The Top Ten Threats

1. HTML/Refresh

Previous Ranking: 1
Percentage Detected: 3.13%

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.

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 2.33%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address from which it tries to download several files. The files are then executed and HTTP protocol is used for comunication with the C&C to receive new commands. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. Win32/Adware.MultiPlug

Previous Ranking: 5
Percentage Detected: 1.93%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it's present into the users system might cause applications to displays advertising popup windows during internet browsing.

4. Win32/TrojanDownloader.Wauchos

Previous Ranking: N/A
Percentage Detected: 1.48%

It is a trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer IP address. Then, attempts to send gathered information to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

5. Win32/Sality

Previous Ranking: 8
Percentage Detected: 1.41%

Sality is a polymorphic file infector. When executed it starts a service and created/deleted registry keys related to security applications activite in the system and to ensure that the malicious process restarts at each reboot of operating system.
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.

6. LNK/Agent.AK

Previous Ranking: 7
Percentage Detected: 1.35%

LNK/Agent.AK 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. This vulnerability became known at the time of discovery of Stuxnet, as it was one of four vulnerabilities that were executed by Stuxnet variants.

7. JS/Kryptik.I

Previous Ranking: 3
Percentage Detected: 1.29%

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.

8. INF/Autorun

Previous Ranking: 10
Percentage Detected: 1.22%

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

9. Win32/Ramnit

Previous Ranking: N/A
Percentage Detected: 1.17%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and also searches htm and html files so as to insert malicious instructions into them. It exploits a vulnerability found on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remoteley 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.

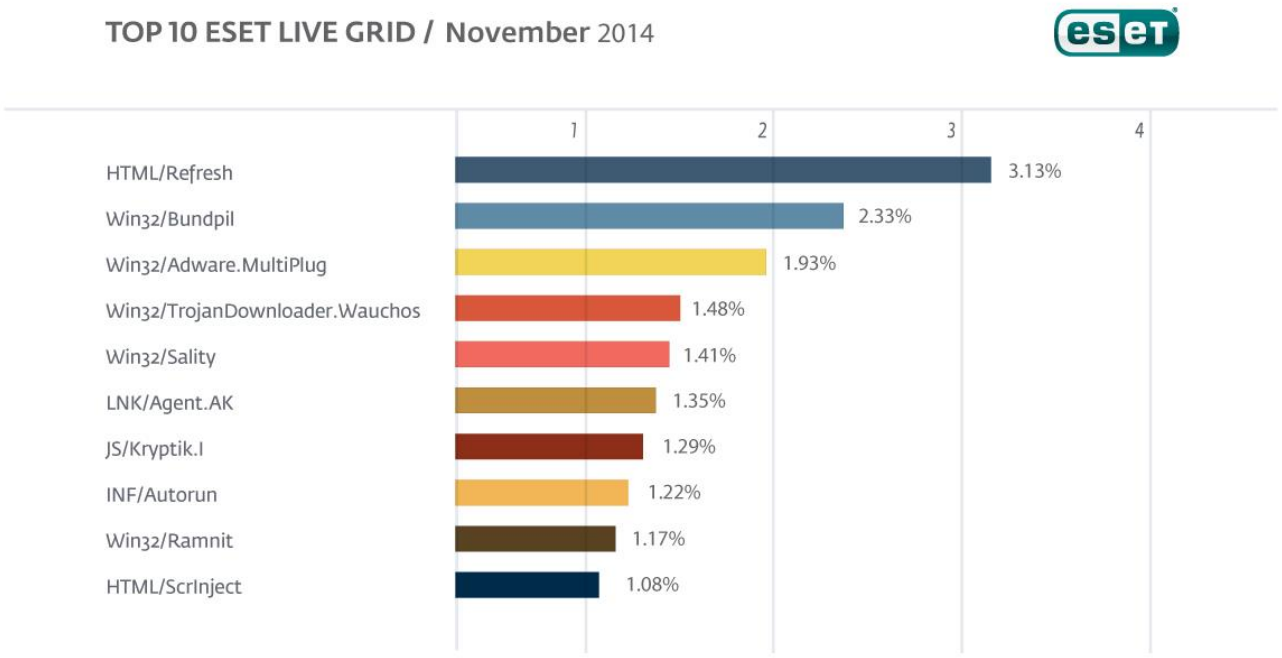
10. HTML/ScrInject

Previous Ranking: 6
Percentage Detected: 1.08%

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

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 3.13% of the total, was scored by the HTML/Refresh 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