August 2016
Feature Article: AV ‘fossils’ versus ‘next-gen’

ENJOY SAFER TECHNOLOGY™

Table of Contents

AV ‘fossils’ versus ‘next-gen’

David Harley, ESET Senior Research Fellow

This article was originally posted on the Antimalware Testing blog.

Now there’s a topic guaranteed to raise eyebrows and clenched fists. Next-generation vendors who insist that ‘traditional’ anti-virus is dead because it relies on signature detection; traditional companies who point out that they haven’t relied on static signatures in decades, and that the groundbreaking technologies claimed by next-gen vendors are not so dissimilar to those used nowadays by ‘traditional’ security suites; complaints that next-gen companies have been using VirusTotal (inappropriately and misleadingly) to ‘prove’ it using stacked testing methodologies, while silently benefiting from the research of the ‘fossils’ whose marketshare they hope to capture.

Well, since I derive a large proportion of my income from a ‘fossil’ anti-malware-oriented security company, I don’t expect you to assume that I’m unbiased. I will say, though, that this article by Kevin Townsend – Inside The Competitive Testing Battlefield of Endpoint Security – strikes me as a pretty good, balanced summary of many of the issues.

Oddly enough, while some of the marketing-rich, fact-impoverished statements I’ve seen from next-gen vendors infuriate me more than I care to say – I prefer to blog without profanity, in general – I’m not altogether without sympathy for their mistrust of mainstream product testing. On the whole, I think AMTSO, warts notwithstanding, has helped in raising the standard of mainstream testing far higher than I could have hoped a few years ago, but I’m not sure that comparative tests *can* be quite as effective as testers would like you to think. Nonetheless, consumers need and deserve some impartial guidance as to which vendors deserve their custom. As long as next-gen vendors claim that no-one is capable of running accurate tests of their products, and while they at the same time claim to be able to run their own flawed pseudo-tests for marketing purposes, they can’t expect to avoid independent and informed criticism. If they actually showed willingness to work with testers (even if not within AMTSO) to work towards more effective testing of their products, they’d gain in trust and credibility. Or would that be too traditional?

*Travelling Hopefully…

David Harley, ESET Senior Research Fellow

Some of the content in this article originally appeared on the Dataholics blog.

Quote Unquote

Ralph Waldo Emerson[1] is often credited with saying that 'Life is a journey, not a destination' though I've also seen it attributed to the Buddha, though that one hasn't so far made it to the Fake Buddha Quotes site. Which suggested to me that an article is long overdue about the flakiness of sites about who said what, and exactly what[2] it was they said. However, it turned out that there were quite a few sites attempting to correct misattribution on quote sites. This one, for example.

Right now, though, I'm wondering why so much marketing takes the quote so literally. (And for once I'm talking about legitimate marketing rather than spam and malvertising.)

As you might imagine, I've done a lot of travelling for ESET in the past few years, quite apart from my own recreational wanderings, though as semi-retirement has beckoned, my urge to wander beyond the shores of the UK has waned dramatically. Still, arranging all those foreign trips for work meetings and conferences have left me vulnerable to a continuing stream of travel-related marketing email.

Perhaps it's me, but I can't imagine that many people plan their holidays or business trips so as to stay in a specific hotel or – even weirder – use a specific shuttle service from/to the airport. So why do I get so much marketing mail that assumes I do? Do people really go to specific places so that they can stay in a specific airport hotel? (But yes, I do understand that you might want to use a specific hotel or shuttle service *if it does* happen to fit with your travel plans.)

---

[1] If Emerson did say it, I've been unable to find where. I've often seen it cited as being in his essay on Self-Reliance, but it isn't. At any rate, it isn't in the essay I've read, in which he certainly said 'A foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines.' He forgot to mention copy editors. But that's probably another rant for another day. (Though the many people who've reaped the benefit of my alleged editing skills may regard any such rant as blatant hypocrisy.)

[2] QUOTATION, n. The act of repeating erroneously the words of another. The words erroneously repeated. (Ambrose Bierce, in The Devil's Dictionary.)

Disclosure and Attribution

All may not seem to have much to do with security in general, but conference travel isn't the only context in which misattribution is a problem. In an article from 2015, Brian Krebs calls for more information from security companies:

> Most experts probably would say it's important to consider attribution insofar as it is knowable, but it's remarkable how seldom companies that regularly publish reports on the latest criminal innovations go the extra mile to add context about the crooks apparently involved in deploying those tools.

Much more recently, journalist Kevin Townsend, while researching an article for Security Week (a blog site for which I used to write occasionally, oddly enough), asked me for commentary on a paper by Scott Charney and others: "From Articulation to Implementation: Enabling progress on cybersecurity norms", wondering whether the paper's suggestions that 'responsible' disclosure should be the international norm and that an international body of independent experts should declare 'attribution' on threats (whether criminal or nation-state) are 'possible, good, realistic?' This was my response.

> I've always believed in – or at least hoped for – responsible disclosure, and I don't have a problem with attempting to formalize it as a norm in the hope of mitigating conflict in politics and commerce. However, there are plenty of players who won't want to go along with such norms. I think we can assume that it will have no impact on those looking for vulnerabilities to exploit in the pursuit of criminal aims. Nation states paying lip service (and maybe even truly engaging with some of the ideas promoted here) will not necessarily want or be able to control the activities of agencies developing (groan) cyber weapons. After all, there are trust issues with being the first to give up attack technologies that everybody else is also working on. The groups selling vulnerabilities and exploits to commercial customers, SCADA customers and state agencies are not going to give up a lucrative and legitimate business opportunity while it remains legitimate. But we shouldn't give up on proposing ethical and moral guidelines just because not everyone will choose to go along with them. They might even have an impact on those companies who use vulnerability research into the products of other companies as a PR exercise, by redefining exactly what 'responsible' means in this context. (I'm thinking of cases where a vulnerability has been shared with a company only just ahead of a press release, with the possibility of further PR based on the reaction time of the targeted company.)
>
> Attribution is trickier. Many of the researchers who are best qualified to consider attribution are all too aware of the difficulties and pitfalls of establishing correct attribution in cases where an attacker has expended as much effort into misdirection as he has into developing the core attack technology. As the Microsoft paper acknowledges, there may be compelling reasons for not talking about attribution even when it's considered 'proven'.

While it isn't usually necessary for security researchers to know exactly who is responsible for an attack in order to implement defences against it, we're as interested in the truth[3] about an attack as Mr Krebs (and more so than some lesser journalists…), but sometimes it's better for the world in general if we don't air *all* our suspicions. Not to mention the peace of mind of our legal departments.

*To travel hopefully is a better thing than to arrive – Robert Louis Stephenson, in *'El Dorado,*

[3] TRUTH, n. An ingenious compound of desirability and appearance. Also from The Devil's Dictionary.

ESET Corporate News

First Twitter-controlled Android botnet discovered by ESET

ESET researchers discovered an Android backdoor Trojan controlled by tweets. Detected by ESET as Android/Twitoor, it's the first malicious app for Android using Twitter instead of a traditional command-and-control (C&C) server. After launch, the Trojan hides its presence on the system and checks the defined Twitter account at regular intervals for commands. Depending on the commands it receives, it can either download other malicious apps or change the C&C Twitter account to another one.

"Using Twitter to control a botnet is an innovative step for an Android platform," said Lukáš Štefanko, the ESET malware researcher who discovered the malicious app. According to Štefanko, communication channels based on social networks are hard to discover and impossible to block entirely – while simultaneously being extremely easy for the crooks to redirect communications to another account.

Android/Twitoor has been active since July, 2016. It can't be found on any official Android app store – according to Štefanko – but probably spreads by SMS or via malicious URLs. It impersonates a porn player app or MMS application but without the functionality. Instead, it has been downloading several versions of mobile banking malware. However, the botnet operators could start distributing other malware at any time, including ransomware, according to Štefanko.

ESET Flawless in VB100 and in AV-Comparatives' Security Tests

Virus Bulletin, the independent security software testing body, has just published its VB100 Comparative Review on SUSE Linux Enterprise Server and VB100 Comparative Review on Windows 8.1 Pro 64-Bit.

In the SUSE Linux Enterprise Server Comparative, Virus Bulletin has tested **ESET Endpoint Security for Linux**, which scored 100% in both - on demand and on access scanning. The same result was reached by **ESET NOD32 Antivirus 9** in the second comparative, with Windows 8.1 acting as the test-bed.

Furthermore, in the most **recent Mac Security Test** by **AV-Comparatives**, **ESET Cyber Security Pro** achieved the maximum score in the Mac malware protection tests.

The latest Mac Security test consisted of Mac malware protection and Windows malware detection parts. In the first part, AV-Comparatives tested the most-recent Mac samples, in the second the most prevalent Windows samples. In both cases *ESET Cyber Security Pro* scored full points.

The Top Ten Threats

1. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 12.36%

JS/Danger.ScriptAttachment is a generic detection of suspicious e-mail attachments.

2. LNK/Agent.DA

Previous Ranking: N/A
Percentage Detected: 3.63%

LNK/Agent.DA is detection name for *.lnk file, which executes trojan Win32/Bundpil.DF. LNK file is part of a Bundpil infection and is created on removable drive with special name "%drive_name% (%drive_size%GB).lnk" convincing user that it's a link to drive content. Actually it points to %system32%\rundll32.exe with a Bundpil DLL component as a parameter.

3. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 3.43%

Win32/Bundpil 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

4. HTML/Refresh

Previous Ranking: 4
Percentage Detected: 1.69%

HTML/Refresh is a trojan that redirects the browser to a specific URL serving malicious software. The malicious program code is usually embedded in HTML pages.

5. Win32/Agent.XWT

Previous Ranking: 3
Percentage Detected: 1.62%

Win32/Agent.XWT is a trojan that serves as a backdoor. It can be remotely controlled and is usually a part of other malware. It collects the operating system version and language settings, then attemps to send the gathered data to a remote machine using HTTP.

6. JS/Adware.Agent.L

Previous Ranking: 5
Percentage Detected: 1.55%

JS/Adware.Agent.L is the detection name for JavaScript code designed to deliver advertisements on an affected PC. When this code is injected into a webpage, it replaces advertisements it finds with new ones from hxxp://x.rafomedia.com. If ads found are already from rafomedia, the malware does not replace them.

7. HTML/ScrInject

Previous Ranking: 6
Percentage Detected: 1.49%

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

8. HTML/FakeAlert

Previous Ranking: N/A
Percentage Detected: 1.36%

HTML/FakeAlert is generic detection name for HTML page showing made-up, fake alert message usually about dummy virus infection or some other problem which is expected to harm the computer or user's data. User is usually urged to contact fake technical support or download and execute fake security solution from the Internet to prevent damage. This kind of page is usually used as a starting point for “Support Scams”.

9. Win32/Ramnit

Previous Ranking: 7
Percentage Detected: 1.23%

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 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.

10. Win32/Sality

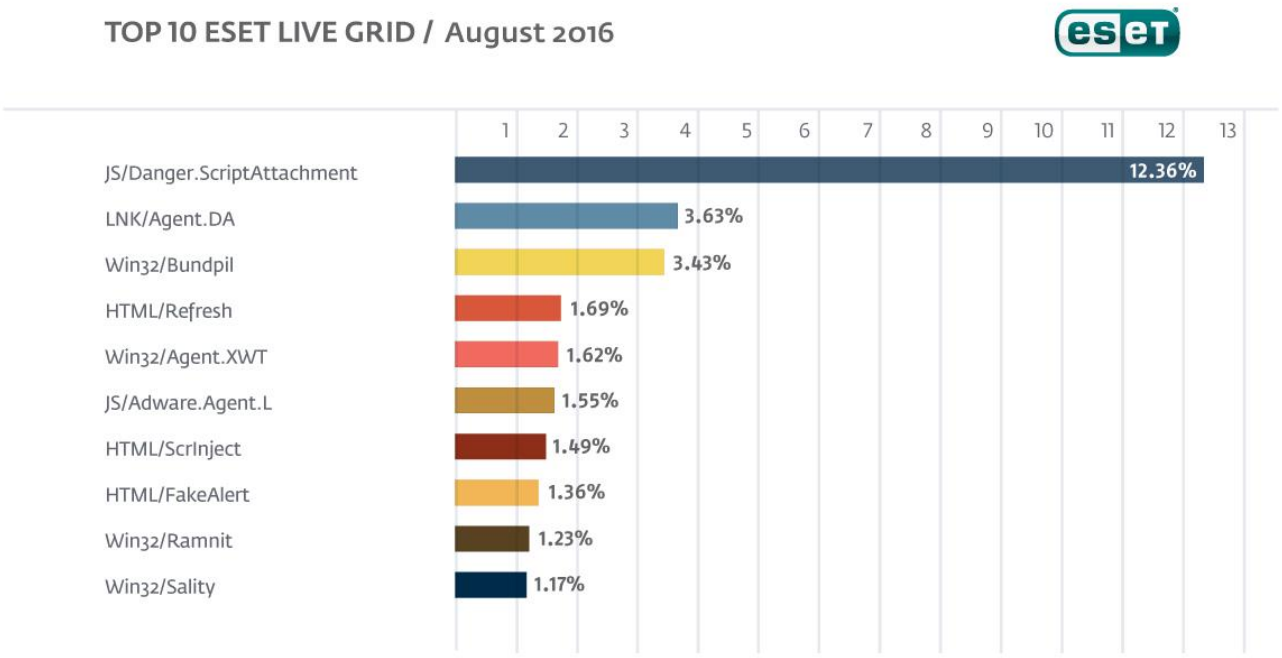
Previous Ranking: 8
Percentage Detected: 1.17%

Sality is a polymorphic file infector. When it is executed registry keys are created or deleted that are related to security applications in the system so as 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

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 12.36% of the total, was scored by JS/Danger.ScriptAttachment.



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 has continued to lead the industry in proactive threat detection. By obtaining its 91st VB100 award in April 2015, 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 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 the United Kingdom, 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:

- VirusRadar
- ESET White Papers
- ESET Conference Papers
- WeLiveSecurity
- ESET Podcasts
- ESET Videos
- Case Studies