March 2015
Feature Article: 50 Shades of Security

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

50 Shades of Security

David Harley, ESET Senior Research Fellow

This article combines material from a blog article on WeLiveSecurity and another on the same topic for ITSecurity UK. (From which I re-used the title, which I like to think of as one of my better efforts.☺) Both articles referred to some commentary requested by Heimdal Security blog for a blog article here. The rest of the article expands on the commentary I sent to Heimdal.

Dinosaur reminiscences

Having started my career in IT and IT security in particular some two and a half decades ago, I sometimes cling to ideas and practices that may seem outdated in the 21st century: I tend to avoid the word 'cyber' (especially as a standalone term', I usually insist on hyphenating anti-virus, I use the term virus to refer to self-replicating malware rather than any old malicious software, and I'm decidedly squeamish about keeping to ethical standards that some younger researchers (actually, nearly all researchers are younger than I am…) may see as quaint.

You may have noticed that those two and a half decades put me in this business even before there was a World Wide Web as most people might understand it (at any rate before that name was used): this means that not only do I remember when security technology was very different to the diverse and sophisticated solutions available today, but I also had plenty of opportunity to observe how the fledgling anti-malware industry adapted to new marketing and PR opportunities.

While there has always been cooperation and collaboration among security researchers that transcends company boundaries, there was less cut-throat competition between companies in those early days than the sort of anti-competition marketing we often see now. To take a small but telling example, anti-virus vendors would not only put up databases of information on specific viruses/malware, but even linked (sometimes) to databases put up by other companies.

Believe it or not…

There have always been people in the anti-malware industry who don't automatically put PR and commercial advantage ahead of public interest, and give credit where it's due. Fortunately, quite a few of them work for ESET. :) We try to be scrupulous about correctly attributing research from other companies, share samples and security information with them, and sometimes collaborate on research, conference papers and presentations, and even share blogs from time to time, though that's fairly unusual. (Here, for example, is a blog from 2010 co-authored by myself and Magnus Kalkuhl -at that time working at Kaspersky - clarifying our essential agreement on an issue raised by the media.)

But not completely unknown. Recently, I was rather pleased to be invited to contribute to a blog article by Aurelian Neagu for Heimdal Security, who asked a number of security researchers to answer the question *Can you name 3 security tips any user needs to follow to stay safe online?*

Balancing at the tipping point

It turns out that 19 people contributed more than 50 tips to the article 50+ Internet Security Tips & Tricks from Top Experts. Some of the contributions come from inside Heimdal and CSIS (the well-regarded security company that originally launched Heimdal), but many come from other security companies and some journalists specializing in security topics. Among those contributors were such luminaries as Microsoft's Troy Hunt, F-

Secure's Mikko Hypponen, CSIS's Peter Kruse, journalists Simon Edwards (Dennis Publishing and AMTSO), Neil Rubenking (PC Magazine) and Kelly Jackson Higgins (Dark Reading) and many more. And some bloke called Harley. ☺

Inevitably, given that the starting point of the blog was that "…we don't want to intervene or alter the answers received," some points are made by more than one person, but there's certainly a wide enough spread of specialty and expertise here to make it worth considering checking out the article, since two people may address the same core issue - passwords, for instance - but make quite different (yet complementary) points.

Going by the Book

The article is even downloadable as an eBook. It doesn't constitute a 'how to' in the sense of an article on how to address a single security issue, but it certainly provides information on a number of ways in which you might make you online experience generally safer.

Education, Education, Education

Here are some relevant points from a conference paper on user education that ESET's Sebastián Bortnik and I presented at AVAR in 2014:

It is not possible to teach the entire world about new threats and remedial practices on a day-to-day basis, and at the same fast rate at which new technologies are adopted. On the other hand, most of the people who have ever received awareness-raising advice are likely to change something in the short term, so it is probably a matter of how frequently they receive the message in order to reinforce the lesson and sustain change. (Bearing in mind that an overfamiliar message may actually dull the recipient's receptivity.) Finally, holistic integration with other approaches to security awareness and enhancement is still needed: the information security community cannot do it by themselves, and improved cooperation and information exchange with other key actors should be encouraged.

We believe that these approaches (and some patience) will bring us to a not-so-distant future where information security is not only something that really matters to the community, but something that even home users can realistically achieve.

If I had to boil my own contribution to the Heimdal article down to a short summary, though, it would be something like this:

Organizations achieve reasonable security by wrapping layers of security around themselves rather than relying on a single magic bullet solutions. Reasonably well-protected individuals apply the same thinking (though normally at much less expense), but they remember that they are themselves an essential 'layer' of security.

As my old friend Ken Bechtel puts it: '...until we get people realizing they are PART of cyber defense in depth, we will always be responding to incidents.'

You can't live by TOAST alone

Having given a bald summary, here's an expanded version of my original comments for Heimdal.

Decades ago, Padgett Peterson coined the acronym TOAST (The Only Antivirus Software That [you'll ever need, or words to that effect], which he applied to the type of security product advertising that sells you on the idea that there is a single product that will keep you totally secure. Meanwhile, true viral

(that is, self-replicating) malware has become just one – relatively small – feature of the threatscape, and it's been a long time since malware was the only type of threat we had to worry about.

Yet it appears that we're still looking for the 100% solution, and when our security fails, we're furious because that solution hasn't met our expectations. Vendor marketing doesn't help when it's based on statements along the lines of "Don't buy product *X, Y, or Z*: buy *our* product." Or, worse still: "Don't buy that type of product: buy *our* product." So we see single solutions that claim to render other types of solution – passwords, anti-virus and firewalls – obsolete, whereas the truly obsolete issue is the idea of single-layer/single-solution security.

Accept no substitutes

Recently I've seen scores of articles that tell me that solution *S* makes passwords obsolete. However, the way to improve authentication isn't just to replace one (admittedly flawed) method with another (hopefully better) method, but to use multi-factor authentication. (Two-factor at least.) Many social media sites now allow you to augment password authentication with at least one secondary authentication method, such as Facebook's Login Approvals, which uses a token (security code) sent to your cell phone by SMS or its own authenticator app. So tip 1 – or at least a suggestion – would be to take advantage of these opportunities.

Going viral

Hopefully, very few people nowadays think that viruses are the only security threat they need to worry about, but how many have thought about which security programs they should install? All too often, the only decision they consciously make is to install an anti-virus program, very likely a free one. As long as what they install is a genuine anti-virus program from a reputable source – as opposed to a fake program (or a genuine security program compromised by malware) – that's certainly better than assuming that they can rely totally on security built into their operating system, applications and internet services, even though those programs and services are generally far more secure by design nowadays than they were 10-20 years ago.

Within a certain range of functionality, a free program may be effective as a for-fee equivalent, but it's unlikely to have the multiple layers of security layers that a full-strength security suite does. Such a suite incorporates not only malware detection but other security features that may include anti-spam, anti-phishing, and other technologies that can indirectly increase the system's resistance to malware infection. Given my association with an anti-malware vendor that sells this kind of technology, the chances are that some readers will dismiss any recommendation I make concerning it as marketing fluff.

Free and worth every penny

So tip 2 would be that you at least do your best to find out what security your internet provider and operating system provide, and how to make the best of that security; and if you really can't bear to spend money on security software, then look into the possibility of reinforcing your free anti-virus with other free but reliable security software such as a desktop firewall. (You'll have to excuse me if I don't recommend specific programs: this isn't actually an approach I recommend at all, but it's better than relying solely on free anti-virus.) Beware of single solutions here, too. I wouldn't want to suggest that you shouldn't worry – or at least find out about – APTs (Advanced Persistent Threats)

and sometimes – especially for businesses – it's worth buying into a service that's better at detecting APTs than mainstream anti-malware, but don't make the mistake of ignoring the massive volumes of less 'sexy' malware that mainstream software deals with pretty effectively.

Own your own security

It's hopefully clear by now that I'm wholeheartedly in favour of multi-layering: where one approach (such as some form of signature detection) fails, something more generic (behaviour blocking or spam filtering, for instance) might. However, there's one security layer I haven't yet considered, and it's at least as important as those I *have* mentioned. It's you. Many kinds of threat (not just malware) rely on manipulating a victim into doing something which will enable the attacker to achieve his aims – we often call this social engineering. Sometimes criminals use very sophisticated tricks in order to con their victims in this way, but a little scepticism goes a long way. You can't teach resistance to social engineering in a paragraph – though I hope it is teachable, and not just something you either have or you don't – but here are a couple of soundbite-length thoughts that do at least go some way towards that goal:

1. As they say (far too often), if it sounds too good to be true, it probably is. On the other hand, threats are often very effective in persuading people to act thoughtlessly. Don't let threatening messages browbeat you into acting without checking, either. Social engineering uses the carrot *and* the stick.

2. Whatever you do, don't fall into the trap of thinking that security software – or Microsoft, or Apple or whatever/whoever – will save you if you make a bad choice about what to click on. Technical solutions don't stop all technical threats such as cross-site scripting and drive-by downloads: they certainly won't protect you against all threats that use social engineering.

ESET Corporate News

AV-Comparatives reviews ESET's next-generation business products

ESET announces the availability of two independent, in-depth security software reviews for the next-generation business products - ESET Endpoint Security and ESET Remote Administrator. The reviews were conducted by the globally recognized independent testing organization AV-Comparatives.

ESET Endpoint Security

AV-Comparatives were very impressed with both the functionality and the user interface of this security product. While it retains the simplicity of the earlier versions, AV-Comparatives commended the modern look of the product's new design, which has been optimized throughout for use with touchscreens.

The testing organization also highlighted the design of the status display, saying it was both clear and provided an easy means of reactivating disabled components. Additionally, the review says that ESET Endpoint Security warnings were "clear and practical, and the software has been secured against removal or deactivation by unauthorized users."

Read the full review.

ESET Remote Administrator

The report highlights the completely new, modern design of the product and found that installation, customization and deployment were simple.

They also noted that security statuses, shown via a number of colorful pie charts, allowed the administrator to find important items easily – finding that the design avoids overwhelming the user. The report concludes by the findings: "Overall we feel ESET have done a tremendous job of making a console that is powerful enough to cope with thousands of clients, but simple enough to use in SMBs as well".

Read the full review.

ESET North America CEO Gives Keynote at Largest Security Conference in Argentina

The largest security conference in Buenos Aires, Argentina, 35° Iberoamerican Congress and Information Security Fair Segurinfo 2015, was held recently kicking-off with a keynote presentation from ESET North America CEO Andrew Lee.

Lee's captivating presentation titled, "Immortal Data - The Future of Everything," was presented in front of a full house, and exposed a future where we will inevitably live in a recorded and registered society, where everything will be captured.

Lee discussed the idea of everything around us being managed by data in the future, and the amassed power in the hands of those who hold that data. Many thought-provoking questions were posed by Lee such as 'what will it be like living in a society where everything you say and everywhere you go is captured?' and 'will anonymity be possible (or desirable)?'

During the presentation, Lee also presented the impact that the exposure of personal information has and how it may be exploited by cybercriminals. He also explored the implications of these changes in society and technology.

The Top Ten Threats

1. Win32/Adware.MultiPlug

Previous Ranking: 1
Percentage Detected: 3.55%

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.

2. Win32/Bundpil

Previous Ranking: 3
Percentage Detected: 2.27%

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 is used for communication with the C&C to receive new commands. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. Win32/TrojanDownloader.Waski

Previous Ranking: 5
Percentage Detected: 1.95%

Win32/TrojanDownloader.Waski is a Trojan that uses HTTP to try to download other malware. It contains a list of two URLs and tries to download a file from the addresses. The file is stored in the location %temp%\¬miy.exe, and is then executed.

4. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.41%

Sality is a polymorphic file infector. When 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

5. HTML/Refresh

Previous Ranking: 2
Percentage Detected: 1.39%

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. LNK/Agent.AV

Previous Ranking: 8
Percentage Detected: 1.38%

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.

7. JS/Kryptik.I

Previous Ranking: 4
Percentage Detected: 1.36%

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. LNK/Agent.AK

Previous Ranking: N/A
Percentage Detected: 1.30%

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.

9. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.29%

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 (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.

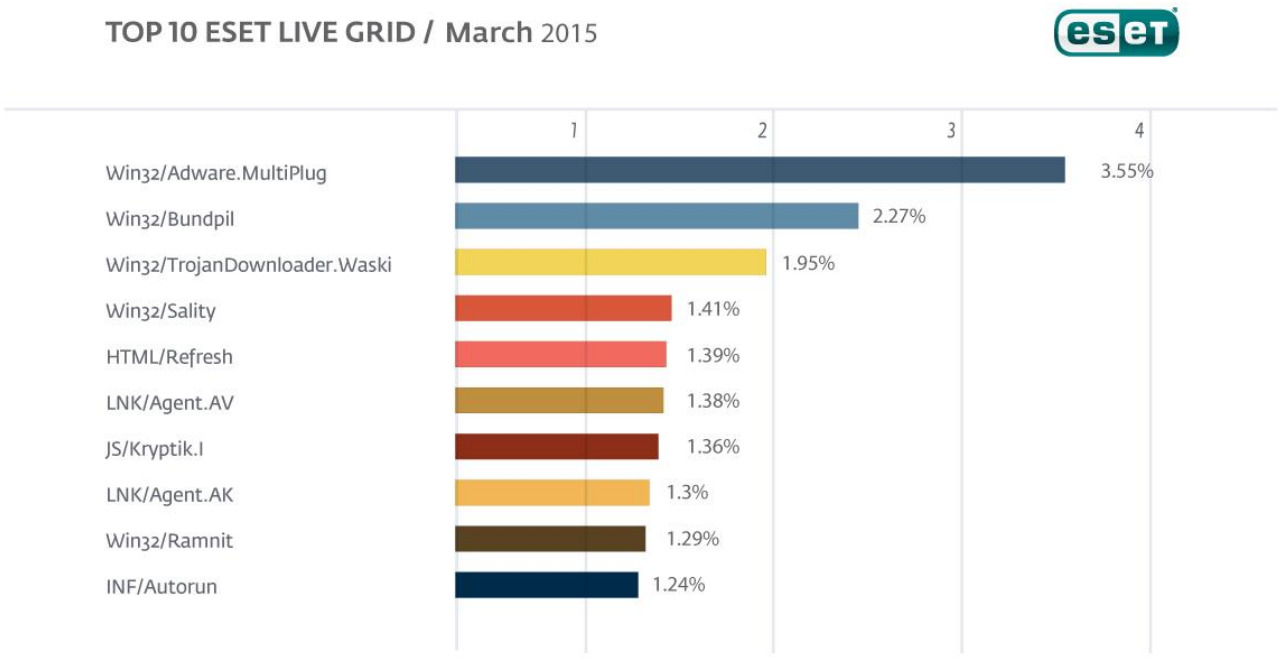
10. INF/Autorun

Previous Ranking: 10
Percentage Detected: 1.24%

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 auto-execute 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.

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 3.55% of the total, was scored by the Win32/Adware.MultiPlug 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