October 2016
Feature Article: Ransomware, Support Scams, and Old-School 419s

ENJOY SAFER TECHNOLOGY™

Table of Contents

Ransomware, Support Scams, and Old-School 419s

David Harley, ESET Senior Research Fellow

This article originally appeared on the ITSecurity blog

In the age of ransomware, it's easy to forget that other attacks like support scams and the venerable (but not venerated) 419 have not disappeared. They've simply become less glamorous and so attracted less media attention. It's hard to say to what extent improved email filtering (in the case of 419s rather than support scams) and the copious warnings from the security industry to its customers have had an impact on their effectiveness.

Tech support scams have clearly not gone away, though they have tended to evolve. I'm not going to go over ground I've already covered elsewhere – for instance, Tech Support Scams: a Beginner's Guide – but they're clearly still happening and still effective enough to make money for somebody.

For example, Malwarebytes CEO Marcin Kleczynski was heavily quoted by Steve Melendez in an article suggesting an ever-increasing correlation between tech support scams using malware and unequivocal ransomware: Tech Support Scams Are Getting More Sophisticated. A Malwarebytes researcher was quoted anonymously as saying that 'We're going to see more aggressive techniques ... In particular, I wouldn't be surprised if they started using ransomware and encrypting people's files.' That's pretty speculative, of course, though there really has been convergence in some respects. But the article also covers a number of aspects of this particular corner of the threat landscape. Kleczynski also makes the point that there is an important distinction between ransomware and support spams, in that victims may not be aware that they've been scammed. It may be true, as the article also suggests, that some scam callers aren't actually fully aware that they're scamming, but I've talked to plenty who clearly knew what they were doing, even if some were simply reading from a script that they didn't properly understand.

In the meantime, a study by Microsoft throws up some interesting statistics regarding the relative proportions of tech support scam victims in various parts of the world, as well as some generational differences. For instance, while many British people are still 'enjoying' contact with support scams, only two percent are reported to have lost money in the last year, whereas out of those who encountered a scam, 22 percent of Indian citizens and 21 percent of US citizens contacted lost money. Across the world, around 13 percent of people in the 18-24 age group are reported to have lost money to online or telephone scammers, whereas only three per cent of over-65s lost money. In personal terms, I think this means that I'm unlikely to lose money, but my blood pressure is at risk due to intrinsic irritability.

I mentioned earlier that improvements in email filtering may have had some impact on the effectiveness of 419s (as it has other email-borne threats, of course). If nothing else, it means that they may be seen far less often in the Inbox. Though it's not unusual for them to be lurking in spam folders and 'infected items'. However, it seems likely that scammers despatch large enough quantities of emails to ensure that quite a low rate of responses can still be profitable.

There again, the type of scam that we usually call a 419 goes back to a time way before the Internet and email, the fax, or regular postal services. More recently, such scams have been transmitted through other electronic channels such as social media. And only today, I found a comment to one of my articles for ESET, that plainly represents a kind of 'reloading scam' where the scammer suggests that there is a fund set up to compensate victims and offers a contact point for such a fund. Variations on this theme normally use a classic 'Advance Fee Fraud' ploy: after the victim responds, it turns out that the payment is conditional on the payment of certain fees, which will be pocketed by the scammers. Of course, there will be no payment.

Facebook and those 'legal' disclaimers

David Harley, ESET Senior Research Fellow

A version of this article originally appeared on the Chainmailcheck blog.

I've mentioned those not-very-useful disclaimers that people keep posting to stop Facebook 'misusing' their posts a number of times. For instance:

Trust, Truth and Hoaxes in Social Media.

Facebook Disclaimer: FB users still missing the point

So I won't press the point again, even though there does some to be another upsurge in such disclaimers, which are based on (a) a misunderstanding of Facebook's view of its users' right to their own posts (Facebook'sview is expressed here) and (b) a mistaken belief that such a disclaimer will somehow affect the existing implicit contract between Facebook and its users.

Sorry, I'm going to quote myself:

…your agreement with Facebook is a contract, as is the case with other social media providers: you can't use a unilateral statement like this to opt out of the contract stipulations you agreed with the company when you joined, as long as they're conditions that Facebook can legally impose (or modify, if it chooses). You can try to negotiate a non-standard contract with a provider, but a service with hundreds of millions of subscribers isn't likely to consider one-to-one contract variations, especially when it isn't charging for the service it provides.

And that remains the case. But I did come across an article you might find interesting in the Washington Post, which tries to explain Why that 'Facebook copyright' hoax will never, ever die. A recent article on WeLiveSecurity- Facebook privacy settings hoax resurfaces again – discusses the latest round of this particular exercise in misinformation.

At a slight tangent from that, I came across an instance where NewsThump apparently attempted to reduce the number of Facebook hoaxes by generating a hoax of its own.

Mark Zuckerberg to give everyone $1000 to stop sharing stupid Facebook hoaxes

Where would the internet be without satire?

I thought of sharing this article on Facebook, but was torn between not wanting to mislead people who lack the hoax/satire recognition gene, and not wanting to offend people who would see right through it anyway by explaining that NewsThump isn't a real news site…

ESET Corporate News

New security solutions from ESET provide added cyber protection

Internet users now have more ways to stay protected from the latest cyber threats with the introduction of two new security solutions released today by the IT security company ESET®: ESET Smart Security Premium and ESET Internet Security.

ESET Internet Security: building on ESET's entry-level product, ESET NOD32 Antivirus®, ESET Internet Security brings users additional peace of mind through smart technologies, such as Webcam Protection, which controls processes and applications that access computer-connected or embedded web cameras; and Home Network Protection, which allows users to test the home routers for known vulnerabilities.

ESET Smart Security Premium: with this new Premium product, users will also have access to these additional security tools: ESET Password Manager, which employs AES-256 encryption – the world's leading standard – to store and pre-fill all passwords; and ESET Secure Data, which uses encryption to ensure secure collaboration and data sharing while also protecting against data theft in the event of loss of a USB key or laptop.

For more information about ESET's security solutions, please visit: https://www.eset.com/us/home/compare/windows-antivirus/.

Dissection of Sednit espionage group

ESET researchers announce the release of their extensive 3-part research paper "En-Route with Sednit". This infamous group of cyber-attackers, also known as APT28, Fancy Bear and Sofacy, has been operating since 2004. Its main objective is stealing confidential information from specific targets.

Over the past several years, the group's high-profile activities have attracted considerable interest among researchers in this field. Hence, the intended contribution of this document is to provide a readable technical description, with tightly grouped indicators of compromise (IOCs), available for immediate leverage by both researchers and defenders alike tasked with analyzing Sednit detections.

For further information, please visit ESET's news portal WeLiveSecurity.com, and read introductory blogposts for Part 1, Part 2 and Part 3, or dive-deep into all 3-parts of the whitepaper at http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-full.pdf

The Top Ten Threats

1. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 7.25%

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

2. Win32/TrojanDownloader.Wauchos

Previous Ranking: N/A
Percentage Detected: 6.11%

This is a trojan which tries to download other malware from the Internet. It collects information about the operating system, including settings and the computer's IP address. Then, it attempts to send the information it has gathered 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.

3. JS/TrojanDownloader.Nemucod

Previous Ranking: 3
Percentage Detected: 4.98%

JS/TrojanDownloader.Nemucod is a trojan that uses HTTP to try to download other malware. It contains a list of URLs and tries to download several files from those addresses. The files are then executed. This Trojan is now associated with ransomware.

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

4. LNK/Agent.DA

Previous Ranking: 4
Percentage Detected: 3.64%

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

5. Win32/Bundpil

Previous Ranking: 5
Percentage Detected: 3.35%

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

6. Win64/TrojanDownloader.Wauchos

Previous Ranking: N/A
Percentage Detected: 2.81%

This is a trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer's IP address. Then, it 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.

7. HTML/Refresh

Previous Ranking: 9
Percentage Detected: 1,70%

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.

8. HTML/FakeAlert

Previous Ranking: N/A
Percentage Detected: 1.69%

HTML/FakeAlert is generic detection name for an HTML page showing a made-up, fake alert message, usually about a fictional virus infection or some other problem which is supposed to harm the computer or user's data. The user is usually urged to contact fake technical support hotlines or download and execute a 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/Agent.XWT

Previous Ranking: 8
Percentage Detected: 1.52%

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.

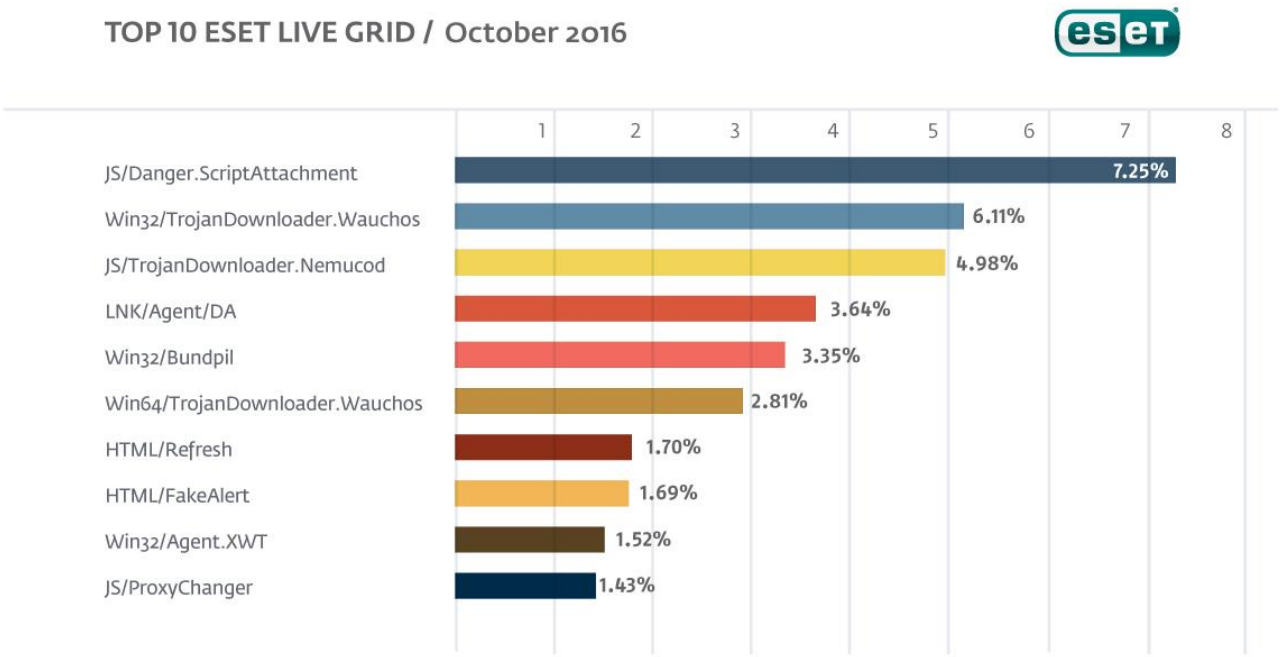
10. JS/ProxyChanger

Previous Ranking: 7
Percentage Detected: 1.43%

JS/ProxyChanger is a trojan that prevents access to certain web sites and reroutes traffic to certain IP addresses.

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 7.25% 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 the 97th award in July 2016, 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