July 2016

Feature Article: Scamming the Would-Be Scammer

ENJOY SAFER TECHNOLOGY™

Table of Contents

Scamming the Would-Be Scammer 3

Beating the 'Microsoft scam' 4

ESET Corporate News 6

The Top Ten Threats 7

Top Ten Threats at a Glance (graph) 10

About ESET 11

Additional Resources 11

Scamming the Would-Be Scammer

David Harley, ESET Senior Research Fellow

*An earlier version of this article was published on the Chainmailcheck blog: [Scamming the would-be scammer](). *

Every so often I find myself dealing with a blog comment by someone claiming to offer a blank ATM card that can be used to hack any ATM to get an unlimited supply of free money. And every time I wonder whether I ought to blog about it, but it's never seemed a high priority. After all, it's pretty obvious that if such a thing actually existed, it couldn't possibly be legal, could it? Even the scammers who offer it tend to admit that it's illegal – one recent example tells me that it's nevertheless untraceable, since it also stops the CCTV camera from 'detecting' you. It also lays golden eggs and predicts the winner of the Kentucky Derby. (I made that last bit up, but it doesn't seem that much more far-fetched.)

So who cares if people who don't have a problem with robbing banks get caught out by a scammer? Well, maybe some of the potential victims are desperate rather than intrinsically amoral.

It's worth noting, maybe, that 419 scammers are often frank about the fraudulent nature of the transaction they're proposing – without making it clear, of course, that it's their 'partner' in crime who will be scammed, not the government or bank – but attempt to justify it by claiming that the money they're offering would otherwise be misused by the organization from which it's stolen. The perpetrators of this scam will sometimes make somewhat similar justifications – 'because the government cannot help us so we have to help our self' – and it's often quite hard to feel much sympathy for a government agency or a bank… Of course, the illegality of the transaction does make it difficult for the victim to report it when they realize they've been scammed.

It's sometimes assumed that this kind of scam is a 419 – I don't know that this is always the case. They're usually badly written, but not necessarily in the same stilted way that characterize so many 419s. [Here's an example]() of a blogger who found a scammer who certainly seems to be based in Nigeria, though.

Furthermore, after I first discussed this topic on a blog, I found a comment on the same blog (but posted to a totally different article, weirdly enough) that reassured me that this magical device does exist, but that…

'due to so many scammers out there, you cant [sic] really tell who is real or fake. I was scammed by three different fake hackers from

Nigerian hoodlums who claimed they do possess the card which they don't.'

You might think that someone who'd been caught three times by the same con might have learned something from the experience, but this individual was persistent if not bright… He claims to have come across a blog to which I have no intention of directing you…

'where about 25 people where thanking this hacker for changing their life with the blank card. Due to my past experience, i was nervous & scared of loosing more money but on the blog i saw an email of Mr. Kelvin who claimed he got this card so i contacted him and he gave me a %100 assurance that this people where real, reliable and trusted…& today i am amongst the people that gives testimony.. STAY AWAY FROM NIGERIA SCUMBAG.'

Well, I'm all in favour of staying away from scumbags, wherever they may be. However, one thing I did notice during years of 419-watching was that 419-ers would quite happily disown any connection with advance fee fraud and dishonest Nigerians while blatantly pushing exactly the same scam. I don't know for sure where this particular 'honest' so-called hacking group is based, but when a scammer starts talking about dishonest Nigerians, I can't help drawing my own conclusions.

So here’s the bad news (though it’s good news for those whose hard-earned cash helps to keep the banks afloat). There ain’t no such card. If you have a few hundred bucks to spend on something so improbable, there’s a scammer someone who’ll gladly relieve you of it and no doubt will feel quite justified in doing so.

Beating the 'Microsoft scam'

David Harley, ESET Senior Research Fellow
[This article previously appeared on the AVIEN blog.]

On the SC Magazine web site, Biocatch's VP of Product Management Oren Kedem asks 'After a decade, why can't we finally be rid of the Microsoft scam?', which is slightly odd, in that he reckons the support scam (no, he wasn't talking about the way Microsoft is pushing Windows 10!) has been around since 'at least 2009 in one form or another'. Well, I first heard about it in 2010, but Steve Burn, something of an authority on the sites that push these 'solutions', has indeed been following them since 2009. Still, that's rather less than a decade.

That doesn't invalidate Kedem's central point, though. In spite of all the publicity we've given to these scams, they're still clearly operational. While much of the action has shifted away from cold-calling to decoy popups and fake alerts, seeding undesirable URLs via SEO and social media, and even real malware, I still see reports on the ESET blog from people who've fallen for tricks like the old CLSID gag. Of course, they haven't necessarily been cold-called, but the scammers are clearly still using tried and tested gambits to 'prove' that the victims need their help.

Kedem suggests that education fails because people fly into a panic and forget what they've been told when a scammer actually captures their attention. There's probably something in that, but in my experience people tend to be fairly good at spotting a scam that's close to something they've previously been warned about. However, they're not so good at extrapolating from one scam to another when the underlying mechanism is the same, but the gambit used appears quite different. Which is why I try to demonstrate attack *principles* as well as just describing an attack. (That often goes for technical attacks as well as social engineering.)

Unfortunately, support scam attacks have proved fairly adaptable over the years. While the scammers themselves are often far from bright, the scripts they work from are sometimes pretty clever. (Fortunately, a not-so-bright scammer will very quickly sound much less convincing if you nudge them away from the comfort of an anticipated response. They'll tend to desperately try to get you back on script, often by ignoring awkward questions and repeating scripted material until it's clear they're not going to get anywhere.) Still, the social engineering gambits they use in those scripts (and even the more technical approaches we've seen recently) are often far brighter than the call-centre drones that deliver them.

Kedem does make an interesting suggestion about making bank employees identify themselves with a 'code of the month' which might have possibilities for reducing phishing. Unfortunately, I can't see how it would help with the 'Microsoft scam'. And while there are ways of implementing educational programmes that might have more impact, getting the home users who are the main targets of support scamming to undergo suitable training may not be so easy.

ESET Corporate News

ESET Rolls Out its Update for Remote Administrator

ESET started offering the latest version of ESET Remote Administrator, its platform-independent, remote management console for businesses. The current version brings improvements and new features to make the lives of IT Administrators easier.

It boasts a built-in task management system to minimize downtime, while enabling actions to be performed automatically based on dynamic group membership, even when endpoints are offline and not connected to ESET Remote Administrator. It has been enhanced with a post-installation wizard for intuitive setup and deployment in any environment and has redesigned mobile device enrollment ideal for mass enrollment of mobile devices. Automatic import to CSV is also a big plus point in favour of the latest version.

With ESET Remote Administrator's improved web interface, IT Administrators and security teams have a full overview of what is happening within the organization and can determine relationships between data and users. It can be installed on Windows as well as Linux servers, and also comes as a virtual appliance. ESET Remote Administrator uses integrated tools, dynamic threat protection, and has a new agent-based architecture to streamline both network security and administrative overhead.

In addition to this update, ESET announced the launch of ESET Remote Administrator (ERA) Virtual Machine® for Microsoft Azure. The product enables IT administrators to drill-down into endpoint security environments at any time, allowing ongoing security management and prompt remediation of problems. It is included with ESET endpoint product licenses and implementation requires no added cost. For more information, please visit http://business.eset.com/azure/.

ESET Flawless in VB100 and VBSpam+

Leading independent testing authority, Virus Bulletin, recently published its first comparative review of business and consumer products on Windows 10 Pro 64-bit. Upon completion, ESET NOD32 Antivirus remained its most reliable performer in the consumer segment, picking up its 95th VB100 award.

Of the 24 consumer products Virus Bulletin tested in full, ESET NOD32 Antivirus continued to display its excellence, delivering no false positives and once again achieving a "Solid" rating for its superb stability.

Virus Bulletin authority has also completed its VBSpam Comparative Review for June. The review reconfirmed that ESET Mail Security for Microsoft Exchange Server remains a market leading choice for spam filtering, receiving its fourth VBSpam+ award in a row.

The Top Ten Threats

1. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 11.68%

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

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 3.93%

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

3. Win32/Agent.XWT

Previous Ranking: 3
Percentage Detected: 2.32%

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.

4. HTML/Refresh

Previous Ranking: 5
Percentage Detected: 1.71%

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. JS/Adware.Agent.L

Previous Ranking: 4
Percentage Detected: 1.67%

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.

6. HTML/ScrInject

Previous Ranking: 9
Percentage Detected: 1.65%

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

7. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.20%

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.

8. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.18%

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

9. Defo

Previous Ranking: N/A
Percentage Detected: 1.12%

Defo is the detection name for program code of an MS-DOS-specific virus.

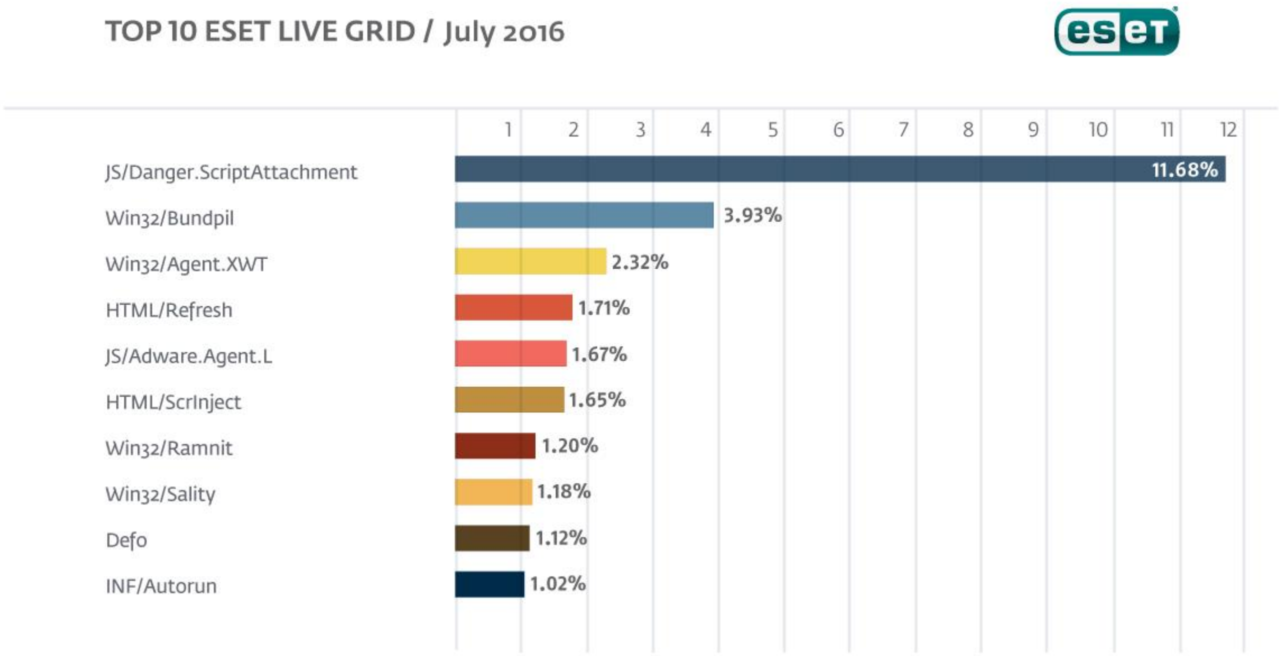
10. INF/Autorun

Previous Ranking: 10
Percentage Detected: 1.02%

INF/Autorun is a generic detection of multiple malicious versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malicious executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malicious executable when the infected drive is mounted. The malicious AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes set 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 11.68% 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