September 2014
Feature Article: Biting the Biter

ENJOY SAFER TECHNOLOGY™

Table of Contents

Biting the Biter 3
ESET Corporate News 5
The Top Ten Threats 6
Top Ten Threats at a Glance (graph) 9
About ESET 10
Additional Resources 10

Biting the Biter

David Harley, ESET Senior Research Fellow

[This article is partly based on articles by David Harley recently published on the AVIEN blog.]

Darren Pauli reports for the Register that Matthew Weeks has released a Metasploit module that exploits a flaw in Ammyy Admin 3.5 to attack a machine being used to 'take over' a client machine.

The rationale here is that Ammyy software is frequently used by support scammers to take over a victim's machine in order to 'prove' that the machine is infected by malware, or to install 'protective' software, or for other nefarious purposes. Well, if you found this post, the chances are you're well aware of support scammer operations, and if you're not, there's lots of information on this site here.

I don't, of course, have any interest in defending the activities – far less the systems – of support scammers, but this approach gives more than a little old-school AV queasiness. Weeks explains:

I don't normally release zero day exploits, but I made an exception in this case because given the reporting and usage of Ammyy Admin I consider it highly unlikely to be used to compromise innocent victims. The primary users at risk of compromise are the scammer groups.

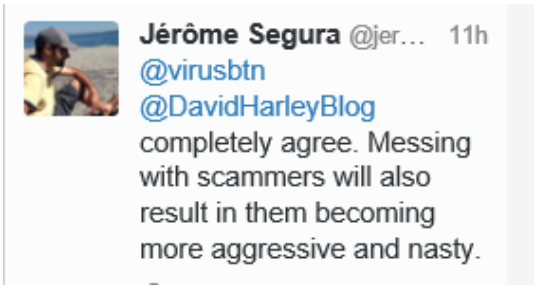
Primary users at risk? Well, he may not be able to see much risk to other groups, but I suspect that others can. In any case, who is going to make use of this? Probably not Weeks, since he acknowledges:

No scammer group has ever called me, and I have never used this except to test it and in demonstrations.

It's certainly not an approach that's going to be available to the victims of the scam, by definition: if they don't have the technical knowledge to recognize the (techno) logical flaws in an attacker's spiel, Metasploit means nothing to them. I can see some of the many people who go out of their way to waste a scammer's time trying this out, but in doing so they may well (as Pauli suggests) place themselves in legal jeopardy (*vide* UK Computer Misuse Act, for example), even if they feel ethically secure hacking a hacker. There may be an ethical justification there by analogy with sinkholing a botnet, for example, but botnet countermeasures also have to be done within legal limits.

Could the threat of such an approach be a deterrent to scammers? Perhaps, though I suspect that once scammers get to know about this kind of countermeasure, they may be quicker than legitimate users of Ammyy software to patch. Or simply move to one of the many alternative remote access systems used in support scams.

After this article was published, Jérôme Segura, who has blogged several times for Malwarebytes on the topic of support scams, pointed out that scammers are also likely to become more aggressive:



It's certainly the case that support scammers have, on occasion, shown considerable aggression when thwarted: not only by adopting a bullying tone, but on occasion by attempting to trash a victim's system.

An anonymous comment to one of my ESET blogs on the topic of support scams observed:

Same, got this scam today, saying they are from Microsoft, and calling to France!! and I thought, how can they expect people in here to speak english, doesn't microsoft have any local team...

It is kind of interesting that the scammers are still trying to expand their 'market' into regions that aren't primarily English-speaking. Perhaps inevitable, given that the US, UK, Australia etc. are so 'over-phished' – at one time I was receiving several of this kind of scam call a day – that it's hard to imagine that there's anyone left to take the bait*.

…and I stopped when they told me to go to www.teamviewer.com

I don't, by the way, think this is an indication of a specific attempt to evade possible hacks via the Ammyy vulnerability mentioned above. While ammyy.com is used so often that the scam is sometimes called the AMMYY scam in the US (and there are those who believe, incorrectly, that Ammyy is responsible for it), other legitimate remote access software is often misused by scammers.

…I confirm they have an indian accent and they say A for apple, O for Orange, I for Indiana, F for Folder, W for Web, E for English, D for Doctor which is not the usual radio alphabet

Certainly most (not quite all) reports of support scam callers refer to what is taken to be an Indian accent. However, I do know of instances where the scammers *have* used the NATO alphabet or a close equivalent. As do many legitimate helpdesk operators, of course, and we know that some of service centres perpetrating this sort of fraud are also executing legitimate support contracts. Indeed, some scammers don't seem to distinguish between legitimate and fraudulent support. So it's probably about the individual's knowledge (or lack of it) rather than a characteristic common to all support scammers.

A few weeks before, Blue Coat's Chris Larson, reported finding a site with a fake anti-virus scan masquerading as Microsoft Security Essentials. However, instead of being prompted as with old-time fake AV to download fake AV, he was prompted to connect with a 'live' support specialist via LiveChat.

That's not quite as novel as it may seem – see Scareware on the Piggy-Back of ACAD/Medre.A by Righard Zwienenberg (from 2012) about a 24/7 chat support service that wasn't, and Netflix Phishing Scam leads to Fake Microsoft Tech Support by Jérôme Segura (2014). Facebook Likes and cold-call scams (2011) describes sites sitting waiting for people to find them rather than (or as well as) proactively cold-calling. And there's lots more related information on the support scam resource page on the AVIEN site.

* There are no grounds for complacency there, though: the same scammers are enthusiastically trying other approaches such as accident compensation scams, the mythical government department of unsecured debts, and so on.) To quote one of my earlier blogs:

Offers of products and services benefiting from a fake government grant. I've had several of these, ranging from mortgage offers to grants for building work. I'm fairly sure our cash-strapped government is not giving away money for kitchen extensions and conservatories.

Refunds for overpaid tax, bank fees, mortgage refunds and so on. I'm trying to remember when I last got a tax refund: probably in the 1970s… Perhaps people really do get such refunds occasionally even in the present climate of 'We shouldn't have taken your money but we can't afford to give it back', but I'm pretty sure that agencies and institutions don't spend a lot of time and money telephoning people who might be entitled to restitution, still less paying Indian call centres to make such calls on their behalf.

ESET Corporate News

AV-Comparatives Declares: "ESET Cyber Security Pro for Mac Provides Outstanding Protection"

ESET Cyber Security Pro, the Internet security software for Mac, was highlighted as outstanding by AV-Comparatives' Mac Security Test and Review 2014. Testing by AV-Comparatives was for the detection of cross-platform malware targeting a wide range of platforms.

The AV-Comparatives test looked, among others, at malware and phishing alerts of Mac security software. With regards to ESET's product it tested, it found the following: "ESET Cyber Security Pro provides outstanding protection against malware with a well-designed user interface. The main program window makes essential functions and information easily accessible and alerts are sensible. The help facilities are exemplary. ESET produced a perfect score in our malware tests, identifying all samples of both Mac and Windows malware."

ESET Researchers Win "Péter Szőr Award" for Windigo paper at Virus Bulletin Conference

ESET was honored last week at the 24th Virus Bulletin International Conference in Seattle, USA when its Research Lab from Canada received the Péter Szőr Award for Best Technical Paper for research on Operation Windigo. "ESET Canada are worthy winners of this inaugural award in memory of the great Péter Szőr. The depth and breadth of the Operation Windigo investigation, the use of a range of groundbreaking techniques, and the high level of collaboration with other researchers and affected parties are all very much in the spirit of Péter's own excellent work. We hope this award will serve to encourage further superior-quality research from ESET and others in the future," said John Hawes, Chief of Operations at Virus Bulletin.

The Top Ten Threats

1. HTML/Refresh

Previous Ranking: N/A
Percentage Detected: 3.89%

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: 1
Percentage Detected: 2.29%

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. JS/Kryptik.I

Previous Ranking: 2
Percentage Detected: 2.03%

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.

4. Win32/Adware.MultiPlug

Previous Ranking: 3
Percentage Detected: 1.88%

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.

5. Win32/RiskWare.NetFilter

Previous Ranking: 4
Percentage Detected: 1.52%

Win32/RiskWare.NetFilter is an application that includes malicious code designed to force infected computers to allow an attacker to remotely connect to the infected system and control it, in order to steal sensitive information or install other malware.

6. LNK/Agent.AK

Previous Ranking: 5
Percentage Detected: 1.46%

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. Win32/Sality

Previous Ranking: 6
Percentage Detected: 1.36%

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

8. HTML/Iframe

Previous Ranking: N/A

Percentage Detected: 1.34%

Type of infiltration: Virus
HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

9. Win32/Danger.DoubleExtension

Previous Ranking: N/A
Percentage Detected: 1.26%

Win32/Danger.DoubleExtension is the name for generic detection of file using two or more extensions in filename (to appear to be document/picture file etc.) while the real file format is PE32. The last file extension has executable form.

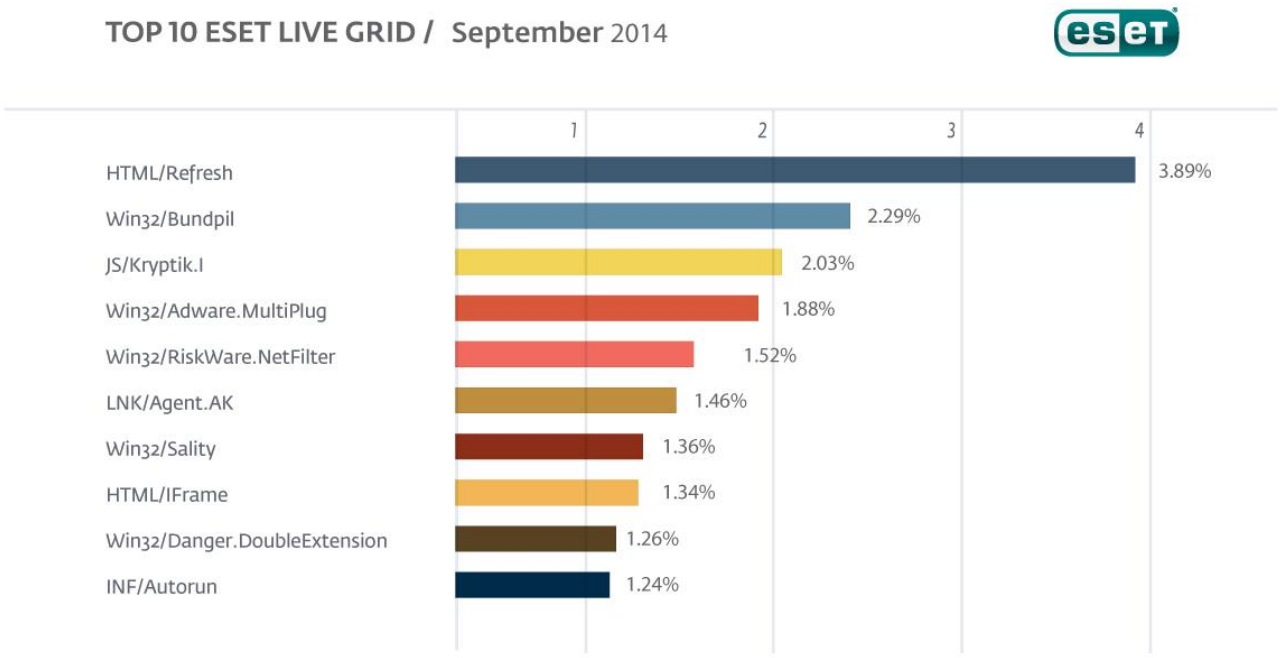
10. INF/Autorun

Previous Ranking: 7
Percentage Detected: 1.2%

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.

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 3.89% 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