January 2016
Feature Article: Tech Support Scams Revisited (Again)

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Tech Support Scams Revisited (Again)

David Harley, ESET Senior Research Fellow

Is Dell's customer database compromised? Plus, iYogi in trouble with Ranger Washington…

This article includes material drawn from an article that originally appeared on the IT Security UK web site on January 7th 2016, and another that appeared on the AVIEN blog on December 21st 2015.

This morning, to my great delight – considering it was ridiculously early – I got my first tech support scam call of 2016. In fact, it's the first I've received for quite a while. Possibly this was because the last wave of scammers learned that I don't suffer scammers gladly, but it's likelier that this reflects the lessening effectiveness of the ploys used by cold callers. And yet I find myself, for the second month running, writing about tech support scams. Clearly, there's life in the old dog's dinner yet…

Is Dell's customer database compromised?

One of the weaknesses of the classic cold-calling tech support scam is that even people who aren't particularly technologically knowledgeable might nevertheless be cautious enough to test the scammer's claim to know something about the potential victim's PC. For instance, by asking him to confirm what version of Windows was being used, or the brand of PC. Which is why the scammers are so fond of the CLSID ploy, where they attempt to persuade the victim that the string *ZFSendToTarget=CLSID{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}* is unique to their PC. Of course it isn't, as I said in that article:

That's the CLSID on both the PCs open on my desk at the moment. Amazingly, it's also the one that the scammer quoted to Herold. And I bet that if you have a recent version of Windows and go through the same steps you'll find that you have it too.

So as more people have learned to recognize that ploy for the deception it is, the scammers have tended to move away from cold-calling and towards the equally deceptive pop-ups that are so often used to lure a victim into calling what they believe, incorrectly, to be a legitimate helpline. Since the victim has actually initiated the phone call, they're already halfway to falling for whatever unlikely tale the scammer spins.

But what if the scammer does know more about you and your machine than you could reasonably expect? Recently, there's been a spate of cold-call scammers claiming to be calling from Dell. According to Nat Hoffelder these"support techs" know 'everything about a customer, including the customer's name, email, account info, and everything down to the support tag and device serial number.' An article by Rod Simmons from May 2015 suggests that this has been happening for several months, if not longer. I first became aware of it from an article published on 10 Zen Monkeys on the 4th of January 2016, which includes links to similar stories.

The article states:

I called the (real) Dell, and spoke to a customer support representative named Mark, who tried to explain how the scammers knew my account history.

"Dell has detected hackers," he said. "They're hacking our web site."

However, I haven't so far been able to find any official confirmation from Dell. The nearest I've found is from someone with the job title Liaison for Customer Care including the statement:

Unfortunately, there are unscrupulous third party entities posing as Dell or Microsoft representatives trying to obtain personal credit card information from Dell customers. Please be assured we take these reports very seriously. DO NOT give them any personal information as they are not associated with Dell.

Dan Goodin said on the 6th of December in an article for Ars Technica that the site has been in frequent communication with Dell, but has not received any answer to the question "…did Dell officials have any reason to believe its customer data had been compromised, and if not, how did they believe the scammers had access to serial numbers, contact information, and past support calls?"

Hoffelder comments "…the scary part is that these scam phone calls have been going on since at least May 2015, and Dell doesn't seem to be able to stop it." Actually, the really scary part is that Dell can't promise that its customers won't get unsolicited calls from the company if they've signed up with Dell's premium support services.

If this did turn out to be the result of a breach at Dell, what could the company do about it? Obviously it wouldn't be able to get the data back from the scammers, but it could notify the users of their products and services – especially the support services. After all, the company was able to respond reasonably appropriately to the recent exposure of backdoor issues with its computers. It could even, perhaps, make infrastructural changes to their database so that the stolen data would no longer be valid, though I don't suppose such an exercise would be particularly cheap. In the absence of more information, I have to agree with Goodin's advice that Dell customers "should presume their support histories and purchase and contact information has been compromised…"

iYogi tech support – sued by State of Washington

The name iYogi will not be unfamiliar to you, if you've been following how the tech support scam has been evolving over the past few years.

In Fake Support, And Now Fake Product Support I described how a legitimate and ethical AV company outsourced its support to the iYogi company in India. This must have seemed at the time an entirely reasonable way of addressing a difficulty that faces security companies with a product version that is free to consumers: what happens when users of that product need support? Running a tech support operation is a significant cost even for companies that charge for all their products (time-limited trials excepted, of course). The idea was that Avast! customers would get free support for Avast!-related queries, but would then be offered an upgrade to a for-fee iYogi support package. However, the AV company's understanding was that:

*… we **never** phone our customers (unless they specifically ask us to of course) and none of the partners we work with do either.*

Unfortunately, it seemed that iYogi's understanding of the situation was rather different. According to Brian Krebs, reported incidents of tech support scam cold-calling from "Avast customer service" did indeed turn out to have originated with iYogi.

While someone describing himself as the co-founder and president of marketing at iYogi strongly denied any connection with the usual gang of out-and-out scammers, Avast! found it necessary to suspend its arrangement with the company. Avast!'s later arrangements for customer support are discussed on the company's blog here.

Here's an extract from a paper I presented at Virus Bulletin in 2012, along with Martijn Grooten (Virus Bulletin), Craig Johnston (formerly an ESET researcher), and Steve Burn of Malwarebytes.

… iYogi, … was contracted to supply support services to Avast!, a highly reputable anti-virus vendor, but was exposed in March by journalist Brian Krebs as using unsavoury selling practices. ... While there are many unverifiable reports about this affair, many of the comments on the Krebs articles suggest that telephone support staff may have been encouraged when selling support contracts to go far beyond the terms of the company's agreement with Avast! Some of the comments claim to be from iYogi employees, some defending it and some agreeing that it engaged in unethical and possibly fraudulent practices.

iYogi's recent activities seem to have continued to attract controversy. Washington State recently announced a lawsuit against iYogi, alleging that 'iYogi's tactics are unfair and deceptive business practices that violate Washington's Consumer Protection Act.' The activities in which the company is alleged to have engaged have a familiar ring, involving deceptive online advertisements, misleading 'diagnostics', aggressive selling of support plans and the company's own anti-virus software.

In a twist I haven't encountered before, the Washington suit filed in King County Superior Court claims that:

iYogi tells the consumer that upgrading to Windows 10 from Windows 7 or 8 costs $199.00 if the upgrade is done independently, but that the upgrade is "included" for free as part of iYogi's five-year service package or for $80 as part of iYogi's one-year package. In fact, an upgrade to Windows 10 is free for Windows 7 or 8 users who choose to do so independently. In addition, iYogi incorrectly tells consumers that their computers will stop working if they do not upgrade to Windows 10 soon.

In the Help Net article cited above, Microsoft is quoted as estimating that 71,000 residents of Washington lose $33m each year, a sizeable proportion of the 3.3m Americans who are estimated to lose $1.5b in a year.

ESET Corporate News

Radicati Group Names ESET a Top Player in Endpoint Security Market Quadrants 2015

ESET was named a Top Player in the Radicati Group's "Endpoint Security – Market Quadrant 2015." ESET's ability to deliver high performing, easy-to-use security software with a low system footprint was noted in the report.

The Radicati Group's Market Quadrant report ranks organizations based on their product functionality and market share. Top Players such as ESET are recognized as being the current leaders of the market, with products that have built up large customer bases. To achieve the Top Player distinction, companies must offer advanced functionality, such as data loss prevention, device control, encryption, patch remediation, URL filtering and mobile protection.

"ESET has shown significant improvements both in product functionality and market share," said Sara Radicati, President and CEO of the Radicati Group, Inc. "ESET's endpoint solutions offer high performance and detection rates, while maintaining low system resource usage, helping businesses of all sizes to remain protected."

ESET's endpoint solutions were commended for their high performance and detection rates, while maintaining low system resource usage. The report also mentions ESET's Live Grid Early Warning System, which leverages real-time data from customers to add new threats to ESET's virus signature databases. The company's recently redesigned ESET Remote Administration is was also highlighted.

"We are proud to deliver security solutions that offer our customers the latest in next generation security protection, while not taking up valuable system resources," said Andrew Lee, CEO of ESET North America. "This recognition builds on ESET's history of award-winning solutions that help protect businesses and the customers they serve from the latest cyber threats."

ESET Earns 'Top Rated' Award from AV-Comparatives

AV-Comparatives, an independent anti-malware testing organization, published its annual Summary Report 2015 providing a market-wide overview and analysis of security products. In this year's report, ESET was one of the five vendors awarded AV-Comparative's *Top Rated Product* badge.

In addition to being named a *Top Rated Product*, ESET Smart Security 9 won the *Silver Award* in the False Positives category and the *Bronze Award* for Proactive Protection. The report highlights the improved graphical user interface (GUI) in ESET Smart Security 9, as well as its "excellent and comprehensive documentation."

"*ESET has been a constant part of our Summary Reports since 2006. With each new version, ESET Smart Security retains its clean*

trademark detection and sustains its low performance impact. With improved graphic design and finger-friendly controls, we believe that ESET products are suitable for use on touchscreens," said Andreas Clementi, CEO at AV-Comparatives.

In 2015, AV-Comparatives subjected 21 Windows security products, from a range of vendors, to rigorous investigation. All were tested for their ability to protect against real-world Internet threats, identify thousands of recent malicious programs, and provide protection without slowing down PCs.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 4.17%

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

2. LNK/Agent.BZ

Previous Ranking: 3
Percentage Detected: 4.01%

LNK/Agent.BZ 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.

3. Win32/Bayrob

Previous Ranking: N/A
Percentage Detected: 3.02%

Win32/Bayrob.D is a trojan that changes results returned by online search engines, usually related to eBay, UPS and AutoCheck; and acquires data and commands from a remote computer or the Internet. When executed, the trojan copies itself into the following location: %windir%\system32\WindowsUpdate.exe (163840 B). This copy is then executed.

4. LNK/Agent.AV

Previous Ranking: 5
Percentage Detected: 1.92%

LNK/Agent.AV is another 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.

5. JS/TrojanDownloader.Iframe

Previous Ranking: 7
Percentage Detected: 1.71%

JS/TrojanDownloader.Iframe is a trojan that redirects the browser to a specific URL location serving malicious software. The malicious code is usually embedded in HTML pages.

6. HTML/iFrame

Previous Ranking: N/A
Percentage Detected: 1.54%

HTML/IFrame is a generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location serving malicious software.

7. HTML/ScrInject

Previous Ranking: 4
Percentage Detected: 1.50%

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

8. Win32/Sality

Previous Ranking: 8
Percentage Detected: 1.46%

Sality is a polymorphic file infector. When it is 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

9. LNK/Agent.BS

Previous Ranking: 6
Percentage Detected: 1.39%

LNK/Agent.BS is another 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.

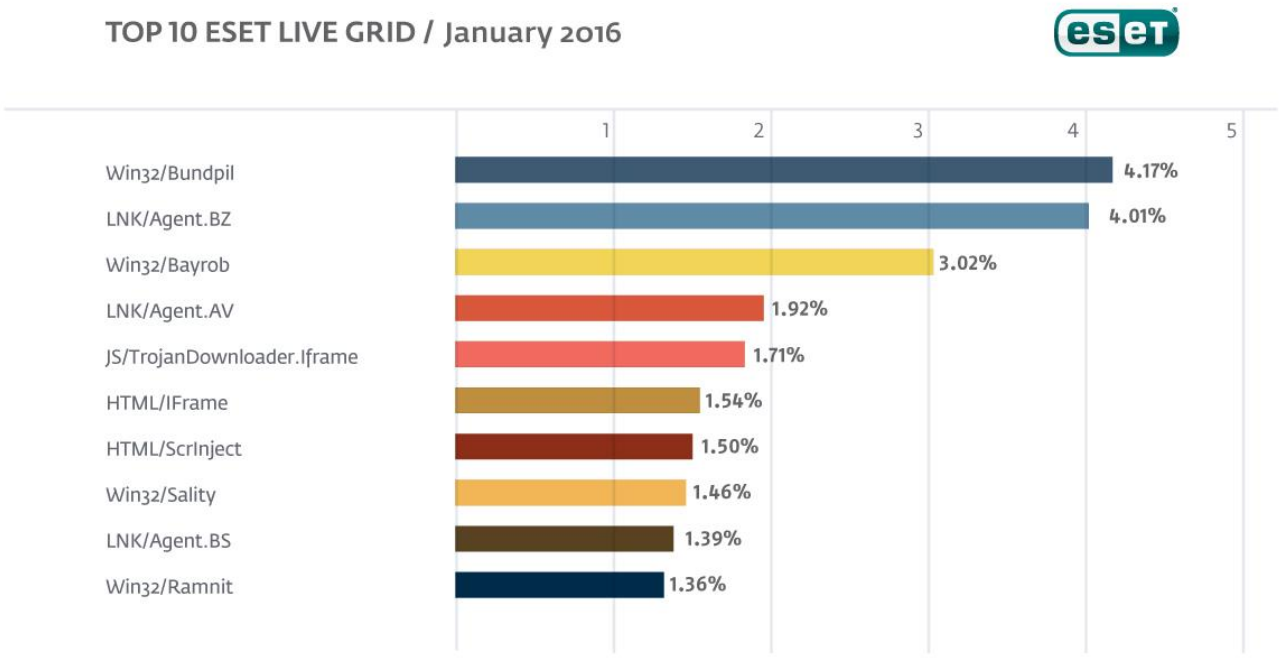
10. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.36%

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 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.

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 4.17% of the total, was scored by the Win32/Bundpil 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 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 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