August 2013

Feature Article: PC Support Scams: still keeping us amused

eset ENJOY SAFER TECHNOLOGY™

Table of Contents

PC Support Scams: still keeping us amused

David Harley CITP FBCS CISSP ESET Senior Research Fellow

A version of this article previously appeared on the Chainmailcheck hoax/scam blog.

It's been a while since I picked up the phone and found myself talking to a support scammer. That may be in part because I'm less likely to pick up a call that is flagged as 'International', 'Withheld' or 'Unknown number'. But when I do pick up a suspiciously anonymous call, it's usually a different kind of scam, PPI reclaim voice spam (mostly automated), and so on.

I haven't missed it a bit. So when I got a phone call from someone with a hard-to-parse Asiatic accent came on the line and started a familiar spiel, it was never likely that I was going to play along for any length of time. Life is too short.

The spiel, by the way, opens something like this, in my experience. Your mileage may vary.

"Am I speaking [or 'Can I speak to'] to Mr Jones?"

In this case, as in most of the support scams I get, the fact that I wasn't the person the scammer was expecting made no difference at all, though he did apologize profusely for getting my name wrong. Sometimes, though, the scammer will go to some length to tell you who you are and where you live, no doubt so that you will believe them when they tell you that they know that your PC is having problems (or causing them for someone else). However, if they manage to get your details right, that only really means that they've managed to check them in a directory.

Actually, the name they usually use when they call me isn't Jones, and I sometimes get calls that appear to be legitimate asking for the same person, so I guess there is a wrong entry on a directory or customer lead list somewhere. My rule of thumb is that if the caller apologizes for bothering me and rings off, it's probably a legitimate call that neither of us have any interest in. Though if the intended call was a sales call, that might raise a question as to whether they'd checked that the number was registered with the UK's Telephone Preference Service, a "do not call" list. Still, if they thought they were dealing with a customer, it's a grey area, at worst.

On this latest occasion, though, the scammer didn't go into the 'you are leaking viruses onto the entire Internet' spiel: instead, having ascertained that I actually had a computer, he started to tell me about computer errors and how they were worse than viruses because anti-virus software doesn't detect them. As he didn't seem deterred by my bursting into laughter, I told him that I'm a security researcher specializing in exposing support scams. As he didn't seem to know what a support scam is, I started to explain it to him, but he rang off. So I don't know exactly where he was going: no doubt he was going to 'prove' to me – perhaps with Event Viewer or ASSOC – that my system was at risk. But while I'm always interested in the latest scammer ploys, sometimes you just don't want to waste a Friday evening scammer baiting. Still, it seems that this is not an unusual approach: this, for instance, was a recent comment to one of my earlier blogs:

"…Said they were getting errors from my machine and my harddrive was corrupted. He prompted me to look at the event viewer, where I scrolled down and came to the first error which I tried to relate to him but he said that is all he needs and the error proves that my machine is infected. I have a good virus program and a good malware program I told him, but he said that the malware was undetectable."

Other recent comments showed that some people are still getting a certain amount of amusement out of yanking the chains of these wretched people. One of them interrupted their spiel by coming over all Anonymous:

We are Anonymous
We are one we are Many
We do not forgive
We do not forget
Expect US....

It amused me, too. I can’t guarantee that this will work in all cases, though.

Another told us:

“I did a quick search on Google for CLSID and found many examples of what a CLSID should look like. I quoted one of them to her and she freaked out because obviously I'm infected. So, I pretended to freak out too. I started screaming for my husband and quoting scripture. Having a blast by now. I kept yelling 'save me Jesus!' over and over. Then I begged her to please, please help me. What in the world am I to do? Poor helpless me!”

And finished off by telling the scammer in no uncertain terms what to expect if their paths crossed. Scary.

If you’re not familiar with this class of cold-call scam, here’s a paper a quartet of us (Martijn Grooten of Virus Bulletin, Steve Burn of Malwarebytes, my former colleague Craig Johnston and myself) presented at Virus Bulletin last year. It’s pretty comprehensive: My PC has 32,539 errors: how telephone support scams really work.

Other papers and blogs written or part-written by ESET researchers:

- FUD and Blunder: Tracking PC Support Scams
- Hanging on the Telephone
- How to recognize a PC support scam
- Misusing VERIFY (and other support scam tricks)
- Online PC Support scam: from cold calling to malware
- FTC cracks down on tech support scams and feds nail fake AV perps

Education as Data Defense

Stephen Cobb, CISSP
Senior Security Researcher, ESET North America

One possible consequence of an information security failure is the compromise of personal information known as a data breach. Each year, the Ponemon Institute tracks the total cost of data breaches based on a broad sample of companies, then calculates the average cost per capita (or person exposed). The latest figure: $136 per record. That's a global average, up from $130 in the previous year's study (based on incidents at 277 companies in 9 countries, the May 2013 report was sponsored by Symantec).

Clearly, digital information systems that handle confidential personal data are crucial to much of what we do today, either as consumers or business people, and failure to protect those systems can have costly consequences. (Bear in mind that the

Ponemon research found organizations in Germany and the U.S. experienced significantly higher costs, $199 and $188 respectively). Nevertheless, many people still seem to think we can keep these systems secure, always available, and always accurate, without providing the people who use them with relevant security training. That's like thinking we can have a safe and reliable transportation system without well-trained mechanics and properly licensed vehicle operators.

Last year, ESET conducted two surveys in America to better understand this phenomenon of cybersecurity under-education. We asked employed Americans if they had ever received computer security training of any kind from their employer. Only 32% said they had. In a second study, we asked a different group of Americans if they had ever taken any classes or training related to protecting their computer and/or personal information. For 68% of respondents, the answer was never. In other words, we can assume that less than a third of the workforce has any cyber security training at all.

This is a serious problem and Verizon's 2013 Data Breach Investigation Report speaks to this problem: The difficulty level of unauthorized intrusions into systems was rated as "low" in 78% of cases. Of course, the reality of a workforce under-educated in the realm of data defense is not news to criminals and other bad actors intent on abusing information technology for their own ends. They already know that employees are often the weakest link in an organization's information security.

As long as high tech security measures can be beaten by low tech attacks that exploit human weaknesses—such as inadequate knowledge and understanding—our data and systems will remain at risk of serious compromise. If your organization needs to be persuaded to spend money on security awareness and training try sharing this calculation: 7,500 customer records exposed at a cost of $136 per record = more than $1 million.

When you consider that equation, spending money on information security training and awareness makes a lot of sense, on the organizational level and within society as a whole. After all, data breaches are not a rare occurrence these days. One reason for this is the underground market in stolen data that is now thriving. Yet some organizations still don't realize that the personally identifiable information stored in their systems, be it customer records or employee records or data managed for a third party, is a target for cyber criminals.

Right now, the burden for security training falls mainly on companies, with some help from organizations like Security Our eCity and Ciber Seguridad. However, in the future your organization could be spared some of these costs if your country was committed to teaching cybersecurity hygiene to everyone, from an early age. We have not yet seen that kind of commitment in America, but that does not mean it is not possible. For example, in Estonia they have made cybersecurity training part of elementary-level school curriculum and they are working on expanding the program into preschool. Clearly, the time to invest in computer security training for employees is now, both at work and in our schools.

ESET Corporate News

ESET launches All New Version of ESET® Mobile Security for Android

ESET announced the launch of the completely rebuilt and redesigned ESET Mobile Security for Android. The next generation mobile product offers improved scanning, Anti-Phishing module and a completely redesigned user interface. ESET Mobile Security for Android enables Android smartphone and tablet users to enjoy safer mobile technology adventures with protection from both real world and digital threats.

“The rise of mobile malware combined with the popularity of Android devices creates a perfect storm of cyber security risk,” said Palo Luka, ESET’s CTO. “ESET is excited to offer a completely rebuilt and free version of our mobile security app that protects your sensitive data from threats giving you peace of mind when browsing the Internet or downloading applications.”

- **Brand New User Interface**—Now tablet, landscape, tap and eye-friendly.

- **Free and Premium Features Available at Google Play**—When installed from the official Android app store, users will benefit from features of the ESET Mobile Security for Android for free. Upgrade to a full version of ESET Mobile Security for Android from within the app for comprehensive and total protection against both digital and real-world threats.

- **Enhanced Antivirus Scanning**—Use variable depth scanning (quick/smart/deep) as well as scheduled and background scanning features. ESET Mobile Security is one of the few mobile security products for Android offering an advanced antivirus engine capable of detecting both known and unknown threats, including the recently discovered Android Master Key related vulnerabilities.

- **Startup and Anti-Theft Wizard**—Enjoy new user-friendly setup.

- **SMS & Call Filter**—Block SMS or incoming calls at specified times.

- **Security Audit**—Monitor installed application permissions such as location tracking, access to contacts, or in-app purchases to close any security loopholes.

- **Enhanced Anti-Phishing Module and Built-in USSD Control Features**—Protect against phishing attacks and web-based attacks via malicious SMS messages, QR codes, or URL links.

“One of our goals with the new version of ESET Mobile Security for Android was to make protection even easier for users,” said Andrew Lee, CEO, ESET NA. “Our new user interface and setup wizards are designed for mobile users looking for simple and powerful security products that are easy to configure, run quietly in the backgroundand require limited resources.”

ESET Mobile Security for Android is offered via web and Google Play. ESET Mobile Security for Android is designed to maximize their mobile security and use their mobile devices in less secure environments. Mobile users are enabled with ESET’s advanced protection as they navigate the Internet from connecting to public Wi-Fi networks and visiting sketchy websites, to clicking on suspicious email or chat messages to downloading apps from third party stores and monitoring their permissions.

According to the Gartner analyst firm, the Android operating system had an estimated market share of over 60 percent in 2012. That popularity makes it an increasingly attractive target for cyber criminals. In addition, from 2011 to 2012, Android malware grew by a factor of 17 according to recent ESET research into mobile cyberthreats. ESET Mobile Security for Android has protected users from some of the most far reaching mobile malware yet detected including 2012’s Android/TrojanSMS.Boxer.AA

In the latest evaluation of Android antivirus products by AV-TEST Institute, a leading independent international IT security and antivirus research firm, ESET Mobile Security for Android detected 99.7 percent of malicious apps, and earned top marks in usability.

Elementra Enhances ESET Endpoint Protection Through Kaseya Platform

ESET announced the newest version of the Elementra Endpoint Protection module. The new module offers greater administrative visibility, notification and security from within the Kaseya platform.

The Endpoint Protection module will allow managed service providers (MSPs) and IT administrators using Kaseya to view their ESET deployments across all client networks, gain real-time status updates and perform important administrative tasks to ensure maximum security. The dashboards also provide at-a-glance views of ESET version details, connection ages and protection states to quickly identify any devices that require attention. The module enables technicians to save time by sending updates and scan tasks to either individual or group machines.

“Since the Endpoint Protection module installs directly into the Kaseya platform, providers will benefit from secure client and server management on a centralized platform,“ said Ignacio Sbampato, ESET Chief Sales and Marketing Officer. “This integration improves the core functionality of the software and retains the ease of use, light footprint and strong protection ESET products are known for.“

The major new features of Endpoint Protection 1.1 include:

Alerts: Kaseya Alerts send automatically when ESET endpoints change from a state of Maximum Protection. These alerts allow technicians to monitor and ammend endpoint state changes from within Kaseya.

Improved Server Management: The ESET Remote Administrator (ERA) server management has been improved to provide more information and functionality. This centers IT technicians on the policies, license keys, licenses and endpoint plug-ins each ERA supports.

“The size and complexity of the development of version 1.1 required a significantly deeper integration with both Kaseya and ESET security products,“ said Duanne O’Brien, VP Engineering, Elementra. “The assistance provided by both of these business partners meant we could focus on the core functionality while tapping into expertise where and when needed, resulting in a more reliable and integrated product for our customers.“

“The combination of the Kaseya IT service management framework and the Elementra ESET solution represents an additional endpoint security opportunity for IT professionals,” said Jim Alves, EVP OEM & Strategic Initiatives of Kaseya.

The Elementra ESET plug-in for Kaseya was designed to meet the growing demand for seamless centralized service management.

Elementra first announced the ESET integration module for Kaseya in December of 2012. The Endpoint Protection 1.1 module can be downloaded and licenses purchased via the Elementra website - www.elementra.com

The Top Ten Threats

1. HTML/Iframe

Previous Ranking: 5
Percentage Detected: 4.26%

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.

2. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 3.45%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address, and it tries to download several files from the address. The files are then executed and the HTTP protocol is used. The worm may delete the following folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. HTML/ScrInject

Previous Ranking: 2
Percentage Detected: 2.59%

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

4. Win32/Sality

Previous Ranking: 4
Percentage Detected: 2.08%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature:

http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

5. INF/Autorun

Previous Ranking: 3
Percentage Detected: 2.06%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case.

6. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.62%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://www.eset.com/threat-center/blog/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders.

7. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.52%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.
The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

8. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.35%

It is a file infector. It's a virus that executes on every system start.It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.

9. Win32/Qhost

Previous Ranking: 10
Percentage Detected: 1.15 %

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.

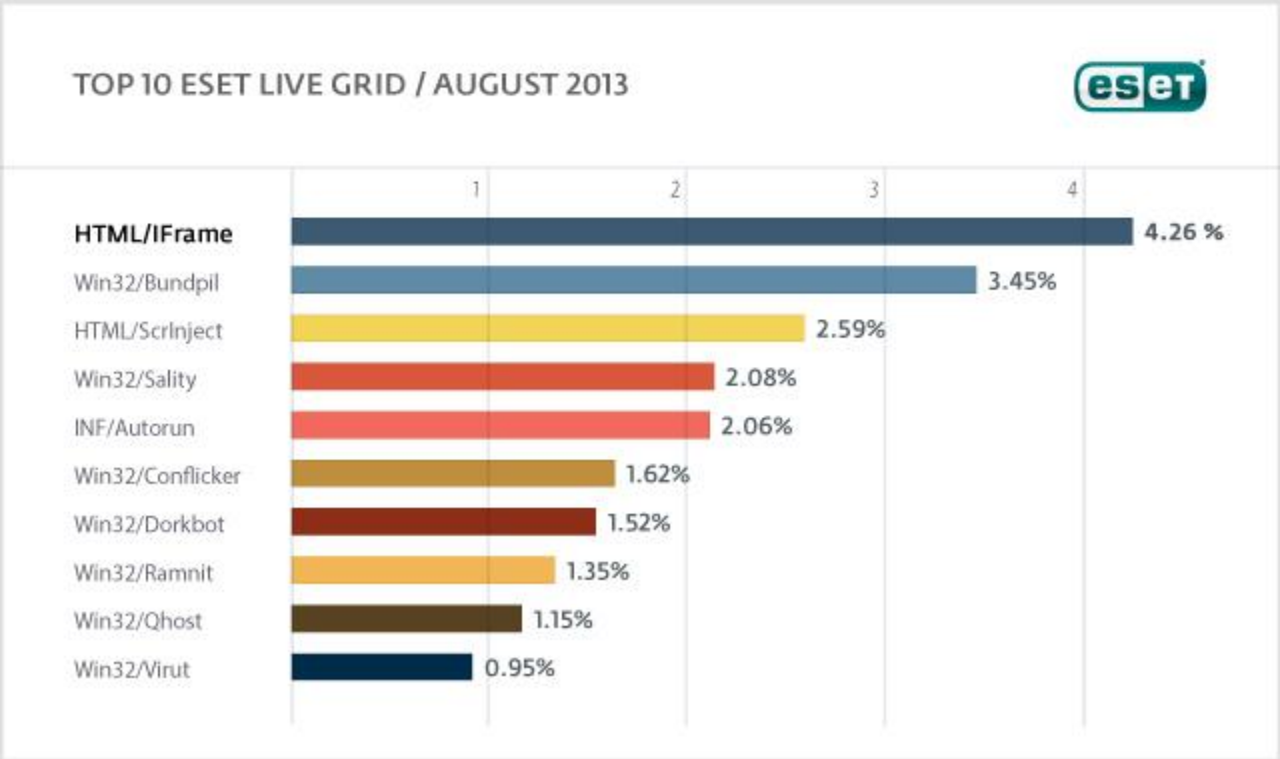
10. Win32/Virut

Previous Ranking: n/a
Percentage Detected: 0.95%

Win32/Virut is a polymorphic file infector. It affects files with EXE and SCR extensions, by adding the threat itself to the last section of the files source code. Aditionally, it searches for htm, php and asp files adding to them a malicious iframe. The virus connects to the IRC network. It can be controlled remotely.

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 almost 4.26% of the total, was scored by the HTML/IFrame 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
- ESET Blog (also available at welivesecurity.com)
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation

ENJOY SAFER TECHNOLOGY™