Global threat report

July 2010

Feature Article: Support Scams On The Rise

ESET

Table of Contents

Feature Article: Support Scams On The Rise

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Several months ago, reports started coming in from our ESET Ireland tech support staff and on online forums, that people are receiving unusual phone calls. These are calls from people claiming to represent online computer repair services, with various different generic names such as PC Support, PC Doctor, Online PC Repairs, etc, and offering to "fix" someone's computer. This sort of scam has been going on quietly since 2008, but has hit big this year. Worst affected, of course, are English speaking countries (and some sites and crimefighting institutions' public warnings have already been set up in UK, USA and Australia), but cases have also been reported in countries with other languages.

Usually the caller says they have MCSEs and Cisco Certified engineers available and offers to fix and optimise the computer remotely and clean it of any malware. The hesitant "customer" is told his system is probably riddled with worms and viruses, and is given simple instructions on how to open the Event Viewer and look for errors and warnings. As the Event Viewer is a reporting tool and therefore usually flags frequent but usually non-critical errors and warnings anyhow, this looks convincing enough for most computer-wary victims to lend the caller an ear, believing that something may actually be seriously wrong with their computer, and being all too ready to believe that their antivirus has let them down.

The interested victim is then usually instructed to access a certain website with Internet Explorer (which is more likely to be targeted for exploits) and download components needed to remotely "fix their computer"(and we all know what that can

entail). But to add insult to injury, the victim is asked for credit card details to pay for the procedure and then offered an extended "Warranty Service" at serious prices, such as 1 year for €99, 2 years €189, or 3 years €289 in some of the reported cases.

A number of similar stories come from the UK. In one case, the caller claimed to belong to a Microsoft-affiliated organization called "Support One Care" and had contacted a prospective victim to tell her that her PC was infected, her AV was out-of-date, and that for a one-off fee of £79 they would install a better product and give her a year's support. But in this case, unlike the above "no-name" magical solution, they claimed that the product they would be installing would be ESET's. And while "Support One Care" is a real India-based company, upon contact, they claimed to have nothing to do with the phone calls.

Investigation by ESET researchers in the US, Ireland and the UK , in consultation with independent researcher Steve Burn, law enforcement and other agencies, has thrown up a number of similar cases, nearly all of them traced back to companies based in Kolkata, India. And sure enough, cracked/pirated versions of ESET software have been installed by the scammers, though of course, being illegitimate copies, they have failed to work. This has led to a number of requests for support being placed with real ESET support desks. We can't tell how many similar scams have used or claimed to use products from other legitimate companies, but as we are aware of many sites offering cracks for other companies, it may be that reports to ESET are just the tip of a mighty iceberg.

So, what we're seeing in these and many other similar cases is a further personalisation and development of computer-related criminal activity. Evidently it is proving financially sound for cyber-criminals to set up call centres with own personnel, then

cold call and bait their way through long lists of phone numbers all over the world, making some easy income in the process. The problem with preventing such scams is that social engineering is very lo-tech in nature, requiring little in the way of technical resources and investment. Scammers are relying on the victims naivety, to grant them access to their computer and credit card details, so there's very little a security company can do to prevent them, apart from keeping its own software up to date so as to block scammer websites and detect the malware they may try to install and use once granted access.

However, David Harley comments that "Since victims of the scam are either not using up-to-date, legitimate security software or are voluntarily replacing it with compromised versions of other products, this may have little impact on the problem."

Most often it is difficult enough even learning of the various scam calls taking place, as there is no single, centrally-organised reporting system for such occurrences known to victims that may smell something fishy in due course: some call the police, some call AV vendors' tech support and some just hang up and forget about it.

Furthermore, Harley comments that "While we're doing our best to warn potential victims of the risk, this fraud is already all too similar to the fake antivirus reports we've grown accustomed to over recent years. It would be all too easy to extend the scam to use completely fake software, and not just antivirus software. Threats like this don't only harm users, but are an assault on the credibility of real security software, system maintenance tools and so on."

A tactic we're trying out at ESET Ireland is to give the topic public exposure with regular monthly newspaper and magazine columns where we explain and warn computer users of the

current cyber-crime activity and ask them to report unusual computer issues to us for further examination. Not only does this provide the public with a regular insight into latest threats and dangers, but it also provides us with valuable feedback from readers, which we can then use in planning improvements in our security solutions. In the case of support scams our message to readers was simple. Unless you know the company you're regularly dealing with, such calls are bogus. Not only are you handing over control of your computer to total strangers who can copy any of your files from it, access your browsing history, or get your stored passwords or banking and credit card details, but you're also handing your credit card numbers to them directly for any kind of possible abuse, and that may go far beyond a single fraudulent payment.

As cyber-criminals are adaptable, this scam comes in many shapes and sizes already, so here, courtesy of researchers David Harley and Steve Burn, are a few links with further elaborations on the support scam from various angles:

Fake AV Support Scams:
http://blog.eset.com/2010/07/20/fake-av-support-scams

Fake AV, Fake Support: http://securityweek.com/fake-av-fake-support

Marketing Misusing ESET's Name:
http://blog.eset.com/2010/06/23/marketing-misusing-esets-name

ALERT: metsupport.com – yet another telephone based fraud (aka SupportOnClick revisited – again):
http://hphosts.blogspot.com/2010/06/alert-metsupportcom-yet-another.html

techonsupport.com, click4rescue.com, pcrescueworld.com: SupportOnClick revisited:

http://hphosts.blogspot.com/2009/12/techonsupportcom-click4rescuecom.html

SupportOnClick: Phoned by Malwarebytes? BigPond? Anyone else?: http://hphosts.blogspot.com/2009/07/supportonclick-phoned-by-malwarebytes.html

SupportOnClick Update:

http://hphosts.blogspot.com/2009/04/supportonclick-update.html

supportonclick.com scamming you by telephone!:

http://hphosts.blogspot.com/2009/03/supportonclickcom-scamming-you-by.html

Fake tech support call scam – prefetch virus logmein123.com:

http://www.digitaltoast.co.uk/fake-tech-support-call-scam-prefetch-virus-logmein123com

New scam – They call you by phone!:

http://www.malwarebytes.org/forums/index.php?showtopic=11156

Staffordshire Council – Telephone computer support warning (PDF):

http://www.staffordshire.gov.uk/NR/rdonlyres/6997DBB0-E31E-4AFB-A886-C9DDEE114204/90090/TelephoneComputerSupportWarning.pdf

Cold call scam warns of virus infection: http://www.h-online.com/security/Cold-call-scam-warns-of-virus-infection–/news/112893

Scareware scammers adopt cold call tactics:

http://www.theregister.co.uk/2009/04/10/supportonclick_scareware_scam

Stuxnet: new 0-day exploit malware attack

During July another worm started spread using a new 0-day exploit in-the-wild. It is related to Microsoft Security Advisory 2286198, which reports a vulnerability in Windows Shell. In brief, the operating system incorrectly parsing shortcuts files (.LNK) in such a way that malicious code may be executed when the icon of a specially crafted shortcut is displayed, even if the user doesn't click on anything, and even if Autorun is disabled.

This vulnerability is being exploited by the malware detected by ESET NOD32 as *Win32/Stuxnet* (and also with generic signatures *LNK/Autostart.A* and *LNK/Exploit.CVE-2010-2568*). Win32/Stuxnet is a worm (and rootkit) that spread through USB devices and reached important volumes of infection, especially in some countries like United States (57,71% after worm was released) and Iran (30,00%). There are some workarounds including restricting user's privileges (always a good idea), or disabling network shares, webDAV and the display of shortcuts, but unfortunately the latter options could have significant impact on some Windows users. Microsoft is working to release a patch, but it's quite possible that there will be no patch for Windows XP SP2 or Windows 2000, which have recently reached the end of their support life.

Also, it is significant that Stuxnet was apparently firstly developed to attack SCADA systems, specifically targeting SIEMENS control systems, (used in critical national infrastructure) using a known default password that the software company hard-coded into its system.

A few days after Microsoft's advisory, ESET identified two new malware families exploiting the same vulnerability. They were *Win32/TrojanDownloader.Chymine.A* and *Win32/Autorun.VB.RP*, both taking advantage of the vulnerability in different ways. There have been subsequent reports of other older malware such as the so-called Zeus botnet and Win32/Sality generating variants incorporating similar exploits

The facts around this so far unpatched vulnerability and 0-day exploit, with several malware families taking advantage of it, international customers of a big company affected by the worm, its dramatic infection rates and the misappropriation of digital signatures; all combined to make Win32/Stuxnet the most significant threat of the month, and probably one of the more important examples of malware we've seen so far this year.

More information about Win32/Stuxnet and the .LNK vulnerability:

(Windows) Shellshocked, Or Why Win32/Stuxnet Sux…
http://blog.eset.com/2010/07/17/windows-shellshocked-or-why-win32stuxnet-sux

Which Army Attacked the Power Grids?
http://blog.eset.com/2010/07/19/which-army-attacked-the-power-grids

Yet more on Win32/Stuxnet
http://blog.eset.com/2010/07/19/yet-more-on-win32stuxnet

Win32/Stuxnet Signed Binaries
http://blog.eset.com/2010/07/19/win32stuxnet-signed-binaries

Win32/Stuxnet: more news and resources
http://blog.eset.com/2010/07/21/win32stuxnet-more-news-and-resources

New malicious LNKs: here we go…
http://blog.eset.com/2010/07/22/new-malicious-lnks-here-we-go

A few facts about Win32/Stuxnet & CVE-2010-2568
http://blog.eset.com/2010/07/22/a-few-facts-about-win32stuxnet-cve-2010-2568

ESET on the conference circuit

In the remainder of the year, ESET's team will be delivering presentations at various international conferences.

In July, during Recon (Montreal), Pierre-Marc Bureau and Joan Calvet made a presentation on Swizzor, an old malware family having been around since, at least, 2002. More information about this threat: http://blog.eset.com/2010/07/15/swizzor-for-dummies

There are also confirmed many presentations for the next months:

In CFET (The 4th International Conference on Cybercrime Forensics Education & Training) helding the 2nd and 3rd of September in the Canterbury Christ Church University, David Harley is presenting on " Antivirus Testing and AMTO: has anything changed?" and "SODDImy and the Trojan Defence".

On the 20th Virus Bulletin International Conference, between 29 September and 1 October in Vancouver, Canada, ESET will be presenting:

"Large-scale experiments malware, how and why so what?" By Joan Calvet, Jean-Yves Marion, Pierre-Marc Bureau and Jose M. Fernandez.

"AV Testing Exposed", by Peter Kosin, Juraj Malcho, Richard Marko and David Harley.

"Call of the WildList: last orders for WildCore-based testing?", By David Harley and Andrew Lee.

On the 13th Association of Anti Virus Asia Researchers International Conference, from 17 to 19 of November, in Bali, David Harley, Lysa Myers and Eddy Willems are presenting "Files and Product Evaluation: the Case for and against Malware Simulation".

New white papers

During July, we released two new white papers that are available in ESET's website:

 "Twenty years before the mouse", by Aryeh Goretsky: ESET LLC's Distinguished Researcher, a veteran of the anti-virus industry from the days when there barely was a virus industry. Written in the form of a personal retrospective, this paper compares the earliest days of PC computer viruses with today's threats, as well as provides a glimpse into the origins of the computer anti-virus industry.
http://www.eset.com/resources/white-papers/EsetWP-20YearsBeforeTheMouse.pdf

"TDL3: The Rootkit of All Evil?", by Aleksandr Matrosov and Eugene Rodionov: account of an Investigation into a Cybercrime Group, this is a comprehensive consideration, by researchers with ESET's partners in Russia, of the distribution

and the internals of the TDL3 Rootkit, and the involvement of the Dogma Millions group.
http://www.eset.com/resources/white-papers/TDL3-Analysis.pdf

The Top Ten Threats

It probably comes as no surprise that Conficker is once again the top-ranking threat, though perhaps it should, given the age of the extant versions. INF/Autorun continues to be prevalent, even though it's now fairly easy to disable the default setting that makes this attack possible.

1. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 12.47%
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.

What does this mean for the End User?
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. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. However, the Conficker Working Group estimates that there are still over 6 million infected machines out there.

2. INF/Autorun

Previous Ranking: 2
Percentage Detected: 5.90%

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.

What does this mean for the End User?

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, as Randy Abrams has suggested in our blog (http://www.eset.com/threat-center/blog/?p=94; http://www.eset.com/threat-center/blog/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

3. Win32/Agent

Previous Ranking: 4
Percentage Detected: 3.65%

ESET NOD32 describes this detection of malicious code as generic, as it describes members of a broad malware family capable of stealing user information from infected PCs.

To achieve this, the malware usually copies itself into temporary locations and adds keys to the registry which refers to this file or similar ones created randomly in other operating system's folders, which will let the process run at every system

startup.

What does this mean for the End User?

This label covers such a range of threats, using a wide range of infection vectors that it's not really possible to prescribe a single approach to avoiding the malware it includes. Use good anti-malware (we can suggest a good product 🙂), good patching practice, disable Autorun, and think before you click.

4. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 3.19%

This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

What does this mean for the End User?

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Research team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at

http://www.eset.com/threat-
center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf

5. Win32/Sality

Previous Ranking: 7
Percentage Detected: 1.54%

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

6. HTML/ScrInject.B

Previous Ranking: 10
Percentage Detected: 1.42%

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

What does this mean for the End User?

Malicious scripts and malicious iframes are a major cause of infection, and it's a good idea to disable scripting by default where possible, not only in browsers but in PDF readers. NoScript is a useful open source extension for Firefox that allows selective disabling/enabling of Javascript and other potential attack vectors.

7. INF/Conficker

Previous Ranking: 6
Percentage Detected: 1.32%

INF/Conficker is related to the INF/Autorun detection: the detection label is applied to a version of the file autorun.inf used to spread later variants of the Conficker worm.

What does this mean for the End User?

As far as the end user is concerned, this malware provides one more good reason for disabling the Autorun facility: see the section on INF/Autorun above.

8. Win32/Dursg.A

Previous Ranking: n/a
Percentage Detected: 1.14%

Win32/Dursg.A is a Trojan, probably of Russian origin, that redirects results of online search engines to web sites that contain adware. The malicious file is obfuscated using UPX run-time compression. The malware modifies information in popular browsers including Internet Explorer, Google Chrome, Mozilla Firefox and Opera relating to well known search engines and other services including Google, Yahoo, MSN, Bing and YouTube, so as to divert user searches to adware-hosting sites when one of a wide range of commonly used keywords is entered.

What does this mean for the End User?

Misdirected searches are often a clear indication of the presence of some form of malware, though there are many possible mechanisms for diverting searches to malicious or unwanted sites. This one spreads by various means, including availability under misleading names on file-sharing (P2P) networks.

For more detailed information see

http://www.eset.eu/encyclopaedia/win32-dursg-a-p2p-worm-agent-aak-w32-sillyp2p-trojan-c?lng=en.

9. Win32/Spy.Ursnif.A

Previous Ranking: 9
Percentage Detected: 0.90%

This label describes a spyware application that steals

information from an infected PC and sends it to a remote location, creating a hidden user account in order to allow communication over Remote Desktop connections. More information about this malware is available at

http://www.eset.eu/encyclopaedia/win32-spy-ursnif-a-trojan-win32-inject-kzl-spy-ursnif-gen-h-patch-zgm?lng=en

What does this mean for the End User?

While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with the esoterica of Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created. In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in patching, and in avoiding unexpected file downloads/transfers and attachments.

10. Win32/Oficla.GN

Previous Ranking: 35
Percentage Detected: 0.80%

Win32/Oficla.GN is a member of a family of trojans that tries to download other malware from the Internet. It is controlled by a remote machine, and is used to download and execute malicious programs from the Internet.

What does this mean for the End User?

Apart from the usual countermeasures as regards updating protective programs, the impact of malware families like this can be mitigated by restricting a user's ability to install and execute programs. Even for home users, we recommend that you don't run from a privileged (administrator) account

routinely. Use such accounts only when you need to.

Top Ten Threats at a Glance (graph)

Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 12.47% of the total, was scored by the Win32/Conficker class of threat.
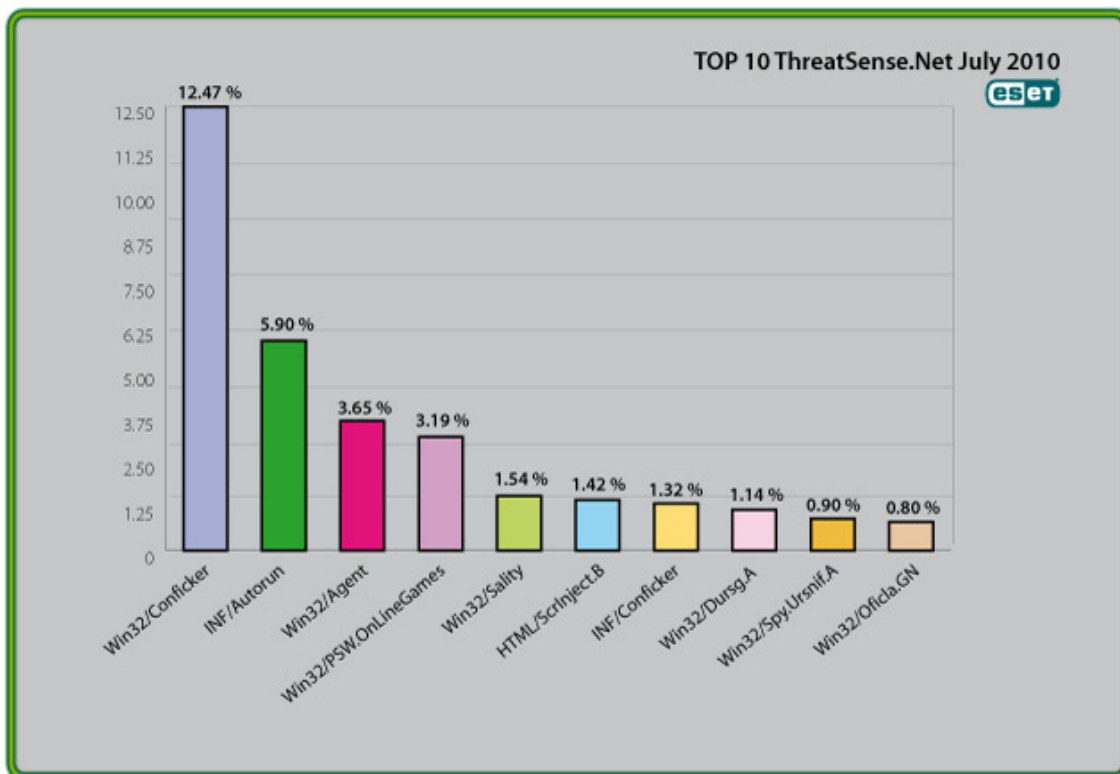
About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

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
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation