November 2010

Feature Article: Stealing from Santa (Scammers' Holiday Season)

Table of Contents

Feature Article: Stealing from Santa (Scammers' Holiday Season)

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Why is Christmas one of the jolliest seasons for cybercriminals? Because this is the time when the most money is spent online in the shortest time, and there are many opportunities for them to make themselves a hefty Christmas bonus as a reward for the other malicious activities they've been busy with throughout the year. And they are actually immoral enough to steal even from Santa!

There are many jobs cybercriminals go to work on in the holiday season, but most involve either getting hold of online shoppers' money without their knowledge, or conning them into handing it over voluntarily. The first category would mainly include stealing online shopping credentials (such as passwords to PayPal, Amazon and others) or credit and other payment card details. This is mainly achieved either through spyware installed on infected computers or through fake websites used instead of legitimate ones to con users into typing in their log in credentials. It may also be done by setting up a website for holiday shopping that simply doesn't deliver the goods users were charged for, or which delivers something of no real value. Another popular scam is Black Hat Search Engine Optimisation (BHSEO) which redirects searches on shopping-related keywords to malicious websites that try to infect the users with rogue antivirus and other malware. Just recently we have encountered malicious SEO regarding The Royal Family and The Korean conflict, while scams related to Christmas-shopping are becoming more sophisticated every year. Once any of these data fall into the hands of cybercriminals, they can be used to purchase real or bogus items, and generate a nice little profit. A spring survey in Ireland revealed that 76% of Irish consumers have been targeted by scams and the frequency of their engagement is expected to intensify during the Christmas season.

Then there is the lowest form of life in the cybercriminal fraternity, the charity abusers. As criminals are all too aware that many people like to make charitable donations when the Christmas spirit is at its most infectious, many fake online charities appear around this time. These are known to surface around any disasters that occurred, so we had many fake Haiti earthquake and Asian tsunami charity scams, and Chilean miner scams were also reported. The global economic crisis is likely to spawn other fake charities in various countries, pretending to appeal for help for impoverished families. While we certainly don't wish to discourage charitable donations, we do appeal to people to choose known and trusted organisations, or to do a proper check up on any others they wish to donate to: for instance, check the charity checklist by The U.S. Federal Trade Commission.

What else can computer users do to protect themselves?

- When searching for a gift online, check what websites you're being directed to. It is always safer to type in the address of the shopping site you wish to access, than to click any link you're offered, as it may lead you somewhere you definitely wouldn't want to go.

- Key words such as the names of popular items, brand names, computer games, sales, deals, could all lead to fake websites where search engines have been poisoned.

- Look for secure "https" connections on the sites where you shop.

- Check your PayPal and card balances regularly for any unusual expenses, and stop credit card payments immediately if you see something suspicious.

- Be careful about emails claiming to be “shipping information“ or “sales invoices“ for items you didn't order, as they could have an infected file or link attached.

- Use different passwords for any sites you use that require an authenticated log-in, so that even if cybercriminals intercept one of your passwords, they won't be able to get to all your sites.

- Overall, use common sense, and do browse for news on the latest scams occasionally, so that you know what you're up against.

How to fool a security researcher

Andrew Lee conducted a fun but disquieting thought experiment in the course of an amusing and informative presentation on user education at the Virus Bulletin Seminar.

Most security researchers have an innate distrust of Facebook, and perhaps all social media. Facebook, though, is particularly untrusted, by virtue of some of its founder’s habit of putting his foot in his mouth, some unfortunate system/administration slip-ups, but most of all the fact that it continuously walks a line between its core business (sharing customer information) and its duty of care to protect its customers from inappropriate disclosure. Does anyone think they always get that balance right? Thought not... Nonetheless, some researchers do have Facebook accounts, and may have more than one reason to do so: research into current FB issues, a means of disseminating security and product information, an extra channel for communication with other researchers, or a combination of these. Some, believe it or not, even use it as a way of communicating with their friends and relatives, just like everyone else. And you’d think that in general, they’d probably be more careful about security and privacy than most. Well, in general, they are. But...

Andrew made use of a flaw affecting Facebook’s signup procedure (no, we’re not going to tell you what it is for obvious reasons, and we expect it to be fixed very shortly in any case) to set up an account in someone else’s name (an individual well-known in the AV industry) without his knowledge. Then he used that account to invite a number of people to be FB friends. During the presentation, he used a live demo to illustrate how many (security) people had responded to the bogus overtures. And yes, several of whom were in the room at the time.

Earlier in his presentation, he’d described three of the main human “vulnerabilities” exploited by social engineers: fear, trust, and greed. This was certainly an illustration of how a violation of trust can cascade: as more people accepted, so the likelihood increased that someone else who received the invitation would be put off their guard when they saw that they had N mutual friends. However, he also made use of another of the “seven deadly vices” described by David Harley in an EICAR paper on social engineering: that is, curiosity. The individual whose identity had been spoofed is well-known as the least likely individual to start using Facebook, so it was natural that people were curious to see what “he” was up to.

Well, no damage done: it wasn’t a real attack. And in any case, it’s reasonable to assume that people whose jobs are focused on security and privacy will be reasonably careful in choosing what data they will publish on Facebook or similar semi-open networks, and the latitude they will allow the company in

sharing it. And this particular loophole is expected to be closed, as already mentioned. However, there are many ways of spoofing identities in social networking. What ways are there to minimize the risk?

Well, in this case, it would have made sense for more people to have confirmed that the invitation was genuine using an "out-of-band", trusted and trustworthy communication channel. Perhaps an email or instant message to a known "good" address, or even (good heavens!) a phone call. Bear in mind, though, that email addresses and phone numbers can also be compromised. It may not seem likely that an attacker would try to manipulate all these channels, but what if you were being used as the target or vector for an individually targeted attack? Teams assembled to target government departments, SCADA facilities and the like are often both knowledgeable and well-resourced (think Stuxnet).

AVAR and After

The 13th AVAR (Association of anti Virus Asia Researchers) Conference took place in Bali from the 17-19th November. The annual AVAR conference is one of the highlights of an anti-malware researcher's year (along with Virus Bulletin and EICAR), and ESET was strongly represented there, as a sponsor and in terms of presence at the podium, with presentations by Randy Abrams (ESET Director of Technical Education) and David Harley (ESET Senior Research Fellow), while Jeff Debrosse (Senior Security Evangelist) was one of the speakers in a panel on "Rogue, Anything Rogue?!?". David's joint paper with Eddy Willems and Lysa Myers on "Test Files and Product Evaluation: The Case for and against Malware Simulation" will be available on the white papers page shortly. Randy's presentation on "Which Part of the Prickly Pear is the Endpoint?" is available as a podcast from Bitpipe.

For further information: Jakarta Post; Chip; PC Plus; AVAR.

However, the presence of security experts from all over the world did not have a lasting effect on Indonesian security, unfortunately. On 26th November the Jakarta Globe reported that the Twitter account of Andy Arief, adviser for disaster management and social affairs to President Susilo Bambang Yudhoyono, had been hacked. Among a number of "politically motivated" jibes was a tweet announcing that Jakarta would be struck on Friday (the following day) by a tsunami.

It's not surprising that tsunamis are considered a serious matter in Indonesia, which was the region most heavily impacted by the 2004 tsunami, and as Urban mentions in his feature article, this generated a number of charity scams, as well as a number of hoaxes, to which David and Randy alluded in their 2009 Virus Bulletin paper "Whatever happened to the Unlikely Lads?" obtainable from the white papers page.

Virus Bulletin Seminar

While the Virus Bulletin conference is the one that anti-malware researchers will never miss if they can avoid it, ESET was delighted to sponsor a smaller, one-day event in London that nevertheless featured speakers of equal calibre: indeed,

several of the speakers are also regular speakers at the VB conference, including Alex Shipp, our own Juraj Malcho (with a presentation based on ESET's Stuxnet analysis at http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf), Martin Overton, Graham Cluley, and Andrew Lee. The full programme, including abstracts, is available at http://www.virusbtn.com/seminar/index, and it's expected that some of the presentations will be made available on the Virus Bulletin web site in due course.

During the course of the seminar, news broke of a rather frightening story from Sky News claiming that the code for Stuxnet is being traded on the black market, and that practically the entire global infrastructure was threatened accordingly. Security luminaries such as Paul Ducklin, David Harley and Roger Thompson think differently: see David's blog article "Stuxnet Code: Chicken Licken or Chicken Run?"

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 5.75%

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, 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.

2. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 4.92%

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&l

ng=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. 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. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 2.54%

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.

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

4. Win32/Sality

Previous Ranking: 4
Percentage Detected: 2.10%

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. Win32/Tifaut.C

Previous Ranking: 6
Percentage Detected: 1.50%

The Tifaut malware is based on the Autoit scripting language.

This malware spreads between computers by copying itself to removable storage devices and by creating an Autorun.inf file to start automatically.
The autorun.inf file is generated with junk comments to make it harder to identify by security solutions. This malware was created to steal information from infected computers.

See INF/Autorun above for discussion of the implications of software that spreads using Autorun.inf as a vector.

6. INF/Conficker

Previous Ranking: 5
Percentage Detected: 1.46%

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.

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.

7. JS/Exploit.CVE-2010-0806.A

Previous Ranking: 29
Percentage Detected: 0.99%

JS/Exploit.CVE-2010-0806.A is a detection for specially crafted JavaScript files, which exploit the CVE-2010-0806 vulnerability. The trojan is usually a part of other malware. By exploiting this vulnerability, an attacker may be able to execute remote arbitrary code on a vulnerable system.

8. Win32/Bflient.K

Previous Ranking: 8
Percentage Detected: 0.88%

Win32/Bflient.K is a worm that spreads via removable media and contains a backdoor. It can be controlled remotely and ensures it is started each time infected media is inserted into the computer.

9. Win32/Spy.Ursnif.A

Previous Ranking: 10
Percentage Detected: 0.81%

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

10. HTML/ScrInject.B

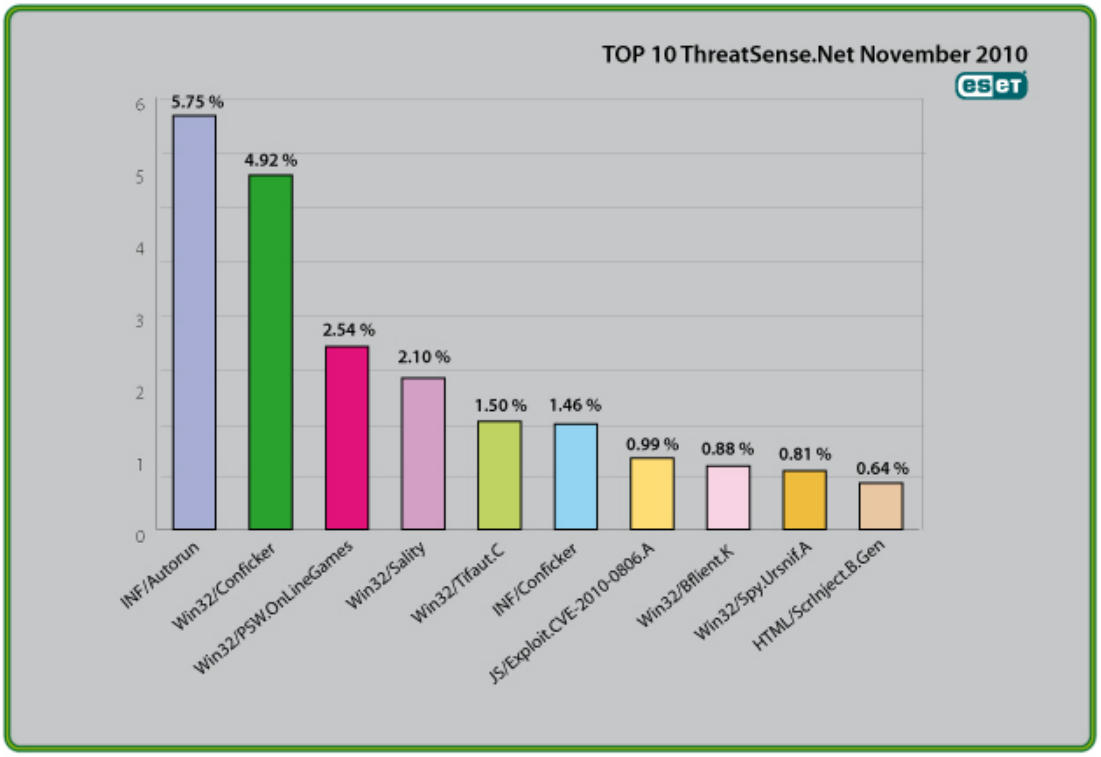
Previous Ranking: 7
Percentage Detected: 0.64%

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

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.

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 5.75% of the total, was scored by the INF/Autorun 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