January 2011

Feature Article: Stuxnet: conspiracy or sensationalism?

eset

Table of Contents

Feature Article: Stuxnet: conspiracy o sensationalism? 3
Tweetie Pie 4
How effective are phishing attacks 5
Merry-go-round: the AMTSO wheel of pain 5
The Top Ten Threats 6
Top Ten Threats at a Glance (graph) 10
About ESET 11
Additional resources 11

Feature Article: Stuxnet: conspiracy o sensationalism?

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

For months now the general public has been bombarded with views from various angles of the Stuxnet worm. What does it really do? Who started it? Why? Was it the Americans and the Israelis? Was it the Chinese? Was it SPECTRE? Oh and there's nuclear facilities. And fundamentalist regimes. And cyber-warfare. And state terrorism. And all kinds of other doomsday buzzwords which we simply cannot ignore, because as we all know, we're always living on the edge of being blown up.

Ok, for the dedicated reader, keen to get into all the ins and outs of the matter, ESET researcher David Harley has been diligently collecting all sorts of Stuxnet information and resources at the ESET blog as a supplement to the comprehensive ESET analysis Stuxnet Under The Microscope:

- http://blog.eset.com/2011/01/03/stuxnet-information-and-resources
- http://blog.eset.com/2011/01/20/stuxnet-information-and-resources-2
- http://blog.eset.com/2011/01/23/stuxnet-information-and-resources-3

Therefore no one can claim we're not taking the topic seriously or without proper expert scrutiny.

There is an additional side to this, however, that isn't quite as entertaining. And that is, that as with practically every story of this sort, this one has also been hijacked mainly for its buzz value, rather than the spectacular significance of anything the malware is actually known to have done. And that in itself is perhaps the greatest damage caused by Stuxnet.

Rather than staying within the realm of rational IT security analysis, it became a barely-understood but hot topic, mysteriously interesting enough to fill headlines and spark conspiracy debates, while in the meantime, *real* cybercrime, its actual goals and direct enough methods are not being covered adequately.

The effect that this has on the general public is to introduce an aura of esoteric mystification around the topics of cybercrime and hacking topics yet again, and that seems to reinforce the ever-present sense of false security induced by the comforting thought "it can't happen to me", since, obviously, these things target governments, banks, corporations, the big players, and not the small and insignificant computer end user.

But this is not actually the case. One report details the cybercrime economic model, another calculates the end costs of cybercriminal activity, yet another claims that "Cyber crime has surpassed drug trafficking as a criminal money-maker". But all agree that it's a clear and present danger aimed directly at people's wallets and steps are being taken to determine the damage values more precisely.

Similarly, the content of ESET's lengthy report is mostly of interest only to other researchers (in and out of the industry), and the relatively few journalists and others with the necessary savvy to understand the technicalities of the exploit code Stuxnet incorporates. Does this mean that it doesn't affect the end user? Obviously not, since it is, ultimately, the end user who is directly affected by the presence of malcode on his machine. That's without considering the ways in which he might be affected eventually, directly or indirectly, by Stuxnet's success in achieving its aims (whatever they might be, exactly), since that remains in the realm of speculation, however fascinating that speculation might be.

Sure, the governmental and corporate levels of computer user are also targeted, as they have been by Stuxnet, but the bulk of the damage is done in the sector where money is easiest to get to. And *that* mainly consists of the home user and small and medium business, due to frequency of transactions coupled with insufficient awareness of all the operational methods employed by cybercriminals.

What is more likely to affect me on the daily level, the conspiracy games of international politics, or someone stealing money via my phone? As ESET's Awareness Coordinator Sebastian Bortnik said in one of his recent blogs: *"Ignorance on behalf of the users is the main advantage for attackers. … An educated user is less likely to be victim than the other ones"* And with sensationalist reporting on a few select topics like the conspiratorial nature of the Stuxnet worm, the bulk of the *important* information is getting lost in the noise.

Tweetie Pie

Richard Adhikari wrote a piece this month (in which he quoted ESET's David Harley) in Tech News World, describing the use of URLs shortened with Google's own goo.gl service in order to drive victims to sites pushing fake security software (Scareware Scam Has Tweeters Atwitter: http://www.technewsworld.com/story/71700.html?wlc=1295642379). In this instance, the compressed URL opens a scareware site via a series of redirects. The site name is shortened by way of obfuscating the real destination in the Ukraine, rather than to ensure that the message fits the Twitter SMS format. However, multiple redirects are used to reduce the likelihood that a suspicious URL will be spotted immediately, as might happen when some sort of previewing has been used to check the real destination. Some shortening sites, such as TinyURL, offer a previewing facility whereby you are shown the real destination and have to confirm that you want to open it, while surl.co.uk actually *requires* you to view the real destination URL and confirm. An article by Joshua Long on How to Preview Shortened URLs (TinyURL, bit.ly, is.gd, and more) provides a great deal of information about shortening services that offer previewing, and even a Firefox add-in that does the same.

Shortened URLs are often a danger sign: the problem is that they can be and are used in many, many legitimate contexts, and redirects reduce the efficacy of previewing.

It is better that you ignore any tweet that contains only a URL, especially a goo.gl link, even from a trusted source: URLs without explanatory text are usually a danger sign in email, FB updates and such. Of course, the likelihood is that such messages will start appearing sooner rather than later with social engineering hooks like the "OMG, I can't believe..." scams so commonly seen on other social network sites (especially Facebook), and people will have to learn to be more discriminating and more cautious. It would, of course, also be helpful if people were a little less trusting when they use social media such as Twitter. (Why would you trust a tweet, *whoever* it's from, that only gives you a compressed URL?) It takes relatively few compromised accounts to cascade poisoned URLs, because people are so trusting when they see a tweet from someone they trust (compare the blight of survey scams and malware on Facebook).

Twitter provides a number of security-oriented links at http://support.twitter.com/groups/31-twitter-basics. And as you'd expect, Twitter has turned up in one context or another time after time on the ESET Threatblog.

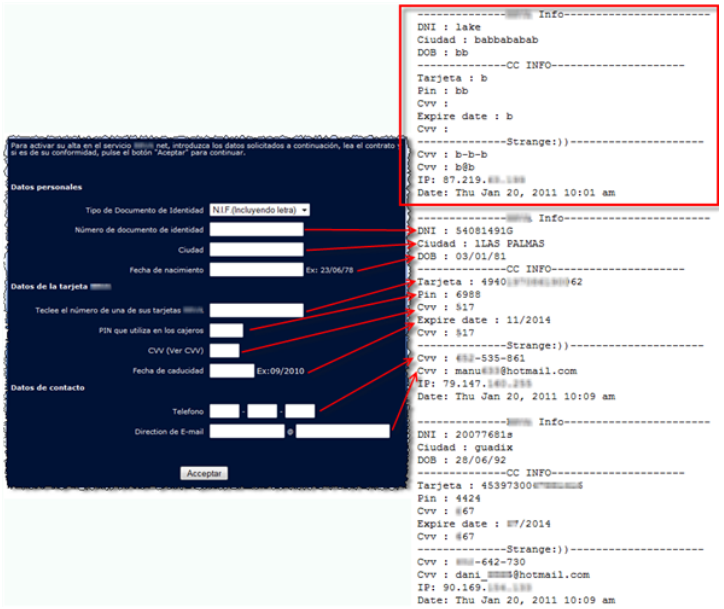
How effective are phishing attacks

ESET Latin America's Research team discovered a classic phishing attack for which they were able to investigate the effectiveness: **one out of every five people who accessed the malicious web site provided their sensitive data**.

The attack started with an email apparently from a famous Latin American bank:using classic social engineering techniques it lured the victim into clicking on and connecting to a web page where they were required to provide their bank account data.

Upon the analysis of the directories, it was found that the data files with the victim's information were recorded on the same phishing server. Analyzing the text file containing the data supplied by the victims, it was found that:

- The first access to the site was on January 20 at 10:01 pm (as illustrated below). The latest registered access was on the same date at 15:24 pm. Therefore, **the attack was active for just over five hours**.
- During those hours, 164 people accessed the phishing site, which indicates an average of about 30 people per hour; therefore, there is a potential victim every two minutes.
- Out of the 164 participants, 35 entered valid credit card data, which indicates an **effectiveness of 21%.**



Phishing attacks have grown steadily in recent years and, as it turnsout , have become a highly profitable attack for cyber criminals, with a high proportion of targeted victims falling for the scam.

More information on the ESET Threatblog: http://blog.eset.com/2011/01/26/inside-a-phishing-attack-35-credit-cards-in-5-hours

Merry-go-round: the AMTSO wheel of pain

The next AMTSO members meeting is at San Mateo, California, on the 10th and 11th February. As usual with the first AMTSO meeting of the year, it's arranged to dovetail conveniently with the RSA. There is more information (including the preliminary agenda) on the AMTSO meetings page at: http://www.amtso.org/meetings.html.

The Anti-Malware Testing Standards Organization (AMTSO) was founded in May 2008 as an international non-profit association that focuses on the addressing the global need for improvement in the objectivity, quality and relevance of anti-malware testing methodologies.

Reasonable and even laudable as those aims may sound to us (ESET participates actively and energetic in the organization's activities), AMTSO has unfortunately attracted a lot of negative publicity in the last year. It's understandable that some testers regard it as a threat, or at least as an attack on their competence, given that AMTSO does want to raise the general level of testing. Some also see it as an assault on their independence: that's perhaps understandable from magazines and organizations that are used to testing a whole range of consumer products. However, even a relatively complex object such as a digital SLR or a DTP package doesn't present the testing difficulties that a security product does, in terms of the complexity of the problems it addresses, and the corresponding methodological problems. While we understand the mistrust engendered by the common view of AMTSO as an anti-virus enclave rather than as a coalition between vendors and testers, the sad truth is that most of the technical expertise that sound testing requires lies between the ears of a few security researchers and even fewer professional testers.

However, some of the criticism has also arisen because of AMTSO's high membership fee (inevitable given its overheads, sadly). That, and the organization's emphasis on technical issues and expertise, has virtually excluded most people from direct participation in AMTSO discussions: hence the view that AMTSO is unacceptably elitist. ESET Research Fellow David Harley, who serves on the AMTSO Board of Director says: »I don't think that lack of representation invalidates the work that's been done by AMTSO over the past few years, but it seems unfortunate that the customer, who should be the main beneficiary of better testing, doesn't have more opportunity to participate. Indeed, it may be that the sting would have been taken out of some of the more widespread criticism if the complaints could have been voiced and addressed closer to home.

At the most recent AMTSO workshop (in Munich last autumn) the membership approved some positive steps towards giving the rest of the internet community more chance to participate in the debate: a subscriber model at a fraction of the cost of full membership, and a web forum. It's likely that some substantial gains will be made by the time of the workshop. Hopefully, they'll go some way to ensuring that the public is better able to evaluate the accuracy of the tests they rely on to make decisions on what security software to use.

The Top Ten Threats

1. Win32/Conficker

Previous Ranking: 2
Percentage Detected: 5.38%

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. 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.

2. INF/Autorun

Previous Ranking: 1
Percentage Detected: 5.30%

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.

3. Win32/PSW.OnLineGames

Previous Ranking: 3
Percentage Detected: 2.17%

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: 1.82%

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/Conficker

Previous Ranking: 5
Percentage Detected: 1.39%

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.

6. Win32/Bflient.K

Previous Ranking: 8
Percentage Detected: 1.19%

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.

7. Win32/Tifaut.C

Previous Ranking: 6
Percentage Detected: 1.09%

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.

8. HTML/ScrInject.B

Previous Ranking: 7
Percentage Detected: 0.84%

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.

9. Win32/Spy.Ursnif.A

Previous Ranking: 9
Percentage Detected: 0.83%

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. Java/TrojanDownloader.Agent.NCA

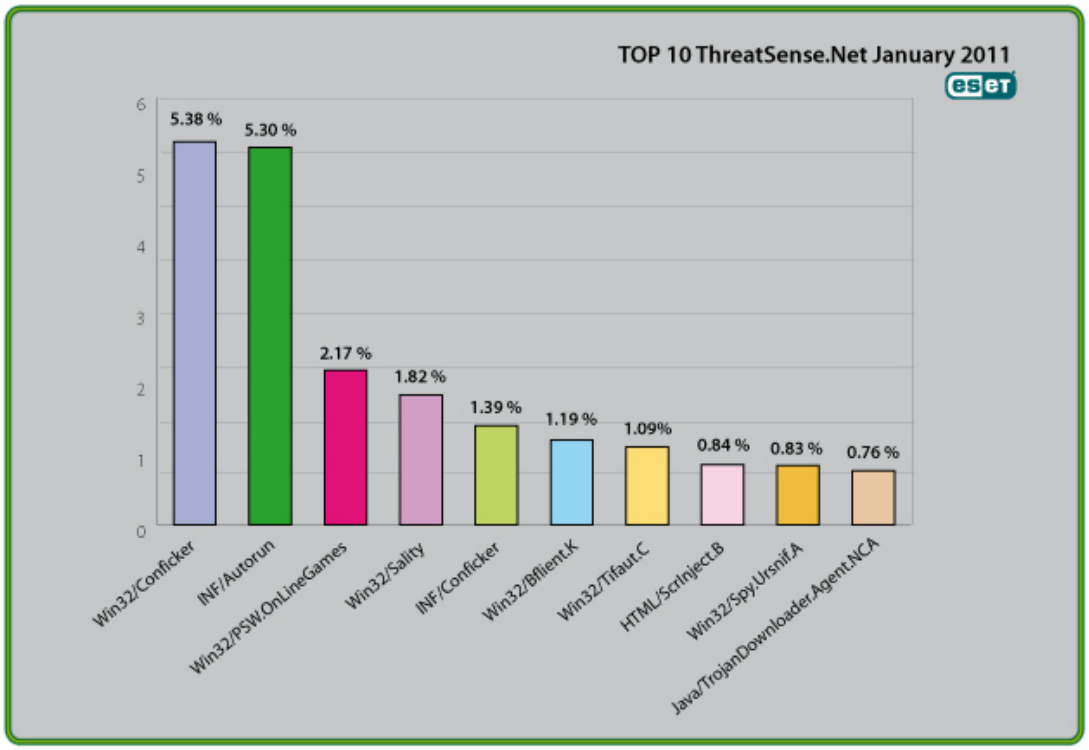
Previous Ranking: 7
Percentage Detected: 0.76%

Java/TrojanDownloader.Agent.NCA is a trojan which tries to download other malware from the Internet. It is written in Java and may be invoked when visiting a malicious website by referencing a malicious Java class file within a Java archive file (.JAR).

When the malicious .JAR archive is processed, the Java class component gets the URL of the file to download from the malicious website.

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 5.38% 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