October 2010

Feature Article: News from the cyber front

Table of Contents

Feature Article: News from the cyber front 3

Stuxnet 4

Securing our eCity Symposium 5

October: month of fakes 5

Virus Bulletin White Papers and others 6

AMTSO Workshop 7

The Top Ten Threats 7

About ESET 11

Additional resources 11

Feature Article: News from the cyber front

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

In principle it may appear that nothing much has changed on the cyber front. Attacks, exploits, botnets, fraud, scams, spam, they are all still there in varying quantities. But there does seem to be some specific change happening by comparisonwith previous years. It appears that the media have begun following global threat trends more consistently and more often, which is definitely good news, though most still prefer just to write about whichever virus is the latest sensation. Unfortunately, credit for this can be attributed less to experts' valiant and continuous efforts to raise awareness, than to the overwhelming growth and presence of cybercriminal activities, which it really isn't possible any longer to ignore. But the media are still mainly influenced by their own perception of the "newsworthiness" of specific topics, so here is a quick look at how certain cybersecurity topics have been covered recently.

Throughout this month Stuxnet has been all over the media, with varying levels of rationality in interpretation. Randy Abrams and David Harley could of course be counted upon for sensible explanations (http://blog.eset.com/2010/10/15/stuxnet-vulnerabilities-for-the-non-geek and http://blog.eset.com/2010/10/15/stuxnet-paper-revision), but multiple conspiracy theories also surfaced. The New York Times, for example, (http://www.cnbc.com/id/39435594) focused on biblical references within the malware's code and pointed the finger towards Israel's pursuance of cyberwarfare against Iran. But without getting into the technicalities of what Stuxnet is or isn't, the interesting part is how the media loved the Stuxnet story in general. It offers mystery (a.k.a. computer stuff, which no-one really understands anyway), international politics (Iran, China, etc...), it's a thriller (targeting nuclear facilities, according to many reports, though the actual target is, like nearly everything else, speculative) and if someone finds a romantic angle to it as well, we could legitimately expect to see a Hollywood blockbuster made soon. But while the media's attention was focused on this still-reverberating story, cybercriminals were, as usual, busy making money.

But, if there isn't any romance in Stuxnet (yet, or as far as we know...), there's plenty, complete with end-of-the-affair heartbreak, of course, in the many reported "Romance fraud" articles that have re-appeared every now and then over the past few years. The Times has been writing for a while on the whole subculture that developed among Ghana's youth, where, supposedly, 80% of the population aged 8-18 are involved with online fraud (http://bit.ly/c4hLxP). To a large extent this has to do with online dating fraud, assuming fake identities and scamming lovesick victims out of large sums of money (http://www.timesonline.co.uk/tol/news/uk/article7141462.ece). Randy Abrams reminded us of the email variation recently in She Loves You, Yeah, Yeah, Yeah (http://blog.eset.com/2010/10/20/scam-of-the-day-aka-she-loves-you-yeah-yeah-yeah). And while one may raise an eyebrow at sensationalist media exploitation of "the naïve lovesick woman who sent piles of money to a fraudster", perhaps it is just stories like these that instil a greater sense of vigilance into the community when it comes to all things online.

Likewise attention grabbing is the "Titanic shock syndrome" (unsinkable and such) with regard to media coverage of anything intended to destabilize systems other than Windows. While Microsoft-targeting malware is taken for granted, malware and exploits targeting other operating systems are still often reported as if the impossible has just happened. Imagine such a minor disturbance as described here (http://www.h-

online.com/security/news/item/Hole-in-Linux-kernel-provides-root-rights-1122180.html) regarding a problem in the Linux kernel making headlines if it had been in Windows.

And for the Believe it Or Not section come stories like the one about the cheekiness of the advertised Online Cybercrime Class (http://krebsonsecurity.com/2010/10/earn-a-diploma-from-scam-u/) which offers courses in fraud, scamming and using malware (and is clever enough not to accept credit cards as payment). Stories like these, which reveal how structured and organised the operations of cybercriminals are becoming, as well as directly demonstrating how profitable such activities can be, do seem to have some eye-catching value to the reader.

Overall, there has been progress made in the way cybersecurity is being reported. It's not just “hackers” and “viruses” any more, but proper distinctions and terminological differentiations are being observed, and more specialised topics regarding malware, vulnerabilities, security, etc are being discussed accordingly. It’s probably too much to hope that journalists will pay as much attention to serious, recurrent, but unglamorous topics as to topics that are more sensational but perhaps less important. Perhaps we can at least hope that journalists will pay more attention to expert reports and less to under-informed opinion makers. Perhaps this will happen more when sufficient damage has been done, whether it’s financial damage or some sort of SCADA disaster.

Stuxnet

Stuxnet is the malware of the year. Not only for its innovative malicious code and SCADA-targeting payload, but also for its success in infecting systems around the world. In response to the demand of our readers, we released last month a paper about the worm, after our researchers and laboratory worked together for a while poring over the code and other information and resources.

The result is a lengthy analysis that considers many questions around Stuxnet:

- Who was responsible for it?
- Was it really the work of a nation team rather than hackers?
- What exactly is its purpose?
- Is it really aimed at Iran?

About the second question, perhaps the one most heard around the world, our analysis of the code certainly indicates the participation of someone who knows SCADA, Siemens software, Programmable Logic Controllers and even SQL: not the skills we normally associate with the samurai (hackers for hire) that governments and certain military groups have often used in the past for cyber espionage. In fact, it's by no means unlikely that this malware project was put together by a team with a range of skills and backgrounds, not unlike the sort of multi-disciplinary tiger team that is often put together to *counter* attacks.

You can download the paper **“Stuxnet Under the Microscope”,** by Alexandr Matrosov, Eugene Rodionov, David Harley and Juraj Malcho. It is a comprehensive analysis of the Stuxnet phenomenon, including its recent history, distribution, implementation and implications. It was published at the end of September but has been updated to version 1.11 (at the time of writing) to include information that was held back pending the release of Microsoft patch MS10-73. As the story of Stuxnet evolves, the analysis is updated to reflect that evolution

Download the white paper:
http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

Securing our eCity Symposium

On October 7th, in San Diego, the second Securing Our eCity Symposium was conducted. More than 150 people discussed during the day the best ways in which to stay safe online. “Stop, think, connect”, was the new global message launched in the context of National Cyber Security Awareness Month, and is the first-ever coordinated message to help all digital citizens be safer and more secure online. The message was created by an unprecedented coalition of private companies, nonprofits and government organizations, in the same spirit as the original Securing Our eCity initiative.

This is the second symposium organized by Securing Our eCity, two years since ESET and San Diego Chamber of Commerce launched the program. Darin Andersen, Chief Operating Officer at ESET, told CNET News [1]: “*San Diego is the first community to implement the messaging in a complete awareness campaign*”.

Today, different cities are launching similar initiatives based on Securing Our eCity, in Buenos Aires, Malaysia and London.

Summarizing, in Darin Andersen’s words: “*This represents the power of people working at a local level to solve problems that have a big impact on many people*”.

[1] http://news.cnet.com/8301-27080_3-20019416-245.html

More information: http://securingourecity.org/

October: month of fakes

During October we have seen a number of different attacks based on a fake message taking the form of a Social Engineering attack. Firstly, we have become aware [1] of a scam where people are cold-called by a support desk where staffers claim Microsoft affiliation or accreditation. They tell the prospective victim that his or her PC is sending out SOS messages due to malware infection or system errors, and offering to fix the problem and, in many cases, install a "better" security program. The caller helpfully explains how to "confirm" the problem by using the Event Viewer to see how many errors and warnings it reports. Sadly, this always flags enough transient errors to frighten a victim into allowing the caller access to both their PC (using a legitimate remote access service) and their credit card details. We became aware of the problem because one of the companies concerned was claiming to install a version of one of ESET's products, and colleagues in the UK and Ireland have received a number of helpdesk calls from customers finding that it did not work.

This ESET’s scams weren’t the only ones during October. We also reported [2] about malware spreading with fake Adobe Updates, using emails headed as “ADOBE PDF READER SOFTWARE UPGRADE NOTIFICATION” and spammed from all over the world. Obviously, the update was a fake, and Adobe does not send emails like this to their customer, who could be infected if they click on the malicious links and don’t have antivirus software to protect them.

[1] http://www.computerweekly.com/Articles/2010/10/04/243165/Security-Zone-Faking-IT-support.htm

[2] http://blog.eset.com/2010/10/17/fake-adobe-updates-2

Virus Bulletin White Papers and others

During the Virus Bulletin Conference [1], in Vancouver, ESET's researches presented different papers in a variety of topics. By kind permission of Virus Bulletin, we published three white papers on our webpage [2]. Copyright for these three papers is held by Virus Bulletin Ltd, but is made available on our site for personal use free of charge:

- "**AV Testing Exposed**" by Peter Kosinár, Juraj Malcho, Richard Marko, and David Harley: considers the good, the bad, and the ugly in comparative testing, and explores how to lie (or even inadvertently mislead) with detection statistics. http://www.eset.com/resources/white-papers/Kosinar-etal-VB2010.pdf

- "**Call of the WildList: Last Orders for WildCore-Based Testing**?" by David Harley and K7's Andrew Lee: Does WildList testing still have a place in testing and certification when dynamic and whole product testing methodologies are now preferred in most testing contexts? http://www.eset.com/resources/white-papers/Harley-Lee-VB2010.pdf

- "**Large-Scale Malware Experiments: Why, How, And So What?**" by Joan Calvet, Jose M. Fernandez, Jean-Yves Marion and Pierre-Marc Bureau (from ESET): discusses how they replicated a botnet for experimental purposes, and what use they made of the results. http://www.eset.com/resources/white-papers/Large-Scale-Malware-Experiments.pdf

Also, we want to congratulate ESET researcher Pierre-Marc Bureau, for being voted by Virus Bulletin Conference delegates as the best newcomer to the the AV industry in the last ten years.

During October, we were featured in other articles and stories about information security, some of which are listed here:

- "**Stuxnet Sux or Stuxnet Success Story?**" by David Harley: Article for Security Week on the vulnerabilities and incident dispersion behind Stuxnet, perhaps 2010's most interesting malware. http://www.securityweek.com/stuxnet-sux-or-stuxnet-success-story

- "**Security Zone: Faking IT support**" by David Harley: An article for (ISC)2's regular column in Computer Weekly on the similarities between rogue AV and fake support scams. (See the item on "October: Month of Fakes" above.) http://www.computerweekly.com/Articles/2010/10/04/243165/Security-Zone-Faking-IT-support.htm

- "**SC Magazine interview: David Harley, senior research fellow at ESET**" is an article by: Dan Raywood of SC Magazine in which he interviewed ESET's David Harley, former manager of the Threat Assessment Centre in the United Kingdom's National Health Service, in conversation about security and the NHS. http://www.scmagazineuk.com/sc-magazine-interview-david-harley-senior-research-fellow-at-eset/article/181678/

[1]http://www.virusbtn.com/conference/vb2010/index

[2] http://www.eset.com/documentation/white-papers

AMTSO Workshop

ESET is heavily involved in the work of AMTSO (the Anti-Malware Testing Standards Organization). A frequent complaint about AMTSO is that it is in some sense elitist, not least because of the heavy membership fee (currently 2000 Euros per year). David Harley, who serves on the Board of Directors of AMTSO, tells us that at the recent AMTSO workshop in Munich, the member approved a new and much cheaper subscription model, which would give individuals and small enterprises much the same input into the activities of the organization as a full member, but without voting rights. There's much more information in the press release at http://www.amtso.org/pr-20101025-amtso-widens-the-conversation-of-anti-malware-testing-with-new-subscription-option.html.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.22%

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: 4.32%

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: 2.62%

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: 6
Percentage Detected: 1.90%

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: 4
Percentage Detected: 1.54%

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/Tifaut.C

Previous Ranking: 5
Percentage Detected: 1.42%

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.

7. HTML/ScrInject.B

Previous Ranking: 7
Percentage Detected: 1.31%

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.

8. Win32/Bflient.K

Previous Ranking: 30
Percentage Detected: 1.08%

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. JS/TrojanClicker.Agent.NAZ

Previous Ranking: 8
Percentage Detected: 0.71%

This malware is a Trojan horse that does not generate copies of itself, but is usually part of other malware.

It contains a list of web addresses to which to send requests, used to simulate clicking on advertisements for financial gain (click fraud).

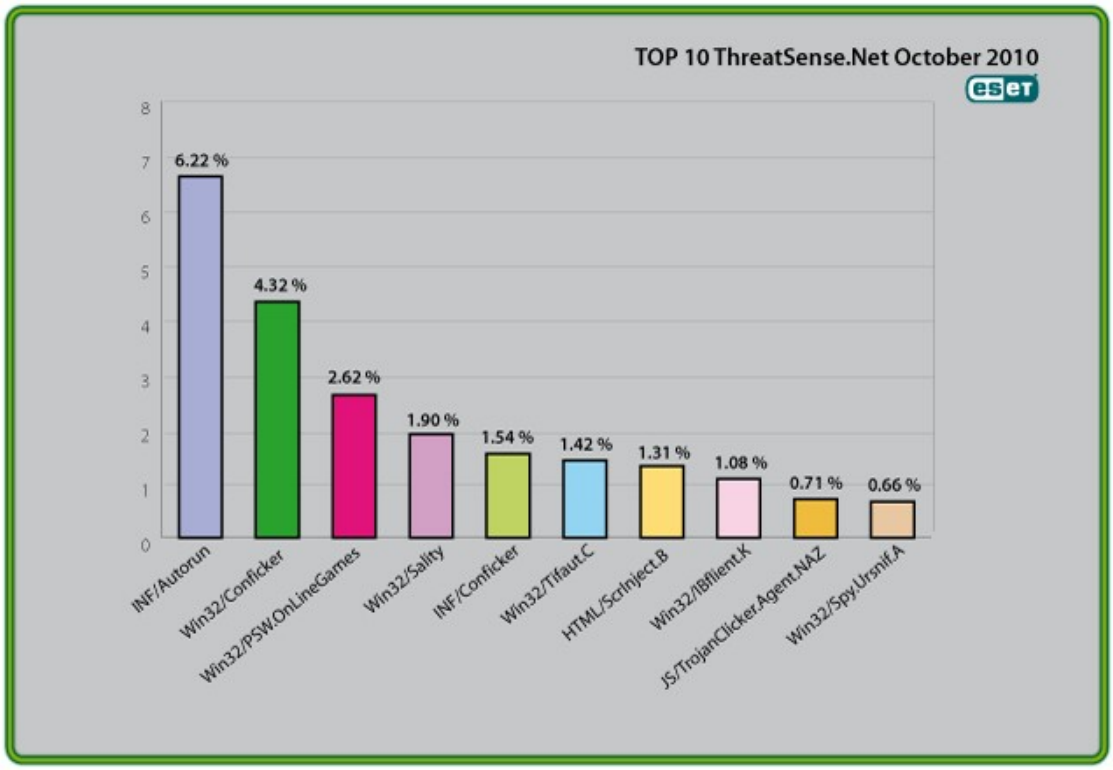
10. Win32/Spy.Ursnif.A

Previous Ranking: 9
Percentage Detected: 0.66%

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

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 6.22% 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