November 2013
Feature Article: It’s a Cyber Weapon, but is it Art?

ENJOY SAFER TECHNOLOGY™

Table of Contents

It's a Cyber Weapon, but is it Art?

David Harley CITP FBCS CISSP ESET Senior Research Fellow

Lars Holdhus contacted ESET's mother ship in Bratislava recently to tell us about his project to build a PDF on cyber weapons to be associated with an art exhibition in Vienna (the one in Austria that is), to be released on 22nd of November. He was particularly interested the Stuxnet Under the Microscope paper put together by Alexandr Matrosov, Eugene Rodionov, Juraj Malcho and myself, and approached us with a view to an email interview/conversation on the topic. He and I exchanged quite a few emails subsequently, and we thought that readers of this publication might find some excerpts from that conversation of interest, especially as the implications of the discussion go far beyond Stuxnet. Please note, though, that the content in the full interview very much represents my own opinions, and I was *not* speaking on behalf of ESET. The interview is part of the paper Dissolution (6edfsdf4c7e7) which also includes articles on Philosophy in a War-Zone by Nick Land, and Museum of Malware by John Menick.

You might think that all there is to say about Stuxnet has been said, but the recent report by Ralph Langner suggests that there are still aspects to consider. However the report came out after we concluded the interview.

Lars Holdhus: ***Stuxnet made us aware on how technology can be made use of in targeted attacks on infrastructure systems. What do you see as possible outcomes of attacks from malware similar to Stuxnet?***

David Harley: I agree that Stuxnet was something of a game-changer in terms of the public and media visibility it brought to the potential of infrastructural attacks. However, discussion of SCADA, ICS and infrastructure-related attacks (potential or actual) was already taking place among security and SCADA specialists when I became interested in the field, and obviously there have been attacks that haven't attracted the same level of interest.

- The Siberian pipeline explosion in 1982, is alleged to have been caused by a CIA logic bomb, but the truth of that story has been debated, while the Desert Storm printer virus is usually held to have been a hoax.

- Byzantine Candor from 2002 onward, targeting military and government agencies in the US.

- Ghostnet, 2007 onward. Multiple targets, including India's embassy in the US and the offices of the Tibetan government in exile.

- Aurora. Targeted Chinese human rights activists and some big players in the US technology industries, notably Google. Proprietary code stolen, activist emails compromised.

- Shadows in the Cloud, 2009 onwards: Targeted Indian and Tibetan government offices and the United Nations. Sensitive correspondence and documents compromised. [Note that targeted attacks on Tibetan and other activists continue to this day: in fact, they're the main thrust in OS X–targeting malware currently.]

- Night Dragon attacks on petrochemical companies like Exxon, Shell and BP.

- Attacks reportedly from Russia on Estonia and Georgia, targeting a range of web sites including government, media and finance organizations.

- Titan Rain: alleged theft of military Intel by China (Lockheed, NASA, Sandia)

- Moonlight Maze: also targeted military intel, allegedly, by Russia (Pentagon, NASA, Dept of Energy, research labs)

While there are indeed 'similar' attacks – Flame, Duqu etc., plus the otherwise unrelated malware like Chymine and some Sality variants that seized upon vulnerabilities that Stuxnet was the first to exploit – Stuxnet represented a somewhat unusual confluence of factors:

- A target specific and 'desirable enough to attract the necessary resources for what seems to have been a massive collaborative effort.

- A highly specific payload requiring highly specialized knowledge both to build and to get to the bottom of when the malware finally tripped alarms in the anti-malware industry.

- The availability of several unknown zero-day vulnerabilities (and the capacity for seeking them out).

- The availability of a parallel and hard-to-fix weakness in the Siemens ICS environment. Not only did the backdoor apparently require serious re-engineering by Siemens, but ICS-targeting malware almost by definition presents operational difficulties in addressing on site even where patches and updates are readily available.

- Targeting a region where political considerations militate against the strict observance of licensing requirements for software from outside the region. This creates an environment somewhat isolated from the mainstream communication channels between vendor and client software, and it's interesting to speculate on how much longer the malware might have remained under the radar if it had not also been picked up in regions that weren't affected (or less affected) by export/import restrictions.

- Use of stolen certificates at a time when malware was far less likely to take that approach, which wasn't particularly taken into account by some security products at that time.

I'm by no means saying that such a combination of factors can never occur again. In fact, if there's one thing that has become very clear over the past few months, it's that governments can always find resources to spend on cyber-espionage at home and abroad: while there is far less discussion of cyber-sabotage and other facets of what many people insist on calling cyberwarfare, it would be naïve to think that the kind of resources that seem to have been thrown at Iran's nuclear industry couldn't be found for other targets.

In fact, while some of the speculation about how modified Stuxnet code could perform all manner of attacks on police telephone networks, hospital systems and so on were close to fantasy, there's no doubt that it did demonstrate how successful a targeted or semi-targeted attack can actually be given a sufficiency of resources and research, and a similar

'tiger team' approach to quite different targets could probably be as effective. It's not only security researchers who learn from experience and evolve into other techniques.

Criminal and nation-state funded malware developers have generally moved away from the use of self-replicating malware towards Trojans spread by other means (spammed URLs, PDFs and Microsoft Office documents compromised with 0-day exploits, and so on). Truly targeted non-replicating malware (aimed at individuals, often using customized social engineering as well as customized code) is much harder to catch. This was so before Stuxnet, of course, but the Stuxnet family's perceived success has certainly had an influence in the take-up of similar stealth techniques by other state-sponsored malware. It's also had knock-on effects in terms of the take-up of technologies that are seen as more effective than conventional anti-virus in countering highly-targeted malware.

LH: Earlier you mentioned that there are several facets of what people refer to as cyber warfare. Could you give some examples of different facets of cyber warfare?

To be honest, I don't think we're seeing real cyberwarfare. Maybe some rough equivalent of the Cold War... It seems to me that the term has been applied indiscriminately to a range of activities whose non-cyber equivalents aren't considered *only* to take place during wartime. Not only sabotage, but surveillance, subversion and espionage, terrorism and even civil espionage and cybercrime. While there is an abundance of incidents that suggest all too many politically-motivated conflicts, I'm not convinced that these add up to a form of all-out malware. It could also be argued that governments have muddied the waters by using the label to cover this range of activities in the hope of making them more palatable to populations increasingly worried about erosion of civil liberties and individual privacy.

LH: That's an interesting take on the term Cyberwar. As technology gets more complex and malware follows the same direction it seems that only a few individuals can follow this development. How can an individual citizen protect him/herself from government funded malware?

DH: Well, to paraphrase Bruce Schneier, if a heavily-sponsored intelligence agency wants access to your system and your secrets, it will get it (unless you happen to be an equally well-resourced and unusually well-protected organization, maybe). If surveillance on major corporations and government agencies is so widespread and so easy, what chance do individuals with limited resources have? Well, they do have the advantage of not generally being of interest to government agencies and therefore not specifically targeted for 'official' policeware or government spyware. As opposed to more generic malware, which – even if it isn't put out in massive spam campaigns – isn't highly targeted either: the bad guys are just hoping to reach vulnerable people or systems. Much top-level government-sponsored surveillance is also more-or-less untargeted, but is the starting point for finding more specific targets.

That doesn't mean that certain agencies don't have their data and/or metadata, because they almost certainly do. However, they're only going to examine data closely that trips alarms, such as certain keywords in metadata, or the suspicion of unusually strong encryption. Not that I'd want to dissuade home users from using better encryption than most of them do, but they can't assume that encryption will keep all their secrets safe. I doubt if using something like PGP would in itself raise a big red flag, but in combination with other 'suspicious' indicators might indeed attract attention.

Using industrial strength security programs isn't likely to do any harm, and we do know that some state-sponsored malware is caught by anti-malware simply because it has suspicious characteristics, even if we don't always know that it originates from an 'official' source.

There are other obvious mitigations like keeping operating systems and applications properly patched. And trying to be resistant to all manner of social engineering, though that's infinitely easier to say than to achieve.

Chronology of a Skype attack

By the middle of May, users around the world started to receive messages from their contacts through different instant-messaging applications, such as Skype and Gtalk. With respect to malware propagation, there is a life cycle from one campaign carried out by the attacker to the next. When the volume of potential victims who receive the same threat through the same propagation channel over a short time period rises over a certain threshold, we can see chain reactions that exceed the attacker's target and start to reach people outside the group of users who were chosen as possible victims. Many of these factors came together on May 20th, when, as well as notifications from the ESET Early Warning System, we got queries from affected computer users and even received messages from contacts that members of the ESET Latin America's Laboratory had associated with their Skype accounts. This threat was detected by ESET Smart Security as a variant of Win32/Kryptik.BBKB, and it managed to lure more than 300,000 users into clicking on the messages and unexpectedly downloading the threat. You can read more on the Chronology of a Skype attack in a dedicated blog post or white paper on WeLiveSecuirty.com.

ESET Corporate News

ESET Ranked by Deloitte as One of the Fastest Growing Technology Companies in Central Europe

ESET appeared in Deloitte's 14th annual ranking of Central Europe's fifty fastest-growing technology companies (Deloitte 2013 Technology Fast 50 Central Europe). The ranking is prepared based on the companies' five-year revenue growth. ESET also dominated Central Europe's Big 5 subcategory, in which it ranked fourth.

ESET Launched New Security Packs

ESET announced the availability of ESET® Multi-Device Security Pack. It enables home customers to enjoy their device with award-winning Internet Security on various platforms. Similarly, ESET® Home Office Security Pack and ESET® Small Business Security Pack do the same for business, in addition to easy administration, company device licensing and maintenance. The Packs include multiple ESET products to provide comprehensive proactive protection across multiple operating systems and endpoints in both home and professional settings.

ClevX DriveSecurity™ in Kingston USB Powered by ESET

ESET partnered with Kingston on their latest Kingston Digital USB flash drives DataTraveler Vault Privacy 3.0 Anti-Virus with ClevX DriveSecurity™ powered by ESET.

ESET Examines the Security of the New and Improved Windows 8.1

Aryeh Goretsky, ESET Distinguished Researcher, reviewed the

security of the latest version of Microsoft® operating system Windows 8.1 that comes up with some under-the-hood improvements. The white paper, 'Windows 8.1 Security – New and Improved', that reviews some of the most anticipated—and controversial—security features of this new ".1" point release of Windows 8, also looks at the adoption rate for Windows 8 and 8.1, discusses new risks introduced by Windows 8.1, and looks at whether or not IT shops and users should upgrade. It can be downloaded from WeLiveSecurity.com White Papers section (in landscape formatting).

ESET Partners with MobiFone to protect their 30 million Subscribers

ESET announced a new partnership deal with MobiFone, one of the largest telecom company in Vietnam. According to this deal that was signed with the support of our partner company in the country, ESET products (ESET NOD32® Antivirus and ESET® Mobile Security for Android) will be sold to MobiFone customers on a monthly subscription model.

Chronology of a Skype attack

By the middle of May, users around the world started to receive messages from their contacts through different instant-messaging applications, such as Skype and Gtalk. With respect to malware propagation, there is a life cycle from one campaign carried out by the attacker to the next. When the volume of potential victims who receive the same threat through the same propagation channel over a short time period rises over a certain threshold, we can see chain reactions that exceed the attacker's target and start to reach people outside the group of users who were chosen as possible victims. Many of these factors came together on May 20th, when, as well as notifications from the ESET Early Warning System, we got queries from affected computer users and even received messages from contacts that members of the ESET Latin America's Laboratory had associated with their Skype accounts. This threat was detected by ESET Smart Security as a variant of Win32/Kryptik.BBKB, and it managed to lure more than 300,000 users into clicking on the messages and unexpectedly downloading the threat. You can read more on the Chronology of a Skype attack in a dedicated blog post or white paper on WeLiveSecuirty.com.

ESET Honored with the 'Manufacturer of the Year 2013' Award in Germany

ESET was honored with the 'Hersteller des Jares 2013' Award (Manufacturer of the Year 2013) by CRN, a renowned professional magazine for ICT sector retailers in Germany in the category of IT security. The finalists included three best scoring companies, from which ESET ranked second.

ESET Go Explore Dropion Reaches Stratosphere in Unique Social Gaming Experiment

ESET has launched a gondola called Dropion into the stratosphere. For this unique social gaming experiment called Stratocaching, ESET partnered with a group of young technology enthusiasts from Czech "No Rocket Science" and Technet.cz.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1

Percentage Detected: 3.68%

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.

2. LNK/Agent.AK

Previous Ranking: n/a

Percentage Detected: 2.11%

LNK/Agent.AK is a link that concatenates commands to run the real or legitimate application/folder and, additionaly runs the threat in the background. It could become the new version of the autorun.inf threat. This vulnerability was known as Stuxnet was discovered, as it was one of four that threat vulnerabilities executed.

3. Win32/Sality

Previous Ranking: 3
Percentage Detected: 1.95%

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

4. INF/Autorun

Previous Ranking: 2
Percentage Detected: 1.94%

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.

5. HTML/ScrInject

Previous Ranking: 5
Percentage Detected: 1.62%

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

6. Win32/Dorkbot

Previous Ranking: 6
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.

7. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.47%

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.

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.

8. HTML/Iframe

Previous Ranking: 4

Percentage Detected: 1.43%

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.

9. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.37%

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.

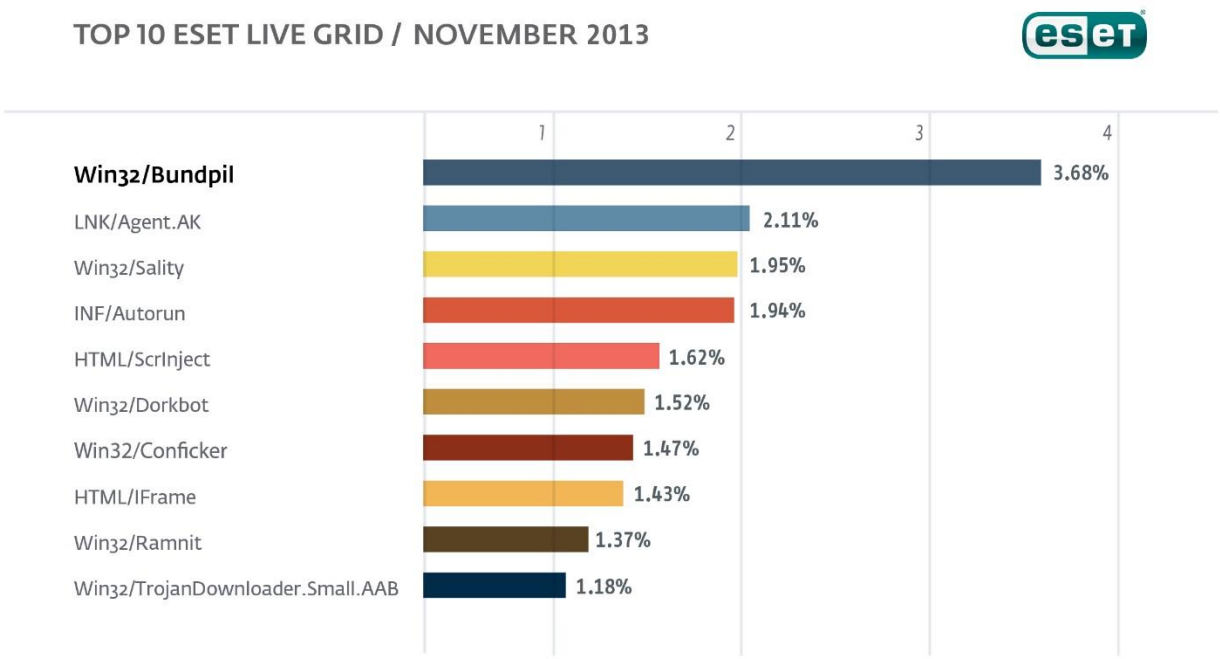
10. Win32/TrojanDownloader.Small.AAB

Previous Ranking: 9
Percentage Detected: 1.18 %

Win32/TrojanDownloader.Small.AAB is a trojan which tries to download other malware from the Internet. When executed, it copies itself into the %temp%\hcbnaf.exe location. The trojan contains a URL address, and it tries to download a file from the address.

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 3.68% of the total, was scored by the Win32/Bundpil 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