# Threat Radar

## May 2014

## Feature Article: CSO So-So So-and-So

ESET ENJOY SAFER TECHNOLOGY™

# Table of Contents

# CSO So-So So-and-So

**David Harley, ESET Senior Research Fellow ESET North America**

**Small Blue-Green World**

I was recently approached to provide commentary for Information Age on the roles of the CSO (Chief Executive Officer) and CISO (Chief Information Security Officer). I don't know if they've used or will use any of it but I'm sure they won't have used it all, so here are some of the questions I was asked and my responses. I haven't worked in areas where I could regard myself as any sort of executive for quite a while, so this is more from the security geek perspective than from the MBA end of the telescope. (No, I don't have an MBA!)

1. What has changed about the job description of the CSO in 2014 compared to recent years? What factors and trends have contributed to this?

C-level security has moved well away from the 'promote-a-geek' culture of a few years ago. In part, this is due to a gradual realization that the tension between security best practice and the need for business processes to have room to breathe is best addressed by management – hybrid management, if you like – with understanding of technical security *and* business processes and infrastructure. One of the main drivers for this change has been the need to conform with a range of standards and legislation that require quite different skills to systems security and administration. The waters have been muddied further in the past year or so as the lines between criminal and state activity, especially with regard to privacy, have become more blurred. Or rather, as recognition of that longstanding blurriness has increased.

2. How prevalent is the CISO (Chief Information Security Officer) role becoming as a distinct role? Will it become more or less common and why? What does this role now encompass?

To me, the main reason to distinguish between CISO and CSO is to emphasise that the latter has responsibility for physical as well as digital security. Regardless of actual job titles, it would seem reasonable to me, with the blurring of distinctions between physical and digital security, to have one person with overall responsibility for security of all flavours. Given the complexity of IT in general, it may make sense in some organizations to have someone with specialist skills (executive, not necessarily hands-on technical) to work specifically in the information security domain. Whether they would work *with* or report *to* the CSO (or equivalent job-title) would probably depend on individuals and organizations. I wouldn't care to formulate an inflexible one-fits-all ruling on that.

3. Is it right that physical and digital security should be merged under one organisational umbrella or should they be kept separate?

It's not really feasible to keep physical and digital security totally isolated from each other. While I'm not going to evangelize on its behalf, (ISC) has recognized that fact for many years, in that physical security is specified as one of the key domains with which CISSP candidates are required to demonstrate knowledge and experience in order to achieve certification, and that's the kind of certification I'd expect to see widely used as one criterion for evaluating a candidate's suitability for a C-level security role. CISSP leans more to the management end of the spectrum than the technical end, and that knowledge is expected to be broad rather than deep, but many would consider that the right end of the spectrum for a C-level officer.

I can remember a time, though, when people whose main responsibility was for physical security were often deemed de facto experts on digital security. Without in any way meaning to understate the importance and complexity of physical infrastructure – especially as more and more physical security becomes reliant on digital technology – that assumption of de facto expertise doesn't cut it anymore. That organizational umbrella needs to be carried by someone who has good knowledge of the physical domain and of digital security.

4. How is the role of the CSO evolving in relation to the C-suite?

Security implementation is usually some way removed from the Board, though in recent years it's become much more common for the company's security 'vision' to be championed on the Board of Directors by a Chief Security Officer. The important thing is to ensure that there is someone who is not only informed enough to fill that role adequately, by virtue of being able to see both ends of the technical<->executive spectrum, but has the authority to ensure that his or her voice is heard and heeded at Board level.

5. What skills and qualities should companies be looking for in a CSO going forward? Is the next generation entering/about to enter the workforce going to be equipped for the role? Is the skillset broadening or narrowing?

Even at CSO level, *Spaf's First Principle of Security Administration still applies: "If you have responsibility for security, but have no authority to set rules or publish violators, your own role in the organisation is to take the blame when something big goes wrong."

In large organisations, it's unlikely that a CSO will be hands-on when it comes to security administration, but needs to be able to marshal convincing arguments for effective security strategies, which seldom come cheap. So you might say the view broadens as the candidate ascends towards the top of the tree. So the set of issues he needs to have some understanding of will broaden too. As will the range of skills of those he supervises.

*That's Professor Eugene Spafford, of CERIAS/Purdue University

6. How should the CSO be a security 'evangelist' fostering security in the wider enterprise amongst employees and external partners and customers?

Up to a point, any C-level manager should be fostering security internally and externally, not least by acknowledging that they need to observe even inconvenient security measures themselves. However, anyone at that level with the word 'security' in their job title should be fully aware of the need to enforce awareness through education, standards, policies and so on.

# ESET Corporate News

## ESET signs exclusive agreement with Ingram Micro to offer comprehensive Endpoint Security Solutions for business

ESET announced a strategic and exclusive distribution alliance with Ingram Micro Inc. (NYSE: IM), the world's largest technology distributor. Ingram Micro will provide U.S. channel partners with quick and efficient access to ESET's full suite of award-winning business solutions to meet growing demand across industry sectors.

The new alliance with Ingram Micro enables ESET to offer a combination of products and services, along with an attractive volume incentive program, increased flexibility for resellers in securing credit, and a facilitated process for securing quotes and placing orders.

## Newest ESET Mobile Security Comes With Proactive Anti-Theft

ESET announced its newest version of ESET Mobile Security, which arms Android™ users with proactive Anti-Theft features to track lost or stolen mobile devices, through an easy-to-use web interface at my.eset.com. While the basic protection is free for a lifetime, it's up to users to decide if they want to subscribe and benefit from Premium features.

Proactive Anti-Theft detects potentially dangerous situations and takes preventative steps to ease the localization of a stolen or lost device. The new functionality for Premium users sends the last location of the device when the battery hits critical level, takes snapshots from front and back camera when the wrong PIN/pattern is entered or an unauthorized SIM change is detected. All data on the device is accessible via the my.eset.com web interface.

ESET Mobile Security provides a set of strong security features improving the Android experience without worrying about cyber threats and comes in free and premium versions. The free version of the application provides basic protection including full device scan, scan of downloaded applications items and basic Anti-Theft functionalities. All Premium features are unlocked after activation of the 30-day trial or buying the license. In the premium version users will find Scheduled Scanning, On-Charger Scan, advanced Proactive Anti-Theft functionalities, including my.eset.com integration, SMS & Call Filter and Security Audit.

# The Top Ten Threats

## 1. Win32/Bundpil

**Previous Ranking: 1**
**Percentage Detected: 2.99%**

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: 2**
**Percentage Detected: 1.87%**

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: 1.56%**

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. HTML/ScrInject

**Previous Ranking: 4**
**Percentage Detected: 1.49%**

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

## 5. INF/Autorun

**Previous Ranking: 5**
**Percentage Detected: 1.47%**

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.

## 6. Win32/Qhost

**Previous Ranking: 6**
**Percentage Detected: 1.37%**

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.

## 7. Win32/Conficker

**Previous Ranking: 7**
**Percentage Detected: 1.22%**

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 treat 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. Win32/Ramnit

**Previous Ranking: 8**
**Percentage Detected: 1.19%**

It is a File infector 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.

## 9. Win32/TrojanDownloader.Waski

**Previous Ranking: 9**
**Percentage Detected: 1.12%**

Win32/TrojanDownloader.Waski is a trojan which tries to download other malware from the Internet. It contains a list of two URLs and tries to download a file from the addresses. The HTTP protocol is used. The file is stored in the location %temp%\miy.exe, and is then executed.

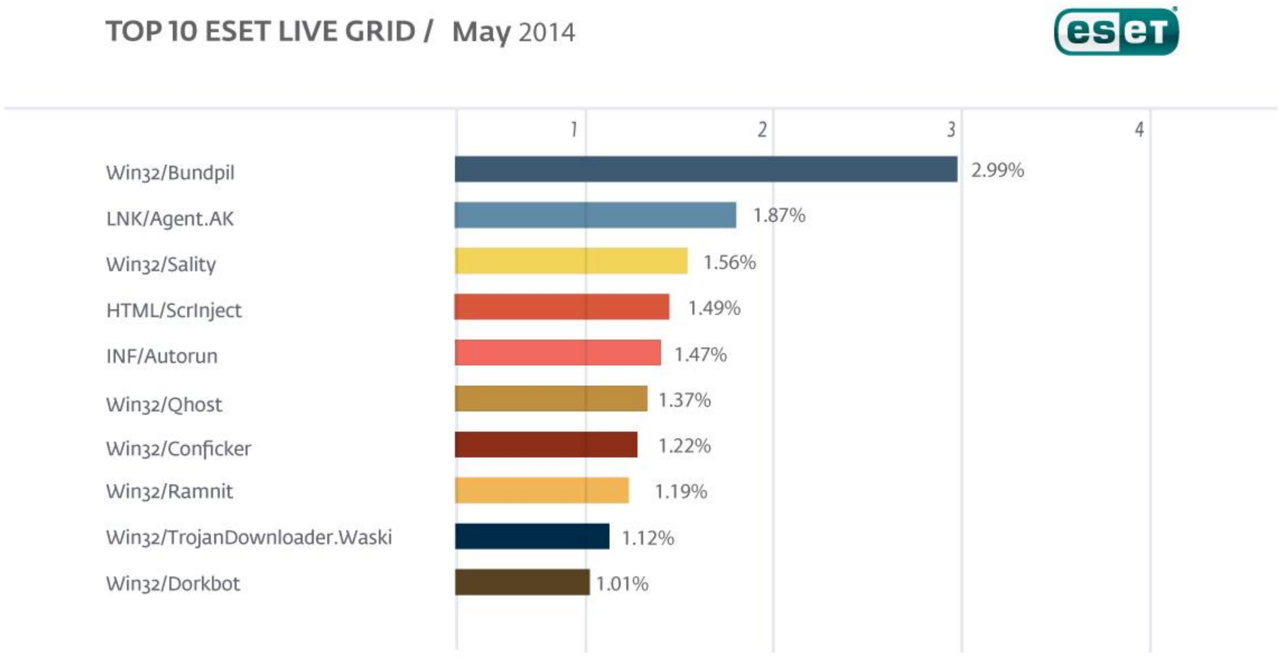
## 10. Win32/Dorkbot

**Previous Ranking: 10**
**Percentage Detected: 1.01%**

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.

# 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 2.99% of the total, was scored by the Win32/Bundpil class of treat.


TOP 10 ESET LIVE GRID / May 2014

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