August 2014
Feature Article: Can the Can (or Arbitrage Outrage)

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Can the Can (or Arbitrage Outrage) 3
Don't Hack the Site, Hack the Human 4
ESET Corporate News 6
The Top Ten Threats 7
Top Ten Threats at a Glance (graph) 10
About ESET 11
Additional Resources 11

Can the Can (or Arbitrage Outrage)

David Harley, ESET Senior Research Fellow ESET North America

Small Blue-Green World

[A shorter version of this article was originally published on the Dataholics blog.]

Mostly I ignore spam - I just see too much of it. Occasionally I write about it, especially if it's technically interesting or a fraud potentially effective enough to deserve a warning to the community. (To some extent, of course, all spam - as opposed to junk mail - is fraudulent.)

This is something slightly different, from my own mailbox. I won't try your patience with the whole email, but Sahil claims to be representing a software development company based in India and specializing in iPhone apps, Android apps and web development.

It isn't a phishing scam, though I'm not convinced it's from a legitimate business, since there are no address details and it comes from a Gmail address. But it is amusing. At least, this bit is:

"We also offer cost arbitrage opportunity wherein we can your backend arm and help you save your delivery cost."

I can't think why they think I'd be attracted by an offer to 'can my backend arm'. (Now that's a mental image I'd quite like to unsee.).

The invitation to unsubscribe is mildly amusing, too:

"Note: - Though this is not an automated email, we keep on sending out these emails to all those people whom we find eligible of using our services. To unsubscribe from future mails (i.e., to ensure that we do not contact you again for this matter), please send a blank mail, with NO as the Subject."

Apparently I'm 'eligible' because I have a blog site and can therefore expect to be besieged by unsolicited offers to improve it.

It's long been security mantra that you shouldn't respond to spam by unsubscribing, as it confirms to the spammer that he has a 'live one'. I'm not convinced that it makes much difference: it doesn't usually incur any penalty to the scammer to keep mailing a dead address. So I've taken to trying out the unsubscribe option in some cases, then storing the message to see whether and how they respond, how soon they re-spam, and so on.

Which is why I know, for instance that there are several companies (closely related, judging by the extraordinary similarities between their messages) who persistently send me marketing emails, and who either don't honour unsubscribe requests or are very bad at maintaining unsubscribe lists. What they usually offer is a list of users of various software: the spam I get usually offers lists of users of anti-virus software from ESET's competitors, but sometimes the choice seems totally arbitrary. (Why would I be interested in a list of SAP users, even if I was in the business of chasing marketing leads?!)

Here's an example of the kind of data they claim to offer:

Company, Name, First Name, Last Name, Title, HQ Phone, Direct No, Email, Address1, Address2, City, State, Zip, Country, Industry, Revenue, Employees, IT Budget, IT Employees, Website, Technology, Company HQ Address1, Company HQ Address2, Company HQ City, Company HQ State, Company HQ Zip, Company HQ Country and LinkedIn link.

Are they legally entitled to offer stuff like this? Well, sometimes they tell me so, stating (for instance) that they are in compliance with the CAN SPAM Act, 2003. But then they also claim that they respect my privacy and will stop contacting me if I jump through the appropriate hoop. As they haven't yet, I'm not inclined to take it for granted that they are telling the truth about compliance, or the accuracy of their data. (Not that information of this sort would be of the slightest use to me anyway.)

Of course, there are many companies that do honour unsubscribe requests. Especially the ones to which I knowingly subscribed in the first place. And it is legitimate, in some circumstances, for companies to send unsolicited mail. I sometimes wish it wasn't, but I can live with it when they offer (and honour) an unsubscribe option.

Don't Hack the Site, Hack the Human

Urban Schrott and David Harley

My colleague at ESET Ireland, Urban Shrott, has flagged quite a few recent phishing scams in the article [How to hack someone's account? Ask them for their password!]

As the article is quite long, I've shortened it for this report, mostly by leaving out the actual emails, but there's a link to the graphic here in each case. Or, of course, you could just go direct to Urban's blog. ☺

DH

ESET Ireland has been following a surge of phishing emails redirecting users to faked banking, PayPal and Microsoft account sites for harvesting login details.

Although a surprisingly large number of people still use passwords like "12345" or "password" for their various accounts, cybercriminals have taken an easier route than trying to hack into peoples' accounts. "Ask and you shall receive" seems to be their motto, so they send out emails that pretend to be coming from legitimate sites, notify the user of some unusual activity, and ask them to confirm or deny that activity by "signing into the service". Except that the service in question isn't actually there, but a faked site instead, which diligently logs all usernames and passwords entered and delivers them to the happy scammers.

In the past weeks, ESET Ireland has received several different emails of the same nature, and here are some examples:

1. Bank of Ireland

An email purporting to come from Bank of Ireland, claiming your account requires an update and providing a fake link *"Click here to complete update"*. The email has some bad spelling errors which give it away.

https://esetireland.files.wordpress.com/2014/07/bank.jpg

2. iTunes

An email pretending to be from iTunes, thanking you for purchasing "World Of Go" for €9.65 , then adding *"If you did not authorize this purchase, please visit the iTunes Payment Cancellation Form within the next 12 hours in order to cancel the payment,"* which requires you to "log in" to the fake iTunes site.

https://esetireland.files.wordpress.com/2014/07/itunes.jpg

3. PayPal

An email looking like a detailed payment receipt, mimicking PayPal, with all the usual PayPal visual clues, claiming you paid $208.00 USD to Agoda Company online hotel booking site, adding *"If you haven't authorized this charge, click the link below to dispute transaction and get full refund – Dispute transaction (Encrypted Link)."* The link, of course, isn't encrypted and simply leads to a PayPal lookalike login harvesting site.

- https://esetireland.files.wordpress.com/2014/07/paypal1.jpg
- https://esetireland.files.wordpress.com/2014/07/paypal21.jpg

4. Microsoft

An email abusing Microsoft's name, with the subject line "Microsoft account unusual sign-in activity" that claims they detected unusual sign-in activity into your account, supposedly from South Africa, which is meant to make people suspicious, then offering a solution *"If you're not sure this was you, a malicious user might have your password. Please Verify Your Account and we'll help you take corrective action."* Of course the only action they'll be taking is signing into your account with the login details you just provided.

- https://esetireland.files.wordpress.com/2014/07/ms12.jpg
- https://esetireland.files.wordpress.com/2014/07/ms22.jpg
- https://esetireland.files.wordpress.com/2014/07/ms3.jpg

What should you do?

First of all, stay informed. The scams you know about are less likely to catch you off guard. We regularly keep you updated on our blog here or on ESET's We Live Security.

Read such mails carefully, checking for clues. If the email had spelling errors or used poor language it is likely faked. A lot of the scammers come from countries where English is not their first language and they give themselves away. Also goes for similar scams as Gaeilge, where they likely used Google translate to try to fool native Irish speakers.

Do not click on links in emails. Even if you do have a Microsoft account and are alarmed by such an email, open your browser and go to Microsoft site directly. Also make sure the website's address looks correct. In the case of the faked Microsoft one above, the website address read "yazarlarparlamentosu.org", which is clearly not "Microsoft"

If you suspect you may have fallen for one of these tricks, change your passwords. To be sure, change them in regular intervals anyway.

If the email you received looks like it's coming from your bank, pick up the phone and ring them instead of just clicking. They're accustomed to scams like these and will advise you appropriately.

Think before you click and enjoy safer technology!

ESET Corporate News

ESET launches Beta version of ESET NOD32 Antivirus and ESET Smart Security

In ESET we are always working to improve the protection we provide, either through new solutions or improvements in our platforms and technology, in order to protect our users against new threats that appear every day.

In this regard, we are pleased to announce that we have launched the Beta of the new version of our popular home solutions: ESET Smart Security and ESET NOD32 Antivirus.

Among the new features, we can highlight the inclusion of a technology that will protect from botnets, an Exploit Blocker module and improvements in the rest of the functionalities already present in the products.

ESET Latin America celebrates 10 years!

During July and August, ESET Latin America office celebrated their 10th anniversary in the region.

What began as a challenge and a commitment of the Global Office in the region, a decade later, is now fully a reality. The company that Ignacio Sbampato and a small team began back in 2004 in Buenos Aires, Argentina, was transformed into a modern workplace of nearly 70 people with offices in Mexico and Brazil.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 2.18%

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. JS/Kryptik.I

Previous Ranking: 2
Percentage Detected: 1.83%

JS/Kryptik is a generic detection of malicious obfuscated JavaScript code embedded in HTML pages; it usually redirects the browser to a malicious URL or implements a specific exploit.

3. Win32/Adware.MultiPlug

Previous Ranking: 7
Percentage Detected: 1.53%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it's present into the users system might cause applications to displays advertising popup windows during internet browsing.

4. Win32/RiskWare.NetFilter

Previous Ranking: 3
Percentage Detected: 1.46%

Win32/RiskWare.NetFilter is an application that includes malicious code designed to force infeted computers to engage in unwanted behaviour. It allows an attacker to remotely connect to the infected system and control it in order to steal sensitive information or install other malware.

5. LNK/Agent.AK

Previous Ranking: 4
Percentage Detected: 1.4%

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.

6. Win32/Sality

Previous Ranking: 5
Percentage Detected: 1.38%

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

7. INF/Autorun

Previous Ranking: 8
Percentage Detected: 1.2%

INF/Autorun is generic detection of the AUTORUN.INF configuration file created by malware. The AUTORUN.INF file contains the path to the malware executable. This file is usually dropped into the root folder of available drives in an attempt to autorun a malware executable when the infected drive is mounted. The AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes present in attempt to hide the file in Windows Explorer

8. HTML/ScrInject

Previous Ranking: 6
Percentage Detected: 1.13%

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

9. Win32/Ramnit

Previous Ranking: n/a
Percentage Detected: 1.1%

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.

10. Win32/Conficker

Previous Ranking: 9
Percentage Detected: 1.08%

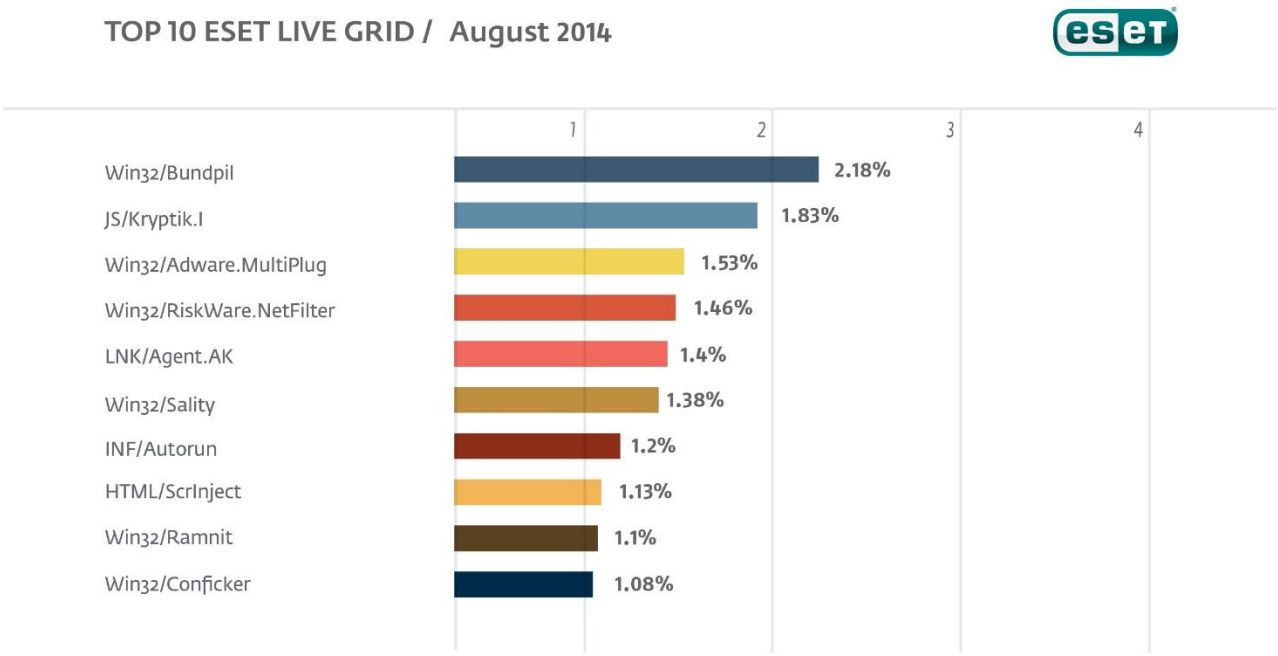
Win32/Conficker is a worm that spreads by exploiting a vulnerability in Server Service. The file is run-time compressed using UPX. When executed, the worm copies itself into the %system% folder using the name %variable%.dll.

The worm starts a HTTP server on a random port and it connects to remote machines to port TCP 445 in attempt to exploit the Server Service vulnerability. If successful, the remote computer attempts to connect to the infected computer and download a copy of the worm.

The worm will attempt to download several files from the Internet, and then they are executed. The worm contains a list of (1) URLs. Windows Firewall is disabled. This vulnerability is described in Microsoft Security Bulletin MS08-067.

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 2.18% 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
- WeLiveSecurity
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation