January 2013
Feature Article: Fact, Fiction, and Old-Time Movies

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Fact, Fiction, and Old-Time Movies

David Harley CITP FBCS CISSP, ESET Senior Research Fellow

In a world where nothing seems to be constant but change, it's good to know that there are, in fact, some things that change fairly slowly. Unfortunately, readiness to believe and spread hoaxes is one of them. Even worse, they're often the same hoaxes that were being spread years and even decades ago. Here's a hoax message - actually two hoaxes shoehorned into the same message - that was passed on to me this month. It goes back well over a decade: my wife (who received it from a well-meaning friend) and I are both pretty sure we saw hoaxes very much like this in the 1990s. While this version was received by email, the same or similar hoaxes are also spread via social media, especially Facebook. By the way, I've cleaned up the hoax text just a little, mostly to remove a plethora of redundant space characters.

> URGENT - PLEASE READ - NOT A JOKE

Well, it's certainly not funny. (Even less so if your name happens to be Simon Ashton.) Perhaps the number of hoaxes passed on with assurances that "this is not a joke" or "this is real", do at least indicate that people are a little more sceptical than they used to be.]

> IF A PERSON CALLED SIMON ASHTON (SIMON25@HOTMAIL.CO.UK) CONTACTS YOU THROUGH EMAIL DON'T OPEN THE MESSAGE. DELETE IT BECAUSE HE IS A HACKER!!

In fact, this message has been spread using a variety of names for the 'hacker' over the years: recent versions name, for example, Christopher Butterfield, Tanner Dwyer, Stefania Colac or Alejando Spiljner. Often, it's claimed that the alleged hacker will contact you with a friend request, which gives it an extra air of authority when spread by Facebook. In those instances, however, you're less likely to encounter the next paragraph, which is email-specific, in a muddled and seriously unconvincing sort of way.

> TELL EVERYONE ON YOUR LIST BECAUSE IF SOMEBODY ON YOUR LIST ADDS HIM THEN YOU WILL GET HIM ON YOUR LIST. HE WILL FIGURE OUT YOUR ID COMPUTER ADDRESS, SO COPY AND PASTE THIS MESSAGE TO EVERYONE EVEN IF YOU DON'T CARE FOR THEM AND FAST BECAUSE IF HE HACKS THEIR EMAIL HE HACKS YOUR MAIL TOO!!!!!.....

And at this point we get an abrupt change of focus topic, though it isn't flagged as such. Still, the fact that the message suddenly stops being all capitals is a bit of a giveaway. Excessive capitalization, by the way, is often a feature of hoax messages, no doubt in order to impress upon us how SERIOUS AND TRUE the message is.

Anyone-using Internet mail such as Yahoo, Hotmail, AOL and so on.. This information arrived this morning, Direct from both Microsoft and Norton. Please send it to everybody you know who has access to the Internet. You may receive an apparently harmless e-mail titled 'Mail Server Report'

Where to start on debunking this? Well, the fact that this targets everyone who uses Internet email and everyone who has Internet access should tell you something about the sender's motivation, and I don't mean sheer altruism.

Back when I first saw this message(or something very close), the idea that a message from Microsoft was likely to be an authoritative indicator of importance in terms of security was less convincing, but since then Microsoft has become both more security-conscious and a security vendor in its own right, so I guess that bit has actually gained (spurious) authority.

The assertion that 'This information arrived this morning' is something of a giveaway in itself. Hoaxes are notoriously vague about exact dates and, in fact, any information that might help you locate authentic information (corroborative or otherwise). The weakness of this approach is that if the recipient actually notices that the message has been forwarded many times to many people, he might actually start thinking about which morning that might have been, and look for more information. However, the impressive list of previous recipients on this particular email strongly suggests that plenty of people don't take that extra conceptual step.

This hoax is a variation on the 'Life is beautiful' hoax, which claimed that the message would include a malicious file masquerading as a Powerpoint presentation called Life is beautiful.pps. As it happens, there was a possibility long ago that a malicious file would arrive with a specific and identifiable filename. Well, I suppose it's still possible, but the authors of real malware learned long ago that there are all too many ways to vary the name of a malicious file spammed out with email, so it's not very likely. In this case, though, the hoax somehow got tangled up with real (but long gone) variants of the Win32/Warezov mass-mailer that arrived in an email claiming to be a 'Mail Server Report'. Sometimes, though not in this case, the hoax picks up an additional 'verified by Snopes' message, based on the fact that Snopes - a well-known reference source for information on hoaxes, urban legends and such - listed the real Warezov malware as true.

> If you open either file, a message will appear on your screen saying: 'It is too late now, your life is no longer beautiful.'

Obviously a hangover from the Life is beautiful version.

> Subsequently you will LOSE EVERYTHING IN YOUR PC, And the person who o sent it to you will gain access to your name, e-mail and password.

The usual drivel. Well, some or all of this *might* happen to you as a result of malware, but not the fictitious malware described in the message.

This is a new virus which started to circulate on Saturday afternoon.. AOL has already confirmed the severity, and the anti virus software's are not capable of destroying it ..

Gosh. This must be some serious virus. Not only has it turned Saturday into the day before Friday (or perhaps it was circulating for a week before anyone noticed their system had been trashed) , but AV is incapable of defeating it. I know that the likes of Imperva are still constantly claiming we can't detect malware, but even they don't usually go so far as to claim that we can't remove malware we know about. And I'm not sure how anyone can know so much about the timeline of a virus that destroys every system it touches.

AOL? Well, I guess that's an indication of how old the hoax is, going back to the days when the newsagents were perpetually tripping over AOL diskettes and CDs that had fallen off computer magazines, and hoaxes were constantly citing AOL and Microsoft in order to make themselves seem more 'authentic' and scary.

> The virus has been created by a hacker who calls himself 'life owner'..

Complete with extra period character to give it more weight. Or at any rate, so as to make the line a little longer. This line is another hangover from 'Life is beautiful'.

Hark! There's the tinkling sound of another angel getting his wings! Oh, sorry: I'm just getting confused between fiction and Frank Capra movies.

Virus Bulletin 2012 - two souvenirs

2012's Virus Bulletin conference in Dallas was pretty successful for ESET: you could barely move for ESET researchers on their way to or from their own presentations. A couple more ESET papers have now been put up on the conference papers page. Both papers were first published in the Virus Bulletin 2012 Conference proceedings, and are available here by kind permission of Virus Bulletin, which holds the copyright.

BYOD: (B)rought (Y)our (O)wn (D)estruction?

By Righard Zwienenberg

Nowadays all employees bring their own Internet-aware devices to work. Employers and institutions such as schools think they can save a lot of money by having their employees or students use their own kit. But is that true, or are they over-influenced by financial considerations?

There are many pros and cons with the BYOD trend. The sheer range of different devices that might need to be supported can cause problems, not all of them obvious. This paper will list the pros and cons, including those for Internet-aware devices that people do not think of as dangerous or even potentially dangerous.

These devices are often 'powered' by applications downloaded from some kind of App-Store/Market. The applications there should be safe, but are they? What kind of risks do they pose for personal or corporate data? Furthermore, the paper will describe different vectors of attack towards corporate networks and the risk of intractable data leakage problems: for example, encryption of company data on portable devices is by no means common practice. Finally, we offer advice on how to handle BYOD policies in your own environment and if it is really worth it. Maybe 'Windows To Go' - a feature of Windows 8 that boots a PC from a Live USB stick which contains Win8, applications plus Group Policies applied by the admin - is a suitable base model for converting BYOD into a Managed By IT Device.

Remember: BYOD isn't coming, it is here already and it is (B)ig, (Y)et (O)utside (D)efence perimeters!

Dorkbot: Hunting Zombies in Latin America

By Pablo Ramos

Win32/Dorkbot appeared at the beginning of 2011, and in just a couple of months the volume of Dorkbot detections increased until it became the malware with the most impact in Latin America over the whole year. This threat uses removable media and social networks as its means of spreading and achieved the highest position in threat ranking statistics in only three months. Ngrbot (as its author prefers to call it, or Win32/Dorkbot as the AV industry prefers) stands out as the favourite crime pack for Latin America's cybercriminals and it is widely disseminated through a wide variety of media and

vectors.

Lots of small botnets have been detected and are being used for information theft such as personal data and home banking credentials from compromised computers. Spreading through .LNK files via removable media, customized messages through social networks like Facebook, and using local news or compromised web pages, systems are being converted into bots controlled through the IRC protocol.

In this paper the main capabilities and features of Win32/Dorkbot are introduced, and we show its evolution into different versions, starting with AUTORUN spreading, and moving on to the use of LNK files and information-stealing techniques. Win32/Dorkbot.B is the most widely spread variant of this worm, its constructor having been leaked and made available on the web. We tracked down one of the active botnets in the region and reviewed the main activities performed by the cybercriminals.

The investigation came up with thousands of bot computers reporting to the bot master, who used several servers and vulnerable web pages for the implementation of phishing attacks and propagation of threats.

Social media messages have been used to spread copies of this malware through Facebook and Windows Live Messenger. Some of the topics used for spreading included presidents, celebrities and accidents all over the continent and the rest of the world. Also, email accounts are being stolen/hijacked by this malware.

We also comment on why and in what ways Win32/Dorkbot's activity in Latin America differs from the rest of the world, including trends that involve Internet usage, social media and user education. These combinations are a direct cause of the massive infection rates detected in the region. The main features, including botnet control, bot commands and protocols are described in this paper.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 3.27%

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. HTML/Iframe.B

Previous Ranking: 3
Percentage Detected: 2.77%

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

3. HTML/ScrInject.B

Previous Ranking: NA
Percentage Detected: 2.66%

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

4. Win32/Qhost

Previous Ranking: 4
Percentage Detected: 2.13%

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.

5. Win32/Sality

Previous Ranking: 12
Percentage Detected: 1.61%

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

6. Win32/Conficker

Previous Ranking: 2
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. 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.

7. Win32/Ramnit

Previous Ranking: 7
Percentage Detected: 1.17%

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

8. Win32/Dorkbot

Previous Ranking: 5
Percentage Detected: 1.15%

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.

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 6
Percentage Detected: 1.08%

It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

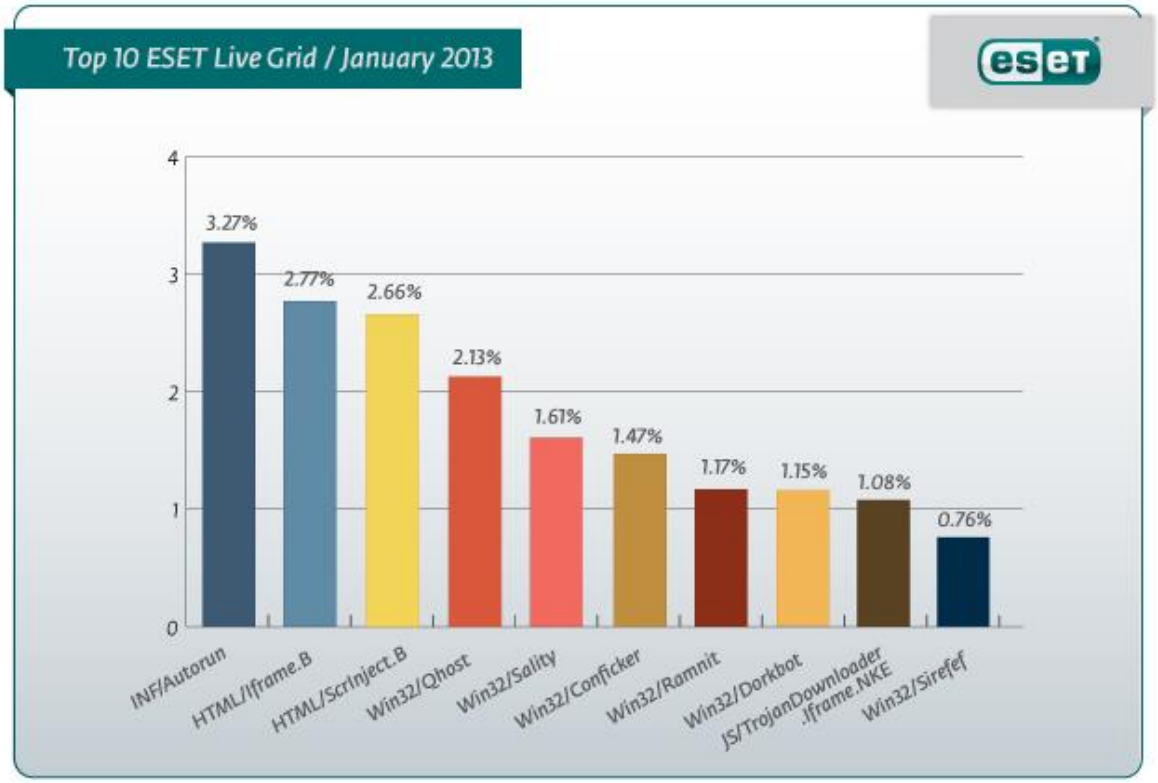
10. Win32/Sirefef

Previous Ranking: 9
Percentage Detected: 0.76%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 3.27% of the total, was scored by the INF/Autorun class of threat.



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