Global threat report

December 2012

Feature Article: ThreatBlogger FootSloggers Review 2012

Table of Contents

ThreatBlogger FootSloggers Review 2012

David Harley, ESET Senior Research Fellow

2012 on the ThreatBlog was far too busy to do justice to in a fairly short article: inevitably, I'll have to leave out some articles. Nevertheless the following summary should at least give you an idea of how the year looked to the blogging team.

January began with a flurry of Facebook-related activity, though it covered a wide range of related topics.

Stephen Cobb wrote about the many scams that preyed on the popular dislike and distrust of Facebook's imminent Timeline feature: Facebook's timeline to fraud-a-geddon? In Facebook, your birthday #1, and survey scams I looked at Facebook memes like 'the song that was #1 when I was born' – in my case it was a snappy little number called Sumer is icumen in, I think.

The Facebook watch site Facecrooks flagged a scam based on a fake app that claimed to tell you how much time you'd wasted – sorry, spent – on Facebook, which reminded one of our readers of the persistent 'see who visits your profile' scam. (Such an app isn't possible.) I wrote about it in Facebook scam: the hours I spend...

In Facebook Fakebook: New Trends in Carberp Activity, Aleksander Matrosov described some changes in the Carberp Trojan, including its gambit for extorting money from Facebook users by displaying a fake Facebook page when they tried to log into FB. The page claims that "Your Facebook account is temporary locked!" and instructs the victim to pay 20 Euros by Ukash voucher.

Of course, other social media were targeted too, as Stephen pointed out in Tricky Twitter DM hack seeks your credentials, malware infection, and more.

In fact, scams were a very prominent feature of the January threatscape: the first blog of the year, with some input from ESET Ireland's Urban Schrott, looked at a 419 scam that the scammer took the trouble to translate into Irish Gaelic, though I can't vouch for the quality of the translation: Irish 419-er seeks Spanish Lady. There was an echo much later in the year when the Irish Times reported the discovery of 'the first Irish virus', though it was actually ransomware rather than a real (self-replicative) virus, with the message translated into Irish: Irish Ransomware Report. Somewhat amusingly, Kafeine also drew my attention to a scam message targeting Ireland but translated into Iranian rather than Irish. Some miscommunication there... Ransomware Part III: another drop of the Irish. And Aryeh Goretsky warned us to Beware of SOPA Scams and ZeuS-related malware, rather bizarrely, passed itself off as a phishing message alert from US-CERT and the Anti-Phishing Working Group (Phishing and Taxes: a dead CERT?). Sebastian Bortnik flagged the way that Malware exploits death of North Korea's Kim Jong-il.

Passwords and passwording has been a pretty constant topic of interest this year, too. In Passwords, passphrases, and big numbers: first the good news... I flagged an interesting paper by Cormac Herley and Paul van Oorschot and linked to a number of resources from ESET and elsewhere that might be of use and interest (so I'm including them here).

- Keeping Secrets: Good Password Practice
- Passwords, passphrases and past caring

- No chocolates for my passwords please!
- Choosing Your Password
- Passphrases A Viable Alternative To Passwords?
- A Research Agenda Acknowledging the Persistence of Passwords
- Hearing a PIN drop

And as Cameron Camp described in Zappos.com breach - lessons learned, Zappos.com experienced one of the first major customer authentication breaches of the year but reacted promptly and efficiently. Cameron also had some good advice for those of us who were enjoying new toys of the tablet persuasion: New Year's resolutions for securing your new tablet. Peter Stancik asked us if it was Time to check your DNS settings? and offered advice on how to tell if your system had been infected by DNSChanger malware in advance of the constantly shifting deadline for the shutting down of the servers that were keeping the owners of infected machines online after the botnet was taken down.

We translated and published an English version of ESET Latin America's predictions for 2012 – New White Paper "Trends for 2012: Malware Goes Mobile" – and Aryeh updated his paper on Possibly Unwanted Applications: Potentially Unwanted Applications White Paper Updated.

In **February**, I came back to Facebook memes that might not be as harmless as they seem in an article for Virus Bulletin: Living the Meme, while in How to improve Facebook account protection with Login Approvals Stephen complimented Facebook on a security measure while clarifying its use.

Cameron looked in CarrierIQ-style data gathering law to require mandatory notification/opt-in? at a bill requiring mandatory consumer consent prior to allowing the collection or transfer of data on smartphones: he also looked at Google's attempts to beat back the rising tide of Android malware in Google responds to Android app Market security with stronger scanning measures, and at social media's commoditization of its customer in Facebook/app data privacy - sharing gone wild, and finished the month with a searching examination of the BYOD trend.

Inevitably, the run-up to Valentine's Day saw lots of malicious activity, and Stephen addressed the problem comprehensively in Cookie-stuffing click-jackers rip off Victoria's Secret Valentine's giftcard seekers. I got the opportunity to talk to senior police officers in the UK about those PC support scams that I've been banging on about since before Columbus sailed the blue: Cybercrime and Punishment, and also Cybercrime, Cyberpolicing, and the Public. I also looked at some data from a survey conducted by Amárach Research on behalf of ESET Ireland, as blogged by Urban Schrott: Your Children and Online Safety, ESET North America CEO Andrew Lee returned to the topic of intellectual property, piracy and legislation: ACTA and TPP: The wrong approach to intellectual property protection. Aryeh Goretsky took a long hard look at Windows Phone 8: Security Heaven or Hell?

On the technical analysis front, Aleksandr Matrosov and Eugene Rodionov shared some more research with us on Olmarik/TDL4: TDL4 reloaded: Purple Haze all in my brain. And Righard Zwienenberg, fresh to ESET but with many, many years in the security industry already, looked at Password management for non-obvious accounts.

Cameron kicked us off in **March** with a series of reports from the huge RSA conference in San Francisco, and Stephen followed up in Information Security Disconnect: RSA, USB, AV, and reality. Several security gurus at RSA who should really have known better told Wired that they don't use antivirus and strongly implied that no-one else should either: I responded to that in Security professionals DO use anti-virus. Stephen made available the excellent Malware Inc. presentation that he made at RSA – Changing how people see the malware threat: images can make a difference – and offered an infographic exploring all the data Google could, potentially exploit: Google's data mining bonanza and your privacy: an infographic. He also considered the issues around employers requiring access to employee Facebook accounts and the spring crop of IRS-related scams: Facebook logins toxic for employers, violate security and privacy principles and Spring Brings Tax-related Scams, Spams, Phish, Malware, and the IRS.

On the more technical front, Righard shared a few surprises with us after he installed Skype onto a new laptop: SKYPE: (S)ecurely (K)eep (Y)our (P)ersonal (E)-communications, followed up with some analysis of Android's locking mechanism that gave me a useful reference for my EICAR presentation in May on PIN Holes: Passcode Selection Strategies, and then looked at Win32/Georbot in From Georgia With Love: Win32/Georbot information stealing trojan and botnet. ESET Canada allowed me access to some of their research so that I was able to sound as if I might know what I was talking about in Kelihos: not Alien Resurrection, more Attack of the Clones. In Modern viral propagation: Facebook, shocking videos, browser plugins, Robert Lipovsky looked in some depth at scam propagation techniques, and in Vulnerable WordPress Leads to Security Blog Infection he looked at Javascript infectors. I looked in depth at some more of the techniques used by support scammers - Support Scammers (mis)using INF and PREFETCH and Fake Support, And Now Fake Product Support, and our Russian colleagues shared lots of information on Blackhole, CVE-2012-0507 and Carberp. And Alexis Dorais-Joncas delved into the murky world of Mac malware: OSX/Imuler updated: still a threat on Mac OS X, and OSX/Lamadai.A: The Mac Payload.

In **April** the questions of quasi-testing and the usefulness (or not) of anti-virus came up again. I finally posted a paper on the topic with Julio Canto of VirusTotal and engaged in a debate of sorts in SC Magazine: VirusTotal, Useful Engines, and Useful AV, and, along with Andrew Lee, tried to introduce a note of sanity into the 'AV isn't worth paying for' debate: Free Anti-virus: Worth Every Penny? So that's sorted that question? Unfortunately not: in December (see below) the same fallacies came up all over again.

Aleksandr looked at a hot-off-the-press exploit kit technique: Exploit Kit plays with smart redirection (amended), and in Phishing Using HTML and Intranet Security Settings Righard dug deep into a rather novel approach to phishing – Phishing Using HTML and Intranet Security Settings – and gave some good advice following the deferment of the FBI's shutdown of servers maintained following the takedown of DNSchanger botnets: DNS Changer (re)lived, new deadline: 9 July 2012!

Stephen introduced another very popular infographic, this time on the Bring Your Own Device: BYOD Infographic: For security it's not a pretty picture. A topic most of us have been asked about or written about many times this year, in blogs, conferences and interviews. He also looked at the legal imperatives that make establishing a WISP (Written Information Security Program) a good idea, Java, Macs and Flashbacks, and took a long hard look at QR Codes and NFC Chips: Preview-and-authorize should be default.

Alexis Dorais-Joncas and Pierre-Marc Bureau both wrote about OSX/Malware (yes, Virginia, there is such a thing), Cameron wrote about Pinterest, and asked Could your next new car be hacked (should you be scared)? And I wrote about PC support scams. Quelle surprise. But maybe it’s never a waste of time to show people How to recognize a PC support scam.

On **May** 1st I thought about going Morris dancing but instead I wrote about a support scam poll on behalf of the Internet Storm Center. For someone who stopped working the helpdesk in 2001, there seem to be an awful lot of support issues in my life. Since I spent most of the month at EICAR, CARO (Aleksandr blogged about his presentation there) and AMTSO, AMTSO in particular rather dominated my writing and even got me an unexpected interview with Infosecurity Magazine. I did have one moment of old-time AV nostalgia, though: Win32/Flamer: the 21st Century Whale.

Stephen had good advice for travellers (thanks, Stephen: came in very useful!) in 11 Tips for protecting your data when you travel and Foreign Travel Malware Threat Alert: Watch out for hotel Internet connections. For stay-at-home, virtual travellers he had more advice in How to stop Twitter tracking you and keep private the websites you visit and made available a video giving the bad guy’s view of a remote access Trojan: Malware RATs can steal your data and your money, your privacy too.

Aryeh posted about a new approach to cruise/vacation property scams: Press One if by LAN, Two if by Sea… And Cameron posted on SMSmishing (SMS Text Phishing) - how to spot and avoid scams, Millions have not reviewed Facebook privacy settings: Here's how, and DNSChanger ‘temporary’ DNS servers go dark soon: is your computer really fixed?

In **June**, Stuxnet and its siblings (or offspring) became a big issue (again): not only because of the fuss about Flamer, but because it suddenly seemed that the US government was claiming part of the credit for Stuxnet, at least. Stephen spoke for us all when he said Stuxnet, Flamer, Flame, Whatever Name: There's just no good malware, and made more good points on The negative impact on GDP of state-sponsored malware like Stuxnet and Flame . He provided more travel advice in Data security and digital privacy on the road, what travelers should know but while the holiday season was just getting into its swing in the Northern hemisphere, he warned that Back to school scams? They may be just around the corner, and advised on how to spot them.

Aryeh, meanwhile, was beset by scams in SMSmishing Unabated: Best Buy targeted by fake gift card campaign and Close Call with a Caribbean Cruise Line Scam. He seems to have become inextricably entangled with cruise scams in the same way that I have with support scams. We both had something to say on the perennial topic of passwords and PINs: Guarding against password reset attacks with pen and paper and Passwords and PINs: the worst choices. But I did manage to get a little time out in Slovenia (and got very sunburnt in Venice), though I was basically there for a conference at the behest of Urban Schrott, of ESET Ireland.

Cameron was mainly focused on social networking, from Google to LinkedIn to Facebook (Your Facebook account will be terminated - again and Facebook policy changes - does the 'crowd' really have a seat at the table?). He still found time to indulge his passion for automotive security, though: How much will your driverless car know about you (and who will it tell)?

On the technical analysis side, Jean-Ian Boutin looked at Win32/Gataka and Robert Lipovsky and Righard Zwienenberg both looked at ACAD/Medre. Meanwhile, Aleksandr Matrosov and I both talked about the ZeroAccess rootkit, while Aleks noted some interesting data around CVE2012-1889: MSXML use-after-free vulnerability.

In **July**, Aryeh blogged about .ASIA Domain Name Scams Still Going Strong instead of cruise line scams and I blogged a couple of times about support scam gambits. Ho, hum. Peter Stancik and myself addressed in several blogs the issue of the final deadline for the turning off of the FBI's servers substituting for the DNSChanger servers. If there's anyone out still out there who doesn't have Internet access any more, I don't think you can blame us.

Righard found some Scareware on the Piggy-Back of ACAD/Medre.A. Aleks blogged about Flame and its siblings and predecessors, updates to the Rovnix framework, Java exploitation, and legal assaults on the Carberp botnet (yay!).

There were more issues with passwords that Stephen and I couldn't resist blogging about: Passwords of Plenty*: what 442773 leaked Yahoo! accounts can tell us and Password Party Weekend? Millions exposed now include Phandroid, Nvidia, me. Stephen also commented on an Instagram vulnerability. Cameron blogged his socks off about BlackHat, Defcon, Free YouTube .mp3 converters - with a free malware bonus, and Gamigo game site hack – lessons learned (and what should you do), and UK journalist Kevin Townsend turned my thoughts to Rakshasha, Hindu demon and allegedly permanent and undetectable backdoor. I think not.

August was a little quieter, and Aleks led off with Flamer Analysis: Framework Reconstruction, while Eugene Rodionov, whose work with Aleks has informed so much of the analysis we've blogged on here, highlighted the Interconnection of Gauss with Stuxnet, Duqu & Flame. Stephen dissected the way the Reveton ransomware snares its victims. Sébastien Duquette blogged a comprehensive analysis of a website selling access to a malware-distribution service. The guys responsible seem to have loved the publicity, but our filtering stopped them piggybacking the blog to get more custom. Come on guys, we're not that dumb...

Robert Lipovsky blogged about Quervar – Induc.C reincarnate? and there was an unexpected intersection between technical analysis and support scams: Support scams and Quervar/Dorifel. In fact, there was a lot of action around support scams this month: AMMYY, whose remote access service is often misused by Indian scammers (in the US, it's often referred to as the AMMYY scam), came up with some useful information and a warning, while one of the scammers who ring me with monotonous regularity provided a little light relief: Support Scammer Anna's CLSID confusion. All good material for the presentations on the topic I'd be making at CFET and Virus Bulletin in September.

Cameron picked up on Mac OSX/iOS hacks at Blackhat - are scammers setting their sights?, Blizzard Entertainment hacking, and photo tagging on Facebook. Stephen offered excellent advice: Java zero day = time to disable Java, in your browser at least. Cameron also blogged at some length about the FinFisher spyware and I took up the theme when one of our readers asked about ESET's detection of the spyware (which we detect as Win32/Belasek.D): Finfisher and the Ethics of Detection.

While I've previously talked about the Top Umpteen bad choices of password, I got fed up with all the journalists simply listing over-used passwords as if all you have to do is not use the top 25 and you're safe, and tried to adopt a more constructive approach: Bad password choices: don't miss the point. However, one of my blogs that month came directly from a conversation with one of the more technically competent journalists working in security, The Register's John Leyden: Carbon Dating and Malware Detection.

September was also fairly quiet in the run-up to the Virus Bulletin conference: like most of the anti-malware industry, we consider VB to be one of the most important events of the year, and as you'll see from my summary of ESET's papers and articles in 2012, we had a lot of presentations to prepare for. Righard and I also presented at a small but invariably interesting forensics conference at Canterbury, in the UK. While I was there, I grabbed an opportunistic photo on my phone that I was able to use almost immediately for a blog on ATM/cashpoint security: again, it derived from an article by a knowledgeable journalist specializing in computer security, the estimable Brian Krebs: ATM Security? Don't bank on it.

Sadly, Pierre-Marc Bureau doesn't often find time to contribute to the blog these days, but when he does, it's always worth reading, and Dancing Penguins – A Case of Organized Android Pay Per Install was no exception. Aryeh also looked at Android security in The Dynamic Duo for Securing your Android: Common Sense and Security Software. And Pierre-Marc also summarized the state of (non-)play with OSX/Flashback in Flashback Wrap Up.

We came across the 'first Irish virus' which appears to have been non-viral ransomware with the message translated into (Irish) Gaelic (Gaeilge). Actually, thanks to researcher 'Kafeine' I subsequently got to see examples of other messages regionalized for other countries and languages. While this kind of malicious activity is no laughing matter, I did get some amusement out of the fact that one example inadvertently used some French text among the Gaeilge, and another apparently got confused between the .ir and .ie Top Level Domains and generated text in Iranian language apparently intended to target speakers of Gaeilge.

I also returned to the topic of PIN selection strategies, commenting on research from DataGenetics: Choosing a non-obvious PIN. Cameron wrote about Facebook timeline security & privacy: steps to keep your account & identity safe, and followed up with Facebook timeline privacy/security: protect your account and identity (2/2). And in a slightly unusual case of the source quoting the journalist(s) I cited conversations with and articles by Kevin Townsend, Dan Raywood, and John Leyden in a post on malware inserted into the supply chain: Nitol Botnet: You Will Never Break The Chain.

In **October**, Cameron blogged about a free Android app from ESET available from Google Play to protect Android devices from the USSD vulnerability: Free Android USSD vulnerability protection from ESET now on Google Play. Aryeh also shared some product information: W8ing for V6: What ESET has in store for Windows 8 Users. Stephen asked, given that October was National Cyber Security Awareness Month, whether How's Your Cyber Security Awareness? Or, do we really need security training? (the answer was yes!) By way of follow-up he disclosed the results of a Harris Poll that found that Younger people less secure online than their elders new study suggests, and in Brutalized! South Carolina breach exposes data security woes at State level, observed that 86% of state CISOs identified "lack of sufficient funding" as the key barrier to addressing cybersecurity. He also picked up on concerns about threats inserted into the supply chain, this time with reference to government paranoia: Huawei? The how, what, and why of telecom supply chain threats.

Aleks contributed some typically detailed technical analysis Olmasco bootkit: next circle of TDL4 evolution (or not?). Stephen gave me a break from writing about support scams and blogged about how FTC cracks down on tech support scams and feds nail fake AV perps, though I couldn't resist blogging a week or two later on why the problem isn't going to disappear completely just yet: Telescammer Hell: What's Still Driving The PC Support Scammers? But of course several of us, as ever, were reporting on scams of one sort or another. Cameron warned us to Avoid Election Season Scams: Donations and cruises to avoid. I talked about telephone scams that weren't about telephone support scam – Telephone Scams: it's not all about PC support – and I finished off the month with an ambitious three-part blog on phishing (with some help from Urban Schrott) which is now available as a single paper. I should probably emphasize that when I wrote about Malware and Medical Devices: hospitals really are unhealthy places... I had no prior knowledge of where the plot of Homeland series two was going (murder by remotely controlled pacemaker). :)

November inevitably continued some similar themes. On the technical front, Jean-Ian Boutin looked at the latest developments concerning Win32/Gataka – or should we say Zutick? Pablo Ramos wrote two blogs on Android/TrojanSMS.Boxer.AA, one of them a deep-dive technical analysis and the other aimed at a more general audience: Don't pay high phone bills: SMS Trojans can trick you via premium-rate numbers. This is an approach we'd like to make more use of, giving our less technical audience a view of why certain malicious technology has an impact on their online lives without boring them with programmatic esoterica, but doing so is something of a challenge for a small blogging team. Writing technical content that is relevant and interesting to the lay reader but still accurate is as demanding in its own way as heavily technical material. In Win32/Morto – Made in China, now with PE file infection, Pierre-Marc managed to find a balance between the two that appealed to a wide range of readers.

In Wauchos Warhorse rides again I looked at an interesting spike spotted by Stephen in UK detections of an elderly malware family. Statistical artifacts are interesting, but not always explicable. Aryeh is the team expert on Windows 8, but in Windows 8: there's more to security than the Operating System I looked at the way current events (such as the release of Win8 and Hurricane Sandy become fodder for social engineering attacks, and in Premium Rate Scams and Hoaxes I looked at a very different aspect of Premium Rate misuse to that blogged by Pablo. In Support Scams and the Surveillance Society and New Support Scam Gambits: Frozen Virus a Frozen Turkey I looked at some new evolutions in PC support scamming. Stephen followed up his speculations on a new angle on data theft (Digital photos demand a second look as picture-stealing threat develops) with a very useful, very popular seasonal piece on Safer cyber-shopping makes for happier holidays: 12 simple safety tips.

At the time of writing, **December** is barely half-way through and already shaping up to be as eventful as any other month this year. There was another Mac-specific attack on Tibetan activists – Spying on Tibetan sympathisers and activists: Double Dockster – while Stephen returned to the vexatious topic of passwording in Password handling: challenges, costs, and current behavior (now with infographic). It's frustrating that such a flawed and heavily exploited authentication technology still dominates our online lives.

Another security company tried to prove that money spent on anti-virus would be better spent on their own products with a poorly-conceived 'test' based on inappropriate use of the VirusTotal service. Righard pointed to some of the flaws in their logic in Why Anti-Virus is not a waste of money and I returned to the theme of misuse of VirusTotal (which I'd already addressed in a joint paper with VT's Julio Canto) in one of my external (non-ESET) blogs. (Some of us do a great deal of blogging and other writing outside ESET, far more than the list of papers and articles below indicates: it would be just too time-and-space-consuming to find and list everything we've written this year.)

The security industry suddenly woke up to the fact that despite Microsoft's attempts to eradicate the misuse of the Autorun functionality in removable media, threats that use that vector continue to thrive. This wasn't exactly news to us: INF/Autorun and its siblings have been dominating our threat reports all along. However, Stephen generated some interesting and useful new material on the topic in My Little Pronny: Autorun worms continue to turn and Are your USB flash drives an infectious malware delivery system?

I was overcome by nostalgia after receiving a 419 claiming to be from the wife of a former Nigerian Head of State: Maryam Abacha rides again: yes, Virginia, there IS a Sani-ty Clause!*. Ontinet's Josep Albors directed my attention to the murky world of boiler room scams and alternative investment scams in Diamonds are forever, and so are investment scams. ESET Latin America offered their predictions for malware trends in 2013 in a paper announced by Sebastian Bortnik: Trends for 2013: astounding growth of mobile malware. Unsurprisingly, Android malware is prominently featured. Other ESET researchers looked into their own crystal balls a little later in the month.

Aleks updated ongoing research on the vulnerabilities in smartcard systems used for banking with news of Win32/Spy.Rambus. Pablo returned to the topic of Dorkbot, the subject of his paper at the Virus Bulletin conference. And Aryeh kicked off a highly seasonal series on securing those Christmas computing goodies. A lot of interest was generated by Pierre-Marc's report of malicious activity in the Linux realm, which prompted talk of a "malicious Apache module" which then prompted a further post to clarify the implications of that phrase.

We look forward to some big changes in the Threat Blog in 2013, and we hope to continue to hold your interest. Although we cannot answer technical support and licensing questions on the blog, we do value your contributions in the form of blog comments and email to askeset@eset.com, and hope you'll continue to tell us what you like and what you don't like so much.

Compliments of the season to all of you, from all of the ESET blogging team, and a happy and prosperous 2013.

ESET Papers and Articles in 2012

Articles

- AMTSO: the Test of Time? Article for Network Security by David Harley, January 2012
- When I'm x64: Bootkit Threat Evolution in 2011 Article for Hakin9 by David Harley, Aleksandr Matrosov & Eugene Rodionov, February 2012
- Living the Meme Article for Virus Bulletin* by David Harley, February 2012
- Are companies too confident about targeted attacks? Article for Computer Weekly by David Harley, July 2012

*Copyright is held by Virus Bulletin Ltd, but is made available on ESET's resources page for personal use free of charge by permission of Virus Bulletin.

Conference Papers

The following conference papers have been published or linked on the White Papers page at [...............]

- After AMTSO: a funny thing happened on the way to the forum Conference paper for EICAR 2012 by David Harley

- PIN Holes: Passcode Selection Strategies Conference paper for EICAR 2012 by David Harley
- FUD and Blunder: Tracking PC Support Scams By David Harley, Martijn Grooten, Craig Johnston and Stephen Burn. Presented at the Cybercrime Forensics Education & Training Conference in September 2012.
- Defeating anti-forensics in contemporary complex threats By Eugene Rodionov and Aleksandr Matrosov. First published in Virus Bulletin 2012 Conference Proceedings*
- My PC has 32,539 errors: how telephone support scams really work Conference paper for Virus Bulletin 2012 by David Harley, Martijn Grooten, Steven Burn and Craig Johnston. First published in Virus Bulletin 2012 Conference Proceedings*
- Festi botnet analysis and investigation Conference paper by Aleksandr Matrosov and Eugene Rodionov. As presented at the AVAR 2102 conference in Hang Zhou.

*Copyright is held by Virus Bulletin Ltd, but is made available on ESET's resources page for personal use free of charge by permission of Virus Bulletin.

The following papers and/or presentations for Virus Bulletin 2012 have not yet been published or linked on the White Papers page.

- BYOD:(B)rought (Y)our (O)wn (D)estruction? by Righard Zwienenberg
- Dorkbot: hunting zombies in Latin America by Pablo Ramos
- Malware and Mrs Malaprop: what do consumers really know about AV? (sponsor presentation) by Stephen Cobb
- LAST-MINUTE PAPER: Gataka: a banking trojan ready to take off? Jean-Ian Boutin
- LAST-MINUTE PAPER: ACAD/Medre: industrial espionage in Latin America? Robert Lipovsky, Sebastian Bortnik
- Cyberwar: reality, or a weapon of mass distraction? Andrew Lee

ESET Conference Presentations

- Carberp Evolution and BlackHole: Investigation Beyond the Event Horizon By Aleksandr Matrosov, Eugene Rodionov, Dmitry Volkov and Vladimir Kropotov, May 2012. A joint presentation for the CARO workshop in Munich by researchers from ESET, Group-IB, and TNK-BP.
- Bootkit Threats: In Depth Reverse Engineering & Defense By Eugene Rodionov and Aleksandr Matrosov, June 2012 for the REcon conference held in Montreal.
- Defeating antiforensics in contemporary complex threats By Aleksandr Matrosov and Eugene Rodionov.

This is the slide deck used for a presentation at the Virus Bulletin 2012

- My PC has 32,539 errors: how telephone support scams really work By David Harley, Steven Burn, Martijn Grooten, and Craig Johnston. This is the slide deck to go with the paper presented at Virus Bulletin 2012
- Win32/Flamer: Reverse Engineering and Framework Reconstruction By Aleksandr Matrosov and Eugene Rodionov: the slide deck from a recent presentation at the 2012 Zero Nights conference
- Festi Botnet Analysis & Investigation By Aleksandr Matrosov and Eugene Rodionov: the slide deck from a recent presentation at the 2012 AVAR conference

White Papers

- Trends for 2012: Malware Goes Mobile By ESET Latin America, January 2012
- ACAD/Medre.A By Robert Lipovsky and Righard Zwienenberg, June 2012
- OSX/Flashback By Marc-Etienne Leveille , September 2012
- Windows 8: FUD* for thought By Aryeh Goretsky, October 2012
- Online Shopping and a Phishing Pheeding Phrenzy By David Harley and Urban Schrott, October 2012
- Boxer SMS Trojan By André Goujon and Pablo Ramos, November 2012

ESET Podcasts

http://www.eset.com/us/resource/presentations/podcast/

ESET Webcasts

http://www.eset.com/us/resource/presentations/webinars/

The Top Ten Threats of 2012

1. INF/Autorun

Percentage Detected: 5.17%

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/ScrInject.B

Percentage Detected: 4.44%

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

3. HTML/Iframe.B

Percentage Detected: 3.51%

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

4. Win32/Conficker

Percentage Detected: 3.00%

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.

5. Win32/Sality

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/Dorkbot

Percentage Detected: 1.55%

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. JS/TrojanDownloader.Iframe.NKE

Percentage Detected: 1.39%

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.

8. Win32/Sirefef

Percentage Detected: 1.31%

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

9. Win32/Ramnit

Percentage Detected: 0.98%

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/Spy.Ursnif

Percentage Detected: 0.76%

This is a spyware application that steals information from an infected computer and sends it to a remote location, creating a hidden user account, in order to allow communication over Remote Desktop connections.

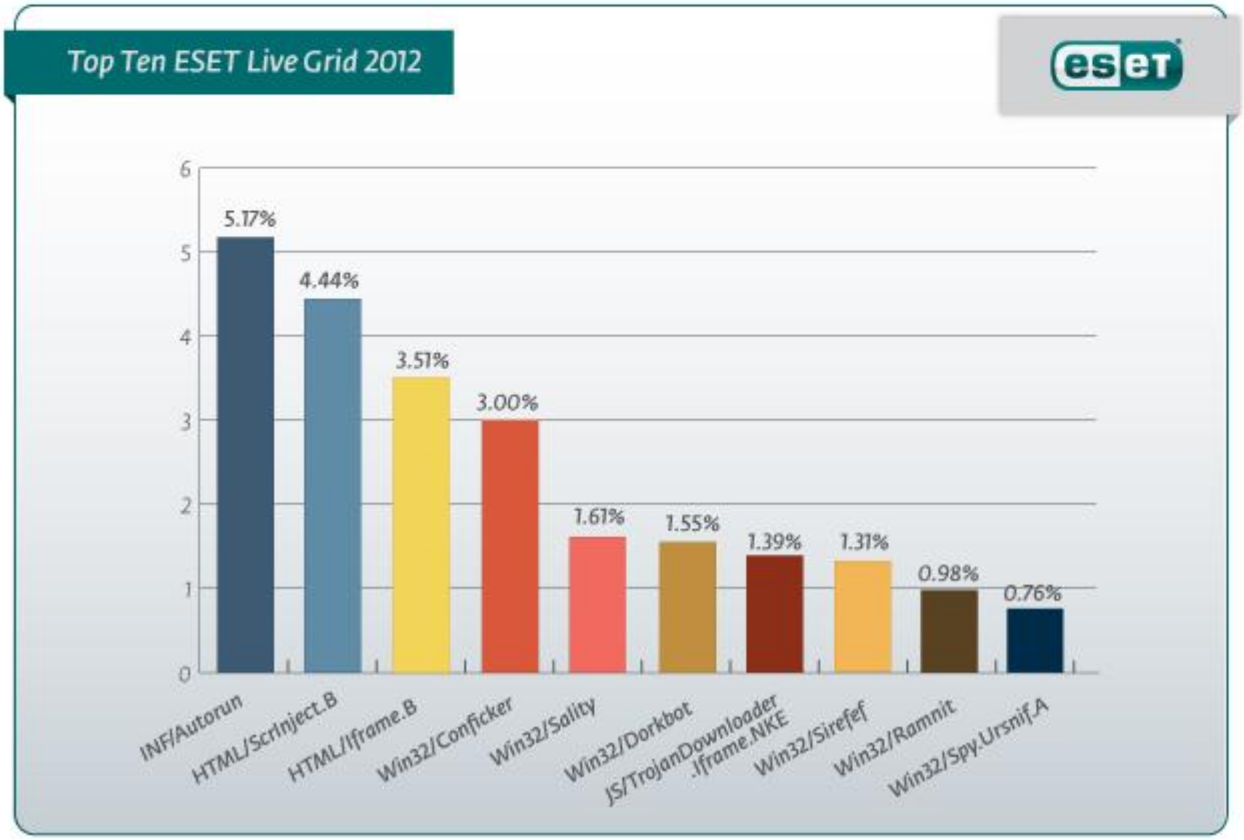
What does this mean for the End User?

While there may be a number of clues to the presence of Win32/Spy.Ursnif.A on a system if you're well-acquainted with esoteric Windows registry settings, its presence will probably not be noticed by the average user, who will not be able to see that the new account has been created.

In any case it's likely that the detail of settings used by the malware will change over its lifetime. Apart from making sure that security software (including a firewall and, of course, anti-virus software) is installed, active and kept up-to-date, users' best defense is, as ever, to be cautious and proactive in patching, and in avoiding unexpected file downloads/transfers and attachments.

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 year INF/Autorun, with almost 5.17% 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