Threat Radar

December 2013 Feature Article: The Year of Surviving Dangerously: Highlights from We Live Security 2013

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

This month we decided to present a retrospective of all 2013, so we develop and delve into the most prominent threats that each month had. Also published an article that specifically addresses the issue of scams during 2013. So, as you can see, the December issue is larger than normal.

Finally, in the Corporate News section you can read the brand new 2014 Trends article, which focused on the challenge of Internet privacy.

The Year of Surviving Dangerously: Highlights from We Live Security 2013

Lysa Myers ESET Security Researcher III

2013 was another very busy year on We Live Security (the website formerly known as the ESET Threat Blog). As in last year's Threat Blog round-up, quite a few articles had to be glossed over to cover the highlights without producing an entire book. I highly recommend you dig around on www.welivesecurity.com to see more. While this article focuses mostly on malware and legislation, David Harley's forthcoming article '2013: a Scammer's Eye View' looks at some of the scams that have crossed our radar, on and off the We Live Security blog. So here are the 2013 highlights:

JANUARY was a particularly busy month in this busy year past. Stephen Cobb and Cameron Camp provided a look into theft statistics and physical security for devices. This advice is particularly timely information to revisit in the post-holiday season when many people have new digital goodies to protect.

Robert Lipovsky provided a brief warning, plus in-depth information on a couple of different threats. The warning pertained to Java vulnerability CVE-2013-0422 being added to a couple of popular exploit packs, thus making it more accessible to attackers. The in-depth information was about a notable threat calling itself PokerAgent that was targeting Facebook credentials, credit card information linked to Facebook accounts, and Zynga Poker account information. Targeting online game credentials is certainly well-trodden territory for online criminals, but this was the first targeting this particular game.

Discussing another interesting shift in malware tactics, Alexis Dorais-Joncas looked at Jabberbot in a series of articles. Bots have been using various different protocols for their Command and Control (C&C) channels over the years, but this was the first example of a bot using IM (specifically the protocol used by Jabber) to coordinate. This was of particular interest to yours truly, as predicting the possibility of using IM for bot coordination was the subject of my first presentation to the Virus Bulletin conference in 2006. Though of course, as it did not come to pass for another 7 years, AIM did not end up being the malware-writers' IM protocol of choice.

It is a popular trope within the commentary around computer security that "AV is dead", meaning that the commenter thinks anti-malware software is not sufficient protection to be "worth the money". This assertion is often accompanied by some statistic about the detection rates of signature-based protection (which is not all that comprises any reputable AV product, and it is only one small component of security suites… but I digress). And some poorly constructed test is often the source of that statistic. David Harley looked at one such pseudo-test that was making the rounds, with some particularly egregious assertions and methodology. He and Larry Bridwell subsequently revisited the issue in a paper for the AVAR conference: Death of a Sales Force: Whatever Happened to

Anti-Virus?

FEBRUARY brought another bumper crop of articles, including several about interesting malware that had been recently discovered. Aleksandr Matrosov discussed the Redyms family of Trojans, its similarity to the TDL family of malware, and its penchant for hijacking the search traffic of affected users. Aleksandr also provided a look into the malware family of Caphaw, which uses a variety of modules to achieve stealth, and additional functionality. Most notably, this malware injects fake data into bank websites visited by affected users, so that they are given erroneous contact information for the bank, and false balance information that blinds the user to money being removed from their account.

Alexis Dorais-Joncas brought up the possibility of a coming arms race between malware authors and anti-DDoS services in his article about Win32/DoS.OutFlare.A. While other security vendors are well familiar with the cat-and-mouse game between their products and bad actors, this malware's attempt to bypass anti-DDoS measures was a first.

Several articles also discussed the dangers of malware spreading by seemingly innocuous means. Righard Zwienenberg took a look at an incident where a popular malware removal tool, ComboFix, was briefly available for download with an added surprise – an infection with a variant of the "popular" Sality virus. Righard also wrote about the importance of including mobile devices in security policy in the workplace, and how moving from allowing users to "Bring Your Own Device" to "Choose Your Own Device" allows for a better balance of security and mobility. Stephen Cobb reported on another incident where NBC.com was briefly hosting malware. While it's noteworthy when such large and popular websites are compromised, we often see compromises of otherwise-innocent websites by malware authors.

The other side of the security trope discussed the previous month, about people announcing the "death of AV", is people declaring that "free AV is enough" security for most computer users. Rather contradictory! But it is always informative to have some real life statistics, to see where people actually fall in their security habits and practices. David Harley reviewed some figures specific to Irish users, and found that almost half the people polled were using free AV products.

MARCH brought with it much discussion about malware and security problems on non-Windows platforms. Stephen Cobb mused on the similarities between the current threat landscape faced by Android users and the early days of Windows. While both started as fairly insecure platforms, it is our hope that Android progresses more quickly to becoming more secure. Cameron Camp also discussed another aspect of Android security, particularly Google's move to get rid of ad-blocking software from its app store. As ad-blocking software is popular on every platform, it may push users to seek these apps from other, potentially less trustworthy sources.

Meanwhile in Mac-land, Stephen Cobb provided protection and remediation tips for OS X users, against a Trojan adware plugin called Yontoo that was hiding behind movie trailers and other media playing links. Stephen also examined a stumble in the password-reset process for AppleID as Apple was rolling out improved security measures, implemented after journalist Mat Honan revealed how his online identity had been severely compromised due to holes in the identity verification processes of a number of vendors, including Apple.

Aleksandr Matrosov examined a pair of Trojans related to banking malware, in a series of articles. The first article looks at the Theola malware which, like the Caphaw Trojan that Aleksandr analyzed the month before, also uses various components including a bootkit to further its end of accessing people's bank accounts. The second post examines the PowerLoader bot-builder that is often found downloading the Gapz and Redyms Trojans, the latter of which was also considered the month prior. The third ties together the similarities between behavior seen in PowerLoader and Gapz Trojans, as observed in the Carberp family of malware. As the title observes, this is indeed a never-ending story!

It seemed for a while that every week brought news of another vendor being breached, and users' passwords being stolen. The next bit of news was often that said vendor would soon be adding two-factor authentication for their users. But what is that, and what does it entail? David Harley answered this question, and explained why you might want to go to the trouble of adding this additional factor when it is available to you.

APRIL began with a couple of articles, by Stephen Cobb and Alexis Dorais-Joncas, warning about the possibility of cyber criminals and other vultures that were utilizing the tragic Boston Marathon bombings to draw people into their scams. This is a good illustration of how malware authors and other criminals will use any opportunity to draw people – especially those that are feeling concerned and eager to help – into bad situations.

Not to be left out of using people's fear to part them from their money, the authors of a fake AV Trojan described by Jean-Ian Boutin falsified malware detection on affected users' machines and locked their screens. It did so in order to get the frightened users to call a support number that would help them remove this imaginary malware and unlock their screen …for a nominal fee. It's a strange move, combining the features of fake AV with ransomware and telephone support scams.

In case Linux users felt left out of the non-Windows-OS malware analysis extravaganza of the previous month, Pierre-Marc Bureau provided prevention and remediation information for a backdoor that was found on compromised Apache webservers, called Linux/Cdorked.A. This begins a series that continues in May. There's no OS that is truly excluded from the threat of malware!

Toward the end of April, Aleksandr Matrosov brought another chapter to the never-ending story of several interrelated malware families. This chapter delved more deeply into the Gapz family of malware, which had been downloaded by Trojans created by the PowerLoader bot-builder.

MAY continued the series of articles on Cdorked.A, begun by Pierre-Marc. Stephen Cobb offered clarification about the stealthy activity of this threat, which can still be detected by various means. Then Marc-Etienne M.Léveillé provided information about servers being affected with this malware in the wild, including those running Lighttpd and nginx – not just Apache. Finally, Stephen gave further context for Cdorked, and explained why Apache servers are so valuable to malware authors. He described a variety of threats that are found on these systems, and provided a roadmap for how to protect your systems against them. And lest folks on other operating systems felt left out, he also provided an expanded security roadmap for all to enjoy, including a variety of resources to help organizations find their way.

Aleksandr Matrosov returned with another thorough analysis of a complex, modular threat – this time, the Avatar rootkit. This threat is available for sale in the criminal underground, and like conventional software, offers an advanced programming interface (API) and a software developer's kit (SDK) that allows people to create additional modules to increase functionality. In the instance of this rootkit, it is unlikely to be a pleasant addition, from the perspective of the general public. This threat, like Jabberbot that was discussed in January, uses a novel C&C method. It coordinates its effort in Yahoo! Forum posts, making it especially difficult to cut off the bot's communication.

One malware trend in recent years has been specific targeting of victims, and in 2013 we saw numerous threats that target a single country or ethnic group. In May there were three articles pertaining to such threats targeting different countries. In the first, Jean-Ian Boutin examined the case of spyware seeking targets in Pakistan by purporting to be military secrets about the Indian armed forces. Alexis-Dorais Joncas discussed the Syndicasec family of malware that is found primarily in Nepal and China, and was spread by postings on Tibet-related blogs. And finally, Robert Lipovsky detailed the Sazoora malware campaign that was arriving in an email purporting to be from the Slovak Tax Office.

It can be a frustrating thing to see the effects of malware, day in and day out, and know that the Good Guys are "hampered" by things like laws and ethics, where the Bad Guys can simply do as they please. Some people seem to be more affected by this than others, and every now and again you will see someone suggest the possibility of aping techniques used by the Bad Guys for "good" reason. David Harley commented on the dangers of that approach in an article on proposals advocating the use of some techniques that are awfully similar to those used by ransomware, as a way to protect intellectual property.

JUNE brought us more discussion of targeted attacks: The first was an analysis by Jean-Ian Boutin of the OS X variant of the Tibet related malware campaign discussed earlier. One might think, with all these targeted attacks, it might be easier to find the culprit than with more prevalent malware, where the original source might get lost in the noise. Aryeh Goretsky reminded us that attribution is quite a tricky thing on the Internet. Even when the evidence could appear quite solid, it can be exceptionally difficult to rule out the possibility that evidence is being planted to divert attention from the true source.

Aryeh also bestowed upon us a white-paper that summarizes the first six month of Windows 8, from a security perspective. The newest version of the OS was a major departure from previous versions in many ways, and in some ways this has strengthened security. But on the other hand, it has also been clear how difficult this change has been for many people. They have been slow to upgrade and replacement "Start Menu" apps have become quite popular.

This month also brought several articles about security strategies, specific to the concerns of an increasingly mobile Internet population. Stephen Cobb looked at the prognosis for the future of telemedicine, given the current, questionable state of security in the healthcare industry. Stephen also imparted a list of tips for protecting home devices like smartphones and tablets, which many folks still view as impervious to malware. Of course, those devices seldom stay at home. David Harley discussed how difficult it makes central IT management, when people bring their own devices to work, despite the perceived increases in productivity due to improved connectivity.

JULY saw the third Critical Infrastructure Cybersecurity Framework Workshop take place in San Diego, organized by the National Institute of Standards and Technology (NIST). Stephen Cobb introduced the workshop, and its purpose of working with stakeholders to develop a voluntary framework to improve cyber security for critical infrastructure in the US. And afterwards, Stephen summarized the content and discussions within the workshop: Would the framework need to be mandatory and regulated in order to be taken seriously?

At the time of writing this article, Bitcoin value is hovering around $1000 USD. Such valuations have prompted the creation of many other, similar “crypto-currencies”. Malware authors have been stealing Bitcoin for quite some time, and they were aware of these alternate “coins” long before the general populace even became aware of Bitcoin. Indeed, malware called MSIL/PSW.LiteCoin.A was discovered to be attempting to steal Litecoin, as Robert Lipovsky explains. In this article he also mentions Scoinet, which is a Bitcoin stealer that uses Tor Hidden Services for its C&C functions. In a later article, Aleksandr Matrosov added further information about the increasing popularity of Tor for hiding and coordinating malware, analyzing two more bots that do so: the Atrax malware family, and Win32/Agent.PTA.

Harking back to the Cdorked problems that garnered so much attention earlier in the year, Darkleech similarly modifies server binaries on Apache systems, as Sebastien Duquette explains. But Darkleech adds several other modules, including a ransomware component. The Expiro virus and its variants likewise add new functionality to an older threat. Artem Baranov analyzed this change in its functionality, to include infection of 64-bit executable files along with its traditional 32-bit file infection.

AUGUST brought urgency to HIPAA 2.0 compliance efforts. Stephen Cobb laid out the importance of these new regulations and the penalties that had been imposed on those who did not comply with HIPAA 1.0 over the course of the previous year. And in a second article Stephen provided some statistics to give context to why data privacy is so important (and not yet adequately implemented) in the US healthcare industry.

Several researchers revisited the ongoing sagas of malware families we’ve analyzed throughout the year, as new details came to light. In the previous installment of the Avatar rootkit analysis, a question had been left open as to what the threat’s payload was, as some functionality was not available at the time of writing. Aleksandr Matrosov found the answer to this question, and described its self-defense tactics.

July’s article on Darkleech set the stage for a post by Jean-Ian Boutin analyzing the ransomware Nymiam, which is a component downloaded by the previous threat. But these are not the only two families tied together in this drama – Jean-Ian was able to tie this threat to a handful of other families that are working together. Similarly, Aleksandr Matrosov’s article on an update to Powerloader showed how malware authors have been utilizing leaked, malicious code to update the functionality of a variety of different families.

Toward the end of August, in an entirely unexpected and perplexing turn of events, the popular Orbital download manager was found to have code that allowed it to perform Distributed Denial of Service (DDoS) attacks against chosen websites. Aryeh Goretsky described the discovery of this strange new functionality.

Walking the line of ethics versus things like privacy, marketing and powerful functionality is a tricky thing for regular software vendors. This is true for security vendors too, and a small part of what AV vendors have done to combat this is to steer entirely clear of those individuals that have written malware. David Harley elucidated why this is doubly true now that most malware is written for financial gain.

SEPTEMBER began with a series of articles from Robert Lipovsky on a new, complex banking Trojan called Hesperbot that was targeting users in the Czech Republic, Turkey and Portugal throughout the spring and summer, and which ESET had previously been detecting generically. The threat was sent in emails that appeared to be an invoice or a postal notice, including an attachment that appeared to be a PDF file, which was in fact an executable file that would steal the banking credentials of affected users.

This was about the same time that the Cryptolocker Trojan had started making its initial appearance, frequently using a similar tactic of arriving in emails with ".PDF.EXE" files that appear to be delivery notices or invoices. These early variants of Cryptolocker were also detected generically, and as they started to become more prevalent, Robert described a big batch of different Filecoder Trojans that hold affected users' files for ransom. As Remote Desktop Protocol (RDP) is a common spreading mechanism for several of these Filecoders, Cameron Camp also offered instructions and advice for locking down this feature of Windows, so it is not open to the Internet at large.

After the fourth NIST Cyber Security Framework workshop in Dallas, Cameron Camp highlighted a topic from the discussions that took place there: Cybersecurity Insurance. This is a type of insurance that has been discussed for a long time but now both insurers and the insured seem to be getting serious, trying to establish what this coverage should entail. Unfortunately, NIST also appeared in the context of the NSA's role in shaping encryption standards. Stephen Cobb offered advice for businesses on reviewing their encryption needs in light of this information.

Have you ever wondered how it is decided, on a blog with moderated comments, why a comment might be rejected? David Harley went into this question, to clarify what details are generally considered. For instance, even if a comment is negative, is it constructive and respectful? That is definitely worth including. Conversely, even if a comment is positive, if its main purpose seems to be to point to some minimally relevant external link, it is liable to be excluded.

OCTOBER began with more commentary on the NIST Framework Workshop in Dallas, this time by Stephen Cobb. One of the questions that was discussed during the meeting was whether regulation would be more or less helpful to the cause of increasing the security of our critical infrastructure. By the end of the month, the Preliminary Cyber Security Framework (CSF) had been released for comment, and included a section on Privacy and Civil Liberties, as Stephen explained.

If one threat was to embody the trends of the year, it would have to involve a popular download manager with mysterious functionality, and some anti-analysis capability. This threat would also need to be specific to one particular country, and to download an Android OS component. Oh look! As Joan Calvet's analysis showed, Kankan has all that and more.

And speaking of converging threat tactics: As Jean-Ian Boutin reported, Nymiam switched from using the Blackhole Exploit Kit that was popular among many threat families throughout the year and beyond, to search-engine poisoning. When a user clicks on a poisoned search result, an archive is downloaded. Within that archive is an executable file with a name similar to the search terms used, often with the filename ending “PDF.EXE”, like Hesperbot and Cryptolocker. The end result of all this was a Lockscreen ransomware that purports to be a warning from the target user’s national police force, demanding $300 USD.

One of the highlights of the fall, at least in the anti-malware industry, is the annual Virus Bulletin conference. This year David Harley and I had the opportunity to present a paper on the difficulties of, and some possible solutions for, Mac security product testing. Both of us have been particularly interested in both third-party testing and Mac malware for quite some time. (This was David’s fourteenth presentation before this conference and he summarized some of the history that led up to this paper.)

One final note about October: my own inaugural post on We Live Security appeared. The global network service provider Akamai had released a report implicating Indonesia as their #1 source of malicious traffic. This surprised me, as I had not previously heard Indonesia mentioned as a major source of malware. But when I learned more about the nature and uses of the Internet in Indonesia, the statistics quickly began to make sense.

NOVEMBER brought more Snowden revelations about mass surveillance, and ESET looked at the effects these may be having. Stephen Cobb relayed news of the potential impact of the revelations with regards to corporate profit, as polls indicated that consumers now view the Internet and big technology companies as being less trustworthy. Around this same time, a coalition of digital rights advocates and academics also published an open letter to AV vendors, asking them a series of questions about detection of NSA malware. Andrew Lee presented ESET’s response to this letter, explaining (among other things) that ESET detects all malware, regardless of its source.

In case you thought things had gotten quiet with the development of the Gapz and PowerLoader Trojan families, Pablo Ramos caught us up on its new spreading mechanism that utilizes Skype, GTalk and other IM clients to spread. While this technique is not new, it is clearly still effective. This month also marked the 25th anniversary of another worm that was also surprisingly effective, and Sebastian Bortnik revealed five little known facts about this threat, which shows a number of ways the Internet has changed (and several ways in which it has not).

Special guest writer Graham Cluley expanded on the topic of how things have changed in malware, and how we must change our behaviors to deal securely with this new reality. Anti-malware products are now more than a simple program to protect one machine, but part of a global immune system that helps to protect the Internet as a whole.

Being part of an interconnected global community such as the Internet is not always wine and roses, and can make for genuinely scary scenarios for some people. In a pair of articles, I explored ways for people in those situations to better protect themselves. The first post was geared towards protecting privacy for survivors of domestic violence, and exploring the extreme difficulty of keeping one’s information from getting into the wrong hands. The second post was a guide for parents and other concerned adults, for helping keep kids safe from the dangers of online predators.

These examples bring up the question of who is responsible for online security and protection. Stephen Cobb discussed the results of a Harris poll that ESET commissioned on this topic. We asked people a variety of questions about who they believe is responsible for security and privacy online. The poll also looked at what actions people take to protect their own privacy as well as that of friends and family. With its focus on attitude to social media, this poll attracted national attention.

November also brought some security improvements within the major operating systems; both Windows and Mac OS X. Aryeh Goretsky introduced a new white paper that illustrates the most anticipated and controversial security improvements in the latest release of Windows, version 8.1. The latest version of Mac OS X, 10.9 – code-named Mavericks, offered a variety of security upgrades too, but I argued that the biggest improvement was that the upgrade was offered for free: The best security is that which actually gets used!

DECEMBER is a time for merriment and shopping in many parts of the world. Bloggers at We Live Security had holiday shopping on their minds as well. We noted that the world's best known online store, Amazon.com was considering a drone-based package delivery fleet. While this might allow for packages to get to some people more swiftly, the general consensus among bloggers was that this would lead to mayhem and hilarity. Cameron Camp pondered how paranoid, shotgun-toting folks in some parts of America might regard drone-based delivery services and brought that perspective to his analysis of the topic.

Big businesses are not the only ones thinking about winning more business during this, or any other time of the year. Stephen Cobb addressed one way for small businesses to compete more effectively for contracts by preparing a written information security program (or WISP). If you want to sell to larger businesses, taking this extra step could help you win out over your competitors. And in case you prefer to hear more on the topic, Stephen linked to his recent webinar on the subject.

All year long, we have focused on some rather complex, rapidly evolving threats, in part because that is what piques a researcher's interest. But complexity is not always the norm as far as malware is concerned. Even some targeted attacks are not always "advanced" threats, per se. Olivier Bilodeau introduced a whitepaper that focused on a handful of threats which managed to achieve their goals with the bare minimum of complication. Sometimes it simply is not necessary to include all the bells and whistles!

One of the most persistent threats faced by both consumers and companies is phishing. David Harley presented a comprehensive review of the subject in four parts available all-in-one as a handy paper titled The Thoughtful Phisher Revisited (PDF). And one of the most perennial topics on security blogs is predictions, of which Stephen Cobb provided a buffet. Our colleagues in Latin America went one better and provided an impresssive 35 page white paper of trend analysis and predictions for 2014.

Unfortunately, it looks like Cryptolocker is going to be around for a while, so I put together "11 things you can do to protect against ransomware, including Cryptolocker". Additional technical advice on protecting Windows and its many component pieces from exploitation by the bad guys was provided in considerable detail by another guest writer, Artem Baranov, Lead Virus Analyst for ESET's Russian distributor.

Sadly, criminals don't take holidays, and some ramp up their activities in the festive season. From Jean-Ian Boutin we learned that a banking Trojan called Qadars has been very active, infecting users throughout the world. Its modus operandi is banking fraud through web injection, using a wide variety of webinjects, some with Android mobile components.

Just as were getting ready to head for the hills for the holidays, independent cybercrime reporter Brian Krebs broke the news about a very high profile card heist. Our vigilant UK correspondent Rob Waugh, who has been providing regular security news coverage for We Live Security, jumped on the Target breach story and published helpful commentary from David Harley. The US press was quick to reach out to ESET experts for comment and I wrote a quick guide for those might be victims.

Finally, did you know that We Live Security has regular podcasts, in addition to webinars? Aryeh Goretsky reminded us to check out the weekly Malware Report, for brief discussions of current topics.

2013: a Scammer's Eye View

David Harley CITP FBCS CISSP ESET Senior Research Fellow

There are plenty of scams effective enough to rate a warning or three, in the hope of alerting potential victims to the kind of gambit they use. And so, even though much of ESET's business is focused on the bits and bytes of malicious software, I've spent a lot of time writing on WeLiveSecurity about tech support scams, phishing emails, 419s and so on. After all, while we see hundreds of thousands of samples of malware every day, a great deal of that (often very sophisticated) malicious code wouldn't get very far if it weren't for the sort of social engineering that persuades a victim to give away his credit card details, or visit a shady web site, or click on a malicious program.

Domain Name Scams

Back in 2012, Aryeh Goretsky blogged about domain registration scams in .ASIA domain name scams still going strong (and referred to several earlier related blogs –). While we haven't blogged again on the topic recently, a stream of comments throughout 2013 indicates a corresponding, ongoing stream of scam messages. Rather like this one, fresh from my ESET mailbox.

> (Mail to the brand holder, thanks)
>
> Dear CEO,
>
> Sorry to bother you inexplicably. We are a China's domain name registration supplier, and there is one thing we would like to confirm with your company. On December 4, 2013, we received an application form online from a company called "XinHua Trading Co.,Ltd" who wants to apply for some domain names and brand name related to **"eset"**. In order to avoid confusion and adverse impact on your company, we need to verify whether this company is a subsidiary of you or did you authorize them to register the related brand name and domain names? Currently, we have not formally accepted the application of that company, we need to get your company's confirmation. Please give us a timely response within 7 work days. So that we can better deal with this case. Thank you.
>
> Best regards,

Well, some will find it 'inexplicable' that this kind of scam is so successful: at least, we assume that it works often enough to make it worth the scammer's time. The social engineering in scams like this is two-fold. First of all, we don't know how often a company in China tries to usurp the branding of a Western company, but it's unlikely that every message like this is based on such an attempt. In fact the similar scams I first came back in 2004 were aimed specifically at clinical/healthcare organizations in the public sector in the UK, and there seems little scope for companies in the Far East to pass themselves off as hospitals or medical practices in the UK. Secondly, the scammer is not really asking "is it OK if we accept this application?" Further down the line, he's going to suggest that if you don't want them to accept the application from someone who doesn't have a right to the branding, you're going to have to buy the domain yourself. At this point, you'd expect a CEO (or whoever), even if they didn't recognize the scam as such, to refer it to the legal department or an outside lawyer, who would probably identify it as at best unnecessary. Does this happen? We don't really know: we only hear from people who know it's a scam, perhaps because they happen to read our blogs.

PC Tech Support Scams

I sometimes think I've been writing about tech support scams forever, though actually I first stepped into that particular mire in 2010. But there's still plenty of scammer action there, as evidenced by a further stream of comments on blogs such as Support desk scams: CLSID not unique, and some more recent blogs like this, which demonstrated some newer techniques and even a Mac-specific attack. Though it surprises me to get a call like the one I got (also) today from someone in an Indian call centre who was so busy talking to one of his mates that he couldn't even be bothered to deliver his spiel properly. After all, most examples of this kind of scam rely on the victim being taken in by the seriously improbable assertion that the scammer somehow has detailed knowledge of the victim's PC. The scammers would, you would think, be discouraged by having to keep ringing round the same diminishing circle of people who still haven't learned to recognize the scam. Yet somehow they keep going, and sometimes manage to find a halfway-convincing new angle (or two). Jerome Segura also came across some interesting approaches that I mentioned here, as well as back-linking to a very relevant article by Jean-Ian Boutin.

Darwin Awards for Scammers

It's not surprising that clever deception makes illegal, immoral profits, and the scam above is, from some of the comments we read, convincing enough to get an initial response from many potential victims. But sometimes it's reassuring to see that not every scammer displays the sort of IQ that makes fools of university professors and quiz kings. (Admittedly, Darwin notwithstanding, very few of them manage to precipitate their own permanent removal from the gene-pool, though it's not unknown for a criminal to end up in a holding cell due to indiscreet use of the Internet, as related in this story from 2009, where a burglar took time out to check his Facebook account on the victim's laptop: Hold the jemmy a second, I need to check Facebook.)

Here are three of my favourite more recent examples. For some reason, all three of them appear to come from westnet.com.au addresses, though they actually have a sort of minimalist 419 feel.

The first two are remarkable for the fact that they don't have a subject. Well, that'll grab your attention, won't it? Well, maybe not…

mibarberralphg2@westnet.com.au has a very straightforward request (or maybe he’s just thinking aloud?)

> I need a partner for biz

Minimalist, or what? I’m sure that most recipients will be desperate to find out what it’s about. Sadly, I wasn’t.

Mr. Leslie [schm.michh@westnet.com.au] is a little more talkative, once you get into the text body.

> Please contact me, we need to talk about Niclas.
>
> Leslie Mcintyre.

Sorry Les, I don’t think we do. Perhaps if I actually knew you, or someone called Niclas. But I’m pretty sure you’re just trying to catch my attention, and the scam will turn out to be another disappointing Advance Fee Fraud.

seaad1@westnet.com.au, however, goes the extra mile and tells us in the subject field that “I am waiting for your response”. Sadly, the effort seems to have exhausted him or her. The body text tells us that:

> I am waiting for your
> response
> I am waiting for your
> response

Yes, I think I get the message. Sadly, *you* won’t be getting one: at least, not from me.

Money Mules and Job Scams

chuoo@hotmail.com, however, is positively chatty. In a message with the subject “F.S.A” invites us enthusiastically to:

> Work with us to start your stable future.
>
> You're close to join a unique place and see inspirational things.
>
> If you are seeking for a challenging opening with a bright future, come work with us.
>
> We would like to offer you a new career of FSA which is untaken for now. Your CV was provided and reviewed by a recruitment agency. An opening that may fit your experience is being offered.
>
> Earnings:
>
> Your salary scale during the probationary period will be 1500 Pounds per month plus 8% commission from each transaction completed. Your total income could easily be about 2500.00 pounds. After the probationary period, your base wage will be 1800.00 Pounds per month, plus 8% commission.
>
> Employee Reimbursements (only after probationary period) Contain:
>
> - Wage plus bonus
>
> - Includes health and dental insurance
>
> - Paid Leave
>
> To apply for the F.S.A. position, please respond to hrdepartment.test@gmail.com.

Thanks,

Bobbi Power

HR Manager

A stable future? Very Christmassy….

FSA? We'll need to do a little guesswork here, since we aren't told which organization with the initials F, S and A is recruiting, which agency is acting on its behalf, or where or what the job is. Presumably in the UK, since the salary is in pounds, though in fact sterling is not the only pound currency. Oddly enough, Syria uses a Syrian Pound, though I suspect that we're not looking at recruitment by the Free Syrian Army. Or indeed the Football Supporters Association, since that was amalgamated into the Football Supporters Federation in 2002. The Financial Services Authority went the other way quite recently, its functions being split between the Financial Conduct Authority and the Prudential Regulation Authority, which is part of the Bank of England. So what does that leave us with? The Food Standards Agency? That doesn't seem likely, looking at the Agency's jobs page. And in general, HR departments for government agencies don't use Gmail as their email provider.

The real clue is in the job description, such as it is: the references to 'transactions' and 'commission', and the lack of other detail about what these transactions consist of, strongly suggest that if there was a job title, it would be money mule. Around ten years ago, email messages offering what was – to all intents and purposes – payment for money-laundering were very common and often quite innovative, with carefully-constructed backlinks to sites closely resembling those of real companies. In a paper Andrew Lee and myself wrote a few years ago, we pointed out the close relationship between phishing and moneylaundering.

> Phishing gangs are part of a complex "black economy" similar to other commercial models … This "economy" entails a number of roles and functions …
>
> …The victim's credentials are converted to cash. The buyer uses the stolen credentials, for instance to buy goods for sale on the black market, or to negotiate loans and mortgages…
>
> …Important to the phishing economy are mule recruitment solicitations, offering "financial management" or "financial agent" jobs that boil down to receiving money and passing it further up the chain after taking a cut as commission.

YARD SCRAPER, INC. SOUTH AFRICA
Head Office: 131 Braamfontein,
Midran-Johannesburg
2050 South Africa

Good Day

I am Mr. Kelvin Powell, President/CEO of Yard Scraper, Inc. South Africa (a company based in the South Africa). A Company that is specialized in import and export of industrial and domestic machinery & equipment, communication accessories and household appliances.

We also deal on mechanical equipment, hardware and minerals, electrical products, medical & chemicals, light industrial products and office equipment, and export into America, Asia and Europe, therefore being a General Mercantile Company.

We currently run our business from America, Asia and Europe but I will be communicating with you from our South Africa Office where I am currently located for now. We are searching for representatives who can help us establish a medium of getting to our customers in America, Asia and Europe as well as making payments

> through you to us. Please if you are interested in transacting business with us we will be most glad to be your partners.
>
> My company is willing to offer you 10% of every payment that comes in
> through you to us. If you are interested, kindly forward to us the
> following information through my private email (infoyardscrapercompany@jmail.co.za):
>
> Full Names
> Company Name
> Telephone & Fax Numbers
> Full contact addresses
> Age
> Sex
>
> Please note that your area of specialization or occupation is of no relevance to resolve to assist us.
>
> Thanks in advance.
> Sincerely.
> Kelvin Powell
> President/CEO of Yard Scraper, Inc.

> Funds transfer/money-laundering scams don't generally purport to come from the same type of institution that phishing scams do, and aren't aimed at cleaning out the victim's accounts: they are more concerned with using the target as a "money mule." They advertise "jobs" via email and recruitment web sites to people prepared to act as their local agents. The mule is often required to open new legitimate accounts with specific financial institutions so as to facilitate moving funds from a phished account with the same institution. The scammer may go to extreme lengths to make the mail look like a serious job offer, backed up by a large and complex web site.

However, these things haven't dried up. In an article on Irish unemployed baited by online scammers, Urban Schrott of ESET Ireland, published a blog post on those cold-hearted individuals who prey on jobseekers. (No, I mean scammers, not the government.)

It's all too common for job offers to turn out to be some form of 419 or other Advance Fee Fraud (AFF) or a poorly paid work-from-home job. However, Urban also quoted an email that looks like a particularly unpleasant variation, where the job offered consists of participating in money laundering as a money mule. Unpleasant, because it's possible for a naive victim to believe they're working for a legitimate company and not realize that they're breaking the law until the police come a-knocking.

Plenty More Phish in the Sea

I won't be discussing phishing scams further in this article, as that's an area I've covered quite comprehensively in 2013 over two blog series – here and here – and some individual articles such as this one, about a paper that aims to profile the victims most likely to fall for a phishing attack. (It's less clear is how you develop a profile while avoiding the pitfalls of stereotyping.)

Mugs, Muggings, and False Friends

My colleagues at ESET Ireland reported this year that an all-too-familiar scam was currently hitting Irish mailboxes. I've talked about 'Londoning' at some length here previously – for instance here and here – but here's a quick summary abstracted from a longer account.

> Someone, apparently someone you know (a friend or a family member) contacts you to tell you that they've been stranded without money abroad somewhere, usually after being mugged at gunpoint. At one time, Americans were frequently being contacted in this way by friends or relatives

> apparently in London, which is why the scam is sometimes referred to as Londoning or The London Scam, though potential victims in the UK were more likely to hear that the mugging victim was somewhere more exotic, like Lagos. And, of course, they need you to send you some money.

Here's a more recent example, mailed with the subject "Unbelievable...Urgent Help!"

> I hope you get this on time, I made a trip to Manila(Philippines) and had my bag stolen from me with my passport and personal effects therein. The embassy has just issued me a temporary passport but I have to pay for a ticket and settle my hotel bills with the Manager.
>
> I have made contact with my bank but it would take me 3-5 working days to access funds in my account, the bad news is my flight will be leaving very soon but i am having problems settling the hotel bills and the hotel manager won't let me leave until i settle the bills, I need your help/LOAN financially and I promise to make the refund once i get back home, you are my last resort and hope, Please let me know if i can count on you and i need you to keep checking your email because it's the only way i can reach you
>
> Regards,
>
> Farrell

Well, 'unbelievable' it certainly is. Not only because of the logical flaws in the story and the inconsistent textual tone, but because this particular example was sent to everyone on a security list. Nice targeting, Farrell. ☺

Dial 419 for more Misinformation

So-called 'Londoning' or 'Stranded in London' scams (of course, they aren't by any means associated *only* with London) are often assumed to be an offshoot of the 419 (Advance Fee Fraud) school of scamming particularly associated with West Africa, especially Nigeria. 419s have featured in my articles for ESET and elsewhere for many years (and not a few in 2013) but as I plan to return to that theme in the very near future in another blog, I won't discuss it at length now. However, there are some ESET papers you might find of use and/or interest:

- Whatever Happened to the Unlikely Lads? A Hoaxing Metamorphosis
- Common Hoaxes and Chain Letters
- The Spam-ish Inquisition

Other Scammer Snapshots

It would be perfectly feasible to spend the year blogging on scams and scamming, and still miss quite a lot of interesting examples. Since my work and interests go far beyond scamming (fascinating though I find the topic, in terms of both the criminal psychology and the victimology), I can't claim to done much more than scratch the surface. Still, a few interesting examples of other scams did catch my attention.

- A variation on the Mystery Shopper scam that misuses the Pinecone Research brand.
- An invite to a conference in California proves to be a

scam, and a very similar spam claims the very same conference is taking place in New York in March.

- A closer look at job scams.
- An idea we had for setting up a link for educating people who can't resist on clicking on dubious links. (Hat tip to Righard Zwienenberg.)
- An article on academic publishing scams (expanded from one originally published on the Anti-Phishing Working Group's eCrime blog).

And here are my two favourite end-of-the-year spams. The first is from g3jbxyo8zk{at}myway.com. (Is that a Welsh name?)

The subject consists of the word "Diploma?" The body text consists of the same word (and question mark) plus a shortened URL. Thank you, g3, but I have all the diplomas I need at this point, thank you. (Actually, I plan on shedding some in the near future, but that's for a completely different article.)

And here's a delightful phishing message,

> HM Revenue & Customs
>
> **Tax Refund Confirmation**
>
> You are eligible to receive a tax refund of 868.50 GBP. Please submit the tax refund request and click here by having your tax refund sent to your Credit Card Account in due time.
>
> Please **continue here** to have your tax refund sent to your Credit Card Account,
>
> Note : A refund can be delayed for varieties of reasons, for example submitting invalid records or applying after deadline.
>
> Best Regards
> HM Revenue & Customs

I'd like to think that most people in the UK would find this slightly suspicious.

- Not just because it comes from the not-very-authentic sounding official email address info@hm.mobi, rather than a more convincing hmrc.gov.uk address. (Of course, a message like this could have the headers spoofed to look as if it came from the real HMRC, so such an address doesn't prove the mail is genuine.)
- Not just because it doesn't seem logical for Her Majesty's tax-collectors to be asking for credit card details: it's not as though people are likely to pay their income tax by credit card. Of course you don't have to hand over your login credentials in order to allow someone to pay money to your bank account, so your barebones bank account details are less useful to a scammer.
- Not just because the English is slightly off.
- And despite the quite authentic-looking

HMRC logo at the top of the message.

But the idea of Her Majesty's professional cheeseparers and official bloodsuckers offering an unprompted tax rebate is just so unlikely, that I think many people would already be laughing at the subject line 'Tax Refund Security Confirmation'.

ESET Corporate News

ESET Releases Annual Threat Trends Predictions for 2014: The Challenge of Internet Privacy

ESET has released its annual predictions for the threatscape in the upcoming year "Trends 2014 - The Challenge of Internet Privacy". This year, in wake of revelations of Edward Snowden related to the US National Security Agency (NSA), the main topic focuses on the growing concern expressed by users regarding their online privacy. The report is specifically elaborating on three main areas of trends for 2014:

- Loss of privacy and mechanisms to improve protection on the Internet.
- Computer threats for Android OS.
- Other: new spread of malicious code in form of ransomware (e.g. filecoders like Cryptolocker); vulnerabilities in Java, ever-present and more complex botnets.

Advanced Banking Trojan "Hesperbot" Which Can Steal Bitcoins, Has New Targets: Germany and Australia

ESET HQ malware research lab has reported new campaigns of the very effective banking Trojan Hesperbot. As previously uncovered by ESET, Hesperbot is using very credible-looking spreading campaigns related to trustworthy organizations and lures victims to run the malware. Based on ESET LiveGrid® data – ESET's cloud-based malware collection system – and research analysis, it has new big targets: banks and users in Germany and Australia. Meanwhile, large infection waves continued in the Czech Republic. Read more also in the *New Hesperbot Targets* WeLiveSecurity.com article by Robert Lipovsky.

Banking Trojan Qadars Targets Users in the Netherlands, France, Italy

ESET Canada malware research lab has recently analyzed a very active banking Trojan dubbed Qadars which is targeting users especially in the Netherlands (75% of detected infections; among other targets are France, Italy, Canada, India and Australia). Qadars uses a wide variety of webinjects, some with Android mobile components that are capable of bypassing two-factor authentication systems of online banking to gain access to user's bank account. Read more also in the *Qadars* WeLiveSecurity.com article by Jean-Ian Boutin.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1

Percentage Detected: 3.96%

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: 2.21%

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: 2.02%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

4. INF/Autorun

Previous Ranking: 4
Percentage Detected: 1.97%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case.

5. HTML/ScrInject

Previous Ranking: 5
Percentage Detected: 1.86%

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

6. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.52%

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.

7. Win32/Dorkbot

Previous Ranking: 6
Percentage Detected: 1.46%

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.

8. Win32/Ramnit

Previous Ranking: 9
Percentage Detected: 1.45%

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.

9. Win32/TrojanDownloader.Wauchos

Previous Ranking: n/a
Percentage Detected: 1.11%

It is a trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer IP address. Then, attempts to send gathered information to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

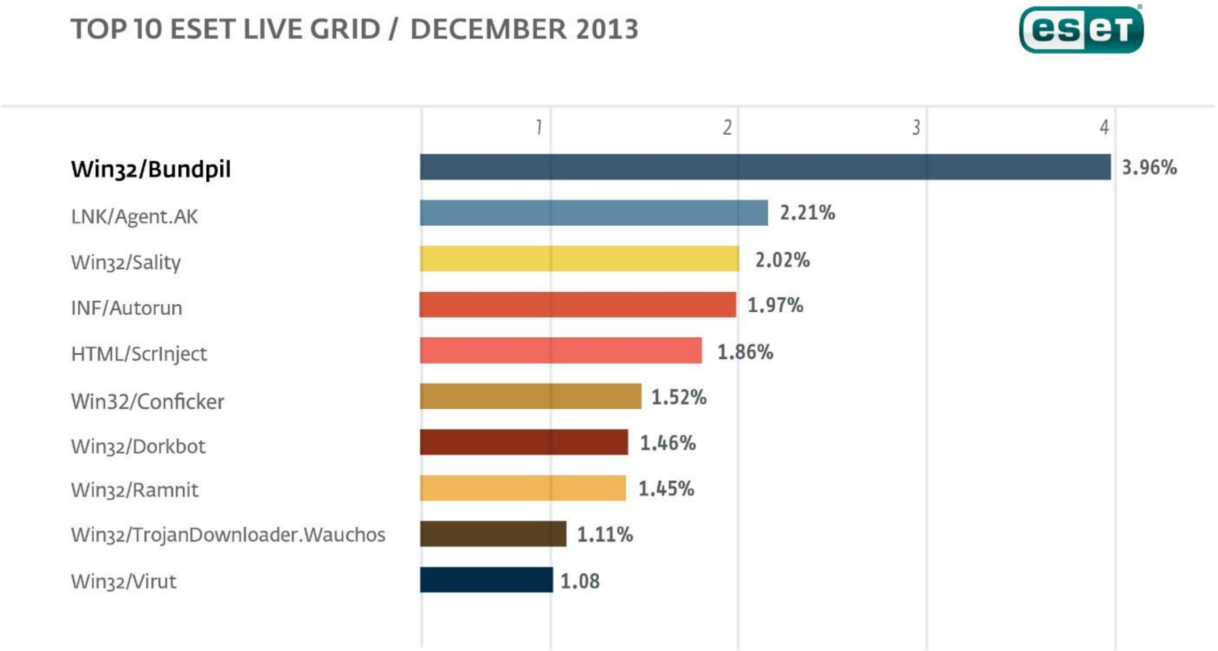
10. Win32/Virut

Previous Ranking: n/a
Percentage Detected: 1.08%

Win32/Virut is a polymorphic file infector. It affects files with EXE and SCR extensions, by adding the threat itself to the last section of the files source code. Aditionally, it searches for htm, php and asp files adding to them a malicious iframe. The virus connects to the IRC network. It 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 almost 3.96% of the total, was scored by the Win32/Bundpil class of treat.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- ESET Blog (also available at welivesecurity.com)
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation

eset ENJOY SAFER TECHNOLOGY™