The Year of Surviving Dangerously

Highlights from We Live Security 2013

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.

Lysa Myers
ESET Security Researcher III