TRENDS 2017: SECURITY HELD RANSOM

ENJOY SAFER TECHNOLOGY™

INDEX

Introduction

For several years, the research team at ESET has been issuing its Trends report, which provides a review of the latest and most significant developments in information security, and presents the key topics of relevance for businesses and users for the upcoming year.

Our analysis of the current state and evolution of technology reveals one aspect that stands out: more and more devices and technologies mean greater challenges when it comes to maintaining information security, regardless of the area of implementation. This leads us to the conclusion that security must be considered at every level, and for this reason, our Trends 2017 report covers a diverse array of issues.

Among all of these, we've decided to talk about the changing outlook around the reporting of vulnerabilities. The fact is, year after year, the number of critical vulnerabilities reported has not fallen, but has instead remained constant or has even shown a slight increasing trend. This highlights the need for manufacturers and developers to further commit to the secure development of information products and services.

In addition, the ever increasing frequency of attacks on large infrastructure and internet services puts discussion of critical infrastructure security back on the table – a theme that has its own special chapter given the sensitivity of this issue. Likewise, we chose to give special attention to the safeguarding of information in the healthcare sector. Throughout that section we present the challenges faced in an industry, which handles very sensitive and critical data and has thus become the target of many attacks.

Linked to the previous points, and to many of the themes we develop in different sections of this report, is legislation regarding security and technology. Meriting a chapter of its own, it is an issue with numerous implications and a matter of fundamental importance that must be undertaken by governments of every country. However, not only is it essential for governments take on this task, but that they also address the challenges of forging agreements with both the private sector and with individuals in their double roles as users and citizens.

It is not just these macroscale issues that pose a challenge for the coming year, but also the problems associated with everyday technological activities, such as mobile device threats or the Internet of Things (IoT). This is nothing new; in fact, it is something we have been talking about since 2012 when we began to see growth in the number of new families of Android malware, and a year later, the appearance of the first malicious codes that affected Smart TVs and other smart devices. This year however, and given the growth of ransomware, we have discovered a new trend on the horizon: the Ransomware of Things or RoT, i.e. the possibility of cybercriminals "hijacking" a device and then demanding a ransom payment in exchange for restoring control to the user.

With regard to the evolution of mobile device threats, the security challenges for the coming year are numerous. Hence, we have provided a review of these throughout the corresponding section. Is the app distribution model really the most suitable? How can the secure development of applications be achieved in the context of incorporating other technologies, such as augmented reality and virtual reality, on

these increasingly powerful devices? Why are security controls not advancing at the same rate?

While video game consoles could be included in the IoT category, we believe they deserve a chapter of their own. This industry has taken on increasing significance and contains a broad spectrum of users with devices that have great processing capacity, which makes them an attractive target for cybercriminals. If we add to that the integration of game consoles with desktop environments, then it highlights the need to talk about security with that particular audience because it involves new attack vectors.

With regard to the corporate environment, it is worth mentioning that the increase in virtualized processing solutions has come to the attention of attackers who seek to violate the security of this type of infrastructure. Therefore, it is likely that we will see an increase in this type of threat, and thus the need to treat these issues as a security trend that systems administrators will face with increasing frequency.

The trends we present in this report don't only have to do with risks and threats; it is also important to underline something else that has been happening in the security industry. This has to do with a new generation of protection tools with a commercial strategy that ignores the development and evolution of security tools in general. Given the importance of this subject, and to avoid confusion, we took on the challenge of demystifying and clarifying what has until now constituted "next-gen" security solutions.

There is a common thread among all these sections and, in general terms, in all matters related to information security: user education and awareness. The speed at which new technologies emerge, reports of attacks, families of malware or security flaws of global impact, make security an ever more important challenge for businesses, governments and users around the world. At the same time, education and awareness on security matters have become increasingly important in order to stop threats from advancing. Throughout the corresponding section, we review the different problems associated with this issue and show that user education is not in step with the pace of new technologies and the threats associated with them.

It is our pleasure to present the report we have prepared at our global ESET Research Laboratories to address the challenges that must be faced with regard to security issues at all levels in 2017. Our idea is for you to enjoy the entire report, to just read about those issues that most interest you or that you identify with in your everyday lives as users.

Finally, we aim to inform readers about what's on the horizon as far as security goes, ensuring that they will be better prepared to tackle the associated challenges and thus be better protected.

RoT: Ransomware of Things

- How ransomware is evolving and could potentially take over every single device?
- Jackware + IoT
- How ransomware family evolved and what to expect

AUTHOR

Stephen Cobb
ESET Senior Security Researcher

1

RoT: Ransomware of Things

One of the trends that I found most worrying in 2016 was the willingness of some humans to participate in the following three activities at scale: hold computer systems and data files hostage (ransomware); deny access to data and systems (Distributed Denial of Service or DDoS); infect some of the things that make up the Internet of Things (IoT). Sadly, I think these trends will continue in 2017 and there is potential for cross-pollination as they evolve. For example, using infected IoT devices to extort commercial websites by threatening a DDoS attack, or locking IoT devices in order to charge a ransom, something I like to call jackware.

Past and future threats

Abusing information systems to extort money is almost as old as computing itself. Back in 1985, an IT employee at a US insurance company programmed a logic bomb to erase vital records if he was ever fired; two years later he was, and it did, leading to the first conviction for this type of computer crime. Malware that used encryption to hold files for ransom was seen in 1989, as David Harley recounts. By 2011, locking computers for a ransom was "stooping to new lows" as my colleague Cameron Camp put it.

So how might these elements evolve or merge in 2017? Some people have been referring to 2016 as "The Year of Ransomware" but I'm concerned that a future headline will read: "The Year of Jackware." Think of jackware as malicious software that seeks to take control of a device, the primary purpose of which is not data processing or digital communications. A good example is a "connected car" as many of today's latest models are described. These cars perform a lot of data processing and communicating, but their primary purpose is to get you from A to B. So think of jackware as a specialized form of ransomware. With regular ransomware, such as Locky and CryptoLocker, the malicious code encrypts documents on your computer and demands a ransom to unlock them. The goal of jackware is to lock up a car or other device until you pay up.

A victim's eye view of jackware might look like this: on a cold and frosty morning I use the car app on my phone to remote start my car from the comfort of the kitchen, but the car does not start. Instead I get a text on my phone telling me I need to hand over X amount of digital currency to re-enable my vehicle. Fortunately, and I stress this: jackware is, as far as I know, still theoretical. It is not yet "in the wild".

Unfortunately, based on past form, I don't have great faith in the world's ability to stop jackware being developed and deployed. We have already seen that a car company can ship more than a million vehicles containing vulnerabilities that could have been abused for jackware: the Fiat Chrysler Jeep problem that was all over the news in 2015. Just as serious as those vulnerabilities was FCA's apparent lack of planning for vulnerability patching in the vehicle design process. It is one thing to ship a digital product in which 'holes' are later discovered – in fact, this is pretty

much inevitable – but it is a different and more dangerous thing to ship digital products without a quick and secure means of patching those holes.

While most "car hacking" research and discussion centers on technical issues within the vehicle, it is important to realize that a lot of IoT technology relies on a support system that extends well beyond the device itself. We saw this in 2015 with VTech, a player in the IoCT space (as in Internet of Children's Things). Weak security on the company's website exposed personal data about children, reminding everyone just how many attack surfaces the IoT creates. We also saw this infrastructure issue in 2016 when some Fitbit accounts had problems (to be clear, the Fitbit devices themselves were not hacked, and Fitbit seems to take privacy seriously). Also this year, bugs discovered in the online web app for BMW ConnectedDrive, which connects BMWs to the IoT. For example, you can use it to regulate your home's heating, lights, and alarm system from inside your vehicle. The possibility that the features and settings of an in-vehicle system could be remotely administered through a portal that could be hacked is unsettling to say the least. And reports of vehicular cyber-insecurity keep coming, like this Wi-Fi enabled Mitsubishi, and hacked radios used to steal BMWs, Audis, and Toyotas.

While I originally thought of jackware as an evolution of malicious code targeting vehicles, it was soon clear that this trend could manifest itself more broadly, think: the Ransomware of Things (RoT). A chilling story from a city in Finland shows one direction that this might take (DDoS attack halts heating in Finland amidst winter). While there was no indication of ransom demands in the reports, it does not take much imagination to see this as the next step. Want us to stop DDoSing the heating system? Pay up!

Stopping the RoT

To stop the IoT become home to the RoT, a number of things need to happen, in two different spheres of human activity. First is the technical sphere, where the challenge of implementing security on a vehicular platform is considerable. Traditional security techniques, like filtering, encrypting, and authenticating can consume costly processing power and bandwidth, adding overhead to systems, some of which need to operate with very low latency. Security techniques like air-gapping and redundancy could potentially add significantly to the cost of vehicles. And we know that controlling costs has always been critical to car manufacturers, down to the last dollar.

The second sphere where action is required to stop the RoT is policy and politics. The outlook here is not good because so far the world has failed abysmally when it comes to cybercrime deterrence. There has been a collective international failure to prevent a thriving criminal infrastructure evolving in cyberspace, one that now threatens every innovation in digital technology you can think of, from telemedicine to drones to big data to self-driving cars. For example, as alluded to in *Challenges and implications of cybersecurity legislation* and its implications, concerned politicians failed to pass legislation in 2016 that would help secure the smart grid, despite bipartisan support.

To be clear, terms like RoT and jackware are not intended to cause alarm. They symbolize things that could come to pass if we do not do enough in 2017 to prevent them from becoming a reality. So let me end with some positive developments. First, a variety of government agencies are stepping up their efforts to make the IoT more secure. In 2016 we saw publication of the Strategic Principles for Securing the

Terms like RoT and jackware are not intended to cause alarm. They symbolize things that could come to pass if we do not do enough in 2017 to prevent them from becoming a reality.

Internet of Things [PDF] from DHS (US Department of Homeland Security), and NIST Special Publication 800-160 [PDF]. The full title of the latter is *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. NIST is the National Institute of Standards and Technology, part of the US Department of Commerce, and over the years the agency has exerted a positive influence on many aspects of cybersecurity. Hopefully, these efforts, and the many others around the world, will help us make progress in 2017 towards securing our digital lives against those who choose to abuse technology to extort us.

Finally, evidence that we might be making some progress, at least in terms of public awareness of the potential for the IoT to bring problems as well as perks and productivity gains, comes from a different kind of publication, the results of an ESET consumer survey. Reported under the title of "Our Increasingly Connected Digital Lives" the survey revealed that more than 40 percent of American adults were not confident that IoT devices are safe and secure. Furthermore, more than half of respondents indicated that privacy and security concerns had discouraged them from purchasing an IoT device. Could the combination of consumer sentiment and government guidance lead companies to make the IoT more resistant to abuse? We may find out in 2017.

Security education and social responsibility

- IT Security education should be on every level of society: school, university, companies, governments, etc.
- Passwords: When are we going to stop letting password security be based on users' moods.

AUTHOR

Camilo Gutiérrez
Head of Awareness and Research at ESET Latinoamérica

Security education and social responsibility

There is a threat that has been among us for many years and 2016 marked the 2nd decade of its spread via email. Millions upon millions of online users have encountered it, but despite many being able to recognize it, the reality is that there are still people who can be deceived by it. For some it occurs out of naivety and ignorance, for others out of simple curiosity, wanting to see what will happen. In the end, they are ensnared.

In case it is not yet clear what I'm talking about it, let's unveil the mystery: it is the infamous "Nigerian scam" or "419 scam". This type of fraud goes back to the aftermath of the French Revolution and probably much earlier, with letters offering to split a lucrative treasure. However, this centuries-old scam, far from disappearing, has gained strength with technologies advance and, over time has spawned many variants which eventually migrated to email. Scams that are based on offering something for nothing, but turn out to require some form of advance payment -in return for empty promises of future reward- are often referred to as Advance Fee Fraud.

Still, after so many years, one still sees messages on social networks and websites with the same type of ploy: "You are visitor number 1,000,000!", "You won the lottery!", "You have been selected for a dream holiday trip!", etc. …. These are just a few examples of the bait offered. But why, as computer threats have continued to evolve to the level of sophistication we now see in terms of targeted attacks, cyber warfare and APTs, have these types of scams remained so successful? The simplest answer is that people still remain vulnerable to psychological manipulation and social engineering.

The threats are changing, but propagation remains unchanged

Just five years ago, in our Trends for 2012 report [PDF], we talked about the growing trend of malware in mobile devices, spearheaded by threats such as botnets. In more recent years, these risks have continued to increase. We are seeing increases in cyber-espionage, targeted attacks and privacy threats. Previous concerns about the potential to leverage large numbers of poorly-secured IoT devices into actual attacks have been realized; furthermore, we believe that in 2017, the number of annual victims of ransomware will continue to rise.

All of these types of threats, which have been evolving over time, have one thing in common: the point of entry is often the user. Attackers continue to entice victims into naïve – and in many cases, irresponsible (albeit unknowingly) – behavior with deceptive emails and messages on social media, as well as booby-trapped USB devices left in car parks, all aimed at tricking them into compromising the safety of their own systems.

Unfortunately, this reality will continue to persist throughout 2017 and beyond, and

attackers will continue to take advantage of it. Despite the potential vulnerabilities in hardware and software that could allow an attacker to take control of a system, the simplest way to do so is through tricking its users. Why invest hours in creating an exploit when a simple email can provide the same type of access to such systems? From another perspective, why would thieves make the effort to dig a tunnel to break into a house when they could just ring the doorbell?

Cybercrime: ruthless and efficient

It seems likely that 2017 will see the continuing evolution of different types of malicious code, that ransomware will continue its infamous reign as the fastest growing threat, and that more IoT devices will be targeted for a broader range of cybercriminal activity. Cybercriminals are becoming increasingly ruthless, to the point that even industries such as healthcare are being attacked, and infrastructural components such as ATMs (cash dispensers) are continually targeted by attackers.

Furthermore, in 2016 it became clear that modern cybercriminals come armed not only with different types of malicious software and social engineering techniques, but also with "business plans" for extortion and extracting some sort of financial gain from their victims.

We have reached the moment where we need to stop talking about security risks in generic terms. It is critical that users, whether corporate or individual, are aware of the types of attacks that can affect them. From email fraud to information theft – all must be considered plausible, and it is important to take the necessary measures both in terms of technology and raising awareness, in order to avoid them.

Education is not just a matter of age

Two types of players inhabit the digital world: the natives, and the immigrants. The former has incorporated use of technology into most aspects of their lives from an early age. The latter, on the other hand, use technology to carry out many of their daily activities despite having had to adapt and make adjustments in order to do so.

One would hope that the digital natives would be less susceptible to these types of scams. However, this year a study by the BBB Institute showed that young people between age 25 and 34 are more susceptible to scams, whereas other studies [PDF] show that the youngest users are those who exhibit the riskiest behavior when it comes to surfing the Internet. They might connect to poorly secured Wi-Fi networks, plug in USB devices given to them by others without taking elementary precautions, and make little use of security solutions.

On the other hand, while digital immigrants can often be more cautious when it comes to using technology, we find that they too can often be the victims of attacks or engage in unsafe behavior. Generally, this is due to a lack of knowledge of the security characteristics of devices, or a lack of information regarding the scope of computer threats and the care that they should take to help avoid them.

In short, when it comes to protection, age does not matter. The need for all users to be aware of the many threats, the ways in which they operate, and the best options for protecting their devices, are all points on which users should be focused in order to stay safe.

The current paradox: the more we know, the less safe we feel

There is no doubt that today, four years after the Snowden revelations, people continue to feel increasingly at risk as concerns their personal data. The paradox is that in reality, there is more information about what is happening with their data than ever before.

The feeling of being monitored is a big concern for many users and recognition of the reality of global surveillance is one of the most important lessons to be learned from the Snowden revelations: if someone is authorized to act covertly and is given a large enough budget, it cannot be assumed – regardless of how good a person they may be – that they will do so properly, ethically and without negative repercussions.

Having said that, neither should we give way to out-and-out paranoia or stop connecting to the Internet altogether. An important challenge we face is the need to educate ourselves about how to be protected online, what types of information to publish, and which measures will ensure that information remains safe and private.

Small changes can make a big difference

At ESET we firmly believe that security is not only a matter of technological solutions, but that there is also a human element to protection. While ongoing efforts to build awareness in terms of computer security exist in many areas of our modern lives, many computer users still do not have sufficient training on this topic. In addition, while many recognize the threats faced by what they see as 'real' computers, they do not have the same awareness when it comes to their mobile devices and even less with regard to their IoT devices.

In 2013, it was estimated that the ratio between the number of mobile devices with a security solution installed and the number of global connections from mobile devices was 4.8%, and by 2018 it is estimated that this ratio could reach 15%. Although this represents a tripling in five years, meaning fewer than one in six smart phones and tablets is running security software.

In the coming years we will continue to see threats spread to all types of devices that are connected to the Internet and which handle sensitive data. Therefore, it is vital to be aware of security at all times and in all contexts, from personal devices with a Wi-Fi connection, to critical infrastructure that are connected and remotely controlled via the Internet.

The reality is that all technologies evolve quickly, and increasing there are means of infestation — means by which attackers can easily take advantage — if users are not educated about them. We cannot allow advances in technology to be turned against users.

In 2017, the trends in terms of protection must keep pace with the realities of extant security incidents. This is why education is vital. If users come to recognize that using passwords as the sole means of online access presents a security risk to their personal data, then they can also recognize that using two-factor authentication, which adds a significant extra layer of security, will tilt the odds back in their favor. The challenge, in addition to enabling them to recognize the threats, is to arm them with security tools that help them keep their information safe and secure. In the absence of such tools, the continued growth of threats and attacks is all but guaranteed.

An important challenge we face is the need to educate ourselves about how to be protected online, what types of information to publish, and which measures will ensure that information remains safe and private.

Likewise, the best way to guarantee the confidentiality of information is to make use of encryption technologies for all forms of communication. As for ransomware, the best way to protect yourself from permanent loss of personal information is having a proper – including offline – backups of the most sensitive or important data.

However, the adoption of these technologies in the coming year starts by acknowledging the threats, which can only happen if there is a base of users who are educated and able to determine what they should be protecting themselves from, and thus the best way to protect themselves.

Education makes the difference

For all of us working in the world of information security, no maxim has proven truer than that which says the weakest link in the chain is the end user.

We have been warned since at least 2015 that there is an increasing volume of information technologies to defend, but the number of people who are skilled enough to make sure of that defense is dangerously low. We must therefore adopt education as the fundamental factor [PDF] that makes the difference. Given that the whole process of training new professionals to work in information security will not happen immediately, the focus over the next few years should be on building awareness among users of basic Internet security measures, since they are the critical mass that attackers take advantage of to score wins.

So, the big challenge for those of us who are responsible for security is to turn ourselves into the first line of defense of information. Educating users regarding current threats and how they spread can make all the difference in reducing the impact of cybercrime in the future. We should not forget that security is the responsibility of everyone and not exclusive to those of us working in IT. These days, information is equally critical whether handled by a reporter or by an executive. The issue becomes even more sensitive when it concerns healthcare professionals and the medical records they handle on a daily basis.

To turn the tide, active participation by governments and companies is necessary. We have reached a point at which education on security issues must be handled in a formal manner, and companies should not simply relegate these issues to be covered as a one-off when inducting new employees. It must be a continuous and ongoing effort. End users must feel they are a part of the entire security chain and must understand firstly, that these threats do exist, and secondly, that the necessary mechanisms to use technology securely also exist.

Mobile security

the reality of malware... augmented?

- Pushing the limits of perception
- Vulnerable apps with unsafe APIs
- Android: an insecure system?
- Malicious apps in official markets
- Easily updated
- Mobile platforms under attack

AUTHOR

Denise Giusto Bilić
ESET Security Researcher

Mobile security: the reality of malware… augmented?

Originally, it was expected that mobile devices would evolve to become handheld computers with capabilities similar to any desktop. It is clear today that our smartphones and tablets have evolved beyond this point, creating new means of technological interaction not previously imagined.

Within the context of socio-technological revolution, the rise of virtual reality technology raises new security risks not only to digital information, but also to users' physical well-being. While these applications collect and store increasingly sensitive data, mobile malware is constantly evolving and becoming more complex, reinforcing the importance of, and need for, secure mobile technology. Given the large number of potential victims, the official app markets are struggling to withstand new barrages of malicious code attempting to infiltrate their trenches.

Does this scenario reflect what awaits us in terms of mobile security trends? Throughout this article, we will discuss how these risks might develop in the near future.

Pushing the limits of perception

Prior to the emergence of Pokémon GO, augmented reality (AR) had never been experienced by so many people previously outside the gaming community, and this has placed the technology at the forefront of mobile trends. At the same time, it is increasingly common to see people using virtual reality devices, thanks to projects such as Google Cardboard, which helped to popularize the concept among the public by making it more accessible.
The success of Pokémon GO in particular has spurred greater interest in AR in general, making other, future AR applications attractive to cybercriminals seeking to inject them with malicious code, and then distributing their creations through malicious servers, hacked sites, unofficial stores and even official app markets.

At the time of writing we are seeing the first public engagement with *Father.IO*, a mobile application that combines augmented and virtual reality in a multiplayer war game. It is likely to be a success in the coming year. Users should try their best to avoid malware impersonating the genuine app, its installation software or user manual.

These technologies pose new security risks, together with other mobile dangers that we mentioned in our **Trends 2016** report [PDF], such as the spread of malware and increasing numbers of vulnerability issues. When the players, as physical entities, become variables in the game, not only must we worry about protecting data on their devices, but also about the safety and security of the players themselves.

Common sense—or the lack of it—will play a crucial role in physical security. We have witnessed cases of people trying to catch Pokémon while driving or on private property, or in highly unsafe areas, or being so absorbed in augmented reality that they forget to pay attention to approaching vehicles when crossing the street.

The confluence of strangers in the same location may also pose additional risks, in that we do not know to whom we may be advertising our presence and activities. This may have been one of the most controversial issues surrounding the emergence of Pokémon GO, as several people were injured in fights in Pokémon gyms or when trying to start battles with strangers.

Because these types of app can endanger the lives of their users, designing a security model that is inherent to the development process will be an essential factor in creating new applications. After all, if there is no consideration of the physical aspects of usability, what can we expect from more technical security flaws and perhaps other failures less visible to users and developers?

Vulnerable apps with unsafe APIs

If there's one problem that has characterized the development of software to date, it is that security considerations are almost invariably deferred until later stages of development, if addressed at all. Aside from a few applications for which compliance with security standards is mandated, few developers are concerned about running vulnerability assessments and code auditing from independent, external experts, before releasing their products to the public.

As mobile devices are promoted as the builders of human relationships that reach beyond the digital space, whether in the workplace, in recreational and sporting activities, or even with the intention of finding love, security becomes a critical factor in preventing unsafe designs from compromising the development process.

For example, researchers recently found that Tinder's API gave—at the time of writing this article—the precise geolocation of the person each time a match occurred. Another notable example is the case of the Nissan Leaf, when it was discovered that some of the vehicle's non-critical controls could be accessed through vulnerabilities in the API provided by the company for mobile development.

Advertising libraries will also play an important safety role. These libraries are widely used by developers on platforms where users are often unwilling to pay for the functionality offered by the app. We typically find at least one of them per application and they often contain unsafe APIs that could be exploited to install malware or steal information.

In addition to these unintentional errors in the development process, there are also malicious creations whose propagation is sometimes facilitated by the less restrictive policies of certain application repositories, allowing criminals to benefit from the perceived reliability of official app stores.

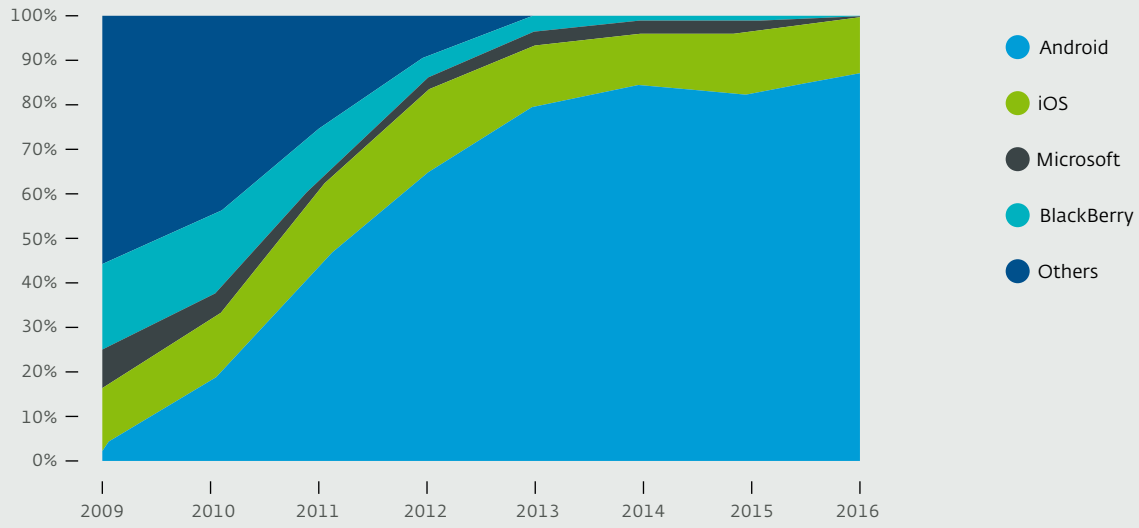
Android: an insecure system?

In 2007, the emergence of iOS revolutionized the mobile device industry by forcing consumers to rethink the role of technological devices in their daily lives. At that time, there was little discussion about the role of information security in mobile innovations and their possible impact on data protection.

Approximately one year after the release of iOS, a new operating system appeared as a plausible competitor: Android, created by Google. With open-source code, a less restrictive app market, the ability to adapt to different OEMs and very flexible customization, Android's market share grew rapidly.

Few developers are concerned about running vulnerability assessments and code auditing from independent, external experts, before releasing their products to the public.

Market share of different mobile operating systems



Source: Statista

By the end of 2009, mobile users began to consolidate into opposing sides based on their preference for either system, betting on one or the other. That was when the first questions emerged about whether the features so appreciated in Android could play a negative role in terms of security. Today we may be seeing the results of that wager.

In the second quarter of 2016, Android was installed on 86.2% of mobile devices in use. The large number of people using this OS makes it the preferred target for attackers. Its migration to other devices such as tablets, televisions, wearables and cars, makes it a potential vector for multi-platform attacks in ever more complex scenarios as new internet-connected home automation systems are developed.

Many factors make multi-platform attacks possible. First, the interconnectivity between devices allows threats and scams to spread easily through social engineering. Then there are components that are common to all devices using the operating system, but which may not be updated promptly or at all by different OEMs. Finally, development frameworks, which allow executables to be easily generated for different devices, are becoming increasingly common and could propagate security flaws between disparate devices. In the internet of things (IoT) it is not hard to imagine more such attacks in the future.

Malicious apps in official markets

A common occurrence in recent times has been the emergence of malicious apps in the official iOS and Android app repositories, a phenomenon that at first seemed extremely rare but that has unfortunately become more common over time. This trend has even affected the Apple App Store, which theoretically has more controls than the Google Play Store for Android.

As for publishing applications, numerous factors encourage the existence of malicious apps in Google's app store. Not only is Android a favorite target for cybercriminals because it has the largest number of

potential victims, but the speed at which apps are published on the Play Store also makes it a potential target for many attackers trying to propagate their threats.

With Android, any developer can create an account with a one-off payment of USD 25, upload an application, and have it published within 24 hours. In contrast, the cost of iOS development membership is more than USD 99 per year and the app approval waiting period can last weeks.

So while improvements to Bouncer (Google's module for automatic analysis and malware detection) are made on a regular basis, and manual code analysis is being strengthened, the huge number of new apps that are created daily and the haste with which they are incorporated into the market makes accurate analysis of each one difficult.

It is possible that in order to reduce future cases of malware introduced into its official app store, Google will need to modify one of these variables—or both—to devote more resources to intensive analysis of a reduced number of applications and/or extend the time needed for the approval process, undermining the speed of publication. One of the several strategies Google might use to reduce the number of candidate applications could be raising the price for developers' accounts.

What is certain is that so long as the policy framework for publication in the Play Store remains unchanged and none of these corrective measures are taken, we can expect to see a greater amount of malware in official stores in 2017 as attackers double down on this new modus operandi and find new mechanisms to evade detection.

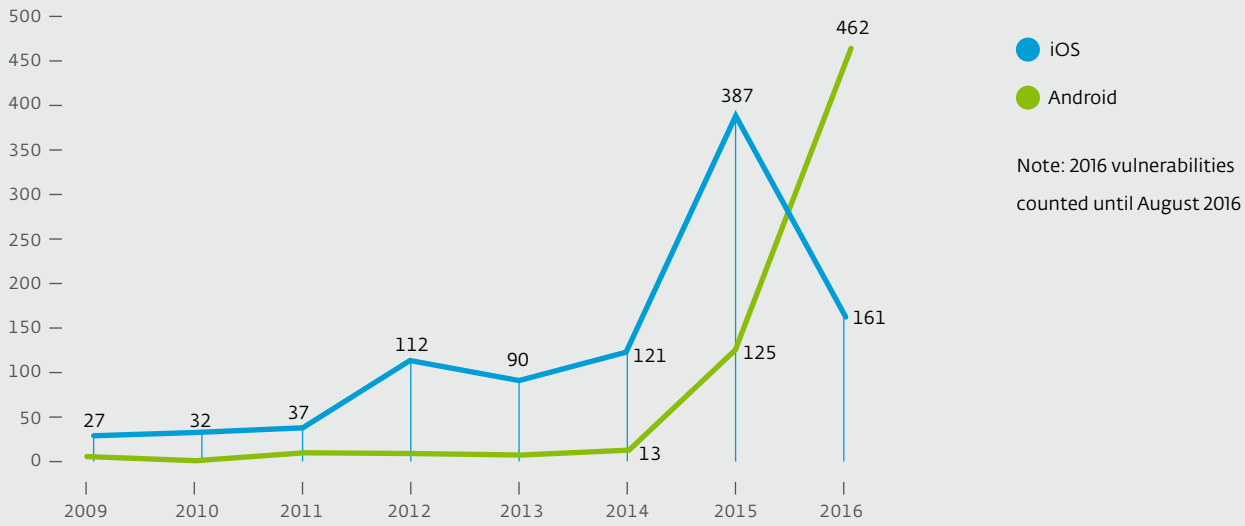
With regard to this last point, it should be noted that there are many techniques that render mobile malware detection difficult: time bombs, dynamic code executed through reflection [PDF], packers, encryption, obfuscated strings, scripts in other programming languages for remote downloading of malicious code, new forms of C&C, anti-emulation, rootkits, etc. But above all, cybercriminals are betting and will continue to bet on social engineering, waiting attentively for the official launch of popular apps to distribute their own fake versions, as happened recently with Pokémon GO, Prisma and Dubsmash.

The speed with which these malicious applications rack up hundreds and even thousands of downloads is a cause for concern among users of the platform. What will happen when cybercriminals decide to greatly increase the complexity of their creations?

Users' different approaches with respect to the installation of applications also plays a counterproductive role when it comes to Android. The ease with which someone can modify an APK obtained from the official store in order to inject malicious code and distribute it through websites or fake app stores, added to the ease with which users install files from untrustworthy sources, results in a higher rate of malware detection (and in the worst case, infestation) compared to other mobile operating systems.

We can expect to see a greater amount of malware in official stores in 2017 as attackers double down on this new modus operandi and find new mechanisms to evade detection.

Annual number of vulnerabilities in Android and iOS since 2009



Source: www.cvedetails.com

Easily updated

Over the years, various research reports have argued that Android's open-source nature inevitably implies a greater number of unprotected vulnerabilities [PDF] and, consequently, an increase in the frequency of attacks. This theory has not yet been completely substantiated, since 2016 is the first year in which Android is on track to finish with a greater number of published vulnerabilities than iOS.

However, the way security patches are deployed continues to leave some Android users unprotected, creating a large window between the time at which the vulnerability is known and the time when OEMs and telephone network operators deploy the security patch for the different versions of the operating system, if they even choose to do so.

For the remainder of 2016, and for 2017, Google's proposed plan for updates for Android 7.0 Nougat on Nexus devices includes monthly security patches in addition to quarterly updates with new functionality and bug fixes. Meanwhile, little progress has been made this year towards reaching a consensus on the rapid release of patches. On the contrary, power struggles for dominance in the mobile device market have resulted in sluggish conflict resolution.

For its part, Samsung, the leading manufacturer of Android devices, refuses to cede control of its devices' OS to Google. Meanwhile, Google is turning to more compliant manufacturers to displace Samsung and reduce its market share.

There are some indications that Google has come up with a new plan to address this issue. Up until then, one of the options available for those Android mobile users who are concerned about having the latest security patches will be to acquire Nexus devices—renamed Pixel by Google—so as to be sure to get updates as soon as possible from the mothership itself.

Mobile platforms under attack

Since 2012, the number of threat detections in the mobile world continues to grow, and we anticipate that this trend will continue next year. This is a statistical reflection of the utmost importance cybercriminals assign to these devices, as the data they store becomes increasingly sensitive.

Beyond the issues raised throughout the previous section, it is important to note that Apple users should not fall prey to a false sense of security. According to data obtained from our products, iOS threat detections still represent less than 1% compared to the number of Android threat detections. However, iOS threat detections are increasing exponentially: the number of detections on iOS so far in 2016 is greater than that for all of 2015, and we can expect this greater exposure to continue in 2017.

In addition, severe vulnerabilities continue to exist. Not long ago, Apple released security patches for a set of zero-day vulnerabilities that gave cybercriminals complete control over iOS devices and were used to spy on individuals.

The growth of mobile malware is an undeniable reality, one that we have been predicting since 2013 [PDF] and which is gaining strength as we speak. During 2015, new variants of malicious code created for Android averaged 200 a month; during 2016, this number rose to 300 new monthly variants (in iOS the number is 2 per month). We would not be surprised to see this increase continue over the next year, averaging 400 new mobile malware variants per month for Android by the end of 2017.

This provides us with a measure not only of the amount of malicious code but also of the speed with which these malicious campaigns evolve. In the coming year we will see more ransomware, more fake apps, more gimmicky malicious code and many more mobile scams through WhatsApp and social networking applications.

As users come to understand the dangers of installing applications from untrusted sources, cybercriminals are likely to be planning new social engineering campaigns through official markets. If so, we should expect to see many more such cases in the coming months. What remains to be seen is what course of action Google and Apple will take to contain the threat.

Together with the increase in the number of new variants of malicious code, a major concern for users of mobile devices will be vulnerabilities not only in the operating system but also in the applications they use. As these apps collect and store data that can be misused to endanger the physical health and safety of their users, it will be a challenge for developers to quickly adopt secure development procedures so as to minimize the risk of exposure, such as that found in poorly designed APIs.

For now, the recent releases of iOS 10 and Android 7.0 Nougat show some remarkable improvements in mobile security, especially in the latter. Google's efforts to unify some aspects of security are becoming more obvious in the various models of phones and tablets now becoming available on the market. In addition, the company continues to have high hopes for its aggressive program of bug hunting as a means of discovering vulnerabilities.

Another remarkable feature of Android 7.0 Nougat is that it has introduced various improvements in handling permissions and applications which will hinder the installation of malware on the device and limit the control such applications obtain, in a clear attempt to thwart the increase of mobile ransomware, one of the main challenges in mobile security.

Vulnerabilities

Reports are decreasing but, are we safer?

- Critical vulnerabilities on the rise
- Secure software development
- The role of PR on naming vulnerabilities such as Heartbleed and how is this good for IT Security
- Bug bounty programs, companies paying for IT Security indirectly better than hiring IT Security staff?

AUTHOR

Lucas Paus
ESET Security Researcher

Vulnerabilities: reports are decreasing but, are we safer?

The rapid global spread of technology and the increasingly numerous types of interconnected devices routinely used, have greatly increased the number of attack vectors available to cybercriminals. This is why the exploitation of vulnerabilities is still one of our major concerns when it comes to corporate security incidents around the globe.

When attackers are able to find and exploit programming defects, they can overcome security barriers on various platforms and take various actions, ranging from data theft to spreading malware and even triggering a system or service crash. This occurs without any need for involvement or action on the user side.

Within the context of this boom in technology and its consequent vulnerabilities, new security challenges have emerged relating not only to digital information, but also in respect to access to critical infrastructure, smart cars, IoT, Industry 4.0 and even the manipulation of operations within smart cities. While operating systems and applications become increasingly focused on being more functional and competitive, there is an emerging need within the market to give a higher priority to secure development in conjunction with more frequent security audits.

In 2016, we saw a strategic alliance between Microsoft and Canonical, with a view to integrating Ubuntu Linux tools into Windows 10. While the potential of a joint platform of this type is sound, it could become a new vector for multi-platform attacks, as is often the case with vulnerabilities in Java or in web browsers.

Will these new scenarios heighten the importance of detecting and immediately mitigating vulnerabilities? Has the number of vulnerabilities encountered been reduced? How can we, with better certainty, ensure the security of information both at home and at work?

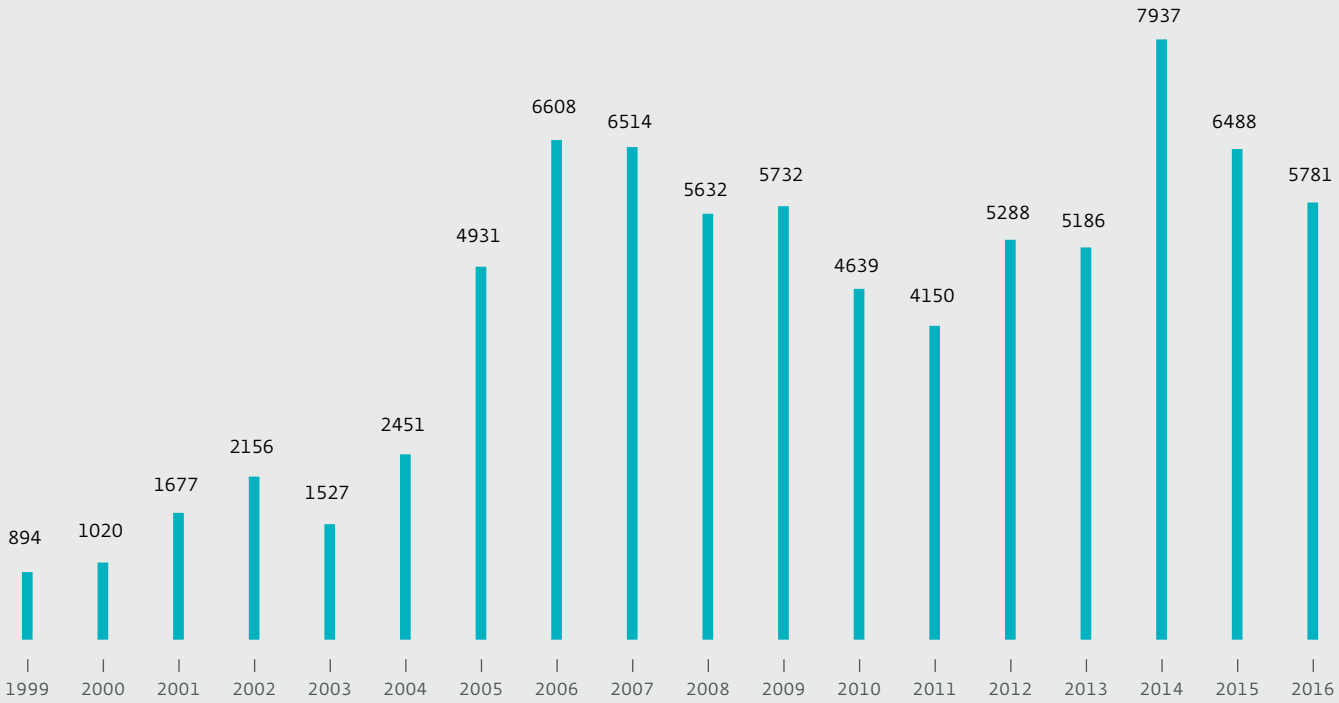
Throughout this section, we will be providing some recommendations to these questions and will also look at how future vulnerabilities might affect us.

The number of vulnerability reports is falling, but is risk also falling?

Paradoxically, despite the advent of new technologies and attack vectors, the total number of all kinds of vulnerabilities reported annually has been falling in recent years. In particular, the number of reported CVEs has fallen, after reaching a historic high in 2014.

At the end of the third quarter of 2014, 5,405 vulnerabilities were published, whereas the figure fell to 5,920 in the same period in 2015. At the end of the third quarter of 2016 (when this article was written), the figure reached 5,781 – almost the same level as last year. In other words, there has been no sudden increase in the total number of vulnerabilities published: in fact, this may represent a gradual downward trend overall, as shown in Figure 2. Since secure development is gaining ground, a sudden rise in the number of reported vulnerabilities in 2017 is not expected.

Figure 1. Vulnerabilities published by year



Source: National Vulnerability Database

However, despite the grounds for optimism presented by this drop in the number of published vulnerabilities, this information conceals a less cheerful aspect when we note how many of these vulnerabilities are regarded as "critical", that is, those that have a greater impact on user security.

At the end of October of 2016, the number of critical reported vulnerabilities corresponded to 40% of total vulnerabilities, a higher percentage than that seen in all previous years, and it looks likely that the trend will continue in the last quarter. Therefore, the overall drop in volume of reported vulnerabilities is less conducive to peace of mind than it at first appears, especially given that reports of critical vulnerabilities are increasing.

However, despite the numbers of vulnerabilities encountered, we cannot disregard the fact that their exploitation is not directly proportional to the number of CVEs reported. The risk that a vulnerability will be actively exploited is related to issues such as the widespread use of a vulnerable application or protocol, the difficulty entailed in its exploitation, and the critical or valuable nature of the information stored and at risk.

For example, CVE-2016-2060 is a critical vulnerability which affects **millions of Android devices**, meaning that some applications obtain privileges enabling them to gain access to the user's private information. As regards protocols, in the case of OpenSSL, we draw your attention to DROWN, a critical vulnerability published in 2016. Its impact was estimated as possibly affecting 25% of the most visited Internet domains, and up to one-third of all servers on the Web. This clearly illustrates how two CVEs can have a significant impact on a range of potential victims, from home users to companies.

Secure software development

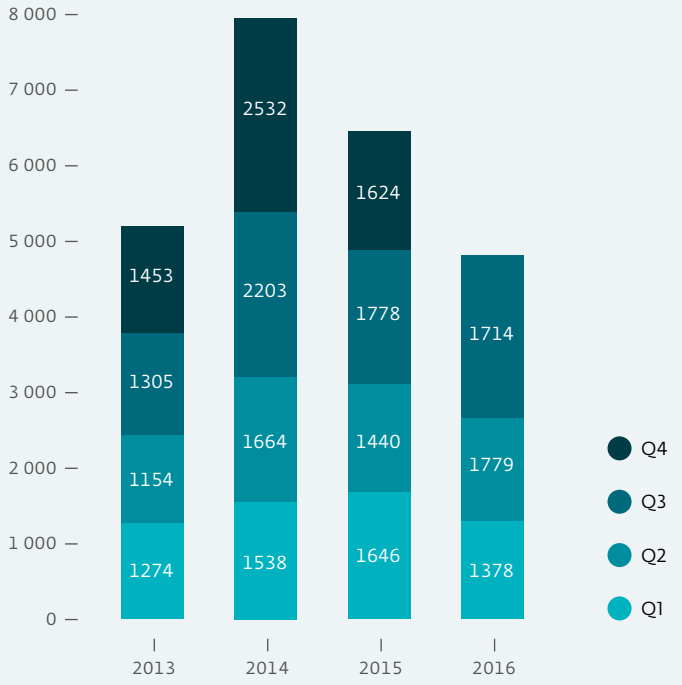
The reduction in the number of reported vulnerabilities can be partly ascribed to new paradigms in systems development. One of the major challenges continually faced in terms of computer security is the way security is applied to new projects.

Previously, we often saw time to market innovations being prioritized ahead of information security. However, whether driven or bound by the constant need for innovation within the technology market, the relegation of information security from program development is a risky practice, not only from the point of view of data protection, but also for the continuity of business. This is especially true since a large-scale incident could have an enormous impact on corporate image, both for the victim and for the vendor.

However, attempts are being made to change this paradigm, and there is a gradual movement towards encouraging security and cryptography experts to provide support for developers from the preliminary phases of a new product's development. Therefore, insofar as these good practices are being improved during the software life cycle (SDLC, Systems Development Life Cycle), we do not expect the number of CVEs to rise sharply. This in turn means a reduction in the likelihood of vulnerabilities being exploited on the various systems that have been developed.

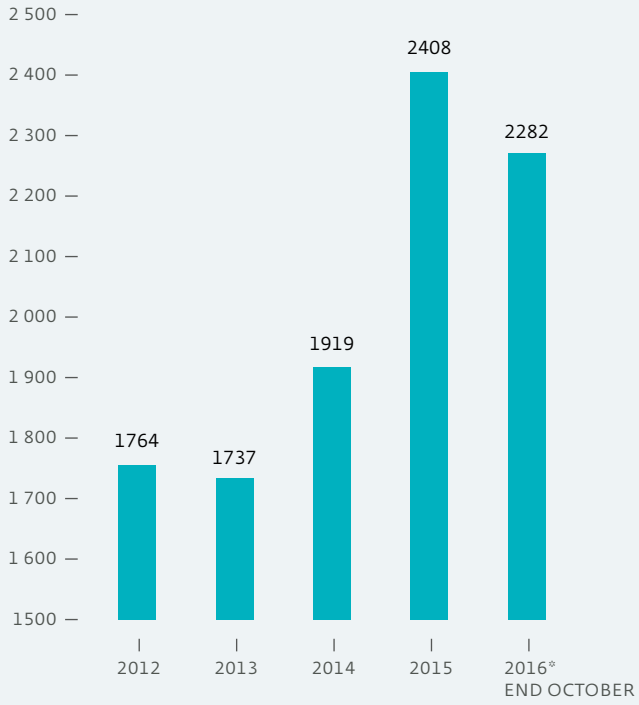
All of these improvements in SDLC are becoming even more necessary if we consider well-known scenarios and developments in technology that have been on the rise in recent years, this includes a growing number of cloud-based applications and services or their future migration, Big Data applications, and Application Programming Interfaces (APIs).

Figure 2. Vulnerabilities per Quarter



Source: National Vulnerability Database

Figure 3. Number of critical reported vulnerabilities



Source: National Vulnerability Database

All of these must be implemented with appropriate input validation and security assured output encoding using cryptographic practices. This is in addition to the proper handling of logs, memory, errors and archives.

To reinforce improvements throughout the development cycle, the challenge for 2017 will be to focus on improving management of the vulnerabilities that will inevitably still be encountered. For manufacturers and developers alike, as well as for users, the challenge will not only be to use control measures to prevent the exploitation of vulnerabilities, but also to carry out satisfactory reporting and management of those vulnerabilities.

Thus, it is expected that implementation of a secure development cycle, based on the consolidation of a design model focused on security, will start to generate synergies between the areas of security and development. This will likely bring us closer to the deployment of more robust, effective and profitable systems.

The prominence of multiple vulnerabilities and their role in raising awareness

From a users' perspective, several recent critical vulnerabilities have not gone unnoticed. For more than three decades, antivirus companies and security researchers have been using various names for different examples of malicious code that have had a major impact; we can cite older examples such as the Morris worm, Melissa, and Sasser, or more current names such as CTB-Locker and Locky. This practice has gone a step further and, since 2014, specific critical vulnerabilities have also been given names. A clear example has been CVE-2014-0160, better known as Heartbleed, a well-known vulnerability with not just a name, but also its very own logo.

Naturally, names seek to characterize threats in an attempt to define a point of reference or an understanding of how they function. In addition, the naming of vulnerabilities is very effective in regards to raising the awareness of various IT departments. In this way they are encouraged, based on the identification of a vulnerability, to take necessary measures to mitigate it.

In 2015 we saw the emergence of names such as FREAK (CVE-2015-0204) and Logjam (CVE-2015-4000) and in 2016, we saw Badlock (CVE-2016-2118) affecting Samba, as well as HTTPoxy (CVE-2016-5387) despite being detected for the first time 15 years ago and DROWN, which affects TLS/SSL protocols.

This naming of vulnerabilities will certainly continue next year and it is hoped that, apart from the marketing effects, these names will increase user awareness so that potential victims take the necessary measures to mitigate the impact said vulnerabilities might have on their systems.

Attack is sometimes the best defense

The notification of vulnerabilities has also been a concern for leading service providers and companies in the world of technology. Years ago, companies adopted a fairly proactive position regarding the management of security and vulnerabilities, notably by generating policies and controls to enforce such management. More recently, policies and controls have been beneficial for the various audits or pen testing that have gained ground mainly in corporate environments where, in many cases, due to regulatory rules and increased awareness of current threats, they need to be carried out periodically.

Heartbleed

DROWN

However, large companies and government agencies are relying on a trend towards simulations of what a real attack might be like. This approach basically consists of hiring security experts to carry out pen testing with remuneration based on results obtained; it has been dubbed the Vulnerability Reward Program. Leading companies such as Facebook, Google or Yahoo! (among many others) are already energetically formalizing this kind of activity, with agencies such as the US Department of Defense not far behind.

For application developers and manufacturers of IoT devices, this kind of program may bring about improvements in their products more quickly, as tests are usually conducted by a larger number of researchers, and vulnerabilities are reported immediately. In addition, tests are carried out over an extended timeframe, meaning that more in-depth explorations can be carried out. We predict that VRPs, and the many researchers participating in them, will extend to the IoT sphere for the foreseeable future.

Conclusion

Companies today, though more concerned with security incidents such as information leaks or unauthorized access to sensitive data, have not substantially improved their security management practices. Therefore, the main challenges to the corporate world in 2017 relate to focusing efforts on the management of technology, and the need to raise their employees' awareness of these risks. This is due in large part to the need for compliance with standards imposed by business regulators.
Added to all this, there is a need to explore further the culture of resilience, which allows leading security experts to act as facilitators in IT areas such as correction of coding errors and mitigation of breach impacts. Management therefore needs to focus on the appropriate implementation of security policies and on plans that enable businesses to continue functioning in the event of a breach. This should also include the appropriate communication of incidents necessary to keep users informed of breaches that entail a risk to them.

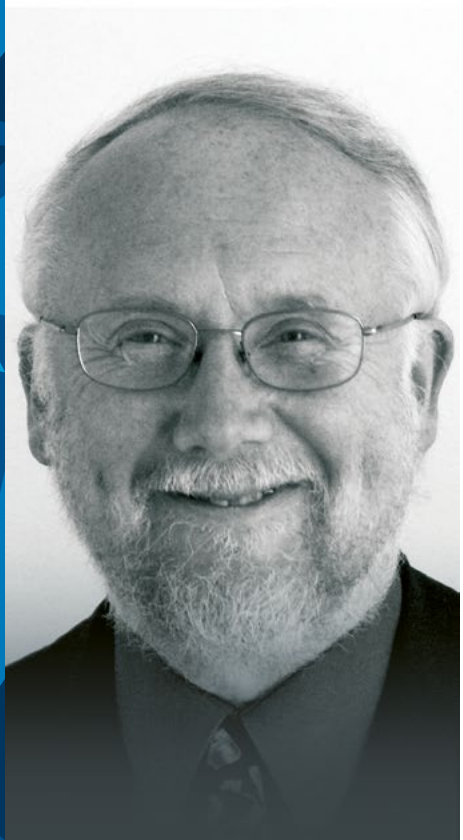
From the developer's point of view, it is to be expected that the paradigm of secure development will continue to be strengthened and, based on greater user awareness of the risks generated by vulnerabilities, it would be unsurprising to see greater demand for increased protection of the personal information that companies manage. Should this occur, secure development may become a competitive differential within the technology industry, and in the future it will become an incentive for developers.

Secondly, while some malcode has always used vulnerabilities in order to propagate, some new malicious programs have started to do so specifically. This is because by simply visiting a link, an unprotected victim can reveal how the information on his or her devices is encrypted, as occurs with some variations of the ransomware CryptoWall 3.0. Similarly, exploit kits will continue to be used largely for the propagation of malware and even for more directed attacks, such as the implementation of APTs against vulnerable sites.

Software vulnerabilities are difficult to predict in many cases; therefore, in order to be able to reduce the risks they entail, it is important to develop plans to raise awareness of good practice and correct management. The use of famous zero-days still leaves systems exposed; however, the antivirus industry has taken note of this trend and has responded via security solutions with advanced heuristics and technologies capable of both detecting these kinds of exploits and blocking them.

Therefore, both security solutions and the management of both updates and vulnerabilities will continue to play a leading role in the mitigation of these kinds of problems. These have the objective either of minimizing or eliminating both gaps in defensive measures and information leaks in the coming years.

'Next-Gen' security software – myths & marketing



AUTHOR

David Harley
ESET Senior Research Fellow

5

'Next-Gen' security software – myths and marketing

The Age of the Dinosaurs

There is a view of the current security market that is often recycled by the media these days. It assumes a split between 'first-gen(eration)' or 'traditional' (or even 'fossil' or 'dinosaur') malware detection technology – which is invariably claimed to rely on reactive signature detection – and (allegedly) superior technologies using 'next-gen(eration)' signature-less detection. This picture is much favoured by some 'next-gen' companies in their marketing, but it doesn't reflect reality.

The Theory of Evolution

First of all, I'd take issue with that term 'first-generation'. A modern mainstream security suite can no more to be lumped in with early 'single layer' technologies – such as static signature scanners, change detection and vaccines – than Microsoft Word can be with ed or edlin. They may have the same fundamental purpose as those long-gone applications – be it detection and/or blocking of malicious software, or the creation and processing of text – but they have a much wider range of functionality. A modern word processor incorporates elements that decades ago would have been considered purely the domains of desktop publishing, spreadsheets and databases.

The Origin of Specious

A modern anti-malware-focused security suite isn't quite so wide-ranging in the programmatic elements it incorporates. Nevertheless, it includes layers of generic protection that go far beyond signatures (even generic signatures). They have evolved into very different generations of product, incorporating technologies that didn't exist when the first security products were launched. To talk about newcomers to the market as if they alone are 'the next generation' that goes beyond primitive signature-specific technology is misconceived and utterly misleading.

Signatures? What Signatures?

Nowadays, even modern, commercial single-layer anti-malware scanners go far beyond looking for specific samples and simple static signatures. They augment detection of known, hash-specific families of malware with the inclusion of elements of whitelisting, behaviour analysis, behaviour blocking, and change-detection (for instance) that were once considered to be pure 'generic' technologies. Not that I recommend in general that people should rely totally on a single-layer scanner such as those often offered for free by mainstream companies: they should be using other 'layers' of protection as well, either by using a commercial-grade security suite, or by replicating the multi-layered functionality of such a suite, while using components drawn from a variety of sources, including a single-layer anti-malware scanner. However, the latter approach requires a level of understanding of threat and security technologies that most individuals don't have. Come to that, not all organizations have access to such a knowledgeable resource in-house, which leaves them potentially at the mercy of marketing masquerading as technical advice.

Back to Basics

Although some next-gen products are so secretive about how their technology actually works that they make mainstream anti-malware products look like open source, it's clear that the distinctions between 'fossilized' and 'next-gen' products are often terminological rather than technological. I don't consider that 'next-gen' products have gone further beyond these basic approaches to defeating malware, defined long ago by Fred Cohen (whose introduction and definition of the term computer-virus to all intents and purposes jumpstarted the anti-malware industry in 1984), than have 'traditional' solutions:

- Identifying and blocking malicious behaviour.
- Detecting unexpected and inappropriate changes
- Detecting patterns that indicate the presence of known or unknown malware.

The ways of implementing those approaches have, of course, become immeasurably more advanced, but that progression is not the exclusive property of recently-launched products. For example, what we generally see described as 'Indicators of Compromise' could also be described as (rather weak) signatures. More than one vendor has failed to differentiate convincingly between mainstream anti-malware use of behaviour analysis and blocking, between its *own* use of (for instance) behavioural analysis/monitoring/blocking, traffic analysis (and so on) and the use of ***the same technologies*** by mainstream anti-malware. Instead, they've chosen to promote a deceptive view of 'fossil technology' and peppered their marketing with a hailstorm of technological buzzwords.

Welcome to the Machine

Consider, for instance, the frequent lauding of 'behaviour analysis' and 'pure' Machine Learning (ML) as technologies that set next-gen apart from first-gen. In the real world, Machine Learning isn't unique to one market sector. Progress in areas like neural networking and parallel processing are as useful in mainstream security as in other areas of computing: for example, without some degree of automation in the sample classification process, we couldn't begin to cope with the daily avalanche of hundreds of thousands of threat samples that must be examined in order to generate accurate detection.

However, the use of terms like 'pure ML' in next-gen marketing is oratorical, not technological. It implies not only that ML alone somehow provides better detection than any other technology, but also that it is so effective that there is no need for human oversight. In fact, while ML approaches have long been well-known and well-used in the mainstream anti-malware industry, they have their pros and cons like any other approach. Not least, in that the creators of malware are often as aware of ML as the security vendors who detect malware, and devote much effort to finding ways of evading it, as is the case with other anti-malware technologies.

On Your Best Behaviour

Similarly, when next-gen vendors talk about behavioural analysis as their exclusive discovery, they're at best misinformed: the term behavioural analysis and the technologies taking that approach have both been used in mainstream anti-malware for decades. In fact, almost any detection method that goes beyond static signatures can be defined as behaviour analysis.

Distinctions between 'fossilized' and 'next-gen' products are often terminological rather than technological.

Natural and Unnatural Selection

Journalist Kevin Townsend asked me recently:

> Is there any way that the industry can help the user compare and choose between 1st [...] and 2nd generation [...] for the detection of malware?

Leaving aside the totally misleading 1st versus 2nd-generation terminology, yes, of course there is. In fact, some of the companies self-promoted as '2nd-generation' and claiming that their technology is too advanced to test have nevertheless pushed an already open door even wider by their own attempts to compare the effectiveness of their own products and those of 'first-gen' vendors. For example, at least one next-gen vendor has taken to using malware samples in its own public demonstrations: if different generations of product can't be compared in an independent test environment, how can such demonstrations be claimed to be accurate in a public relations exercise? Other misleading marketing from next-gen vendors includes claims that "1st-gen products don't detect 'file-less' malware in memory" (which we've done for decades). One particularly inept example used a poorly constructed survey based on Freedom of Information requests to 'prove' 'traditional' anti-malware's 'abject failure' without attempting to distinguish between attacks and successful attacks.

Testing and Pseudo-testing

More commonly, VirusTotal (VT) is misused by misrepresenting its reports as if VT and similar services are suitable for use as 'multi-engine AV testing services', which is not the case. As VT puts it:

> VirusTotal should not be used to generate comparative metrics between different antivirus products. Antivirus engines can be sophisticated tools that have additional detection features that may not function within the VirusTotal scanning environment. Because of this, VirusTotal scan results aren't intended to be used for the comparison of the effectiveness of antivirus products.

VT can be said to 'test' a *file* by exposing it to a batch of malware detection engines. But it doesn't use the full range of detection technologies incorporated into those products, so it doesn't accurately test or represent product effectiveness. One next-gen vendor talked up its own detection of a specific ransomware sample a month before the same sample was submitted to VirusTotal. However, at least one mainstream/traditional vendor was detecting that hash a month before that next-gen detection was announced. You simply can't measure a product's effectiveness from VirusTotal reports, because VT is not a tester and its reports only reflect part of the functionality of the products it makes use of. Otherwise, there'd be no need for reputable mainstream testers like Virus Bulletin, SE Labs, AV-Comparatives and AV-Test, who go to enormous lengths to make their tests as accurate and representative as possible.

Towards Cooperation

One of the more dramatic turnarounds in 2016 took place when VirusTotal changed its terms of engagement in order to make it harder for next-gen companies to benefit from access to samples submitted by "1st-gen" companies to VirusTotal without contributing to VT themselves. To quote VirusTotal's blog:

> ...all scanning companies will now be required to integrate their detection scanner in the public VT interface, in order to be eligible to receive antivirus results as part of their VirusTotal API services. Additionally, new scanners joining the community will need to prove a certification and/or independent reviews from security testers according to best practices of Anti-Malware Testing Standards Organization (AMTSO).

While many vendors in the next-gen space initially responded along the lines of "It's not fair", "The dinosaurs are ganging up on us", and "We don't use signatures so we don't need VT and we don't care", it seems that several big names were subsequently prepared to meet those requirements by joining AMTSO and thus opening themselves up to independent testing. (By that I mean real testing, not pseudo-testing with VirusTotal.) Since next-gen vendors have tended in the past to protest that their own products cannot be tested, especially by the 'biased' testers represented in AMTSO, perhaps this suggests the possibility of an encouraging realization that not all customers rely purely on marketing when they make purchasing decisions.

Share and Share Alike

Why have next-gen vendors now decided that they do need to work with VirusTotal? Well, VT shares the samples it receives with vendors and provides an API that can be used to check files automatically against all the engines VT uses. This allows vendors not only to access a common pool of samples shared by mainstream vendors, but to check them against indeterminate samples and their own detections, thereby training their machine learning algorithms (where applicable).

And why not? That's not dissimilar to the way in which longer-established vendors use VirusTotal. The difference lies in the fact that under the updated terms of engagement the benefit is three-way. Vendors (of any generation) benefit from access to VirusTotal's resources and that huge sample pool. VirusTotal benefits as an aggregator of information as well as in its role as a provider of premium services. And the rest of the world benefits from the existence of a free service that allows them to check individual suspect files with a wide range of products. Widening that range of products to include less-traditional technologies should improve the accuracy of that service, while the newer participants will, perhaps, be more scrupulous about not misusing VT reports for pseudo-testing and marketing when they themselves are exposed to that kind of manipulation.

Vendors (of any generation) benefit from access to VirusTotal's resources and huge sample pool.

Whole-Product Testing

The way that AMTSO-aligned testers have moved towards 'whole-product testing' in recent years is exactly the direction in which testers need to go in order to evaluate those less 'traditional' products fairly. (Or, at any rate, as fairly as they do mainstream products.) It can be argued, though, that testers can be conservative in their methodology. It's not so long ago that static testing was the order of the day (and to some extent still is among testers not aligned to AMTSO, which has discouraged it since the organization's inception). AMTSO, despite all its faults, is greater (and more disinterested) than the sum of its parts because it includes a range of researchers both from vendors and from testing organizations, and marketing people aren't strongly represented. Thus, individual companies on either side of the divide are less able to exert undue influence on the organization as a whole in pursuit of their own self-interest. If the next-gen companies can grit their teeth and engage with that culture, we'll all benefit. AMTSO

has suffered in the past from the presence of organizations whose agenda seemed to have been overly-focused on manipulation or worse, but a better balance of 'old and new' vendors and testers within the organization stands a good chance of surviving any such shenanigans.

Into the Cenozoic

Several years ago I concluded an article for Virus Bulletin [PDF] with these words:

> But can we imagine a world without AV, since apparently the last rites are being read already? ... Would the same companies currently dissing AV while piggybacking its research be able to match the expertise of the people currently working in anti-malware labs?

I think perhaps we have an answer to that. But if the self-styled next generation can come to terms with its own limitations, moderate its aggressive marketing, and learn the benefits of cooperation between companies with differing strengths and capabilities, we may yet all benefit from the détente.

Healthcare challenges

Ransomware and the Internet of Things are the tip of the iceberg

- Ransomware is the tip of the iceberg
- Medical and Fitness devices
- Securing medical devices

AUTHOR

Lysa Myers
ESET Security Researcher

Healthcare challenges: Ransomware and the Internet of Things are the tip of the iceberg

Last year's Anthem and Premera breaches made the general public more aware of the importance of security in healthcare organizations. 2016 has brought fewer instances of massive healthcare breaches, but sadly this does not suggest that the problem has been solved. In fact, this year has brought a surfeit of successful ransomware attacks in a variety of industries, and medical facilities have been a particularly juicy target for this type of threat. This, coupled with an upsurge in internet-connected medical devices and fitness trackers, indicates that the future of healthcare is likely to continue to bring significant challenges.

Ransomware is the tip of the iceberg

One might think of the swelling tide of ransomware as a problem in and of itself. While it is causing huge headaches and monetary loss, the success of ransomware is symptomatic of a greater problem.

Ransomware is a type of threat that can generally be mitigated by following minimum security practices for endpoints and the network. In fact, in the wake of the discovery of the first ransomware variants, security experts may have taken it somewhat less seriously because it can be so easily thwarted even when the malware file itself is not detected before execution: a victim need only restore from backups to get around the ransom demands.

Except that when it comes to practical, real-world protection, security measures are often not implemented in the way that the security community would hope. It may appear initially that it is costlier to restore from backups than to accede to ransom demands. Some businesses may not make regular backups at all. Security products designed to detect malicious emails, files, links or traffic may be improperly configured, or simply absent. Backup strategies may not be properly implemented, so that backups are also vulnerable to ransomware attacks or other risks. Users may disable or go around security products if they feel those measures are preventing them from doing their jobs. Whatever the root cause, the end result is that affected businesses may feel they need to pay criminals in hopes of getting their data back.

In healthcare, where quick access to data can be a matter of life and death, the cost of being hit with ransomware is significantly magnified. Criminals know this and are deliberately targeting medical organizations. It will take some simple but powerful action to reverse this trend. But by setting in place a solid base of security, we may be able to decrease both the effects of future malware threats and the risk posed by new technology.

The importance of assessing and remediating risk

We've discussed on WeLiveSecurity the importance of risk assessment in healthcare. By regularly categorizing assets and transmission methods, you can pinpoint possible vulnerabilities and risks. When you take into account the likelihood and potential cost of those risks, you can get a sense of which things you should address most urgently.

In the case of ransomware, there are a few ways that risk assessment could help address the situation:

- What assets are at risk of being encrypted by ransomware?
- What transmission methods allow the ransomware to enter your network?
- What methods allow the threat to receive commands to encrypt your files?
- What is the likelihood of being hit by this threat?
- What is the potential monetary damage caused by a successful attack?

The assets at risk of being encrypted are, unfortunately, almost any data or systems that are accessible on your network or by the Internet. The origins of ransomware attacks are often phishing emails containing malware files or links via which to download malicious files. So the transmission method in this instance would be considered email, with a focus on social engineering. The malware typically needs to be able to call back out to a Command & Control channel to receive instructions, which many variants do using common protocols like HTTP or HTTPS. While the specifics of monetary damage vary from one organization to another, the likelihood of being attacked is currently very high for all industries and sizes of business.

To reduce the risk, there are a variety of things you can do. For example:

- Backups performed regularly and then verified are a very effective way to mitigate damage once a system or network is affected.
- Network segregation may limit the effects of malware once it's on your systems.
- Filtering email for spam and phishing, as well as blocking popular file-types used by malware authors, can help decrease risk of the malware ever reaching your users.
- Educating users early and often can decrease the odds of the malware being executed.
- Encouraging your users to submit suspicious emails or files to IT or security staff can help increase the effectiveness of your filtering methods.
- Anti-malware software used on the gateway, network and endpoint can help identify and prevent malware from entering your network, or decrease damage done if it should succeed in getting past initial defenses.
- Firewalls and intrusion prevention software may help identify unknown or unwanted network traffic.

These steps would not simply mitigate the risk of ransomware; they could also help reduce the likelihood of a variety of other types of attacks. Thoroughly assessing risk and improving an organization's overall security posture can significantly decrease both the frequency and severity of all types of security breaches.

Medical & Fitness devices

As the healthcare industry becomes more computerized, more healthcare practitioners and patients are utilizing medical and fitness devices. These devices are often full of sensitive information, yet security and privacy are often an afterthought. As we've seen with the ransomware trend, the risk of having highly sensitive information without a solid base of security can lead to significant problems. But since this technology is fairly new, now is a good time to focus on how to secure these devices.

Medical devices in healthcare networks

Medical devices used within hospital networks can be large and expensive machines, which are often run on common – and all too often very outdated – operating systems (such as Windows XP Embedded). These devices often provide easy access to the rest of the hospital network where many different types of sensitive information are kept: financial information for billing, identity information for insurance purposes, as well as health-related information generated by patient visits. From a criminal perspective, this is a wealth of lucrative data – potentially more than ten times as valuable as credit or debit card details alone.

Medical devices in a hospital often use a similar operating system to desktop machines, so you may be able to use the same technology and techniques to secure them. Though if a device is using a severely outdated (and potentially unsupported) operating system, it must be given significant additional protection. It might be preferable to keep the machine completely disconnected from all network connections, though care must still be taken to protect against threats spread by removable media.

Medical devices and trackers at home

Medical devices and trackers used at home are typically very small, so that they can be worn or implanted without being obtrusive. Most use either proprietary or Linux-based operating systems. They may be connected to the Internet or they may be able to sync with a mobile device or desktop computer. And like hospital-based devices, they may also be updated infrequently, if at all.

A device used by a patient at home doesn't usually store payment card information, but there may be other data on these devices that criminals could find useful to steal or modify such as: email address, username and password, GPS data including home or work address. In addition, it could indicate when the user is away from home or asleep. An attack on an implantable medical device could allow criminals to make a variety of changes to prescribed measures, which could cause serious (or even fatal) medical problems.

On a personal medical device, it is most important to keep the machine from being used to harm users or to compromise their privacy. An attack on an Internet-enabled insulin pump or pacemaker will naturally be significantly different from one on a fitness tracker. The security measures needed to protect the devices will be the same, though an insulin pump or pacemaker may need to have more stringent settings enabled by default.

Securing medical devices

Manufacturers of both personal and hospital-based medical devices have the opportunity to lead a shift towards better security by giving it serious consideration, starting in the design phase. There are a variety of things device makers should be doing to make devices more secure:

Fitness devices are often full of sensitive information, yet security and privacy are often an afterthought.

- **Design for privacy** – Learn the seven principles of Privacy by Design.
- **Encrypt Data** – Protect data both on disk and in transit with strong encryption, when sent via email, web or IM, or when synced with the user's computer.
- **Clarify data storage options** – Give users the ability to store tracked info locally, rather than just in the cloud.
- **Authenticate account access** – Verify that users are who they say they are. It is especially important to authenticate before allowing the viewing, sharing or modifying of information on implanted devices, as the consequences of misuse are significantly higher. Provide multi-factor authenti-cation for online account access.
- **Create a fail-safe state** – Errors and malfunctions happen. Devices must default to a state that maintains access to critical functionality and does not endanger users when problems occur.
- **Assume code may be used maliciously** – Legitimate code may be used in a way that forces the device to execute unauthenticated code. It is vital to handle errors in a way that takes into account this possibility so that devices cannot be used maliciously.
- **Prepare for vulnerabilities** – Establish and openly publish a responsible disclosure policy for vulnerability reports.
- **Prepare for breaches** – Create an incident response plan so that you can react appropriately in the event of a data breach. This will both save time and allow you to choose your words wisely, in the event of an emergency.
- **Prepare for government scrutiny** – The FTC and FDA are both watching the medical device space closely, so making changes now can help avoid legal problems and hefty fines down the road.

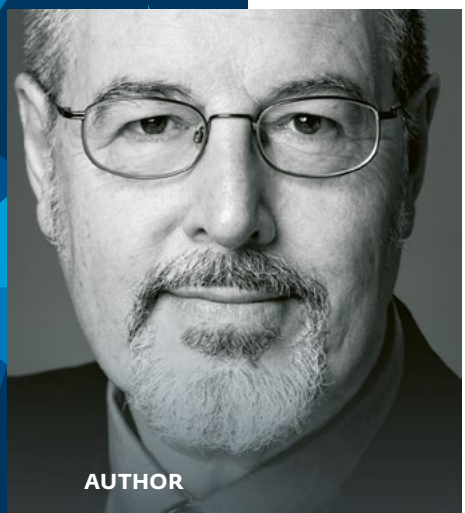
The security of the healthcare industry is likely to be in the spotlight for the foreseeable future. Despite the current troubles, the opportunity exists to make a significant transformation that could serve as a model of positive change for other industries, as the Internet of Things makes its way into our homes and workplaces.

Threats to critical infrastructure: the internet dimension

› Malware-influenced Power outages such as BlackEnergy and more critical infrastructure (Power, Water but also chain supply, Smart Cities, San Diego example) could be more frequent than we thought.

AUTHOR

Cameron Camp
ESET Security Researcher



AUTHOR

Stephen Cobb
ESET Senior Security Researcher

Critical Infrastructure

Cyberattacks on critical infrastructure were a key trend in 2016 and we expect them to continue to generate headlines and disrupt lives in 2017. The very first article of 2016 on WeLiveSecurity was Anton Cherepanov's analysis of BlackEnergy, malicious code used in attacks on Ukrainian power companies that resulted in electricity outages of several hours for hundreds of thousands of homes in that part of the world. However, before discussing this and other incidents, it will be helpful to discuss terminology. It seems "infrastructure" can mean different things to different people, and not everyone agrees on what "critical" means in this context.

Defining incidents

In the US, the Department of Homeland Security (DHS) is charged with protecting critical infrastructure, which it categorizes into 16 sectors, "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." You can find links to detailed definitions of those 16 sectors at dhs.gov, but we wanted to list their titles here to give you a sense of how pervasive critical infrastructure is:

All of these sectors rely to some extent on the digital infrastructure known as the internet, but sometimes there is confusion between critical infrastructure and the internet infrastructure. The difference is clear if we look at two key incidents of 2016: the Ukrainian power outages mentioned at the outset, and the phenomenon known as the Dyn IoT DDoS of October 21 (which we abbreviate to 10/21).

16 sectors of critical infrastructure in the US

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Troubling incidents

The power supply attacks in Ukraine were enabled by the internet infrastructure. The attackers used email and other forms of internet connectivity to gain a foothold in networked power company computers. In some targeted organizations a lack of effective impediments allowed attackers to access, over the internet, the applications that remotely control electricity distribution. ESET researcher Robert Lipovsky put the attacks in context like this: "On December 23rd, 2015, around half of the homes in the Ivano-Frankivsk region in Ukraine (population around 1.4 million) were left without electricity for several hours." A power outage like that is clearly an attack on critical infrastructure, as well as a possible harbinger of things to come if it was a trial run for future attacks.

The 10/21 incident was a series of large Distributed Denial of Service (DDoS) attacks that leveraged tens of millions of internet-connected devices (collectively referred to as the Internet of Things or IoT), to target the servers of a company called Dyn that provides Domain Name Service (DNS) to a lot of well-known US companies. DNS is the "address book" for the internet, a system for making sure that information requests on the internet are delivered to the right host (server, laptop, tablet, smartphone, smart fridge, and so on). The effect of 10/21 was to prevent or delay traffic to websites, internet content servers, and other internet services like email. Because of the highly inter-dependent nature of internet services, 10/21 negatively impacted, through a chain reaction of escalating collateral damage, a significant percentage of US commercial enterprises even though they were not the immediate target of the attack.

Consider a company that sells software online, it's web store is not targeted by the attackers but traffic to the site drops because the servers dishing up online adverts for the company's products are not reachable. Web pages at the company's website fail to load properly because they rely on a content delivery network (CDN) that is temporarily unreachable. Even when customers can complete their online purchases, some cannot reach the content server to download the product they just bought. Some cannot activate their purchase because the software licensing server times out. Frustrated customers email the company. Customer support phone lines light up. The company phone greeting is changed to inform callers of the situation. Online ad campaigns and search engine keyword buys are suspended to save money and reduce frustration among potential customers. Revenue is lost. Staff are diverted from normal duties.

Of course, different companies were impacted differently by 10/21. Some experienced prolonged outages, others were offline for just minutes, but even one minute of internet time can represent a lot of transaction. For example, Amazon's online retail revenue per minute is over $200,000. In that same minute over 50,000 apps are downloaded from Apple's app store. Clearly, 10/21 demonstrated how vital the internet infrastructure is to everyday commerce, but was it also an attack on critical infrastructure? We did not hear any reports of 10/21 impairing critical activating sectors such as transportation, water, agriculture, energy, and so on. Yet it is not hard to see how variations of the 10/21 attack on DNS could impact elements of the critical infrastructure, like airline ticketing, supply chain communications, or even power distribution. And it is possible to see such attacks as part of a pattern pointed out by security technologist Bruce Schneier: "Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the Internet."

..expect an interesting and complex mix of political and social reactions from nation states that now need to wrestle with the implications of an attack on critical infrastructure...

A troubling outlook

The likely trend for 2017 is further probing of critical infrastructure via the internet infrastructure. A variety of different attackers will continue to look for ways to cause damage, deny service, or hold data hostage. We also expect further attacks on the internet infrastructure itself, disrupting access to data and services. And of course, some of those data and services could be vital to the smooth running of one or more of the 16 categories of critical infrastructure. For example, some criminal hackers have shown a willingness to target medical data and systems. This trend is likely to be global.

At the same time, we know there are plenty of efforts underway in different countries to improve the cybersecurity of the systems that support critical infrastructure. In the US, there are now 24 ISACs, as in Information Sharing and Analysis Centers, covering most aspects of the 16 critical infrastructure sectors and providing expedited channels of communication and knowledge sharing on cybersecurity. In September, the Industrial Internet Consortium published a proposed security framework for the Industrial Internet of Things, in an effort to achieve broad industry consensus on how to secure this rapidly growing sector.

We sincerely hope that efforts like this, and others around the world, get the backing and resources they need to succeed; however, for this to happen it will take more than good intentions. It might even require political pressure from the folks most likely to suffer from cyberattacks on critical infrastructure, the electorate. For example, you might think that legislation giving the government more power to protect the electric grid from cyberattacks was a slam dunk. Indeed, in April of 2016 the US Senate approved such legislation, which has bipartisan support. Yet, with 2017 rapidly approaching, the bill had still not been passed.

As the global landscape becomes increasingly interconnected and interdependent across political, physical, and ideological boundaries, expect an interesting and complex mix of political and social reactions from nation states that now need to wrestle with the implications of an attack on this critical infrastructure, and what, if any, is an appropriate defensive and/or offensive response to an attack. To say we have a challenging year ahead is probably an understatement.

Challenges and implications of cybersecurity legislation

- Cybersecurity: organization, collaboration and diffusion across the globe
- Challenges and implications of the enactment of laws relating to cybersecurity
- Working towards the development and popularization of cybersecurity culture

AUTHOR

Miguel Ángel Mendoza
ESET Security Researcher

8

Challenges and implications of cybersecurity legislation

Technology has had an impact on nearly every aspect of society, and will continue to do so in the coming years. Many of today's activities are increasingly dependent on information systems, electronic devices, and data networks – a trend which is leading to hyperconnectivity. At the same time, we are seeing new threats and vulnerabilities emerge, and as a result, security risks are increasing in number, frequency and impact.

Therefore, the ascendancy of technology in today's societies, and the risks associated with its use, demonstrate the need to protect information and other assets at various levels and in various fields, not just for industries, companies and users, but also for countries. Legislation in several countries is requiring increased and improved security, based on objective moral and ethical criteria.

The promulgation of laws relating to the scope of cybersecurity highlights the importance of implementing large-scale regulatory frameworks, which would contribute to reducing security incidents and preventing IT crime, all while developing and establishing a culture of cybersecurity.

But despite the benefits that such legislation may bring to data security, the reality is that there are various tensions, positions and counterpoints, which mean that setting it up is not an easy task. In this section, we will look at some of the most significant legislation, in international terms, and some of the current and future challenges facing states, companies and users/citizens around the world.

Cybersecurity: organization, collaboration and diffusion across the globe

Recent times have seen a trend towards new cybersecurity legislation across the world. Based on collaboration between public and private sectors to effect the exchange of information and the creation of national cybersecurity agencies, the aim is to develop tools to cope with the risks of the digital era and to legislate against cybercrime.

European Union

The EU recently adopted the NIS Directive for the security of information networks and systems, seeking the promotion of legislation encouraging member countries to be equipped and prepared to respond to incidents, by having a Computer Security Incident Response Team (CSIRT) and a national authority competent in this area.

The creation of a CSIRT network is intended to promote rapid and effective cooperation, the exchange of risk-related information, and the development of a culture of security among sectors vital to Europe's economy and society, such as energy, transport, finance, health, and digital infrastructure. The new laws are aimed at

encouraging the homogeneous development of cybersecurity capacities and at preventing incidents that threaten economic activities, infrastructure, the confidence of users, and the operation of systems and networks critical to each country.

United States

At the end of 2015, the United States Congress approved what is known as the Cybersecurity Act of 2015 to protect the country from cyberattacks responsibly and promptly, through a framework promoting the exchange of information between the private sector and the government about computer threats.

Under the act, information about a threat found on a system may be shared with the aim of preventing attacks or mitigating risks that may affect other companies, agencies or users. Through the use of information gathering, security checks and other protective measures, organizations and governments are able to coordinate intelligence and defensive actions.

Latin America

In a recent report, a model was applied to determine cybersecurity capacity in Latin America and the Caribbean. This document highlights the importance of responsible disclosure of information in public and private sector organizations when a vulnerability is identified.

It also emphasizes the importance of legislative frameworks, investigation, the processing of electronic evidence, and the training of judges and prosecutors in the field of cybersecurity. Adherence to international conventions, such as the Budapest Convention, and being a signatory to cross-border agreements for cooperation, are other decisive factors. Similarly, adoption of best practices along with the use of security technologies are considered, for the formation of a "resilient cyber society".

Asia-Pacific

Another study seeking to ascertain the level of sophistication in cybersecurity, which focused on countries in the Asia-Pacific region [PDF], also considers legislation as a basic indicator of the security landscape. In 2016, several countries in this region have launched new cybersecurity policies or strategies, and have also updated existing standards, in order to adapt to new challenges and emerging issues.

For example, Australia has implemented a cybersecurity strategy, which provides for additional funds and has sought increased commitment from the private sector to engage with the country's cyber policy. Other countries, like New Zealand, have launched national cybersecurity strategies, focusing on improving their resilience, international cooperation, and the ability to respond to cybercrime.

Challenges and implications of the enactment of laws relating to cybersecurity

The current status of risks presents the need for regulatory frameworks for security management – an increasingly popular organizational trend. Similarly, when we refer to legislation, we are referring to the application of standards on a large scale, with a view to cybersecurity regulation at the national level.

Generally, legislation is quite effective when it comes to regulating behavior. However, there are challenges to be overcome for effective application of the laws. For example, the Global Agenda Council Report on Cybersecurity [PDF] presents the challenges faced by countries that have started to legislate in this area, based on the *Budapest Convention*. Nevertheless, these countries can enter into other global or regional conventions, and even take part in specific local initiatives.

Adoption of best practices along with the use of security technologies are considered, for the formation of a "resilient cyber society".

Evidence suggests that, given the influence of technology and the habits it instils, implementation of legislation can impact various stakeholders ranging from technology companies to users themselves. These tensions lead to different conflicts and challenges, which we shall consider below.

Delay in the enactment of laws

Various elements determine the creation of laws in different countries, so their promulgation depends on a multiplicity of factors; for example, political issues or other issues affecting local initiatives, or adherence to international agreements encouraging the same level of development for cross-border collaboration.

However, it is on account of these same conditions and characteristics that legislation is often postponed. For example, in 2016 almost half of the countries that have ratified their participation in the Budapest Convention have taken a decade or more to complete the said ratification, due to – among other things – the delay in the development of their laws. Moreover, the Convention just focuses on certain legal aspects within the range of possibilities related to the scope of cybersecurity.

Laws falling behind in context and time

In connection with the previous point, it should also be considered that technology is advancing at a rapid rate; the development of standards may, therefore, fall far behind technological advances. Just as organizations continuously update their standards in response to evolving risks and new technologies, the law must be in the vanguard in responding to the present and emergent issues which may need to be regulated.

Perhaps the way to rectify this disparity between technological innovation (and the risks it entails) and the enactment of appropriate legal measures, is to focus on regulating human behaviors, especially since technologies can become obsolescent in a relatively short period. This may prove to be the most reliable way for regulation to be effective, but it is also important to note that this could lead to rising tensions in the future. An example of this might be trying to regulate behaviors which, on occasion, are converted into tacit consent, such as the use of social networks, which are not supported by legislative enactment.

Technical and legal heterogeneity

We should also consider that countries vary in the ways in which they adhere to international or regional conventions, and these differences even determine specific initiatives for the development of their laws. Legal and technical disparities make it difficult to respond to, investigate, and rule on cybersecurity incidents, and inhibit international collaboration.

For example, regional or bilateral initiatives are developed to meet specific needs, as is the case with the EU-US Privacy Shield, a framework seeking to protect the fundamental rights of anyone in the EU whose personal data are transferred to companies in the US. This, of course, does not take into account collaboration with other countries or regions.

Conflicts of laws and basic principles

In this same context, legislation is generally quite effective when it comes to regulating behavior; however, there are no perfect laws. On the contrary, they can always be improved, particularly if we consider that there are projects which could undermine not only the principles on which the internet is based but even certain basic human rights.

Based on the idea that the internet is free and has no physical borders, there are cases where although legislation applies on a national level, constitutional or legal conflicts arise, mainly concerning the meanings and conceptions of privacy and free-

dom of expression. In this case, the eternal debate between privacy and security may come into play.

Limitations on the scope of application

Similarly, the absence of legislation or agreements on specific aspects of certain issues can undermine international collaboration, even within the same territory. Public and private sectors face a challenge when it comes to access to information for investigations, with implications for security, the right to privacy, and commercial interests, mainly of tech companies.

As an example, we have the well-known case between the FBI and Apple, in which a US judge requested the cooperation of the technology giant in order to unlock the iPhone of a terrorist involved in an attack, or the recent case in which a judge in Rio de Janeiro ordered the blocking of WhatsApp throughout Brazil and fines against Facebook. Such events clearly demonstrate the need for local and cross-border agreements to collaborate, which avoid conflicting interests.

Working towards the development and popularization of cybersecurity culture

The promulgation of laws relating to cybersecurity has gained prominence at an international level for some years now, on account of the number, frequency, and impact of incidents recorded worldwide. Various initiatives regard legislation in this area as a fundamental factor that increases a country's level of maturity. The aim is therefore to have legal measures in place for protection at various levels and in various fields.

To this end, legislators have also started to consider the elements necessary for security in their countries, including their capacity to respond to large-scale incidents, the protection of their critical infrastructure, their ability to collaborate with other countries, and even to consider the development of a security culture which can be instilled in the population. Not to mention issues that are already well-known, such as privacy, the protection of personal details, and cybercrime.

We are facing a growing trend in the development of new legislation that defines how a country's assets are protected in the context of cybersecurity, as well as promoting cooperation and collaboration between the public and private sectors of each country, and also at an international level so as to thwart current and emerging information threats and attacks.

However, despite the benefits this may represent, there are challenges that need to be overcome to achieve this aim and to understand the characteristics, needs and conditions that apply in both the public and the private sectors, and of all stakeholders in their roles as both users and citizens. Obstacles to and limitations on collaboration may include a lack of trust, ineffective legislation, and differing interests between the various sectors.

In the light of these challenges and tensions, we can see the need to define clear rules for all stakeholders, perhaps based on international, regional or local agreements, which consider all parties, with the objective of making legislation truly effective, capable of being applied and executed. Without a doubt, there is still much to be done, requiring collaboration between governments, private initiatives, the academic sector, and of course, users. All this aims to achieve a broad objective: working towards the development of a cybersecurity culture.

We are facing a growing trend in the development of new legislation that defines how a country's assets are protected in the context of cybersecurity.

Gaming platforms

The risk of the integration between consoles and computers

› The integration from gaming consoles with computers is growing and this could have an impact in terms of information security. One the one side, there are many hardware resources available, which could be interesting for an attacker. On the other, videogames are integrating with computers such as the Xbox connecting with Windows and starting to share login credentials and so on. Also important to note Steam Machine and its security implications and secure software development has a bigger role on the gaming industry.

AUTHOR

Cassius Puodzius
ESET Security Researcher

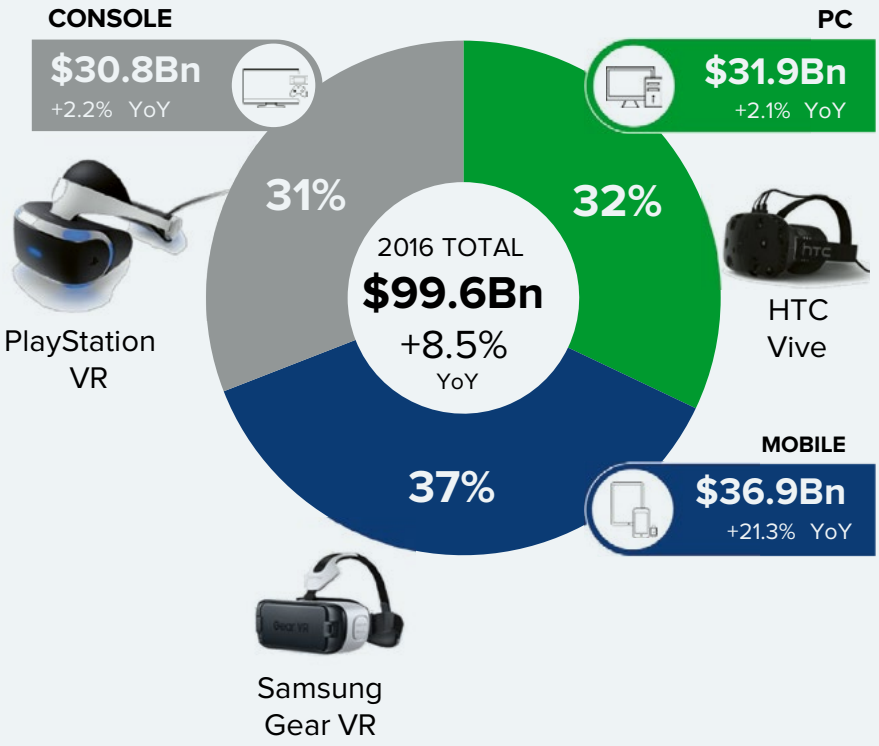
Gaming platforms: The risk of the integration between consoles and computers

Video games use cutting-edge technologies comprising advanced hardware and software to deliver a compelling entertainment experience to users. Gaming is so popular and successful that it now constitutes a significant portion of the whole global entertainment market and, undeterred by financial crises, has been growing rapidly and is expected to continue its expansion [PDF] in the foreseeable future.

Myriads of people around the globe spend great amounts of money to play games on many different platforms, such as video game consoles, PCs and mobile phones. Unsurprisingly, gaming platforms are valuable targets for blackhats looking for fame, fun and profit.

According to Newzoo's 2016 Global Games Market Report [PDF], games will attain a growth rate of 8.5% year-over-year (YoY, year-on-year in UK) in 2016, achieving a revenue of almost $100Bn. Mobile games play an important role in that result, since games on mobile phones and tablets will be re-

Figure 1: Gaming market share, size and YoY growth in 2016



Source: resources.newzoo.com

sponsible for $36.9Bn by the end of 2016, representing 37% of the gaming market. Projected growth in the gaming market over the next few years indicates a total revenue reaching $118.6Bn by 2019.

Maturation of mobile gaming (which attracts lots of new casual players) and the alluring gaming experience available across a wide range of platforms, have enabled the video game industry to experience steady success; consequently, the gaming market's growth has two chief strategies: ***diversification*** and ***casual gaming***.

Threat landscape in the gaming industry

Gaming business models have evolved radically in the last few years, which may be partially attributed to hedging against security-related threats. Nevertheless, such hazards also keep adapting to changes and continue to jeopardize the security of games.

In the past, games generated revenue primarily through "packed software sales" [PDF], whereby users pay a license fee upfront and own the right to play the game for as long as they want. Although this continues to be a relevant business model in the gaming market, it has been shrinking over past few years.

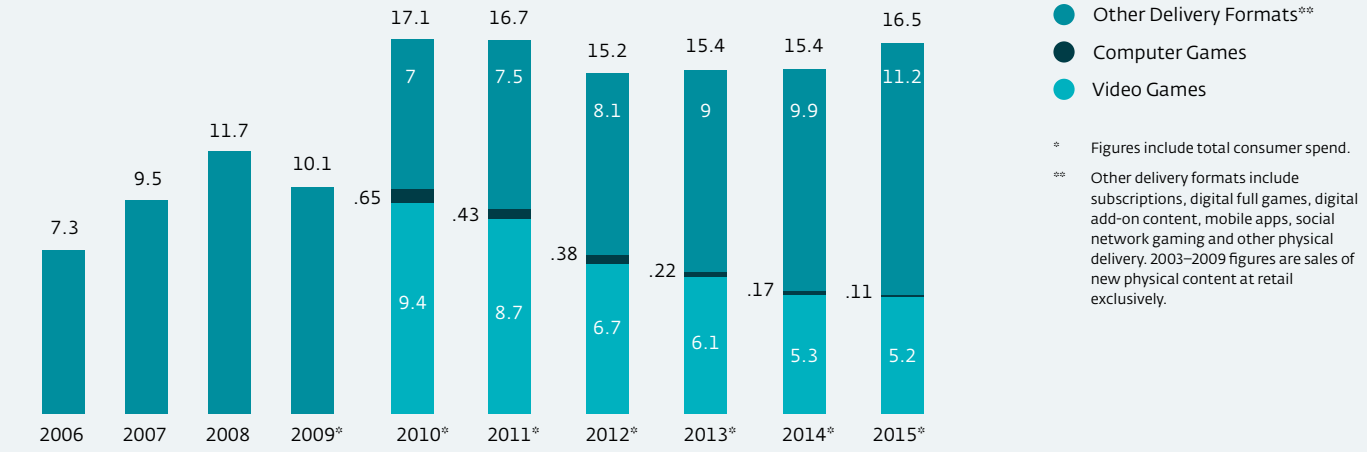
Figure 2: Recent history of console game hacking

DEVICE	YEAR	SECURITY	HACKED	FOR	FOR
PS 2	1999	?	?	Piracy	—
dbox2	2000	signed kernel	3 months	Linux	pay TV decoding
GameCube	2001	encrypted boot	12 months	Homebrew	piracy
Xbox	2001	encrypted / signed bootup, signed executables	4 months	Linus Homebrew	piracy
iPod	2001	checksum	< 12 months	Linux	—
DS	2004	signed / encrypted executables	6 months	Homebrew	piracy
PSP	2004	signed bootup / executables	2 months	Homebrew	piracy
Xbox 360	2005	encrypted / signed bootup, encrypted / signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linus Homebrew	leaked keys
PS3	2006	encrypted / signed bootup,encrypted / signed executables, hypervisor, eFuses, isolated SPU	4 years	Homebrew Piracy	piracy
Wii	2006	encrypted bootup	1 month	Linux	piracy
Apple TV	2007	signed bootloader	2 weeks	Linux	Front Row piracy
iPhone	2007	signed / encrypted bootup / executables	11 days	Homebrew SIM-Lock	piracy
iPad	2010	signed / encrypted bootup / executables	1 day	Homebrew	piracy

Source: https://www.youtube.com/watch?v=PRgtFXz4Quc

Threat level 1 2 3 4 5 6

Figure 3: Growth of "Other Delivery Formats" in the US game market over the last 10 years



Source: The NPD Group/Retail Tracking Service; Games Market Dynamics: U.S. See more in PDF here

One of the reasons that game companies have been moving away from this model is piracy. For instance, Nintendo, a giant in the game industry, pleads against counterfeiting: *"Piracy continues to be a significant threat to Nintendo's business, as well as [to] over 1,400 game development companies working to provide unique and innovative games for the Nintendo platform."*

Despite efforts by the industry to deploy security countermeasures aimed at combating piracy, we have seen continual console hacking for decades. A recent example being 2016's *failOverflow* hack group that released a PlayStation 4 hack, which was not focused on counterfeiting, but did, however, enable piracy as a side effect.

To cope with piracy as well as to diversify the gaming business model, over recent years the industry has had some success by improving "other delivery formats" [PDF]. Such delivery formats comprise subscriptions, full versions of digital games (as opposed to packed shareware or demo versions available for download), digital add-on contents, mobile and social network games, as well as other forms of sales that differ from the traditional packaged game software.

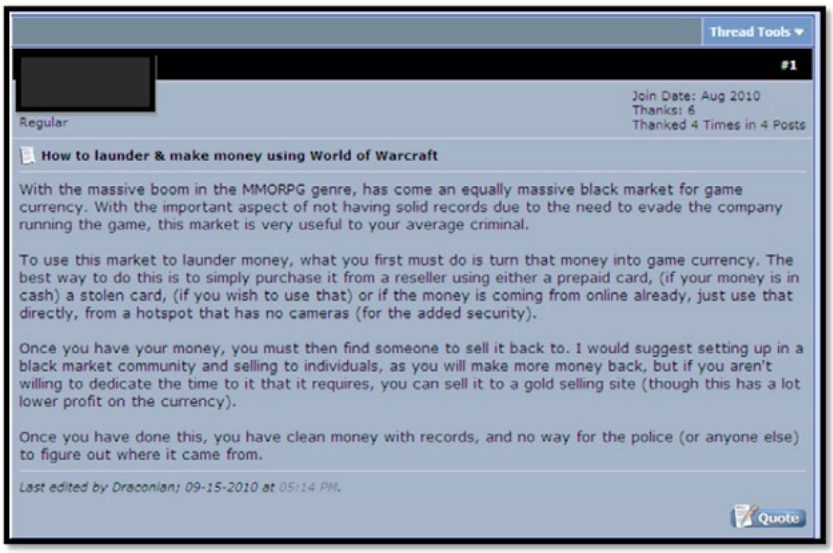
Such novel business models are more internet-dependent than ever before. Furthermore, game platforms endowed with network connections carry a greater level of risk to computer security, since cyber-aggressors may exploit vulnerabilities in order to control the game platform remotely or install malware in order to gain access to players' sensitive information.

Nonetheless, hyping online gaming is nothing new. Online games for PCs date from the early days of the commercial internet, due to the possibility of installing network boards onto computers, and with the expansion of broadband internet, online gaming followed the trend by releasing very successful titles. These attracted vast numbers of players, becoming what is known as massively multiplayer online games (MMOs). For instance, in 2010 the game *World of Warcraft* (WoW) achieved a peak of 12 million subscribers worldwide.

Figure 4: Stealing items from a WoW user's account

Source: http://www.wonderlandblog.com/wonderland/2009/01/wow-account-hacked.html

Figure 5: Forum post about how to launder dirty money with MMO



Source: https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf

Online gamers have to deal with common cyberthreats, such as malware-wrapped game installers, which bind Trojans into game software, or malicious campaigns that portray themselves as making popular games available – such as those that we have seen this year exploiting the launch of Pokémon Go – but also spread malware or steal players' accounts. However, as the business model evolves, new kinds of threats arise.

When players engage in gaming, it is not uncommon to find that they are willing to exchange real money for virtual, in-game, goods. Hence, cybercriminals use online games for *money laundering*. Virtual in-game goods are sold on e-commerce sites like eBay, after game items have been stolen from other players' accounts [PDF] or bought using dirty money [PDF], cashing in on real and clean money.

In the case of WoW, this kind of incident was noteworthy enough to push Blizzard to issue a security alert after a spate of unauthorized logins and player reports of "money laundering" scams in 2013.

Another way that cybercriminals go after user data is by directly assaulting game companies. Companies like Blizzard, Steam, Sony (and others) suffered from data breaches that pose risks such as money laundering, as previously mentioned, or direct financial losses for the company and customers, when credit card data and customers' personal information are stolen.

Cyberthreats notwithstanding, console games started to go online about a decade ago – after all, they represent a huge and profitable market. Console game giants like Microsoft (Xbox), Nintendo (Wii) and Sony (PlayStation) went live from 2002 with Xbox Live being the first, followed by Nintendo Wi-Fi Connection (2005) and PlayStation Network (a.k.a. PSN, 2006), respectively.

All the initiatives referenced above are online delivery services designed to supply multiplayer gaming and digital media. As a matter of fact, they have undergone considerable remodeling since their creation; for instance, Nintendo Wi-Fi Connection was replaced by Nintendo Network (a.k.a. NN) in 2012.

Altogether, the network communities comprise almost 185 million members. Such high numbers of members turned these game networks into great targets for hacktivism. On Christmas Eve 2014, a cyber-hacker team known as Lizard Squad carried out successful DDoS attacks against PlayStation Network and Xbox Live. These took down services for many hours and stopped only after Lizard Squad was granted 3000 MegaPrivacy vouchers. It should be clear by now that the threat landscape in the game industry is very challenging. This is no surprise considering the market's size, wealth and welfare. Game companies are investing heavily in cyber threat counter measures, and at the same time, pursue market expansion by releasing games on a larger number of platforms in order to attract more people to play.

Convergence and future threats

The ever-increasing number of players, in conjunction with in-game monetary transactions, poses major security challenges for the future. On top of that, integrated networking of gaming consoles with computers and mobiles is growing fast, this can have a significant impact on gaming's information security in the coming years.

Newzoo's 2016 Global Games Market Report reveals that 87% of console gamers also play games on PCs, and it designates the PC as the "hub for console gaming". To support this statement, it is noted in the report that PCs and mobiles are essential devices, whereas video game consoles are not. Furthermore, the report stresses that PCs are devices much more suitable for online content sharing than consoles and also the fact that PC users upgrade more often and routinely than console users do.

Different gaming platforms, which used to evolve independently, are starting to dovetail, meaning that games are being developed to provide the same user experience irrespective of which platform they run on. As a result, different gaming platforms are evolving toward rendering games (as well as other content types) in a similar manner, hence their convergence.

Game companies are investing heavily in cyber threat counter measures, and at the same time, pursue market expansion by releasing games on a larger number of platforms in order to attract more people to play.

Microsoft dubbed their convergence strategy the "buy once, play everywhere" model. In 2013, Microsoft hired Jason Holtman, formerly in charge of the popular Steam PC game service at Valve, to lead Microsoft's game platform evolution. The company depicted this strategy as "the idea of playing a game on your Xbox, and then moving to your PC and picking up where you left off, without having to re-purchase the game or replay through the same levels".

In fact, the idea of partial interoperability is, to some extent, already implemented by console vendors. Wii U is able to stream games to GamePad, while PlayStation 4 streams to Vita. In the case of Microsoft's Xbox, the aim is to stream games to PCs.

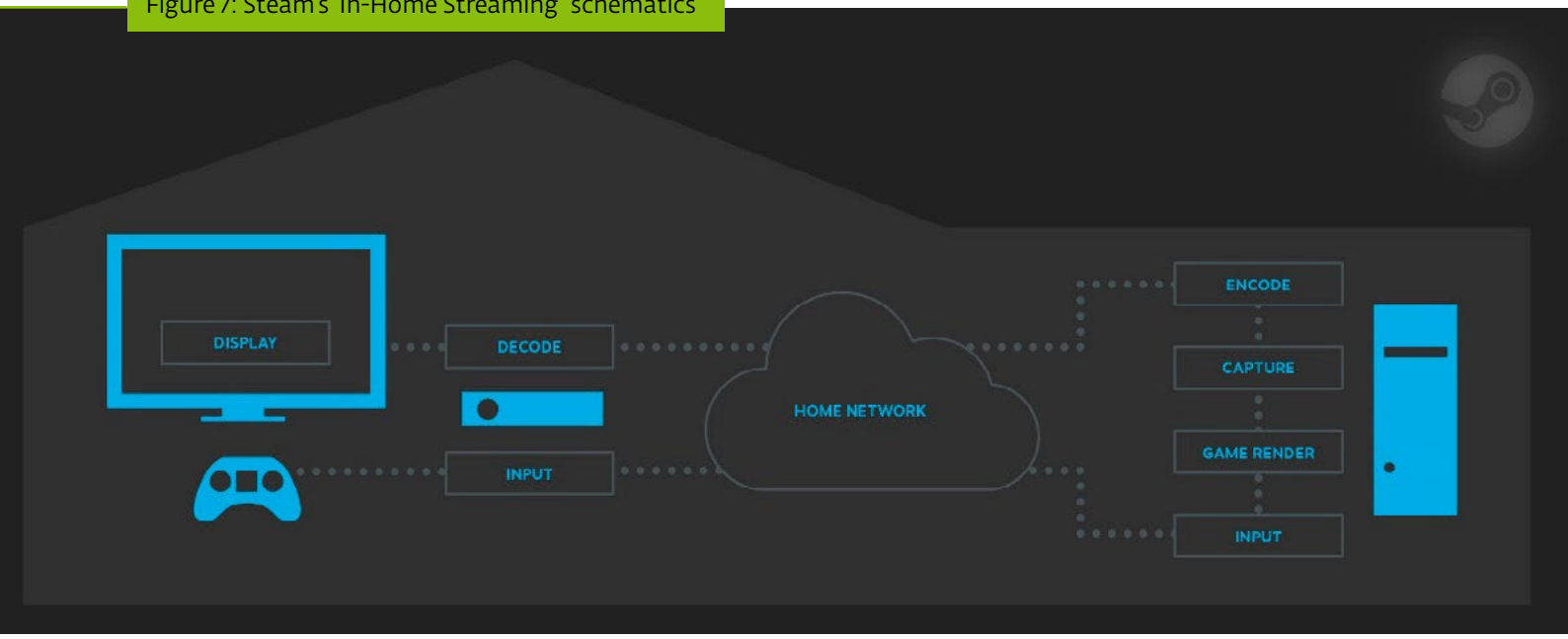
At the beginning of 2015, Microsoft announced plans to revamp its Xbox App for PC, which was launched in 2012 to provide Xbox users with Xbox Live access, remote control and second screen functionality. As of 2015, Xbox and Windows 10 were tightly integrated to construct Microsoft's gaming environment ideal. A few months after the Xbox App announcement, Xbox-to-PC streaming was released at GDC 2015. In 2016, it was the turn of the Xbox App for both iOS and Android, when the app was rebranded and revamped to include features from the Windows 10 Xbox App.

As a consequence of such integration, spyware running on compromised PCs and mobiles could snoop on players' chats and get access to different apps' passwords that were previously restricted to Xbox consoles only.

Figure 6: Microsoft's gaming platforms supported by Xbox App

Source: Microsoft's Xbox WireMicrosoft's Xbox Wire

Figure 7: Steam's "In-Home Streaming" schematics



Source: Steam

It may seem that the evolution of console games towards integration with other platforms is a one-way movement. However, Valve, an American game company well established in online gaming for PCs, is heading in the opposite direction.

Valve's portfolio includes very successful titles such as Half-Life, Counter-Strike and Dota. Valve is also the owner of Steam, the world's largest online gaming platform, which was one of TeslaCrypt's targets. TeslaCrypt is ransomware that encrypts more than 185 different types of files associated with games.

In 2015 Steam announced a record 125 million active users worldwide. On its website, Steam provides real-time stats about the platform showing, at the time of writing, a peak of almost 12.5M users logged in over the past 48 hours.

In May 2014, a feature called "In-Home Streaming" was released by Steam. This allows players who have multiple computers running Steam within the same network to join in and perform remote installation, launch games and play across different computers.

On the one hand, through In-Home Streaming, users can play a PC game on a lower-end computer connected to a primary gamer PC, and neither of the two computers even have to run the same operating system. On the other hand, In-Home Streaming permits full access to remote desktops by design, which could be used by hackers and malware for lateral movement in order to access and control different hosts inside the network.

Figure 8: Fastest apps to achieve 50 million downloads worldwide through October 2016

Based on worldwide Google Play release dates and download install ranges.

Source: sensortower.com

At the end of 2013, Valve launched SteamOS, a Linux distribution designed to run Steam games. The development of SteamOS paved the way for Valve's main strategy to gain further console gaming market share, Steam Machines. Valve launched Steam Machine in November 2015: this is a console-like gaming computer that runs SteamOS and allows users to play Steam (online) games on TV screens.

While games reach different platforms, there is a great effort being made to preserve a consistent playing experience across all those platforms. Thus ***convergence*** plays an important role alongside ***diversification***. At this point in time, it is uncertain which game companies will be most successful in their diversification strategies; nevertheless, it is fair to say that ***convergence*** is a cornerstone of the game industry.

Even wearables are becoming platforms for games. After the tremendous success of Pokémon Go, a game app released in 2016 that surpassed 500 million downloads around the world, Niantic Labs announced that an Apple Watch Pokémon Go app is already scheduled for release.

From a security standpoint, convergence brings great concern, since there will be more (valuable) data flowing to and from many different devices and platforms. In addition, other available resources will be at risk of being exploited for intrusion or control, allowing, for instance, the building of IoT botnets such as those that have emerged recently and affected many business, such as Twitter, Spotify, PayPal and many others.

At a personal level, games have access to data that are often sought by cybercriminals, such as personal and financial information. Furthermore, as gaming reaches new platforms, it allows even more data to become available – for instance, by exploiting a security flaw in games running on a wearable device, cybercriminals could steal health records from victims.

As games become increasingly online-based, their attack surfaces widen, thus it becomes important to raise the bar for security. Threats currently faced by the game industry are likely to reach platforms where they have not been witnessed so frequently before, while security incidents will tend to have even greater impact.

Homes and companies, especially due to recent discussions on the use of video games as a means to increase productivity in workplaces, may be exposed to cyber threats just by allowing or enabling games on their networks. The mere presence of a game console inside the office may expose the whole company to APTs that use the game platform as a foothold to pivot into internal networks – it is worth remarking that printers are often footholds for intrusion.

Moreover, security incidents related to games will have a greater potential impact on players. Case in point, Microsoft had the private key for the "xboxlive.com" digital certificate accidentally leaked in November 2015, and this could have been used to impersonate Microsoft's servers by way of attacking not only console players of Xbox Live, but also PC and mobile players.

Besides the usual care that we should always take with online games, especially when it comes to blockbuster releases such as 2016's Pokémon Go, the escalation of data flowing between devices during game play should be taken into account by game developers. They should work to make it harder to let players' gaming devices be exploited for malicious purposes and become entry points for attacks against home and business networks.

Denouement

We have discussed the evolution strategy of the game industry and how it is strongly related to the incorporation of new platforms. As a result of gaming's growth strategy, gaming platforms converge and become more interconnected, therefore their attack surfaces are likely to widen while the impact of security incidents tend to reach even further than at present.

From a security standpoint, common cyberthreats - such as malware and malicious campaigns using social engineering – jeopardize online gaming safety. In addition, particular security hazards, such as console and game hacking, MMO money laundering, data breaches and denial of services, may specifically target games.

Despite security threats, game platforms are becoming highly integrated. Xbox App interconnects games on consoles, computers and mobiles, while Steam's "In-Home Streaming" unifies the Steam Machine and computers running different operating systems.

Meanwhile, new platforms that carry users' sensitive data (even unprecedented types of data, such as health records accessible via wearables) are also evolving into game platforms, which makes them prime targets for cybercriminals. Consequently, the theme of security information should be treated as a transversal and key issue for games.

Conclusion

In this new edition of our Trends report, we looked at a wide variety of topics ranging from macroscale issues, such as critical infrastructure or legislative challenges that countries must tackle, to more everyday concerns closer to users, such as threats to IoT devices or video game consoles.

Despite the diversity of issues covered in the different sections, there is one common thread throughout them all: the human factor.

A phrase that has become almost dogma in information security is that the end user is the weakest link in the security chain, and commonly used by cybercriminals to spread their threats. This is undeniable, and hence the need for users and businesses to recognize security threats, how they propagate and what measures to implement in order to protect their privacy and information. However, the current concept of awareness is not enough: the relevance of the human factor has to be moved up to a higher level of importance.

We are at a juncture where the emergence of new applications and devices is accelerating: virtual reality, augmented reality, technology integration at all levels (from game consoles to IoT devices), server virtualization in the corporate environment and others. All these innovations could – and surely will – create new attack vectors for cybercriminals to take advantage of, and that is on top of the already long list of existing vectors.

This situation is further aggravated by the many users who easily fall victim to phishing campaigns or download malicious applications onto their devices without having protected them properly. The outlook becomes even more bleak when we look just over the horizon and see that everything is set for threats like RoT (Ransomware of Things) to explode. In short: we are at a stage in which we have users using latest generation technology, but with security concepts from over 10 years ago.

The dizzying advance of technology poses other challenges when it comes to the risks faced by users, and therefore to their awareness. Behind every new application or device, there is a group of people who should be thinking about information security from the design stage forward. The fact that there are increasing numbers of critical vulnerabilities is no accident; it is also clear that the attack surface is growing, making it necessary to consider security from project conception onward.

Likewise, awareness should extend to the industries and sectors that previously were not so bound to information security. Given the sensitive information they handle, we highlight security in critical infrastructure and the healthcare sector as important trends for the coming year. However, proper management and effective controls, in addition to supporting legislation and regulations, must also accompany education and awareness in these environments.

Beyond the somewhat pessimistic tone this review may have, the reality is that there are many possibilities for ensuring the secure use of technology. 2017 is shaping up to be a year in which security challenges will continue to grow and we are on cue to take on those challenges. This is not just about educating the end user; governments need to adopt legislative frameworks that promote cybersecurity issues, ranging from the provision of formal education on security issues to properly protecting critical infrastructure. In this sense, it is also imperative that businesses commit to carrying out proper information security management and that developers don't prioritize usability over the security of their products.

Information and its management are key aspects of today's societies, and therefore its proper protection is vital. Given the multiplicity of aspects and stakeholders involved, no one can take their eye off of it. So it is time to take charge of all aspects of security presented throughout this report, a joint effort among all the different parties involved: from large technology manufacturers, companies and governments down to, of course, users. If we can achieve consensus and agreement around these issues, the future of information security will be promising.

About ESET

Since 1987, ESET® has been developing award-winning security software that now helps over 100 million users to Enjoy Safer Technology. Its broad security product portfolio covers all popular platforms and provides businesses and consumers around the world with the perfect balance of performance and proactive protection.

The company has a global sales network covering more than 200 countries and territories, and regional offices in Bratislava, San Diego, Singapore and Buenos Aires. For more information visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

www.eset.com

ENJOY SAFER TECHNOLOGY™