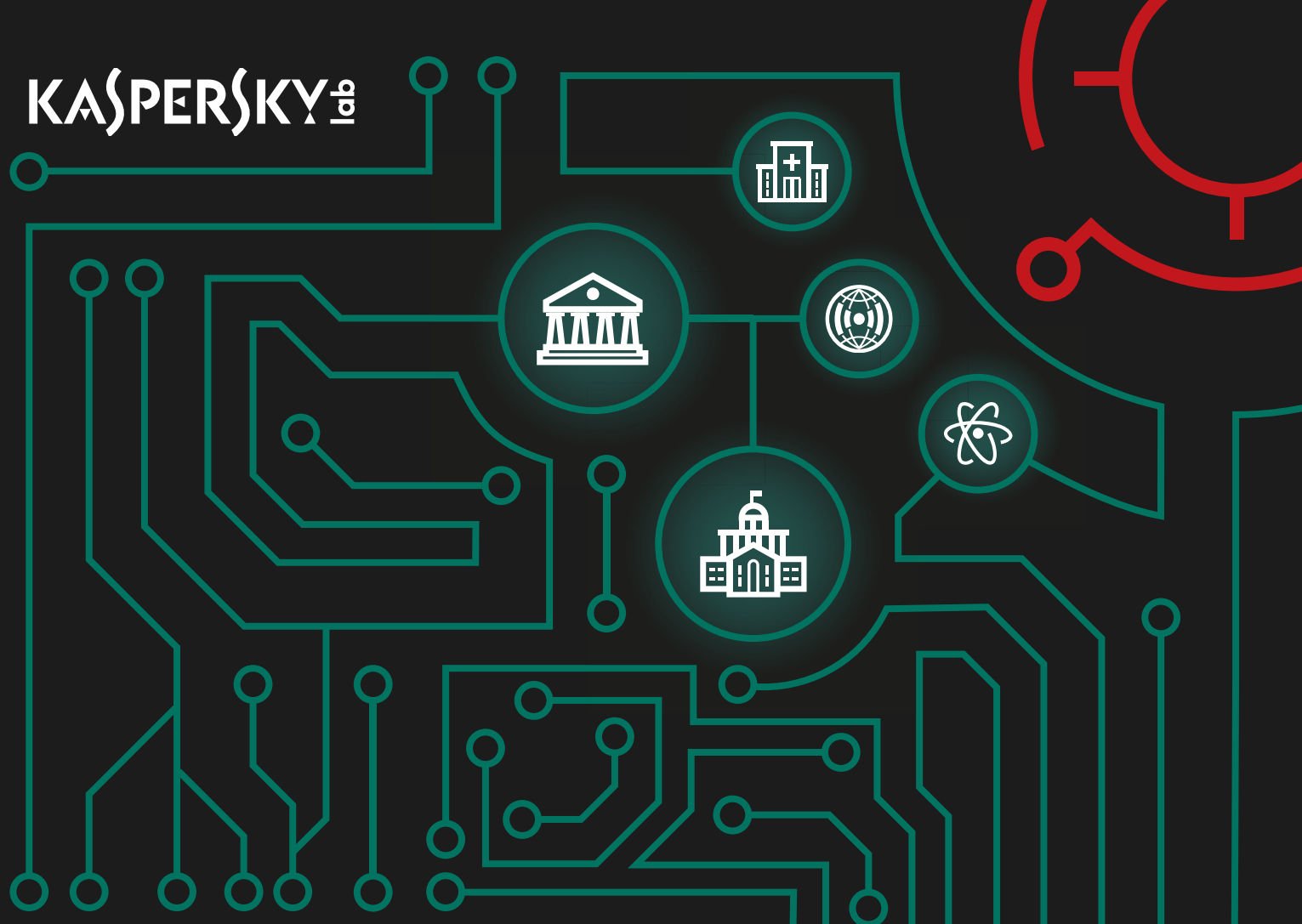
KASPERSKY lab



Kaspersky Security Bulletin:

KASPERSKY LAB THREAT PREDICTIONS FOR 2018

CONTENTS

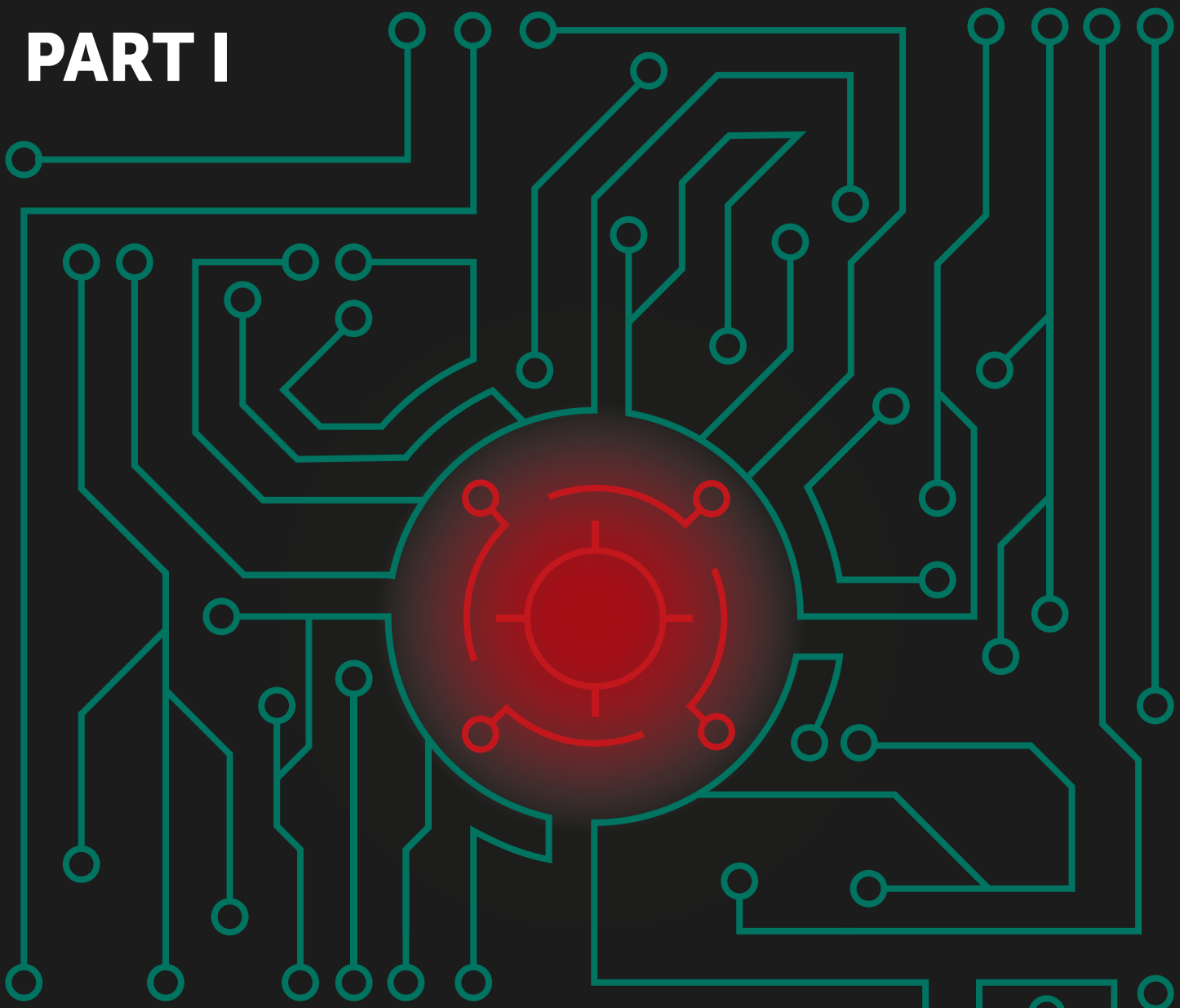
INTRODUCTION

In 2017, sophisticated threat actors continued to make the headlines with audacious politically motivated attacks and thefts. But this year, such events had to share the media limelight with a different kind of threat, targeting businesses of all sizes and spreading at breath-taking speed. Any gaps in network security, software patching, or employee awareness were ruthlessly exposed in the wave of destructive ransomware attacks of May and June, and more. The ultimate cost for some enterprises has run into hundreds of millions of dollars.

To reflect the growing need for enterprises to understand and prepare for the cyberthreats facing their sector, the Kaspersky Security Bulletin Predictions for 2018 includes not just the major targeted threat predictions prepared by the Global Research and Analysis Team, but a new section on industry and technology threat predictions.

All predictions are grounded in the research and experience gathered by Kaspersky Lab's experts over the course of 2017. They are our best estimate of what lies ahead, based on what we know now – and we hope that they will provoke thought, build awareness and drive action.

PART I



ADVANCED PERSISTENT THREAT PREDICTIONS

GREAT

INTRODUCTION

As hard as it is to believe, it's once again time for our APT Predictions. Looking back at a year like 2017 brings the internal conflict of being a security researcher into full view: on the one hand, each new event is an exciting new research avenue for us, as what were once theoretical problems find palpable expression in reality. This allows us to understand the actual attack surface and attacker tactics and to further hone our hunting and detection to address new attacks. On the other hand, as people with a heightened concern for the security posture of users at large, each event is a bigger catastrophe. Rather than consider each new breach as yet another example of the same, we see the compounding cumulative insecurity facing users, e-commerce, financial, and governmental institutions alike.

As we stated last year, rather than thinly-veiled vendor pitching, our predictions are an attempt to bring to bear our research throughout the year in the form of trends likely to peak in the coming year.

OUR RECORD

Did we get it right?

As a snapshot scorecard of our performance last year, these are some of our 2017 predictions and some examples where relevant:

Espionage and APTs:

Passive implants showing almost no signs of infection come into fashion – Yes!

Ephemeral infections / memory malware – Yes!

Espionage goes mobile – Yes!

Financial Attacks:

The future of financial attacks – Yes!

Ransomware:

Dirty, lying ransomware – Yes!

Industrial threats:

The ICS Armageddon didn't come yet (and we are happy to be wrong on that), however, we've seen ICS come under attack from Industoyer – Yes!

IoT:

A brick by any other name – Yes!

Information Warfare:

Multiple examples – Yes!

WHAT CAN WE EXPECT IN 2018?

More supply chain attacks

Kaspersky Lab's Global Research and Analysis Team tracks over 100 APT (advanced persistent threat) groups and operations. Some of these are incredibly sophisticated and possess wide arsenals that include zero-day exploits, fileless attack tools, and combine traditional hacking attacks with handovers to more sophisticated teams that handle the exfiltration part. We have often seen cases in which advanced threat actors have attempted to breach a certain target over a long period of time and kept failing at it. This was either due to the fact that the target was using strong internet security suites, had educated their employees not to fall victim to social engineering, or consciously followed the Australian DSD TOP35 mitigation strategies for APT attacks.

In general, an actor that is considered both advanced and persistent won't give up that easily, they'll continue poking the defenses until they find a way in.

When everything else fails, they are likely to take a step back and re-evaluate the situation. During such a re-evaluation, threat actors can decide a supply chain attack can be more effective than trying to break into their target directly. Even a target whose networks employ the world's best defenses is likely using software from a third-party. The third party might be an easier target and can be leveraged to attack the better protected original target enterprise.

During 2017, we have seen several such cases, including but not limited to:

- Shadowpad
- CCleaner
- ExPetr / NotPetya

During 2018, we expect to see more supply chain attacks, both from the point of discovery and as well as actual attacks.

These attacks can be extremely difficult to identify or mitigate. For instance, in the case of Shadowpad, the attackers succeeded in Trojanizing a number of packages from Netsarang that were widely used around world, in banks, large enterprises, and other industry verticals. The difference between the clean and Trojanized packages can be dauntingly difficult to notice – in many cases it's the command and control (C&C) traffic that gives them away.

For CCleaner, it was estimated that over 2 million computers received the infected update, making it one of the biggest attacks of 2017. Analysis of the malicious CCleaner code allowed us to correlate it with a couple of other backdoors that are known to have been used in the past by APT groups from the 'Axiom umbrella', such as APT17 also known as Aurora. This proves the now extended lengths to which APT groups are willing to go in order to accomplish their objectives.

Our assessment is that the amount of supply chain attacks at the moment is probably much higher than we realize but these have yet to be noticed or exposed. During 2018, we expect to see more supply chain attacks, both from the point of discovery and as well as actual attacks. Trojanizing specialized software used in specific regions and verticals will become a move akin to waterholing strategically chosen sites in order to reach specific swaths of victims and will thus prove irresistible to certain types of attackers.

More high-end mobile malware

In August 2016, CitizenLab and Lookout published their analysis of the discovery of a sophisticated mobile espionage platform named Pegasus. Pegasus, a so-called 'lawful interception' software suite, is sold to governments and other entities by an Israeli company called NSO Group. When combined with zero-days capable of remotely bypassing a modern mobile operating systems' security defenses, such as iOS, this is a highly potent system against which there is little defense. In April 2017, Google published its analysis of the Android version of the Pegasus spyware which it called Chrysaor. In addition to 'lawful surveillance' spyware such as Pegasus and Chrysaor, many other APT groups have developed their own mobile malware implants.

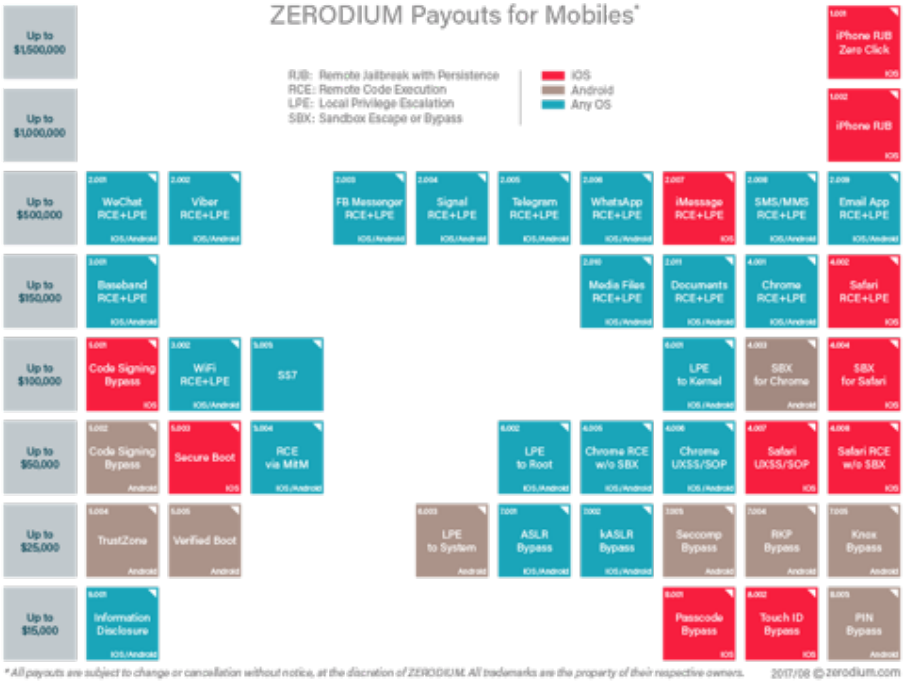
In 2018 more high-end APT malware for mobile will be discovered, as a result of both an increase in the attacks and improvement in security technologies.

Due to the fact that iOS is an operating system locked down from introspection, there is very little that a user can do to check if their phone is infected. Somehow, despite the greater state of vulnerability of Android, the situation is better on Android where products such as Kaspersky Internet Security for Android are available to ascertain the integrity of a device.

Our assessment is that the total number of mobile malware existing in the wild is likely higher than currently reported, due to shortcomings in telemetry that makes these more difficult to spot and eradicate. We estimate that in 2018 more high-end APT malware for mobile will be discovered, as a result of both an increase in the attacks and improvement in security technologies designed to catch them.

More BeEF-like compromises with web profiling

Due to a combination of increased interest and better security and mitigation technologies being deployed by default in operating systems, the prices of zero-day exploits have skyrocketed through 2016 and 2017. For instance, the latest Zerodium payout chart lists up to $1,500,000 for a complete iPhone (iOS) Remote jailbreak with persistence attack, which is another way of saying 'a remote infection without any interaction from the user'.



The incredible prices that some government customers have most certainly chosen to pay for these exploits mean there is increasing attention paid towards protecting these exploits from accidental disclosure. This translates into the implementation of a more solid reconnaissance phase before delivering the actual attack components. The reconnaissance phase can, for instance, emphasize the identification of the exact versions of the browser used by the target, their operating system, plugins and other third-party software. Armed with this knowledge, the threat actor can fine tune their exploit delivery to a less sensitive '1-day' or 'N-day' exploit, instead of using the *crown jewels*.

The usage of profiling toolkits such as 'BeEF' will increase in 2018 with more groups adopting either public frameworks or developing their own.

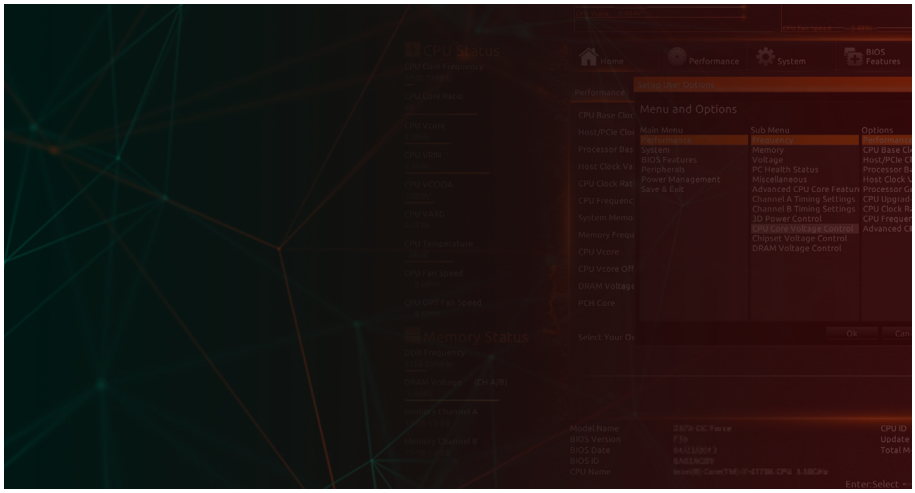
These profiling techniques have been fairly consistent with APT groups like Turla and Sofacy, as well as Newsbeef (a.k.a. Newscaster, Ajax hacking team, or 'Charming Kitten'), but also other APT groups known for their custom profiling frameworks, such as the prolific Scanbox. Taking the prevalence of these frameworks into account in combination with a surging need to protect expensive tools, we estimate the usage of profiling toolkits such as 'BeEF' will increase in 2018 with more groups adopting either public frameworks or developing their own.

Sophisticated UEFI and BIOS attacks

In 2018 we will see the discovery of more UEFI-based malware.

The Unified Extensible Firmware Interface (UEFI) is a software interface which serves as the intermediary between the firmware and the operating system on modern PCs. Established in 2005 by an alliance of leading software and hardware developers, Intel most notable amongst them, it's now quickly superseding the legacy BIOS standard. This was achieved thanks to a number of advanced features that BIOS lacks: for example, the ability to install and run executables, networking and Internet capabilities, cryptography, CPU-independent architecture and drivers, etc. The very advanced capabilities that make UEFI such an attractive platform also open the way to new vulnerabilities that didn't exist in the age of the more rigid BIOS. For example, the ability to run custom executable modules makes it possible to create malware that would be launched by UEFI directly before any anti-malware solution – or, indeed, the OS itself – had a chance to start.

The fact that commercial-grade UEFI malware exists has been known since 2015, when the Hacking team UEFI modules were discovered. With that in mind, it is perhaps surprising that no significant UEFI malware has been found, a fact that we attribute to the difficulty in detecting these in a reliable way. We estimate that in 2018 we will see the discovery of more UEFI-based malware.



Destructive attacks continue

Beginning in November 2016, Kaspersky Lab observed a new wave of wiper attacks directed at multiple targets in the Middle East. The malware used in the new attacks was a variant of the infamous Shamoon worm that targeted Saudi Aramco and Rasgas back in 2012. Dormant for four years, one of the most mysterious wipers in history has returned. Also known as Disttrack, Shamoon is a highly destructive malware family that effectively wipes the victim machine. A group known as the 'Cutting Sword of Justice' took credit for the Saudi Aramco attack by posting a Pastebin message on the day of the attack (back in 2012), and justified the attack as a measure against the Saudi monarchy.

The Shamoon 2.0 attacks seen in November 2016 targeted organizations in various critical and economic sectors in Saudi Arabia. Just like the previous variant, the Shamoon 2.0 wiper aims for the mass destruction of systems inside compromised organizations. While investigating the Shamoon 2.0 attacks, Kaspersky Lab also discovered a previously unknown wiper malware that appears to be targeting organizations in Saudi Arabia. We've called this new wiper StoneDrill and have been able to link it with a high degree of confidence to the Newsbeef APT group.

2017 has been a tough year in terms of destructive attacks. They will continue to rise, leveraging its status as the most visible type of cyberwarfare.

In addition to Shamoon and Stonedrill, 2017 has been a tough year in terms of destructive attacks. The ExPetr/NotPetya attack, which was initially considered to be ransomware, turned out to be a cleverly camouflaged wiper as well. ExPetr was followed by other waves of 'ransomware' attacks, in which there is little chance for the victims to recover their data; all cleverly masked 'wipers as ransomware'. One of the lesser known facts about 'wipers as ransomware' is perhaps that a wave of such attacks was observed in 2016 from the CloudAtlas APT, which leveraged what appeared to be 'wipers as ransomware' against financial institutions in Russia.

In 2018, we estimate that destructive attacks will continue to rise, leveraging its status as the most visible type of cyberwarfare.

More subversion of cryptography

In March 2017, IoT encryption scheme proposals developed by the NSA came into question with Simon and Speck variant ISO approvals being both withdrawn and delayed a second time.

In August 2016, Juniper Networks announced the discovery of two mysterious backdoors in their NetScreen firewalls. Perhaps the most interesting of the two was an extremely subtle change of the constants used for the Dual_EC random number generator, which would allow a knowledgeable attacker to decrypt VPN traffic from NetScreen devices. The original Dual_EC algorithm was designed by the NSA and pushed through NIST. Back in 2013, a Reuters report suggested that NSA paid RSA $10 million to put the vulnerable algorithm in their products as a means of subverting encryption. Even if the theoretical possibility of a backdoor was identified as early as 2007, several companies (including Juniper) continued to use it with a different set of constants, which would make it theoretically secure. It appears that this different set of constants made some APT actor unhappy enough to merit hacking into Juniper and changing the constants to a set that they could control and leverage to decrypt VPN connections.

In 2018 more severe cryptographic vulnerabilities will be found and patched, be they in the standards themselves or the specific implementations.

These attempts haven't gone unnoticed. In September 2017, an international group of cryptography experts have forced the NSA to back down on two new encryption algorithms, which the organization was hoping to standardize.

In October 2017, news broke about a flaw in a cryptographic library used by Infineon in their hardware chips for generation of RSA primes. While the flaw appears to have been unintentional, it does leave the question open in regards to how secure are the underlying encryption technologies used in our everyday life, from smart cards, wireless networks or encrypted web traffic. In 2018, we predict that more severe cryptographic vulnerabilities will be found and (hopefully) patched, be they in the standards themselves or the specific implementations.

Identity in e-commerce comes into crisis

The past few years have been punctuated by increasingly catastrophic large-scale breaches of personally identifiable information (PII). Latest among these is the Equifax breach reportedly affecting 145.5 million Americans. While many have grown desensitized to the weight of these breaches, it's important to understand that the release of PII at scale endangers a fundamental pillar of e-commerce and the bureaucratic convenience of adopting the Internet for important paperwork. Sure, fraud and identity theft have been problems for a long time, but what happens when the fundamental identifying information is so widely proliferated that it's simply not reliable at all? Commerce and governmental institutions (particularly in the United States) will be faced with a choice between scaling back the modern comforts of adopting the Internet for operations or doubling down on the adoption of other multi-factor solutions. Perhaps thus far resilient alternatives like ApplePay will come into vogue as de facto means of insuring identity and transactions, but in the meantime we may see a slowdown in the critical role of the Internet for modernizing tedious bureaucratic processes and cutting operational costs.

More router and modem hacks

Routers and modems are critically important to daily operations, and tend to run proprietary pieces of software that go unpatched and unwatched.

Another known area of vulnerability that has gone vastly ignored is that of routers and modems. Be they home or enterprise, these pieces of hardware are everywhere, they're critically important to daily operations, and tend to run proprietary pieces of software that go unpatched and unwatched. At the end of the day, these little computers are Internet-facing by design and thereby sitting at a critical juncture for an attacker intent on gaining persistent and stealthy access to a network. Moreover, as some very cool recent research has shown, in some cases attackers might even be able to impersonate different Internet users, making it possible to throw off the trail of an attacker entirely to a different connecting address. At a time of increased interest in misdirection and false flags, this is no small feat. Greater scrutiny of these devices will inevitably yield some interesting findings.

A medium for social chaos

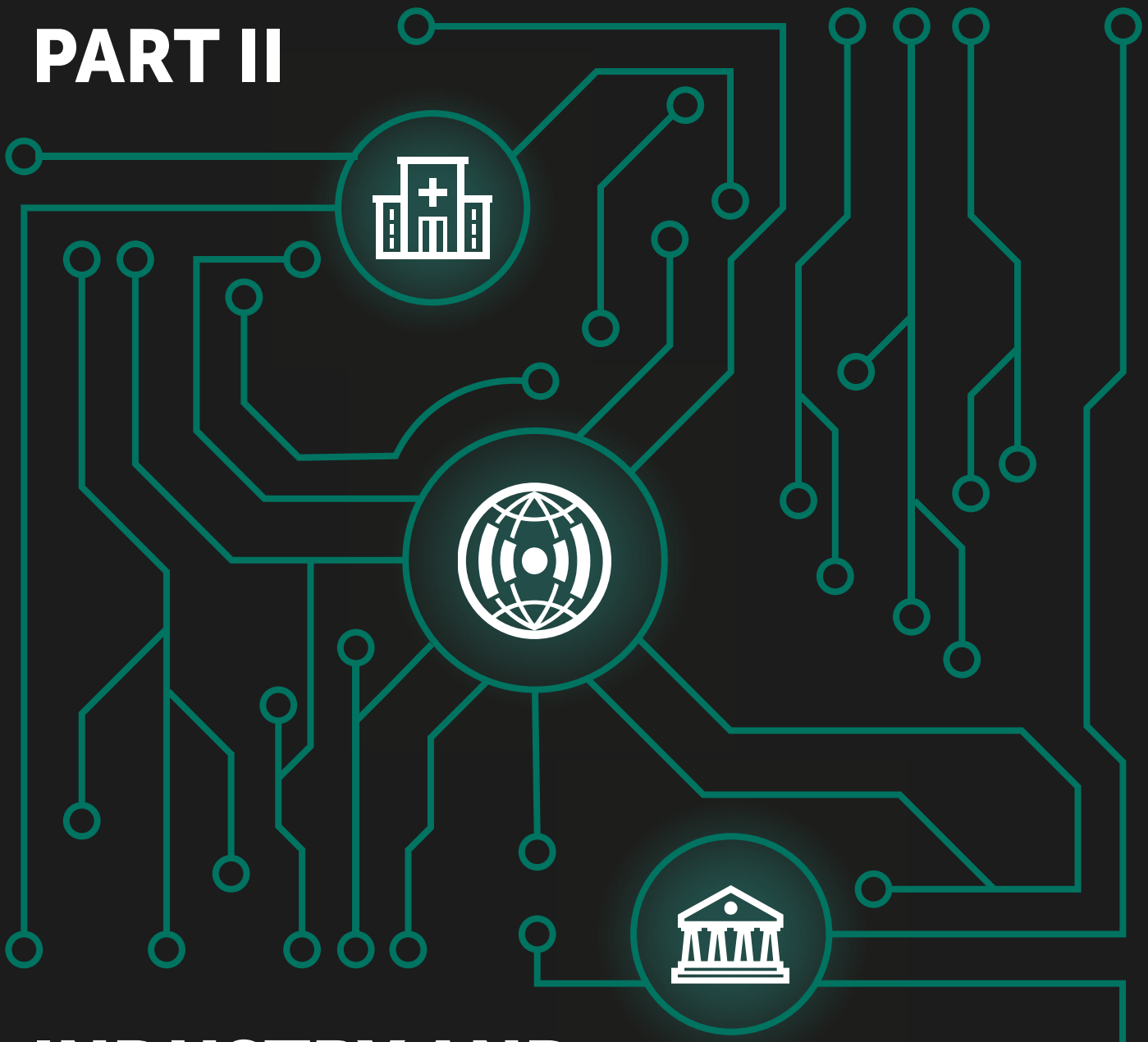
Beyond the leaks and political drama of the past year's newfound love for information warfare, social media itself has taken a politicized role beyond our wildest dreams. Whether it's at the hand of political pundits or confusing comedic jabs at Facebook's CEO by South Park's writers, eyes have turned against the different social media giants demanding some level of fact-checking and identification of fake users and bots attempting to exert disproportionate levels of social influence. Sadly, it's becoming obvious that these networks (which base their success on quantified metrics like 'daily active users') have little incentive to truly purge their user base of bots. Even when these bots are serving an obvious agenda or can be tracked and traced by independent researchers. We expect that as the obvious abuse continues and large bot networks become accessible to wider swaths of politically unsavory characters, that the greater backlash will be directed at the use of social media itself, with disgusted users eagerly looking for alternatives to the household giants that revel in the benefits of the abuse for profits and clicks.

CONCLUSION

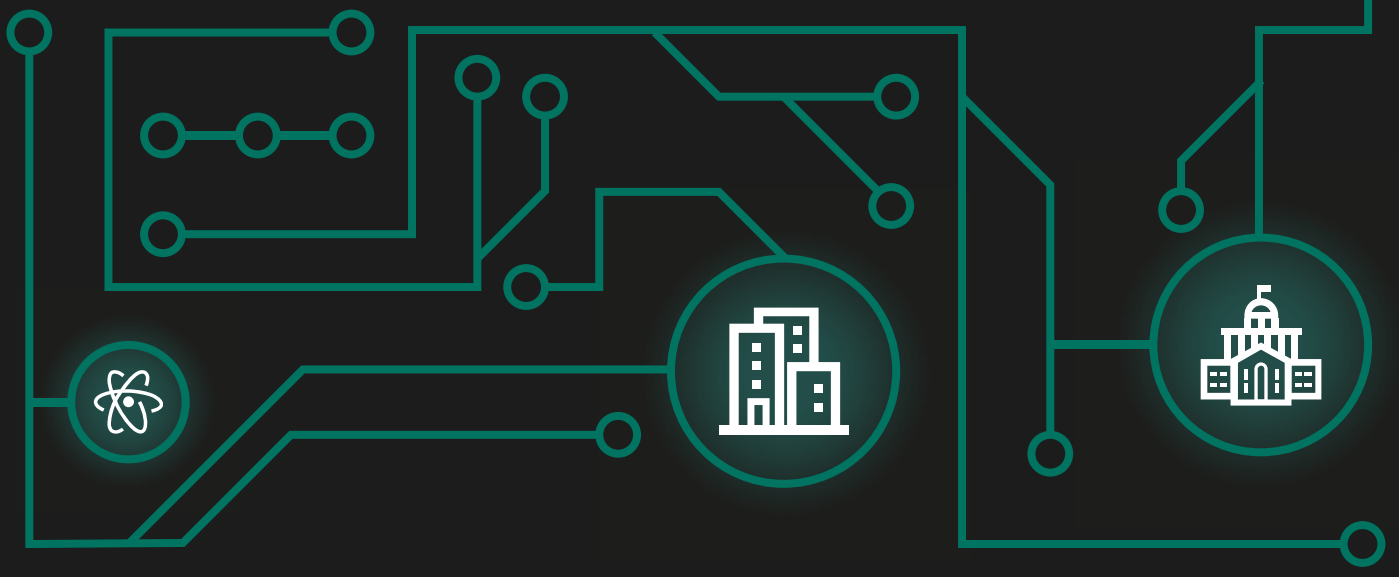
In 2017 we pronounced the death of Indicators of Compromise. In 2018, we expect to see advanced threat actors playing to their new strengths, honing their new tools and the terrifying angles described above. Each year's themes and trends shouldn't be taken in isolation – they build on each other to enrich an ever-growing landscape of threats facing users of all types, be it individuals, enterprise, or government. The only consistent reprieve from this onslaught is the sharing and knowledgeable application of high-fidelity threat intelligence.

While these predictions cover trends for advanced targeted threats, individual industry sectors will face their own distinct challenges. In 2018, we wanted to shine the spotlight on some of those as well.

PART II



INDUSTRY AND TECHNOLOGY PREDICTIONS



INTRODUCTION

We live in a connected world, where digital technologies have become an embedded part of everyday existence for individuals and organizations. This has introduced new vulnerabilities and threats. Some industry sectors are currently bigger targets for cyberattack than others. For our industry and technology predictions we have chosen a number of such areas; presenting some of the key risks that could lie ahead and their potential impact.

Threat Predictions for Automotive

THE LANDSCAPE IN 2017

Modern cars are no longer just electro-mechanical vehicles. With each generation, they become more connected and incorporate more intelligent technologies to make them smarter, more efficient, comfortable and safe. The connected-car market is growing at a five-year compound annual growth rate of 45% — 10 times faster than the car market overall.

The connected-car market is growing at a five-year compound annual growth rate of 45% — 10 times faster than the car market overall.

In some regions (e.g. the EU or Russia) two-way connected systems (eCall, ERA-GLONASS) are extensively implemented for safety and monitoring purposes; and all major auto manufacturers now offer services that allow users to interact remotely with their car via a web interface or a mobile app.

Remote fault diagnostics, telematics and connected infotainment significantly enhance driver safety and enjoyment, but they also present new challenges for the automotive sector as they turn vehicles into prime targets for cyberattack. The growing risk of a vehicle's systems being infiltrated or having its safety, privacy and financial elements violated, requires manufacturers to understand and apply IT security. Recent years have seen a number (here, here, and here) of examples highlighting the vulnerability of connected cars.

WHAT CAN WE EXPECT IN 2018?

Gartner estimates that there will be a quarter of a billion connected cars on the roads by 2020. Others suggest that by then around 98% of cars will be connected to the Internet. The threats we face now, and those we expect to face over the coming year should not be seen in isolation – they are part of this continuum – the more vehicles are connected, in more ways, the greater the surface and opportunities for attack.

The threats facing the automotive sector over the coming 12 months include the following:

Vulnerabilities introduced through lack of manufacturer attention or expertise, combined with competitive pressures. The range of connected mobility services being launched will continue to rise, as will the number of suppliers developing and delivering them. This ever-growing supply (and the likelihood of products/suppliers being of variable quality), coupled with a fiercely competitive marketplace could lead to security short cuts or gaps that provide an easy way in for attackers.

Vulnerabilities introduced through growing product and service complexity. Manufacturers serving the automotive sector are increasingly focused on delivering multiple interconnected services to customers. Every link is a potential point of weakness that attackers will be quick to seize on. An attacker only needs to find one insecure opening, whether that is peripheral such as a phone Bluetooth or a music download system, for example, and from there they may be able to take control of safety-critical electrical components like the brakes or engine, and wreak havoc.

No software code is 100% bug free – and where there are bugs there can be exploits. Vehicles already carry more than 100 million lines of code. This in in itself represents a massive attack surface for cybercriminals. And as more connected elements are installed into vehicles, the volume of code will soar, increasing the risk of bugs. Some automotive manufacturers, including Tesla have introduced specific bug bounty programs to address this.

Further, with software being written by different developers, installed by different suppliers, and often reporting back to different management platforms, no one player will have visibility of, let alone control over, all of a vehicle's source code. This could make it easier for attackers to bypass detection.

Apps mean happiness for cybercriminals. There are a growing number of smartphone apps, many introduced by car manufacturers, which owners can download to remotely unlock their cars, check the engine status or find its location. Researchers have already demonstrated proof of concepts of how such apps can be compromised. It will not be long before Trojanized apps appear that inject malware direct into the heart of an unsuspecting victim's vehicle.

With connected components increasingly introduced by companies more familiar with hardware than software, there is a growing risk that the need for constant updates could be overlooked. This could make it harder, if not impossible for known issues to be patched remotely. Vehicle recalls take time and cost money and in the meantime many drivers will be left exposed.

Connected vehicles will generate and process ever more data – about the vehicle, but also about journeys and even personal data on the occupants – this will be of growing appeal to attackers looking to sell the data on the black market or to use it for extortion and blackmail. Car manufacturers are already under pressure from marketing companies eager to get legitimate access to passenger and journey data for real time location-based advertising.

Fortunately, growing awareness and understanding of security threats will result in the first cyber secure devices for remote diagnostic and telematics data appearing on the market.

Further, lawmakers will come up with requirements and recommendations for making cybersecurity a mandatory part of all connected vehicles.

Last but not least, alongside existing safety certification there will be new organizations set up that are responsible for cybersecurity certification. They will use clearly defined standards to assess connected vehicles in terms of their resistance to cyberattacks.

Recommended action

Addressing these risks involves integrating security as standard, by design, focused on different parts of the connected car ecosystem. Defensive software solutions could be installed locally on individual electrical components — for instance, the brakes — to reinforce them against attacks. Next, software can protect the vehicle's internal network as a whole by examining all network communications, flagging any changes in standard in-vehicle network behaviour and stopping attacks from advancing in the network. Overarching this, a solution needs to protect all components that are connected externally, to the Internet. Cloud security services can detect and correct threats before they reach the vehicle. They also can send the vehicle over-the-air updates and intelligence in real time. All of this should be supported with rigorous and consistent industry standards.

Threat Predictions for Connected Health

THE LANDSCAPE IN 2017

We found open access to around 1,500 devices used to process patient images.

In 2017, Kaspersky Lab research revealed the extent to which medical information and patient data stored within the connected healthcare infrastructure is left unprotected and accessible online for any motivated cybercriminal to discover. For example, we found open access to around 1,500 devices used to process patient images. In addition, we found that a significant amount of connected medical software and web applications contains vulnerabilities for which published exploits exist.

This risk is heightened because cyber-villains increasingly understand the value of health information, its ready availability, and the willingness of medical facilities to pay to get it back.

WHAT CAN WE EXPECT IN 2018?

The threats to healthcare will increase as ever more connected devices and vulnerable web applications are deployed by healthcare facilities. Connected healthcare is driven by a number of factors, including a need for resource and cost efficiency; a growing requirement for remote, home-based care for chronic conditions like diabetes and ageing populations; consumer desire for a healthy lifestyle; and a recognition that data-sharing and patient monitoring between organizations can significantly enhance the quality and effectiveness of medical care.

The threats to healthcare will increase as ever more connected devices and vulnerable web applications are deployed by healthcare facilities.

The threats facing these trends over the coming 12 months include the following:

Attacks targeting medical equipment with the aim of extortion, malicious disruption or worse, will rise. The volume of specialist medical equipment connected to computer networks is increasing. Many such networks are private, but one external Internet connection can be enough for attackers to breach and spread their malware through the 'closed' network. Targeting equipment can disrupt care and prove fatal – so the likelihood of the medical facility paying up is very high.

There will also be a rise in the number of targeted attacks focused on stealing data. The amount of medical information and patient data held and processed by connected healthcare systems grows daily. Such data is immensely valuable on the black market and can also be used for blackmail and extortion. It's not just other criminals who could be interested: the victim's employer or insurance company might want to know as it could impact premiums or even job security.

There will be more incidents related to ransomware attacks against healthcare facilities. These will involve data encryption as well as device blocking: connected medical equipment is often expensive and sometimes life-critical, which makes them a prime target for attack and extortion.

The concept of a clearly-defined corporate perimeter will continue to 'erode' in medical institutions. More workstations, servers, mobile devices and equipment go online. This will give criminals more opportunities to gain access to medical information and networks. Keeping defenses and endpoints secure will be a growing challenge for healthcare security teams as every new device will open up a new entry point into the corporate infrastructure.

Sensitive and confidential data transmitted between connected 'wearables', including implants, and healthcare professionals will be a growing target for attack as the use of such devices in medical diagnosis, treatment and preventative care continues to increase. Pacemakers and insulin pumps are prime examples.

National and regional healthcare information systems that share unencrypted or otherwise insecure patient data between local practitioners, hospitals, clinics and other facilities will be a growing target for attackers looking to intercept data beyond the protection of corporate firewalls. The same applies to data shared between medical facilities and health insurance companies.

The growing use by consumers of connected health and fitness gadgets will offer attackers access to a vast volume of personal data that is generally minimally protected. The popularity of health-conscious, connected lifestyles means that fitness bracelets, trackers, smart watches, etc. will carry and transmit ever larger quantities of personal data with only basic security – and cybercriminals won't hesitate to exploit this.

Disruptive attacks – whether in the form of denial of service attacks or through 'ransomware' that simply destroys data (such as WannaCry) – are a growing threat to increasingly digital health care facilities. The ever increasing number of work stations, electronic records management and digital business processes that underpin any modern organization broadens the attack surface for cybercriminals. In healthcare, they take on an extra urgency, as any disruption can in real terms become a matter of life or death.

Last, but not least, emerging technologies such as connected artificial limbs, implants for smart physiological enhancements, embedded augmented reality etc. designed both to address disabilities and create better, stronger, fitter human beings – will offer innovative attackers new opportunities for malicious action and harm unless they have security integrated from the very first moment of design.

Threat Predictions for Financial Services and Fraud

THE LANDSCAPE IN 2017

Customer data is a key enabler for large-scale fraud attacks.

In 2017 we've seen fraud attacks in financial services become increasingly account-centric. Customer data is a key enabler for large-scale fraud attacks and the frequency of data breaches among other successful attack types has provided cybercriminals with valuable sources of personal information to use in account takeover or false identity attacks. These account-centric attacks can result in many other losses, including that of further customer data and trust, so mitigation is as important as ever for businesses and financial services customers alike.

WHAT CAN WE EXPECT IN 2018?

2018 will be a year of innovation in financial services as the pace of change in this space continues to accelerate. As more channels and new financial service offerings emerge, threats will diversify. Financial services will need to focus on omni-channel fraud prevention to successfully identify more fraud crossing from online accounts to newer channels. Newer successful payment types will see more attack attempts as their profitability for attack increases.

2018 will be a year of innovation in financial services as the pace of change in this space continues to accelerate.

Real-time payment challenges

Increasing demand from consumers for real-time and cross-border financial transactions results in pressure to analyse risk more quickly. Consumer expectations for friction-free payments make this task even more challenging. Financial services will need to rethink and make 'Know Your Customer' processes more effective. Machine learning and eventually AI-based solutions will also be key in meeting the need for quicker fraud and risk detection.

Social engineering attacks

Financial services will need to stay focused on tried and tested attack techniques. In spite of more sophisticated emergent threats, social engineering and phishing continue to be some of the simplest and most profitable attacks – exploiting the human element as the weakest link. Customer and employee education should continue to improve awareness of the latest attacks and scams.

Mobile threats

According to the latest Kaspersky Cybersecurity Index, ever more online activity now takes place on mobile. For example, 35 per cent of people now use their smartphone for online banking and 29 per cent for online payment systems (up from 22 per cent and 19 per cent respectively in the previous year). These mobile-first consumers will increasingly be prime targets for fraud. Cybercriminals will use previously-successful and new malware families to steal user banking credentials in creative ways. In 2017 we saw the modification of malware family Svpeng. In 2018, other families of mobile malware will re-surface to target banking credentials with new features. Identification and the removal of mobile malware is essential to financial services institutions to stop these attacks early.

For example, 35 per cent of people now use their smartphone for online banking and 29 per cent for online payment systems.

Data breaches

Data breaches will continue to make the headlines in 2018 and the secondary impact on financial institutions will be felt through fake account set ups and account take-over attacks. Data breaches, although harder to commit than individual fraud attacks against customers, are hugely profitable to criminals thanks to the high volume of customer data exposed in one hit. Financial services should regularly test their defences and use solutions to detect any suspicious access at the earliest stages.

Cryptocurrency targets

More financial institutions will explore the application of cryptocurrencies, making attacks on these currencies a key target for cybercriminals. We already saw the occurrence of mining malware increasing in 2017 and more attempts to exploit these currencies will be seen in 2018. Solutions capable of detecting the latest malware families should be used as well as combining the latest threat intelligence into prevention strategies. [See Threat Predictions for Cryptocurrencies for further information on this threat.]

Account takeover

More secure physical payments through chip technology and other Point of Sale improvements, have shifted fraud online in the past decade. Now, as online payment security improves through tokenisation, biometric technology and more, fraudsters are shifting to account takeover attacks. Industry estimates suggest fraud of this type will run into billions of dollars as fraudsters pursue this highly profitable attack vector. Financial services will need to rethink digital identities and use innovative solutions to be sure that customers are who they say they are, every time.

Pressure to innovate

More and more businesses will venture into payment solutions and open banking offerings in 2018. Innovation will be key to incumbent financial service firms seeking a competitive advantage over an increasing number of competitors. But understanding the regulatory complications can be challenging enough, never mind evaluating the potential for attack on new channels. These new offerings will be targets for fraudsters upon release and any new solution not designed with security at the core will find itself an easy target for cybercriminals.

Fraud-as-a-Service

International underground communication amongst cybercriminals means that knowledge is shared quickly and attacks can spread globally even faster. Fraud services are offered on the dark web, from bots and phishing translation services to remote access tools. Less experienced cybercriminals purchase and use these tools, meaning more attempted attacks for financial services to block. Sharing knowledge across departments as well as looking to threat intelligence services will be key in mitigation.

ATM attacks

ATMs will continue to attract the attention of many cybercriminals. In 2017, Kaspersky Lab researchers uncovered, among other things, attacks on ATM systems that involved new malware, remote and fileless operations, and an ATM-targeting malware called 'Cutlet Maker' that was being sold openly on the DarkNet market for a few thousand dollars with a step-by-step user guide. Kaspersky Lab has published a report on future ATM attack scenarios targeting ATM authentication systems.

Threat Predictions for Industrial Security

THE LANDSCAPE IN 2017

The most significant threat to industrial systems in 2017 was encryption ransomware.

2017 was one of the most intense in terms of incidents affecting the information security of industrial systems. Security researchers discovered hundreds of new vulnerabilities, researched new threat vectors targeting ICS and industrial processes, collected and analyzed statistics on accidental infections of industrial systems and detected targeted attacks on industrial enterprises (specifically, Shamoon 2.0/StoneDrill). And, for the first time since Stuxnet, discovered and analyzed a malicious toolset targeting physical systems: CrashOverride/Industroyer, which some experts have categorized as a 'cyberweapon'.

However, the most significant threat to industrial systems in 2017 was encryption ransomware. According to Kaspersky Lab ICS CERT, in the first half of the year, industrial information systems in 63 countries across the globe came under numerous attacks involving encryption ransomware, belonging to 33 different families. The WannaCry and ExPetr destructive ransomware attacks appear to have changed forever the attitude of industrial enterprises to the problem of protecting essential production systems.

WHAT CAN WE EXPECT IN 2018?

A rise in general and accidental malware infections

With few exceptions, cybercriminal groups have not yet discovered simple and reliable schemes for monetizing attacks on industrial information systems. Accidental infections and incidents in industrial networks caused by 'normal' (general) malicious code aimed at more traditional cybercriminal targets such as corporate networks, will continue in 2018. At the same time, we are likely to see such situations result in more severe consequences for industrial environments. The problem of regularly updating software in industrial systems in line with the corporate network will remain unresolved, despite repeated warnings from the security community.

Increased risk of targeted ransomware attacks

The WannaCry and ExPetr attacks taught both security experts and cybercriminals that operational technology (OT) systems can be even more vulnerable to such attacks than IT systems, and can also be accessed through the Internet. Moreover, the damage caused by malware in the OT network can exceed that in the corresponding corporate network, and 'firefighting' in the case of OT is much more difficult. Industrial companies have demonstrated how poorly organized and inefficient their staff can be when it comes to cyberattacks on their OT infrastructure. All of these factors make industrial systems a desirable target for ransomware attacks.

More incidents of industrial cyberespionage

The growing threat of organized ransomware attacks against industrial companies could trigger development of another, related area of cybercrime: the theft of industrial information systems data to be used for the preparation and implementation of targeted (including ransomware) attacks.

New underground market segments focused on attacks on industrial systems

In recent years, we have seen growing demand on the black market for zero day exploits targeting ICS. This tells us that criminals are working on targeted attack campaigns. We expect to see threat actors step up activity in this area in 2018, which is likely to result in the emergence of new segments focused on ICS configuration data and ICS credentials stolen from industrial companies and, possibly, offerings of botnets with 'industrial' nodes. Design and implementation of advanced cyberattacks targeting physical objects and systems requires an expert knowledge of ICS and relevant industries. Demand for such expertise is expected to drive growth in such areas as 'malware as a service', 'attack vector design as a service', 'attack campaign as a service' and other services related to attacks on industrial enterprises.

New types of malware and malicious tools

We will probably see new malware being used to target industrial networks and assets, with features including stealth and the ability to remain inactive in the IT network to avoid detection, only activating in the less secure OT infrastructure. Another possibility is the emergence of ransomware targeting field-level ICS devices and physical assets (pumps, switches, etc.).

Changes in national regulations

In 2018, new regulatory initiatives concerning industrial automation systems will come into effect in some countries. Among other consequences, this will force companies that own critical infrastructure objects and industrial assets to put more effort into their cybersecurity assessment. As a result of this, we will probably see new vulnerabilities identified in industrial systems. We may also learn of incidents at industrial enterprises and previously unknown attacks.

Criminals will take advantage of threat analyses published by security researchers

In 2017, researchers did a good job finding and making public various new vectors of attacks on industrial assets and infrastructure and performing deep analysis of the malicious toolsets found. All of this is good for the security of industrial facilities. However, criminals could also make use of this information. For example, hacktivists could take advantage of the CrashOverride/Industroyer toolset disclosure to run denial-of-service attacks on power systems; criminals may develop targeted ransomware and may even invent monetizing schemes for blackouts. The PLC worm concept could inspire criminals to create real-world malicious worms that spread from one PLC to another; while others could try to implement malware using one of the standard languages for programming PLCs. It is even possible that some threat actors will attempt to develop PLC malware operating at a low level based on an approach demonstrated by information security researchers. The latter two approaches could pose a serious problem for developers of existing security solutions.

Growing availability of, and investment in industrial cyber insurance

Cyber-risk insurance is becoming an integral part of risk management for industrial enterprises. Until recently, risks associated with cybersecurity incidents were excluded from insurance contracts – in effect, insurance companies equated them with terrorist attacks. But the situation is changing, with new initiatives introduced both by cybersecurity companies and by the main players in the insurance industry. In 2018, this will increase the number of industrial automation system audits/security assessments, as well as the number of recorded and investigated cybersecurity incidents.

Threat Predictions for Cryptocurrencies

THE LANDSCAPE IN 2017

In the first eight months of 2017, Kaspersky Lab products protected 1.65 million users from malicious cryptocurrency miners. By the end of the year we expect this number to exceed two million.

Today, cryptocurrency is no longer only for computer geeks and IT pros. It's starting to affect people's daily life more than they realize. At the same time, it is fast becoming an attractive target for cybercriminals. Some cyberthreats have been inherited from e-payments, such as changing the address of the destination wallet address during transactions and stealing an electronic wallet, among other things. However, cryptocurrencies have opened up new and unprecedented ways to monetize malicious activity.

In 2017, the main global threat to users was ransomware: and in order to recover files and data encrypted by attackers, victims were required to pay a ransom in cryptocurrency. In the first eight months of 2017, Kaspersky Lab products protected 1.65 million users from malicious cryptocurrency miners, and by the end of the year we expect this number to exceed two million. In addition, in 2017, we saw the return of Bitcoin stealers after a few years in the shadows.

WHAT CAN WE EXPECT IN 2018?

2018 is likely to be the year of malicious web-miners.

With the ongoing rise in the number, adoption and market value of cryptocurrencies, they will not only remain an appealing target for cybercriminals, but will lead to the use of more advanced techniques and tools in order to create more. Cybercriminals will quickly turn their attention to the most profitable money-making schemes. Therefore, 2018 is likely to be the year of malicious web-miners.

Ransomware attacks will force users to buy cryptocurrency

Cybercriminals will continue to demand ransoms in cryptocurrency, because of the unregulated and almost anonymous cryptocurrency market: there is no need to share any data with anyone, no one will block the address, no one will catch you, and there is little chance of being tracked. At the same time, further simplification of the monetization process will lead to the wider dissemination of encryptors.

Targeted attacks with miners

We expect the development of targeted attacks on companies for the purpose of installing miners. While ransomware provides a potentially large but one-off income, miners will result in lower but longer earnings. Next year we will see what tips the scales.

Rise of miners will continue and involve new actors

Next year mining will continue to spread across the globe, attracting more people. The involvement of new miners will depend on their ability to get access to a free and stable source of electricity. Thus, we will see the rise of 'insider miners': more employees of government organizations will start mining on publicly owned computers, and more employees of manufacturing companies will start using company-owned facilities.

Web-mining

Web-mining is a cryptocurrency mining technique used directly in browser with a special script installed on a web-page. Attackers have already proved it is easy to upload such a script to a compromised website and engage visitors' computers in mining and, as a result add more coins to the criminals' wallets. Next year web-mining will dramatically affect the nature of the Internet, leading to new ways of website monetization. One of these will replace advertising: websites will offer to permanently remove a mining script if the user subscribes to paid content. Alternatively, different kinds of entertainment, such as movies, will be offered for free in exchange for your mining. Another method is based on a website security check system – Captcha verification to distinguish humans from bots will be replaced with web mining modes, and it will be no longer matter whether a visitor is bot or human since they will 'pay' with mining.

Fall of ICO (Initial Coin Offering)

ICO means crowdfunding via cryptocurrencies. 2017 saw tremendous growth of this approach; with more than $3 billion collected by different projects, most related in some way to blockchain. Next year we should expect ICO-hysteria to decline, with a series of failures (inability to create the ICO-funded product), and more careful selection of investment projects. A number of unsuccessful ICO projects may negatively affect the exchange rate of cryptocurrencies (Bitcoin, Ethereum etc.), which in 2017 experienced unprecedented growth. Thus we will see a decrease in the absolute number of phishing and hacking attacks targeting ICO, smart contracts and wallets.

CONCLUSION

Connected technologies have the power to make life better and safer, but they bring with them new vulnerabilities that cyberattackers will be quick to exploit. As indicated at the start of this report, these predictions are grounded in the experience and insight gained over the last year by our expert researchers. They are opinions, and not all of them may be realized. But being prepared is half the battle, and the security industry, of which we are an active part, will continue to match the cybercriminals' latest tools and techniques with ever better threat intelligence and security solutions, to make the world a safer place for all except the bad guys.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis and thoughts

Kaspersky Lab blog

Threatpost, latest threat news

Eugene Kaspersky blog

Kaspersky Lab ICS CERT

KASPERSKY lab