TREND MICRO | research

MAPPING THE FUTURE

Dealing With Pervasive and Persistent Threats

TREND MICRO SECURITY PREDICTIONS FOR 2019

CONTENTS

Published by Trend Micro Research

TREND MICRO SECURITY PREDICTIONS FOR 2019

In 2019 and beyond, the biggest trends expected to have an impact on technology and security are the advances in artificial intelligence and machine learning brought about by the ever-growing volume of data that can be processed and analyzed; the continued adoption of cloud computing by enterprises the world over; and the developments in smart devices, homes, and factories — to say nothing of the looming 2020 rollout of 5G, the latest phase of mobile communications geared toward further increasing internet speeds. Furthermore, 2019 will be an important year for political developments including the finalization of Brexit and the holding of landmark elections in several countries. These technological and sociopolitical changes will have a direct impact on security issues in 2019.

Cybercriminals are expected, as usual, to home in on these movements, where the opportunity for profit is likely, fast, and relatively easy to navigate. In 2019, the implications of digital intrusions will be more far-reaching in terms of scope and consequence: Actual fraud using breached credentials will rise, more lives will be claimed as a result of sextortion, collateral damage will be observed as countries grow their cyber presence. Morever, the success of cyberpropaganda and fake news will have the power to decide the fate of nations. Consequently for enterprises, new challenges will include the lack of skilled manpower, which will cause budget pressure as they seek expert IT security staff; outsourcing will increase. Also, cyber insurance will experience unprecedented growth, since penalties for breaches and noncompliance are also expected to grow.

Our security predictions for the year ahead are based on our experts' analysis of the progress of current and emerging technologies, user behavior, and market trends, and their impact on the threat landscape. We have categorized them according to the main areas that are likely to be affected, given the sprawling nature of the technological and sociopolitical changes under consideration.

CONSUMERS

04

Social Engineering via Phishing Will Replace Exploit Kits as Attack Vector

Cases of phishing will markedly increase in 2019. Phishing attacks — where an attacker pretends to be a reputable person or entity so they can lure someone into disclosing sensitive information — have been around for a long time. But through the years threat actors have been finding ways to minimize user interaction in their conduct of cybercrime. Exploit kits, for example, gained popularity because they could automatically determine the relevant exploit to use on a target based on the victim's software versions.

However, in recent years, the state of quasi-monoculture — large communities of devices all running more or less the same software and operating systems (OSs) — has been breaking down. Five years ago, Windows was king,[1] but now no single OS holds more than half of the market.[2] Cybercriminals have to make a choice: spend hours on exploits or campaigns that work only on a small chunk of the computing population and that software vendors can curb with a patch, or go back to the classic technique for which there had never been a reliable, lasting solution — social engineering.

We will continue to see a decrease in exploit kit activity, something we have noted in our exploit kit activity data.

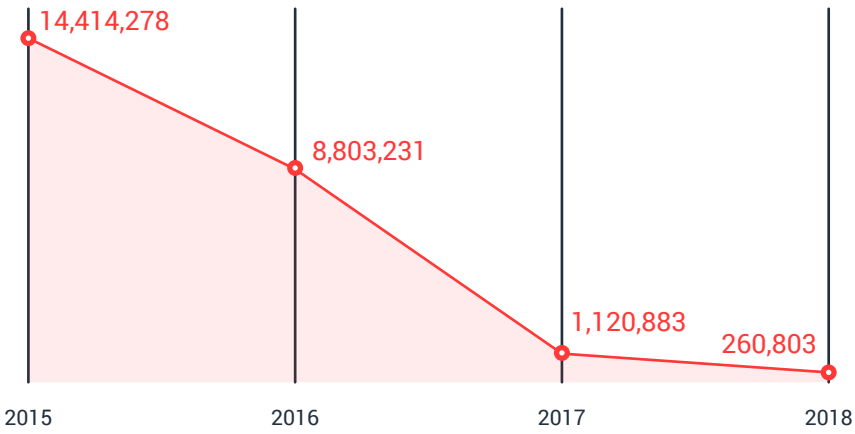


Figure 1. Exploit kit activity blocked decreased over the years, based on data from the Trend Micro™ Smart Protection Network™ infrastructure as of Q3 2018.

Phishing attacks are picking up, based on our data feeds, and this rising trajectory will continue in 2019.

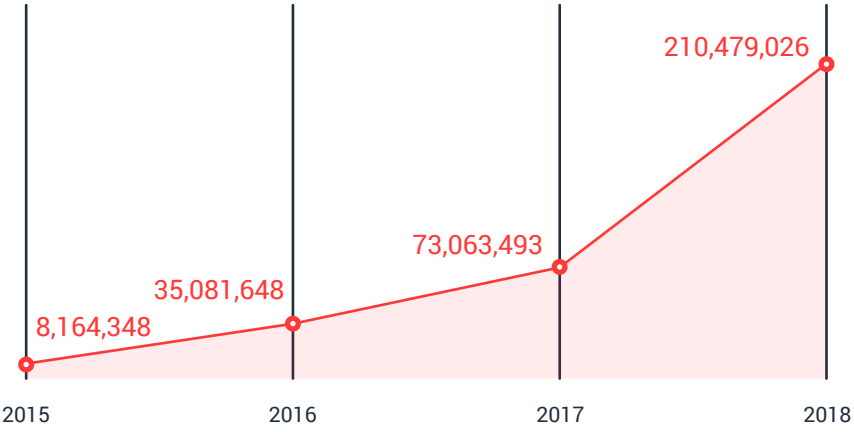


Figure 2. Phishing-related URLs blocked increased over the years, based on data from the Trend Micro Smart Protection Network infrastructure as of Q3 2018.

We will see phishing attempts not only in email but also in SMS and messaging accounts. Cybercriminals will target the usual online banking credentials, but they will also go after accounts used for cloud storage and other cloud services. We will also see completely new types of attacks like SIM-jacking, which relies quite heavily on social engineering. In SIM-jacking, criminals impersonate a target and convince a phone carrier's tech support staff to port a "lost" SIM card to one they already own, effectively taking control of a target's online presence, which is often associated with one's mobile phone number.[3]

In terms of socially engineered content, we foresee cybercriminals using real-world sporting or political events like the 2019 Rugby World Cup in Japan, the 2020 Summer Olympics in Tokyo, and the upcoming elections in different countries. Cybercriminals, for example, will create fake sites purporting to sell advance event tickets, deploy fake ads for free or discounted items, or send relevant election- or sport-related content that carry malicious links.

Chatbots Will Be Abused

Online communication has expanded beyond email messaging. As more tech-savvy and always-online youth use the internet, messaging apps have become a socially accepted channel between individuals or between an individual and a company rendering some form of online customer service or support. This new norm, combined with the preference for social engineering discussed earlier, will open new opportunities for cybercriminals.

We predict that attacks abusing chatbots will become rampant in 2019. In the same way that telephone attacks evolved to take advantage of prerecorded messages and interactive voice response (IVR) systems, attackers will design chatbots that can hold an initial conversation with a target to create a convincing pretext for eventually sending over a phishing link or obtaining personal information. Attackers will explore a wide range of possible payloads, including manipulation of orders, installation of a remote access trojan (RAT) in the target's computer, or even extortion.

E-Celeb Accounts Will Be Abused in Watering Hole Attacks

Still in line with the trend toward craftier social engineering tactics, **cybercriminals will compromise famous YouTubers and other "online-famous" personalities' social media accounts.** Cybercriminals will look for accounts that have several million followers and will work on taking over these accounts via targeted phishing attacks and the like. These attacks will shine a light on account security in mainstream media, but not before millions of users following these accounts have been affected by whatever payload the attackers have in store for them. The followers' computers may be infected by infostealers or made to join campaigns for distributed denial of service (DDoS) or cryptocurrency mining. They may even have their accounts turned into troll ones.

Actual Mass Real-World Use of Breached Credentials Will Be Seen

A recent report by Ponemon Institute and Akamai highlighted that credential stuffing — the automated injection of stolen username and password combinations from a single breach into several other popular websites — is becoming more and more severe.[4] Because of the volume of data breaches in the past years and the likelihood that cybercriminals will find a lot of users recycling passwords across several websites, we believe that **we will see a surge in fraudulent transactions using credentials obtained by cybercriminals from data breaches.**

Cybercriminals will use breached credentials to acquire real-world advantages such as registering in mileage and rewards programs to steal the benefits. They will also use these accounts to register trolls on social media for cyberpropaganda, manipulate consumer portals by posting fake reviews, or add fake votes to community-based polls — the applications are endless.

Sextortion Cases Will Rise

We will see an increase in reports of teenagers and young adults being extorted for non-monetary reasons like sextortion. Even if there is no guarantee that a blackmailer will come through, the highly personal nature of this kind of attacks will make the victim seriously consider fulfilling the attacker's demands, whether that means money or sexual favors. **As sextortion, in particular, becomes more widespread,[5, 6, 7] this kind of attacks will affect, perhaps even claim, more lives in 2019.**

ENTERPRISES

Home Networks in Work-From-Home Scenarios Will Open Enterprises to BYOD-like Security Risks

Enterprise IT will observe more and more attacks where the entry points are employees' internet-connected home devices. This is the unexpected but inevitable intersection of two trends: the rise of remote-working arrangements and the increasing adoption of smart devices in the home.

More employees are taking advantage of the option of accomplishing work at home (aka telecommuting, mobile work, or work-from-home). As reported by Gallup, 43 percent of American employees were working remotely in 2016, up from 39 percent in 2012.[8] And according to a global workforce survey conducted by Polycom, nearly two-thirds of employees took advantage of "anywhere working" in 2017, up from just 14 percent in 2012.[9] Like BYOD (bring your own device), work-from-home challenges the visibility of enterprise data movements whenever employees use their home internet to access cloud-based apps and collaboration software for chat, videoconferencing, and file sharing.

Already, home networks typically have printers and access storage devices that employees find convenient for work as well as for home use, resulting in a mixed-use (i.e., personal and business) scenario. In addition, sharing the remote worker's home network are more smart home devices than ever before; IDC projects double-digit growths in all smart home device categories through 2022.[10] Unfortunately, in terms of security, this means that every unsecured device on an employee's *home* network will be a potential entry point for attackers into the *enterprise* network.

Our researchers have already proved how smart speakers, for example, can leak personal data.[11] **We will see a few targeted attack scenarios in 2019 that will make use of smart speaker weaknesses to access enterprise networks through employees' home networks.**

GDPR Regulators Will Penalize the First High-Profile Violator the Full 4%

Regulators for the General Data Protection Regulation (GDPR) from the European Union (EU) have not immediately exercised their new powers. But very soon they will make an example out of a large, noncompliant company, fining it the full 4 percent of its global annual turnover.

The GDPR is a more mature model of privacy compliance. In fact, many organizations had already paid fines under the previous Data Protection Directive for over a decade,[12] so violators will feel the teeth of the regulation sooner than they expect. We will also see more data breach disclosures overall in 2019 than in the previous year due to the GDPR as there are already reports that some agencies are inundated with new disclosures needing investigation.[13] On the bright side, the disclosures will also give enterprises greater visibility and insight on how threat actors are compromising other organizations.

This will have the inevitable effect of emphasizing the prevalent difficulty in complying with the finer points of the regulation and will push regulators to clarify or add more details about what security technologies are actually needed. **Companies will also be forced to rethink the worth of data-mining activities inherent in current advertising models, given the high price tag of a possible violation. In fact, we predict that by 2020, up to 75 percent of new business applications will have to make the hard decision of choosing between compliance and security**. While privacy and security are not mutually exclusive, efforts to ensure data privacy compliance will have a detrimental effect on a company's ability to adequately determine the source and details of a security threat.

Real-World Events Will Be Used in Social Engineering Attacks

In the previous section, we predicted that phishing attacks will become more prevalent. In the context of the enterprise, **real-world events such as the upcoming elections in several countries in 2019, sporting events like the 2020 Summer Olympics in Tokyo, and even political instability and divisive issues like Brexit, will be used as premise for socially engineered attacks against companies**. We predict that there will be a lot of cybercriminal activity taking advantage of these events and issues. They will be used in regular cybercrime, email fraud, and social engineering against enterprises.

Cybercriminals will also focus more effort on obtaining information about employees using their social media presence in order to craft increasingly convincing phishing attacks.

Business Email Compromise Will Go 2 Levels Down the Org Chart

Business email compromise (BEC) remains a very potent and lucrative means of funneling money from companies. We believe that as a result of the focus on C-level officers as targets of fraud in news articles about BEC,[14] **cybercriminals will attack employees further down the company hierarchy**. For instance, cybercriminals will target the CxO's secretary or executive assistant, or a high-ranking director or manager in the finance department.

Automation Will Be a New Wrinkle in Business Process Compromise

Business process compromise (BPC) — in which specific business processes are silently altered to generate profit for attackers — will be an ongoing risk for enterprises. **Automation will add a new layer of challenge in securing business processes against BPC.** Forrester predicts that automation will result in the loss of 10 percent of jobs in 2019.[15]

As more aspects of monitoring and function are conducted through software or online applications, threat actors will have more opportunity to infiltrate these processes if they are not secured from the outset. Automation software will have vulnerabilities and integration with existing systems will introduce loopholes. Furthermore, since threat actors will try to find weaknesses in a target company's suppliers, partners, or vendors to accomplish their goals, automation will introduce risks in the supply chain as well.

Digital Extortion's Wide Field of Application Will Be Explored

Given the insights from our future-looking research on online blackmail or digital extortion,[16] we expect to see more polished executions or iterations of the same cybercriminal business model. In 2019, **we will see cybercriminals using the maximum fine for noncompliance with the GDPR as a guideline or ceiling for demanded ransom**. They will do so in the hopes that panicked and unwitting enterprises would rather pay the ransom than disclose the breach.

We will also see a few cases of a version of blackmail in the corporate scene in the form of online smear campaigns against brands. In these cases, attackers will demand ransom to cease spreading "fake news"-style propaganda against target brands.

GOVERNMENTS

The Fight Against Fake News Will Buckle Under the Pressure of Various Elections

In the EU, a "profound shake-up" is expected in the important European Parliament elections in 2019, according to Carnegie Europe,[17] even as European countries like Greece, Poland, and Ukraine hold their own national elections. Nigeria and South Africa will also be having their elections, along with several countries in Asia like India and Indonesia. **We believe that in 2019, the improvements social media has made to fight fake news post-2016 will not be enough to keep up with the deluge of cyberpropaganda surrounding these democratic exercises.**

As noted in our paper "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public," the triad necessary for fake news to proliferate can be disrupted only if any of the elements — platforms, motivation, tools — is either dismantled or inadequately managed.[18] Motivation will never go away, and the tools are difficult to corner since the same tools can be used for legitimate purposes. Governments have expressed interest in regulating social media platforms,[19] but we believe there will not be enough time for these sites to clear the internet "airwaves" of fake news. Adding to the technical difficulty of tamping down fake news is the existence of different languages in any large geographic areas like the EU, unlike in the U.S., where English is mostly used in social media posts.

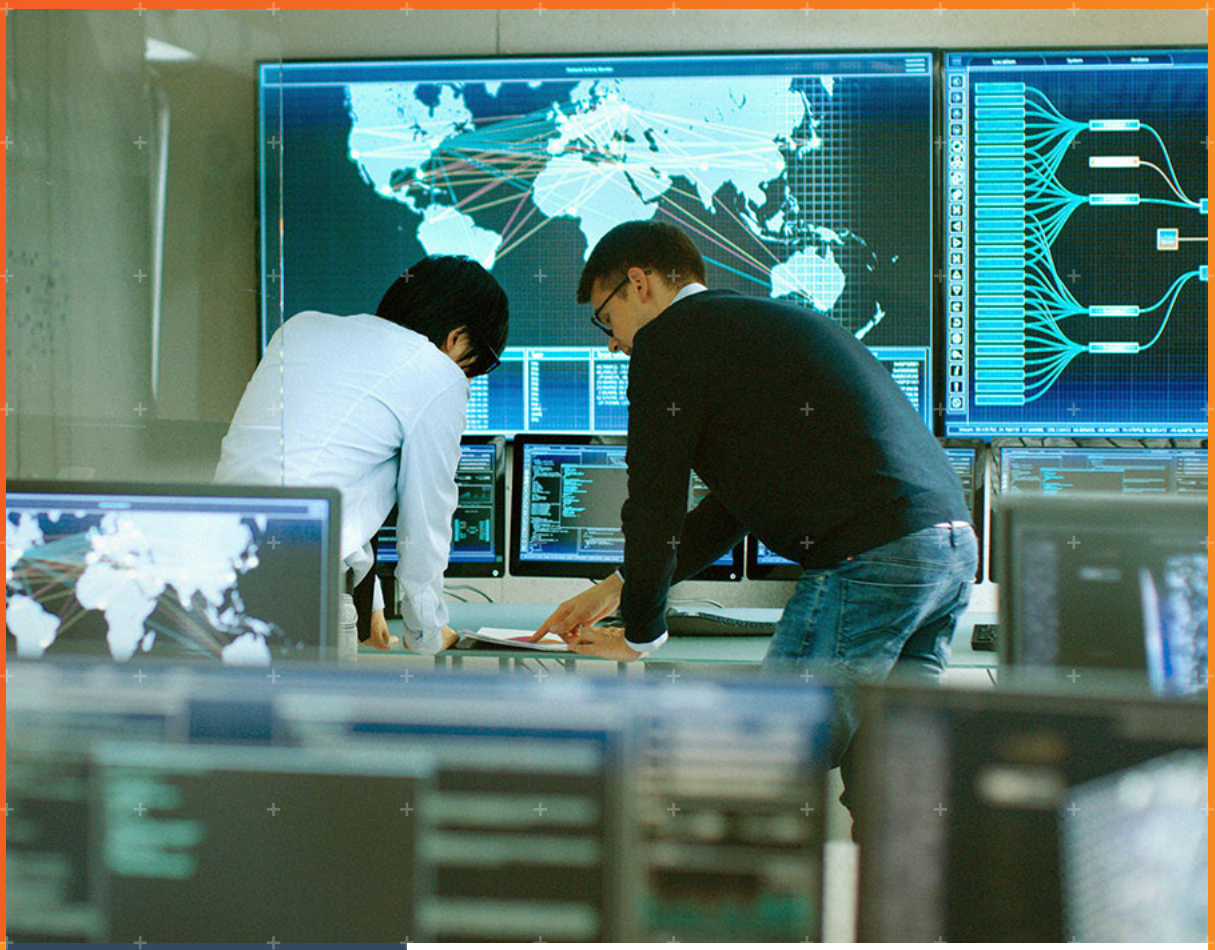
Unfortunately, the side of technology that allows fake news propagators to sway public sentiment has become even more powerful. Case in point is the so-called "Photoshop for audio" from Adobe,[20] which may very well be abused as a tool for deception. While Adobe has not released any further information about the software, it foreshadows where things are going in terms of the growing difficulty of distinguishing fact from fakery.

Innocent Victims Will Get Caught in the Crossfire as Countries Grow Their Cyber Presence

Targeted attacks will continue among traditional players, but in 2019, even countries not usually called out will be involved as well. Nations that are firming up their cyber capabilities for whatever reason will seek to support and empower domestic hackers either in preparation for or in response to perceived or prior attacks. **The bad news is these developments will have spillover effects on innocent victims completely unrelated to these cyber responses.** Individuals, companies, and even large organizations including those that have wide-ranging effects on the general public will be caught in the crossfire as countries grapple with how to conduct their operations. We already saw this happen with WannaCry[21] and NotPetya[22] — the collateral damage will only increase.

Regulatory Oversight Will Intensify

The existing conversations around security will push governments to increase regulatory supervision not only of privacy matters but also over both the consumer and industrial segments of the internet of things (IoT). In the U.S., California's bill requiring manufacturers to enforce the use of strong passwords on their smart devices[23] is merely one step in this direction. We expect to see national governments prohibiting the use of unsecure consumer and industrial IoT devices starting with legislation to be introduced in 2019.



SECURITY INDUSTRY

Cybercriminals Will Use More Techniques to Blend In

In response to security vendor technologies, specifically the renewed interest in machine learning for cybersecurity, **cybercriminals will use more malicious tactics to "blend in."** New ways of using normal computing objects for purposes other than their intended uses or designs — a practice known as "living off the land" — will continue to be discovered, documented, and shared. We have been observing some of these, including:

- The use of unconventional file extensions like .URL, .IQY, .ISO, .PUB, and .WIZ.
- Less reliance on actual executables, as in the use of "fileless" components, Powershell, scripts, and macros.
- Digitally signed malware as previously observed in our research "Exploring the Long Tail of (Malicious) Software Downloads,"[24] already a rampant technique that will continue to be abused because of its effectiveness.
- New activation methods, beyond previously observed techniques like using Mshta, Rundll32, Regasm, or Regsvr32.[25]
- The abuse of email accounts or online storage services and apps as command-and-control access points, or download or exfiltration sites.
- Minimally modifying or infecting legitimate system files.

Enterprises relying on machine learning technology as their *sole* security solution will be up for a challenge as more cybercriminals use these techniques, among others, to infect systems. We expect such cybercriminal tactics to become much more pronounced in 2019.

99.99% of Exploit-Based Attacks Will Still Not Be Based on 0-Day Vulnerabilities

Zero-day exploits — pieces of in-the-wild malware that use software vulnerabilities of which the affected vendors are unaware — have been a point of focus in IT security, making headlines whenever a new attack is discovered because they are relatively rare.

On the one hand, it is difficult for cybercriminals to find undiscovered software vulnerabilities because of the existing infrastructure of responsible disclosure that rewards vulnerability researchers for their findings, including Trend Micro's Zero Day Initiative (ZDI). And even if they do, all it takes is the discovery of the attack for vendors to be prompted to take proper action. On the other hand, the most accessible opportunity for cybercriminals is the window

of exposure that opens up between the release of a new patch and when it is implemented on enterprise systems. Patch administrators will need the proper strategy and amount of time to apply patches, and such efficiency issues will provide enough time for cybercriminals to mount an attack. Since the vulnerability details themselves have been published during disclosure, research time to use the weakness is significantly reduced.

In 2019, successful exploit-based attacks will involve vulnerabilities for which patches have been available for weeks or even months but have not been applied yet. We will continue to see cases of n-day exploits being a bane in network security.

Highly Targeted Attacks Will Begin Using AI-Powered Techniques

Targeted attacks by well-funded threat actors will start to use techniques powered by artificial intelligence (AI) for reconnaissance. Using AI will give them the ability to predict the movements of executives or other persons of interest. They can use AI to determine when and where corporate executives are expected to be in the future, e.g., the hotels their companies typically book them in, the restaurants they pick for meetings, and other preferences that can help narrow down their next likely locations.

For their part, security vendors will shore up defensive AI techniques of their own. Security teams will likewise draw on AI, in much the same way as with machine learning, to understand at a much more intimate level what an enterprise's baseline activities are in order to immediately be alerted when something out of the ordinary happens as far as security is concerned. Such futuristic scenarios afford a peek into the next frontier of AI technology and what it means for security.

INDUSTRIAL CONTROL SYSTEMS

Real-World Attacks Targeting ICSs Will Become a Rising Concern

Countries learning and exercising their cyber capabilities will conduct attacks against smaller players' critical infrastructure. They will do so to gain political or military advantage, or to test out capabilities against countries that do not yet have the capacity to retaliate, among other possible motivations. Whether the attacks will center on water, electricity, or manufacturing industrial control systems (ICSs) will depend on the threat actor's intent or opportunity. But the incidents will highlight weaknesses such as those meant to be curbed by the EU network and information security directive (NIS Directive) with its regulations for operators of essential services.[26]

The conduct of these attacks will be the same as any targeted attack that starts in reconnaissance until the threat actor's goals are met. A successful ICS attack will impact the target facility through operational shutdowns, damaged equipment, indirect financial losses, and at worst, health and safety risks.

HMI Bugs Will Continue to Be the Primary Source of ICS Vulnerabilities

Based on ZDI data, a large portion of vulnerabilities related to software used with supervisory control and data acquisition (SCADA) systems were in human-machine interfaces (HMIs),[27, 28] which serve as the main hub for managing the different diagnostic and controller modules in a facility. ICSs in general, which include distributed control systems (DCSs) and different field devices as well as SCADA systems, all use some form of HMI, and **in 2019, we will see even more HMI vulnerabilities being reported**.

For the time being, these kinds of software are more readily available to vulnerability researchers. It has also been known that HMI software is not as robustly secure as software from the likes of Microsoft and Adobe for various reasons, including the incorrect assumption that this kind of software will run only in isolated or on air-gapped environments.[29] Additionally, maintenance and upgrade of HMI software can be affected or hindered by the existing market movements around small vendors getting acquired by bigger ones or regional players merging with others.

CLOUD INFRASTRUCTURE

Misconfigured Security Settings During Cloud Migration Will Result in More Data Breaches

Data migration to the cloud is an enterprise-wide effort that should entail the same level of planning, commitment, and involvement as any physical relocation — perhaps even more. Each cloud migration is unique in terms of scope and pacing, and any industry best practice will still need to be fine-tuned to a company's specific circumstances and actual needs.

We predict that we will see more major data breach cases that will be a direct result of misconfigurations during migration to the cloud. Transitioning on-premise or private cloud data to a cloud service provider can open up the enterprise to security risks unless the enterprise has a good handle on what exactly is happening to its data. Cloud storage buckets may be private by default, but an existing bucket from outside will carry its existing permissions. Access policies must therefore be well understood, well implemented, and well maintained throughout the bucket's use.

Cloud Instances Will Be Used for Cryptocurrency Mining

Cloud mining is an existing alternative for legitimate cryptocurrency mining enthusiasts whereby, quite simply, a miner buys CPU power from a provider instead of investing in equipment. There are different payment schemes for this business model, but the main appeal of cloud mining is that it is easy to start and maintain, which makes sense for some miners for whom hardware or electricity may be a roadblock.

By a tiny stretch of the imagination, **more and more cybercriminals will try their hand at hijacking cloud accounts for mining cryptocurrency or maintaining control over alternative ones**. This means that the media-reported incidents of cryptojacking — the unauthorized use of computers to mine cryptocurrency — discovered in cloud environments in 2018[30] is a sign of a rising trend, not a one-off trial by cybercriminals. Cloud bucket scanner tools are already available; add to that the difficulty of getting the multiple security settings for each cloud deployment correctly, and cybercriminals will inevitably find their way toward this direction. We also expect more cryptojacking malware to minimize the risk of detection by throttling resource usage.

More Cloud-Related Software Vulnerabilities Will Be Discovered

In terms of attacker preference, cybercriminals will still go after easy pickings like account credentials to cloud assets in order to control databases. However, the research into cloud infrastructure weaknesses will not remain stagnant. **As cloud adoption grows, we will see cloud infrastructure vulnerability research begin to gain ground,** especially as the open-source community finds more uses for and digs deeper into software such as Docker, a containerization program, and Kubernetes, a container orchestration system.

Both Docker[31] and Kubernetes[32] are widely adopted for use in cloud-based deployments. There have already been a few Kubernetes vulnerabilities disclosed in recent years,[33] and a major one with a "critical" rating was discovered in December 2018.[34] Meanwhile, in one notable instance of researchers delving into cloud infrastructure vulnerabilities, more than a dozen malicious Docker images were found by Kromtech to have been downloaded at least five million times by unsuspecting developers over a span of a year before they were pulled out.[35]

SMART HOMES

Cybercriminals Will Compete for Dominance in an Emerging IoT 'Worm War'

As more smart devices connect to home networks, routers will continue to be an attractive attack vector for cybercriminals wanting to take control of any number of devices for whatever end. **The smart home environment will repeat a technically memorable era in information security history: the so-called "worm wars" in the worm outbreak era of the early 2000s**.[36]

Recent router-based attacks that affect smart devices, or IoT attacks, are mostly based either on the same leaked source code from the Mirai malware,[37] which first infected networked devices on Linux in August 2016,[38] or from other similarly behaving malware. These pieces of malware use a handful of known exploits and mostly bad logins and passwords to get into devices, which means that they are all auto-scanning the internet and discovering the exact same devices. Since there are a finite number of devices and only one piece of malware needs to be in control of a single device to execute payloads and perform malicious activities like DDoS attacks, cybercriminals will begin adding code to lock out any other hacker from using the device or kick out an existing malware infection, thereby becoming its exclusive owner. Security experts will find these behaviors familiar. The writers of Netsky started a worm war with the hackers behind other prominent worms of the time, Mydoom and Bagle.

The First Case of Senior Citizens Falling Easy Victims to Smart Health Device Attacks Will Emerge

Smart device vulnerabilities will continue to be found by researchers, enthusiasts, and attackers alike. But the actual attacks will remain sporadic in the coming years as long as a clear and easy path toward profit has not yet emerged for cybercriminals. Beyond 2019, it is easy to speculate how vulnerability researchers or even hackers will try to hack smart devices and systems, especially those associated with significant research and market adoption, e.g., self-driving cars.[39] For now, cybercriminals are solely trained on the money, and since there are many other avenues for profit, a global smart device attack is unlikely to occur in 2019.

In the narrower realm of health trackers, however, we believe that **the first few real-world victims of a smart health device attack will be seniors.** Companies are exploring the senior citizen customer base as potential users of smart trackers or other internet-connected health devices,[40] such as those that monitor heart rates or give out alerts to connected accounts when the elderly user slips or falls. In the past, senior citizens have been targets of phone scams because of their relative wealth, given their retirement savings.[41] We believe that we will see seniors becoming easy victims of attacks that abuse these devices as early as 2019. For one thing, elderly users of health trackers will not be computer-savvy enough to check the privacy settings of these devices, resulting in data leakage of confidential medical information, or to keep their accounts secure, allowing cybercriminals to access health-related and other personal data.

Beyond 2019, we will also see more "voice attacks"[42] affecting users of all ages as research into vulnerabilities in smart voice recognition matures and as smart assistants become a more ubiquitous feature of smart homes.

Getting Ready for the Year Ahead

More Unknowns Require Intelligent Multilayered Security for Enterprises

The realities of modern hybrid data center architectures and evolving endpoint/end-user access and mobility — including partners and other third parties that connect to the network — will demand a lot more from IT security teams in 2019. The IT security skill set shortage will thus become more pronounced,[43] and augmenting existing expertise with intelligent, efficient, and multilayered security technologies will become more critical.

Protecting enterprise networks from ever-changing threats requires an astute perception of how security risks should be managed. The full range of known and unknown threats can never be addressed by a single newfangled technology because each new breed of threat challenges different aspects of IT security. Enterprises should not look for a "silver bullet" but rather a cross-generational blend of threat defense techniques that applies the right technique at the right time:

- Malware prevention (anti-malware, behavioral analysis, machine learning, web reputation).
- Network security (intrusion prevention, firewall, vulnerability analysis).
- Email and collaboration security (anti-spam).
- System security (application control, integrity monitoring, log inspection).
- Specialized detection engines, custom sandboxing, and global threat intelligence (for unknown threats).
- Endpoint security.
- Integrated data loss prevention.

This solution should be optimized to the reality of where and how users actually connect to the network in terms of platforms and devices. Finally, IT security teams must be empowered by these technologies to view network activities, assess threats, and take proper action.

Developers Must Embrace DevOps Culture With Security as a Focus

DevOps combines software development (Dev) processes with IT operations (Ops) in order to shorten the systems development life cycle in a much more efficient and integrated manner. DevSecOps — DevOps with a focus on security — leads to strong security practices and baked-in security every step of the way. Software developers should adopt this mindset, along with its practical range of tools, in order to reap not only security benefits but also cost reductions.

Design weaknesses and other vulnerabilities, including those that leak personal information, are often discovered after the software has been installed in production computers or devices, and they could decrease significantly if security is integrated in development as early as in the planning phase.

Users Must Take up Responsible Digital Citizenship and Security Best Practices

Users' ability to distinguish truth from untruth, particularly on the internet, will become more important in 2019. Spreading awareness about the mechanics behind fake news will hopefully make the public more resistant to opinion manipulation. State and local governments will do well to include cybersecurity awareness training in schools and conduct the same for the public at large.

Social engineering essentially relies on the same human weaknesses, so users must apply the same level of critical thinking necessary in their social media consumption to their diligence in checking whether an email or a phone call is indeed coming from a trusted source.

Consumer devices like computers, tablets, and smartphones must be protected from threats like ransomware, dangerous websites, and identity thieves, primarily by ensuring that complete protection is available via anti-malware solutions. These technologies must also include data protection to safeguard valuable files, thwart new threats, and ensure that online monetary transactions are securely carried out.

Users should change their passwords regularly, have unique passwords for different accounts, take advantage of multifactor authentication features whenever possible, or use a password manager tool to help securely store credentials.

Smart home administrators should also secure their routers and devices by checking the products' default settings and understanding how to set them securely, regularly updating firmware, connecting only to secure networks, setting up firewalls to allow traffic only on specific ports, and setting up "guest networks" to minimize the unnecessary introduction of new devices to the network. Also, where possible, owners should review the devices' log histories. Of course, unique and strong passwords for routers and devices should also be enforced.

The threat landscape promises a lot of challenges for almost all sectors of the internet-using public in 2019 even as faster internet, for better or worse, looms on the horizon with the 5G rollout. But the available tools and technologies should empower users and enterprises into positioning themselves more securely in the fight against cybercriminals and other emerging threat actors. A deep understanding of these issues is a step in the right direction.

References

1. StatCounter. *Statcounter Global Stats.* "Operating System Market Share Worldwide, Jan-Dec 2013." Last accessed on 13 November 2018 at http://gs.statcounter.com/os-market-share/all/worldwide/2013.

2. StatCounter. *Statcounter Global Stats.* "Operating System Market Share Worldwide, Oct 2017 – Oct 2018." Last accessed on 13 November 2018 at http://gs.statcounter.com/os-market-share.

3. Lorenzo Franceschi-Bicchierai. (17 July 2018). *Motherboard.* "The SIM Hijackers." Last accessed on 13 November 2018 at https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin.

4. Ponemon Institute. (June 2018). *Akamai.* "The Cost of Credential Stuffing: Asia-Pacific." Last accessed on 13 November 2018 at https://www.akamai.com/us/en/multimedia/documents/white-paper/the-cost-of-credential-stuffing-asia-pacific.pdf.

5. Donna Freydkin. (9 February 2018). *Today.* "How online 'sextortion' drove one young man to suicide." Last accessed on 28 November 2018 at https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735.

6. Lizzie Dearden. (4 May 2018). *Independent.* "Five British men have killed themselves after falling victim to online 'sextortion', police reveal." Last accessed on 28 November 2018 at https://www.independent.co.uk/news/uk/crime/blackmail-online-sextortion-suicides-videos-photos-sexual-police-advice-a8337016.html.

7. David Goodwin. (8 November 2018). *Greenock Telegraph.* "Inverclyde youngsters fall victim to 'sextortion' gangs." Last accessed on 28 November 2018 at https://www.greenocktelegraph.co.uk/news/17204102.inverclyde-youngsters-fall-victim-to-sextortion-gangs/.

8. Gallup. (2017). *Gallup.* "State of the American Workplace." Last accessed on 27 November 2018 at https://news.gallup.com/file/reports/199961/SOAW_Report_GEN_1216_WEB_FINAL_rj.pdf.

9. Polycom. (2018). *Polycom.* "The Changing World of Work." Last accessed on 13 November 2018 at http://www.polycom.com/content/dam/polycom/common/documents/whitepapers/changing-needs-of-the-workplace-whitepaper-enus.pdf

10. IDC. (1 October 2018). *IDC.* "All Categories of Smart Home Devices Forecast to Deliver Double-Digit Growth Through 2022, Says IDC." Last accessed on 13 November 2018 at https://www.idc.com/getdoc.jsp?containerId=prUS44361618.

11. Stephen Hilt. (27 December 2018). *Trend Micro Security Intelligence Blog.* "The Need for Better Built-in Security in IoT Devices." Last accessed on 13 November 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/iot-devices-need-better-builtin-security/.

12. Greg Young and William J. Malik. (3 May 2018). *Trend Micro Simply Security.* "What HIPAA and Other Compliance Teaches Us About the Reality of GDPR." Last accessed on 13 November 2018 at https://blog.trendmicro.com/what-hipaa-and-other-compliance-teaches-us-about-the-reality-of-gdpr/.

13. Phil Muncaster. (14 September 2018.) *Infosecurity Magazine.* "ICO Swamped with GDPR Breach Over-Reporting." Last accessed on 28 November 2018 at https://www.infosecurity-magazine.com/news/ico-swamped-with-gdpr-breach/.

14. David Meyer. (4 December 2018). *Fortune.* "How Email Scammers Are Using Marketeer Methods to Target CFOs." Last accessed on 5 December 2018 at http://fortune.com/2018/12/04/targeted-email-fraud/.

15. Forrester Research. (14 November 2018). *ZDNet.* "Automation will become central to business strategy and operations." Last accessed on 14 November 2018 at https://www.zdnet.com/article/automation-will-become-central-to-business-strategy-and-operations/.

16. David Sancho. (30 January 2018). *Trend Micro Security Intelligence Blog.* "Digital Extortion: A Forward-looking View." Last accessed on 13 November 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/digital-extortion-forward-looking-view/.

17. Alberto Alemanno. (27 June 2018). *Carnegie Europe.* "Europe Up for Grabs: The Looming Battle Lines of the 2019 European Parliament Elections." Last accessed on 13 November 2018 at https://carnegieeurope.eu/2018/06/27/europe-up-for-grabs-looming-battle-lines-of-2019-european-parliament-elections-pub-76691.

18. Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (13 June 2017). *Trend Micro Security News.* "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.

19. Charles Hymas. (20 September 2018). *The Telegraph.* "Government draws up plans for social media regulator following Telegraph campaign." Last accessed on 13 November 2018 at https://www.telegraph.co.uk/news/2018/09/20/government-draws-plans-social-media-regulator-following-telegraph/.

20. Sebastian Anthony. (7 November 2018). *Ars Technica.* "Adobe demos "photoshop for audio," lets you edit speech as easily as text." Last accessed on 13 November 2018 at https://arstechnica.com/information-technology/2016/11/adobe-voco-photoshop-for-audio-speech-editing/.

21. Lily Hay Newman. (12 May 2017). *Wired.* "The Ransomware Meltdown Experts Warned About Is Here." Last accessed on 28 November 2018 at https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

22. Andy Greenberg. (22 August 2018). *Wired.* "The Untold Story of Notpetya, The Most Devastating Cyberattack in History." Last accessed on 28 November 2018 at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

23. Adi Robertson. (28 September 2018). *The Verge.* "California just became the first state with an Internet of Things cybersecurity law." Last accessed on 13 November 2018 at https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

24. Trend Micro Forward-Looking Threat Research Team. (5 April 2018). *Trend Micro Security Intelligence Blog.* "Understanding Code Signing Abuse in Malware Campaigns." Last accessed on 13 November 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/understanding-code-signing-abuse-in-malware-campaigns/.

25. MITRE ATT&CK. *MITRE.* "Tactic: Execution." Last accessed on 13 November 2018 at https://attack.mitre.org/tactics/TA0002/.

26. European Union Agency for Network and Information Security. *ENISA.* "NIS Directive." Last accessed on 5 December 2018 at https://www.enisa.europa.eu/topics/nis-directive.

27. Trend Micro. (23 May 2017). *Trend Micro Security News.* "The State of SCADA HMI Vulnerabilities." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

28. Brian Gorenc. (9 July 2018). *Zero Day Initiative.* "Checking In: A Look Back at the First Half of 2018." Last accessed on 28 November 2018 at https://www.zerodayinitiative.com/blog/2018/7/9/checking-in-a-look-back-at-the-first-half-of-2018.

29. Trend Micro. (23 May 2017). *Trend Micro Security News.* "The State of SCADA HMI Vulnerabilities." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

30. Charlie Osborne. (15 May 2018). *ZDNet.* "Cryptojacking attacks surge against enterprise cloud environments." Last accessed on 28 November 2018 at https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/.

31. Steven J. Vaughan-Nichols. (21 March 2018). *ZDNet.* "What is Docker and why is it so darn popular?" Last accessed on 28 November 2018 at https://www.zdnet.com/article/what-is-docker-and-why-is-it-so-darn-popular/.

32. Udi Nachmany. (1 November 2018). *Forbes.com.* "Kubernetes: Evolution of an IT Revolution." Last accessed on 28 November 2018 at https://www.forbes.com/sites/udinachmany/2018/11/01/kubernetes-evolution-of-an-it-revolution/#366fcb4554e1.

33. CVE Details. *CVE Details.* "Kubernetes: List of security vulnerabilities." Last accessed on 28 November 2018 at https://www.cvedetails.com/vulnerability-list/vendor_id-15867/product_id-34016/Kubernetes-Kubernetes.html.

34. Steven J. Vaughan-Nichols. (3 December 2018). *ZDNet.* "Kubernetes' first major security hole discovered." Last accessed on 3 December 2018 at https://www.zdnet.com/article/kubernetes-first-major-security-hole-discovered/.

35. Security Center. (12 June 2018). *KromTech Security Center.* "Cryptojacking invades cloud. How modern containerization trend is exploited by attackers." Last accessed on 28 November 2018 at https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers.

36. Trend Micro. *Trend Micro Security Intelligence Blog.* "Threat Morphosis: The Shifting Motivations Behind Digital Threats." Last accessed on 13 November 2018 at http://blog.trendmicro.com/threat-morphosis/.

37. Brian Krebs. (1 October 2016). *Krebs on Security.* "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 28 November 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

38. Trend Micro. (13 September 2016). *Trend Micro Security News.* "Linux Security: A Closer Look at the Latest Linux Threats." Last accessed on 28 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-security-a-closer-look-at-the-latest-linux-threats.

39. Spencer Hsieh. (5 October 2018). *Virus Bulletin.* "Security issues of IoV devices." Last accessed on 28 November 2018 at https://www.virusbulletin.com/conference/vb2018/abstracts/security-issues-iov-devices/.

40. Christina Farr and Jillian D'Onfro. (23 July 2018). *CNBC.* "Google is mulling a new market for Nest smart home products: seniors." Last accessed on 13 November 2018 at https://www.cnbc.com/2018/07/20/google-nest-senior-living-aging.html.

41. McCall Robison. (15 November 2018). *MarketWatch.* "These common scams target seniors—how to avoid them." Last accessed on 28 November 2018 at https://www.marketwatch.com/story/these-common-scams-target-the-elderlyhow-to-avoid-them-2018-11-15.

42. Trend Micro. (11 April 2018). *Trend Micro Security News.* "Threats to Voice-Based IoT and IIoT Devices." Last accessed on 28 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-to-voice-based-iot-and-iiot-devices.

43. Jon Oltsik. (11 January 2018). *CSO Online.* "Research suggests cybersecurity skills shortage is getting worse." Last accessed on 13 November 2018 at https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html.

For Raimund Genes (1963-2017)

TREND MICRO™ | research

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com