



PARADIGM  
SHIFTS

Trend Micro Security Predictions for 2018



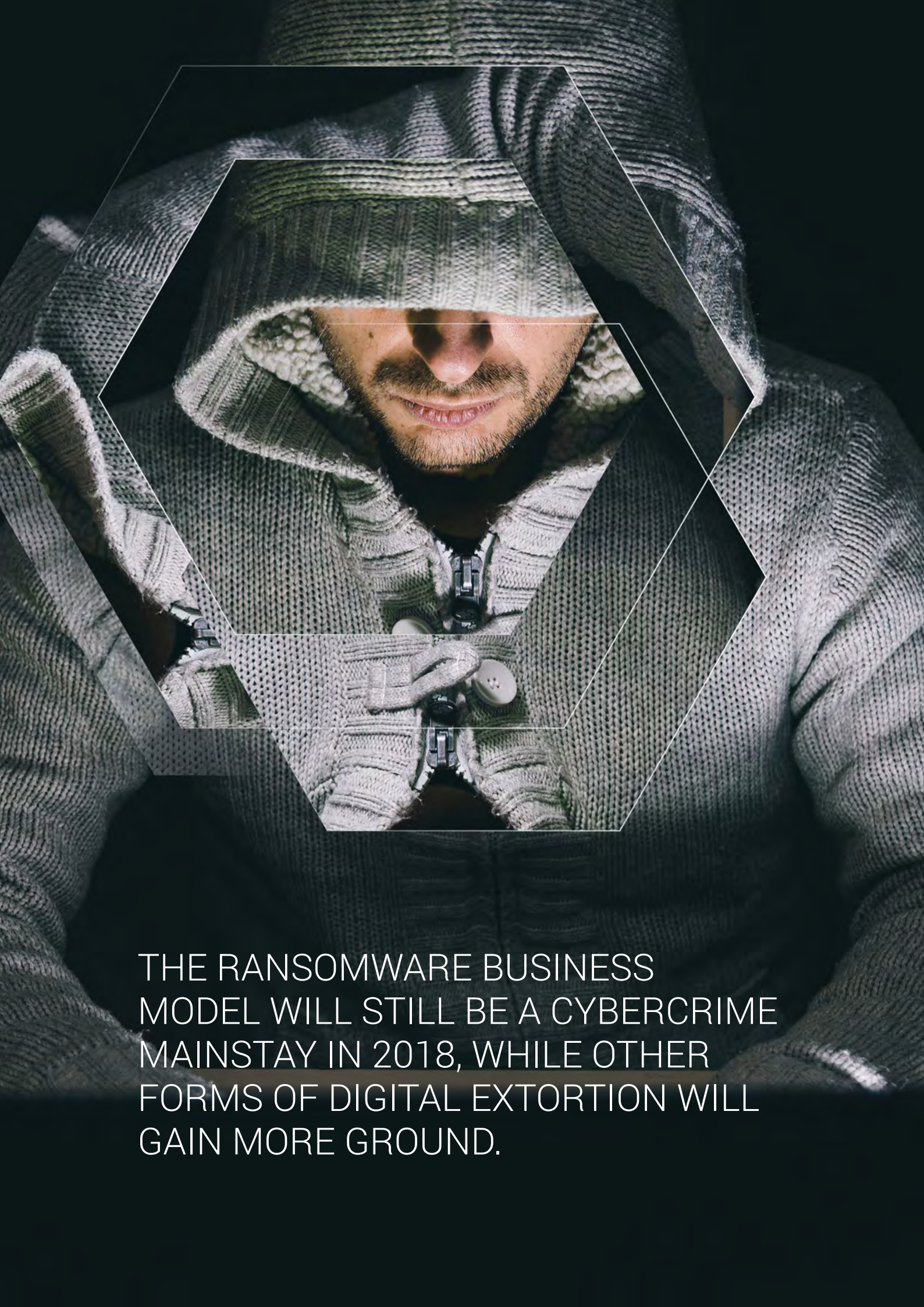
Skills and resources — these are the two elements that make up an attacker's arsenal. An attacker, however, cannot set out to break security or even perform sophisticated attacks without finding weak points in a system first. Massive malware attacks, email-borne heists, hacked devices, and disrupted services — all of these require a vulnerability in the network, whether in the form of technology or people, in order to be pulled off.

Increased connectivity and interaction over insecure networks are a given. Unfortunately, poor implementation of technologies adds to the likelihood of threats being realized. Having protection where and when it's needed will become the backbone of security in this ever-shifting threat landscape.

In 2018, digital extortion will be at the core of most cybercriminals' business model and will propel them into other schemes that will get their hands on potentially hefty payouts. Vulnerabilities in IoT devices will expand the attack surface as devices get further woven into the fabric of smart environments everywhere. Business Email Compromise scams will ensnare more organizations to fork over their money. The age of fake news and cyberpropaganda will persist with old-style cybercriminal techniques. Machine learning and blockchain applications will pose both promises and pitfalls. Companies will face the challenge of keeping up with the directives of the General Data Protection Regulation (GDPR) in time for its enforcement. Not only will enterprises be riddled with vulnerabilities, but loopholes in internal processes will also be abused for production sabotage.

These are the threats that will make inroads in the 2018 landscape. As such, they will serve as further proof that the days of threats being addressed with traditional security solutions are behind us. As environments become increasingly interconnected and complex, threats are redefining how we should look at security.

Trend Micro has looked into the current and emerging threats, as well as the security approaches tailored for the landscape. Read on to find out how to make informed decisions with regard to the security focus areas that will figure prominently in 2018.



THE RANSOMWARE BUSINESS MODEL WILL STILL BE A CYBERCRIME MAINSTAY IN 2018, WHILE OTHER FORMS OF DIGITAL EXTORTION WILL GAIN MORE GROUND.



For 2017, we predicted that cybercriminals would diversify ransomware into other attack methods. True enough, the year unfolded with incidents such as [WannaCry and Petya's](#) rapidly propagated network attacks, [Locky and FakeGlobe's](#) widespread spam run, and [Bad Rabbit's](#) watering hole attacks against Eastern European countries.

We do not expect ransomware to go away anytime soon. On the contrary, it can only be anticipated to make further rounds in 2018, even as other types of digital extortion become more prevalent. Cybercriminals have been resorting to using compelling data as a weapon for coercing victims into paying up. With [ransomware-as-a-service](#) (RaaS) still being offered in underground forums, along with bitcoin as a secure method to collect ransom, cybercriminals are being all the more drawn to the business model.

## Ransomware maturity as a catalyst for digital extortion campaigns

If the evolution of cybercriminal tactics over the years is any indication, cybercriminals are now going straight for the money instead of tricking users into giving up their credentials. The early online threats were heavy on [infostealers](#) and malware that hijacked banking transactions to steal private information. Then, the breed of threats went out to disguise themselves as anti-malware solutions ([FAKEAV](#)), whereby users were duped into downloading the software and paying up to regain access to the victimized computers. Emulating this behavior of [FAKEAV](#), ransomware took the stage from then on.

The current success of ransomware campaigns – especially their extortion element – will prompt cybercriminals looking to make generous profits out of targeting populations that will yield the most return possible. Attackers will continue to rely on phishing campaigns where emails with ransomware payload are delivered en masse to ensure a percentage of affected users. They will also go for the bigger buck by targeting a single organization, possibly in an Industrial Internet of Things (IIoT) environment, for a ransomware attack that will [disrupt the operations](#) and affect the production line. We already saw this in the fallout from the massive [WannaCry](#) and [Petya](#) outbreaks, and it won't be long until it becomes the intended impact of the threat.

Extortion will also come into play when GDPR gets imposed. Cybercriminals could target private data covered by the regulation and ask companies to pay an extortion fee rather than risk punitive fines of up to 4 percent of their annual turnover. Companies will have ransom prices associated with them that cybercriminals can determine by taking publicly available financial details and working out the respective maximum GDPR fines the companies could face. This will drive an increase in breach attempts and ransom demands. Moreover, we expect GDPR to be used as a social engineering tactic in the same way that [copyright violations](#) and [police warnings](#) were used in past [FAKEAV](#) and ransomware campaigns.

Users and enterprises can stay resilient against these digital extortion attempts by employing effective web and email gateway solutions as a first line of defense. Solutions with high-fidelity machine learning, behavior monitoring, and vulnerability shielding prevent threats from getting through to the target. These capabilities are especially beneficial in the case of ransomware variants that are seen moving toward [fileless delivery](#), in which there are no malicious payloads or binaries for traditional solutions to detect.

### Prominent Cybercriminal Business Models Over the Years

2018	Ransomware and DIGITAL EXTORTION will be the land of milk and honey for cybercriminals.
2017	Unprecedented ransomware outbreaks occur through WANNACRY and PETYA.
2016	New ransomware families spike by 752%, RANSOMWARE-AS-A-SERVICE (RaaS) emerges.
2015	Ransomware steadily grows, and continues to encrypt and demand payment.
2014	Ransomware BITCRYPT encrypts files and demands bitcoin payment.
2013	Ransomware CRYPTOLOCKER encrypts files, locks systems, and demands \$300 payment.
2011	Trojan SPYEE steals millions of dollars.
2010	First Android Trojan, DROIDSMS, emerges.
2009	Trojans spread via malicious links on Twitter.
2008	Worm KOOFACE targets Facebook users. FAKEAV steals credit card information using fake antivirus scare messages.
2007	Infostealer ZEUS is discovered.
2004	Online banking malware that logs keystrokes or changes banking interfaces flourishes.

SOURCES:

<http://blog.trendmicro.com/trendlabs-security-intelligence/threat-morphosis/>  
<https://www.trendmicro.com/vinfo/us/security/definition/ransomware>  
<https://documents.trendmicro.com/assets/rpt/rpt-setting-the-stage.pdf>



CYBERCRIMINALS WILL EXPLORE  
NEW WAYS TO ABUSE IoT DEVICES  
FOR THEIR OWN GAIN.

The massive [Mirai](#) and [Persirai](#) distributed denial-of-service (DDoS) attacks that hijacked IoT devices, such as digital video recorders (DVRs), IP cameras, and routers, have already elevated the conversation of how vulnerable and disruptive these connected devices can be. Recently, the IoT botnet [Reaper](#), which is based on the Mirai code, has been found to catch on as a means to compromise a web of devices, even those from different device makers.

We predict that aside from performing DDoS attacks, cybercriminals will turn to IoT devices for creating proxies to obfuscate their location and web traffic, considering that law enforcement usually refers to IP addresses and logs for criminal investigation and post-infection forensics. Amassing a large network of anonymized devices ([running on default credentials](#) no less and having virtually no logs) could serve as jumping-off points for cybercriminals to surreptitiously facilitate their activities within the compromised network.

We should also anticipate more IoT vulnerabilities in the market as many, if not most, manufacturers are going to market with devices that are not secure by design. This risk will be compounded by the fact that patching IoT devices may [not be as simple as patching PCs](#). It can take one insecure device that has not been issued a fix or updated to the latest version to become an entry point to the central network. The KRACK attack proved that even the [wireless connection](#) itself could add to the security woes. This vulnerability affects most, if not all, devices that connect to the WPA2 protocol, which then raises questions about the security of 5G technology, which is slated to sweep connected environments.

## Devices that will be targeted for disruptions and cybercrime

With [hundreds of thousands](#) of drones entering the U.S. airspace alone, the prospect of overseeing the aerial vehicles can be daunting. We expect that reports of drone-related [accidents](#) or [collisions](#) are only the start of it, as hackers have already been found to [access](#) computers, [grab](#) sensitive information, and [hijack](#) deliveries. Likewise, pervasive home devices such as wireless speakers and voice assistants can enable hackers to determine house locations and attempt break-ins.

We also expect cases of biohacking, via [wearables and medical devices](#), to materialize in 2018. Biometric activity trackers such as heart rate monitors and fitness bands can be intercepted to gather information about the users. Even life-sustaining [pacemakers](#) have been found with vulnerabilities that can be exploited for potentially fatal attacks.

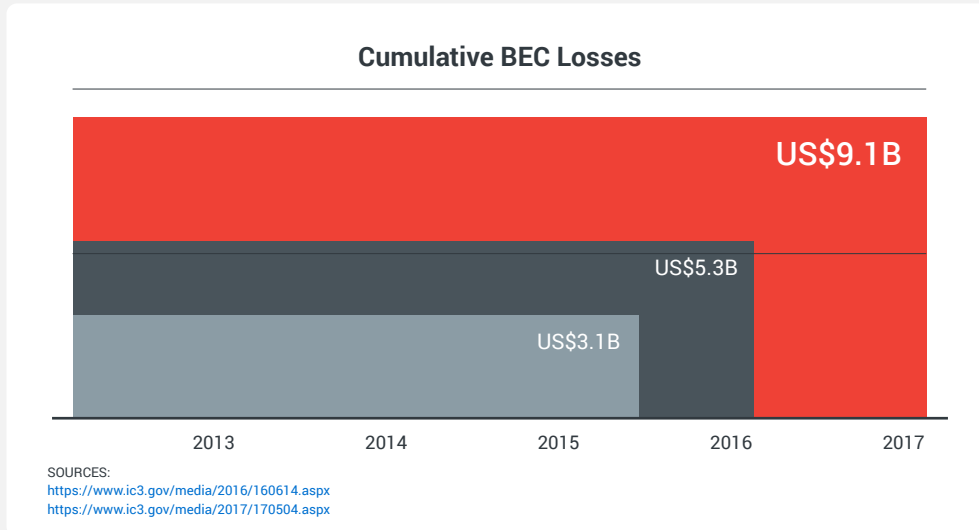
What adopters and regulators should recognize now is that not all IoT devices have built-in security, let alone hardened security. The devices are open to compromise unless manufacturers perform regular risk assessments and security audits. Users are also responsible for setting up their devices for security, which can be as simple as changing default passwords and regularly installing firmware updates.





GLOBAL LOSSES FROM BUSINESS  
EMAIL COMPROMISE SCAMS WILL  
EXCEED US\$9 BILLION IN 2018.

According to the Federal Bureau of Investigation (FBI), BEC scams have been reported in over a hundred countries and had a marked increase of 2,370 percent in identified exposed losses between January 2015 and December 2016. This isn't surprising since BEC scams are to cybercriminals what burglary is to "offline" criminals. BEC scams are quick, require very little scouting, and can yield big gains depending on the target, as evidenced by the **US\$5 billion** recorded losses.




We predict that BEC incidents will only multiply in 2018, leading to more than US\$9 billion\* in global losses. This hike in the projected reported losses will be brought on partly by a growing awareness around BEC and the tactics used, which will result in better identification and increased reporting of the scams. Mainly, it will be rooted in how BEC scams bank on phishing approaches that time and again have proved to be effective. We will continue to see BEC scams that involve company executives being impersonated to wire sums of money. We've been observing it in the increase of BEC attack attempts involving CEO fraud. It's also interesting to note that instead of planting keyloggers, BEC scammers are turning to phishing PDFs and sites, which are cheaper than keyloggers with crypting services. With phishing, they can still compromise accounts, and at lower costs at that.

The simplicity of knowing a target organization's hierarchy (which may even be publicly available on social media and corporate websites) and the brevity of the emails make a case for BEC as an efficient ploy to funnel money. There is, however, another financially driven enterprise threat that is expected to still be wielded by cybercriminals, especially those who are willing to do the long con: **Business Process Compromise (BPC)**. With BPC, cybercriminals learn the inner workings of the organization, particularly in the **financial** department, with the aim of modifying internal processes (possibly via corporate supply chain vulnerabilities) and hitting the mother lode. But given that it requires long-term planning and more work, BPC is less likely to make headlines in 2018, unlike the much simpler BEC.

BEC can be deflected if employee training is in place, as it is reliant on social engineering. Companies should implement strict protocols on internal processes, especially when making any kind of transaction. Small- and medium-sized businesses, as well as enterprises, should employ multiple verifications, whereby another established communication channel, such as a phone call, is at one's disposal for double-checking. Web and gateway solutions that provide accurate detection of social engineering tactics and forged behaviors may also be able to block BEC threats.

\* US\$9 billion is based on computing the monthly average of reported losses from June to December 2016 and multiplying it by 12. This only assumes that there is a flat growth for reported BEC incidents and victims.

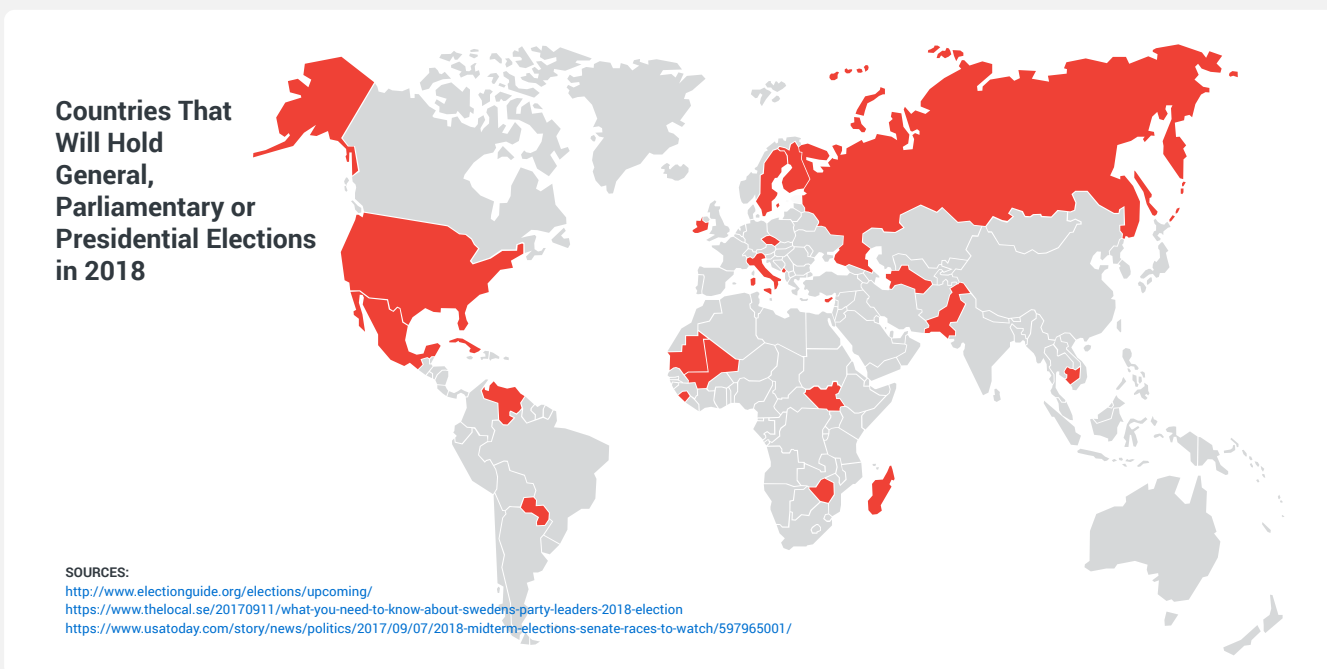


A close-up photograph of a person's hands using a laptop and a smartphone. The person is holding the smartphone in their right hand, looking at the screen. Their left hand is on the laptop keyboard. The image is overlaid with a complex geometric pattern of white lines forming various shapes, including diamonds and triangles, against a warm, orange-toned background. The text is positioned in the lower-left quadrant of the image.

CYBERPROPAGANDA CAMPAIGNS  
WILL BE REFINED USING  
TRIED-AND-TESTED TECHNIQUES  
FROM PAST SPAM CAMPAIGNS.

The **fake news** triangle consists of: motivations the propaganda is built on, social networks that serve as a platform for the message, and tools and services that are used to deliver the message. In 2018, we expect cyberpropaganda to spread via familiar techniques: those that were once used to spread spam via email and the web.

Do-it-yourself (DIY) kits in the form of software, for instance, can perform automated social media spamming. Even black hat search engine optimization (SEO) has been adapted to social media optimization (SMO), with a user base of hundreds of thousands able to provide traffic and numbers to different platforms. **From spear-phishing emails** sent to foreign ministries to the blatant use of documents to discredit authorities, dubious content can spread freely and spark forceful opinions or even real protests.



**Fabricated information**, additionally, can put businesses in a bad light and even hurt their performance and reputation. Researchers are even looking into audio and video manipulation tools that allow **realistic-looking footage** to further blur the line between authentic and fake. Manipulated political campaigns will continue to mount smear tactics and deliberately shift public perception, as allowed by the tools and services readily available in underground marketplaces.

It is likely that the upcoming **Swedish general election** will not be exempt from attempts to influence the voting outcome through fake news. The interest will also be hot on the heels of the U.S. midterm elections, as **social media can be wielded** to amplify divisive messages, as in the alleged meddling in the **previous U.S. presidential election** and the “troll farm” behind a Twitter **influencer**.

Each time fake news gets posted and reposted, a reader encountering the same content grows familiar with it and takes it as truth. Having the eye to distinguish fake news from not will be tough, as propagandists use old techniques that have proved effective and reliable.

Fake news and cyberpropaganda will press on because there has been no dependable way to detect or block manipulated content. Social media sites, most notably **Google** and **Facebook**, have already pledged a crackdown on bogus stories propagating across feeds and groups, but it has had **little impact** so far. That being the case, the final screening will still be dependent on the users themselves. But as long as users are not educated in flagging false news, such content will continue to permeate online and be consumed by unsuspecting and undiscerning readers.





THREAT ACTORS WILL RIDE ON  
MACHINE LEARNING AND BLOCKCHAIN  
TECHNOLOGIES TO EXPAND THEIR  
EVASION TECHNIQUES.

Knowing what is unknown. That's one of the key promises of machine learning, the process by which computers are trained but not deliberately programmed. For a relatively nascent technology, machine learning shows great potential. Already, however, it's become apparent that machine learning may not be the be-all and end-all of data analysis and insights identification. Machine learning lets computers learn by being fed loads of data. This means that machine learning can only be as good and accurate as the context it gets from its sources.

Going into the future, machine learning will be a key component of security solutions. While it uncovers a lot of potential for more accurate and targeted decision-making, it poses an important question: Can machine learning be outwitted by malware?

We've found that the CERBER ransomware uses a loader that certain machine learning solutions aren't able to detect because of how the malware is packaged [to not look malicious](#). This is especially problematic for software that employs pre-execution machine learning (which analyzes files without any execution or emulation), as in the case of the UIWIX ransomware (a WannaCry copycat), where there was [no file](#) for pre-execution machine learning to detect and block.

Machine learning may be a powerful tool, but it is not foolproof. While researchers are already looking into the possibilities of machine learning in monitoring traffic and [identifying possible zero-day exploits](#), it is not far-fetched to conjecture that cybercriminals will use the same capability to get ahead of finding the zero-days themselves. It is also possible to deceive machine learning engines, as shown in the [slight manipulation of road signs](#) that were recognized differently by autonomous cars. Researchers have already demonstrated how machine learning models have [blind spots](#) that adversaries can probe for exploitation.

While machine learning definitely helps improve protection, we believe that it should not completely take over security mechanisms. It should be considered an additional security layer incorporated into an in-depth defense strategy, and [not a silver bullet](#). A multilayered defense with end-to-end protection, from the gateway to the endpoint, will be able to fight both known and unknown security threats.

Another emerging technology that is poised to reshape businesses and that we see being abused is the blockchain. Blockchain technology has generated a lot of buzz in the context of digital cryptocurrencies and as a form of no-fail security. Adoption of the decentralized ledger is projected to be widespread in [five to 10 years](#). Currently, however, many initiatives are already being built on blockchain, ranging from [technology](#) and [finance](#) industry startups and giants to entire [governments](#) – all with the goal of revolutionizing business models.

Blockchain works by having a required consensus among the participants, which makes [unauthorized changes or deliberate tampering](#) with the blockchain difficult to do. The more transfers there are, the more the series becomes complex and obfuscated. This obfuscation, likewise, can be seen as an opportunity by cybercriminals looking into enhancing their attack vectors. They have already managed to target the blockchain in the [Ethereum DAO hack](#), which led to over US\$50 million worth of digital currency lost.

Like most promising technologies that were thought secure at one point, machine learning and blockchain warrant close attention.



MANY COMPANIES WILL TAKE  
DEFINITIVE ACTIONS ON THE GENERAL  
DATA PROTECTION REGULATION  
ONLY WHEN THE FIRST HIGH-PROFILE  
LAWSUIT IS FILED.



The European Union (EU) will finally be rolling out [GDPR](#) in May 2018, with an expected extensive impact on data handling of companies that engage with EU citizens' data – even if the said companies are outside Europe. In our [research](#), we found that the majority of C-level executives (in 57 percent of businesses) shun the responsibility of complying with GDPR, with some unaware of what constitutes personally identifiable information (PII) and even unbothered by potential monetary penalties.

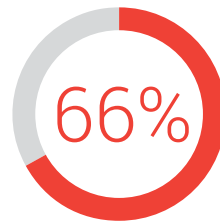
Laggards will fully heed the brunt of GDPR only when the retributions are imposed by the regulators. Data privacy watchdogs can interfere with business operations by altogether [banning companies from processing certain data](#). There is also the possibility that lawsuits, both from the authorities and from the citizens themselves, will come into the picture.

The American credit reporting agency Equifax, for instance, would have faced a staggering fine, as some U.K. consumers were [reportedly affected](#) too, if the breach had happened after the GDPR implementation had gone into effect and it hadn't come forward with the incident sooner than it chose to. A considerable penalty would have also been imposed on the international ride-hailing company Uber, which announced a [data breach](#) over a year after the fact. [Noncompliance with breach notification](#) will prompt regulators to issue fines of up to €20 million, or up to 4 percent of the company's global annual turnover of the preceding financial year, whichever is greater.

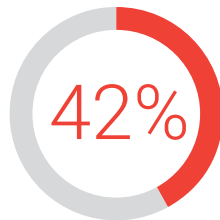
Companies waking up to the GDPR enforcement, therefore, will find the importance of having a dedicated data protection officer (DPO) who can spearhead data processing and monitoring. DPOs are particularly needed in enterprises and industries that handle sensitive data. Companies will be required to review their data security strategy, including classifying the nature of data and distinguishing EU data from data associated with the rest of the world.

Other regions will have to catch up with their data regulations by having a similar framework of wide-ranging scope and tougher penalties for compliance failure. The U.S. Food and Drug Administration (FDA) has already [recognized](#) several European drug regulatory authorities to improve its inspections. Australia is gearing up to enact its own data breach notification laws based on the [Privacy Amendment \(Notifiable Data Breaches\) Act 2017](#), while U.K.'s [Data Protection Bill](#) is getting updated to match EU's laws after Brexit. Meanwhile, the EU-U.S. Privacy Shield deal will have to prove how binding it is in spite of [concerns](#) expressed by the EU.

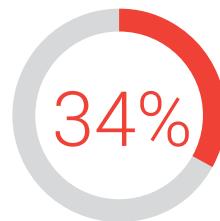
### GDPR Is Coming. Are You Prepared?



of businesses appear to be dismissive of the extent of GDPR fines.



of businesses don't know email marketing databases contain PII.



of businesses have invested in technology to identify intruders.

SOURCE:

<http://newsroom.trendmicro.com/press-release/commercial/trend-micro-research-reveals-c-level-executives-are-not-prepared-gdpr-imple>





ENTERPRISE APPLICATIONS  
AND PLATFORMS WILL BE AT  
RISK OF MANIPULATION AND  
VULNERABILITIES.

In today's environment, where the Industry 4.0 makes cyber-physical systems and production processes increasingly interconnected and software-defined, risks can stem from several areas within. The notion of having a digital twin, a virtual replica or simulation of the real-world production or process, is enabling enterprises to address performance issues that may arise in real physical assets. However, we believe that while it's poised to transform operations, the production network can be infiltrated by malicious actors aiming to manipulate the system and cause operational disruptions and damages. By manipulating the digital twin itself, these actors can make production processes look legitimate when they have, in fact, been modified.

In addition, production data that is directly (or indirectly) handed over via manufacturing execution systems (MES) to SAP or other enterprise resource planning (ERP) systems is also in danger of being compromised. If a manipulated piece of data or wrong command is sent to an ERP system, machines will be liable to sabotage processes by carrying out erroneous decisions, such as delivery of inaccurate numbers of supplies, unintended money transfers, and even system overloads.

Enterprise systems will not be the only ones targeted; in 2018, we expect to continue to see security flaws in Adobe and Microsoft platforms. What's going to be particularly interesting, though, is the renewed focus on browser-based and server-side vulnerabilities.

For years, the vulnerabilities of well-known browser plug-ins like Adobe Flash Player, Oracle's Java, and Microsoft Silverlight have been targeted. We predict that in 2018, however, weaknesses in JavaScript engines will beset the modern browsers themselves. From [Google Chrome's V8 crashing issues to Microsoft Edge's Chakra being open source](#), [JavaScript-based browser vulnerabilities](#) will make more appearances in 2018 given the wide use of the script on the web.

Attackers will also take a renewed focus on using server-side vulnerabilities to deliver malicious payloads. We predict that the use of Server Message Block (SMB) and Samba exploits that deliver ransomware will be more pronounced in 2018. [SMB vulnerabilities](#), in particular, can be exploited without any direct interaction with the user. In fact, an SMB vulnerability was used in the [EternalBlue](#) exploit that crippled many networks running on Windows during the WannaCry and Petya ransomware attacks, and in the more recent Bad Rabbit attacks that exploited [EternalRomance](#). The [open-source Samba](#) on Linux, similarly, is capable of exploiting vulnerabilities in the SMB protocol.

Attacks against production processes through SAP and ERP mean that enterprises will need to take the security of related applications as priority. Access to the applications will need to be managed and monitored to avoid any unauthorized access.

Users and enterprises are advised to routinely check for software updates and apply patches once they are available. However, as administrators can stumble over immediate deployment of updates, we recommend integrating vulnerability shielding into systems so that platforms are protected against unpatched and zero-day vulnerabilities. Network solutions should also secure connected devices from potential intrusions through virtual patching and proactive monitoring of web traffic.



# Tackling Security in 2018

Given the broad range of threats the landscape currently bears and will expect to face in 2018 – from vulnerabilities and ransomware to spam and targeted attacks – what enterprises and users alike can best do is to minimize the risk of compromise at all layers.

## Better visibility and multilayered security defense for enterprises

To combat today's expansive threats and be fortified against those yet to come, organizations should employ security solutions that allow visibility across all networks and that can provide real-time detection and protection against vulnerabilities and attacks. Any potential intrusions and compromise of assets will be avoided with a dynamic security strategy that employs cross-generational techniques appropriate for varying threats. These security technologies include:

- **Real-time scanning.** Active and automatic scans allow highly efficient malware detection and improved machine performance.
- **Web and file reputation.** Malware detection and prevention through web reputation, anti-spam techniques, and application control protect users from ransomware attacks and exploits.
- **Behavioral analysis.** Advanced malware and techniques that evade traditional defenses are proactively detected and blocked.
- **High-fidelity machine learning.** Human inputs augmented with threat intelligence data allow rapid detections and accurate defenses against known and unknown threats.
- **Endpoint security.** Security that employs sandboxing, breach detection, and endpoint sensor capabilities detect suspicious activities and prevent attacks and lateral movement within the network.

## Best practices and sustained protection for end-users

Having different devices and applications to access information is becoming second nature in today's increasingly connected world. Regardless of device, application, or network, users will be able to fill the security gaps with proper configurations:

- **Change default passwords.** Use unique and complex passwords for smart devices, especially for routers, to significantly reduce the possibility of attackers hacking into the devices.
- **Set up devices for security.** Modify devices' default settings to **keep privacy in check** and implement encryption to prevent unauthorized monitoring and use of data.
- **Apply timely patches.** Update the firmware to its latest version (or enable the auto-update feature if available) to avoid unpatched vulnerabilities.
- **Deflect social engineering tactics.** Always be mindful of emails received and sites visited as these can be used for spam, phishing, malware, and targeted attacks.

Enterprises and users are better positioned if protections in place are able to cover the entire threat life cycle with multiple security layers. From the email and web gateway to the endpoint, having a connected threat defense ensures maximum protection against the constantly evolving threats of 2018 and beyond.

For Raimund Genes (1963 - 2017)

Created by:

**TrendLabs**

The Global Technical Support and R&D Center of TREND MICRO

**TREND MICRO™**

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit [www.trendmicro.com](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud