THE NEXT TIER

Trend Micro Security Predictions for 2017

People waking up to the threat landscape of 2017 will say it is both familiar and unchartered terrain. After all, while our predictions for 2016 have become reality, they only opened doors for more seasoned attackers to explore an even broader attack surface. In 2016, online extortion exploded, a smart device failure indeed caused damage, the need for Data Protection Officers (DPOs) became ever more pressing, and data breaches became as commonplace as ever.

New challenges will arise in 2017. Ransomware operations will break off into several routes—fuller, as more variants are produced; deeper, as well-planned targeted attacks are launched; and wider, as threats affect nondesktop targets like mobile and smart devices. Simple-but-effective Business Email Compromise (BEC) attacks will become cybercriminals' next new favorite, while we will begin to see more hard-hitting Business Process Compromise (BPC) attacks like the US$81-million Bangladesh Bank heist. More Adobe and Apple vulnerabilities will be discovered and exploited. Even innocuous smart devices will play a role in massive distributed denial-of-service (DDoS) attacks and Industrial Internet of Things (IIoT) devices will be targeted by threat actors. The General Data Protection Regulation (GDPR) implementation looms nearer, and as enterprises scramble to change processes to comply, administrative costs for those affected will skyrocket, even as they grapple with threat actors worldwide bent on infiltrating their networks for various motives. This is the next tier of digital threats, requiring next-level solutions.

Trend Micro has been in the security business for more than two decades now. Our real-time monitoring of the threat landscape, along with the findings of our Forward-Looking Threat Research (FTR) Team, has allowed us to understand the different drivers that determine how the landscape moves and toward where. Read on to see how 2017 and beyond looks like.

1

Ransomware growth will plateau in 2017, but attack methods and targets will diversify.

We accurately predicted that 2016 would be the "Year of Online Extortion." Ransomware's attack chain—combining a wide array of delivery methods, unbreakable encryption, and fear-driven schemes—transformed this old favorite into a foolproof cybercriminal cash cow. Ransomware as a service, a setup where a ransomware operator rents his infrastructure to cybercriminals encouraged even the nontechnical to get into the game. Also in 2016, some ransomware code was shared with the public, allowing hackers to generate their own versions of the threat. These resulted in a staggering 400% spike in the number of ransomware families from January to September.

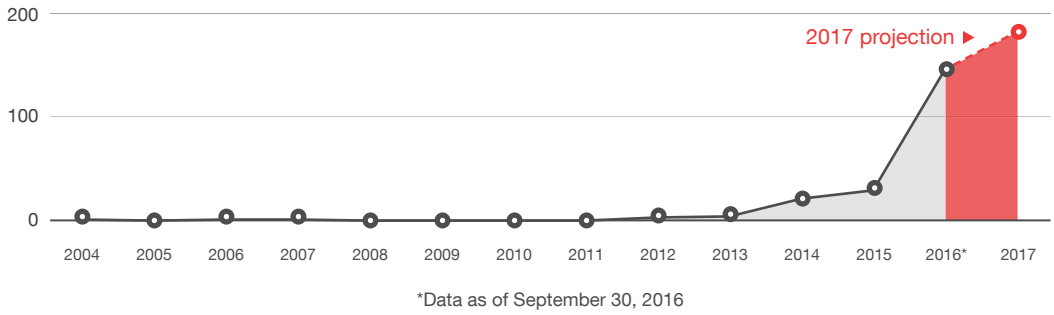


Figure 1: Annual number of ransomware families, including 2017 projection

We predict a 25% growth in the number of new ransomware families in 2017, translating to an average of 15 new families discovered each month. Although the tipping point has passed in 2016, a period of stabilization will push competing cybercriminals to diversify, hitting more potential victims, platforms, and bigger targets.

We also predict that ransomware will become an increasingly commonplace component of data breaches. Cybercriminals will first steal confidential data to sell in underground markets, then install ransomware to hold data servers hostage, doubling their profit.

Mobile ransomware will likely follow the same trajectory as desktop ransomware given how the mobile user base is now a viable, untapped target. Nondesktop computing terminals like point-of-sale (PoS) systems or ATMs may also suffer extortion-type attacks.

There is currently little value in taking smart devices hostage as the effort to attack them outweigh the possible profit. For example, it is easier and cheaper to replace a hacked smart light bulb than to pay the ransom. On the other hand, attackers threatening to take control of a car's brakes while it is on the expressway might turn a profit, but again, the effort required to perform such an attack does not make it a very viable means of extortion.

It is now clearer to enterprises that suffering a ransomware attack has become a realistic possibility and a costly business disruption. Ransomware (against industrial environments) and IIoT attacks will cause bigger damage as threat actors can get more money in exchange for getting a production floor back online, for instance, or switching facility temperatures back to safer ranges.

While there is no silver bullet that can protect potential targets from ransomware attacks 100% of the time, it is best to block the threat at its source, via Web or email gateway solutions. Machine-learning technology is likewise a strong complement to multilayered security that can detect even unique and newly created ransomware.

2

IoT devices will play a bigger role in DDoS attacks; IIoT systems in targeted attacks.

Thousands of webcams that people didn't think twice about securing became the stronghold for the Mirai DDoS attack that took down major websites. Connected devices, like sleeper agents, are innocuous until activated by cybercriminals. We predict that in 2017, more cyber attacks will find the Internet of Things (IoT) and its related infrastructure front and center, whether threat actors use open routers for massive DDoS attacks or a single connected car to stage highly targeted ones.

We predict that cybercriminals will use Mirai-like malware in DDoS attacks. From 2017 onward, service-oriented, news, company, and political sites will get systematically pummeled by massive HTTP traffic either for money, as a form of indignation, or as leverage for specific demands.

Unfortunately, we also predict that vendors will not react in time to prevent these attacks from happening. In the Mirai attack, webcam recalls were indeed triggered by the vendor, but it did not exactly prompt similar code reviews on unaffected but still controllable connected devices. Therefore, there will always be a potent attack surface available to threat actors.

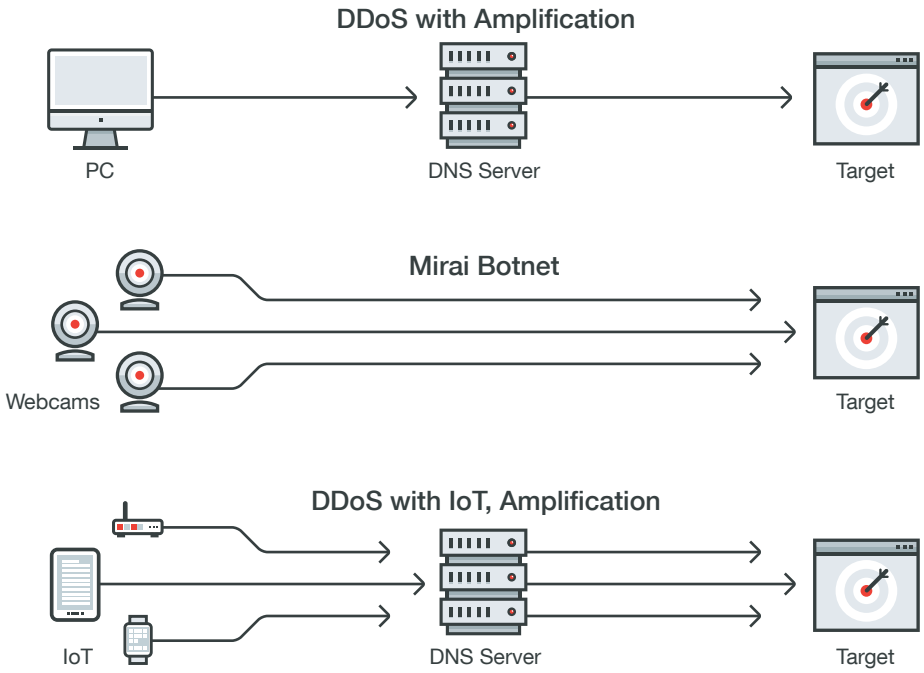


Figure 2: The Mirai botnet did not need a Domain Name System (DNS) server to knock a target offline, but it did lock out a swath of users from sites. Theoretically, IoT botnets can amplify DDoS attacks and cause more damage.

Likewise, as IoT introduces efficiencies into industrial environments like manufacturing and energy generation, threat actors will build on the effectiveness of the BlackEnergy attacks to further their own ends. Together with the significant increase in the number of supervisory control and data acquisition (SCADA) system vulnerabilities (30% of the total number of vulnerabilities found by TippingPoint in 2016), the migration to IIoT will introduce unprecedented dangers and risks to organizations and affected consumers in 2017.

These dangers can be proactively addressed by vendors who sell smart devices and equipment by implementing security-focused development cycles. Barring that, IoT and IIoT users must simulate these attack scenarios to determine and protect points of failure. An industrial plant's network defense technology must, for instance, be able to detect and drop malicious network packets via network intrusion prevention systems (IPSs).

3

The simplicity of Business Email Compromise attacks will drive an increase in the volume of targeted scams in 2017.

Targeting finance departments worldwide, BEC is about hacking an email account or tricking an employee to transfer funds over to a cybercriminal's account. There is nothing special about the attack, except perhaps the reconnaissance required to gain insights into the best way to craft a believable email—but even that is often just a well-designed search engine query away.

We predict that this simplicity will make BEC, specifically CEO fraud, a more attractive mode of attack for cybercriminals. The scam is easy and cost-effective, not requiring so much in terms of infrastructure. But the average payout for a successful BEC attack is US$140K—the price of a small house. The total estimated loss from BEC in two years is US$3 billion. In comparison, the average payout for a ransomware attack is US$722 (currently 1 Bitcoin), which could reach up to US$70K if an enterprise network is hit.

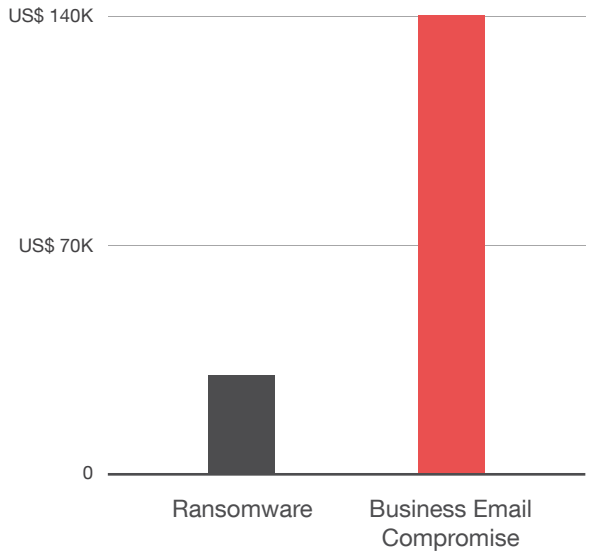


Figure 3: Comparison of average enterprise payouts for ransomware and BEC attacks

The relative payout speed will also drive this projected increase. Based on our BEC research using Predator Pain cases, attackers were able to net US$75 million in just six months. The slower wheels of justice when it comes to cross-border crime, meanwhile, will increase the threat's attractiveness. For instance, it took over two years before a Nigerian national got arrested for scamming several companies since 2014.

BEC is especially hard to detect because these emails do not contain malicious payloads or binaries, but enterprises should be able to block these threats at the source using Web and email gateway solutions. These security technologies will be able to identify abnormal traffic and malicious file behaviors or components, but defending against BEC scams will remain difficult if victims continue to willingly hand over money to cybercriminals. Companies must implement stringent policies for normal and out-of-the-ordinary transactions, which include layers of verification and thresholds for large sums requiring more validation, before executing transfers.

4

Business Process Compromise will gain traction among cybercriminals looking to target the financial sector.

The Bangladesh Bank heist caused losses of up to US$81 million. Unlike BEC, which relies on erroneous human behavior, the heist stemmed from a much deeper understanding of how major institutions processed financial transactions. We are calling this category of attacks "BPC."

We predict that BPC will go beyond the finance department, although fund transfers will remain its most typical endgame. Possible scenarios include hacking into a purchase order system so cybercriminals can receive payment intended for actual vendors. Hacking into a payment delivery system can likewise lead to unauthorized fund transfers. Cybercriminals can hack into a delivery center and reroute valuable goods to a different address. This already happened in an isolated incident in 2013, where the Antwerp Seaport shipping container system was hacked in order to smuggle drugs.

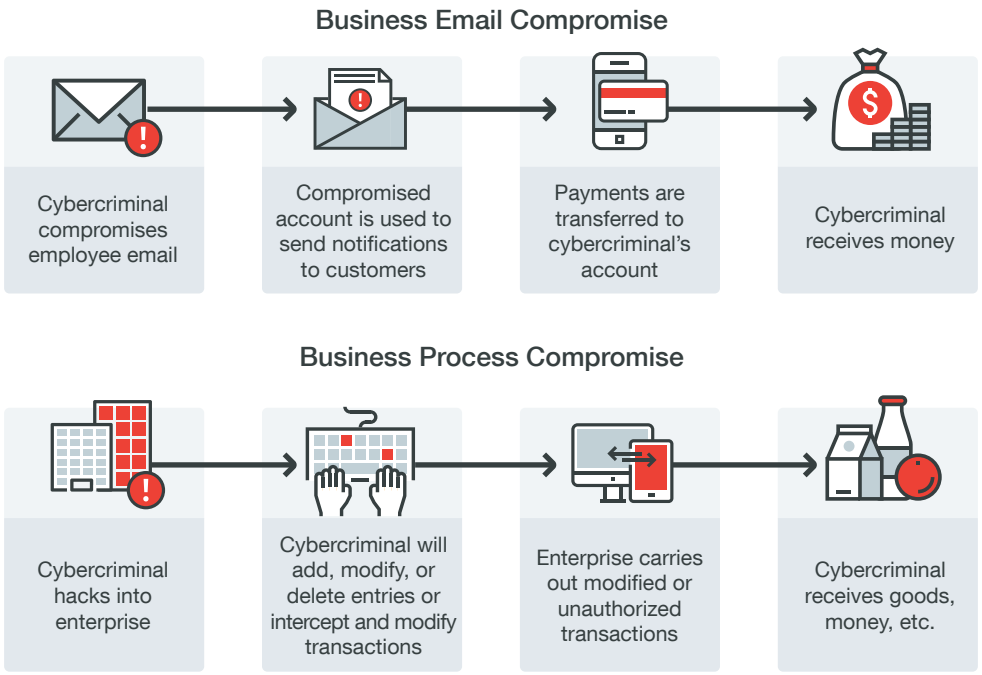
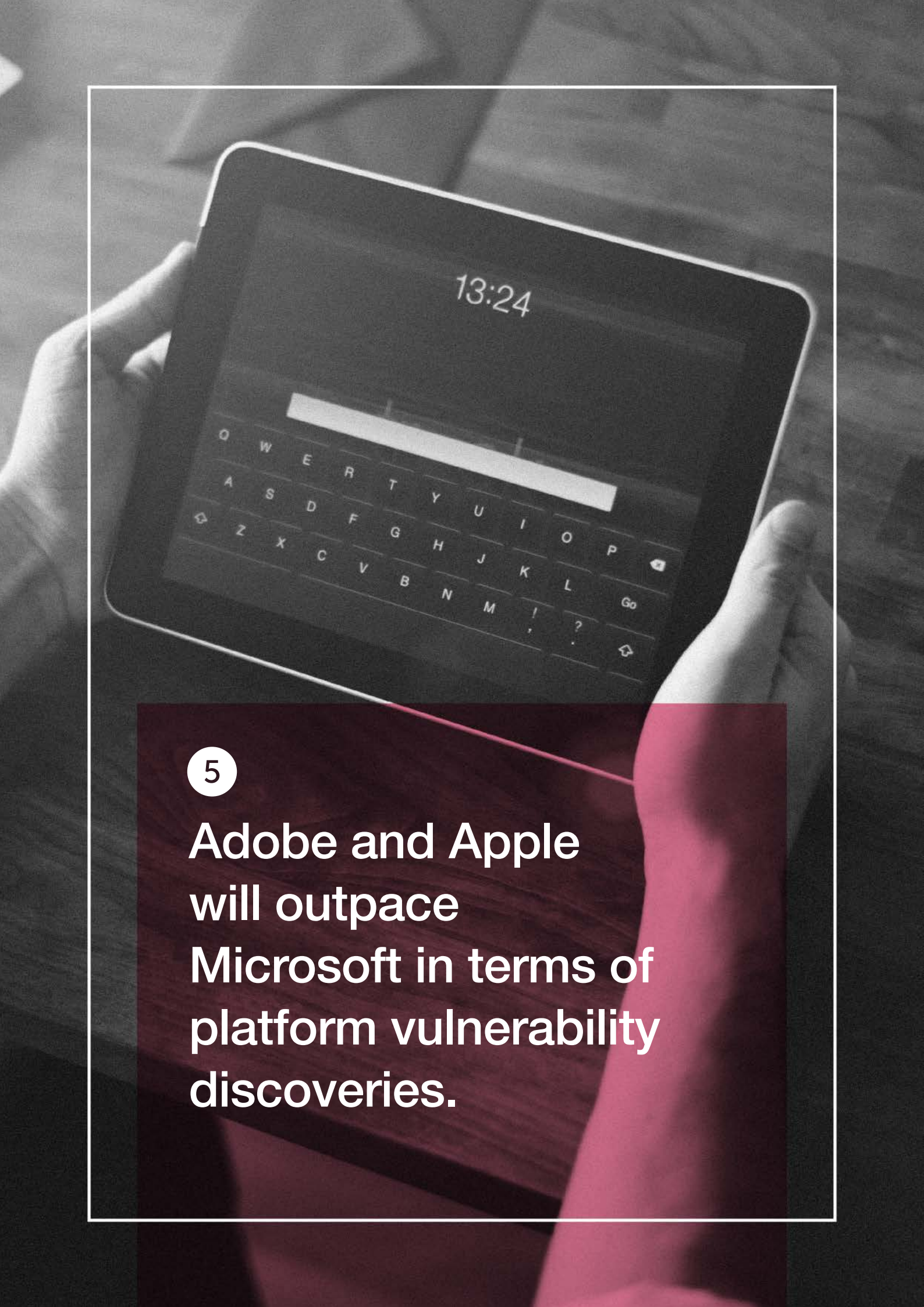


Figure 4: BEC versus BPC attacks

Cybercriminals staging BPC attacks will still solely go after money instead of political motives or intelligence gathering, but the methods and strategies used in these and targeted attacks will be similar. If we compare the payout between ransomware attacks in enterprise networks, the average payout of BEC attacks and the potential gain in BPC attacks (US$20,000, US$140,000, and US$81 million, respectively), it is easy to see why cybercriminals or even other threat actors like rogue states in need of more funds will be more than willing to take this route.

Enterprises have limited visibility of the risks associated when business processes are attacked. The typical security focus is to ensure that devices do not get hacked into. Cybercriminals will take full advantage of this delayed realization. Security technologies like application control can lock down access to mission-critical terminals while endpoint protection must be able to detect malicious lateral movement. Strong policies and practices regarding social engineering must be part of an organization's culture as well.



5

Adobe and Apple will outpace Microsoft in terms of platform vulnerability discoveries.

Adobe outpaced Microsoft for the first time in 2016 in terms of vulnerability discoveries. Among the vulnerabilities disclosed through the Zero-Day Initiative (ZDI) so far in 2016 were 135 vulnerabilities in Adobe products and 76 in Microsoft's. 2016 was also the single-biggest year for Apple® in terms of vulnerability as 50 vulnerabilities were disclosed as of November, up from 25 the previous year.

We predict that more software flaws will be discovered in Adobe and Apple products in addition to Microsoft's. Apart from the fact that Microsoft's PC shipments have been declining in recent years as more users opt for smartphones and professional-level tablets instead, the vendor's security mitigations and improvements will also make it more difficult for attackers to find more vulnerabilities in its OS.

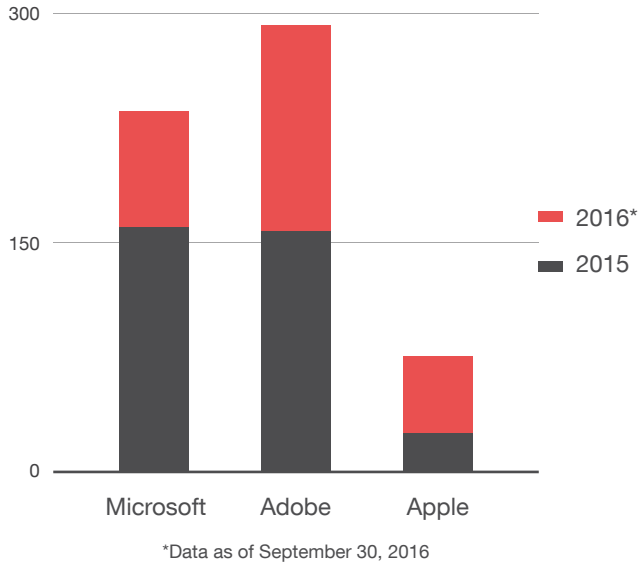
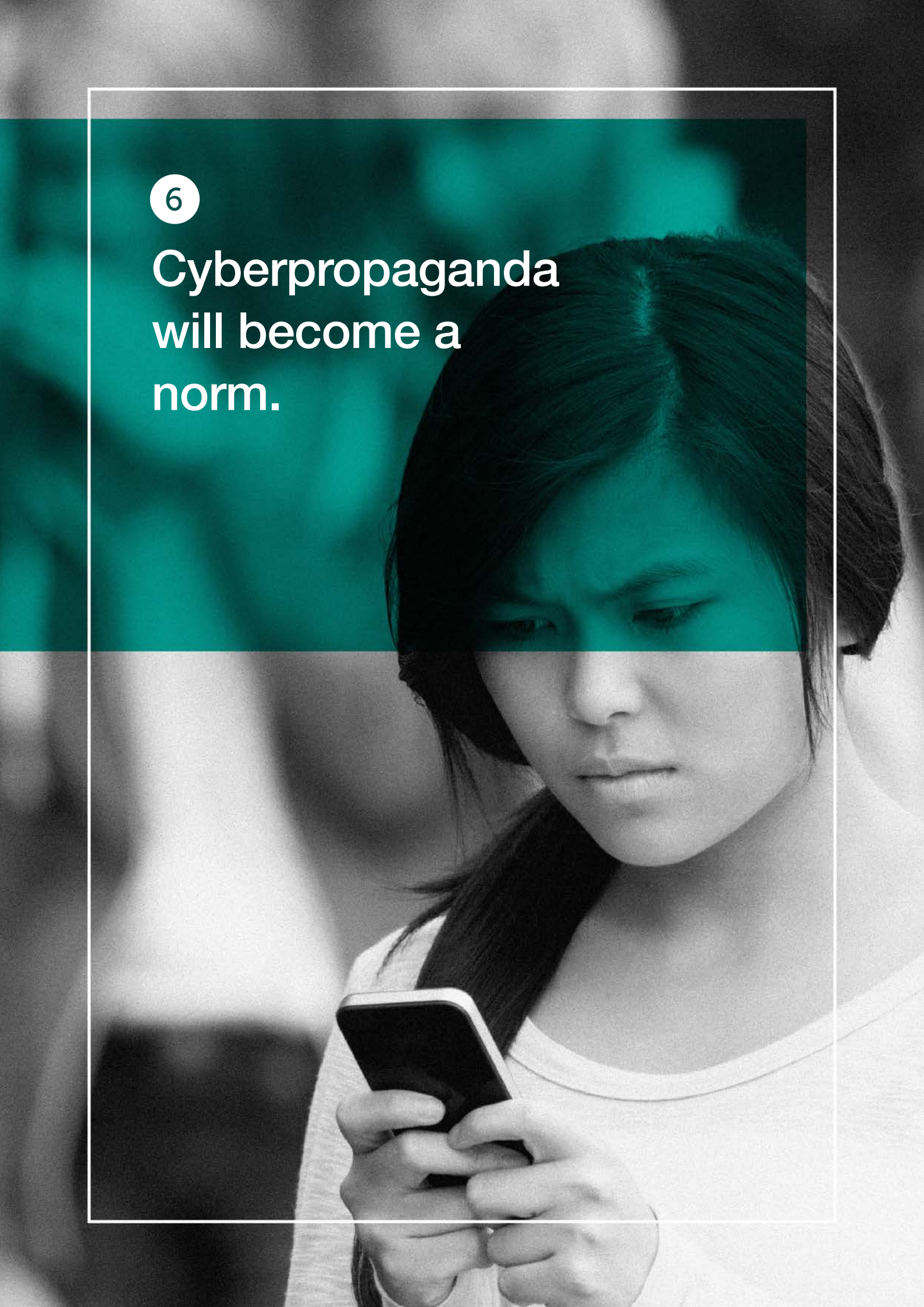


Figure 5: Microsoft, Adobe, and Apple vulnerabilities disclosed by the ZDI

The discovery of Adobe vulnerabilities will invariably lead to the development of exploits that can then be integrated into exploit kits. Exploit kits will continue to be part of the threat landscape, but cybercriminals may find even more use for them apart from delivering ransomware. Exploit kit usage dwindled after the arrest of the Angler Exploit Kit creator, but as with BlackHole and Nuclear, other exploit kits will simply take over.

Apple software will likewise be abused as more users buy Macs. The US Mac shipment increased, allowing Apple to gain a bigger market share compared with the previous year. In addition to Microsoft's security improvements, this gain will further drive cybercriminals' attention to non-Microsoft alternatives. Also, since Apple no longer supports iPhone® 4S, we will see more exploits for flaws patched in supported versions be used to find similar flaws that will no longer be patched in unsupported versions.

Vulnerability shielding is the only way to proactively and reliably protect against unpatched and zero-day vulnerabilities. While exploits are an existing reality for a lot of enterprises, especially those that still choose to use unsupported, legacy, or orphaned software, vulnerability shielding's role becomes especially important when highly popular and widely used software like Apple's and Adobe's are concerned. Apple and Adobe product users should also protect endpoints and mobile devices from malware that exploit these vulnerabilities.



6

Cyberpropaganda will become a norm.

In 2016, close to half of the world's population (46.1%) now have Internet access, whether through smartphones, traditional computing devices, or Internet kiosks. This means more and more people now have fast and easy access to information, regardless of source or credibility.

The rise in the Internet penetration has opened the opportunity for invested parties to use the Internet as a free-for-all tool to influence public opinion to go one way or another. The outcome of the recent elections in different countries reflects the power of social media and various online sources of information when it comes to political decision-making.

Most recently, we have seen platforms like WikiLeaks used for propaganda—with highly compromising materials leaked through the site just a week before the US elections. In our continuous monitoring of the cybercriminal underground, we also noted script kiddies advertise their earnings from fake election-related news. They claim to make around US$20 per month by driving traffic to fabricated smear content about electoral candidates. There are also existing groups of dedicated cyber agents who are paid to post propaganda materials on social media sites like Facebook and LinkedIn. They take advantage of the platforms' electronic content filtering to multiply the visibility of their content.

The lack of vetting for accuracy of information, coupled with avid sharers who wish to sway people with opposing beliefs or simply to support their own, has led to the popularity of these fake content and memes. All this makes it very difficult for casual, unsophisticated Internet users to distinguish between facts or otherwise.

We have yet to see the direct impact of Facebook and Google's move to pull out advertising from sites bearing fake news, and of Twitter's to expand its mute function so users can tune out abusive attacks or conversations.

The upcoming elections in France and Germany, including subsequent movements similar to the United Kingdom (UK)'s withdrawal from the European Union (EU), also known as Brexit, will be influenced by what is being shared and done using electronic media. We will likely see more sensitive information used in cyberpropaganda activities stem from espionage operations such as PawnStorm.

Entities that are able to navigate public opinion using this means in a strategic manner will be able to produce results that favor them. In 2017, we will see much more use, abuse, and misuse of social media.

7

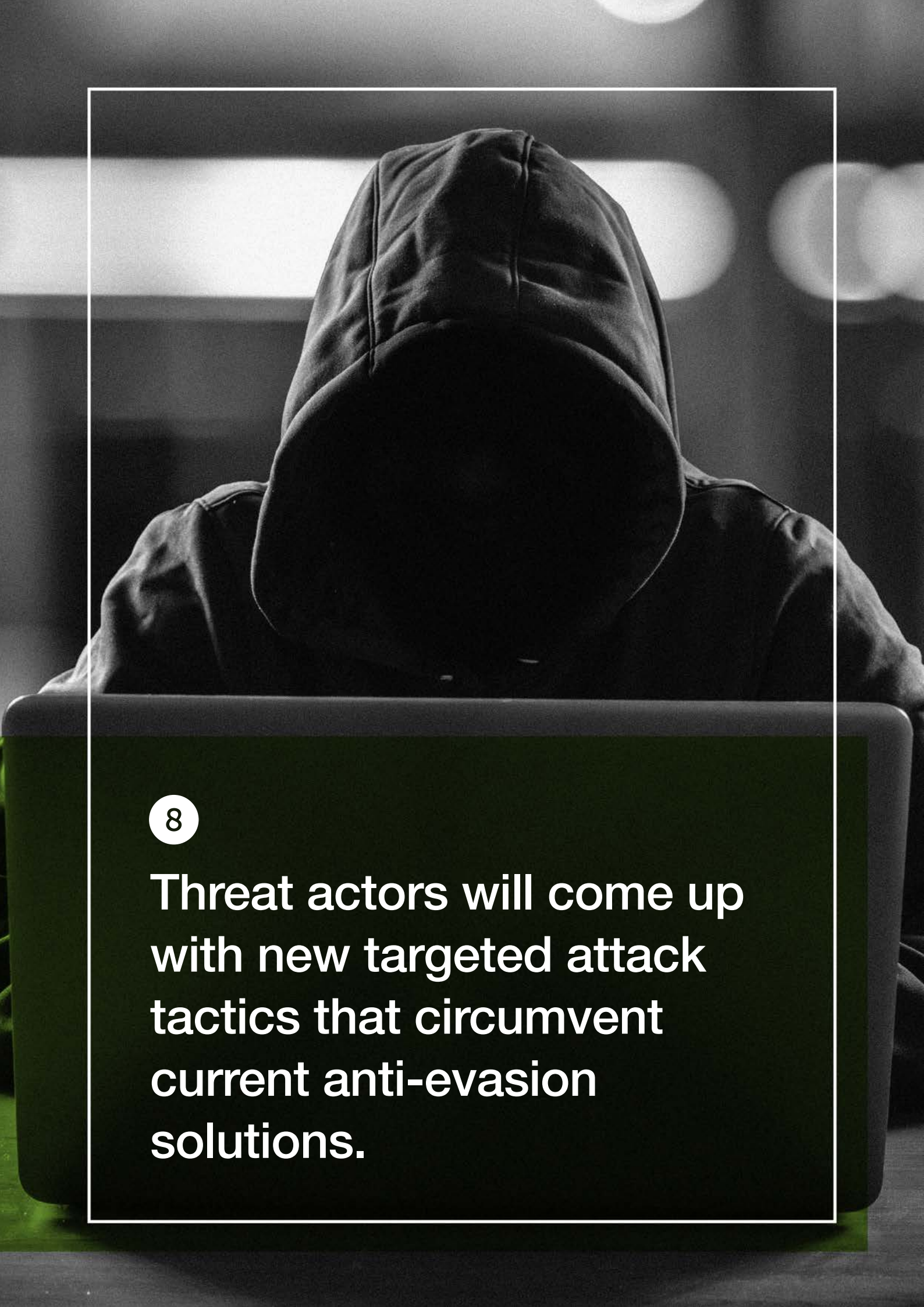
General Data Protection Regulation implementation and compliance will raise administrative costs across organizations.

The GDPR—the EU's response to the clarion call for data privacy—will impact not just EU member states but all entities worldwide that capture, process, and store the personal data of EU citizens. By the time it is enforced in 2018, enterprises can be fined as much as 4% of a company's global turnover for noncompliance.

We predict that the GDPR will force changes in policies and business processes for affected companies that will significantly raise administrative costs. The GDPR requires the following changes, among others:

- **A DPO is now mandatory.** We predicted that less than half of enterprises will have hired DPOs by the end of 2016. That forecast is shaping up to be accurate, which means a large brand-new line item for hiring, training, and keeping a new senior-level employee will appear under company expenses.
- **Users must be informed of their newly outlined user rights and companies must ensure users are able to exercise them.** This paradigm shift, that EU citizens own their personal data and thus collected data is merely "on loan," will impact entire data-related workflows.
- **Only the minimum data required to use a service must be collected.** Enterprises must revise their data-collection practices to adjust.

These changes will force enterprises to conduct a top-to-bottom review of data processing in order to ensure or establish compliance and segregate EU data from the rest of the world's. It will be especially difficult for multinational companies who will have to consider building entirely new data storage systems just for EU data. They will also need to review the data protection clauses of their cloud storage partners. Enterprises must invest in a comprehensive data security solution, including employee training, to enforce compliance to the GDPR.



8

Threat actors will come up with new targeted attack tactics that circumvent current anti-evasion solutions.

Targeted attack campaigns were first documented close to a decade ago. Threat actors have grown more seasoned, while network infrastructures have remained largely the same. As we observe attackers' movements and ability to adjust their tools, tactics, and procedures (TTPs) to be able to target different organizations in different countries, we predict new and unexpected techniques to emerge in future targeted attacks.

We predict that this learning curve will mean using more methods primarily intended to evade most modern security technologies developed in recent years. Threat actors, for instance, typically used binaries, then moved on to documents, and are now using more script and batch files. They will start doing more deliberate sandbox detection to see if a network pushes unknown files to a sandbox resource and will even target or inundate sandboxes. We also predict that virtual machine (VM) escapes will become highly prized components of advanced exploit chains. VM escape bugs will have various other attack applications in the cloud, apart from sandbox evasion.

These technical improvements on the attacker front will pose greater demands from IT or security administrators. They must seek out security technologies that can help them get a complete view and gain full control of their entire network and data workflow, while identifying not only indicators of compromise (IoCs), but also indicators of attack at the onset.

Unknown threats can either be new variants of known, existing threats, or completely unknown threats that have yet to be discovered. Security solutions that use machine learning can be used to protect against the former, while sandboxing will be able to manage the latter. Instead of sticking to one security strategy, cross-generational multilayered technology developed through extensive experience gained from monitoring, responding to, and devising proactive measures against targeted attacks will be extremely important in battling these kinds of campaigns.

How Do We Meet Attacks Head-On?

Machine learning is not a new-fangled security technology, but it is poised to be a crucial element in battling known and unknown ransomware threats and exploit kit attacks, among others. Machine learning is deployed through a layered system with human- and computer-provided inputs running through mathematical algorithms. This model is then pitted against network traffic, allowing a machine to make quick and accurate decisions about whether the network content—files and behaviors—are malicious or not.

Enterprises must also ready themselves with proven protection against the anti-evasion techniques that threat actors will introduce in 2017. This challenge calls for a combination (versus a silver-bullet type approach) of different security technologies that should be available across the network to form a connected threat defense. Technologies like:

- Advanced anti-malware (beyond blacklisting)
- Antispam and antiphishing at the Web and messaging gateways
- Web reputation
- Breach detection systems
- Application control (whitelisting)
- Content filtering
- Vulnerability shielding
- Mobile app reputation
- Host- and network-based intrusion prevention
- Host-based firewall protection

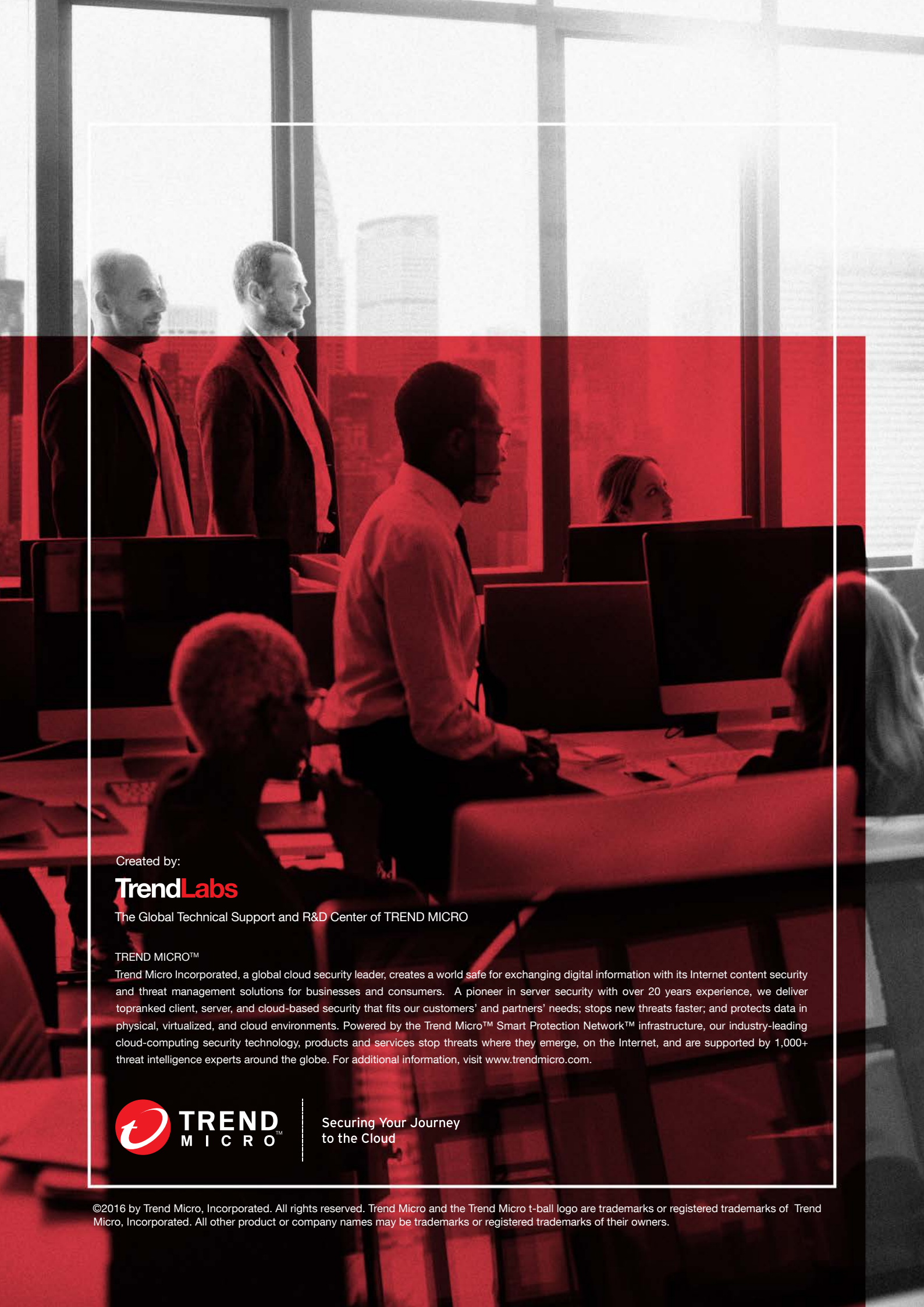
A majority of today's threats can be detected by the aforementioned techniques working together, but in order to catch zero-day and "unknown" threats, enterprises must use behavior and integrity monitoring as well as sandboxing.

IoT affords both risks and conveniences. Smart device users should learn to secure their routers before allowing any smart device to access the Internet through them. They should then include security as a consideration when buying a new smart device. Does it provide for authentication or allow password changes? Can it be updated? Can it encrypt network communications? Does it have open ports? Does its vendor provide firmware updates?

Enterprises that collect data from EU citizens should expect a bump in administrative expenses as they grapple with major process changes and hire DPOs to comply with the GDPR. A thorough review of a company's data protection strategy will also help in passing audits.

These new challenges require a new take on endpoint security, a cross-generational security approach combining proven threat-detection techniques for known and unknown threats with advanced protection techniques such as application control, exploit prevention and behavioral analysis, sandbox detection, and high-fidelity machine learning.

Training employees against social engineering attacks and about the latest threats like BEC will complete the security culture needed to fortify an enterprise's defenses for 2017 and beyond.



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 topranked 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.

TREND MICRO™

Securing Your Journey to the Cloud