
# The 2017 Security Threat Landscape

*2017 was rife with global ransomware attacks, large-scale vulnerability threats, debilitating BEC scams, the rise of cryptocurrency risks, ever-evolving IoT threats, and a continued stream of data breaches. How did businesses fare in their midst? And what should companies do to manage their enterprise risk in 2018?*

## The Paradox of Cyberthreats in 2017

Though the ransomware volume did plateau in 2017 as we expected, the threat continued to wreak havoc on a massive scale worldwide.[1]

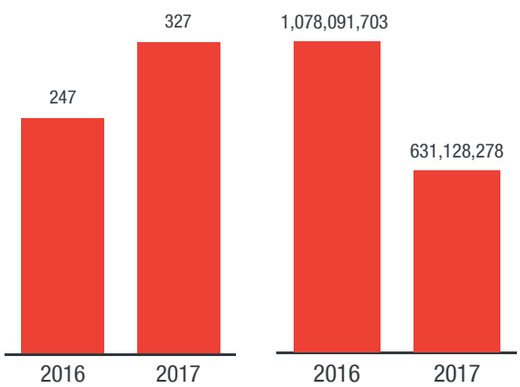


*Figure 1. More ransomware families emerged in 2017 but fewer major players despite the said rise*

Ransomware attacks impacting business operations continued to increase in 2017. Ransomware attacks from WannaCry to Petya resulted in production line downtime at Honda, Nissan, Renault, and even Cadbury. The likelihood and impact of these attacks increased 10 times with the convergence of capable ransomware and the wormlike capabilities of the EternalBlue exploit. This malicious marriage resulted in an attack that affected 300,000 computers across 150 countries in just a matter of days.[2] Petya, meanwhile, proved lethal as well with the advent of a variant capable of completely wiping a system's hard disk and displaying a blue screen of death (BSoD) as ransom note. Petya reportedly affected 12,500 computers in 165 countries across the globe.[3]

> The global ransomware damage cost was predicted to exceed **US$5B** in 2017.

These attacks, if nothing else, highlighted the need for CISOs to rethink and reassess their operational risk exposure. No longer can we look at these threats solely as an IT risk but rather as a combined IT and operational technology (OT) risk that could result in billions in losses globally.

The need for risk-based vulnerability management couldn't be greater in 2018. We've seen Dirty COW, for instance, cause grief among 5,000 users in more than 40 countries prior to its discovery in 2017.[4] With the help of external researchers via our Zero Day Initiative (ZDI), we discovered and disclosed a record number of 1,008 new vulnerabilities in 2017, only a small percentage of these were and will continue to be weaponized in exploit attacks. The time from disclosure to exploitation has decreased dramatically though, significantly impacting the landscape.

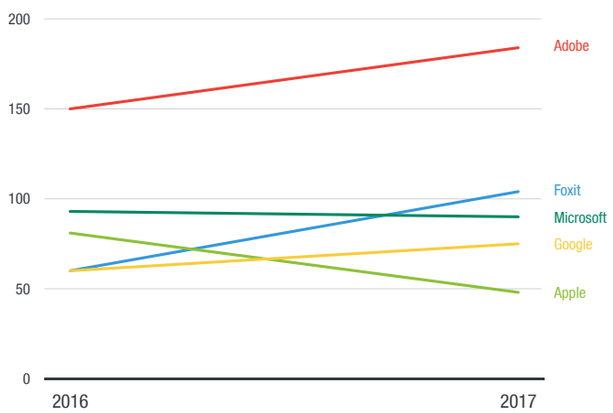


*Figure 2. A variation in vulnerability count direction was seen*

Increases in both the overall number of zero-day vulnerabilities (disclosed without a patch available) and that specifically affect supervisory control and data acquisition (SCADA) systems were seen as well.

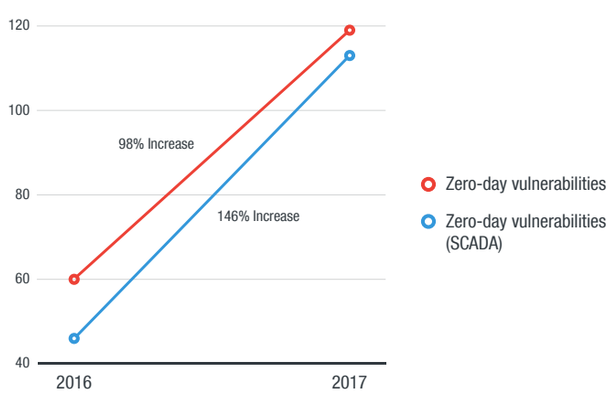


*Figure 3. A marked increase in the volume of zero-day vulnerabilities was seen*

Business email compromise (BEC) attacks continued to grow exponentially, raking in huge profits at the expense of companies worldwide. Although simplistic in scope, these attacks were large in scale. The FBI's Internet Crime Complaint Center (IC3)

received more than 12,000 complaints amounting to a loss of US$360 million in 2016 alone.[5] These deceptively simple socially engineered attacks are incredibly adept at finding and exploiting systemic communication vulnerabilities in organizations. CISOs will need to expand their training and awareness programs to include the boardroom as well as the server room to mitigate them.

> Losses resulting from BEC scams reached **US$5B** in 2017.

As in the past, BEC scammers continued to spoof (as senders) and target (as recipients) company executives throughout 2017.

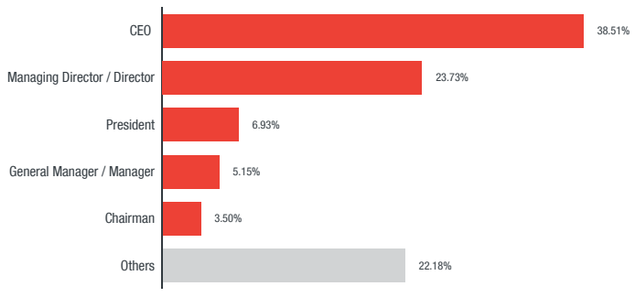


*Figure 4. CEO emerged as most spoofed (senders) by BEC scammers*

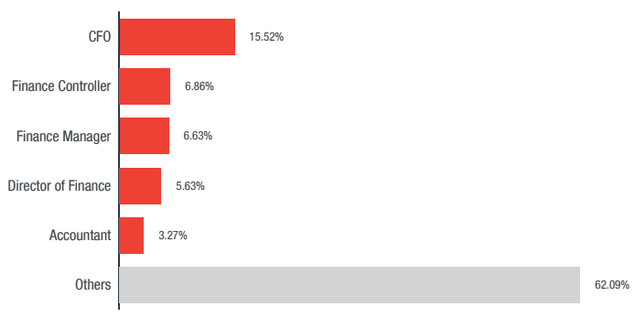


*Figure 5. CFO remained the most targeted position by BEC scammers*

The global risk of automated attacks increased in 2017, as cybercriminals used IoT botnets to gain huge cryptocurrency profits. Before 2017 drew to a close, the value of 1 bitcoin reached an all-time high at close to US$20,000.[6] This drew not just the attention of interested investors but also profiteering cybercriminals. Cryptocurrency holders and even platforms fell prey to various attacks across platforms (mobile devices and apps, social media, etc.).[7]


*Figure 6. Various cryptocurrency attack methods*

With the profitability offered by cryptocurrencies, it was not surprising then that 2017's IoT botnets trailed their sights on mining instead of causing distributed denial-of-service (DDoS) disruptions.

These criminal shifts in tactics and platforms are not new but highlight their collective ability to pivot and monetize activities in various ways. The dynamic nature of these threats require CISOs and their teams to be highly vigilant of changes and be prepared to adapt quickly.

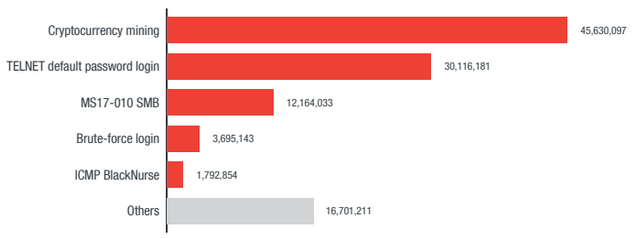


*Figure 7. Cryptocurrency mining and TELNET events outnumbered others*

Even with shifts to digital extortion within the criminal underground, the traditional data breach still remains a major risk to companies and organizations worldwide. Companies, regardless of size, continued to suffer from breaches led by Yahoo whose 3-billion user base faced the risk of personally identifiable information (PII) theft.[8]

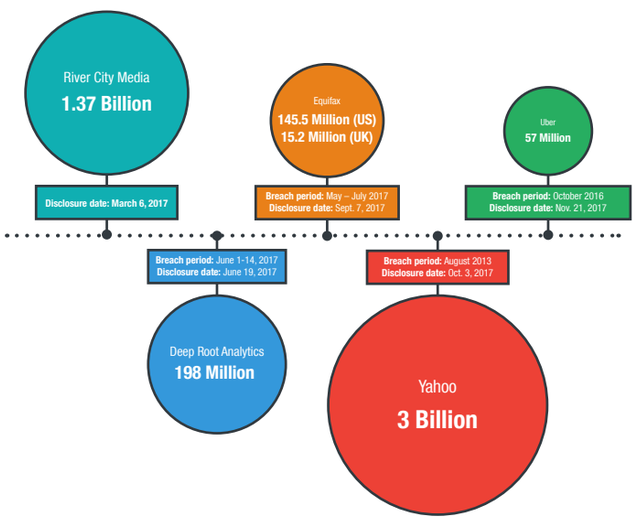


*Figure 8. Biggest data breaches disclosed in 2017*

What seemed insignificant caused massive disruptions and what were seen as diminishing actually evolved to become more targeted and destructive. In 2017, the real world stood witness to the paradox of cyberthreats.

## Paradigm Shifts in 2018

In 2018, we expect the ransomware business model to remain a cybercrime mainstay as other forms of digital extortion gain more ground. The success that massively destructive ransomware campaigns gained will inspire threat actors to gain even greater profits from victims.

On the traditional threat front, BEC scams are expected to cause businesses worldwide to incur as much as US$9 billion in losses.

Machine learning and blockchain technologies, meanwhile, are

bound to be abused by threat actors to better evade detection.

An increasing number of vulnerabilities in new IoT/industrial IoT (IIoT) devices will be exploited to disrupt normal business operations and consequently affect companies' bottom line.[9]

As technologies evolve and improve, so will the threats and risks that will affect them.

## What Enterprises Can Do

Given the wide range of threats we expect to face, enterprises would benefit most by minimizing risks across the network. Better visibility and connected, multilayered security defense are critical.

To combat current and emerging threats, enterprises can employ security solutions that allow visibility across the network and provide real-time detection and protection against vulnerabilities and attacks. Potential intrusions and compromise can be avoided with a dynamic security strategy that employs cross-generational techniques to address any and all 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.

Encouraging employees to always keep security in mind, not just for the company's but also their personal protection, will also help. Remind them to keep these best practices in mind:

- **Change default passwords.** Use unique and complex passwords for smart devices, especially routers, to significantly reduce the possibility of device hacking.
- **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 vulnerability exploitation.
- **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.

**References:**


1. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
2. https://www.cbsnews.com/news/cyberattack-wannacry-ransomware-north-korea-hackers-lazarus-group/
3. https://blog.trendmicro.com/petya-expands-its-scope-a-global-ransomware-threat/
4. https://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/
5. https://pdf.ic3.gov/2016_IC3Report.pdf
6. https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited/
7. http://www.bbc.com/news/technology-42409815;
   https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/;
   https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/;
   https://blog.trendmicro.com/trendlabs-security-intelligence/new-retadup-variants-hit-south-america-turn-cryptocurrency-mining/;
   https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coinhive-miner-the-6th-most-common-malware;
   https://blog.trendmicro.com/trendlabs-security-intelligence/eitest-campaign-uses-tech-support-scams-deliver-coinhives-monero-miner/
8. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/yahoo-all-three-billion-user-accounts-affected-in-2013-data-breach
9. https://www.trendmicro.com/vinfo/ph/security/research-and-analysis/predictions/2018