Trend Micro '2016 Security Roundup' reveals 752% increase in Ransomware

81 billion cyber threats blocked, an increase of 56%

DUBAI: Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, yesterday released its annual security roundup report, "2016 Security Roundup: A Record Year for Enterprise Threats," which proves 2016 was truly the year of online extortion. Cyber threats reached an all-time high in 2016, with ransomware and Business Email Compromise (BEC) scams gaining increased popularity among cybercriminals looking to extort enterprises. A 752 percent increase in new ransomware families ultimately resulted in $1 billion in losses for enterprises worldwide.

Trend Micro and the Zero Day Initiative (ZDI) discovered 765 vulnerabilities in 2016. Of these, 678 were brought to ZDI through their bug bounty program, then ZDI verifies and discloses the issue to the affected vendor. Compared to vulnerabilities discovered by Trend Micro and ZDI in 2015, Apple saw a 145 percent increase in vulnerabilities, while Microsoft bugs decreased by 47 percent. Additionally, the use of new vulnerabilities in exploit kits dropped by 71 percent, which is partially due to the arrest of the threat actors behind Angler that took place in June 2016.

"As threats, have diversified and grown in sophistication, cybercriminals have moved on from primarily targeting individuals to focusing on where the money is: enterprises," said Ed Cabrera, chief cybersecurity officer for Trend Micro. "Throughout 2016 we witnessed threat actors extort companies and organizations for the sake of profitability and we don't anticipate this trend slowing down. This research aims to educate enterprises on the threat tactics actively being used to compromise their data, and help companies adopt strategies to stay one step ahead and protect against potential attacks."

In 2016, the Trend Micro Smart Protection Network(tm) blocked more than 81 billion threats for the entire year, which is a 56 percent increase from 2015. In the second half of 2016, more than 3,000 attacks per second were blocked for customers. During this time, 75 billion of blocked attempts were email based, illustrating that email remains the top entry point for threats. Report highlights include:

Growth of Ransomware

Throughout the course of 12 months, the number of ransomware families grew from 29 to 247. One leading factor to explain this increase is the profitability of ransomware. Although individuals and organizations are encouraged not to pay the ransom, cybercriminals still managed to rake in roughly $1 billion last year. BEC Scams on the Rise - Much like ransomware, BEC scams proved to be incredibly lucrative for cybercriminals, resulting in an average of $140,000 in losses for companies around the globe. These scams also highlighted the effectiveness of social engineering techniques for threat actors targeting enterprises.

Variety of Vulnerabilities

Trend Micro and the Zero Day Initiative (ZDI) discovered a record high number of vulnerabilities in 2016, most of which were found in Adobe Acrobat Reader DC and Advantech's WebAccess. Both applications are widely used throughout enterprise and Supervisory Control and Data Acquisition (SCADA) systems. Angler Exploit's Exit - Following the arrest of 50 cybercriminals, the once dominant Angler exploit kit slowly faded out of the spotlight until it ceased to exist. While it didn't take long for new exploit kits to burst onto the scene in Angler's absence, by the end of 2016, the amount of vulnerabilities included in exploit kits had decreased by 71 percent.

Trojans and ATM Malware

Cybercriminals have been using ATM malware, skimming cards and banking Trojans for a while now. However, the attacks have diversified in recent years, giving threat actors access to personally identifiable information (PII) and credentials, which can also be used to gain a foothold inside enterprise networks. Mirai's Massive Attack - In October 2016, attackers took advantage of poorly secured IoT devices to issue a distributed denial-of-service (DDoS) attack that hijacked approximately 100,000 IoT devices and forced websites such as Twitter, Reddit and Spotify to go offline for several hours.

Yahoo's History Making

Yahoo experienced the largest data breach in history in August 2013, compromising 1 billion account users' information. However, the incident was not disclosed until three months after reports of a separate data breach in September 2016, which involved 500 million more accounts. These events stirred up the responsible disclosure conversation and the accountability companies have to their customers regarding the security of user data.

LONDON: Photo shows London landmarks, including the BT Tower and the London Eye on the skyline in London. British telecoms giant BT Group has agreed to legally separate its broadband unit Openreach to remedy concerns over competition in the sector, the company announced yesterday. — AFP

Financial institutions under pressure to ramp up security

DUBAI: Financial institutions are under pressure to ramp up security, with trends such as the increased take-up of mobile banking putting banks' IT infrastructure defenses at growing risk of cyber-attack. Increasingly, customers are playing an important role in highlighting security incidents, with a quarter (24%) of financial institutions saying that some of the threats they faced in 2016 were identified and reported to them by a customer.

According to the Financial Institutions Security Risks research from Kaspersky Lab and B2B International, security investment is a high priority for banks and financial institutions. Suffering from attacks both on their own infrastructure and on their customers, retail banks spend three times as much on IT security as comparably sized non-financial institutions. Moreover, 64% of banks admit that they will invest in improving their IT security regardless of the return-on-investment, in order to meet the growing demands of government regulators, top management and even their customers.

Despite banks putting serious efforts and budgets into safeguarding their perimeters against known and unknown cyber-threats, protecting the breadth of IT infrastructure that now exists - from traditional to specialized, ATMs and Point-of-Sale terminals - has proved difficult. The vast and ever-changing threat landscape, coupled with the challenge of improving the security habits of customers, has provided fraudsters with ever more points of vulnerability to exploit.

Emerging Risks

Emerging risks related to mobile banking are highlighted in the report as a trend that can expose banks to new cyberthreats. 42% of banks predict that an overwhelming majority of their customers will use mobile banking within three years, but admit that users are too careless in their online behavior. The majority of the banks surveyed admitted (46%) that their customers are frequently under attack from phishing attempts, with 70% of banks also reporting financial fraud incidents as a result, leading to monetary loss.

Rising phishing and social engineering attacks on customers have seen banks reassess their security efforts in this area. 61% of respondents see improving the security of apps and websites that their customers use as one of their main security priorities, closely followed by the implementation of more complex authentication and verification of log-in details (a key priority for 52%). Although they are vulnerable to the phishing tricks and tools that target their customers, banks are still more concerned about another 'old enemy' - targeted attacks. And they've got good reasons to be worried - targeted attack methods are becoming more common-place, with malware-as-a-service platforms even being used to harm financial organizations.

Persistent Threats

Experience of real incidents shows us that investments into security in the financial industry are well worth it in most cases -financial institutions report significantly fewer security events than companies of the same size in other industries- with the only exception of targeted attacks and malware. The detection of abnormal, potentially malicious activity, combining legitimate tools with fileless malware, requires a combination of advanced anti-targeted solutions and extended security intelligence. Still, 59% of financial firms are yet to embrace third-party threat intelligence.

Types of general security event experienced: Malware and targeted attacks are the only incidents that banking organizations experience more than their peers in other industries. Sharing threat intelligence would help banks to identify new and emerging threats quickly, an important point for them to note, considering the low levels of concern banks have about some of their most vulnerable devices, such as ATMs. Sharing more third party intelligence, in this respect, could help banks prepare for threats that they may not otherwise expect.

ATM Protection

Banks show comparatively low levels of concern about the threat of financial loss due to attacks on ATMs, despite being highly vulnerable to attacks of this nature. Only 19% of banks are concerned with attacks on ATM and cash withdrawal machines, despite the growing rate of malware targeting this part of a banks' infrastructure (in the 2016 threats review we've reported a 20% growth in ATM malware compared to 2015).