Trend Micro Survey Finds Ransomware Threatens Businesses in Egypt

28 percent of business leaders do not have incident response plans in case of infection and there is no recognition of the threat's magnitude

CAIRO, 31st October 2017

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, conducted a survey in partnership with Enterprise, the daily e-news round-up of economics, business and most important news, which was designed to uncover the magnitude of the ransomware threat in Egypt. The survey was aimed at top business leaders, a quarter of the survey respondents were c- suite executives, while about 30 percent were either IT Directors or staff, and 2 percent were dedicated internet security specialists.

The survey examined whether companies are being targeted by ransomware and if they have the right expertise and security systems necessary to protect themselves from such threats. According to the survey results, 81percent believed that ransomware is a real threat to their business, and 41percent are unsure or unaware about the interworking of ransomware.

Of those attacked, 30 percent were attacked by WannaCry, and 4 percent by both WannaCry and Petya. These two ransomware variants are more modern types that emerged in 2017, and are collectively categorized as crypto-ransomware. They operate by encrypting certain file types on infected systems and forcing users to pay the ransom through anonymous online payment methods in exchange for a decryption key.

According to Trend Micro's mid-year security round up, these types of ransomware crippled an unprecedented number of computers from across the globe – nearly 300,000 machines from WannaCry alone. More than a billion email accounts had been leaked from the database of the spam operator River City Media, which was just one of a handful of high-profile stories from 2017.

Commenting on this global threat is Noura Hassan, Egypt's Country Manager for Trend Micro, "We conducted this survey to understand the Egyptian business community's stance regarding ransomware. During the first half of 2017, business email compromise (BEC) was still one of the top threats enterprises are facing. According to a document published by the Federal Bureau of Investigation in the USA in May, global losses attributed to BEC scams since 2013 have reached US$5.3 billion."

A large majority of the survey respondents (91 percent) who were infected with ransomware stated that they did not pay the ransomware requested and are unaware whether their employers had opted to abide by the payments or not. However, 28 percent are unprepared with a response plan in case of ransomware infection.

Based on the survey results, businesses are advised to understand the real threats that come along with being insufficiently prepared for an attack. The results also revealed that 48 percent of respondents do not have a program to educate employees on the hazards of phishing attacks. Businesses advised to include readily available information to their employees on how to deal with these attacks to better safeguard all of our information online.

“The rise of hacking or malware as the primary breach method may be attributed to attackers finding more entry points into enterprise networks. The consequences of ill protection and knowledge of these ransomware attacks are extremely destructive and can result in: data theft, drawn-out downtimes, violations of worker and customer safety, among others,” Noura Hassan added.

According to Trend Micro’s report released in October 2017 discussing the Middle Eastern and North African cyber underground community, evidence reveals that the regional market place is not as profit driven in comparison to Russia or China. However, the “spirit of sharing” is one of the most apparent forces behind distribution of crime ware in the region. The regional marketplaces are also flooded with do-it-yourself kits that provide resources enabling beginners to launch their own cybercriminal business.

“A common practice among its players is to readily hand out codes, malware, and instruction manuals for free. Crypters, typically used to obfuscate malware, as well as SQL injection tools, keyloggers, and basic malware builders, are given away—a reflection of the culture within the regions’ underground scene” Noura Hassan stated.

The products and services that have become cybercriminal staples across the world are also available in the Middle East and North African underground. Products include credit card dumps, online accounts, credentials, and malware. Stolen identities are available in bundles that include passport scans and copies of driver’s license and local utility bills.

“The regions’ underground somewhat resembles France’s in terms of how members are authenticated. Seeing and buying most of the wares on display require registration. In many Turkish forums, for instance, viewing links and posts requires an account. Registration has a vetting process, entails joining fee paid in Bitcoin, and even a language barrier—most of the underground sites are in Arabic, but many of its members also post in English, and occasionally, French,” Hassan added.

As part of its commitment to increasing awareness and understanding of ransomware threats for businesses in Egypt, Trend Micro recommends a strong backup strategy, a patch management process and using anti-malware software. Turning on automatic updates is also a safeguard from ransomware, as well as disconnecting all external hard drives and devices after use. Attackers use online platforms such as Google, Facebook and others to trick users into downloading ransomware, clicking links or opening emails from unknown sources are another method for inviting ransomware. If a device has been infected there are prime steps to taken, including: Alerting an IT specialist, powering off the device as fast as possible and removing the laptop from the docking station while disconnecting all cables and Wi-Fi.

About Trend Micro
Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

For more information contact:

Mai Yousrey
01016994491
mai.yousery@publicistinc.com