Cyber Espionage Tops the List as Most Serious Threat Concern to Global Businesses in 2017

Rise in nation-state and ransomware attacks seen as increasing risk to national critical infrastructure, according to new research from Trend Micro

DALLAS--(BUSINESS WIRE)--Latest research from Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, reveals that 20 percent of global organizations rank cyber espionage as the most serious threat to their business, with a quarter (26 percent) struggling to keep up with the rapidly evolving threat landscape. In addition, one in five (20 percent) U.S. organizations have suffered a cyber espionage-related attack in the last year.

The research, which surveyed 2,402 enterprise IT decision makers across Europe and the U.S., shows cyber espionage topping the list of largest security concerns for 2017, followed by targeted attacks (17 percent) and phishing (16 percent). Businesses in Italy (36 percent), France (24 percent), Germany (20 percent) and Netherlands (17 percent) topped the list for regions who fear cyber espionage the most, which is notable in light of their respective elections taking place this year across Europe.

Raimund Genes, chief technology officer for Trend Micro, said, “The data shows fears over foreign government interference in democratic processes are now very real, as we saw with accusations over Russian involvement in the U.S. presidential elections. As general elections occur around the world, we see cyber propaganda becoming the norm this year, and the repercussions will be felt within businesses as they struggle to protect themselves from potentially disastrous cyber breaches.”

Eight out of 10 countries cited the increasing unpredictability of cyber criminals (36 percent overall) as one of the three biggest challenges to protecting against cyber threats. A further 29 percent flagged a lack of understanding of latest threats and a quarter (26 percent) are struggling to keep up with the rapidly evolving landscape and increasing sophistication of cybercriminal activity.

“As more of our critical data is being moved online, nation states are now targeting businesses to obtain this data and businesses are struggling to keep up, which could also be placing critical infrastructure at risk,” said Genes. “Nation states are able to use far more sophisticated methods, enabling them to target institutions such as hospitals, utilities and traffic signals, with far more disastrous consequences.”

According to the research, almost two-thirds (64 percent) of businesses experienced a ‘known’ major cyber-attack in the past 12 months, with the average being four. Amongst this group, ransomware was by far the most common threat type, with 78 percent of respondents claiming to have been attacked at least once in the period. In fact, only 16 percent of those who had experienced an attack had not suffered a ransomware attack.

In line with Trend Micro’s security predictions for 2017, just 10 percent of organizations think ransomware will pose a threat in 2017, despite a 748 percent increase in ransomware attacks in 2016, resulting in $1 billion in losses for enterprises worldwide1. The number of ransomware families is predicted to grow by a further 25 percent in 20172, diversifying to devices such as mobile phones, IoT devices and Industrial IoT devices (IIoT).

“As the Internet and the real world intersect, hackers are increasingly infiltrating critical systems and infrastructure,” said Genes. “With the IIoT introducing risks to enterprises utilizing Industrial Control Systems, this has significant consequences. We saw this with the recent attack on Ukraine’s national grid leaving 225,000 homes without power, and research showing that traffic signalling systems are easily searchable online.”

Business Email Compromise (BEC) – also known as CEO fraud or “whaling” – was pegged as a threat by just 12 percent of respondents, indicating that businesses are underestimating the impact of these attacks. BEC scams are proving to be incredibly lucrative, resulting in an average of $140,000 in losses for global companies in 20163.

“There’s no silver bullet for cyber security; these threats are constantly evolving,” stressed Genes. “While many organizations will be wooed by exciting new security technologies, this Elastoplast approach means they will be quickly bypassed and become obsolete. The increasingly unpredictable tactics used by well-funded cybercriminals and the fast evolving threat landscape highlights the fundamental need for businesses to have a layered defense to greatly reduce the risk.”

As enterprises defend against the more than 500,000 new, unique threats created every day4, Trend Micro recommends that organizations consider a connected multi-layered security approach that centralizes visibility into and control over endpoint, network, web, email, cloud and physical and hybrid cloud servers to speed up time to protect, detect and respond. This should include smart capabilities that provide maximum protection such as intrusion prevention, behavioral analysis, exploit prevention, application control, anti-malware and content filtering, integrity monitoring, response and containment, machine learning and sandbox analysis. IT leaders should prioritize solutions that are optimized to work across a variety of environments to minimize the impact on IT.

Notes to editors

The survey of 2,402 ITDMs in the UK, U.S., France, Germany, Italy, Netherlands, Sweden, Norway, Austria and Switzerland was commissioned by Trend Micro and conducted by Opinium in February 2017.

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.

_____

1 Trend Micro 2016 Security Threat Report
2 Trend Micro 2017 Security Predictions: "The Next Tier," 2016
3 Trend Micro 2017 Security Predictions: "The Next Tier," 2016
4 Trend Micro Threat Research, 2016

Contact:

Trend Micro Incorporated
Jerrod Resweber, 972-499-6614
publicrelations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY
