Trend Micro Predicts More Sophisticated Attacks Will Dominate 2019

Cybercriminals adapt tactics to prey upon evolving corporate technology environments

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its 2019 predictions report, warning that attackers will increase the effectiveness of proven attack methods by adding more sophisticated elements to take advantage of the changing technology landscape. The report, *Mapping the Future: Dealing with Pervasive and Persistent Threats*, highlights the growing threats faced by consumers and organizations that are exacerbated by the increasingly connected world.

“As we head into 2019, organizations must understand the security implications of greater cloud adoption, converging IT and OT, and increasing remote working,” said Greg Young, vice president of cybersecurity for Trend Micro. “Cybercriminals will continue to follow a winning formula – exploiting existing flaws, social engineering and stolen credentials – to drive profits. As both the corporate attack surface and unknown cyber threats increase, it’s more important than ever for organizations to put more resources behind employee education to help protect against these growing attacks.”

The role of social engineering in successful attacks against businesses and individuals will continue to increase throughout the year. Since 2015, the number of phishing URLs blocked by Trend Micro has increased by nearly 3,800 percent. This offsets the lessening reliance on exploit kits, which has decreased by 98 percent in the same time. Additionally, attackers will continue to rely on known vulnerabilities that remain unpatched in corporate networks for 99.99 percent of exploits, as this remains a successful tactic.

Trend Micro also predicts attackers will leverage these proven methods against growing cloud adoption. More vulnerabilities will be found in cloud infrastructure, such as containers, and weak cloud security measures will allow greater exploitation of accounts for cryptocurrency mining. This will lead to more damaging breaches due to misconfigured systems.

Attackers will also implement emerging technologies like AI to better anticipate the movements of executives. This will lead to more convincing targeted phishing messages, which can be critical to BEC attacks. Additionally, it is likely that BEC attacks will target more employees who report to C-level executives, resulting in continued global losses.

SIM swapping and SIM-jacking will be a growing threat to take advantage of remote employees and everyday users. This attack method allows criminals to hijack a cell phone without the user’s knowledge, making it difficult for consumers to regain control of their devices. Additionally, the smart home will be an increasingly attractive target for attacks that leverage home routers and connected devices.

To find out more on these and many more 2019 predictions, read the full report here.

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 6,000 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.

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:

https://newsroom.trendmicro.com/2018-12-11-Trend-Micro-Predicts-More-Sophisticated-Attacks-Will-Dominate-2019