# Trend Micro Finds Shifting Threats Require Businesses to Rethink Security Priorities

**2018 roundup report reveals substantial growth in phishing, cryptocurrency mining and BEC**

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its 2018 Security Roundup Report, which depicts a threat landscape that has evolved heavily through both approach and tactics. One shift in attacks that businesses should be aware of is the rapid growth of cryptocurrency mining, which increased 237 percent in the same time. Overall, attacks that capitalize on the human desire to respond to urgent requests from authority are on the rise, such as Business Email Compromise (BEC) and phishing, with phishing URL detections having increased an incredible 269 percent compared to 2017.

“The changes across the threat landscape in 2018 reflect a change in cybercriminal’s mindset,” said Jon Clay, director of global threat communications for Trend Micro. “Today’s most prevalent attacks are targeted and well planned, as opposed to one-size-fits-all attacks of the past. Knowing this pattern, we’re developing products that can outsmart these attack methods and allow us to be one step ahead of the bad guys.”

The number of BEC attacks in 2018 increased by 28 percent. While these attacks are less frequent than phishing attacks, they are more sophisticated and take more careful planning for cybercriminals and they yield an average of $132,000 per attack. As these attacks contain no malware and go undetected by traditional security measures, companies need to increase their protection against these attacks with smart solutions that analyze the email writing style of key executives in order to identify whether the email may be fraudulent. Trend Micro’s Writing Style DNA does exactly that and effectively helps detect Business Email Compromise (BEC) attacks.

Another area of change across the threat landscape in 2018 was seen in zero-day vulnerabilities. Trend Micro’s Zero Day Initiative (ZDI) bought and disclosed more vulnerabilities in 2018 than ever before, including 224 percent more Industrial Control System bugs. This is particularly significant for organizations that struggle to implement patches across their systems. While zero-day exploits are less and less common, known vulnerabilities were used to execute the largest attacks in 2018. These tactics rely on vulnerabilities that have had patches available for months, even years, yet remain exposed in corporate networks.

Another strong indicator of how the threat landscape is shifting can be seen in the types of threats that decline. Ransomware detections decreased by 91 percent compared to 2017, along with a 32 percent decrease in new ransomware families. This reinforces the shift in attack tactics, as ransomware does not require extensive planning, technical skills or ingenuity due to the large number of resources available for malicious hackers in the cybercriminal underground.

Trend Micro’s ongoing research and most advanced threat intelligence influences future product enhancements to ensure customers remain a step ahead of malicious actors.

To find out more on the key developments in the 2018 threat landscape, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unraveling-the-tangle-of-old-and-new-threats.

**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:
TMICY

---

https://newsroom.trendmicro.com/2019-02-26-Trend-Micro-Finds-Shifting-Threats-Require-Businesses-to-Rethink-Security-Priorities