Trend Micro Report Reveals Mounting Cloud Email Threats to Office 365 Require Second Layer of Defense

Cloud App Security report highlights the dangers of relying solely on built-in email security

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced that its Cloud App Security tool blocked nearly nine million high-risk email threats in 2018 as attackers continued to evolve their tactics, highlighting the importance of investing in multi-layered protection for online platforms like Office 365.

The findings from Trend Micro's Cloud App Security report detail how escalating email threat levels are exposing organizations to an increased risk of fraud, spying, information theft, and spoofing. As email remains a staple communication and collaboration tool globally, it is convenient for cybercriminals to leverage this integral, trusted platform for compromising attacks.

"Organizations are increasingly looking to cloud email services to boost productivity and agility, but the Cloud App Security report reveals that—from credential phishing to business email compromise (BEC) and the use of unusual file types—hackers are employing a variety of new tactics to evade built-in controls, making it critical to invest in a second layer of defense," said Kevin Simzer, chief operating officer at Trend Micro.

As the report reveals, email remains one of the most popular threat vectors. In total, the solution detected and blocked nearly 9 million high-risk email threats in 2018. This number was even after Cloud App Security was used as a second filter for emails that passed through Office 365. A Trend Micro customers' detection result is available in the report.

This underscores that sophisticated, multi-layered security is imperative for cloud-based email security as part of the shared responsibility model.

Simzer continued, "Microsoft is a valued partner of ours and by no means the only provider targeted by these evolving tactics. While its internal controls are a great starting point, organizations must take shared responsibility for security in the cloud. Think of third-party email protection as the tires of your favorite car — an essential add-on."

To improve the tool's detection rates even further, Trend Micro has added new capabilities that combine Computer Vision and Artificial Intelligence technology to "see" fake websites. This additional technique is applied to suspected phishing emails after filtering based on sender, content, and URL reputation.

The new capabilities sit alongside other Trend Micro email security features. These strategic offerings include AI-powered Writing Style DNA to combat BEC attacks, machine learning-based detection of suspicious email content, sandbox malware analysis, document exploit detection, and file, email, and web reputation technologies. Cloud App Security also leverages the power of the Trend Micro Smart Protection Network, which blocked more than 41 billion email threats in 2018.

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 workloads, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With more than 6,000 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

Contact:

Kateri Daniels
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704

JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2019-03-04-Trend-Micro-Report-Reveals-Mounting-Cloud-Email-Threats-to-Office-365-Require-Second-Layer-of-Defense