Cloud-based email protection saw a rise in BEC, phishing and email-borne malware

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its 2019 Cloud App Security Roundup report. The report highlights changes in messaging-specific threats detected last year, the use of more sophisticated malware, and the potential abuse of emerging technologies in artificial intelligence to inform future business protection strategies.

In 2019, Trend Micro blocked 12.7 million high-risk email threats for customers leveraging cloud-based email services from Microsoft and Google. This second layer of defense caught threats beyond those detected by the cloud email services' built-in security.

"Organizations are leveraging the power of SaaS-based applications in greater numbers to drive productivity, cost savings and growth. However, in doing so they may be opening themselves up to risk if they only rely on built-in security," said Wendy Moore, vice president, product marketing at Trend Micro. "As our report shows, built in security is not enough on its own to stop today's cybercriminals. Businesses must take ownership of cloud protection and find a multi-layered third-party solution to enhance their platform's native security functionality."

More than 11 million of the high-risk emails blocked in 2019 were phishing related, making up 89% of all blocked emails. Of these, Trend Micro detected 35% more credential phishing attempts than in 2018. Additionally, the number of unknown phishing links in such attacks jumped from just 9% of the total to more than 44% in 2019. This may demonstrate that scammers are registering new sites to avoid detection.

The report also shows that criminals are getting better at tricking the first layer of defense against Business Email Compromise (BEC) attacks, which typically look at attacker behaviors and intention analysis of the email content. The percentage of BEC attacks caught by AI-powered authorship analysis increased from 7% in 2018 to 21% in 2019.

Emerging phishing techniques outlined in the report include the increasing use of HTTPS and targeting Office 365 administrator accounts. This enables malicious hackers to hijack all connected accounts on the targeted domain and use them to send malware, launch convincing BEC attacks and more. To this end, Trend Micro blocked nearly 400,000 attempted BEC attacks, which is 271% more than in 2018.

In the face of such threats, Trend Micro recommends the organizations take the following mitigation steps:

- Move away from a single gateway to a multi-layered cloud app security solution
- Consider sandbox malware analysis, document exploit detection, and file, email, and web reputation technologies to detect malware hidden in Office 365 and PDF documents
- Enforce consistent data loss prevention (DLP) policies across cloud email and collaboration apps
- Choose a security partner that can offer seamless integration into their cloud platforms, preserving user and admin functions
- Develop comprehensive end user awareness and training programs

The report's findings were based on data generated by Trend Micro Cloud App Security™, an API-based solution that protects a range of cloud-based applications and services, including Microsoft® Office 365™ Exchange™ Online, OneDrive® for Business, SharePoint® Online, Gmail, and Google Drive.

To find out more, please read the complete report here: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

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 secures your connected world. For more information, visit www.trendmicro.com.

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009
OTC Pink:
TMICY

---

https://newsroom.trendmicro.com/2020-03-10-Trend-Micro-Blocked-13-Million-High-Risk-Email-Threats-in-2019