Trend Micro Report Reveals 265% Growth in Fileless Events

Threats in 2019 bring the ultimate test of defenses by evading traditional security

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today published its roundup report for the first half of 2019, revealing a surge in fileless attacks designed to disguise malicious activity. Detections of this threat alone were up 265% compared to the first half of 2018.

The findings in 2019 so far confirm many of thepredictions Trend Micro made last year. Namely, attackers are working smarter to target businesses and environments that will produce the greatest return on investment.

“Sophistication and stealth are the name of the cybersecurity game today as corporate technology and criminal attacks become more connected and smarter,” said Jon Clay, director of global threat communications for Trend Micro. “From attackers, we saw intentional, targeted, and crafty attacks that stealthily take advantage of people, processes and technology. However, on the business side, digital transformation and cloud migrations are expanding and evolving the corporate attack surface. To navigate this evolution, businesses need a technology partner that can combine human expertise with advanced security technologies to better detect, correlate, respond to, and remediate threats.”

Along with the growth in fileless threats in the first half of the year, attackers are increasingly deploying threats that aren’t visible to traditional security filters, as they can be executed in a system’s memory, reside in the registry, or abuse legitimate tools. Exploit kits have also made a comeback, with a 136% increase compared to the same time in 2018.

Cryptomining malware remained the most detected threat in the first half of 2019, with attackers increasingly deploying these threats on servers and in cloud environments. Substantiating another prediction, the number of routers involved in possible inbound attacks jumped 64% compared to the first half of 2018, with more Mirai variants searching for exposed devices.

Additionally, digital extortion schemes soared by 319% from the second half of 2018, which aligns with previous projections. Business email compromise (BEC) remains a major threat, with detections jumping 52% compared to the past six months. Ransomware-related files, emails and URLs also grew 77% over the same period.

In total, Trend Micro blocked more than 26.8 billion threats in the first half of 2019, over 6 billion more than the same period last year. Of note, 91% of these threats entered the corporate network via email. Mitigating these advanced threats requires smart defense-in-depth that can correlate data from across gateways, networks, servers and endpoints to best identify and stop attacks.

To read the complete report, *Evasive Threats, Pervasive Effects: 2019 Midyear Security Roundup*, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/evasive-threats-pervasive-effects.

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
NQB:
TMICY

https://newsroom.trendmicro.com/2019-08-27-Trend-Micro-Report-Reveals-265-Growth-in-Fileless-Events