Trend Micro Q3 Security Roundup Report Showcases Vulnerabilities and Aftermath of Data Breaches

Cracks in the mobile ecosystem, Internet-connected devices and network infrastructure are highlighted

DALLAS--(BUSINESS WIRE)--The interconnectivity of technology has led to a point where many devices are potentially vulnerable, and in the third quarter, the real world impacts of cyberattacks became clear. Trend Micro Incorporated (TYO: 4704; TSE: 4704) today announced its security roundup report, "Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks," which analyzes the vulnerabilities and repercussions of attacks seen last quarter. The report unravels the aftermath of security breaches, loopholes found in mobile platforms and exploits posing risks not only to user privacy, but also to physical safety. Additionally, these security gaps serve as a prelude to potentially massive events that Trend Micro believes will greatly impact 2016.

"The evolution of breaches is beginning to take a turn toward real-world effects on enterprises' bottom lines and people's lives," said Raimund Genes, CTO, Trend Micro. "The emergence of numerous vulnerabilities and other data breaches that occurred in this quarter are bound to release more confidential and potentially destructive information to the public, which could then be sold to the highest bidder on the Deep Web."

Data breaches experienced last quarter, such as Ashley Madison, spurred a chain of attacks, in which dumping stolen confidential information in public domains tarnishes victims' reputations, causing far greater damage than simple business disruptions. Cybercriminals, who leveraged the compromised information to launch extortion attacks and blackmail users, caused catastrophe for both Avid Life Media, the site owner, and more than 30 million Ashley Madison users – with reports of victim suicides in response to the impact this attack had on their personal lives.

Additionally, security breaches impacting the healthcare industry were prevalent in the third quarter, including the attack on the UCLA Health System where personal records of approximately 4.5 million patients were compromised. In fact, health and personally identifiable information (PII) was the second-most stolen data type out of all data breach categories. These instances reinforce why the healthcare industry continues to be an appealing target for cybercriminals.

Attackers are continuing to set their sights on mobile device users, taking advantage of gaps in security that exist on the iOS and Android platforms. The discovery of vulnerabilities in Android highlighted the need for a more integrated set of security strategies, while modified versions of app creation tools debunked the notion that the iOS walled garden approach to security can spare the platform from attacks.

"As Trend Micro analysts have observed, cyberspace has become more punitive and attacks are no longer isolated," said Tom Kellermann, chief cybersecurity officer, Trend Micro. "To mitigate future breaches and reduce risk, enterprises must focus on intrusion suppression and address the advent of secondary infections. Integrating breach detection systems with intrusion prevention systems is fundamental to decreasing the time hackers dwell on their networks. Organizations should expect to be hit, and preparing to overcome this challenge will become the mantra in the winter of 2016."

The following are a few report findings, highlighting third quarter activities:

- **Data breach dumps were used to fuel further attacks and extortion.** The successful attacks against The Hacking Team and Ashley Madison greatly affected the security and computing industries.
- **Discovery of weak points in mobile platforms emphasize existing problems in both ecosystems.** In response to the recent spate of Android vulnerability discoveries, Google finally announced regular security updates for the platform.
- **Cybercriminals use the "shotgun approach" on PoS malware, primarily affecting small businesses.** Attacks seen in the third quarter involved PoS malware launched through "old" techniques like spamming, as well as tools like macro malware, exploit kits and botnets.
- **Political personalities surface as targets of ongoing espionage campaigns.** Analysis of recent data revealed that Pawn Storm has expanded its targets from mostly U.S. targets to Russian entities.
- **Angler Exploit Kit continues to be a widely-used tool, with access numbers increasing by 34 percent.** Angler Exploit Kit creators updated their arsenal this past quarter, which resulted in attackers using their creation to distribute new malware.
- **New research raises issues on the security of Internet-ready devices.** Attackers are now modifying target-tank information, which could have dire consequences for the general public.

For the complete report, please visit: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/vulnerabilities-prelude-impending-attacks

About Trend Micro

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Built on more than 26 years of experience, our solutions for consumers, businesses and governments provide layered data

Built on more than 26 years of experience, our solutions for consumers, businesses and governments provide layered data security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by more than 1,200 threat experts around the globe. For more information, visit TrendMicro.com.

Contact:

Trend Micro Incorporated
Thomas Moore, 972-499-6648
thomas_moore@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2015-11-17-Trend-Micro-Q3-Security-Roundup-Report-Showcases-Vulnerabilities-and-Aftermath-of-Data-Breaches