Trend Micro 2015 Security Roundup Details Top Breaches, Vulnerabilities and Cyber Underground

DALLAS--(BUSINESS WIRE)--Today, Trend Micro Incorporated (TYO: 4704; TSE: 4704) released its annual security roundup report, "Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies," which dissects the most significant security incidents from 2015. The research confirms attackers are now bolder, smarter and more daring in attack vectors, cyberespionage efforts and cyber underground activity on a global basis.

"Our observations for 2015 have confirmed that traditional methods of protecting data and assets are no longer sufficient and should be reassessed to maintain the highest level of corporate and personal security," said Raimund Genes, CTO, Trend Micro. "The prevalence and sophistication of extortion, cyberespionage and expanding targeted attacks now dictate that organizational security strategies must be prepared to defend against a potentially greater onslaught in 2016. This realization can help the security community better anticipate and respond to what attackers are trying to accomplish."

Online extortion and cyberattacks were a top concern in 2015, with several high-profile organizations being victimized. Ashley Madison, Hacking Team, the Office of Personnel Management and Anthem were a few of these high-profile attacks that left millions of employees and customers exposed. The healthcare industry witnessed its share of data breaches. Between Anthem and Premera Blue Cross, more than 90 million customers' personal and sensitive data was exposed.

Additional report highlights include:

- **Pawn Storm and Zero-Days –** In 2015 there were 11 zero-days discovered by Trend Micro researchers in addition to the long-running cyberespionage campaign Pawn Storm, which utilized several zero-day exploits to target high-profile organizations, including a U.S. defense organization, the armed forces of a NATO country and several foreign affairs ministries.
- **Deep Web and Underground Explorations** – In 2015, cybercriminal markets began to penetrate the recesses of the Deep Web. Each underground market mirrors the culture in which it resides, offering specific wares most profitable in each region.
- **Smart Technology Nightmares** – Attacks against connected devices accelerated in 2015, proving their susceptibility. Smart cars and businesses, seen in Trend Micro's GasPot experiment, were among a few of the new concerns brought by IoT technologies.
- **Angler, the 'King of Exploit Kits' –** From malvertising to Adobe Flash, Angler Exploit Kit gained notoriety in 2015 as the most used exploit. Accounting for 57.3 percent of overall exploit kit usage. Japan, the U.S. and Australia were among the most impacted countries for this attack.
- **Data Held Hostage –** Crypto-ransomware rose to 83 percent of overall ransomware use in 2015. Cryptowall was the most frequently used variant, arriving on users' computers via email or malicious downloads.
- **Takedowns versus DRIDEX –** The seizure and takedown of the notorious DRIDEX botnet contributed to a significant decrease in detections within the U.S. However, this led to a resurgence due to the Command and Control infrastructure being hosted on a bulletproof hosting provider, making it virtually impossible to eradicate altogether.

For the complete report, please visit: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/setting-the-stage-landscape-shifts-dictate-future-threat-response-strategies

About Trend Micro

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Built on 27 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/2016-03-08-Trend-Micro-2015-Security-Roundup-Details-Top-Breaches-Vulnerabilities-and-Cyber-Underground