Trend Micro Q1 2015 Roundup Finds New Variations on Proven Attack Methods

Healthcare, iOS, Adobe, PoS targeted by malware, zero-day exploits

DALLAS--(BUSINESS WIRE)--A combination of newer and older threat variations defined the cybersecurity landscape in the first quarter of 2015. Malvertising, zero-day vulnerability exploitation, "old-school" macro malware and the decade-old FREAK vulnerability are just a few of the highlights in Trend Micro Incorporated's (TYO: 4704; TSE: 4704) new report, "Bad Ads and Zero-Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices." From an industry perspective, healthcare and retail point-of-sale systems have also seen an uptick in threat activity. The report reinforces how complacency can present major cybersecurity risks in an era where the margin for error has been significantly diminished.

"Even though we are early in the year, it is clear 2015 is shaping up to be noteworthy in terms of volume, ingenuity and sophistication of attacks," said Raimund Genes, CTO, Trend Micro. "The rise in attacks against the healthcare industry, combined with the rise in malvertisements, reflects that technology users are being assailed from all angles. It is clear businesses and individuals alike need to be proactive in protecting against threats. As a business, how would your IT-Security policies look like in a Zero Trust Environment? An aggressive and different security posture is critical to keep financial, personal and intellectual property safe."

Adware also topped the list of mobile threats, with Trend Micro now documenting more than five million Android threats to date — nearing the predicted total of eight million by the close of 2015. In fact, top malicious and high-risk apps blocked by Trend Micro were adware related, reflecting this increase.

Trend Micro researchers also found zero-day exploits targeting Adobe software utilized malvertisements and no longer required victims to visit or interact with malicious sites to become infected.

The healthcare industry experienced a notable rise in cyber-attacks, in addition to iOS™ and point-of-sale (PoS) systems continuing to be targeted. Since exploitations in these areas have been in their infancy for several years, researchers believe this rise is primarily due to a lack of preparedness—a sizable oversight that should be addressed.

"The question we have to ask is, 'are we doing enough to protect ourselves from security threats?'" added Genes. "While we need to constantly update our systems to protect against new attacks, the first quarter of 2015 clearly showed we need to also watch out for older threats, and how no industry or system should feel exempt."

Report highlights include:

- **Healthcare Industry Hit by Massive Attacks:** Major healthcare service providers, such as Premera Blue Cross and Anthem, suffered data breaches that exposed millions of customers' financial and medical data.
- **Old Threats Invigorated with New Targeted Attack Tools, Tactics and Procedures:** Rocket Kitten and those behind Operation Pawn Storm set their sights on new targets, proving that targeted attacks are evolving.
- **Exploit Kits Grew in Sophistication:** Exploit kits constantly add new exploits to their arsenals, adding to their allure to expert and novice attackers.
- **Crypto-Ransomware Volume Soared, Expands to Enterprises:** Crypto-ransomware expanded their target base to enterprise users, no longer exclusively pursuing consumers.
- **Macro Malware, Old but Still Effective:** The resurgence of macro malware suggest cybercriminals are taking advantage of user security complacency, through reliance on Microsoft Office® defaults.
- **Decade-Old FREAK Security Flaw Brought on Patch Management Challenges:** As more vulnerabilities emerge in open source OSs and applications, IT administrators will find it increasingly

difficult to mitigate risks.

For the complete report, please visit: http://www.trendmicro.com/vinfo/us/security/roundup/.

A blog post regarding the report can be viewed here: http://blog.trendmicro.com/1q-2015-security-roundup/.

About Trend Micro

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Built on 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
Thomas Moore, 972-499-6648
thomas_moore@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009

---

https://newsroom.trendmicro.com/2015-05-19-Trend-Micro-Q1-2015-Roundup-Finds-New-Variations-on-Proven-Attack-Methods