Trend Micro Q2 2015 Roundup Finds New Threats to Public Sectors

Public utilities, government attacks and targeted threats dominate the quarter

DALLAS--(BUSINESS WIRE)--The second quarter of 2015 was wrought with high profile vulnerabilities and hacks. Cybercriminals became more inventive in their attack methods to infiltrate and abuse existing technologies that are often overlooked. These developments are analyzed in the Trend Micro Incorporated (TYO: 4704; TSE: 4704) Q2 security roundup report released today, "A Rising Tide: New Hacks Threaten Public Technologies." It details the evolution of tools and methods attackers use to get the greatest return on every cybercrime investment.

"In the second quarter, we saw a shift in the threat landscape with cyber criminals becoming more sophisticated and creative, amplifying existing methods of attack, and using them in new ways," said Raimund Genes, CTO, Trend Micro. "The ethereal outlook on the threat of cybercrime can no longer be held by the general population. This quarter demonstrated that the potential damage caused by cyber attacks extends far beyond a simple software bug to hacks of airplanes, smart cars and television stations."

Hackers are taking more strategic approaches, refining their approach and targeting more selective victims to improve their infection rates. This is reflected by the exponential increase in the use of several traditional attack methods, including a 50 percent increase in the integration of the Angler exploit kit, a 67 percent growth in overall exploit kit-related threats, and CryptoWall ransomware becoming highly targeted, with 79 percent of infections occurring in the U.S.

Additionally, government entities have realized the full impact of cyberattacks during the second quarter with massive data breaches on both the Internal Revenue Service (IRS) in May and the U.S. Office of Personnel Management (OPM) system in June. The OPM data breach was the largest of its kind to date, exposing personally identifiable information of approximately 21 million individuals. Other government agencies were impacted by targeted campaigns using macro malware, new command and control (C&C) servers, and the continued use of newly exploited vulnerabilities and 0-days Pawn Storm.

When looking at the Q2 threat landscape as a whole, the U.S. is a major player in both deploying and receiving various attacks, with malicious links, spam, C&C servers and ransomware are all having a major presence.

Report highlights include:

- **Hacks causing disruptions to public utilities**
  Broadcast networks, airplanes, automated vehicular systems and home routers pose not only the risk of malware infections, but physical inconveniences and threats.
- **Lone wolf cybercriminals gain notoriety via successful ransomware and PoS attacks**
  FighterPoS and MalumPoS deployed by solo hackers "Lordfenix" and "Frapstar," along with Hawkeye keylogger attacks, demonstrated that single individuals are capable of making a significant impact in today's threat marketplace.
- **Government entities fight back against cybercrime**
  Interpol, Europol, the Department of Homeland Security and the FBI all played a role in taking down longstanding botnet operations. Additionally, the indictment of Silk Road founder Ross Ulbricht brought to light the nebulous nature and dangers of the Dark Web.
- **National and political impacts were made by attacks on government organizations**
  The attack on OPM was a shocking realization that no one's personal data is safe. Macro malware, island-hopping and C&C servers were among the tactics used to target government data in this and similar breaches.
- **Public-facing websites and mobile devices were threatened in new ways**
  While threats to software are always present, vulnerabilities in Web apps were proven to be just as dangerous. Attackers will leverage any vulnerability available and custom applications need custom security attention to ensure those entry points are eliminated.

For the complete report, please visit: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-rising-tide-new-hacks-threaten-public-technologies.

A blog post regarding the report can also be viewed here: http://blog.trendmicro.com/a-rising-tide-new-hacks-threaten-public-technologies/.

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

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2015-08-18-Trend-Micro-Q2-2015-Roundup-Finds-New-Threats-to-Public-Sectors