New IBM X-Force Study Finds Leading Financial Malware Spread Globally in 2016

The U.S. and the U.K. Experienced the Most Financial Malware Attacks in 2016, Japan Sees International Malware Infiltrate Its Borders

CAMBRIDGE, Mass., March 31, 2017 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced new research from IBM X-Force, revealing that cybercriminals scaled their most successful financial malware tools globally in 2016. The leading malware tool Zeus and its variants Neverquest and Gozi, kept their global rankings as the top three malware from the previous year, as cybercriminals retooled them to operate in new countries and regions.

The report, "The Shifting Panorama of Global Financial Cybercrime," leverages data from the nearly 300 million protected endpoints across the globe monitored by IBM Trusteer and IBM X-Force. The report reveals top financial malware in countries including: The United States, the United Kingdom, Canada, Japan, New Zealand, Australia, Brazil, Germany, Asia, and the United Arab Emirates.

IBM X-Force found that cybercriminals expanded their reach into new regions by establishing networks and partnerships with local crime factions. These new relationships gave them access to new target email lists, an understanding of local banking credential requirements, and regional money laundering operations. For example, the cybercriminals operating TrickBot, which emerged in August 2016, launched the malware during a testing and development period to turned it into a banking Trojan and worked out the bugs before its actual deployment in the U.K. and other English-speaking countries. It then promptly moved to Germany.

"The level of cooperation between organized crime rings marks a significant shift in strategy," said Limor Kessem, Executive Security Advisor, IBM Security. "While the sharing of tools and services was common in forums on the dark web, this deeper collaboration outside that environment demonstrates that to scale globally, deeper cooperation between criminals is required."

Financial-focused cybercrime proved to be worth the investment of resources for cybercriminals in 2016. According to the recent 2017 IBM X-Force Threat Intelligence Index, IBM X-Force revealed that the Financial Services industry experienced a resurgence with cybercriminals as it became the most targeted industry by cyberattacks in 2016 after dropping to third in 2015. Interestingly, while Financial Services was targeted the most by cyber-attacks last year, data from the X-Force report shows it was only third in compromised records.

Geographic Trends and Malware Crosses Borders

While the U.S. and the U.K. were the most targeted with financial malware attacks in 2016, some new markets began to emerge as targets of cybercriminals. For example, Japan which historically remained isolated from cybercrime due to a lack of local tools and its complex language, saw new malware families target the country. The leading financial malware targeting Japan included Gozi, URLZone, and Shifu, which are operated by well-known Eastern European cybercrime gangs. Their presence in the region marked an evolution of the fraud infrastructure in Japan.

Brazil also saw itself in the sights of cybercriminals globally in 2016 as the country hosted the 2016 Summer Olympics. Notably, the Zeus Trojan was not often seen in Brazil until 2016 due to a lack of local technical skills required to operate the advanced botnet operation needed to deploy the malware. Zeus's code was the basis of three commercial malware iterations, Zeus Panda, FlokiBot, and Zeus Sphinx, which were adapted to target Brazilian banks and payment platforms.

To learn more about the financial malware landscape and its global evolution in 2016, download the IBM X-Force report "The Shifting Panorama of Global Financial Cybercrime" at http://ibm.co/2oiWi5N.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligenceblog.

Contact:

Kelly Kane
IBM Security, External Relations
413-297-2668
kkane@us.ibm.com

SOURCE IBM