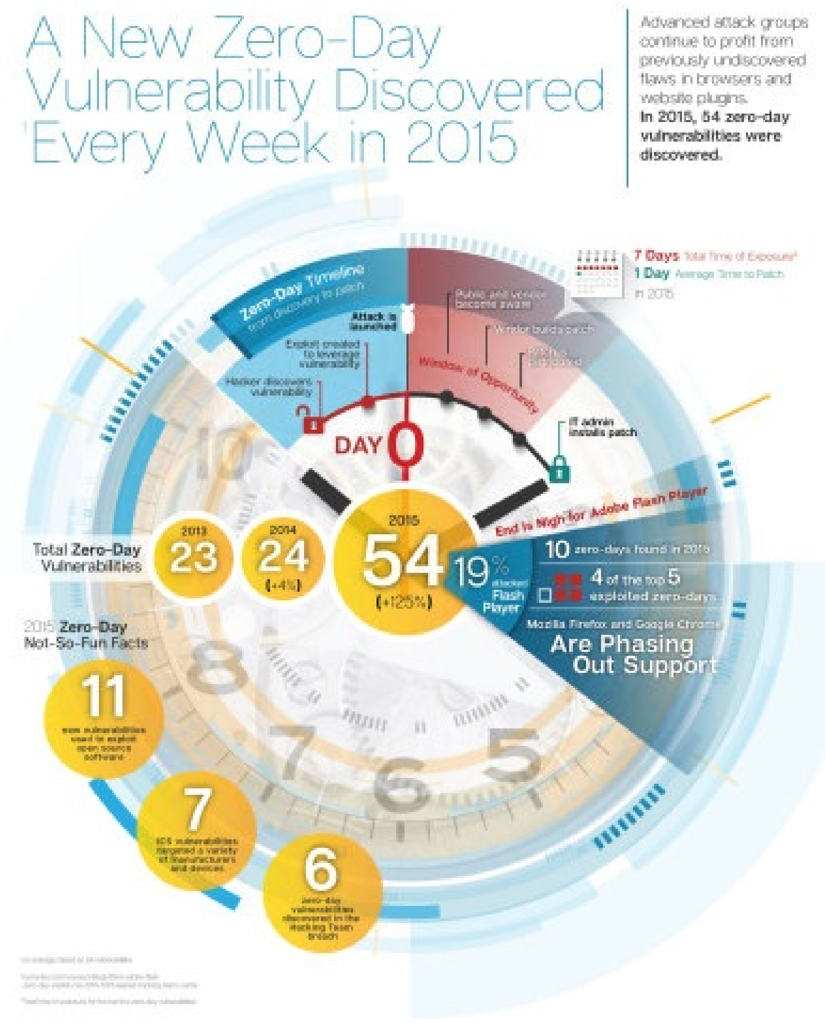
One New Zero-Day Discovered on Average Every Week in 2015, Twice the Rate of a Year Ago as Advanced Attackers Exploit, Stockpile and Resell High-Value Vulnerabilities
Tuesday, April 12, 2016 04:01:00 AM (GMT)

- Symantec Report Reveals a Record Nine Mega-Breaches;
- Half a Billion Personal Records Stolen or Lost in 2015;
- Crypto-ransomware Attacks Grew by 35 Percent

Symantec's (Nasdaq:SYMC) Internet Security Threat Report (ISTR), Volume 21, reveals an organizational shift by cybercriminals: They are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. This new class of professional cybercriminal spans the entire ecosystem of attackers, extending the reach of enterprise and consumer threats and fueling the growth of online crime.

This Smart News Release features multimedia. View the full release here:
http://www.businesswire.com/news/home/20160411006340/en/



2016 Internet Security Threat Report, Symantec (Graphic: Symantec)

"Advanced criminal attack groups now echo the skill sets of nation-state attackers. They have extensive resources and a highly-skilled technical staff that operate with such efficiency that they maintain normal business hours and even take the weekends and holidays off," said Kevin Haley, director, Symantec Security Response. "We are even seeing low-level criminal attackers create call center operations to increase the impact of their scams."

Advanced professional attack groups are the first to leverage zero-day vulnerabilities, using them for their own advantage or selling them to lower-level criminals on the open market where they are quickly commoditized. In 2015, the number of zero-day vulnerabilities discovered more than doubled to a record-breaking 54, a 125 percent increase from the year before, reaffirming the critical role they play in lucrative targeted attacks. Meanwhile, malware increased at a staggering rate with 430 million new malware variants discovered in 2015. The sheer volume of malware proves that professional cybercriminals are leveraging their vast resources in attempt to overwhelm defenses and enter corporate networks.

Over Half a Billion Personal Records Stolen or Lost in 2015

Data breaches continue to impact the enterprise. In fact, large businesses that are targeted for attack will on average be targeted three more times within the year. Additionally, we saw the largest data breach ever publicly reported last year with 191 million records compromised in a single incident. There were also a record-setting total of nine reported mega-breaches. While 429 million identities were exposed, the number of companies that chose not to report the number of records lost jumped by 85 percent. A conservative estimate by Symantec of those unreported breaches pushes the real number of records lost to more than half a billion.

“The increasing number of companies choosing to hold back critical details after a breach is a disturbing trend,” said Haley. “Transparency is critical to security. By hiding the full impact of an attack, it becomes more difficult to assess the risk and improve your security posture to prevent future attacks.”

Encryption Now Used as a Cybercriminal Weapon to Hold Companies’ and Individuals’ Critical Data Hostage

Ransomware also continued to evolve in 2015, with the more damaging style of crypto-ransomware attacks growing by 35 percent. This more aggressive crypto-ransomware attack encrypts all of a victim’s digital content and holds it hostage until a ransom is paid. This year, ransomware spread beyond PCs to smartphones, Mac and Linux systems, with attackers increasingly seeking any network-connected device that could be held hostage for profit, indicating that the enterprise is the next target.

Don’t Call Us, We’ll Call You: Cyber Scammers Now Make You Call Them to Hand Over Your Cash

As people conduct more of their lives online, attackers are increasingly focused on using the intersection of the physical and digital world to their advantage. In 2015, Symantec saw a resurgence of many tried-and-true scams. Cybercriminals revisited fake technical support scams, which saw a 200 percent increase last year. The difference now is that scammers send fake warning messages to devices like smartphones, driving users to attacker-run call centers in order to dupe them into buying useless services.

From the Experts: Security Tips and Tricks

As attackers evolve, there are many steps businesses and consumers can take to protect themselves. As a starting point, Symantec recommends the following best practices:

For Businesses:

- **Don’t get caught flat-footed:** Use advanced threat and adversary intelligence solutions to help you find indicators of compromise and respond faster to incidents.
- **Employ a strong security posture:** Implement multi-layered endpoint security, network security, encryption, strong authentication and reputation-based technologies. Partner with a managed security service provider to extend your IT team.
- **Prepare for the worst:** Incident management ensures your security framework is optimized, measureable and repeatable, and that lessons learned improve your security posture. Consider adding a retainer with a third-party expert to help manage crises.
- **Provide ongoing education and training:** Establish simulation-based training for all employees as well guidelines and procedures for protecting sensitive data on personal and corporate devices. Regularly assess internal investigation teams—and run practice drills—to ensure you have the skills necessary to effectively combat cyber threats.

For Consumers:

- **Use strong passwords:** Use strong and unique passwords for your accounts. Change your passwords every three months and never reuse your passwords. Additionally, consider using a password manager to further protect your information.
- **Think before you click:** Opening the wrong attachment can introduce malware to your system. Never view, open, or copy email attachments unless you are expecting the email and trust the sender.
- **Protect yourself:** An ounce of protection is worth a pound of cure. Use an internet security solution that includes antivirus, firewalls, browser protection and proven protection from online threats.

- **Be wary of scareware tactics:** Versions of software that claim to be free, cracked or pirated can expose you to malware. Social engineering and ransomware attacks will attempt to trick you into thinking your computer is infected and get you to buy useless software or pay money directly to have it removed.
- **Safeguard your personal data:** The information you share online puts you at risk for social engineered attacks. Limit the amount of personal information you share on social networks and online, including login information, birth dates and pet names.

Symantec will host a webinar on this year's ISTR results on **Tuesday, May 3, at 9:00 a.m. PT.** For more information or to register, please go here.

About the Internet Security Threat Report

The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from Symantec's Global Intelligence Network, which Symantec analysts use to identify, analyze and provide commentary on emerging trends in attacks, malicious code activity, phishing, and spam.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

NOTE TO U.S. EDITORS: If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at http://www.symantec.com/news. All prices noted are in U.S. dollars and are valid only in the United States.

View source version on businesswire.com: http://www.businesswire.com/news/home/20160411006340/en/

--30-- CP/SF

Contact:

Symantec
Mara Mort, 650-527-7455
Mara_Mort@symantec.com
or
Edelman for Symantec
Jenn Foss, 503-471-6804
Jenn_Foss@edelman.com

Industries: Women, Technology, Consumer Electronics, Data Management, Internet, Networks, Software, Telecommunications, Security, Mobile/Wireless, Consumer, Family, Men
Languages: English

Primary Identifiers: NLOK-US
Related Identifiers: NLOK-US, US871503108
Source: Symantec Corporation
Subjects: Survey, Photo/Multimedia, Webcast