ISTR

Internet Security Threat Report

One Page Summary

Volume 21, Published April 2016

Symantec

The 2016 Internet Security Threat Report (ISTR) provides an overview and analysis of the year in global threat activity. It is compiled using data from the Symantec™ Global Intelligence Network, which our global cybersecurity experts use to identify, analyze, and provide commentary on emerging trends in the threat landscape.

KEY FINDINGS

Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36 percent from the year before. Remarkably, these numbers no longer surprise us. Attacks against businesses and nations hit the headlines with such regularity that we've become numb to the sheer volume and acceleration of cyber threats. The 2016 ISTR covers a wide range of the 2015 cyber threat landscape, but some areas deserve special attention.

A New Zero-Day Vulnerability Discovered Each Week

Attackers profit from flaws in browsers and website plugins

In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125 percent increase from the year before. Or put another way, a new zero-day vulnerability was found every week (on average) in 2015. Given the value of these vulnerabilities, it's not surprising that a market has evolved to meet demand.

Half a Billion Personal Records Stolen or Lost

Companies aren't reporting the full extent breaches

In 2015, we saw a record-setting total of nine mega-breaches, and the reported number of exposed identities jumped to 429 million. But this number hides a bigger story. In 2015, more companies chose not to reveal the full extent of their data breaches. A conservative estimate of unreported breaches pushes the number of records lost to more than half a billion.

Vulnerabilities Found in Three Quarters of Websites

Web administrators still struggle to stay current on patches

There were over one million web attacks against people each day in 2015. Cybercriminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. Nearly 75 percent of all legitimate websites have unpatched vulnerabilities, putting us all at risk.

Spear-Phishing Campaigns Targeting Employees Increased 55 Percent

Cyber attackers are playing the long game

In 2015, large businesses targeted for attack once was most likely to be targeted again at least three more times throughout the year. All businesses of all sizes are potentially vulnerable to targeted attacks. In fact, spear-phishing campaigns targeting employees increased 55 percent in 2015. No business is without risk.

Ransomware Increased 35 Percent in 2015

Cyber criminals are using encryption as a weapon

An extremely profitable type of attack, ransomware will continue to ensnare PC users and expand to any network-connected device that can be held hostage for a profit. In 2015, ransomware found new targets in smart phones, Mac, and Linux systems. Symantec even demonstrated proof-of-concept attacks against smart watches and televisions in 2015.

100 Million Fake Technical Support Scams Blocked

Cyber scammers now make you call them

Fake technical support scams have evolved from cold-calling unsuspecting victims to the attacker fooling victims into calling them directly. Attackers trick people with pop-up error alerts, thus steering the victim to an 800 number where a "tech support rep" attempts to sell the victim worthless services. In 2015, Symantec blocked 100 million of these attacks.

LEARN MORE

For more information about the cyber threat landscape and the potential impact it has against you and your organization, download the 2016 Symantec Internet Security Threat Report at:

www.symantec.com/threatreport