Volume 20, Published April 2015

ISTR 20

2015 INTERNET SECURITY THREAT REPORT ONE PAGE SUMMARY

The 2015 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

If there is one thing that can be said about the threat landscape, and cybersecurity as a whole, it is that the only constant is change. This can clearly be seen in 2014: a year with far-reaching vulnerabilities, faster attacks, files held for ransom, and far more malicious code than in previous years. The 2015 ISTR covers a wide range of the 2014 cyber threat landscape, but some areas deserve special attention.

Cyberattackers Are Leapfrogging Defenses in Ways Companies Lack Insight to Anticipate

As organizations look to discover attackers using stolen employee credentials and identify signs of suspicious behavior throughout their networks, savvy attackers are using increased levels of deception and, in some cases, hijacking companies' own infrastructure and turning it against them. Symantec saw that advanced attackers targeted five out of six large companies in 2014, a 40 percent increase from the year before.

Attackers Are Moving Faster, Defenses Are Not

Within four hours of the Heartbleed vulnerability becoming public in 2014, Symantec saw a surge of attackers stepping up to exploit it. Reaction time has not increased at an equivalent pace. Advanced attackers continue to favor zero-day vulnerabilities to silently sneak onto victims' computers, and 2014 had an all-time high of 24 discovered zero days. Attackers jumped in to exploit these vulnerabilities much faster than vendors could create and roll out patches. In total, the top five zero-days of 2014 were actively exploited by attackers for a combined 295 days before patches were available.

Attackers Are Streamlining and Upgrading Their Techniques, While Companies Struggle to Fight Old Tactics

In 2014, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased eight percent overall. But attackers became more efficient, deploying 14 percent less email towards 20 percent fewer targets.

On top of this, 60 percent of all targeted attacks struck small- and medium-sized organizations. These organizations often have fewer resources to invest in security, and many are still not adopting basic best practices like blocking executable files and screensaver email attachments. This puts not only the businesses, but also their business partners, at higher risk.

Malware Used In Mass Attacks Increases and Adapts

While advanced targeted attacks may grab the headlines, non-targeted attacks still make up the majority of malware, which increased by 26 percent in 2014. In fact, there were more than 317 million new pieces of malware created in 2014, meaning nearly one million new threats were released into the wild each day. However, it's not just about quantity. Quality matters and malware authors have figured out ways to avoid detection, including by testing for virtual machines before executing their code. In 2014, up to 28 percent of all malware was "virtual machine aware." This should serve as a wake-up call to security researchers who are dependent on virtual sandboxing to observe and detect malware.

Learn More

For a more in-depth view of the cyber threat landscape, to understand how these changes affect you and your organization, and to learn how to best defend against these threats, download the 2015 Symantec Internet Security Threat Report at:
www.symantec.com/threatreport