ISTR

INTERNET SECURITY THREAT REPORT ONE PAGE SUMMARY ⌖ 2014

Symantec's Global Intelligence Network is made up of more than 41.5 million attack sensors and records thousands of events per second. It monitors threat activity in more than 157 countries and territories through a combination of Symantec products and services and other third-party data sources. This network gives our analysts unparalleled sources of data from which to identify and analyze the trends in Internet security threats. Each year we condense our security intelligence and knowledge into the Symantec Internet Security Threat Report (ISTR).

Key Findings

In 2013, much attention was focused on cyber-espionage, threats to privacy and the acts of malicious insiders. However, the end of 2013 provided a painful reminder that cyber-crime remains prevalent and that damaging threats from cyber-criminals continue to face businesses and consumers. The 2014 ISTR once again covers a wide range of the threat landscape, but some areas deserve special attention.

Targeted Attacks Grow and Evolve

The number of targeted attack campaigns increased by 91 percent in 2013. Symantec also found that the length of these campaigns was three times longer than campaigns in 2012. This year, Symantec introduced a new targeted attack calculation that uses epidemiology concepts commonly applied to public health issues that estimates the actual risk industries face of being targeted for attack. For example, while the most targeted attacks in 2013 were against governments and the services industry, the industries most at risk of being attacked were mining and manufacturing.

2013 was the Year of the Mega Data Breach

The total number of data breaches in 2013 was 62 percent higher than in 2012 with 253 total breaches. However, even a 62 percent increase does not truly reflect the scale of the breaches last year. 2013 was the year of the mega breach, with 8 of the data breaches exposing more than 10 million identities.

Ransomware Attacks Grew by 500 Percent in 2013 and Turned Vicious

Scammers continued to leverage profitable ransomware scams in which the attacker pretends to be law enforcement, demanding a fake fine of between $100 and $500. First seen in 2012, these threats escalated in 2013, growing by 500 percent. Symantec also saw a vicious evolution in ransomware in 2013 with the appearance of Ransomcrypt, commonly known as Cryptolocker, which encrypts a victim's files. This evolution can cause even more damage in businesses by encrypting network drives where critical business information may be stored.

Attackers are Turning to the Internet of Things

A wide variety of Internet-connected devices such as baby monitors, security cameras and routers were hacked in 2013. We also saw security researchers demonstrate attacks against smart televisions, automobiles and medical equipment. While the benefit to attackers of compromising these devices may not be immediately clear and there is still a lot of hype, the risk is real. Internet of Thing (IoT) devices will become access points for targeted attackers and become bots for cyber-criminals.

Learn More

These highlights offer just a glimpse into what Symantec observed throughout 2013. For a more in-depth view of the dynamic threat landscape, to understand how these changes affect you and your organization, and to learn how to best defend against these threats, download the 2014 Symantec Internet Security Threat Report, Volume 19 at: www.symantec.com/threatreport