Symantec Internet Security Threat Report (ISTR) April 2015 Executive Summary

If there is one thing that can be said about the threat landscape, and Internet security 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.

While 2013 was seen as the Year of the Mega Breach, 2014 had high-profile vulnerabilities grabbing the headlines. Data breaches are still a significant issue, since the number of breaches increased 23 percent and attackers were responsible for the majority of these breaches. However, attention shifted during the year from what was being exfiltrated to the way attackers could gain access.

Vulnerabilities have always been a big part of the security picture, where operating system and browser-related patches have been critical in keeping systems secure. However, the discovery of vulnerabilities such as Heartbleed, Shell Shock, and Poodle, and their wide-spread prevalence across a number of operating systems, brought the topic front and center. The conversation has shifted from discussing "threat X that exploits a vulnerability" to detailing how "vulnerability Y is used by these threats and in these attacks."

This is one of many constants that changed in 2014. Based on the data collected by the Symantec Intelligence Network and the analysis of our security experts, here are other trends of note in 2014.

Attackers Are Moving Faster, Defenses Are Not

Within four hours of the Heartbleed vulnerability becoming public, 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-day vulnerabilities. As we observed with Heartbleed, attackers moved in to exploit these vulnerabilities much faster than vendors could create and roll out patches. In 2014, it took 204 days, 22 days, and 53 days, for vendors to provide a patch for the top three most exploited zero-day vulnerabilities. By comparison, the average time for a patch to be issued in 2013 was only four

days. The most frightening part, however, is that the top five zero-days of 2014 were actively used 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. They notably used less effort than the previous year, deploying 14 percent less email towards 20 percent fewer targets. Attackers also perfected watering hole attacks, making each attack more selective by infecting legitimate websites, monitoring site visitors and targeting only the companies they wanted to attack.

Further complicating companies' ability to defend themselves was the appearance of "Trojanized" software updates. Attackers identified common software programs used by target organizations, hid their malware inside software updates for those programs, and then waited patiently for their targets to download and install that software—in effect, leading companies to infect themselves. Last year, 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.

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. In 2014, Symantec observed advanced attackers:

- Deploying legitimate software onto compromised computers to continue their attacks without risking discovery by anti-malware tools.
- Leveraging a company's management tools to move stolen IP around the corporate network.
- Using commonly available crimeware tools to disguise themselves and their true intention if discovered.
- Building custom attack software inside their victim's network, on the victim's own servers.
- Using stolen email accounts from one corporate victim to spear-phish their next corporate victim.
- Hiding inside software vendors' updates, in essence "Trojanizing" updates, to trick targeted companies into infecting themselves.

Given all of this stealthy activity, it's not surprising that Symantec Incident Response teams brought in to investigate one known breach to an organization discovered additional breaches still in progress. Almost no company, whether large or small, is immune. Five out of every six large companies (2,500+ employees) were targeted with spear-phishing attacks in 2014, a 40 percent increase over the previous year. Small- and medium-sized businesses also saw an uptick, with attacks increasing 26 percent and 30 percent, respectively.

Malware Used In Mass Attacks Increases and Adapts

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 last year, meaning nearly one million new threats were released into the wild each day. Some of this malware may not be a direct risk to organizations and is instead designed to extort end-users.

Beyond the annoyance factor to IT, however, it impacts employee productivity and diverts IT resources that could be better spent on high-level security issues. Malware authors have various tricks to avoid detection; one is to spot security researchers 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. It also makes clear that virtual environments do not provide any level of protection. Certain malware like W32.Crisis, upon detecting a virtual machine, will search for other virtual machine images and infect them.

Digital Extortion on the Rise: 45 Times More People Had Their Devices Held Hostage in 2014

While most people associate "extortion" with Hollywood films and mafia bosses, cybercriminals have used ransomware to turn extortion into a profitable enterprise, attacking big and small targets alike. Ransomware attacks grew 113 percent in 2014, driven by more than a 4,000 percent increase in crypto-ransomware attacks. Instead of pretending to be law enforcement seeking a fine for stolen content, as we've seen with traditional ransomware, crypto-ransomware holds a victim's files, photos and other digital media hostage without masking the attacker's intention. The victim will be offered a key to decrypt their files, but only after paying a ransom that can range from $300-$500—and that's no guarantee their files will be freed. In 2013, crypto-ransomware accounted for a negligible percentage of

all ransomware attacks (0.2 percent, or 1 in 500 instances). However, in 2014, crypto-ransomare was seen 45 times more frequently. While crypto-ransomware predominately attacks devices running Windows, Symantec has seen an increase in versions developed for other operating systems. Notably, the first piece of crypto-ransomware on mobile devices was observed on Android last year

Cybercriminals Are Leveraging Social Networks and Apps to Do Their Dirty Work

Email remains a significant attack vector for cybercriminals, but there is a clear movement toward social media platforms. In 2014, Symantec observed that 70 percent of social media scams were manually shared. These scams spread rapidly and are lucrative for cybercriminals because people are more likely to click something posted by a friend. Mobile was also ripe for attack, as many people only associate cyber threats with their PCs and neglect even basic security precautions on their smartphones. In 2014, Symantec found that 17 percent of all Android apps (nearly one million total) were actually malware in disguise. Additionally, grayware apps, which aren't malicious by design but do annoying and inadvertently harmful things like track user behavior, accounted for 36 percent of all mobile apps.

Internet of Things Is Not a New Problem, But an Ongoing One

Symantec continued to see attacks against Point of Sales systems, ATMs, and home routers in 2014. These are all network-connected devices with an embedded operating system, though they're not often considered part of the Internet of Things (IoT). Whether officially part of the IoT or not, attacks on these devices further demonstrate that it's no longer only our PCs at risk. And the potential for cyberattacks against cars and medical equipment should be a concern to all of us.

Risks to many IoT devices are exacerbated by the use of smartphones as a point of control. Symantec discovered that 52 percent of health apps—many of which connect to wearable devices—did not have so much as a privacy policy in place, and 20 percent sent personal information, logins, and passwords over the wire in clear text. Some of this may reflect the attitudes of end users. In a Norton survey, one in four admitted they did not know what they agreed to give access to on their phone when downloading an application. And 68 percent were willing to trade their privacy for nothing more than a free app.