Security

2016 | Dell Security Annual Threat Report

Executive Summary

Introduction

Breaches in 2015 succeeded not because the victims lacked security altogether, but because thieves found and exploited a small hole in their security program.

While every year brings new, high-profile data breaches, cybercriminals went especially big in 2015, elevating both the magnitude of data breached and the size of organizations targeted. Victims included large insurance companies; government institutions like the U.S. Office of Personnel Management (OPM); retailers including Walmart, CVS and Costco; and online businesses like the Ashley Madison dating site. And as in years past, these breaches succeeded not because the victims lacked security altogether, but because thieves found and exploited a small hole in their security program.

Whether through a third-party vendor, an infected laptop, social engineering or plain malware, hackers made the most of their opportunities in 2015. But each successful hack provides an opportunity for security professionals to learn from others' oversights. They arm us with new insights we can use to examine our own strategies and shore up holes in our own defense systems. That's why each year we present the most common attacks observed by the Dell SonicWALL Threat Research Team, while offering a glimpse into emergent threats for the coming year. Our goal is to help organizations of all sizes more effectively prevent attacks in 2016, both from known threats and those yet to emerge.

64 million unique malware samples

73 percent increase from 2014

In 2015, we blocked **2.17 trillion** IPS attacks and **8.19 billion** malware attacks. Moreover, we saw a 73 percent increase in unique malware samples compared with 2014, more than triple the number in 2013. It's clear that attackers are putting more effort each year into infiltrating organizational systems with malicious code.

Key findings include:

- Exploit kits evolved to stay one step ahead of security systems, with greater speed, heightened stealth and novel shapeshifting abilities.
- Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption continued to surge, leading to under-the-radar hacks affecting at least 900 million users in 2015.
- Malware for the Android ecosystem continued to rise compared to 2014, putting the lion's share of the smartphone market at risk.
- Malware attacks nearly doubled to 8.19 billion; popular malware families continued to morph from season to season and differed across geographic regions.

The data was gathered by the Dell SonicWALL Global Response Intelligence Defense (GRID) Network, which sources information from a number of devices and resources including:

- More than 1 million security sensors in nearly 200 countries and territories;
- Shared cross-vector threat-related information between security systems, including firewalls, email security, endpoint security, honeypots, content filtering systems and sandbox technology in Dell's threat centers;
- Dell SonicWALL proprietary malware analysis automation;
- Malware/IP reputation data from tens of thousands of firewalls and email security devices around the globe;
- Shared threat intelligence from more than 50 industry collaboration groups and research organizations;
- Intelligence from freelance security researchers; and
- Spam alerts from millions of computer users protected by Dell SonicWALL email security devices.

Threat findings from 2015

One of the best ways to predict and prepare for emergent threats is to analyze information about recent breaches. Dell's predictions and security recommendations for 2016 revolve around four key findings from 2015:

1 Exploit kits evolved to stay one step ahead of security systems, with greater speed, heightened stealth and novel shapeshifting abilities.

In 2015, exploit kit behavior continued to be dynamic, creating a rise in the number and types of kits available. The year's most active kits proved to be Angler, Nuclear, Magnitude and Rig. The sheer volume of exploit kits available gave attackers limitless opportunities to target the latest zero-day vulnerabilities, including those appearing in Adobe Flash, Adobe Reader and Microsoft Silverlight.

Dell SonicWALL noted a few key evolutions in 2015's exploit kits, including:

- **Use of anti-forensic mechanisms to evade security systems –** In September 2015, the Dell SonicWALL Threat Research Team discovered a major, unclassified exploit kit, which the team named Spartan. This kit effectively hid from security systems by encrypting its initial code and generating its exploitative code in memory, never writing to disk.
- **Upgrades in evasion techniques, such as URL pattern changes –** Dell SonicWALL observed the Nuclear exploit kit first using `search?q` as part of the URL for its landing page redirect campaign in September 2015. In October 2015, this URL segment changed to /`url?sa`, making it difficult for anti-virus software and firewalls to keep up. It was also common for kits to check for anti-virus software or virtual environments, such as VMware or VirtualBox, and to modify their code accordingly for higher success rates.
- **Changes to landing page redirection techniques –** Cybercriminals no longer necessarily use standard document.write or iframe redirection. In 2015, some of the larger attacks like

Magnitude used steganography, which involves concealing the file, message, image or video within another file, message, image or video.

- **Modifications in landing page entrapment techniques –** Some attacks directly called JavaScript's functions to determine the browser and plugins victims were using, rather than leveraging the entire JavaScript PluginDetect library in plain or obfuscated form.

2 Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption continued to surge, leading to under-the-radar hacks affecting at least 900 million users in 2015.

Using SSL/TLS encryption, or HTTPS traffic, skilled attackers can cipher command and control communications and malicious code to evade intrusion prevention systems (IPS) and anti-malware inspection systems. These attacks can be extremely effective, simply because most companies do not have the right infrastructure to detect them. Legacy network security solutions typically either don't have the ability to inspect SSL/TLS-encrypted traffic or their performance is so low that they become unusable when conducting the inspection.

Attackers took full advantage of this lack of visibility, coupled with the growth of HTTPS traffic throughout the year. In August 2015, an attack leveraged SSL/TLS encryption to disguise an infected advertisement on Yahoo, exposing as many as 900 million users to malware. This campaign redirected Yahoo visitors to a site that was infected by the Angler exploit kit.[i] An additional 10 million users were likely affected in the weeks prior by accessing ads placed by a marketing company called E-planning.[ii]

Dell SonicWALL noted an increase in the number of HTTPS connections, as well as geographical differences in its use:

- In the fourth quarter of 2015, HTTPS connections (SSL/TLS) made up an average of 64.6 percent of web connections, outpacing the growth of HTTP throughout most of the year.
- In January 2015, HTTPS connections were 109 percent higher than in the previous January. Furthermore, each month throughout 2015 saw an average of 53 percent increase over the corresponding month in 2014.
- On virtually opposite ends of the spectrum, HTTPS made up 81.6 percent of web connections in North Korea in 2015, while it made up only 34.4 percent in South Korea. China had by far the lowest HTTPS usage at only 8.63 percent of web connections.

3 Malware for the Android ecosystem continued to rise compared to 2014, putting the lion's share of the smartphone market at risk.

In 2015, Dell SonicWALL saw a wide range of new offensive and defensive techniques that attempted to increase the strength of attacks against the Android ecosystem.

Stagefright was, in theory, one of the most dangerous vulnerabilities ever discovered for Android. The vulnerability was embedded deeply in the Android operating system and affected all of the estimated 1 billion devices running Froyo 2.2 to Lollipop 5.1.1.[iii] Thankfully, Dell SonicWALL and other security organizations observed no infections from Stagefright before Google discovered and patched it.

Dell SonicWALL noted a few emerging trends among the attacks against Android devices in 2015:

- **Android-specific ransomware began to gain popularity throughout the year.** In September 2015, Dell SonicWALL observed a new ransomware variant that added a randomly generated PIN to the typical ransomware lock screen.

- **Android malware writers continued to find innovative ways to evade detection and analysis.** In 2015, they began shipping malicious code as part of a library file, rather than a classes file, which is more commonly scanned by anti-virus software. Taking this a step further, 2015 saw the rise of a new Android malware called AndroidTitanium that stored its malicious contents on a Unix library file in the lib folder as `libTitaniumCore.so.` This .so file was loaded as a native library by the classes from the `classes.dex` file. By simply referring to the content saved somewhere else, the malware kept the `classes.dex` file itself free of malicious content.
- **The financial sector continued to be a prime target for Android malware, with a number of malicious threats targeting banking apps on infected devices.** In November 2015, Dell SonicWALL discovered an Android campaign created to steal credit card and banking-related information from infected devices. Many of the malicious Android packages (APKs) in this campaign used the official Google Play Store as a conduit to trick victims into entering their credit card information. Some also monitored a few hardcoded apps, particularly financial apps, in order to steal login information. These malicious apps could also remotely execute commands received via SMS messages and transfer device-related data to the attackers.

4 Malware attacks nearly doubled to 8.19 billion; popular malware families continued to morph from season to season and differed across geographic regions.

In 2015 alone, Dell SonicWALL received 64 million unique malware samples, compared to 37 million in 2014. Moreover, the number of attack attempts almost doubled, from 4.2 billion in 2014 to 8.19 billion in 2015. This pervasive threat is wreaking havoc on the cyber world and causing significant damage to government agencies, organizations, companies and even individuals. Sometimes malware narrowly targets one population by design; sometimes it affects certain groups more heavily for external reasons.

The type of malware in circulation that Dell SonicWALL observed in 2015 varied widely across timeframes, countries and interest groups:

- **Long-lasting malware –** The Dyre Wolf corporate banking Trojan was one of the most active malware variants of the year. It came onto the scene in February of 2015 and remained somewhat active through December. By April, companies had already lost between $1.5 and $6.5 million to Dyre Wolf.[iv,v]Dyre Wolf enjoyed such a long lifespan for several reasons including its profitability (attractive to attackers), frequent binary code updates, sophisticated anti-detection techniques and ease of spreading.

  The combination of Dyre Wolf and Parite topped malware network traffic through 2015. Other long-lasting malware included TongJi, a widely used malicious JavaScript by multiple drive-by campaigns; Virut, a general cybercrime botnet active since at least 2006; and the resurgence of Conficker, a well-known computer worm targeting the Microsoft Windows operating system since 2008.[vi]
- **Geographically dominant malware –** There was a strong geographic correlation to the popularity of individual malware variants throughout 2015. One geographical attack that made its political intentions clear was the Upatre Trojan, which was dominant in Germany in June and July 2015. Upatre presented compromised users with an anti-drone message, urging victims to stand up to the U.S Government against the use of drones in war.[vii]

In October and November 2015, the Spartan exploit kit discovered by Dell SonicWALL was most highly concentrated in Russia. Meanwhile, the Windows XP malware CVE-2010-2568 was extremely popular in India, where the operating system is still in widespread use.

Key industry observations of 2015

In today's connected world, it's vital to maintain 360 degrees of vigilance. Your security program extends from your own software and systems, to employees' training and access, to everyone who accesses your network or data.

Other key vulnerabilities and attacks from 2015:

The Common Vulnerabilities and Exposures (CVE) system reported about **8,000 NEW VULNERABILITIES** and **more than 2/3** of them were related to **network attacks**

96 TRILLION hits for application traffic during the year, compared to **88 TRILLION** in 2014

ANGLER exploit kit was the **top exploit kit** used throughout the year, followed by **Nuclear, Magnitude and Rig**

SERVERS were the **number one attack target** in the category of intrusion attacks

We released **14 advisories** addressing **Microsoft security bulletins,** including **OUT-OF-BAND ZERO-DAY ATTACK ADVISORIES**

TOP 2 MICROSOFT ZERO-DAYS actively being used by popular exploit kits such as Angler: **Microsoft Windows OpenType Font Driver Remote Code Execution** and **Microsoft Internet Explorer Remote Memory Corruption Vulnerability**

The **XCODEGHOST** vulnerability arose from a malicious version of Xcode, Apple's official iOS and OS X app development tool affecting more than **500 MILLION** iOS users

Multiple well-known **zero-day vulnerabilities** were released, particularly for **ADOBE FLASH**

Predictions for 2016

Based on our 2015 observations and industry knowledge, we predict four trends to emerge in 2016:

1. The battle between HTTPS encryption and threat scanning will continue to rage, as companies fear performance trade-offs.
2. Many Flash zero-day viruses were discovered and exploited in 2015. However, this number will drop gradually because major browser vendors, such as Google and Mozilla, have stopped supporting Flash plugins.
3. Malicious threats will target Android Pay through the vulnerabilities of Near Field Communication (NFC). These attacks may leverage malicious Android apps and point-of-sale (POS) terminals, tools that are easy to acquire and manipulate for hackers.
4. In July 2015, Wired magazine reported that two hackers remotely gained control of a 2014 Jeep Cherokee.[viii] There are few cars currently equipped with Android Auto, but with time the number is expected to grow. We can expect malicious entities to invade this new frontier soon, possibly via ransomware (where the victim must pay to exit the vehicle) or even more dangerous intent.

Final takeaways

Once again in 2015, a massive number of breaches succeeded against organizations who thought they were doing everything right. The solution is for companies to approach security as an end-to-end problem. From the creation and storage of data to its consumption and every transit channel in between, if security is weak at any point, the whole system risks collapsing.

Picture a security program as one of architecture's most fundamentally stable shapes: the arch. If all the pieces of the arch are in place, it's an unshakeable structure, even gaining strength as it gains load. However, if one of the pieces of the arch is missing or flimsy, the arch will crumble under the slightest weight, no matter how strong the other bricks are.

For security professionals, that means examining your program from every angle, asking each of the following questions:

1. Do we have enough resources allocated to detect and prevent data breaches?

2. Do we have a dedicated security team to immediately respond to threats?

3. Do we have a complete set of compliance in place? For example, regular-based endpoint AV scans should be applied for individual employees.

4. Do our third-party vendors comply with the security standards?

While absolute perfection may be unattainable, striving for a near-perfect level of security across the board is the only way to avoid breaches like those experienced in 2015. That means it's up to IT leaders like you to create strong policies that extend to all departments of their organizations. It's equally imperative to communicate why those policies are important and to maintain oversight of their execution.

Be knowledgeable, be methodical, and finally, be a strong champion for end-to-end security in your organization. The best way to ensure your organization does not become a victim of data breaches is by learning from the mistakes of organizations that have.

As a global leader in network security, it is Dell's mission to help companies proactively protect their data from common and emergent threats. We hope this complete Dell Security Annual Threat Report empowers organizations of all sizes to become more prepared, informed, vigilant, and successful in preventing attacks throughout 2016. **Learn more**: Visit www.sonicwall.com.

The complete Dell Annual Threat Report is available online at
http://www.sonicwall.com/whitepaper/2016-dell-security-annual-threat-report8107907

Resources

[i] Joe Curtis, “Yahoo malvertising attack leaves 900 million at risk of ransomware,” IT Pro, August 4, 2015, http://www.itpro.co.uk/security/25094/yahoo-malvertising-attack-leaves-900-million-at-risk-of-ransomware

[ii] Jeremy Kirk, “Over 10 million web surfers possibly exposed to malvertising,” Network World, July 27, 2015, http://www.networkworld.com/article/2953453/over-10-million-web-surfers-possibly-exposed-to-malvertising.html

[iii] Kris Carlon, “New Stagefright security exploit puts a billion Android devices at risk,” AndroidPIT, October 2015, https://www.androidpit.com/what-is-stagefright-on-android-am-i-affected-and-what-can-i-do

[iv] John Kuhn, “The Dyre Wolf Campaign: Stealing Millions and Hungry for More,” Security Intelligence, April 2, 2015, https://securityintelligence.com/dyre-wolf/

[v] David Gilbert, “How Ryanair was hacked to see $5m stolen from its bank account,” International Business Times, April 30, 2015, http://www.ibtimes.co.uk/how-ryanair-was-hacked-see-5m-stolen-its-bank-accounts-1499206

[vi] “Virut,” Wikipedia, https://en.wikipedia.org/wiki/Virut

[vii] “Upatre used for political spam campaign,” Dell SonicWALL Security Center, March 19, 2015, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=797

[viii] Andy Greenberg, “Hackers remotely kill a Jeep on the highway – with me in it,” Wired, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/