Dell Security

2016 Dell Security Annual Threat Report

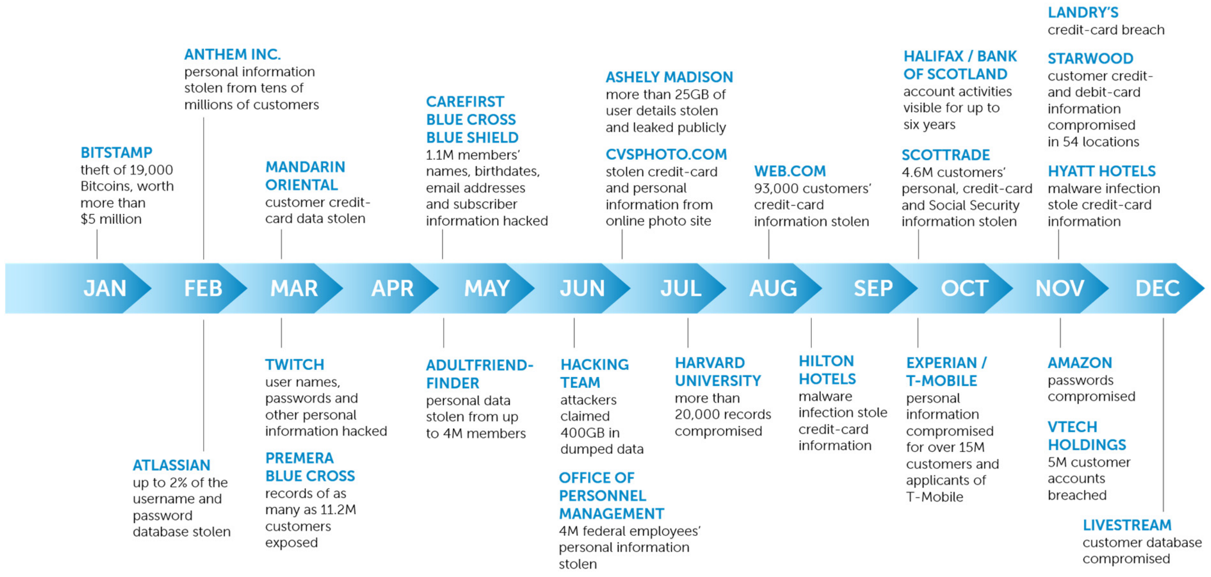
Table of Contents

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.

Fig 1: Timeline of high profile breaches in 2015


JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
BITSTAMP theft of 19,000 Bitcoins, worth more than $5 million
ANTHEM INC. personal information stolen from tens of millions of customers
ATLASSIAN up to 2% of the username and password database stolen
MANDARIN ORIENTAL customer credit-card data stolen
TWITCH user names, passwords and other personal information hacked
PREMERA BLUE CROSS records of as many as 11.2M customers exposed
CAREFIRST BLUE CROSS BLUE SHIELD 1.1M members' names, birthdates, email addresses and subscriber information hacked
ADULTFRIEND-FINDER personal data stolen from up to 4M members
HACKING TEAM attackers claimed 400GB in dumped data
OFFICE OF PERSONNEL MANAGEMENT 4M federal employees' personal information stolen
ASHELY MADISON more than 25GB of user details stolen and leaked publicly
CVSPHOTO.COM stolen credit-card and personal information from online photo site
HARVARD UNIVERSITY more than 20,000 records compromised
WEB.COM 93,000 customers' credit-card information stolen
HILTON HOTELS malware infection stole credit-card information
HALIFAX / BANK OF SCOTLAND account activities visible for up to six years
SCOTTRADE 4.6M customers' personal, credit-card and Social Security information stolen
EXPERIAN / T-MOBILE personal information compromised for over 15M customers and applicants of T-Mobile
LANDRY'S credit-card breach
STARWOOD customer credit- and debit-card information compromised in 54 locations
HYATT HOTELS malware infection stole credit-card information
AMAZON passwords compromised
VTECH HOLDINGS 5M customer accounts breached
LIVESTREAM customer database compromised

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.

Cybercriminals have great monetary incentive to constantly improve results while simultaneously improving efficiencies. At this intersection of high impact and low effort sits the exploit kit, a pre-packaged software system that can be used to infiltrate servers and automatically exploit vulnerabilities. Typically, these kits come pre-loaded to attack certain vulnerabilities, but can also be tweaked on the fly to exploit the newest weaknesses, often the same day they are discovered.

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.

Notable trends in exploit kits

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 exploit kit used malvertising tactics to load an Adobe Flash file on a victim's browser. This file downloaded an XML file containing another encrypted Flash file that contained yet a third file used to exploit the Flash Software vulnerability. Spartan effectively hid from security systems by encrypting its initial code and generating its exploitative code in memory, never writing to disk, where it could have been detected.
- **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. (Of course, once exploit components are known, conventional signatures can be written to detect them.) 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 used steganography, which involves concealing the file, message, image or video within another file, message, image or video. Specifically, the Magnitude exploit kit created an iframe from a specially crafted image file to redirect victims to its landing page.

- **Modifications in landing page entrapment techniques –** Cybercriminals used different techniques for spreading malware. For example, 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, as in the past.

Dell SonicWALL and the discovery of the Spartan exploit kit

In September 2015, while monitoring for exploits within the GRID network using an automated URL filtering and review process, the Dell SonicWALL Threat Team discovered a new exploit kit. This novel kit leveraged Adobe Flash vulnerability CVE-2015-5122 to infiltrate victims' systems. The team named the kit "Spartan" as its code displayed a function labeled "This is Sparta."

How it worked

1. Spartan used a URL redirection technique to fetch its landing page, which in turn loaded a Flash file.
2. This Flash file downloaded an XML file that contained another encrypted Flash file.
3. This second Flash contained another embedded Flash file (third Flash file), which finally exploited the Adobe Flash Software vulnerability.

Purpose

The goal of this exploit kit was likely to open the victim up to receiving further malware. Dell SonicWALL did not observe a payload in its environment. However, exploit kits often exist to distribute password stealers, ransomware and other infections.

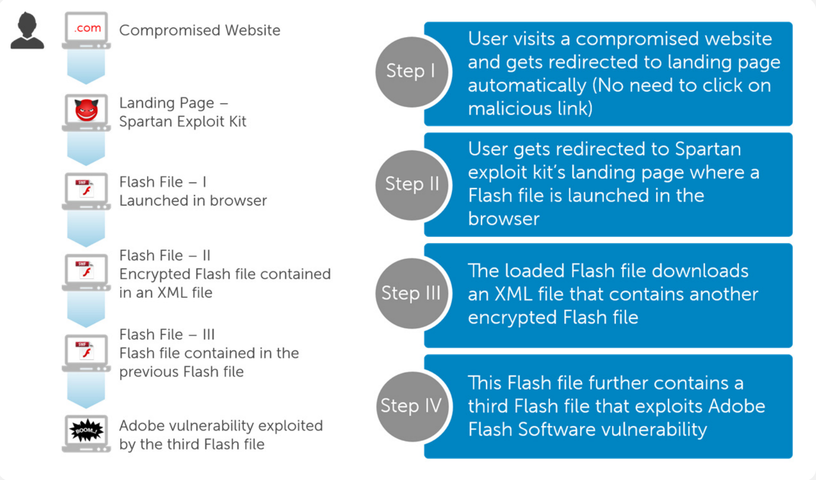
Distribution method

Victims came into contact with Spartan via malicious advertisements, some of which were encountered on vertoz.com. The exploit was delivered using HTTP, with some of the components XOR-encrypted.

Infection cycle

The flow chart in Figure 2 gives a high level description of how the Spartan exploit kit infected a system.

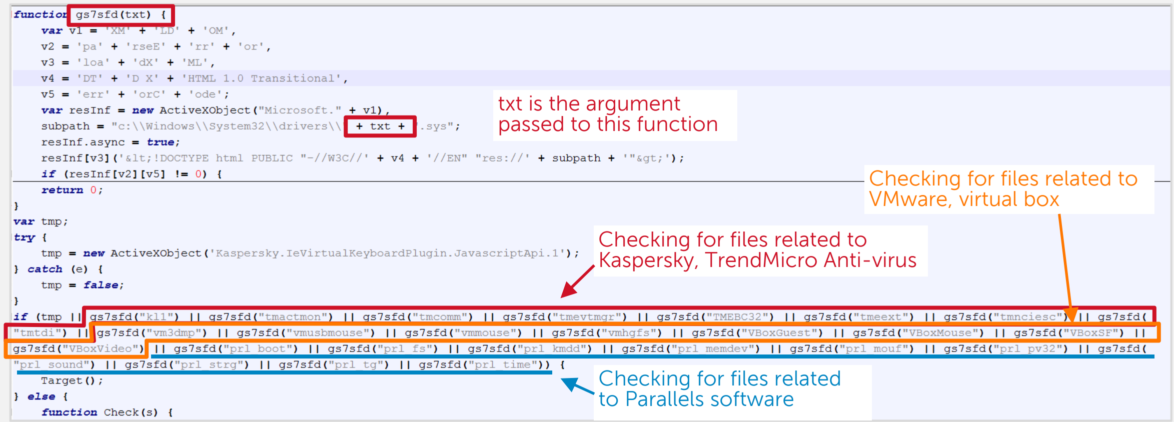
Fig. 2: Flow chart of the Spartan infection chain


.com
Compromised Website
Landing Page – Spartan Exploit Kit
Flash File – I Launched in browser
Flash File – II Encrypted Flash file contained in an XML file
Flash File – III Flash file contained in the previous Flash file
Adobe vulnerability exploited by the third Flash file
Step I
User visits a compromised website and gets redirected to landing page automatically (No need to click on malicious link)
Step II
User gets redirected to Spartan exploit kit's landing page where a Flash file is launched in the browser
Step III
The loaded Flash file downloads an XML file that contains another encrypted Flash file
Step IV
This Flash file further contains a third Flash file that exploits Adobe Flash Software vulnerability

Evasion tactics

The Spartan exploit kit used the JavaScript code in Figure 3 to detect the existence of AV and virtual machine on the infected system.

Fig. 3: Exploit kits often run a virtual environment check as part of their JavaScript routines



```
function gs7sfd(txt) {
    var v1 = 'XM' + 'LD' + 'OM',
    v2 = 'pa' + 'rseE' + 'rr' + 'or',
    v3 = 'loa' + 'dX' + 'ML',
    v4 = 'DT' + 'D X' + 'HTML 1.0 Transitional',
    v5 = 'err' + 'orC' + 'ode';
    var resInf = new ActiveXObject("Microsoft." + v1),
    subpath = "c:\\Windows\\System32\\drivers\\" + txt + ".sys";
    resInf.async = true;
    resInf[v3]('&lt;!DOCTYPE html PUBLIC "-//W3C//' + v4 + '//EN" "res://' + subpath + '"&gt;');
    if (resInf[v2][v5] != 0) {
    return 0;
}
var tmp;
try {
    tmp = new ActiveXObject('Kaspersky.IeVirtualKeyboardPlugin.JavascriptApi.1');
} catch (e) {
    tmp = false;
}
if (tmp || gs7sfd("kl1") || gs7sfd("tmactmon") || gs7sfd("tmcomm") || gs7sfd("tmevtmgr") || gs7sfd("TMEBC32") || gs7sfd("tmeext") || gs7sfd("tmnciesc") || gs7sfd(
"tmtdi") || gs7sfd("vm3dmp") || gs7sfd("vmusbmouse") || gs7sfd("vmmouse") || gs7sfd("vmhgfs") || gs7sfd("VBoxGuest") || gs7sfd("VBoxMouse") || gs7sfd("VBoxSF") ||
gs7sfd("VBoxVideo") || gs7sfd("prl_boot") || gs7sfd("prl_fs") || gs7sfd("prl_kmdd") || gs7sfd("prl_memdev") || gs7sfd("prl_mouf") || gs7sfd("prl_pv32") || gs7sfd(
"prl_sound") || gs7sfd("prl_strg") || gs7sfd("prl_tg") || gs7sfd("prl_time")) {
    Target();
} else {
    function Check(s) {
```

txt is the argument passed to this function

Checking for files related to VMware, virtual box

Checking for files related to Kaspersky, TrendMicro Anti-virus

Checking for files related to Parallels software

Other notable attributes

Spartan was highly immune to detection by security solutions for two reasons:

- Initial components used encryption
- Exploitative code was generated in memory and never written to disk

Groups targeted

Spartan proved to be the most dominant malware affecting Russia in both October and November 2015.

Status

This exploit kit is likely inactive at the moment. The known host `xml-vzsqw.qokmesopqs.xyz` was brought down, but it is fairly common for these randomly generated domains to only be active for less than a day. Unfortunately, Spartan's traits make it an ideal candidate for future campaigns, thus we anticipate the resurgence of this exploit kit leveraging new techniques in the near future.

How to avoid falling victim to exploit kits

Exploit kits only have power when companies do not update their software and systems, so the best way to defeat them is to follow security best practices:

1. Keep up with updates and patches.
2. Have a host-based anti-virus system.
3. Utilize an intrusion prevention system (IPS) and ensure it's up-to-date on the latest threats.
4. Isolate the corporate network environment into multiple zones, such as LAN, WLAN and VLAN; implement multifactor authentications for cross visiting.
5. Apply web browser plugins to control the script execution, such as the NoScript plugin for Firefox/Chrome.

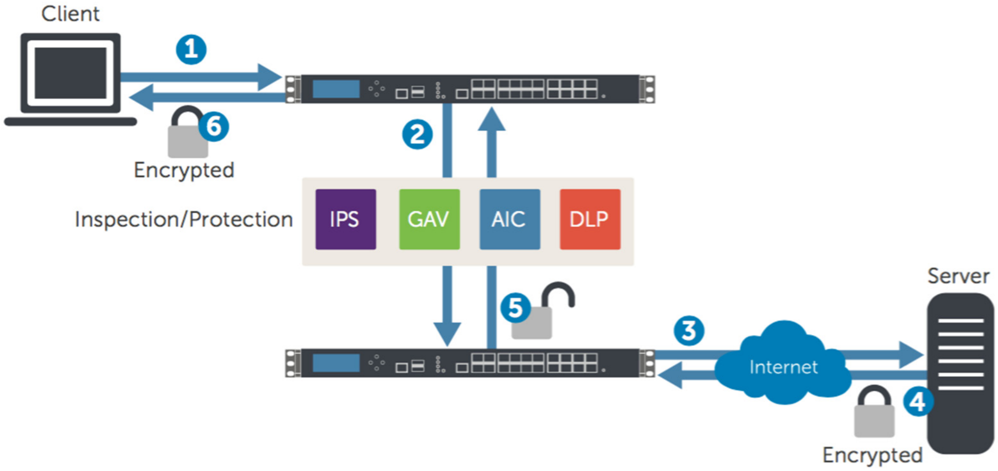
2 Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption continued to surge, leading to under-the-radar hacks affecting at least 900 million users in 2015.

In last year's Threat Report, we discussed the growth of SSL/TLS encryption, or HTTPS traffic, as a mixed bag – a positive trend in many ways, but also a tempting new threat vector for hackers. Using SSL/TLS, 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.

HTTPS traffic inspection by a next-generation firewall (NGFW) requires six additional compute processes compared to plain-text traffic inspection, as shown in Figure 4.

Fig 4: SSL/TLS inspection requires six processes[i]



SSL Inspection – Client Deployment Mode

❶ Client initiates SSL handshake with server

❷ NGFW intercepts request and establishes session using its own certificates in place of server

❸ NGFW initiates SSL handshake with server on behalf of client using admin defined SSL certificate

❹ Server completes handshake and builds a secure tunnel between itself and NGFW

❺ NGFW decrypts and inspect all traffic coming from or going to client for threats and policy violations

❻ NGFW re-encrypts traffic and sends along to client

The two processes that affect performance most are establishing a secure connection and decrypting and re-encrypting the traffic for a secured data exchange. The performance penalty can be as high as 81 percent in some cases, effectively prohibiting SSL/TLS inspection for companies operating on legacy security systems.[ii]

Notable SSL/TLS-based attacks and data

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 an advertisement on Yahoo in precisely this way, 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.[iii] An additional 10 million users were likely affected in the weeks prior by accessing ads placed by a marketing company called E-planning.[iv]

IN AUGUST 2015
an attack leveraged an
advertisement on
YAHOO
exposing as many as

900
MILLION

This campaign redirected
visitors to a site that was
infected by the
ANGLER
EXPLOIT KIT

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 January 2014. 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.

Fig. 5: Global HTTPS web connections vs. HTTP in billions.

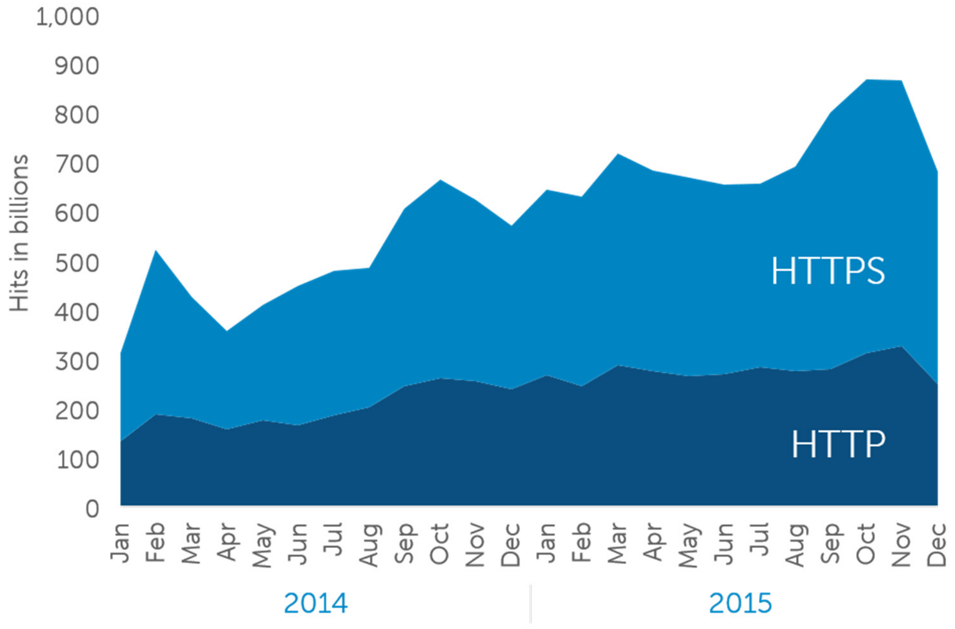
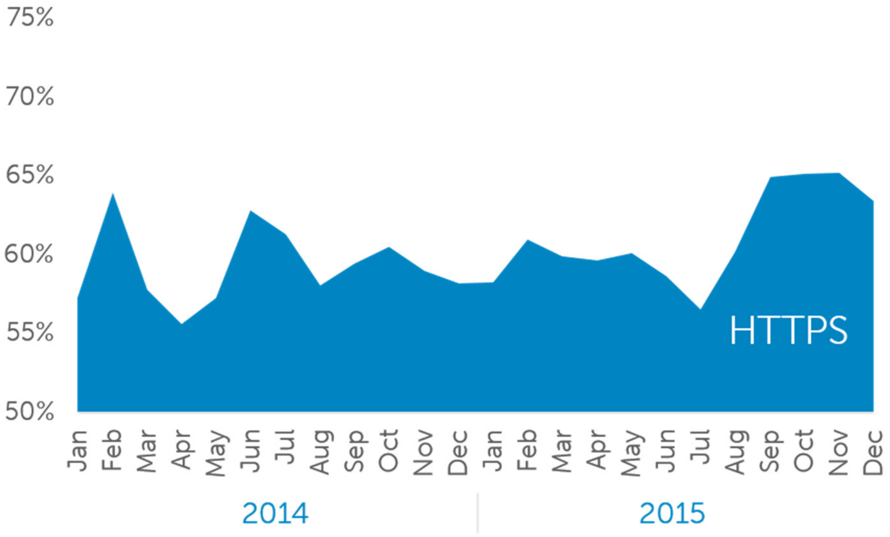


Fig. 6: HTTPS hits as a percent of total global web connections.



How to avoid falling victim to SSL/TLS-based attacks

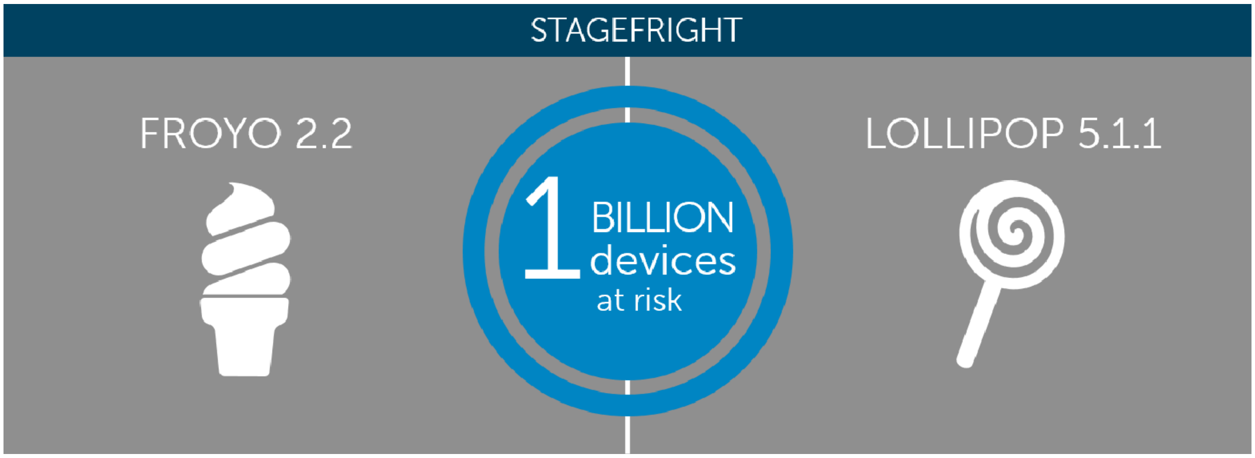
The good news is that there are ways to enjoy the security benefits of SSL/TLS encryption without providing a tunnel for attackers:

1. If you haven't conducted a security audit recently, undertake a comprehensive risk analysis to identify your risks and needs.
2. Upgrade to a capable, extensible NGFW with integrated IPS and SSL-inspection design that can scale performance to support future growth.
3. Update your security policies to defend against a broader field array of threat vectors and establish multiple security defense methods to respond to both HTTP and HTTPS attacks.
4. Train your staff continually to be aware of the danger of social media, social engineering, suspicious websites and downloads, and various spam and phishing scams.
5. Inform users never to accept a self-signed, non-valid certificate.
6. Make sure all your software is up-to-date. This will help protect you from older SSL exploits that have already been neutralized.

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.[v] With Stagefright, attackers could use videos sent over text message as an attack vector through the `libStageFrightmechanism`, which Android uses to process video files. Because text message apps automatically process videos for instant viewing, a massive number of Android users could have potentially accessed compromised files, had the vulnerability been exploited. Thankfully, Dell SonicWALL and other security organizations observed no infections from Stagefright before Google discovered and patched it.



Notable trends in Android attacks

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

1. **Perhaps in response to the success of CryptoWall and CryptoLocker in the PC world, Android-specific ransomware began to gain popularity throughout the year.** LockDroid/PornDroid for Android has been present since late 2014, but it has evolved over time. In September 2015, Dell SonicWALL observed a new variant that added a randomly generated PIN to the typical ransomware lock screen. Attackers demanded $500 as a ransom for unlocking the device and removing the lock screen.

2. **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.
3. **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, as shown in Figure 4 – 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.

Android's Marshmallow operating system, released in October 2015, included a slew of new security features aimed at reducing the impact of mobile malware infections. Of course, as attackers try and circumvent these security defenses, we can expect malicious attacks to continue in 2016.

How to avoid falling victim to Android malware

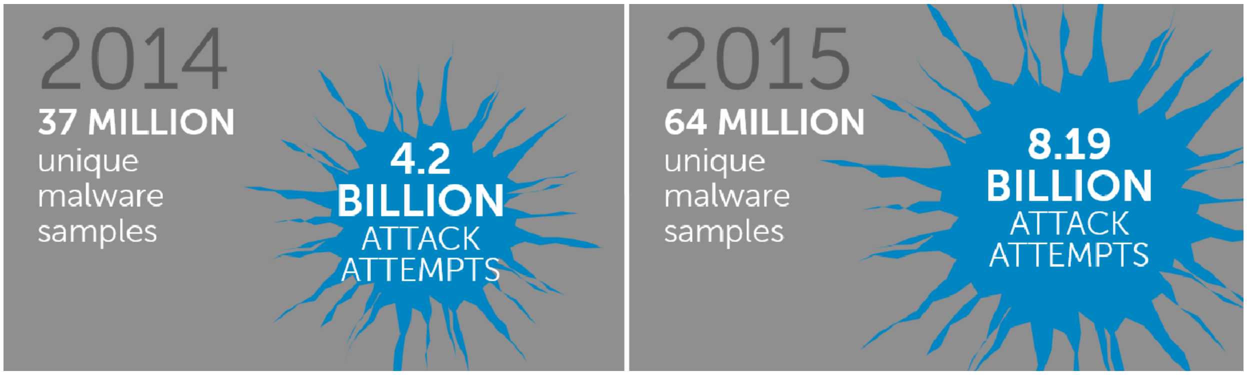
There are several precautions Android users can take to avoid this onslaught of new malware:

1. Install applications only from trusted play stores like Google Play.
2. Keep the option to install applications from unknown sources un-checked in System Settings.
3. Keep the option to verify applications checked in System Settings.
4. Keep both options under "Verify Apps" checked in Google Settings > Security.
5. Keep an eye on the permissions requested from untrusted and unknown applications, and disallow any suspicious requests.
6. Secure your internal WiFi network and be cautious when you connect to untrusted public WiFi.
7. Avoid rooting the device, as it increases the damage caused by possible infection.
8. Upgrade, if possible, to the latest version of Android.
9. Install AV and other mobile security apps for Android devices.
10. Enable remote wipe.

Fig. 7: Android apps hackers monitored to collect login data in 2015

Package name	Application name	Nature of application
au.com.bankwest. mobile	Bankwest	Finance
org.banksa.bank	BankSA Mobile Banking	Finance
com.commbank.netbank	CommonWealth Bank	Finance
com.commerzbank_photoTAN	Commerzbank AG	Finance
de.commerzbanking.mobil	Commerzbank	Finance
com.commerzbank.msb	Commerzbank MSB CashManagement	Finance
de.postbank.finanzassistent	Finance Assistant PRO	Finance
au.com.ingdirect.android	ING Bank	Finance
com.ing.diba.smartsecure2	ING-DiBa SmartSecure	Finance
com.ing.diba.mbbr2	ING-DiBa Banking + Brokerage	Finance
de.ing_diba.kontostand	ING-DiBa Kontostand	Finance
com.db.mm.deutschebank	Meine Bank	Finance
au.com.nab.mobile	National Australia Bank	Finance
mobile.santander.de	Santander UK Personal Banking	Finance
com.lufthansa.android.lufthansa	Lufthansa	Travel

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.

In this report, we've already discussed a few ways malware can be distributed. The threat vectors are almost unlimited, ranging from email spam to wearable cameras, electric cars and Internet of Things (IoT) devices.[vi, vii] However, malware sometimes is designed for specific targets, for example Black Friday shoppers or groups who speak a certain language.[viii] In this sense, the nature of the malware plays a very important role in its distribution and infection chain.

For example, in November, a Martel Frontline Camera with GPS was found to be pre-loaded with an old worm virus, `Win32/Conficker.B!inf`, which targeted the Windows operating system.

The following characteristics of the malware made it a good choice for this attack:

1. Conficker uses many advanced malware techniques to evade detection.
2. Conficker worm can easily spread and infect nearby systems.
3. Conficker can connect to Botnet, send data and receive commands.

For reasons like these, the type of malware in circulation varied widely throughout 2015 across timeframes, countries and interest groups.

Malware discovered in police body cameras

Like most technology providers, Dell Security partner iPower Technologies follows strict security protocols, regularly auditing and scanning clients' IT infrastructure and endpoint devices for vulnerabilities and malware. It was during one such routine audit that iPower discovered malware on a Martel Frontline body camera used by one of the company's law-enforcement clients.

Soon after iPower engineers connected the client's USB camera to a computer, multiple security systems on the iPower test environment were alerted to a new threat. This turned out to be a variant of the pervasive Conficker worm.

iPower immediately quarantined the malware and connected a different camera to a virtual lab PC that did not have antivirus. The team's Dell SonicWALL NGFW instantly notified them that the virus was trying to spread on the LAN. To stop this from happening, the firewall blocked the virus from communicating with command-and-control servers on the public Internet.

The iPower team stopped the threat before any damage occurred and issue an advisory that Conficker had resurfaced, an old malware being retooled and repurposed for a new world.

Notable trends in malware

TIME FACTOR

The popularity of individual malware variants changes over time, and the lifespan of each is typically not long. Most malware has a lifespan of only a few days or weeks before being noticed and rendered ineffective. For example, CVE-2015-0313, an Adobe Flash zero-day vulnerability, was prevalent in September in Russia, but quickly became much quieter after the vulnerability was patched. By contrast, there were several malware families that remained active throughout 2015, creating a huge wake of destruction.

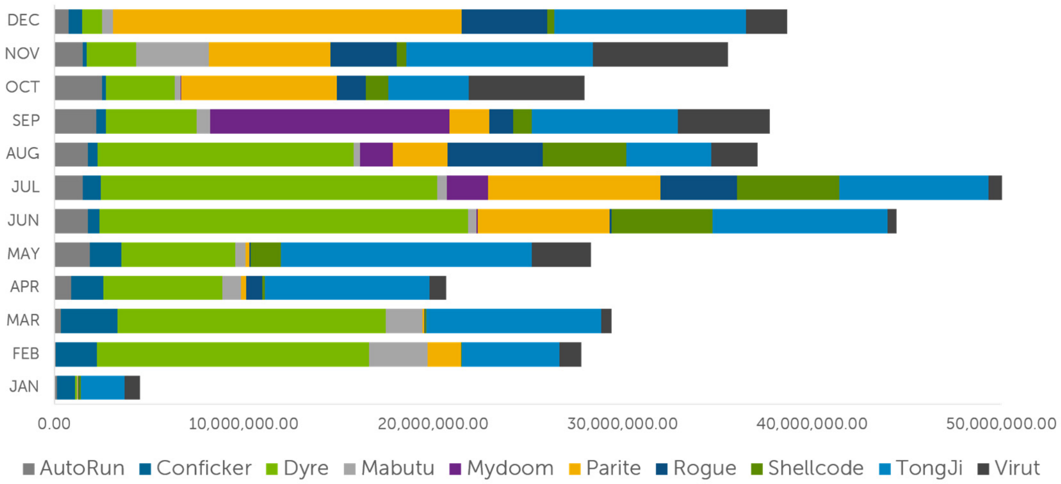
The Dyre Wolf banking Trojan was one of the most active malware variants of the year. It came onto the scene in February of 2015 and remained somewhat active through December. Like its Dyre predecessors, the Dyre Wolf malware targeted companies' banking information, rather than that of individuals. To accomplish these attacks, it deployed a number of tactics including spear phishing, distributed denial-of-service (DDoS) and social engineering to circumvent two-factor authentication processes. By April, companies had already lost between $1.5 and $6.5 million to Dyre Wolf.[ix,x]

There are a few reasons Dyre Wolf enjoyed such a long lifespan, while other malware variants proved to be a flash in the pan:

1. It targeted banks across the globe, making it especially profitable and attractive for attackers.
2. Hackers released new binary code versions quickly, sometimes in just a few days, making it difficult to identify.
3. It employed sophisticated techniques to avoid detection, for example using the Invisible Internet Project (I2P) for command and control communications.
4. It was easy to spread with tactics as simple as spam attachments. [xii]

.The combination of Dyre Wolf and Parite topped malware network traffic through 2015. Other long-lasting malware included TongJi, 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.[xii]

Fig. 8: Top 10 malware families by incidence from January to December 2015



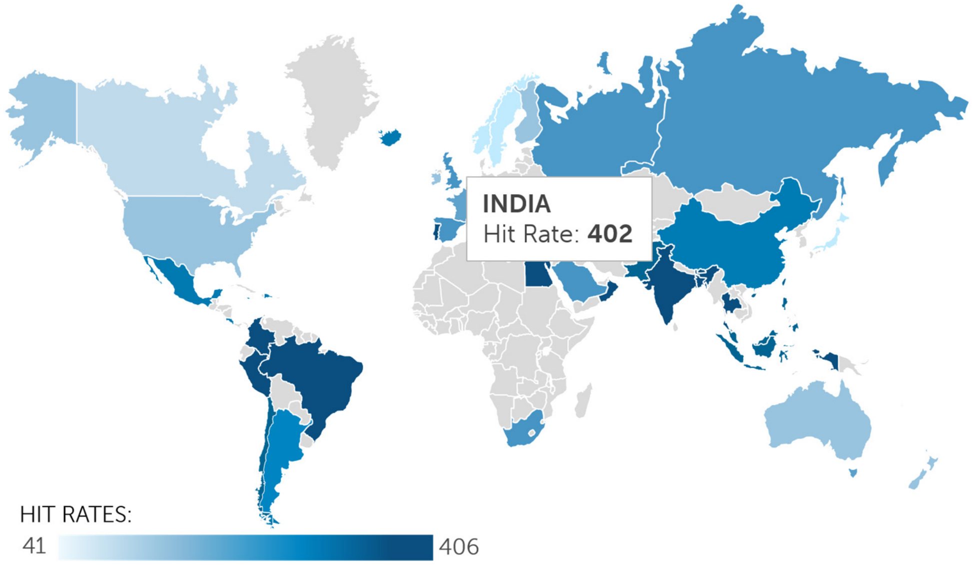
GEOGRAPHIC FACTOR

There is a strong geographic correlation to the popularity of individual malware variants. For example, 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.[xiii]

Another example was the Spartan exploit kit. In October and November 2015, the Spartan exploit kit discovered by Dell SonicWALL was most highly concentrated in Russia. While it's often difficult to determine the motives behind a geographically based attack, they are extremely common.

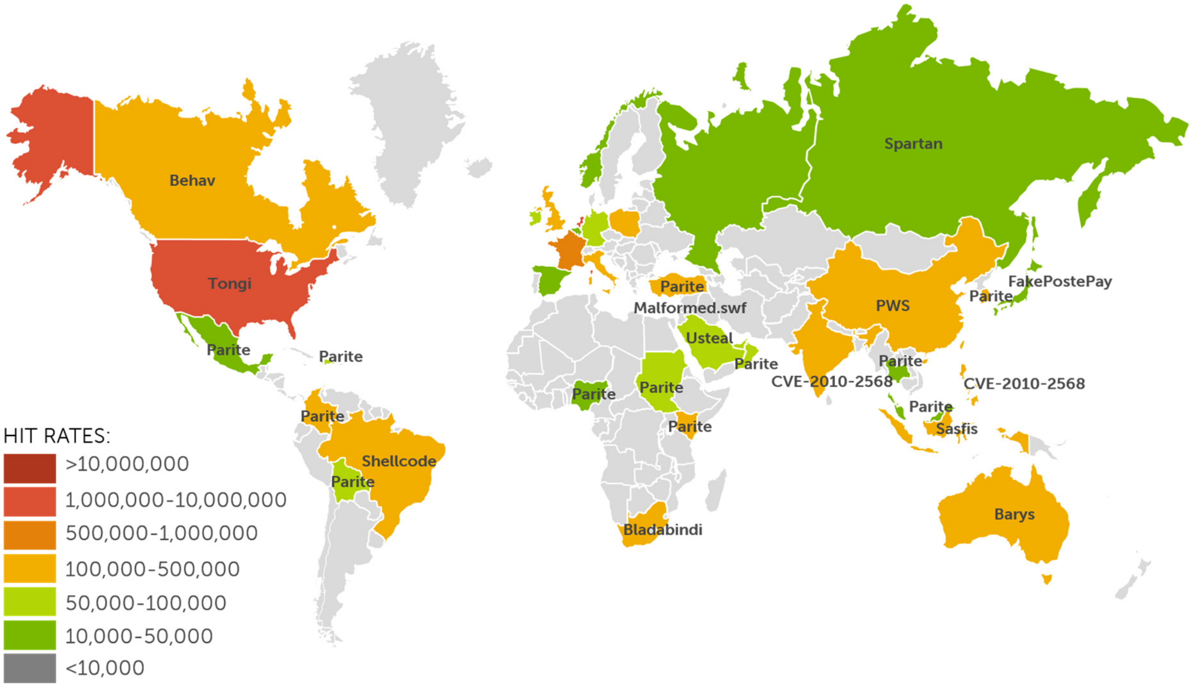
However, sometimes geographically dominant malware trends are not necessarily intentional. Usually when new software or operating systems launch, their adoption begins in developed areas, such as the United States and Europe, and gradually expands to other regions. Therefore, malware that targets older systems such as Windows XP is observed more in developing countries, as highlighted in Figure 9.

Fig 9: Windows XP usage across the globe – India represents 40 percent.



One example of this in 2015 was CVE-2010-2568, an old vulnerability exploiting Windows XP. Dell SonicWALL observed that CVE-2010-2568 was extremely popular in India in November 2015, where the operating system is still in widespread use.

Fig 10: Most popular malware by country in November 2015.



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.[xiv] 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.

Resources

[i] Ken Dang, “The Future All Encrypted Internet: Is Your Security Platform Ready?”, Dell TechCenter Blog, April 27, 2015, http://en.community.dell.com/techcenter/security/network-mobile-email/b/weblog/archive/2015/04/27/the-future-all-encrypted-internet-is-your-security-platform-future-ready

[ii] “SSL Performance Problems,” NSS Labs, June 2013, https://library.nsslabs.com/reports/ssl-performance-problems

[iii] 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

[iv] 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

[v] 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

[vi] “Hidden Virus Discovered in Martel Police Body Camera,” iPower Technologies, November 12, 2015, http://www.goipower.com/?pageId=40

[vii] 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/

[viii] “Spam campaign roundup: The Thanksgiving Day edition,” Dell SonicWALL Security Center, November 25, 2015, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=878

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

[x] 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

[xi] “Dyre.E: New variant of Dyre Trojan spreads Upatre malware,” Dell SonicWALL Security Center, 2015, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=783

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

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

[xiv] 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/