SONICWALL™

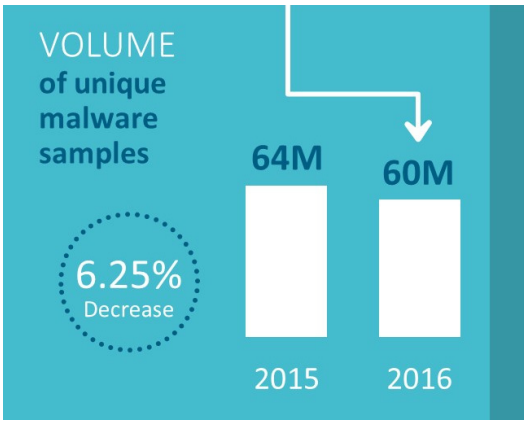
# 2017 Annual Threat Report

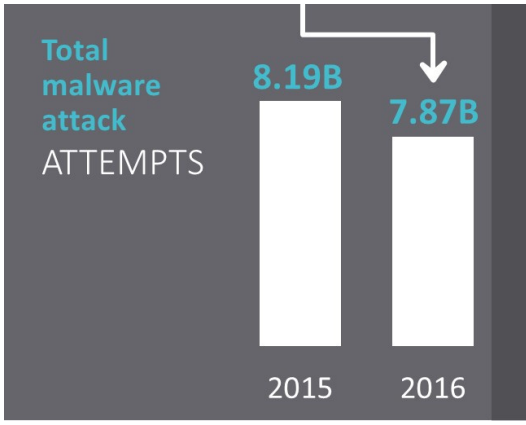
# Table of Contents

# Introduction

2016 could be considered a highly successful year from the perspective of both security professionals and cyber criminals. Security teams leveraged groundbreaking technologies to successfully fend off attacks that would have devastated their organizations in years past. At the same time, we saw the rise of new cyber threats that targeted organizations of all sizes and led to serious financial consequences for many.

It would be inaccurate to say the threat landscape either diminished or expanded in 2016 – rather, it appears to have evolved and shifted. Cybersecurity is not a battle of attrition; it's an arms race, and both sides are proving exceptionally innovative.




According to the SonicWall Global Response Intelligence Defense (GRID) Threat Network, security teams achieved a solid share of victories in 2016. Unlike in years past, SonicWall saw the volume of unique malware samples collected fall to 60 million compared with 64 million in 2015, a 6.25 percent decrease. Total attack attempts dropped for the first time in years, to 7.87 billion from 8.19 billion in 2015.

In addition, the broader adoption of chip and PIN technology in countries such as the United States seems to have cooled cyber criminals' interest in point-of-sale (POS) system attacks to the tune of an 88 percent decrease in POS malware variants since 2015, as observed by the SonicWall GRID Threat Network. Law enforcement and cyber investigations helped contribute to the mid-year disappearance of three exploit kits that ran rampant in early 2016—Angler, Neutrino and Nuclear. Meanwhile Secure Sockets Layer/Transport Layer Security (SSL/TLS) encrypted traffic continued to rise in volume, pointing to a positive overall trend in online security.

However, the SonicWall GRID Threat Network also observed an exponential increase in the number of advanced threats via ransomware, from nearly 4 million attack attempts in 2015 to 638 million in 2016, a 167x year-over-year increase. These attacks were typically delivered by phishing campaigns and hidden from detection using SSL/TLS encryption. The rise of ransomware-as-a-service (RaaS) made it easier than ever for cyber criminals to access and deploy ransomware. As a result, many organizations struggled to find answers on how to protect themselves and how to properly respond to the dilemmas raised by this new breed of cyber threat.

Security teams were also faced with the rapid evolution of other threats. Internet of Things (IoT) devices were successfully compromised on a massive scale and used to mount distributed denial-of-service (DDoS) attacks that disrupted high-profile companies including Airbnb, Netflix, Reddit, Twitter and Spotify. Cyber criminals also found new ways to compromise Android™ devices using overlay attacks, despite operating system security updates.

As cybersecurity enters a new era of automated breach prevention, not just breach detection, security companies may begin to achieve even greater victories in the cyber arms race. But it's ultimately up to the businesses at the center of the fight to ensure they're armed for battle. The goal of the SonicWall Annual Threat Report is to define the cybersecurity battlefield in order to enable companies and individuals around the world to mount an impenetrable defense in 2017 and beyond.

# Key **Threat Report Findings** from 2016

## Security Industry Advances

**Point-of-sale** malware creation declined by 93 percent since 2014 after high-profile retail breaches led to more proactive security measures across the industry.

**Secure Sockets Layer/Transport Layer Security** encrypted traffic grew by 38 percent, partly in response to growing cloud application adoption.

**Dominant exploit kits** Angler, Nuclear and Neutrino disappeared in mid-2016.

**Unique malware samples** collected fell to 60 million in 2016 compared with 64 million in 2015, a 6.25 percent decrease, whereas total attack attempts dropped to 7.87 billion in 2016 from 8.19 billion in 2015.

## Cyber Criminal Advances

**Ransomware** use grew by 167x year-over-year and was the payload of choice for malicious email campaigns and exploit kits.

**IoT** devices were compromised on a massive scale due to poorly designed security features opening the door for distributed denial-of-service attacks.

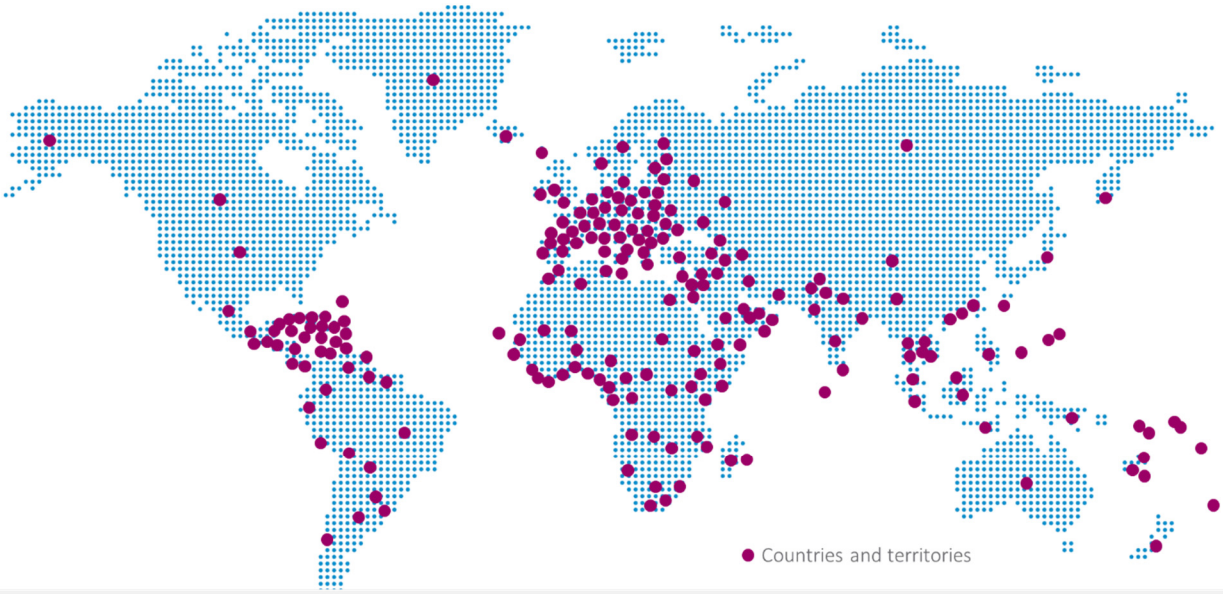
**Secure Sockets Layer/Transport Layer Security** encrypted malware provided an uninspected backdoor into the network that cyber criminals could exploit.

**Android** devices saw increased security protections but remained vulnerable to overlay attacks.

## Data for the 2017 SonicWall Annual Threat Report was gathered by the SonicWall GRID Threat Network, which sources information from global devices and resources including:

- More than 1 million security sensors in nearly 200 countries and territories
- Cross-vector threat-related information shared among SonicWall security systems, including firewalls, email security, endpoint security, honeypots, content filtering systems and SonicWall Capture multi-engine sandbox technology
- SonicWall malware analysis automation framework, fully developed internally
- 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
- Spam alerts from millions of computer users protected by SonicWall email security solutions

### SonicWall GRID Threat Network



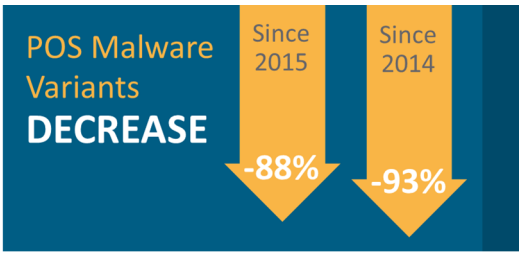

| 1.0M+ | 200+ | 24x7x365 | < 24 Hr. | 100K+ | 100K+ |
|---|---|---|---|---|---|
| Sensors | Countries and territories | Monitoring | Response to 0-day vulnerabilities | Malware samples collected daily | Malicious events analyzed daily |

## The creation of new point-of-sale malware declined by 93 percent since 2014 after high-profile retail breaches led to more proactive security measures across the industry.

If 2016 was the year of ransomware, 2014 was the year of point-of-sale (POS) malware attacks. That year, the SonicWall Global Response Intelligence Defense (GRID) Threat Network observed a 333 percent increase in the number of new POS malware countermeasures developed and deployed compared with the year prior. This finding came as no surprise to members of the retail and cybersecurity industries, as we saw well-known companies including Home Depot, Target, Michaels, Staples and many others suffer massive data breaches in 2014, exposing the credit card data for hundreds of millions of consumers.[i, ii, iii]

Since then many retailers have upgraded elements of their security programs to better protect customer data and avoid a repeat performance of 2014. Retailers now have a better understanding of the vulnerabilities and risks their digital environments present and how to defend against attacks using the Payment Card Industry Data Security Standard (PCI-DDS) checklist and other ongoing security measures. Perhaps the single largest shift we've seen since 2014 has been the wider adoption of chip-based POS systems in countries that were years behind on this technology, such as the United States. Chip-based POS systems ensure every transaction is issued a unique verification code that can only be used once. Compared with traditional credit cards featuring magnetic strips with static data, chip cards are much more difficult to fake and also more difficult to steal usable information from.[iv]

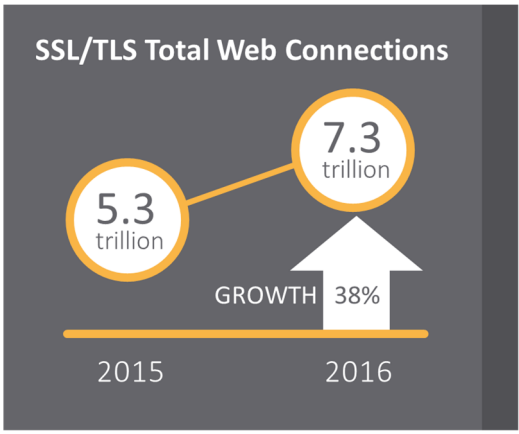
Thanks at least in part to these positive security trends, the SonicWall GRID Threat Network saw the number of new POS malware variants decrease by 88 percent since 2015 and 93 percent since 2014. This implies that cyber criminals are becoming less interested in devoting time to POS malware innovation. While we should not read this as a sign that POS malware is disappearing, it's clear that cyber thieves have been focused elsewhere in recent months. And it's an even better sign that when an industry truly makes security a priority, positive changes can happen.

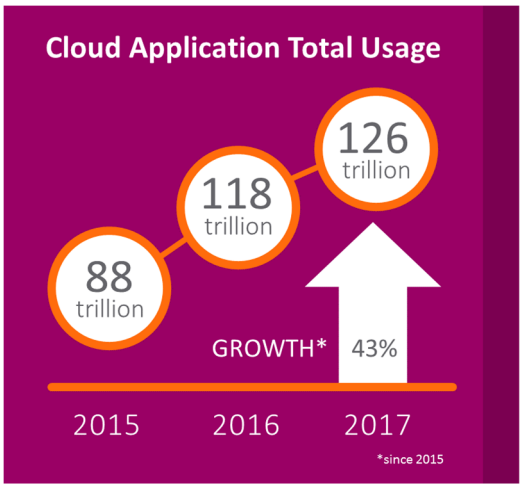
## Secure Sockets Layer/Transport Layer Security encrypted traffic grew by 38 percent, partly in response to growing cloud application adoption.

The trend toward Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption has been on the rise for several years. As web traffic grew throughout 2016, so did SSL/TLS encryption, from 5.3 trillion web connections in 2015 to 7.3 trillion in 2016 according to the SonicWall Global Response Intelligence Defense (GRID) Threat Network. The majority of web sessions that the SonicWall GRID Threat Network detected throughout the year were SSL/TLS-encrypted, comprising 62 percent of web traffic.

As a means of protecting privacy and data integrity, the growth of SSL/TLS encryption is undeniably a positive trend. Signified by a HTTPS URL and lock icon on browsers, SSL/TLS encryption was primarily developed to provide secure authentication on the web for e-commerce and other financial transactions. However, it has become more widespread as a way of protecting privacy and security on websites that did not originally require encryption, such as search engines and search results.




One reason for the increase in SSL/TLS encryption is the growing enterprise appetite for cloud applications. As cloud applications have improved their feature sets and proven their reliability over time, they've become a more viable option for enterprises that appreciate the fact they are more affordable, easier to implement and less taxing to manage than applications hosted on premise. The SonicWall GRID Threat Network has seen cloud application total usage grow from 88 trillion in 2014 and 118 trillion in 2015 to 126 trillion in 2016. SSL/TLS encryption wraps around all interaction with cloud services, which could account for some of the SSL/TLS traffic growth. NSS Labs predicts that SSL/TLS traffic will account for 75 percent of online interactions by 2019.[v]


This growth is likely to spike even further in 2017 thanks to Google's September 2016 announcement that, beginning in January 2017, the Google Chrome browser would mark all HTTP sites collecting passwords or credit cards as "not secure." The company went on to state this was part of a larger plan to eventually mark all HTTP traffic as such.[vi]

While this trend toward SSL/TLS encryption is overall a positive one, it also merits a word of caution. As we've discussed in past SonicWall Annual Threat Reports, SSL/TLS encryption makes it more difficult for cyber thieves to intercept payment information from consumers, but it also provides an uninspected and trusted backdoor into the network that cyber criminals can exploit to sneak in malware.

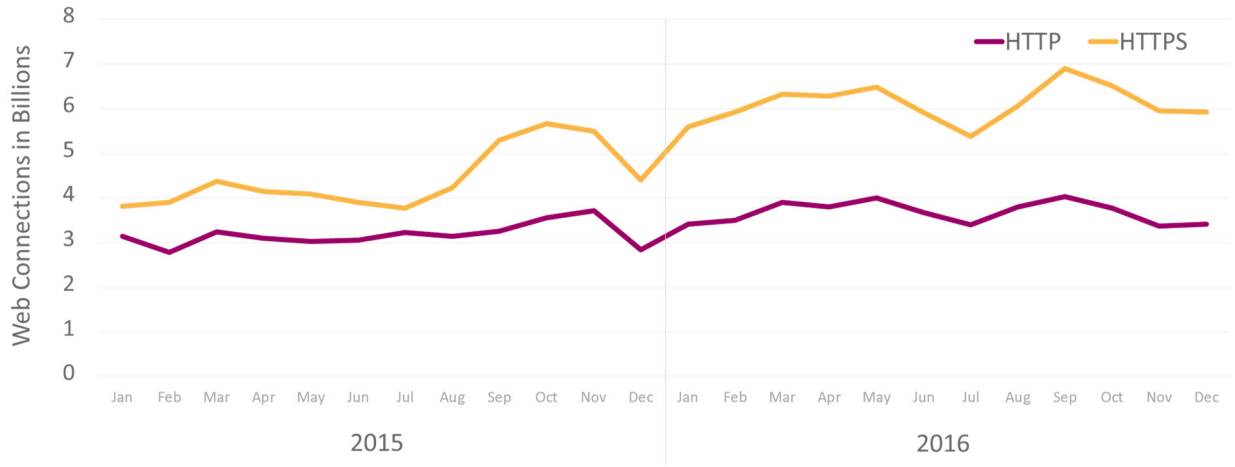
NSS Labs reported seeing an increase in both the number and sophistication of threats that leveraged encryption, observing a 72 percent year-over-year growth in this type of attack.[vii]

The reason this security measure can become an attack vector is that most companies still do not have the right infrastructure in place to perform deep packet inspection (DPI) in order to detect malware hidden inside of SSL/TLS-encrypted web sessions. While most next-generation firewalls are equipped to perform DPI, they typically suffer such a massive loss of performance when doing so that it isn't viable for companies to enable this feature. Unfortunately, without these protections in place, the rest of a company's security posture is moot as the majority of traffic entering the network is not being inspected.

Simply put, SSL/TLS encryption remains a mixed bag for security teams. Organizations that don't inspect SSL/TLS traffic are shutting their eyes to well over half of what's entering their networks. But companies who are prepared and vigilant for threats lurking in encrypted traffic will enjoy an unprecedented level of privacy and security as a result of this changing tide.

**62%**
of web connections were SSL/TLS-encrypted

**Global HTTPS vs. HTTP Web Connections**



## Dominant exploit kits Angler, Nuclear and Neutrino disappeared in mid-2016.

As 2016 began, the malware market was dominated by a handful of exploit kits, particularly Angler, Nuclear and Neutrino. However, following the arrest of more than 50 Russian hackers for leveraging the Lurk Trojan to commit bank fraud, the Angler exploit kit suddenly stopped appearing.

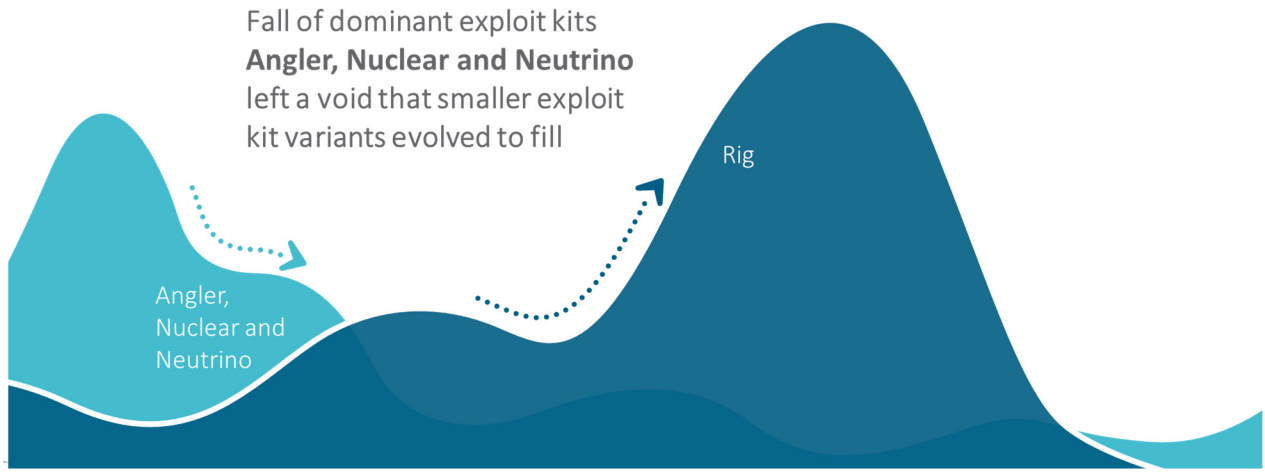
The coincidence seemed unlikely enough that many believe Angler's creators were among those arrested.[viii] For a while following Angler's disappearance, Nuclear and Neutrino saw a surge in usage, before quickly fading out as well.

To fill this void, the remaining exploit kits began to fragment into multiple, smaller versions. The SonicWall Global Response Intelligence Defense (GRID) Threat Network observed that by the third quarter of 2016, the Rig exploit kit had evolved into three versions leveraging different URL patterns, landing page encryption and payload delivery encryption: Rig standard; Rig-V, also known as Rig VIP version; and Rig-E, or the Empire version. As Neutrino's standard version faded away, Neutrino-V, known as the VIP version, started appearing.

As different versions of these exploit kits were introduced, they evolved to utilize multiple levels of obfuscation rather than simple JavaScript obfuscation. In the case of Rig, SonicWall observed the use of cryptographic algorithms to obfuscate landing pages and payloads.

As with spam and other distribution methods in 2016, SonicWall saw exploit kits become part of the ransomware delivery machine, making variants of Cerber, Locky, CrypMIC, BandarChor, TeslaCrypt and others their primary payloads throughout the year.

However, exploit kits never really recovered from the massive blow they received early in the year with the takedown of their dominant families. As security teams continue to discover and expose high-profile cyber attackers, we can hope to see the downfall of many other pervasive threats in 2017.

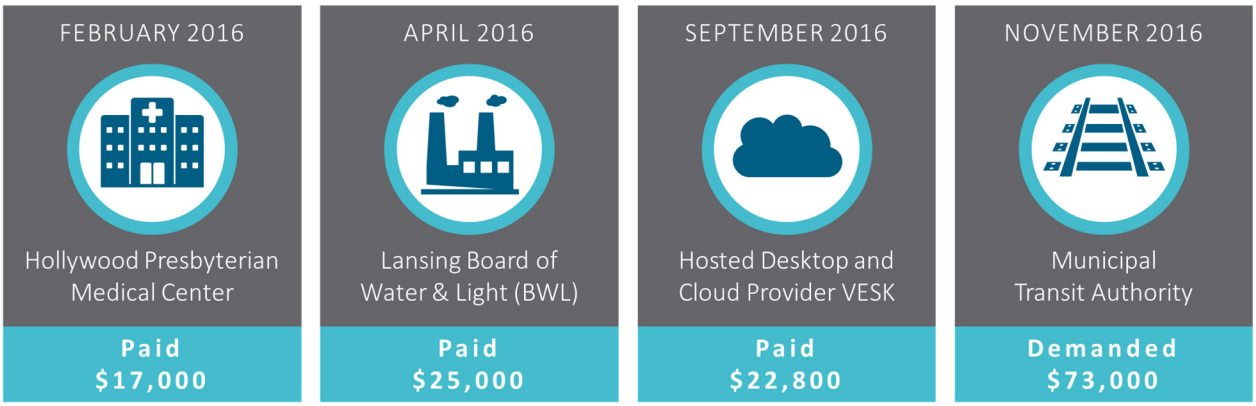


## Ransomware use grew by 167x year-over-year and was the payload of choice for malicious email campaigns and exploit kits.

The meteoric rise of ransomware in 2016 is unlike anything we've seen in recent years. The SonicWall Global Response Intelligence Defense (GRID) Threat Network detected an increase from 3.2 million ransomware attack attempts in 2014 and 3.8 million in 2015 to an astounding 638 million in 2016. By the end of the first quarter, $209 million in ransom had been paid by companies, and by mid-2016, almost half of organizations reported being targeted by a ransomware attack in the prior 12 months.[ix]

The SonicWall GRID Threat Network observed ransomware attacks against businesses of all sizes throughout the year. While many victims of ransomware chose not to publicize the attacks, several breaches received national attention. Hollywood Presbyterian Medical Center in Los Angeles admitted to paying $17,000 in bitcoin to regain access to its data in February 2016, while the Lansing Board of Water & Light (BWL) revealed they paid ransomware attackers $25,000 in April 2016.[x, xi] In the U.K. in September 2016, hosted desktop and cloud provider VESK handed over 29 bitcoins, worth about $22,800 USD at the time.[xii] And in November 2016, the San Francisco Municipal Transit Authority had to open its fare gates when a ransomware attack took down its payment and email systems, demanding 100 bitcoins, or about $73,000 at the time.[xiii]

### Key Ransomware Attacks in 2016



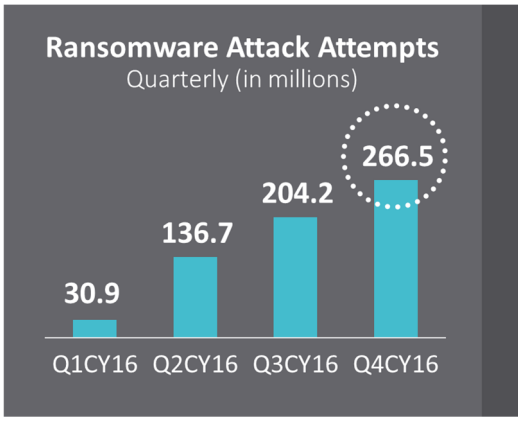
Each of these organizations, and the countless others who were hit with ransomware, faced an urgent and terrifying decision: whether or not to pay the ransom. Those who opted to pay were sometimes able to negotiate a lower ransom to regain access to their systems. Some, like the Kansas Heart Hospital that was attacked in May 2016, paid the ransom only to still be denied access to their data.[xiv]

Sadly, whether the ransom was paid or not, the total cost of these attacks could be enormous. Only 42 percent of companies attacked were able to fully recover their data from a backup.[xv] While the Lansing BWL paid $25,000 in ransom, administrators revealed that responding to the attack cost them $2.4 million, with 99 percent of the cost covering their cyber emergency response team; stabilization and restoration efforts; and enhancements to cybersecurity technology and personnel.[xvi] Add to that the likelihood of increased insurance premiums and the costs will continue to mount in the months to come. It is a steep price to pay simply because an employee opened a compromised file.[xvii]

The unprecedented growth of ransomware was likely driven by easier access in the underground market and supported by the low cost of conducting a ransomware attack; the ease of spreading it; and the low risk of being caught or punished. The rise of ransomware-as-a-service (RaaS) made ransomware significantly easier to obtain and deploy. Individuals who wanted to profit from ransomware didn't need to be expert coders, they simply needed to download and deploy a malware kit. Some RaaS providers offered their malware for free, while others charged a flat rate, typically $100 or less, or a percentage of the take—often 20 percent.[xviii, xix]

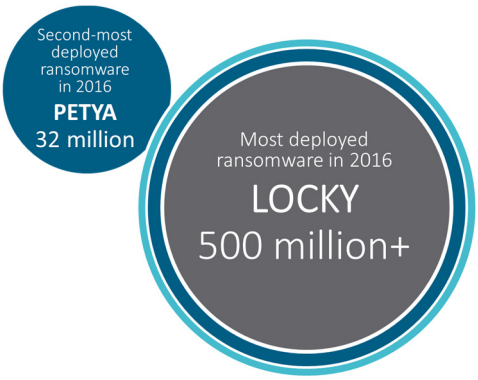
Another factor driving the usage of ransomware was the mass adoption of Bitcoin. Before cryptocurrencies, ransomware attacks simply were not feasible due to the risks associated with accepting trackable payments.

Throughout the year, the SonicWall GRID Threat Network discovered a few key ransomware trends:




- **Ransomware remained on an upward climb throughout the year.** SonicWall GRID Threat Network data showed that ransomware attacks were not likely to decrease going into 2017, as the incidence continued to rise quarter-over-quarter through the end of December 2016. The first major spike came in March 2016 when ransomware attack attempts shot up from 282,000 to 30 million over the course of the month, for a first-quarter total of 30.9 million hits. This upward trend continued throughout the year, with the fourth quarter closing at 266.5 million ransomware attack attempts.
- **The most popular payload for malicious email campaigns in 2016 was ransomware, typically Locky.** Nemucod, a Trojan downloader used to distribute ransomware, was utilized in 79 percent of malware-delivering spam attacks in 2016. Contrast this with 2015, when the most popular

malware variants distributed through spam were data-stealing Trojans from the Dridex family. Locky was by far the most-deployed ransomware, utilized in about 90 percent of Nemucod attacks and more than 500 million total attacks throughout the year, compared with second favorite Petya, which was only used in 32 million attacks. Locky was most commonly delivered via email as a Microsoft Word document attachment under the guise of an invoice from a vendor requiring payment. When the targeted user would open the attachment, he or she would be instructed to enable macros, which would set off a chain reaction leading to the encryption of the user's files and the service of a ransom demand.




- **No industry was spared from ransomware attack attempts.** Industry verticals were targeted almost equally, with the mechanical and industrial engineering industry reaping 15 percent of average ransomware hits, followed by a tie between pharmaceuticals (13 percent) and financial services (13 percent), and real estate (12 percent) in third place.
- **Exploit kits began using ransomware as a payload.** In 2015, we saw exploit kits delivering malware such as worms, downloaders, infostealers and botnets. However, the SonicWall GRID Threat Network discovered that most of the malware distributed by exploit kits in 2016 was ransomware, commonly from the Locky, Cerber, CrypMIC, BandarChor, TeslaCrypt families and others.
- **Companies in the United Kingdom were 3x as likely as United States companies to be targeted by ransomware.** The SonicWall GRID Threat Network observed that the United States experienced the highest number of ransomware attacks in 2016 due to the large volume of businesses. However, companies in the United Kingdom were almost three times as likely as U.S. companies to be targeted with ransomware, when accounting for the smaller number of businesses in the U.K. and the high saturation of ransomware. On the other hand, China was least likely to be targeted, possibly due to the country's restricted access to Bitcoin and low usage of Tor.[xx, xxi]

With the high likelihood of becoming a target for ransomware, it's important for all organizations to back up their data continuously to a backup system that is either not always online or utilizes authentication. This will help ensure that if you're hit with ransomware, you don't accidentally revert to an encrypted backup.

## Internet of Things devices were compromised on a massive scale due to poorly designed security features, opening the door for distributed denial-of-service attacks.

With their integration into the core components of our businesses and lives, Internet of Things (IoT) devices provide an enticing attack vector for cyber criminals who are becoming more interested as IoT becomes increasingly widespread.

IoT attacks surged in 2016 for a few reasons. IoT developers and startups have been under pressure to beat competitors to market, often leading them to launch their devices without fully baked security features in place. That same lack of security focus means unsecured onboarding experiences in which users are never presented with an option to change their password from the default. Furthermore, when cyber thieves discover a weakness in a device's firmware, they are able to exploit it ad infinitum, as the manufacturer rarely has a team dedicated to updating and patching those issues or informing users they've been compromised. Without any regulations, guidelines or accountability for IoT device makers, the world of IoT has become a massive, management environment and a playground for cyber criminals.

These security gaps in IoT devices enabled cyber thieves to launch the largest distributed denial-of-service (DDoS) attacks in history during 2016. In September and October 2016, attackers leveraged hundreds of thousands of IoT devices with weak telnet passwords to launch DDoS attacks using the Mirai botnet management framework. The first significant attack was on hosting company OVH and the second on major DNS service provider Dyn, which caused service outages for prominent websites including Airbnb, Netflix, Reddit, Twitter, Spotify and many others.[xxii, xxiii, xxiv]

While the exact cost of these attacks has not been revealed, DDoS attacks in general are estimated to cost businesses an average of $22,000 per minute, with the cost ranging as high as over $100,000 per minute.[xxv] With the average DDoS attack lasting six hours, the financial impact can be enormous.

The SonicWall Global Response Intelligence Defense (GRID) Threat Network observed vulnerabilities in all categories of IoT devices in 2016, including smart cameras, smart wearables, smart home, smart vehicle, smart entertainment and smart terminals. During the height of the Mirai surge in November 2016, SonicWall found the United States was by far the most targeted, with 70 percent of DDoS attacks directed towards the region, followed by Brazil (14 percent) and India (10 percent).

To prevent your IoT devices from falling victim to a DDoS attack, make sure your devices are behind a next-generation firewall which scans for IoT-specific malware like Mirai. It is also critical to segregate all IoT devices on a separate zone from the rest of the network in case the device becomes compromised.

**Gaps in IoT devices exposed the largest DDoS attack in history via Mirai botnet**


**DDoS attacks** are estimated to cost businesses

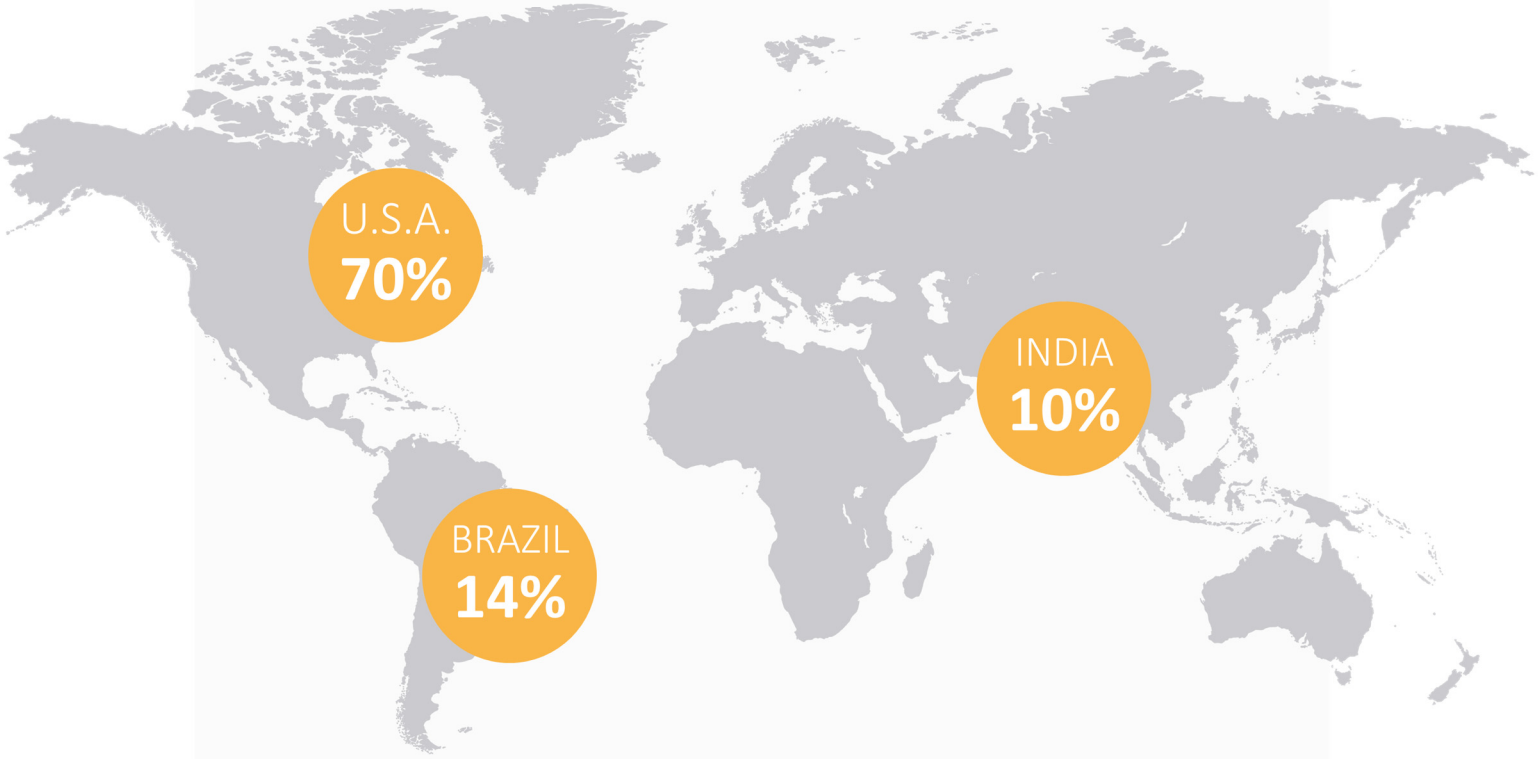
*an average of*
**$22,000 per minute**

with the cost ranging as high as over $100,000 per minute.[i]

*With the average DDoS attack lasting six hours, the financial impact can be enormous.*

## IoT DDoS Attacks

Top 3 countries targeted by DDoS attacks in
November during the height of the Mirai botnet surge



## Android devices saw increased security protections but remained vulnerable to overlay attacks.

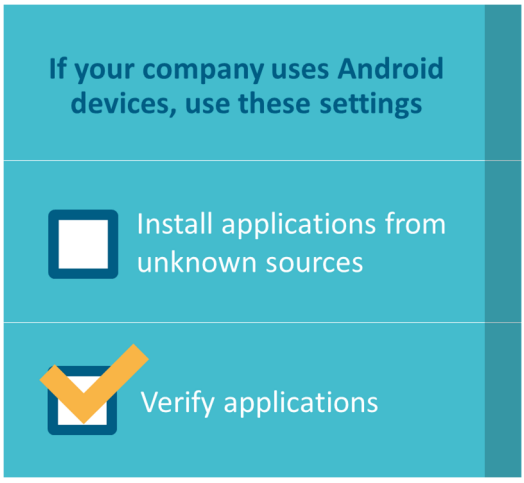
There's no question Google worked hard in 2016 to patch the vulnerabilities and exploits that cyber criminals have used against Android in the past. In the first quarter, we saw the slow but steady adoption of the new Android operating system, Android Marshmallow 6.0, which was designed with additional security features including a revamped approach to permission granting, more frequent security patches and full-disk encryption. Google followed that with Android 7.0 Nougat, which incorporated additional security measures.[xxvi, xxvii]

However, attackers used novel techniques to beat these security measures and Android remained a popular, risk-prone target in 2016:

- **Cyber criminals leveraged screen overlays to steal login information and other data.** Where overlays have been used in the past to deliver ransom demands to ransomware victims, attackers used them in 2016 to mimic legitimate app screens and trick users into entering sensitive data. The SonicWall Global Response Intelligence Defense (GRID) Threat Network observed this functionality being used in multiple Android Banker campaigns and others.[xxviii] When Android responded with new security features to combat overlays, SonicWall observed attackers circumventing these measures by coaxing users into providing permissions that allowed overlays to still be used.[xxix]
- **With HummingBad, ad-fraud malware evolved to also seek root access.** HummingBad malware bombarded victims' Android devices with an insupportable number of advertisements. While the focus of HummingBad seemed to be generating revenue based on accidental ad clicks, the malware also gave attackers root access to victims' devices, implying a more sinister attack might still be on the horizon.[xxx]
- **Android malware leveraged the aid of security testing tools like Metasploit.** When Metasploit penetration testing added the ability to infiltrate Android devices, the SonicWall GRID Threat Network observed malware strains that contained these Android-specific Metasploit modules. This indicates that malware authors have begun using Metasploit as an aid to infect Android devices.[xxxi]
- **Compromised adult-centric apps declined on Google Play but continued to find victims on third-party app stores.** Ransomware was a common payload, but so were self-installing apps. The SonicWall GRID Threat Network observed more than 4,000 distinct apps with self-installing payloads in a matter of two weeks.[xxxii, xxxiii]
- **DressCode gave us a taste of what corporate Android malware could look like.** SonicWall observed a threat across multiple Android apps that used the Socket Secure (SOCKS) protocol to establish a connection with the attacker's command and control server, turning the user's device into a proxy. In this

way, attackers could circumvent company firewalls and access any resource connected to the infected device. No known victims have been identified at this time, however, we can interpret DressCode as a sign of threats to come. [xxxiv]

If your company uses Android devices, keep the option to "install applications from unknown sources" un-checked and both options to "verify applications" checked. Avoid rooting, and install anti-virus and other mobile security apps for Android devices. Enable "remote wipe" in case your device is stolen or compromised with ransomware.



# Predictions for 2017

The more clearly we can determine cyber attackers' current focus, the better we can infer their next moves. Understanding that today's cyber criminals are highly motivated to launch low-effort, quick-payout attacks and have been experimenting with Internet of Things (IoT) and other new methods of attack, we can predict some elements of the threat terrain ahead.

## Point-of-Sale Malware

- Point-of-sale malware innovation will remain low as thieves continue to enjoy the quicker payoff and relative ease of launching ransomware attacks.

## SSL/TLS Encryption

- Encrypted malware and advanced threats will grow as HTTPS web connections become standard across industries.

## Exploit Kits

- The exploit kit threat landscape will remain fragmented among new and smaller exploit kits after the downfall of major players we saw at the beginning of 2016. In addition, multiple versions of each exploit kit will remain in the wild.
- We'll see an additional emphasis on ransomware as the payload of choice for exploit kits as it magnifies and thrives beyond the healthcare and financial industries.

## Ransomware

- The movement to ransomware-as-a-service (RaaS) will continue to make ransomware available to a broader range of less-sophisticated cyber threat actors, who are likely to use additional deployment techniques as they grow in experience and confidence.
- Attackers will begin to use malware to take control of IoT devices and demand ransom as soon as those devices reach greater saturation in households and corporate environments. For example, a thief could potentially suspend company production lines, city power grids, fleets of delivery vehicles or even connected personal health devices like pacemakers in exchange for ransom.

- Ransomware attacks will become more creative as attackers identify more repositories of valuable data that they can exploit. For example, ransomware has already expanded to attack poorly secured websites and databases on the web, holding entire sites or databases for ransom due to IT administrators' failure to keep up with best security practices.
- Email will continue to be a highly effective distribution vector for ransomware as companies scramble to put more effective advanced threat prevention systems and employee training procedures in place.


## Internet of Things

- IoT-based distributed denial-of-service (DDoS) attacks will continue after the success of the Mirai botnet's model and may begin to more frequently target e-commerce sites and others that heavily depend on uptime for profitability. DDoS attacks may also serve as a diversion for simultaneous exfiltration attacks.
- The mass compromise of IoT devices will be used for financial gain in ways beyond DDoS attacks. We may begin to see large privacy leak incidents involving location data, camera videos and health-related information.
- Attackers may begin to exploit IoT vulnerabilities to take control of property, for example by stealing a drone or taking control of a smart car's steering wheel.

## Android Malware

- Ransomware will continue to plague the Android ecosystem, as mobile devices typically contain sensitive user data and many do not utilize cloud backup.
- Overlay-based malware will continue to increase in numbers.
- Malware authors will look for ways to target Android fingerprint readers.
- We can expect to see more Android malware that makes use of third-party tools and services to increase the attack potency.
- As Android Auto and Android Pay become more mainstream, malware creators will try to leverage these new threat vectors.
- Flash and Silverlight will continue to be the major target applications for exploit kits. However with the decrease of Flash usage, the number of exploits kits leveraging them will decline.

# Best Practices for an Effective Security Program

With the decline of point-of-sale (POS) malware variants and exploit kits, it's clear that there can be real and viable progress in the war against cyber criminals. The tools and resources available to organizations have never been more capable of creating and supporting a supreme level of security. However, it falls to each individual security team to follow best practices for their infrastructure.

- ☑ Build a "human firewall" by teaching your employees, especially those dealing with payments, how to deal with potential threats, such as malicious emails and suspicious pop-ups. Tell your users never to accept a self-signed, non-valid certificate.
- ☑ Isolate the corporate network environment into LAN, WLAN and VLAN zones and implement multifactor authentication for cross-visiting. Isolate critical systems, Internet of Things (IoT) devices and POS systems as well.
- ☑ Deploy a next-generation firewall that is capable of high-performance Secure Sockets Layer/Transport Layer Security (SSL/TLS) inspection enabled to ensure you are able to inspect all traffic regardless of ports, protocols or file size, decompressing and decrypting every packet and examining every byte to identify threats quickly.
- ☑ Standard sandboxing solutions do not catch encrypted malware since they cannot see inside encrypted traffic. SSL/TLS inspection is a necessity, as is a network sandbox that will block traffic until it reaches a verdict and not only detect zero-day attacks but prevent them in an automated fashion.
- ☑ Add content filtering to keep users from visiting dubious sites, and use a gateway anti-virus and intrusion prevention system to protect them from compromised "good" sites.
- ☑ For organizations who do fall victim to a ransomware attack, before reverting to a backup it's smart to ensure it's a real attack by identifying the name of the ransomware. This is often either presented in the ransom note or discoverable by searching the support email address provided. If identifying the name is difficult, it's worth trying to close out of the screen using Alt-F4 on Windows or Command-W on Mac OS X or forcing the device to restart. The ability to close a ransomware prompt is often a sign the ransomware is fake.[xxxv]
- ☑ Keep all software, including browsers, operating systems and IoT firmware, up-to-date with security patches.
- ☑ Update your security settings to increase browser security levels, disable remote desktop protocol (RDP) and select "Show File

Extensions." Also be sure to restrict Microsoft Office files containing macros.

- ☑ Deploy an enforced endpoint solution so you can detect a system that's been compromised outside the network and flag it for remediation.
- ☑ Apply web browser plugins, such as the NoScript plugin for Firefox/Chrome, to control script execution.
- ☑ Ensure you are using multiple layers of defense and properly integrated products. Start with a security policy that trusts nothing (network, resources, etc.) and nobody (vendors, franchisees, internal personnel, etc.), and add exceptions where needed.

# Final Takeaways

As the cyber arms race continues, the threat landscape is continually shapeshifting. The abundance of affordable and available ransomware makes it easier than ever for attackers to achieve a quick payout. Meanwhile, the number of threat vectors and insecurities within a typical organization are only growing and becoming more entrenched. It's unsurprising that many of today's cyber attacks are launched through email or lurking in the 62 percent of web traffic that is encrypted.

But the good news is today's cybersecurity technology is more than capable of protecting organizations from the vast majority of attacks. Legacy firewalls may only prevent against known threats and early next-generation firewalls (NGFWs) are limited to detecting, not preventing zero-day attacks. But some modern NGFWs are remarkably good at not only detecting but preventing ransomware, data theft and the full assortment of advanced threats.

To be effective against today's threats, firewalls must block files until they can be scanned and found to be innocuous, blocking zero-day threats at the gateway. Since most advanced threats enter organizations through email, sandboxes should extend to cover email security appliances. At the same time, companies must leverage Secure Sockets Layer/Transport Layer Security (SSL/TLS) decryption technology to ensure that zero-day threats aren't lurking in encrypted traffic coming into the network. By utilizing these three separate techniques for finding zero-days, businesses can dramatically improve their security effectiveness over a single-engine approach, making it virtually impossible for malware to succeed.

In order to continue gaining ground against cyber threats, companies of all sizes need to reexamine their security best practices and identify where vulnerabilities may be evident. It's not enough to think like a security professional, you must think like an attacker to truly see where your program is weak.

Start with the following questions:

- Are we segmenting at-risk computers from critical data and services?
- Are we leveraging advanced network detection features, including a multi-engine sandbox that supports automated prevention?
- Do we back up and securely store our critical data offline? Have we performed tests to ensure we can revert to that data if needed? When was the last time we practiced our incident response plan?
- Do we continually monitor and patch known vulnerabilities?
- Do we engage in application whitelisting, only allowing approved programs to run on our networks? Are we limiting the ability for high-risk applications to run on our network?
- Do we have a complete and documented cybersecurity risk analysis for our organization?

**It's not enough to think like a security professional, *you must think like an attacker* to truly see where your program is weak.**

- Which business operations are mission critical, which can we continue without, and how long can we operate without them?
- Do we have an effective "human firewall," including continual training of staff on best practices for recognizing and avoiding spam and malware?
- Have we attempted to hack our own systems? If so, did we address any vulnerabilities we found and add what we learned to our incident response plan? Have we conducted a standard security penetration test on our public-facing portals?

As the malware and attack landscape continues to evolve, security teams will continue to innovate swiftly and decisively to cut cyber criminals off at every turn. The tools that today's businesses need to emerge victorious against cyber criminals are readily available, and as thieves continue to innovate security solutions will continue to evolve in lockstep.

But neither security teams nor cyber criminals are at the center of the battle. The ones in the trenches are the enterprises, SMBs and organizations around the globe that are being targeted by cybercrime on a daily basis. The outcome of this cyber war is up to you. Equip yourself daily with a renewed understanding of the shifting battlefield. Then take up arms and be prepared with a strong and strategic defense.

Over a 25-year history, SonicWall has been the industry's trusted security partner. Only SonicWall can uniquely deliver an end-to-end, automated, real-time breach prevention solution that can manage threats across any delivery vehicle, package type, network and device. SonicWall's next-generation firewalls, high-performance SSL inspection, Capture multi-engine cloud sandbox service, SonicPoint wireless security, email security with encryption and anti-phishing protection, and SSL-secure mobile access are all built upon a block-until-verdict foundation that delivers true automated, real-time breach prevention to help organizations prevent today's advanced threats.

**The complete 2017 SonicWall Annual Threat Report is available online at**
**https://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/**

# Resources

[i] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg Businessweek, March 13, 2014, http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

[ii] Gene Marks, "Why The Home Depot Breach Is Worse Than You Think," Forbes, September 22, 2014, http://www.forbes.com/sites/quickerbettertech/2014/09/22/why-the-home-depot-breach-is-worse-than-you-think/

[iii] Katie Lobosco, "Michaels Hack Hit 3 Million," CNN Money, April 18, 2014, http://money.cnn.com/2014/04/17/news/companies/michaels-security-breach/

[iv] Sienna Kossman, "8 Facts about EMV credit cards," Creditcards.com, December 20, 2016, http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php

[v] Jason Pappalexis, "TLS/SSL: Where Are We Today?", NSS Labs, October 24, 2016, http://www2.nsslabs.com/l/46762/2016-10-17/4fy6lv

[vi] Emily Schechter, "Moving towards a more secure web," Google, September 8, 2016, https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html

[vii] Jason Pappalexis and Jayhendra Pathak, "The Encrypted Web: Part 2 – Malicious Traffic," NSS Labs, December 13, 2016, https://www.nsslabs.com/research-advisory/library/industry/encryption/the-encrypted-web-part-2-malicious-traffic/

[viii] Kevin Townsend, "Did Angler Exploit Kit Die with Russian Lurk Arrests?" Security Week, June 13, 2016, http://www.securityweek.com/did-angler-exploit-kit-die-russian-lurk-arrests

[ix] "Roundup: Ransomware Statistics 2016 [Infographic]," ArmadaCloud, 2016, http://www.armadacloud.com/roundup-ransomware-statistics-2016/

[x] Trevor Mogg, "Hollywood Hospital Pays $17,000 to Ransomware Hackers," Digital Trends, February 18, 2016, http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/

[xi] Bradley Barth, "Lansing, Mich., utility admits paying ransomware demand," SC Magazine, November 10, 2016, https://www.scmagazine.com/lansing-mich-utility-admits-paying-ransomware-demand/article/572180/

[xii] Kat Hall, "VESK coughs up £18k in ransomware attack," The Register, September 29, 2016, http://www.theregister.co.uk/2016/09/29/vesk_coughs_up_18k_in_ransomware_attack/

[xiii] Samuel Gibbs, "Ransomware attack on San Francisco public transport gives everyone a free ride," The Guardian, November 28, 2016, https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

[xiv] "Roundup: Ransomware Statistics 2016 [Infographic]," ArmadaCloud, 2016, http://www.armadacloud.com/roundup-ransomware-statistics-2016/

[xv] "Roundup: Ransomware Statistics 2016 [Infographic]," ArmadaCloud, 2016, http://www.armadacloud.com/roundup-ransomware-statistics-2016/

[xvi] Lansing Board of Water & Light, "Board meeting Agenda," November 15, 2016, https://www.lbwl.com/uploadedFiles/MainSite/Content/About_the_BWL/BWL_Governance/Minutes_and_Agendas/Packets/bwl_Nov2016_mtg_pkt.pdf

[xvii] Doug Olenick, "Cyberattack knocks Lansing utility offline," SC Magazine, April 28, 2016, https://www.scmagazine.com/cyberattack-knocks-lansing-utility-offline/article/528577/

[xviii] "Huge wave of Locky Ransomware spread via JavaScript spam," SonicWall Security Center, February 19, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=901

[xix] Timothy Weaver, "Ransomware-as-a-Service Takes 20%," MajorGeeks, August 17, 2016, http://www.majorgeeks.com/news/story/ransomware_as_a_service_takes_20.html

[xx] Allen Scott, "These are the World's Top 10 Bitcoin-Friendly Countries," Bitcoin.com, March 29, 2016, https://news.bitcoin.com/worlds-top-10-bitcoin-friendly-countries/

[xxi] "Top-10 countries by directly connecting users," TorMetrics, https://metrics.torproject.org/userstats-relay-table.html?start=2016-01-02&end=2016-12-01

[xxii] Swati Khandelwal, "World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices," The Hacker News, September 27, 2016, http://thehackernews.com/2016/09/ddos-attack-iot.html

[xxiii] Nicky Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, October 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[xxiv] Darrell Etherington, "Large DDoS attacks cause outages at Twitter, Spotify and other sites," TechCrunch, October 21, 2016, https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

[xxv] Adrienne LaFrance, "How Much Will Today's Internet Outage Cost?" The Atlantic, October 21, 2016, http://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/

[xxvi] John E Dunn, "Android Marshmallow's 10 most important security features," Techworld, September 30, 2015, http://www.techworld.com/picture-gallery/security/android-marshmallows-10-most-important-security-features-3626468/

[xxvii] Al Sacco, "Google details security features in Android 7.0 'Nougat,'" CIO, August 16, 2016, http://www.cio.com/article/3108382/android/google-details-security-features-in-android-7-0-nougat.html

[xxviii] "Android Banker steals credit card information and targets certain banking apps," SonicWall Security Center, March 7, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=906

[xxix] "Malicious banker tries to bypass Android Marshmallow security barriers," SonicWall Security Center, September 16, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=967

[xxx] "Android Ad campaign HummingBad infects millions of devices," SonicWall Security Center, July 8, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=944

[xxxi] "Metasploit enhanced Android malware spotted in the wild," SonicWall Security Center, April 15, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=920

[xxxii] "New Android Lockscreen campaign spotted in the wild," SonicWall Security Center, May 12, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=929

[xxxiii] "Self-installing porn apps rampage the Android ecosystem," SonicWall Security Center, June 17, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=940

[xxxiv] "DressCode Android malware equipped to infiltrate corporate networks," SonicWall Security Center, October 21, 2016, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=978

[xxxv] Fahmida Y. Rashid, "How to tell if you've been hit by fake ransomware," InfoWorld, April 29, 2016, http://www.infoworld.com/article/3062552/security/how-to-tell-if-youve-been-hit-by-fake-ransomware.html