2016 CTAP

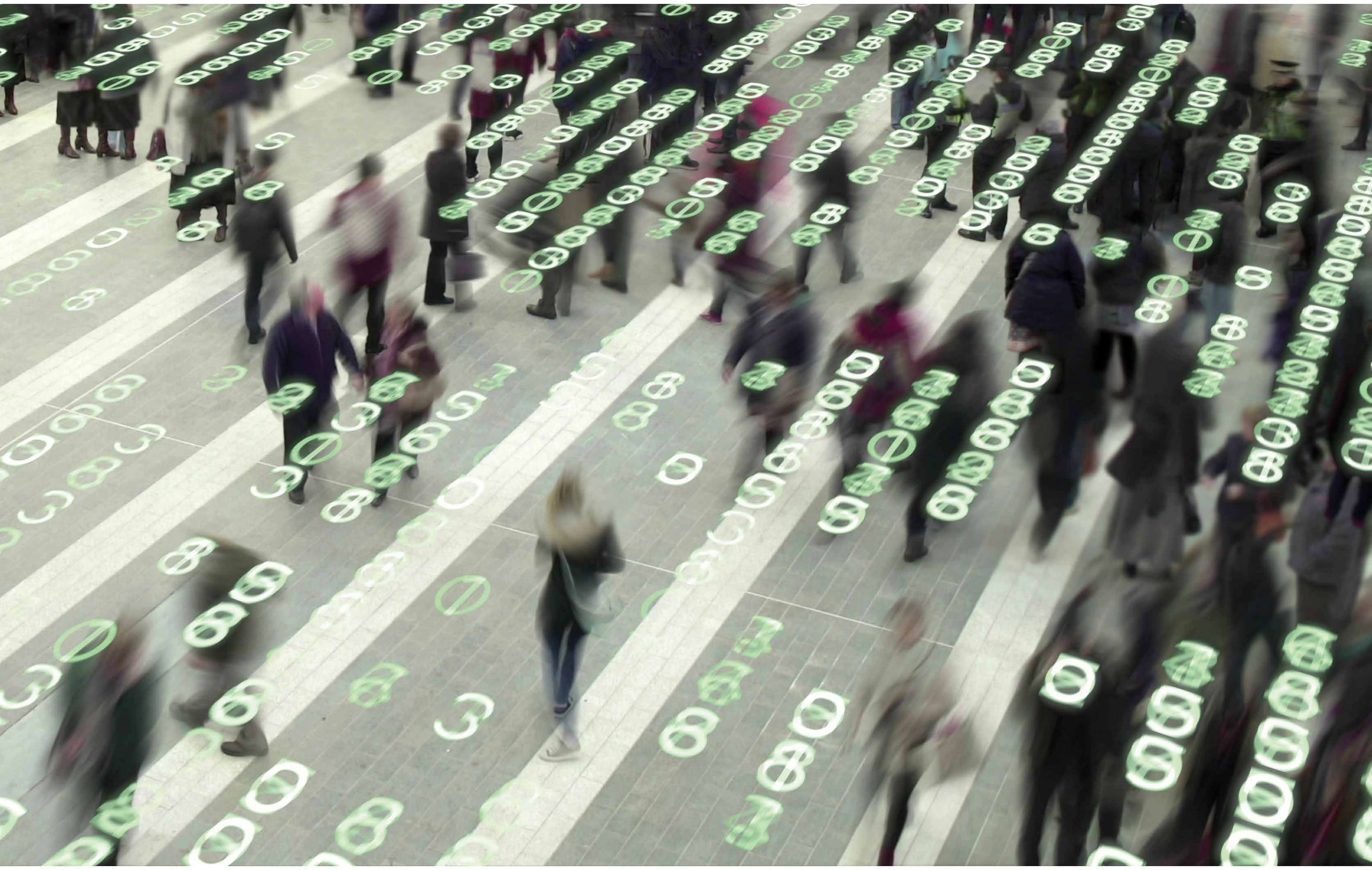
Threat Landscape Report

Foreword

Cyber criminals and other threat actors continue to push forward with new tricks and tools to gain access to vulnerable networks and lucrative corporate data. The threat landscape moves very quickly—making it difficult for security teams to keep up, let alone respond. It's a perfect storm: the growth of threats combined with the rapid expansion of devices utilizing network resources means that the job of protecting both businesses and the data housed inside becomes a seemingly herculean feat.

While the headlines about yet another data breach continue to grab our collective attention, what is frequently overlooked is the long-term impact to a business—both quantitatively and qualitatively. Avoiding breaches entirely does not appear to be a realistic goal; it's just not possible to eliminate every single source of risk or vulnerability in today's complex enterprise networks.

Enterprise networks urgently need solutions that provide high-performance and comprehensive threat protection across every facet of the attack surface. Solutions must be seamless, easy to manage, and provide complete visibility into every corner of their infrastructure. With those goals in mind, enterprises will be able to respond to security incidents with agility - and be uniquely prepared for the future demands of their business.



The Fortinet 2016 CTAP Threat Landscape Report

Introduction

In today's breakneck world of information security, it is paramount that both security staff and executives who are responsible for maintaining the security of their networks to stay current on the types of threats, incidents, and traffic impacting their networks. The threat landscape continues to evolve – what was an effective strategy last year may no longer apply today.

Beyond that, the demands on your infrastructure continue to expand at greater and greater speeds: today's threat landscape is making unprecedented demands on your network. Content, applications, and transactions all require incredible amounts of bandwidth and room to grow into the future. Coupled with the regular demands on your network, it's clear that securing all of this information and data is no easy feat.

The data used in this report was obtained from Fortinet customers and prospective customers as part of our Cyber Threat Assessment Program (CTAP). This data was collected from within live production environments all over the world and consists of millions of events and incidents. More information on the data collected can be found in the Data Methodology section of this report. This report focuses on key metrics from the following verticals:

- Education
- Finance & Finance-related Businesses
- Technology
- Healthcare

Additional data is provided that focuses on company size. In the following pages, we present specific data showing the types of attacks attempted on these networks and other key findings that we believe are of interest.

Key Findings

- Enterprises of every size and any specific area continue to face a multitude of threats from every area and type.
- Attackers have been able to rapidly build up automated systems and tools to probe networks for exploitable vulnerabilities, especially well-known ones that are easy to scan for (like Shellshock, Heartbleed, etc.)
- The majority of malware threats we see in live customer environments continue to depend on two key areas for delivery: malicious content delivered through web browsing, and through email attachments or links leading to malicious content.
- As predicted in earlier reports, botnets such as ZeroAccess, which were the focus of concerted efforts to defeat, have made a significant effort to rebuild and infect machines. The financial incentives for these bot owners are massive, and this trend should continue.
- Advertising content continues to be both a source of significant traffic passing across enterprise networks today, and has been shown to be a potential source of malware as third-party advertising networks are subverted or tricked into delivering malicious ads.
- Application control appears to be a continual challenge for administrators. We continue to see a significant amount of peer-to-peer traffic, primarily BitTorrent and gaming activity. Enterprises should exercise significant caution when building application control policies on their networks—the legal liability around unintentionally allowing employees, customers, or users to use their networks to retrieve or share potentially infringing/copyrighted content is very real. Further, we have seen in our research malicious content being piggybacked on top of applications and files downloaded through many popular torrent sites.
- Social media applications, both in the browser and via mobile applications, continue to eat up a significant amount of network resources, with Facebook being the largest by a wide margin. It is important for administrators to understand that due to the ability for content to rapidly spread through these channels, coupled with a general lack of knowledge and understanding among users, malicious content can reach end users quite rapidly.
- Other sources of drain on networks continue to be multimedia; YouTube and other video sources continue to eat up large amounts of traffic entering enterprise networks. Enterprises are faced with two choices: either block it all or ensure that you have the infrastructure to handle the traffic. You must have security technologies in place that allow your users to safely access the content they want and need, as well as the throughput to successfully monitor all the traffic passing through.

Overall Stats

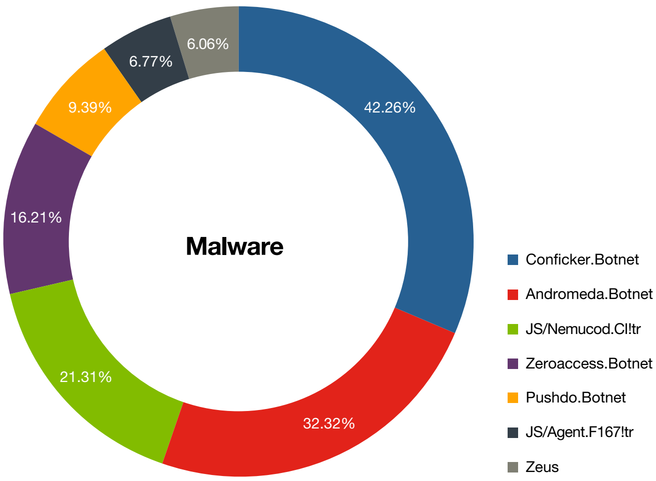
Overview

- **32.14 Million Attempted Attack Events:** It's clear that enterprises of every size and vertical continue to face a constant and consistently hostile landscape.

On a whole, threats on networks come from many different sources. Botnet activity continues to be a significant cause for concern for every vertical, as well as companies of every size. Botnet owners that use multiple methods to build their armies and campaigns to expand their footprint are seen on a regular basis. Malware continues to be spread via two key vectors: email and web traffic. We did notice other vectors such as infection attempts via instant messaging platforms, but this was much smaller in scale.

Malware

- **71 Different Malware Variants Detected:** Utilizing increasingly sophisticated campaigns to expand their footprint, botnet activity is still dominant and a significant concern for security teams.

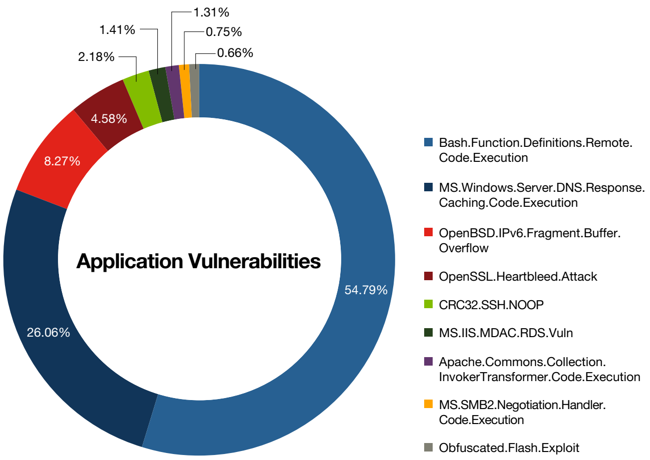


As the above chart shows, overall malware traffic seen passing through enterprise networks is heavily weighted toward bot activity. This is not surprising: many bots are excessively "chatty," making the opportunities to detect their activity plentiful.

Nemucod is an interesting standout among all the malicious infections: in the latter parts of 2015 this Trojan was being used in campaigns to distribute the most recent versions of disk encrypting ransomware. Variants such as Teslacrypt and Cryptolocker were seen being distributed via Nemucod.

Application Vulnerabilities:

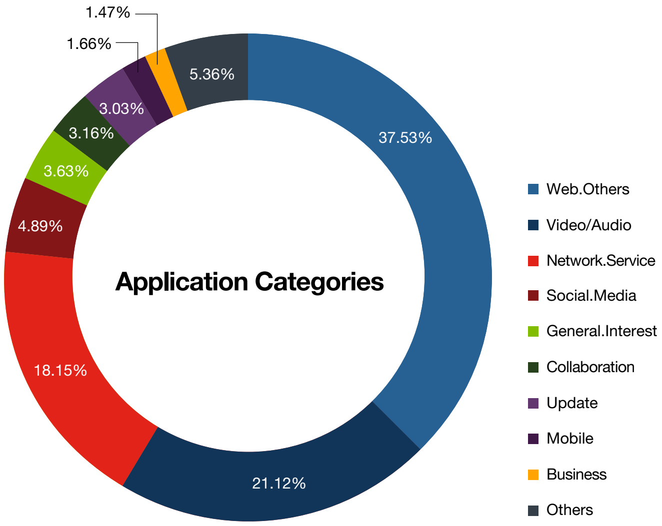
- **357,420 attempts to compromise applications** were detected within the top-10 list of application vulnerabilities alone.



Among all participants in this report, we saw a massive number of attempts by attackers to scan for and exploit the Shellshock vulnerability. Shellshock was a vulnerability in the ubiquitous Bash program that can allow an attacker to remotely execute arbitrary code on a vulnerable system. Bash is commonly used in many Linux, Unix, and Mac OS X systems.

Application Categories

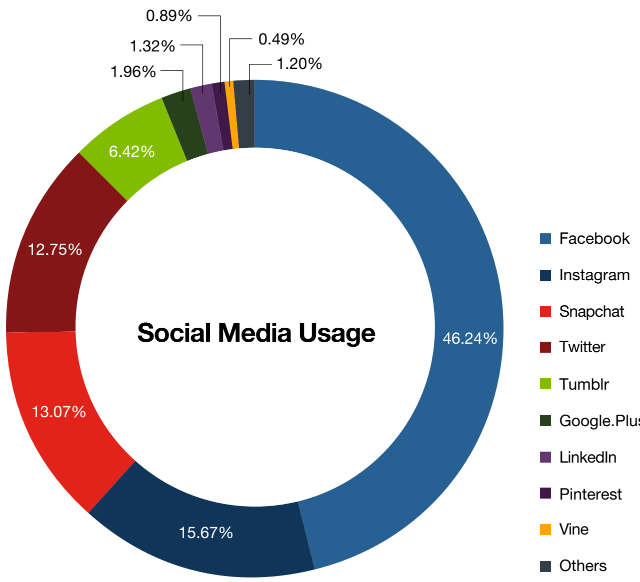
- **26.01% of network traffic is used to browse social media or stream video and audio.** Fortunately, the rest of the traffic is put to productive uses like cloud-based applications, email, and system updates.



Across all company sizes and verticals, traffic passing through networks shows that the single largest category of traffic was considered "other" web traffic. Our analysis of this traffic showed that the majority of this traffic was directly related to the day-to-day operation of the business. In-house applications, cloud-based traffic, and other business intelligence applications were the largest piece of this. From a threat perspective, enterprises must maintain a constant state of vigilance to ensure those applications remain up-to-date, patched from all known vulnerability issues, and (unless absolutely necessary) hosted on segments of the network that are not accessible from the public Internet. Of particular interest among the collected data is the fact that a full one-quarter of all traffic passing through these networks was multimedia and social media applications. This massive amount of traffic can be of concern to administrators who struggle with throughput on their networks.

Social Media Usage

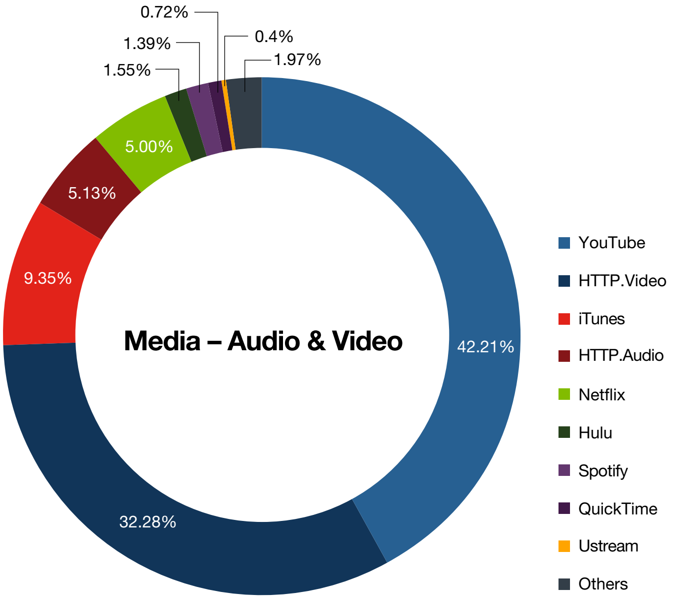
- **Facebook represents 46.24%** of all social media traffic, while most major social media platforms are accessed by users at work. .



Virtually all of the major social media platforms were seen across all networks, with Facebook taking up almost half of the share of traffic. Threats and attempts to exploit users via social media channels are a common and very real worry for security administrators. The best suggestion for organizations around social media continues to be creating awareness and knowledge as to the threats that can be delivered via social media. Twitter bots, malicious Facebook apps, and other scams pop up on virtually everyone's social media feeds. On a vulnerable system, it can only take a split second for a user to mindlessly click on a story offering a free $100 gift card from some major retailer. Once clicked, they're redirected to a watering-hole server and are delivered malware.

Media – Audio & Video

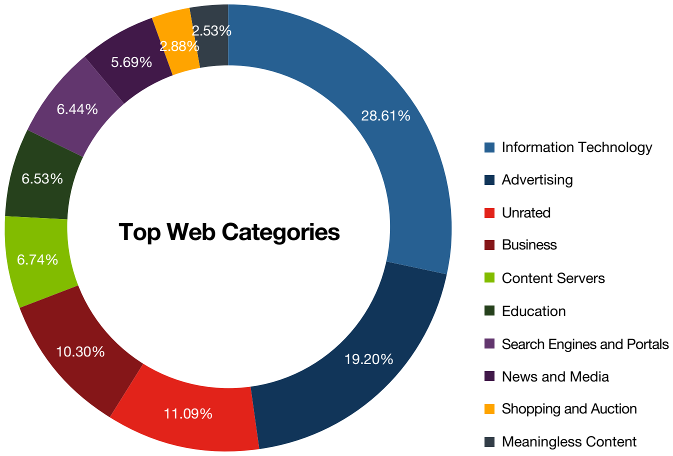
- **YouTube makes up 42%** of streamed video/audio content on corporate networks. Video content served via HTTP combined with YouTube, Netflix, Hulu represent **80% of all video/audio streamed** within the workplace.

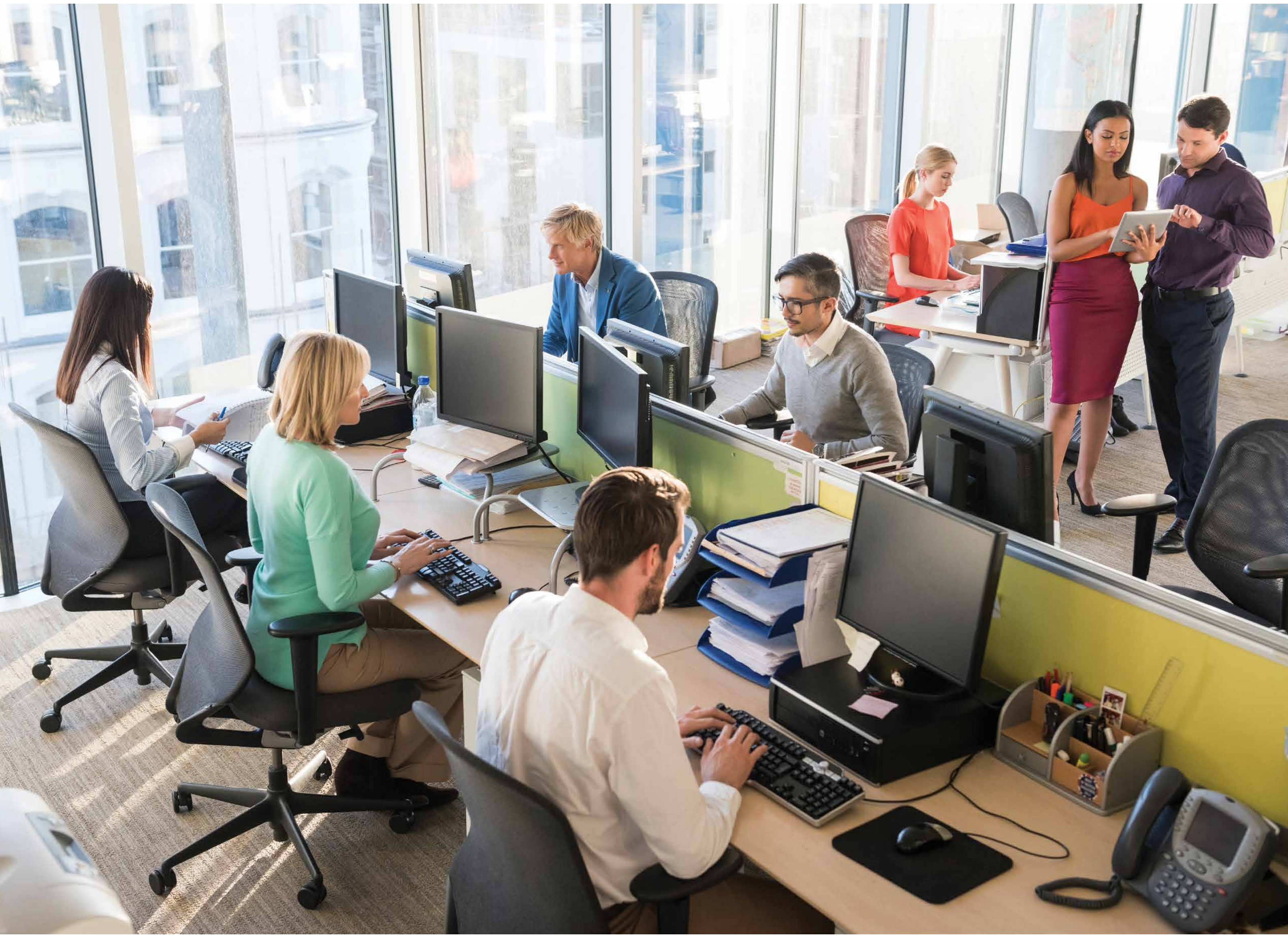


Three-quarters of all the media traffic passing across all participants' networks during this period was video traffic from both YouTube and other web sources. While not malicious in of itself, the impact on corporate network performance can be substantial, slowing other applications and needs to a crawl.

Top Web Categories

- **19.2% of traffic consists of advertising.** While difficult to avoid while browsing the Internet, advertising-based attack strategies have risen in popularity in recent years.



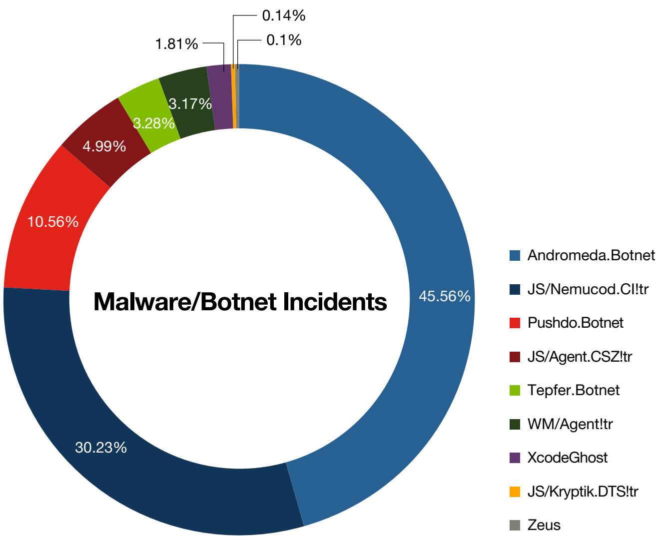


Stats by Company Size

Small Businesses - Overview

In this report, we define small business as companies and organizations consisting of fewer than 100 employees. Because of the small number of employees, it can be very difficult to have enough resources to protect everyone. IT staff size is small and is usually required to wear many hats in the business—security is just one of many key pieces of an IT admin's function in a small environment. Unfortunately, this can lead to gaps in defences. If an incident occurs and causes damage, the impact to the business can often be insurmountable.

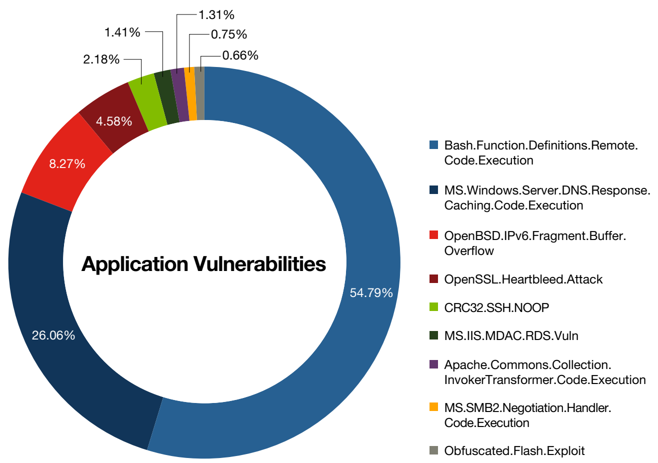
Malware/Botnet Incidents



Late in 2015, we saw a spike in W32/Bayrob Trojan infection attempts. Bayrob in its many variants has been around for years, but that hasn't stopped attackers from attempting to use it to gain access to systems. Like many Trojans, Bayrob is typically delivered via infected attachments inside emails, using impersonation to entice victims to open the malware. Like many other Trojans, Bayrob is used to gather as much information about the target system as possible, including credit card information and banking credentials. For attackers, grabbing hold of this information can prove incredibly lucrative—there have been many cases of tens of thousands of dollars being stolen and transferred overseas before the business can respond. In the case of smaller businesses, that kind of loss may not be something they can recover from.

Almost half of the malware threats reaching small businesses during this period were related to malware used to deliver Cryptolocker-style malware. This particularly nefarious family of malware will encrypt the contents of the victim's entire hard drive (and often any writable network shares the victim has access to). Once the data is encrypted, it is almost always impossible to decrypt unless the victim pays a ransom to the attacker via hard-to-trace payment methods like Bitcoin or pre-paid credit cards. In the case of smaller companies and organizations, losing access to key data may be unacceptable and very difficult to recover from, leading these companies to begrudgingly pay out the ransom in order to regain access to their irreplaceable files and data. It is absolutely critical for small business owners to have cold backups of their data made on a regular basis. The backups must be created on a regular basis and not left connected to critical systems. In many cases even an external hard drive via USB that is plugged in every Friday afternoon and removed when files are transferred can be enough to get your business up and running quickly.

Application Vulnerability Exploits

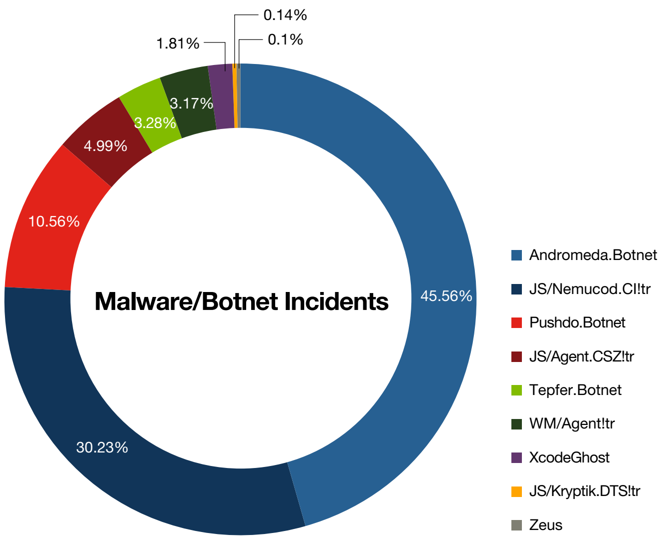


Looking at the types of application vulnerabilities and exploits used by attackers on small businesses over the course of the report period, we see some very common threats used: Shellshock, attacks against OpenSSL, overflows, and SQL injections led the charts. These attacks are predicated on the fact that small businesses can find it difficult to rapidly respond to and mitigate application vulnerabilities based on third-party issues. Even worse, due to the demands on IT staff, companies may not even have full visibility to all of the applications facing the Internet. Attackers only need to find a small crack or fissure in your network to gain traction and begin to move. These types of weaknesses are simple to exploit and can be easily scanned for by hackers who are looking everywhere on the Internet for vulnerable systems.

Mid-Sized Businesses - Overview

We consider mid-sized organizations to have more than 100 and fewer than 1000 employees. Mid-sized companies face similar issues that smaller businesses have when it comes to security resources: many do not have staff solely dedicated to security. Their infrastructures may be haphazardly or casually built, leading to potential gaps in security coverage and an incomplete visibility of every corner of their network.

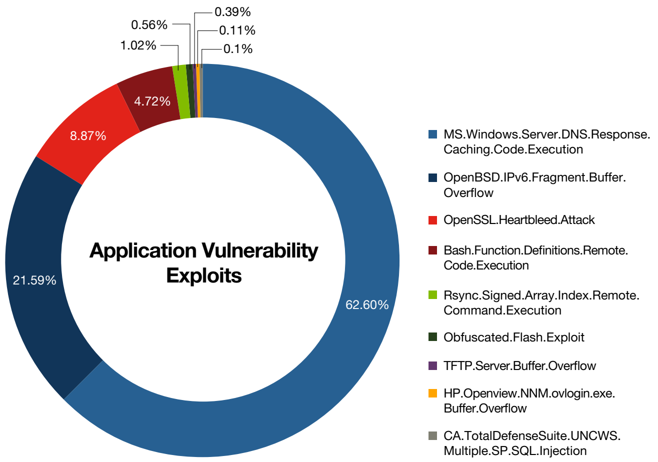
Malware/Botnet Incidents



As mid-sized businesses come in every shape, size, and function it makes sense that we'd see a varied amount of malware and bot incidents: from botnet infections, to web-based threats, to executable malware usually delivered via email—all major attack vectors are represented in this group. Of particular note in this segment is the appearance of the iOS

XcodeGhost malware that appeared last year. We will go into further detail on XcodeGhost later in this report.

Application Vulnerability Exploits

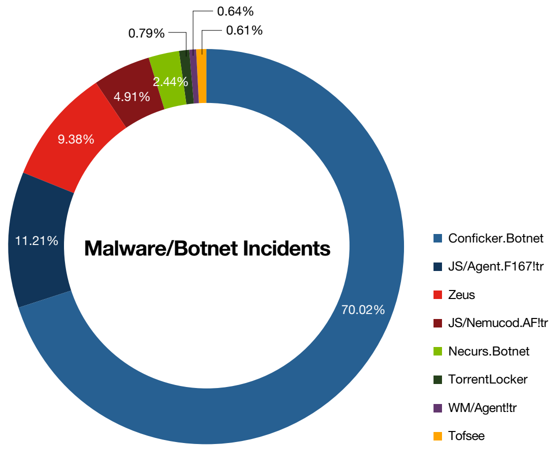


Microsoft released a security update and related bulletin (MS15-127) late in 2015 to address a critical vulnerability found in Windows Server products being used as DNS servers. As many businesses use Microsoft Windows Server products in multiple roles (Active Directory Services, web servers, DNS, etc.), the potential impact on servers was substantial. Our appliances detected a massive spike in attempts to scan for and exploit unpatched Windows Server installations in the hopes of finding public facing machines being used as DNS servers. Issues like these, while not detected in the wild prior to patches being made available, reinforce the message that IT staff must remain on top of security updates in order to deploy them as soon as possible. In the window between patches being made available and patches being installed, it is crucial that your security infrastructure be watching for probes, scans, and threats built around these vulnerabilities.

Large Businesses - Overview

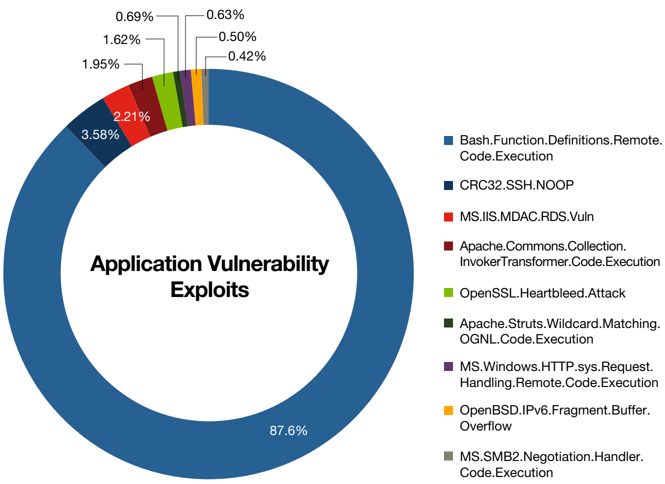
For the purposes of this report, we define large businesses as any organization with more than 1000 employees. Typically these businesses have more robust defences, and dedicated IT staff focused on security. But even with a more evolved defensive posture and more resources, it can be a daily challenge for IT staff to protect users and infrastructure from attack. And what about the difficulty in ensuring you have complete visibility to every device and application on your network, as well as being aware of every ingress and egress point to the Internet? It can be a hard challenge for teams to maintain complete control over their environments.

Malware/Botnet Incidents



As we saw with mid-sized organizations, attacks are varied and cover all the common vectors. Botnet infections and attacks continue to be seen in enterprises, and due to the large scale of enterprise networks, can take some time to remediate. Other key incidents of note were attempts to install the stalwart ZeuS Trojan and campaigns to install malware via malicious web content.

Application Vulnerability Exploits



As we've seen in other cases, attackers are scanning wide swaths of publicly addressable IP space looking for unpatched machines. Their focus is on the well-documented open source vulnerabilities in OpenSSL, SSH, Bash, and other products. It is critical for enterprises to deploy security protections immediately after these issues become public knowledge while they wait for a window to patch their systems. Attackers are quick to build automated tools to find unpatched machines and use them as an initial vector into an enterprise.

Focus on Select Key Verticals

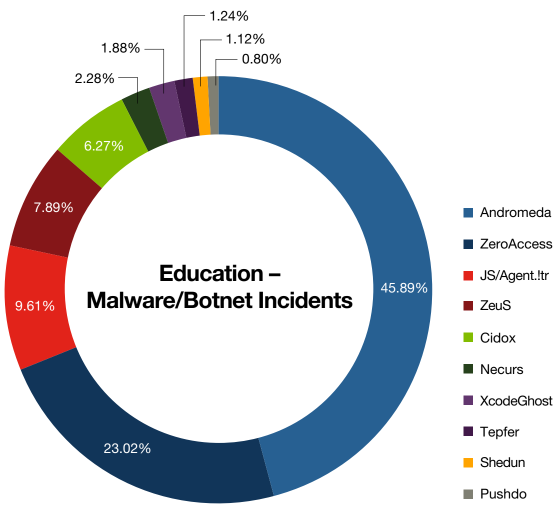
Education

Overview

- Education Organizations represented 27.4% of all attack events in this report and came in second for overall malicious network activity.
- 7 of the top 10 threat incidents were botnets like Andromeda and Zeroaccess.

Our findings show that attackers continue to use a varied toolkit in the hopes of gaining access to the networks and data of schools and universities. Universities are likely to be most at risk of attack due to the sheer size of their infrastructures and threats from both inside and outside their environments. From curious students trying to virtually explore or cause mischief, to foreign actors looking to abscond with research data, to cyber criminals hoping to steal computing resources to mine cryptocurrencies—educational organizations can find themselves in an incredibly hostile environment and under constant assault.

Malware/Botnet Incidents

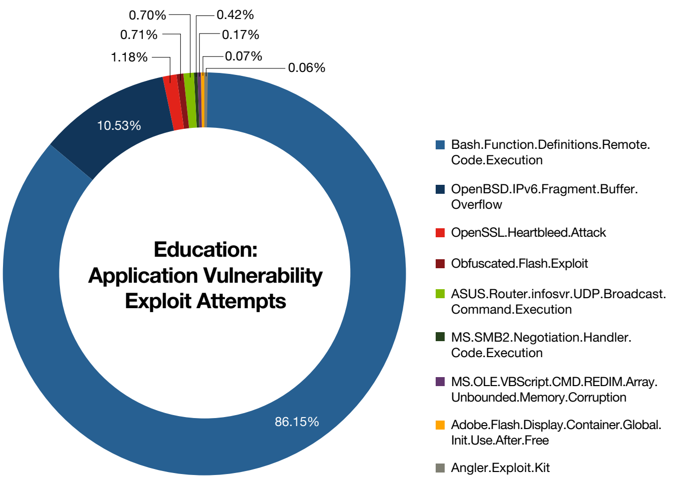


Of the top ten infections we saw inside education environments, seven of them were bots. Leading the list were the stalwarts Andromeda and ZeroAccess, both of which have been incredibly active and prolific over the past few years. As we predicted in previous Threat Landscape Reports, the attempts to silence ZeroAccess would prove to be only temporary; the actors behind ZeroAccess have been able to make a lot of income off of infections. It was reasonable to assume that they would rebuild their bot armies as quickly as possible.

ZeuS continues to infect many thousands of hosts. Unfortunately, awareness and good security habits among both students and staff were likely the key vector of infection: people continue to click on links and attachments in emails that led to compromise.

Perhaps the most interesting piece of information inside the collected data was the appearance of iOS malware XcodeGhost. Late in 2015, researchers discovered malware targeting Apple iPhone and iPad users. The vector of infection was unique, especially considering Apple's industry-leading efforts to keep iOS applications free from malicious code. XcodeGhost was determined to be the result of iOS developers unintentionally downloading a version of Apple's Xcode Integrated Development Environment (IDE) and creating their applications using the modified environment. Unfortunately, these apps were able to make it through Apple's review process and were made available for download on the AppStore. The messaging and chat application WeChat was one very notable victim of XcodeGhost—and literally hundreds of millions of users are users of WeChat.

Application Vulnerability Exploit Attempts

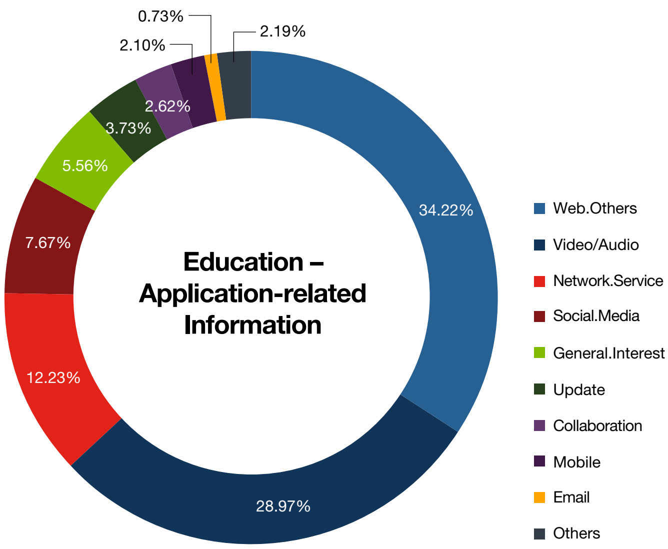


2015 had no shortage of new exploits and vulnerabilities uncovered, but attackers continued to use older vulnerabilities in the hopes of gaining a foothold inside networks. Shellshock appeared late September 2014 and is used by many systems. Thankfully many organizations were quick to patch their affected machines—the very real danger of another SQL Slammer-style worm was legitimate. Attackers almost 18 months later continue to scan the Internet looking for unpatched machines to infect, all the more reason to ensure that all the machines in your infrastructure are quickly and rapidly patched.

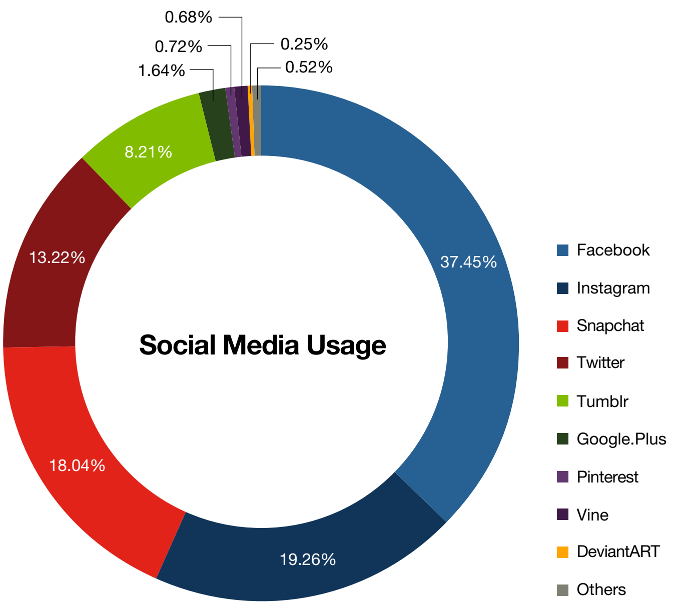
Application-Related Information

As one would expect in an Education environment, we saw a significant amount of data being consumed for entertainment purposes. All of the major social media platforms were in active, regular use and media streaming consumed almost a full third of traffic crossing Education networks. Gaming and peer-to-peer (as well as other traffic) consumed a major chunk of bandwidth—again, not entirely unexpected in these environments.

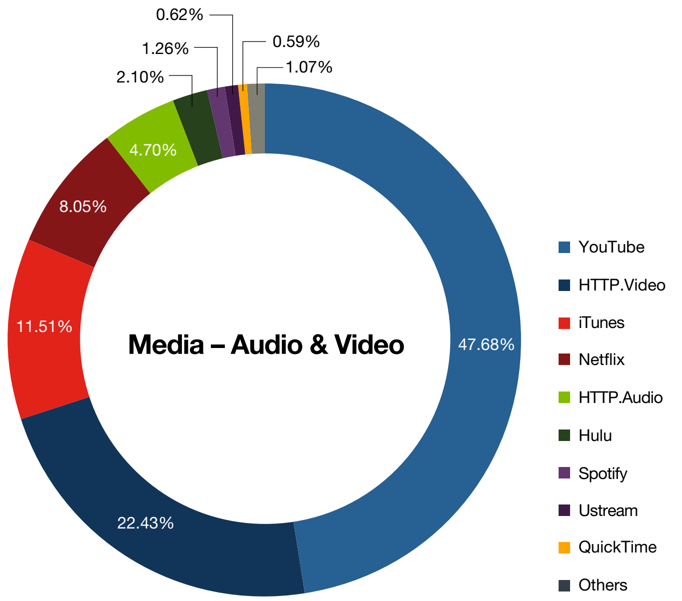
Application Categories



Social Media Usage



Media Streaming



Banking/Finance/Insurance/Consulting

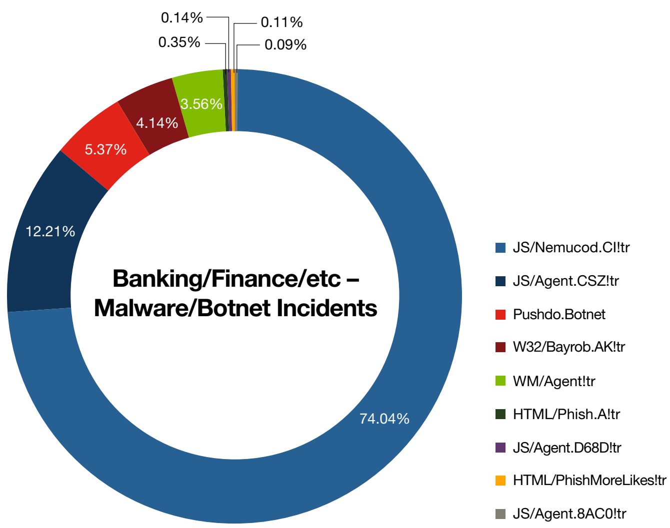
Overview

- 44.6% of all malicious activity was targeted at the Banking and Finance industry.
- The Nemucod Trojan accounted for 74% of all malware activity in the top 10 threats.
- The data demonstrates an emphasis on land-and-expand attack strategies designed to infiltrate and persist within the network.

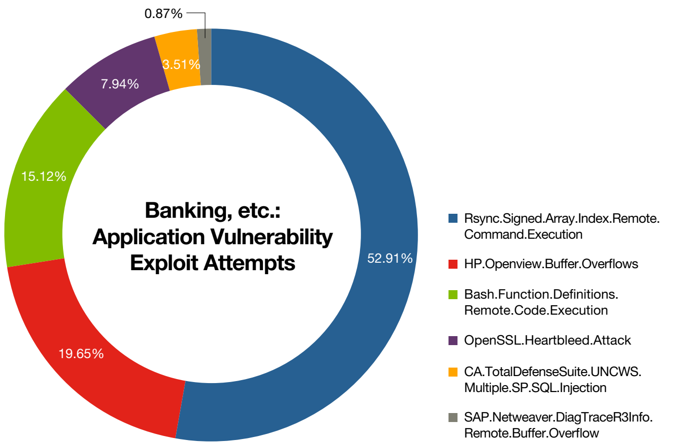
In the case of organizations working in the world of banking, finance, and other related industries, we found that attackers used much different tools and methods in their attempts to gain access or deliver malicious code. As you might expect in environments such as these, the largest volume of attacks we saw were attempts to exploit enterprise applications such as those provided by HP and SAP. Of course, as with virtually every industry connected to the Internet today, phishing attacks, malicious web code and botnets also were seen in significant volumes. Attackers will often use these methods as a way of casting a wide net in the hopes of hooking something of significant value, or using those initial compromises as ways to gain traction inside a network and begin their explorations.

Malware/Botnet Incidents

The Nemucod Trojan was the largest threat detected in these networks, and that does not seem out of place here: Nemucod is often used as an initial infection and used to pull down other infections. Nemucod was being used late in 2015 to spread ransomware as part of a massive campaign detected by Fortinet and many other security vendors. A typical Nemucod infection attempt is sent using email as the attack vector. The emails will usually contain an attachment such as a receipt or invoice, in the hopes that an unwitting victim will open the attachment and launch the malware.



Application Vulnerability Exploit Attempts



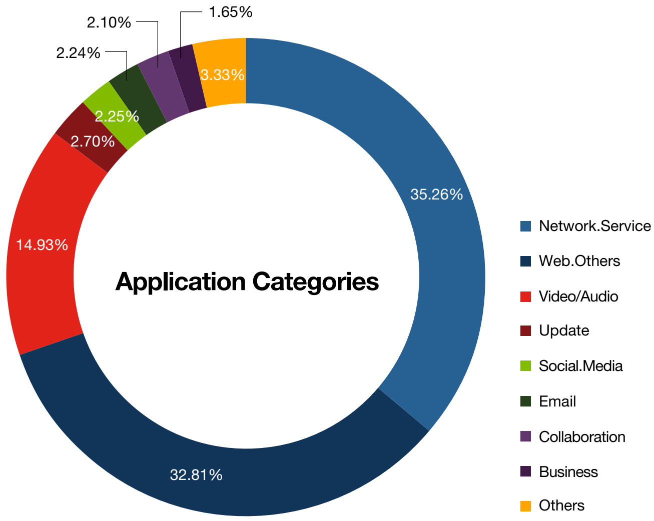
As you can see in the chart above, attempts to exploit vulnerabilities in applications were largely focused on two key areas: big name attacks like Shellshock and Heartbleed and enterprise-level applications. We can infer two key points from this information: attackers are scanning as much IP space as they can looking for vulnerable systems that have not been patched (such as older vulnerabilities like the rsync RCE), and they are likely using automated tools to do so.

Perhaps the question we should be asking is why are attackers attempting to exploit a decade-plus-old vulnerability that should have been patched long ago? In many enterprises, administrators have been forced to maintain very old legacy systems that they have been unable to replace. Many of those systems have had support long since abandoned by vendors, leaving them to fend for themselves. Security staff must pay close attention to the potential of these specific applications and servers and properly protect them from external access.

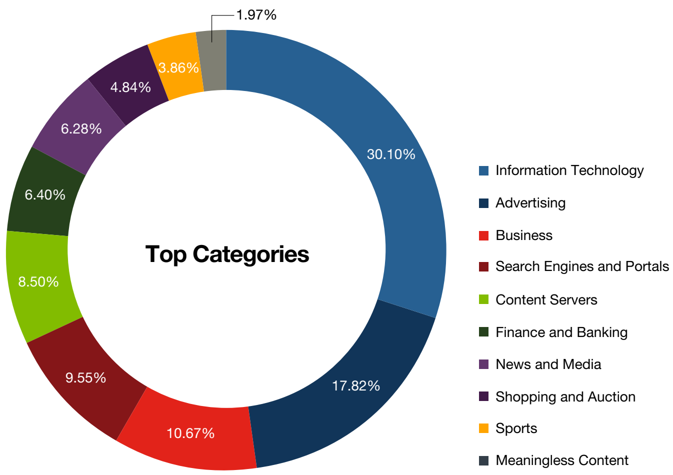
Application-Related Information

As is common in most enterprises and corporations today, a large portion of traffic coming into networks is purely advertising content that is served along side other web traffic. A significant portion of traffic seen was being used to access internal and external business intelligence or other related assets. Ensuring you have complete visibility to all the applications traversing your network can be of critical importance to building an effective protection strategy.

Application Categories



Top Categories



Technology

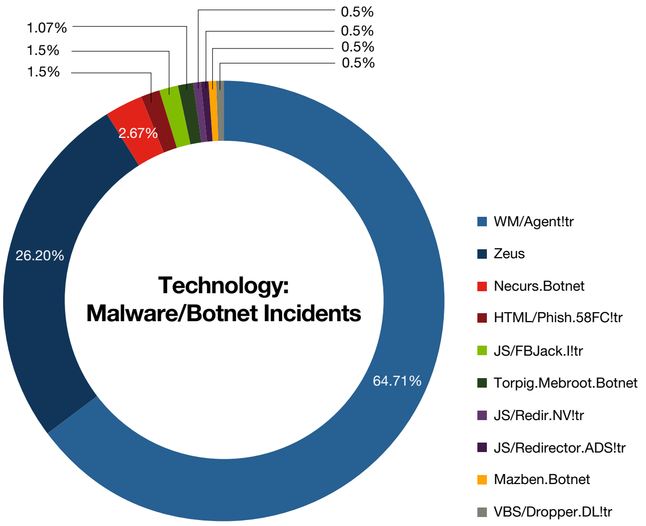
Overview

- The Technology Sector shared only 1.1% of overall attack activity.
- Shellshock and Heartbleed top the list of the most prevalent application vulnerabilities that affect technology industry networks.
- Trojans were again the primary tools employed by hackers.

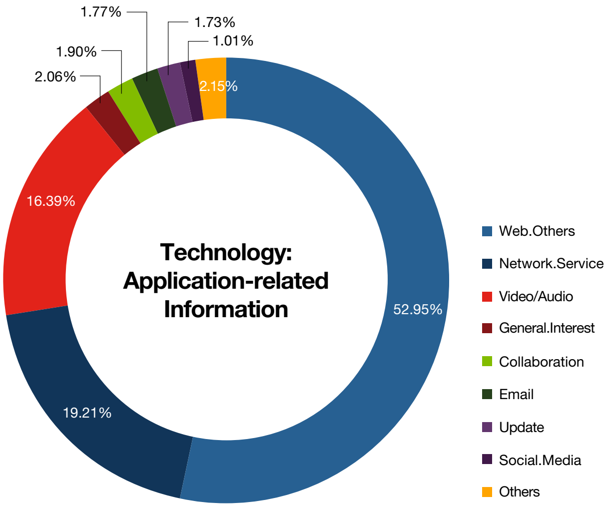
Similar to the events detected and seen with financial organizations, companies providing technology solutions found themselves under continual scan and attempts to exploit Shellshock and Heartbleed topped the list. We saw a large number of attempted attacks occurring via email delivery, which still remains one of the most common vectors used by attackers today. Browser-based attempts rounded out the list.

With the impact of a breach or successful attack, hackers will often scan and probe IP spaces belonging to technology companies in the hopes of finding a wayward system deployed without protection or using unpatched versions of software. Once they've found a system, they can gain a beachhead inside the company and begin to plan further movement and attack throughout the network.

Malware/Botnet Incidents

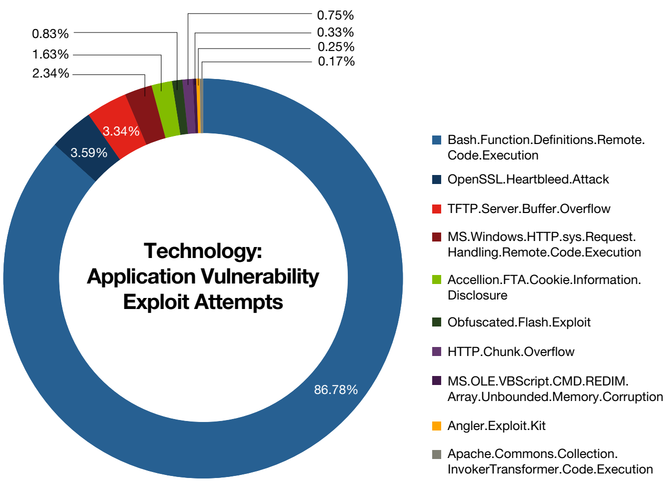


Application-Related Information

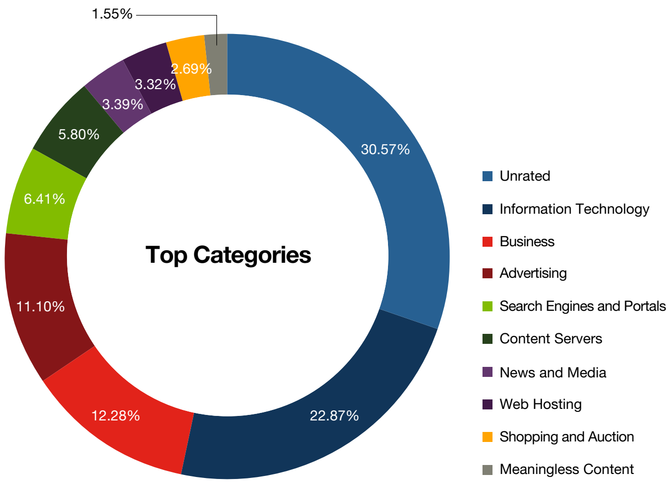


Application Vulnerability Exploit Attempts

Companies in the technology sector are seen as high-value targets for attackers, mainly because of the potential for massive bounty: invaluable intellectual property, huge troves of personal information, email archives, and other proprietary information that may be worth a substantial amount of money to the right buyer.



Top Categories



The data shown here shows clearly that the technology organizations that participated have invested substantially in in-house business solutions to allow their employees to complete their day-to-day tasks. We saw both cloud-based and inside the network applications being used by the participating companies. Like other verticals, though, both advertising traffic and multimedia use a sizeable percentage of available bandwidth.

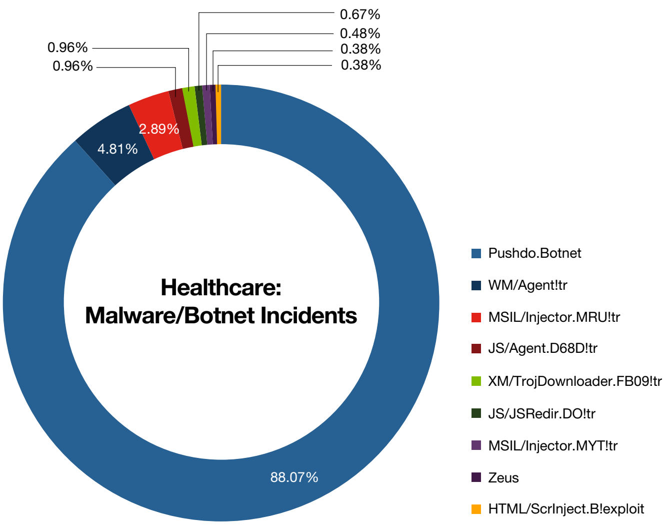
Healthcare

Overview

- Healthcare ranked third in overall malicious activity with 10.6% of attack events.
- The healthcare industry is unique in the appearance of automated exploit kits, namely Angler and Nuclear, both have been tied to the delivery of far-reaching and lucrative ransomware campaigns like TeslaCrypt and CryptoWall 4.0.

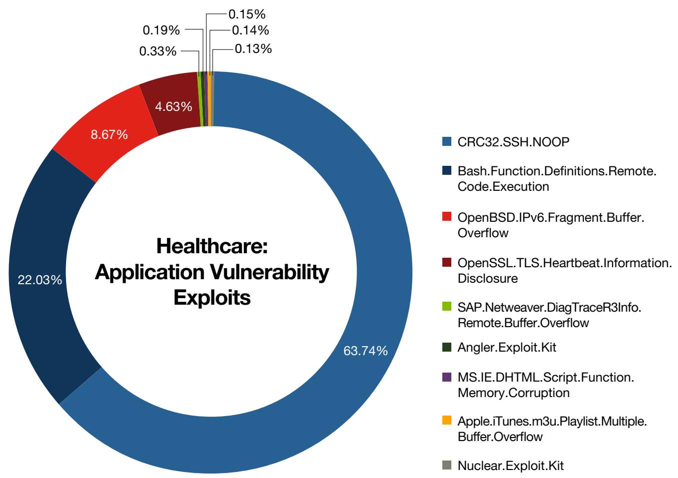
The security needs of businesses working in the healthcare vertical are unique in comparison to other sectors: unique regulatory frameworks, the extreme sensitivity of patient and diagnostic data as well as an abundance of IoT devices all lead to a large attack surface and incredible potential for loss.

Malware/Botnet Incidents



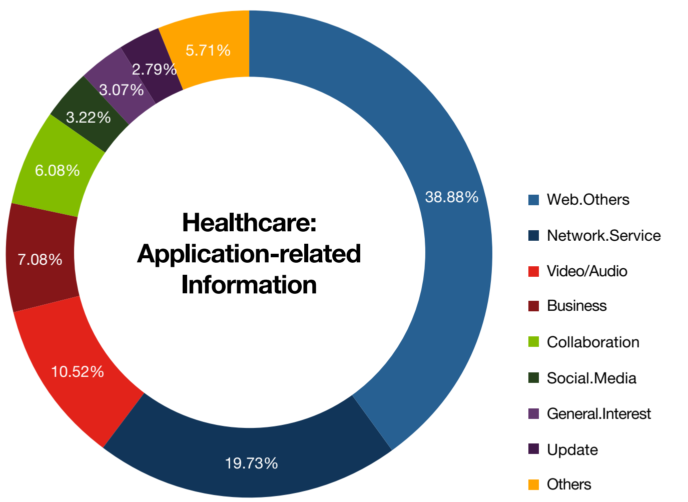
One participant was victim to a botnet attack that took some time to remediate. This led to a massive skewing of the data collected. If we ignore that outbreak, we see that the remainder of incidents recorded among the other participants shows a large trend towards information stealing malware and Trojans, likely in the hopes of gaining access to healthcare records. Healthcare records can fetch a substantial premium in the underground markets over other data like credit cards. The information contained inside healthcare records can be used for many purposes, including impersonation in order to commit financial fraud. Healthcare IT must pay special heed to ensuring that the data they are the shepherds of is adequately protected.

Application Vulnerability Exploit Attempts



The CRC-32 compensation attack isn't new. In fact, it's well over a decade old. This vulnerability affected a large number of systems and vendors, and patches were made available reasonably fast at the time. That being said, even now some SSH implementations still allow some measure of fallback to older versions of the SSH protocol to ensure compatibility of all SSH clients. Penetration testers, of both the white- and black-hat varieties, will often include checking for this vulnerability when scanning networks in the hopes of finding an ancient machine or networking device with SSH exposed to the Internet. As exploit code has been available for a long time, it is a trivial matter to exploit the device and gain access. Situations such as these make it critical for all security staff to have complete visibility to every asset on their network, and to conduct regular penetration audits on their own infrastructure.

Application-Related Information



When you consider how busy most staff and employees working in healthcare environments are, it is no surprise to see social media usage low. Over half of the traffic seen in our data was IT- and device-related networking traffic as well as internal applications. It is important for healthcare facilities, as they embrace providing better connectivity for patients and visitors, to prepare for a growth in other traffic types in the future: proper network segmentation and adequate bandwidth will be essential to ensure healthcare networks can scale to match the demands that are asked of it.

Recommended Actions

The data highlighted in this report clearly shows that organizations of all types face threats from all angles on a continual basis. Attackers are targeting companies of every size in the hopes of gaining access to the valuable assets inside the network.

With that in mind, we offer a few recommendations:

- Identify all the legal requirements facing your specific business. Do they require specific security controls or technologies? If so, are you currently able to meet those needs?
- To stay ahead of the threats, cybersecurity professionals need to know what these hackers are after and understand the unique attack strategies that they employ as a result.
- Ensure your data is protected, segmented and monitored. Does your HR staff need access to sales data? Do your developers need access to data from your POS infrastructure? If teams have no need to see it, ensure that you have built your infrastructure to prevent that access as much as possible.
- "Flat" networks can be easy for attackers to move through once they've gained a foothold. Building extensive physical and logical separation is key to slowing attackers and detecting them before they can cause significant losses or damage. Deploying internal firewall appliances between segments on your network can assist in watching for incidents that have managed to breach your perimeter or endpoint defences.
- Regularly review your security posture. Security is a continuous effort and must be both tested and reviewed; both qualitative and quantitative efforts are required. Regular audits by an independent party can provide a fresh perspective and unique methods that your staff may not have.
- End user education remains an integral piece of the puzzle. If you are going to allow your employees to access content that has the potential to deliver malicious content, regular training and testing should be part of your efforts. Can your employees spot a malicious email, even if it appears to come from someone they know?

About FortiGuard Labs

For more than 10 years, Fortinet's dedicated security research team, FortiGuard Labs, has led the industry in innovation, powering all top-rated Fortinet security platforms. This accomplished group is composed of over 200 dedicated security threat researchers, engineers, and forensic specialists tasked with outsmarting cybercriminals and delivering cutting-edge protection tools to our global customers—assuring some of the fastest response times in the industry to new vulnerabilities, attacks, viruses, botnets, and other threats.

The FortiGuard Labs team collaborates with the world's leading threat monitoring organizations to advise and learn of emerging threats and new trends in the threat landscape. Additionally, the team contributes to the overall security industry by identifying and responsibly reporting vulnerabilities directly to vendors of hardware, operating systems, and applications.

FortiGuard Labs have teams operating in North America, Asia, and Europe. In a typical week, FortiGuard Labs process over 220 TB worth of threat samples and update approximately:

- 2 million antivirus signatures
- 18,000 intrusion prevention (IPS) rules
- 250 million URL ratings in 78 categories
- 47,000,000 anti-spam signatures

In addition, FortiGuard Labs track more than:

- 5,800 application control signatures
- 700 database security policies
- 3,000 web application firewall attack signatures

FortiGuard Labs has also discovered and responsibly disclosed hundreds of zero-day threats across the entire threat landscape—from popular and common software, to mobile, to IoT devices, and everything in-between.

About Fortinet

Fortinet is a global leader and innovator in network security. Our mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a provider of network security appliances and security subscription services for carriers, data centers, enterprises, distributed offices, and MSSPs. Because of constant innovation of our custom ASICs, hardware systems, network software, management capabilities, and security research, we have a large, rapidly growing, and highly satisfied customer base—including the majority of the Fortune Global 100—and we continue to set the pace in the network security market. Our market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond network security to help secure the extended enterprise.

Fortinet is headquartered in Sunnyvale, California, with offices around the world. Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong and seasoned management team with deep experience in networking and security.

Appendix: Data Collection & Methodology

The data in this report was gathered from hundreds of participating companies who wanted to gain a deeper understanding into their network infrastructures.

To participate in the assessment, each company was provided a FortiGate network security appliance to install in transparent mode inside their existing security network infrastructure for a period of three to seven days.

The data represented in this report was collected from live production environments. This assessment program process provides each company with an individualized report that highlights critical gaps in their current security solutions and policies.

- The data presented in this report was anonymized and contains no identifiable information. Any data that may have revealed information as to the layouts or the identity of an individual corporation or organization was sterilized.
- The devices used were configured in a method that allowed them to capture and analyze the traffic passing through them without providing any security features or impacting network traffic.
- Participating companies ranged between small, medium, large, and enterprise organizations in key industries including Education, Finance/Banking, Healthcare, and Technology.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonee
06560, Aples-Maritimes,
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Feb 23, 2016