SECURITY LIFECYCLE REVIEW

ACME

14 July 2015

Report Period: 6 Days
Start: Sun, Jun 07, 2015
End: Sun, Jun 14, 2015

PREPARED BY:
Palo Alto Networks
Palo Alto Networks

www.paloaltonetworks.com

paloalto NETWORKS®

EXECUTIVE SUMMARY FOR ACME

Key Findings:

- **268** total applications are in use, presenting potential business and security challenges. As critical functions move outside of an organization's control, employees use non-work-related applications, or cyberattackers use them to deliver threats and steal data.
- **62** high-risk applications were observed, including those that can introduce or hide malicious activity, transfer files outside the network, or establish unauthorized communication.
- **3,195,868** total threats were found on your network, including vulnerability exploits, known and unknown malware, and outbound command and control activity.

The Security Lifecycle Review summarizes the business and security risks facing **ACME**. The data used for this analysis was gathered by Palo Alto Networks during the report time period. The report provides actionable intelligence around the applications, URL traffic, types of content, and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk exposure.

268
APPLICATIONS IN USE

62
HIGH RISK APPLICATIONS

3,195,868
TOTAL THREATS

3,195,010
VULNERABILITY DETECTIONS

834
KNOWN THREATS

24
UNKNOWN THREATS

Report Period: 6 Days
Start: Sun, Jun 07, 2015
End: Sun, Jun 14, 2015

Applications at a Glance

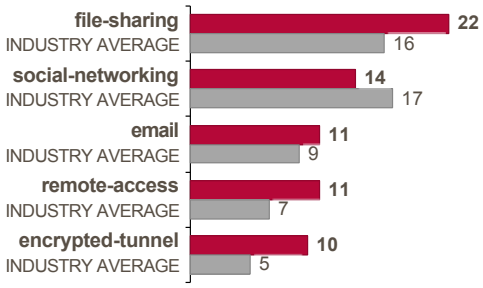
Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision on potential risk versus business benefit.

Key Findings:

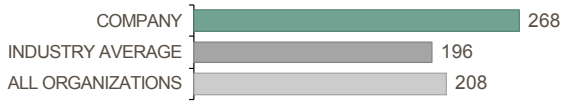
- High-risk applications such as **file-sharing, social-networking and email** were observed on the network, which should be investigated due to their potential for abuse.
- **268** total applications were seen on the network across **24** sub-categories, as opposed to an industry average of **196** total applications seen in other **High Technology** organizations.
- **474.3GB** was used by all applications, including **networking** with **211.22GB**, compared to an industry average of **2.43TB** in similar organizations.

High-Risk Applications

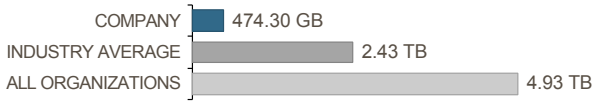
The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.



Number of Applications on Network

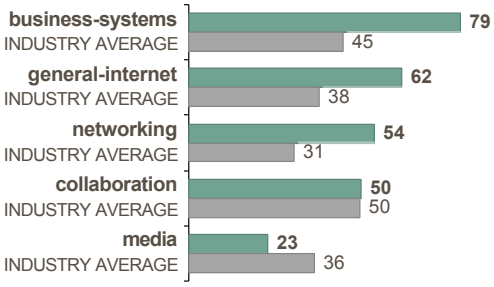


Bandwidth Consumed by Applications



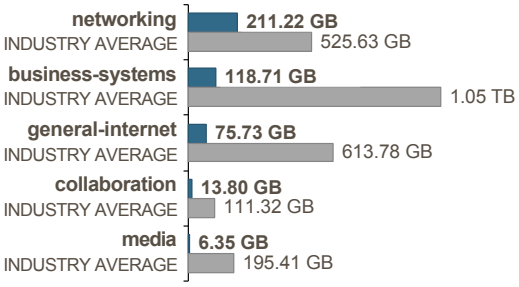
Categories with the Most Applications

The following categories have the most applications variants, and should be reviewed for business relevance.



Categories Consuming the Most Bandwidth

Bandwidth consumed by application category shows where application usage is heaviest, and where you could reduce operational resources.



Applications that Introduce Risk

The top applications (sorted by bandwidth consumed) for application subcategories that introduce risk are displayed below, including industry benchmarks on the number of variants across other **High Technology** organizations. This data can be used to more effectively prioritize your application enablement efforts.

RISK LEVEL

5
4
3
2
1

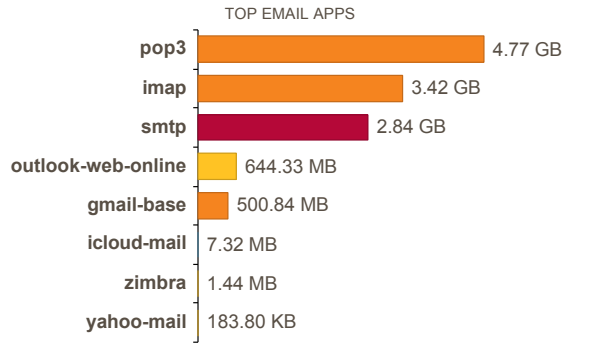
Key Findings:

- A total of **268** applications were seen in your organization, compared to an industry average of **196** in other **High Technology** organizations.
- The most common types of application subcategories are **internet-utility, management and infrastructure**.
- The application subcategories consuming the most bandwidth are **encrypted-tunnel, infrastructure and software-update**.

Email - 12.16GB

11 9

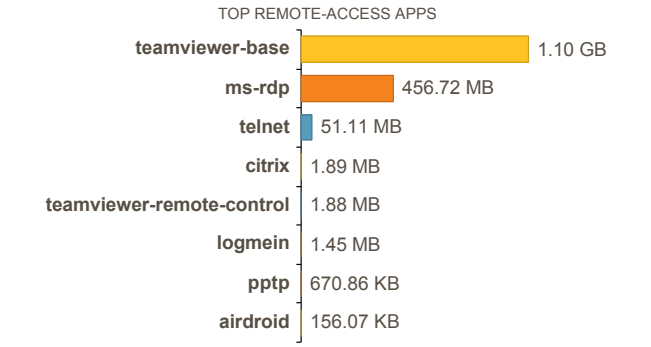
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Remote-Access - 1.6GB

11 7

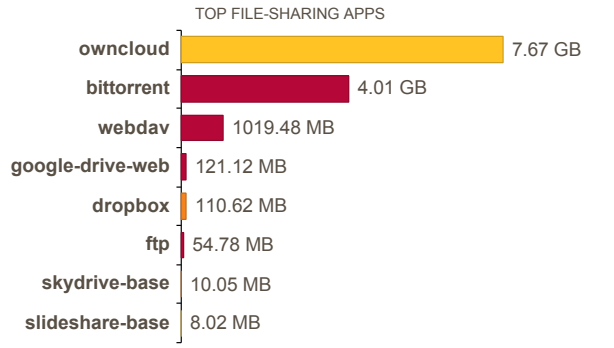
APPLICATION VARIANTS VS INDUSTRY AVERAGE



File-Sharing - 12.98GB

22 16

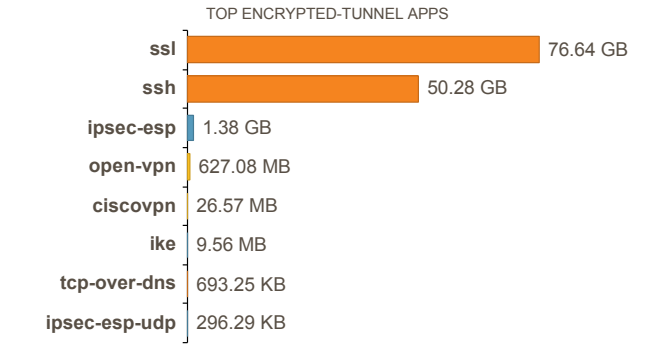
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Encrypted-Tunnel - 128.95GB

10 5

APPLICATION VARIANTS VS INDUSTRY AVERAGE



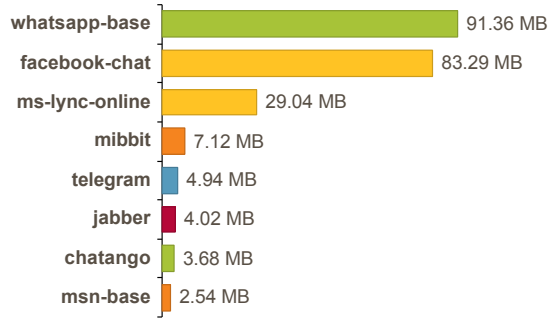
Applications that Introduce Risk (Continued)

Instant-Messaging - 227.04MB

12 10

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP INSTANT-MESSAGING APPS



Social-Networking - 1.28GB

14 17

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP SOCIAL-NETWORKING APPS

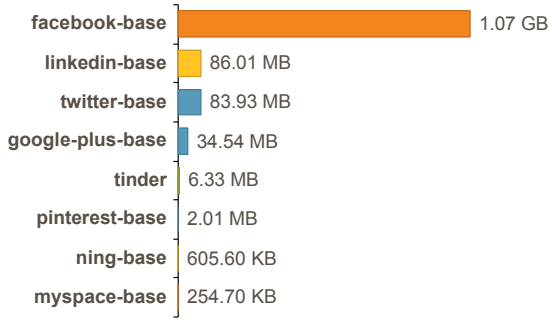
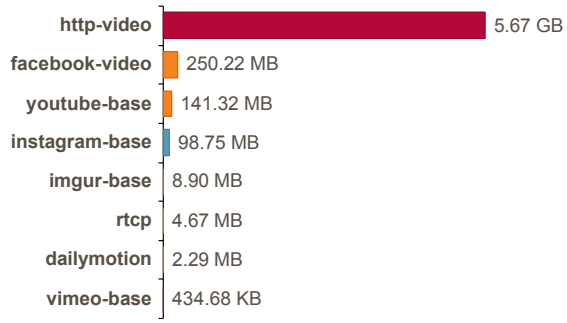


Photo-Video - 6.16GB

13 23

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP PHOTO-VIDEO APPS



Proxy - 1.19GB

3 2

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP PROXY APPS

Applications that Introduce Risk — Detail

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
4	pop3	collaboration	email	client-server	4.77GB	57356
4	imap	collaboration	email	client-server	3.42GB	6755
5	smtp	collaboration	email	client-server	2.84GB	115038
3	outlook-web-online	collaboration	email	browser-based	644.33MB	17571
4	gmail-base	collaboration	email	browser-based	500.84MB	3284
2	icloud-mail	collaboration	email	client-server	7.32MB	13
3	zimbra	collaboration	email	browser-based	1.44MB	34
3	yahoo-mail	collaboration	email	browser-based	183.8KB	26
4	ssl	networking	encrypted-tunnel	browser-based	76.64GB	2782592
4	ssh	networking	encrypted-tunnel	client-server	50.28GB	668279
2	ipsec-esp	networking	encrypted-tunnel	client-server	1.38GB	17
3	open-vpn	networking	encrypted-tunnel	client-server	627.08MB	275
3	ciscovpn	networking	encrypted-tunnel	client-server	26.57MB	24
2	ike	networking	encrypted-tunnel	client-server	9.56MB	574
4	tcp-over-dns	networking	encrypted-tunnel	client-server	693.25KB	8
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	296.29KB	485
3	owncloud	general-internet	file-sharing	client-server	7.67GB	107111
5	bittorrent	general-internet	file-sharing	peer-to-peer	4.01GB	30852
5	webdav	general-internet	file-sharing	browser-based	1019.48MB	168511
5	google-drive-web	general-internet	file-sharing	browser-based	121.12MB	462
4	dropbox	general-internet	file-sharing	client-server	110.62MB	8669
5	ftp	general-internet	file-sharing	client-server	54.78MB	11282
4	skydrive-base	general-internet	file-sharing	browser-based	10.05MB	376
3	slideshare-base	general-internet	file-sharing	browser-based	8.02MB	206
1	whatsapp-base	collaboration	instant-messaging	client-server	91.36MB	1340

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
3	facebook-chat	collaboration	instant-messaging	browser-based	83.29MB	250
3	ms-lync-online	collaboration	instant-messaging	client-server	29.04MB	652
4	mibbit	collaboration	instant-messaging	browser-based	7.12MB	79
2	telegram	collaboration	instant-messaging	client-server	4.94MB	415
5	jabber	collaboration	instant-messaging	client-server	4.02MB	88
1	chatango	collaboration	instant-messaging	client-server	3.68MB	509
4	msn-base	collaboration	instant-messaging	client-server	2.54MB	163
5	http-video	media	photo-video	browser-based	5.67GB	990
4	facebook-video	media	photo-video	browser-based	250.22MB	105
4	youtube-base	media	photo-video	browser-based	141.32MB	129
2	instagram-base	media	photo-video	client-server	98.75MB	1204
4	imgur-base	media	photo-video	browser-based	8.9MB	323
1	rtcp	media	photo-video	client-server	4.67MB	3
4	dailymotion	media	photo-video	browser-based	2.29MB	331
5	vimeo-base	media	photo-video	browser-based	434.68KB	8
5	http-proxy	networking	proxy	browser-based	1.19GB	33453
5	socks	networking	proxy	network-protocol	144.09KB	649
4	freegate	networking	proxy	client-server	628Bytes	6
3	teamviewer-base	networking	remote-access	client-server	1.1GB	40350
4	ms-rdp	networking	remote-access	client-server	456.72MB	10726
2	telnet	networking	remote-access	client-server	51.11MB	28602
3	citrix	networking	remote-access	client-server	1.89MB	406
2	teamviewer-remote-control	networking	remote-access	client-server	1.88MB	2
4	logmein	networking	remote-access	client-server	1.45MB	13
4	pptp	networking	remote-access	network-protocol	670.86KB	53

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
3	airdroid	networking	remote-access	browser-based	156.07KB	50
4	facebook-base	collaboration	social-networking	browser-based	1.07GB	31521
3	linkedin-base	collaboration	social-networking	browser-based	86.01MB	4174
2	twitter-base	collaboration	social-networking	browser-based	83.93MB	8013
2	google-plus-base	collaboration	social-networking	browser-based	34.54MB	305
1	tinder	collaboration	social-networking	client-server	6.33MB	24
2	pinterest-base	collaboration	social-networking	browser-based	2.01MB	143
3	ning-base	collaboration	social-networking	browser-based	605.6KB	28
4	myspace-base	collaboration	social-networking	browser-based	254.7KB	54

Notes:

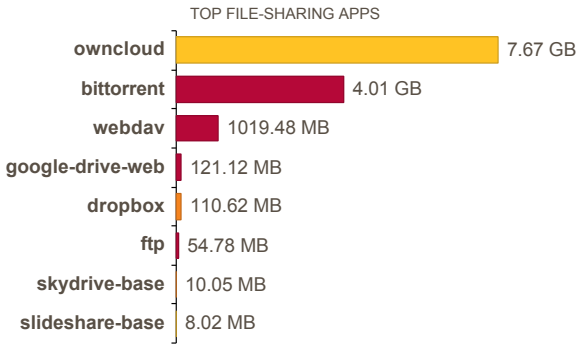
SaaS Applications

SaaS–based application services continue to redefine the network perimeter, often labeled “shadow IT”, most of these services are adopted directly by individual users, business teams, or even entire departments. In order to minimize data security risks, visibility and proper policy must be maintained for SaaS applications.

File-Sharing - 12.98GB

22 16

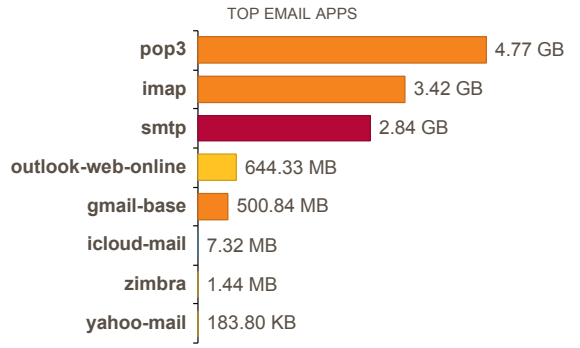
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Email - 12.16GB

11 9

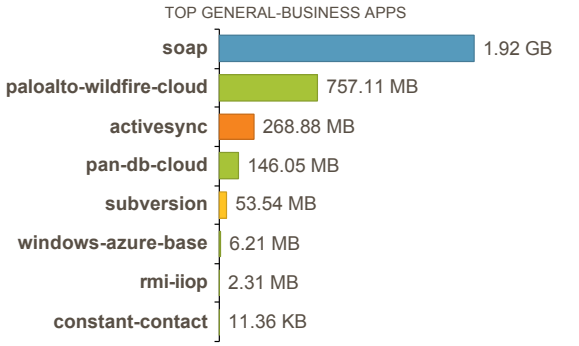
APPLICATION VARIANTS VS INDUSTRY AVERAGE



General-Business - 3.13GB

8 8

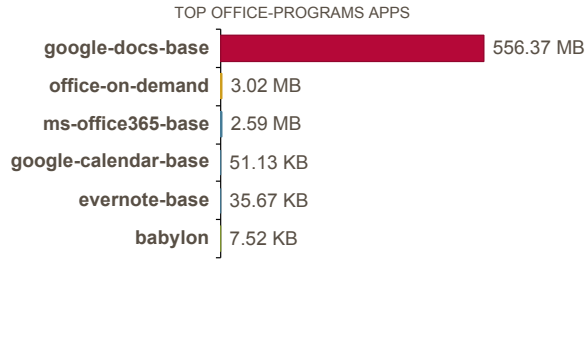
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Office-Programs - 562.07MB

6 5

APPLICATION VARIANTS VS INDUSTRY AVERAGE



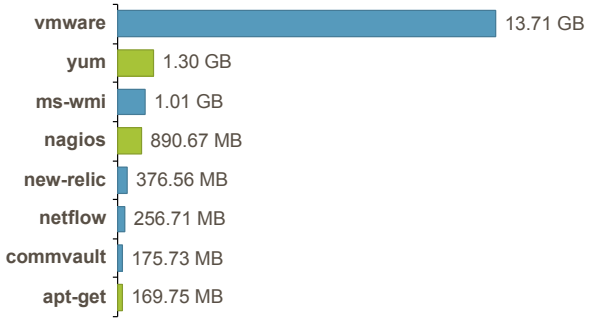
SaaS Applications (Continued)

Management - 17.96GB

29 13

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP MANAGEMENT APPS

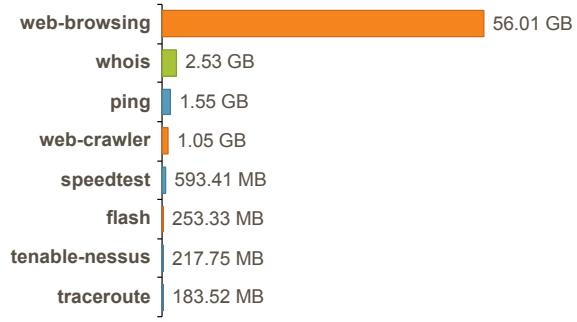


Internet-Utility - 62.75GB

41 22

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP INTERNET-UTILITY APPS

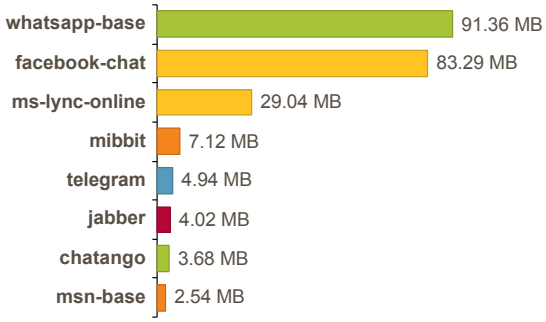


Instant-Messaging - 227.04MB

12 10

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP INSTANT-MESSAGING APPS

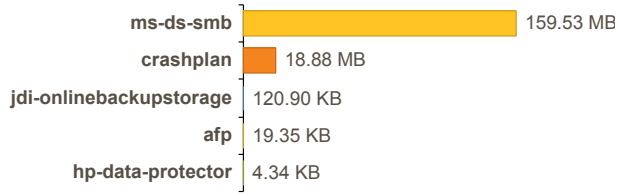


Storage-Backup - 178.56MB

5 3

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP STORAGE-BACKUP APPS



URL Activity

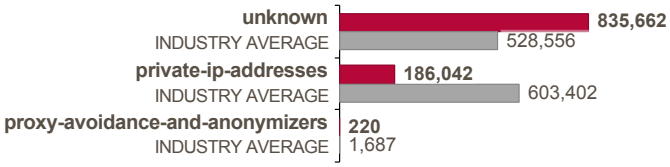
Uncontrolled Web surfing exposes organizations to security and business risks, including exposure to potential threat propagation, data loss, or compliance violations. The most common URL categories visited by users on the network are shown below.

Key Findings:

- High-risk URL categories were observed on the network, including **unknown, web-hosting and educational-institutions**.
- Users visited a total of **5,417,856** URLs during the report time period across **54** categories.
- There was a variety of personal and work-related Web activity present, including visits to potentially risky websites.

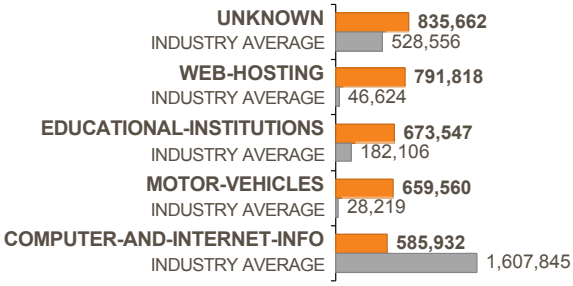
High-Risk URL Categories

The Web is a primary infection vector for attackers, with high-risk URL categories posing an outsized risk to the organization. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unknowns.



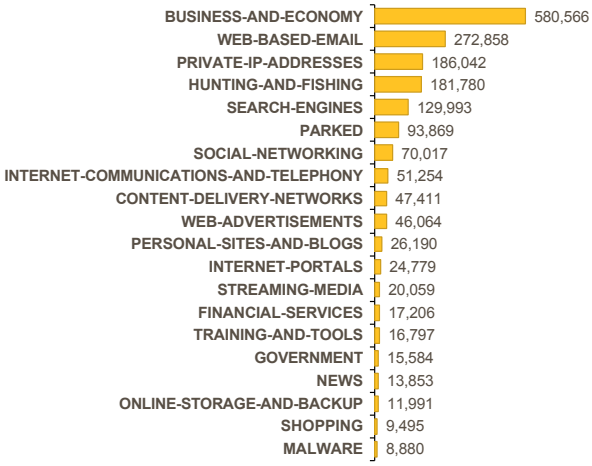
High-Traffic URL Categories

The top 5 commonly visited URL categories, along with industry benchmarks across your peer group, are shown below.



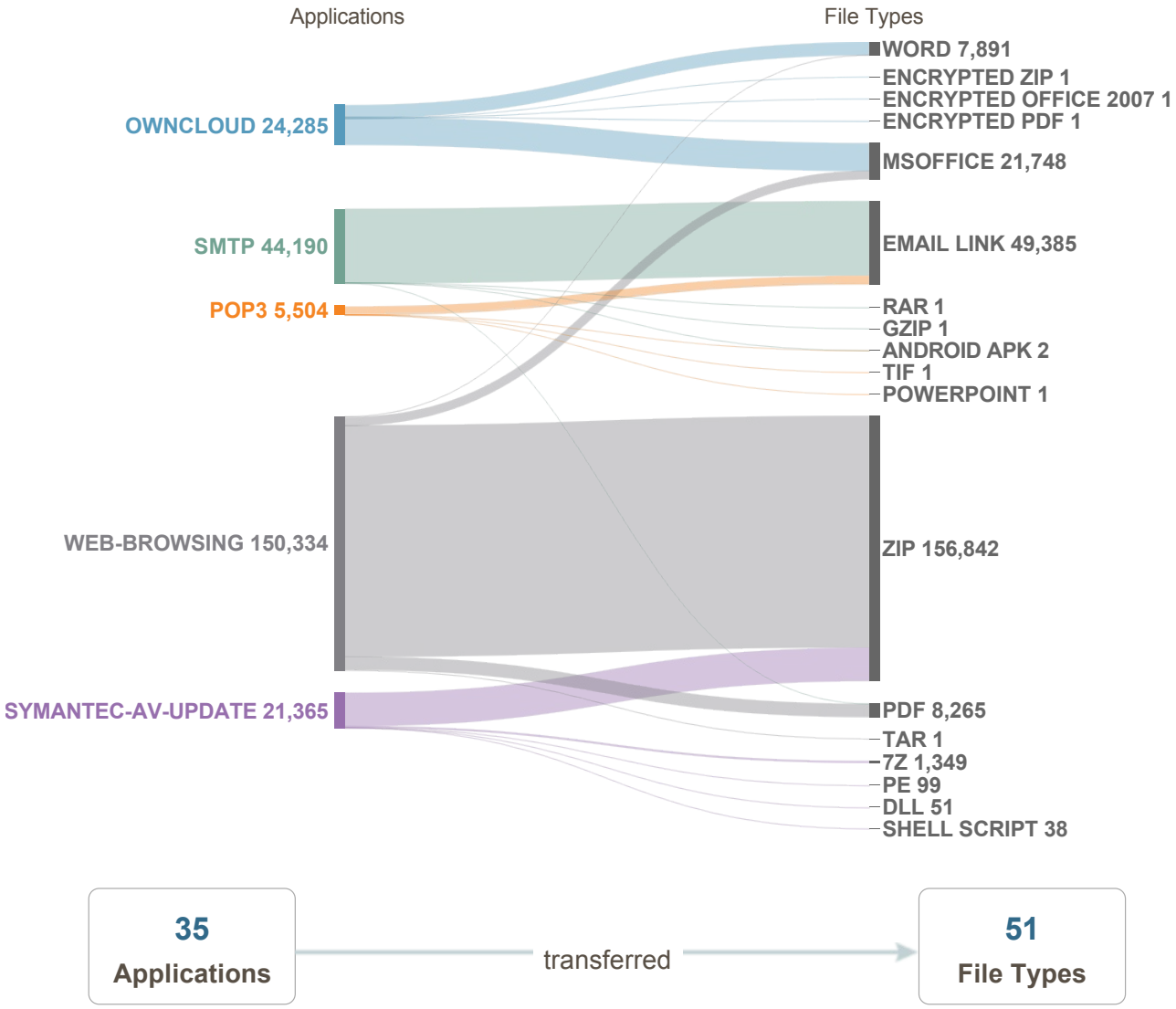
Commonly Used URL Categories

The top 20 most commonly visited URL categories are shown below.



File Transfer Analysis

Applications that can transfer files serve an important business function, but they also potentially allow for sensitive data to leave the network or cyber threats to be delivered. Within your organization, **286** total files were observed, across **51** different file types, delivered via a total of **35** total applications. The image below correlates the applications most commonly used to transfer files, along with the most prevalent file and content types observed.



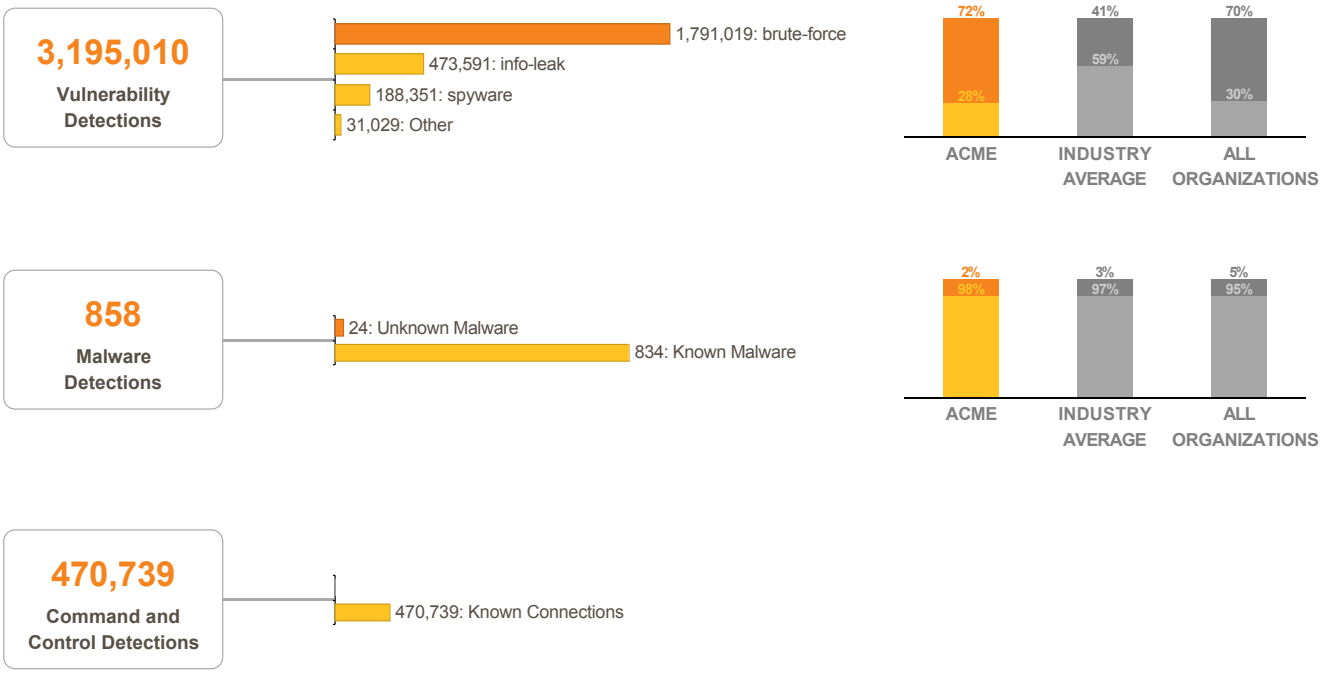
35 Applications — transferred → **51** File Types

Threats at a Glance

Understanding your risk exposure, and how to adjust your security posture to prevent attacks, requires intelligence on the type and volume of threats used against your organization. This section details the application vulnerabilities, known and unknown malware, and command and control activity observed on your network.

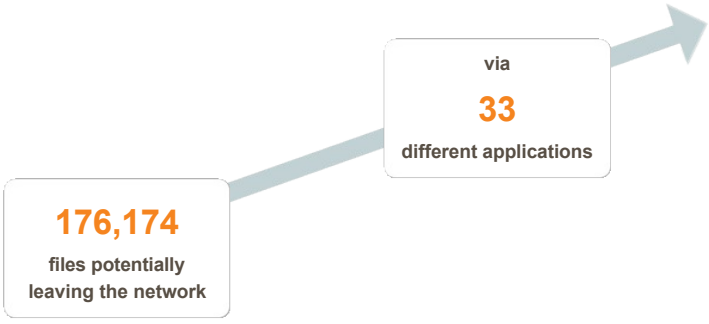
Key Findings:

- **3,195,010** total vulnerability exploits breachwere observed in your organization, including **brute-force, info-leak and spyware**.
- **858** malware events were observed, versus an industry average of **858** across your peer group.
- **470,739** total outbound command and control requests were identified, indicating attempts by malware to communicate with external attackers to download additional malware, receive instructions, or exfiltrate data.



Files Leaving the Network

Transferring files is a required and common part of doing business, but you must maintain visibility into what content is leaving the network via which applications, in order to limit your organization's exposure to data loss.



High-Risk and Malicious File Type Analysis

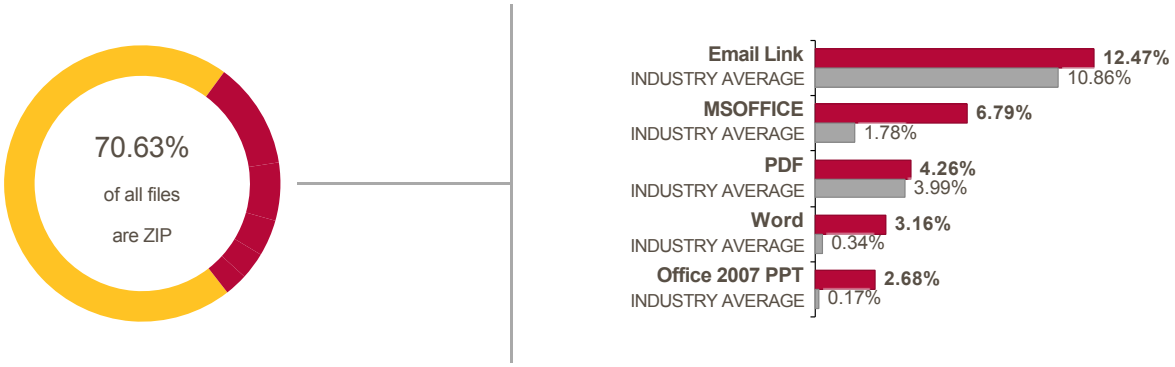
Today's cyber attackers use a variety of file types to deliver malware and exploits, often focusing on content from common business applications present in most enterprise networks. The majority of commodity threats are delivered via executable files, with more targeted and advanced attacks often using other content to compromise networks.

Key Findings:

- A variety of file-types were used to deliver threats, and prevention strategies should cover all major content types.
- You can reduce your attack surface by proactively blocking high-risk file-types, such as blocking executable files downloaded from the Internet, or disallowing RTF files or LNK files, which are not needed in daily business.

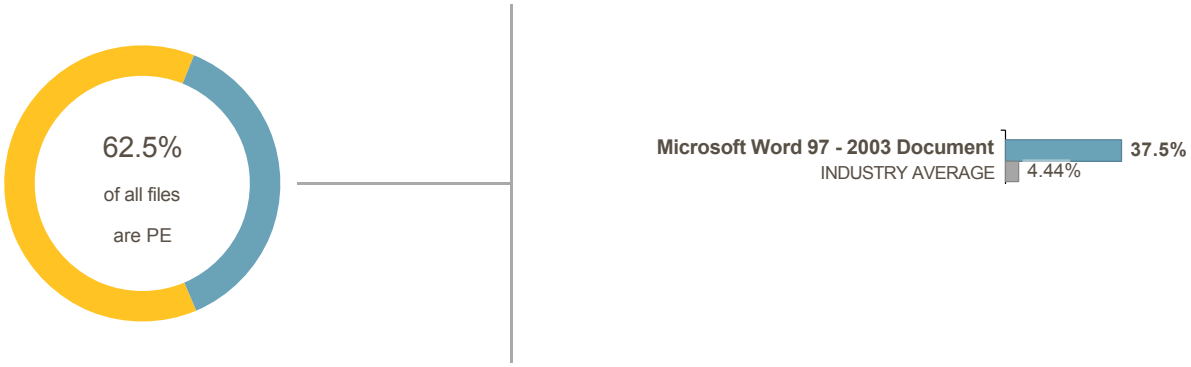
High-Risk File Types

The file types shown represent a greater risk to the organization due to a combination of new vulnerabilities being discovered, existing and unpatched flaws, and prevalence of use in attacks.



Files Delivering Unknown Malware

We recommend investigating the files that may be used to deliver threats both within your organization, and across your peer group. Together, these trends allow you to take preventive action such as blocking high-risk file types across different user groups.

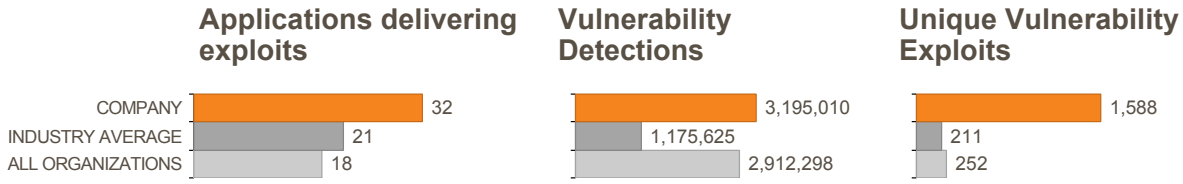


Application Vulnerabilities

Application vulnerabilities allow attackers to exploit vulnerable, often unpatched, applications to infect systems, which often represent one of the first steps in a breach. This page details the top five application vulnerabilities attackers attempted to exploit within your organization, allowing you to determine which applications represent the largest attack surface.

Key Findings:

- **32** total applications were observed delivering exploits to your environment.
- **3,195,010** total vulnerability were observed, with the top three categories being **dns, ntp and netbios-ns**.
- Out of the total vulnerabilities discovered, **1,588** unique vulnerabilities were found, meaning attackers used the same vulnerability exploits over and over again.



Vulnerabilities per Application (top 5 applications with most detections)

DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
1,025,291	**dns**			
4	ISC BIND OPT Record Handling Denial of Service Vulnerability	High	dos	CVE-2002-1220
1	Microsoft Windows NAT Helper DNS Query Denial of Service	High	dos	CVE-2006-5614
369,545	DNS ANY Queries Brute-force DOS Attack	Medium	brute-force	0
369,545	DNS ANY Queries Brute-force DOS Attack	Medium	brute-force	
33,530	Suspicious DNS Query (Trojan-Downloader.andromeda:hzmksreiuojy.com)	Medium		
432	Suspicious DNS Query (generic:swtsik.com)	Medium		
455	Suspicious DNS Query (generic:uaxkpp.com)	Medium		
524	Suspicious DNS Query (generic:yxjtwf.com)	Medium		
505	Suspicious DNS Query (generic:eyfznt.com)	Medium		
501	Suspicious DNS Query (generic:suunyu.com)	Medium		
883,153	**ntp**			
762	NTP Reserved Mode Denial of Service Vulnerability	High	dos	CVE-2009-3563
882,391	NTP Denial-Of-Service Attack	Low	brute-force	CVE-2013-5211

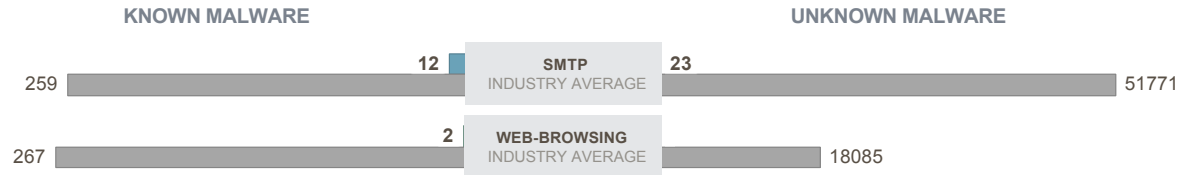
DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
291,848	**netbios-ns**			
145,924	NetBIOS nbtstat query	Info	info-leak	0
145,924	NetBIOS nbtstat query	Info	info-leak	
188,353	**sip**			
188,340	Sipvicious.Gen User-Agent Traffic	Low	spyware	
11	Sipvicious.sundayddr User-Agent Traffic	Low	net-worm	
1	SIP Register Request Attempt	Low	brute-force	0
1	SIP Register Request Attempt	Low	brute-force	
120,853	**mssql-db**			
50,443	Microsoft SQL Server User Authentication Brute-force Attempt	High	brute-force	0
50,443	Microsoft SQL Server User Authentication Brute-force Attempt	High	brute-force	
19,065	MSSQL Login failed for user 'sa' execution	Info	overflow	CVE-2000-1209
451	MSSQL DB Login Authentication Failed	Info	brute-force	0
451	MSSQL DB Login Authentication Failed	Info	brute-force	

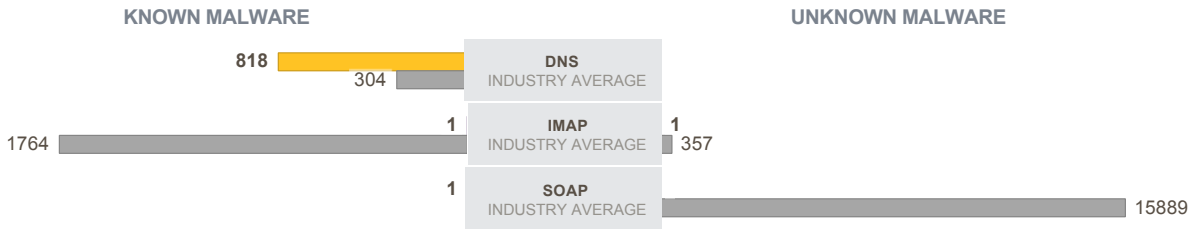
Known and Unknown Malware

Applications are the primary vectors used to deliver malware and infect organizations, communicate outbound, or exfiltrate data. Adversaries' tactics have evolved to use the applications commonly found on the network into which traditional security solutions have little or no visibility.

Key Findings:

- **5** total applications were observed delivering malware to your organization, out of **268** total applications on the network.
- Many applications delivering malware are required to run your business, which means you need a solution that can prevent threats, while still enabling the applications.
- While most malware is delivered over HTTP or SMTP, advanced attacks will often use other applications, including those on non-standard ports or employing other evasive behavior.





5
applications found delivering malware

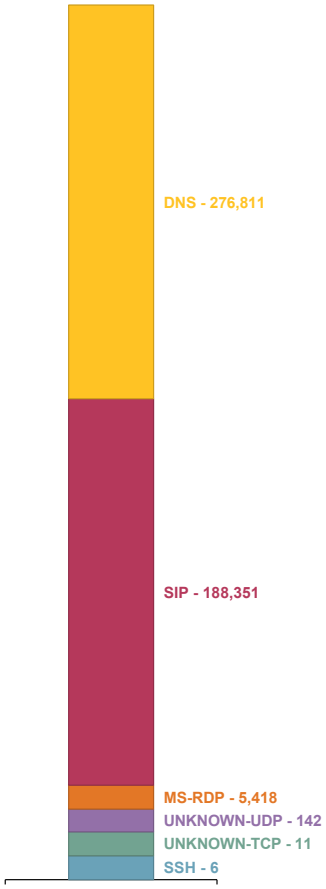
Command and Control Analysis

Command-and-control (CnC) activity indicates a host in the network has been infected by malware, and is attempting to connect outside of the network to malicious actors. Understanding and preventing this activity is critical, as attackers use CnC to deliver additional malware, provide instruction, or exfiltrate data.

Key Findings:

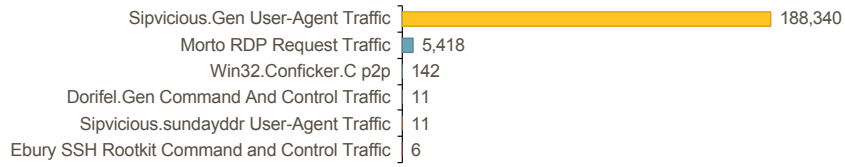
- **6** total applications were used for command-and-control communication.
- **470,739** total command and control requests were observed originating from your network.
- **276,811** total suspicious DNS queries were observed.

COMMAND AND CONTROL ACTIVITY BY APPLICATION



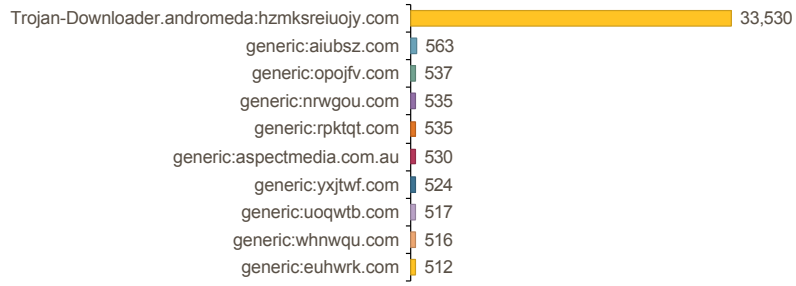
Spyware Phone Home: 193,928

This image below represents compromised hosts attempting to connect external malicious CnC servers.



Suspicious DNS Queries: 276,811

While DNS is a common and necessary application, it is also commonly used to hide outbound CnC communication, as shown in the chart below.



Summary: ACME

The analysis determined that a wide range of applications and cyber attacks were present on the network. This activity represents potential business and security risks to **ACME**, but also an ideal opportunity to implement safe application enablement policies that, not only allow business to continue growing, but reduce the overall risk exposure of the organization.

Highlights Include:

- High-risk applications such as **file-sharing, social-networking and email** were observed on the network, which should be investigated due to their potential for abuse.
- **268** total applications were seen on the network across **24**, as opposed to an industry average of **196** total applications seen in other **High Technology** organizations.
- **3,195,010** total vulnerability detections were observed, with the top three categories being **dns, ntp and netbios-ns**.
- **858** malware events were observed, versus an industry average of **858** across your peer group.
- **6** total applications were used for command and control communication.

268
APPLICATIONS IN USE

62
HIGH RISK APPLICATIONS

3,195,868
TOTAL THREATS

3,195,010
VULNERABILITY DETECTIONS

834
KNOWN THREATS

24
UNKNOWN THREATS

Recommendations:

- Implement safe application enablement polices, by only allowing the applications needed for business, and applying granular control to all others.
- Address high-risk applications with the potential for abuse, such as remote access, file sharing, or encrypted tunnels.
- Deploy a security solution that can detect and prevent threats, both known and unknown, to mitigate risk from attackers.
- Use a solution that can automatically re-program itself, creating new protections for emerging threats, sourced from a global community of other enterprise users.