SECURITY LIFECYCLE REVIEW

Acme

PREPARED BY

Palo Alto Networks
Acme
www.paloaltonetworks.com

Report Period: 8 Days
Tue, Jun 20, 2017 - Tue, Jun 27, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY FOR Acme

Key Findings:

- **328** 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.
- **75** high-risk applications were observed, including those that can introduce or hide malicious activity, transfer files outside the network, or establish unauthorized communication.
- **6,752** 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.

328
APPLICATIONS IN USE

75
HIGH RISK APPLICATIONS

6,752
TOTAL THREATS

3,580
VULNERABILITY EXPLOITS

22
KNOWN MALWARE

84
UNKNOWN MALWARE

Report Period: 8 Days
Start: Tue, Jun 20, 2017
End: Tue, Jun 27, 2017

Applications at a Glance

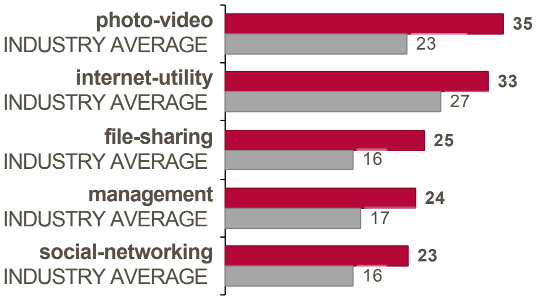
Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision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

Key Findings:

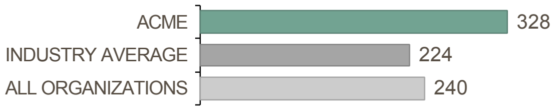
- High-risk applications such as **photo-video, internet-utility and file-sharing** were observed on the network, which should be investigated due to their potential for abuse.
- **328** total applications were seen on the network across **28** sub-categories, as opposed to an industry average of **224** total applications seen in other **High Technology** organizations.
- **561.42GB** was used by all applications, including **collaboration** with **134.46GB**, compared to an industry average of **624.47GB** in similar organizations.

High-Risk Applications

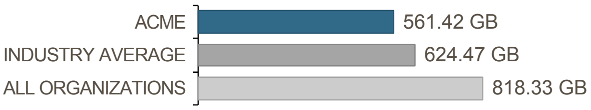
The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.



Number of Applications on Network

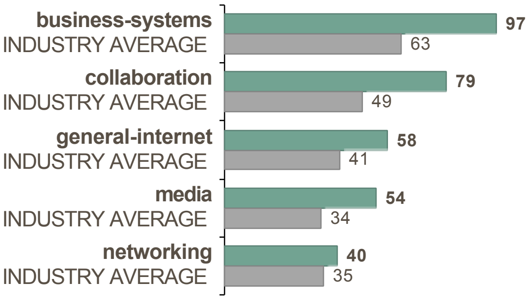


Bandwidth Consumed by Applications



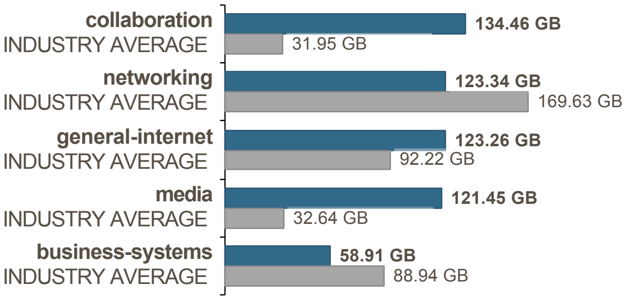
Categories with the Most Applications

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.

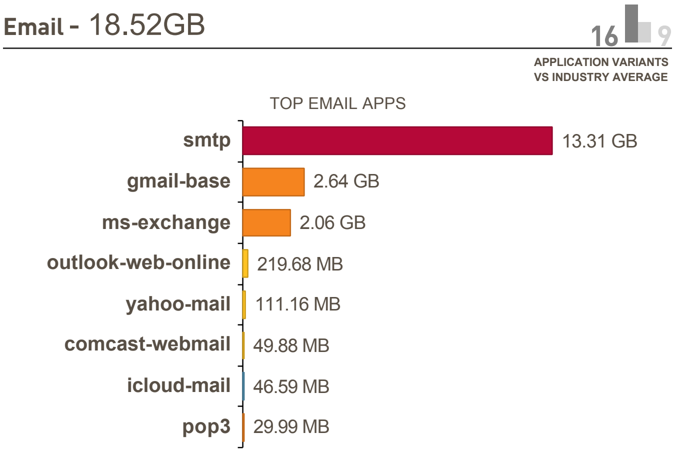
RISK LEVEL

5]- High
4
3
2
1

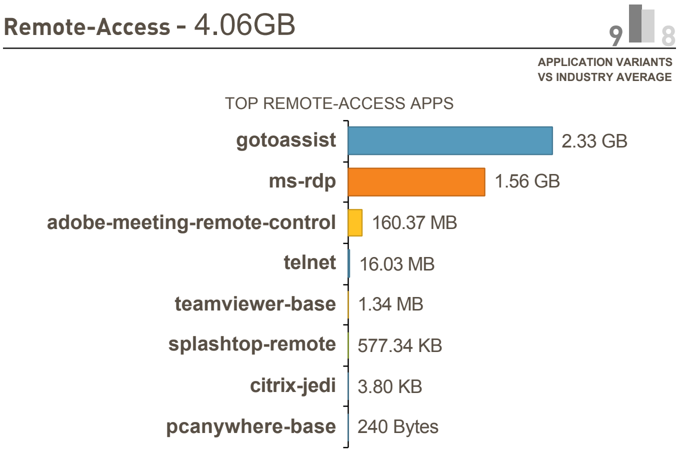
Key Findings:

- A total of **328** applications were seen in your organization, compared to an industry average of **224** in other **High Technology** organizations.
- The most common types of application subcategories are **photo-video, internet-utility and file-sharing**.
- The application subcategories consuming the most bandwidth are **internet-conferencing, encrypted-tunnel and internet-utility**.

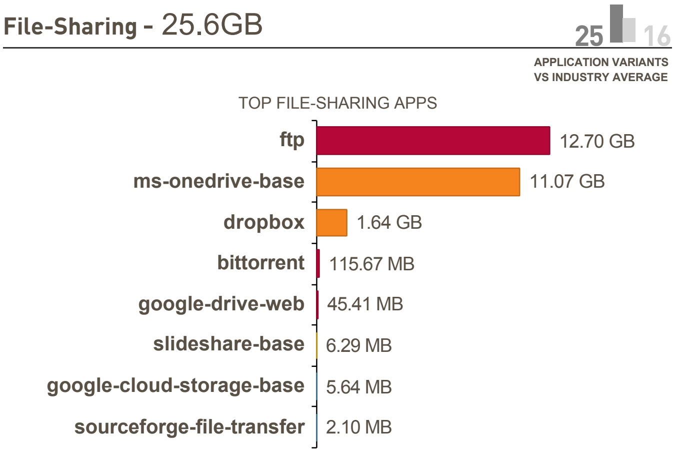
Email - 18.52GB



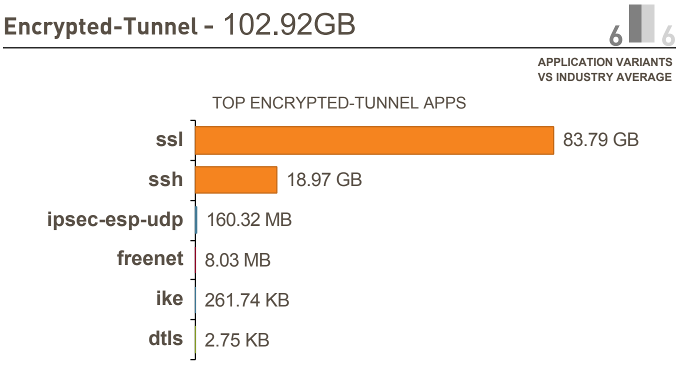
Remote-Access - 4.06GB



File-Sharing - 25.6GB

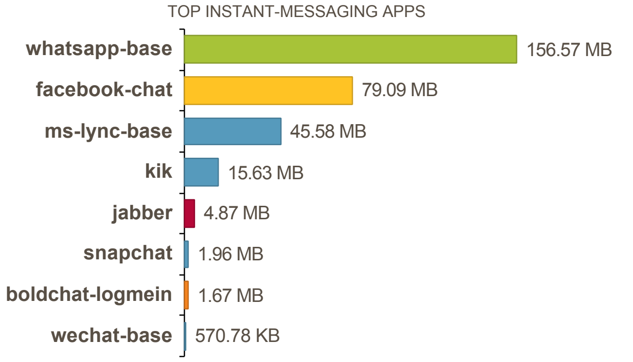


Encrypted-Tunnel - 102.92GB



Instant-Messaging - 306.75MB

12 10
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Social-Networking - 8.34GB

23 16
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

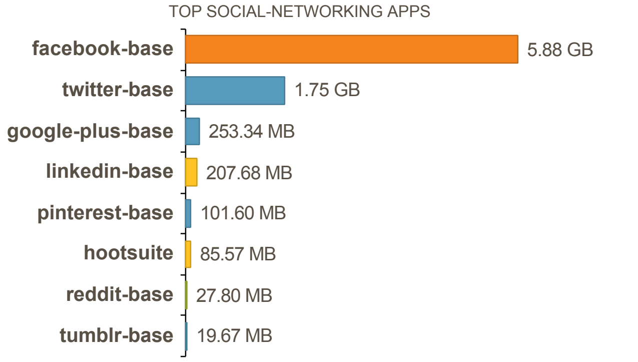
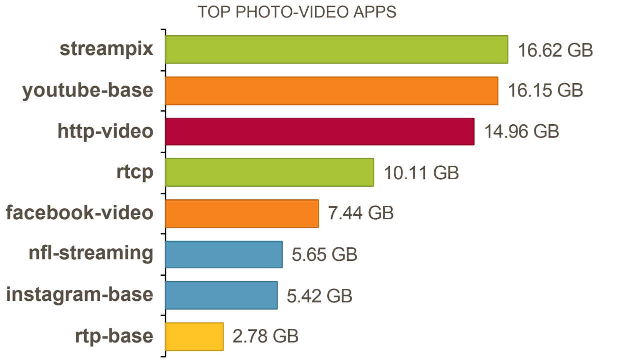


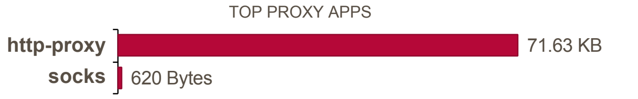
Photo-Video - 85.63GB

35 23
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Proxy - 72.24KB

2 2
APPLICATION VARIANTS
VS INDUSTRY AVERAGE



Applications that Introduce Risk — Detail

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
5	smtp	collaboration	email	client-server	13.31GB	71157
4	gmail-base	collaboration	email	browser-based	2.64GB	10348
4	ms-exchange	collaboration	email	client-server	2.06GB	1703
3	outlook-web-online	collaboration	email	browser-based	219.68MB	9106
3	yahoo-mail	collaboration	email	browser-based	111.16MB	2087
3	comcast-webmail	collaboration	email	browser-based	49.88MB	462
2	icloud-mail	collaboration	email	client-server	46.59MB	1418
4	pop3	collaboration	email	client-server	29.99MB	155
4	ssl	networking	encrypted-tunnel	browser-based	83.79GB	1927883
4	ssh	networking	encrypted-tunnel	client-server	18.97GB	6289
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	160.32MB	251
5	freenet	networking	encrypted-tunnel	peer-to-peer	8.03MB	12852
2	ike	networking	encrypted-tunnel	client-server	261.74KB	296
1	dtls	networking	encrypted-tunnel	client-server	2.75KB	4
5	ftp	general-internet	file-sharing	client-server	12.7GB	914
4	ms-onedrive-base	general-internet	file-sharing	client-server	11.07GB	1345
4	dropbox	general-internet	file-sharing	client-server	1.64GB	4957
5	bittorrent	general-internet	file-sharing	peer-to-peer	115.67MB	38294
5	google-drive-web	general-internet	file-sharing	browser-based	45.41MB	302
3	slideshare-base	general-internet	file-sharing	browser-based	6.29MB	64
2	google-cloud-storage-base	general-internet	file-sharing	browser-based	5.64MB	37
2	sourceforge-file-transfer	general-internet	file-sharing	client-server	2.1MB	5
1	whatsapp-base	collaboration	instant-messaging	client-server	156.57MB	2789
3	facebook-chat	collaboration	instant-messaging	browser-based	79.09MB	1328
2	ms-lync-base	collaboration	instant-messaging	client-server	45.58MB	30

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	kik	collaboration	instant-messaging	client-server	15.63MB	334
5	jabber	collaboration	instant-messaging	client-server	4.87MB	13
2	snapchat	collaboration	instant-messaging	client-server	1.96MB	76
4	boldchat-logmein	collaboration	instant-messaging	browser-based	1.67MB	164
2	wechat-base	collaboration	instant-messaging	client-server	570.78KB	201
1	streampix	media	photo-video	client-server	16.62GB	171
4	youtube-base	media	photo-video	browser-based	16.15GB	5578
5	http-video	media	photo-video	browser-based	14.96GB	967
1	rtcp	media	photo-video	client-server	10.11GB	677
4	facebook-video	media	photo-video	browser-based	7.44GB	3662
2	nfl-streaming	media	photo-video	browser-based	5.65GB	104
2	instagram-base	media	photo-video	client-server	5.42GB	7593
3	rtp-base	media	photo-video	client-server	2.78GB	664
5	http-proxy	networking	proxy	browser-based	71.63KB	90
5	socks	networking	proxy	network-protocol	620Bytes	1
2	gotoassist	networking	remote-access	browser-based	2.33GB	185721
4	ms-rdp	networking	remote-access	client-server	1.56GB	650
3	adobe-meeting-remote-control	networking	remote-access	browser-based	160.37MB	2
2	telnet	networking	remote-access	client-server	16.03MB	8
3	teamviewer-base	networking	remote-access	client-server	1.34MB	22
1	splashtop-remote	networking	remote-access	client-server	577.34KB	133
2	citrix-jedi	networking	remote-access	client-server	3.8KB	14
2	pcanywhere-base	networking	remote-access	client-server	240Bytes	4
4	facebook-base	collaboration	social-networking	browser-based	5.88GB	50900
2	twitter-base	collaboration	social-networking	browser-based	1.75GB	17459

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	google-plus-base	collaboration	social-networking	browser-based	253.34MB	5111
3	linkedin-base	collaboration	social-networking	browser-based	207.68MB	7694
2	pinterest-base	collaboration	social-networking	browser-based	101.6MB	1816
3	hootsuite	collaboration	social-networking	browser-based	85.57MB	1028
1	reddit-base	collaboration	social-networking	browser-based	27.8MB	389
2	tumblr-base	collaboration	social-networking	browser-based	19.67MB	236

Notes:

SaaS Applications

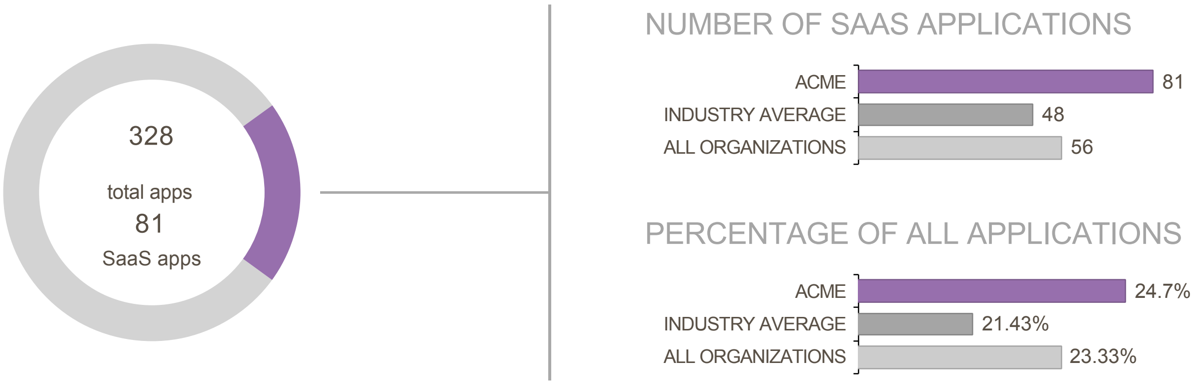
SaaS–based application services continue to redefine the network perimeter. Often labeled “shadow IT,” most of these services are adopted directly by individual users, business teams, or even entire departments. In order to minimize data security risks you need control over SaaS applications used your network .

Key Findings

- **File-Sharing** subcategory has the most number of unique SaaS applications.
- In terms of data movement, **vidyo** is the most used SaaS application in your organization.

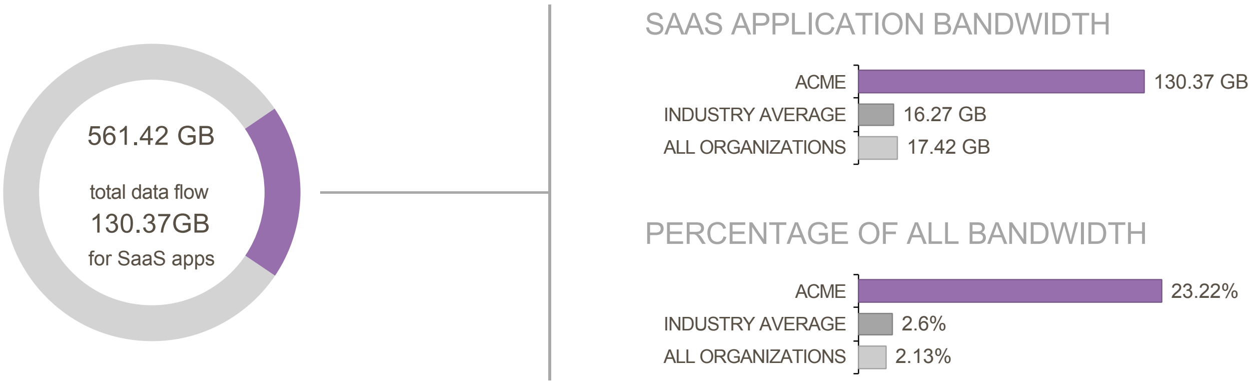
SaaS Applications by Numbers

Review the applications being used in your organization. To maintain administrative control, adopt SaaS applications that will be managed by your IT team



SaaS Application Bandwidth

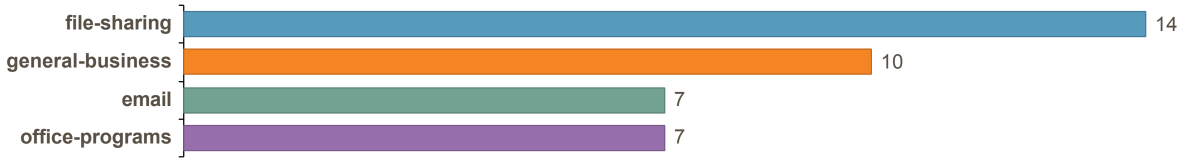
Monitor the volume of data movement to and from SaaS applications. Understand the nature of the applications and how they are being used



TOP SAAS APPLICATION SUBCATEGORIES

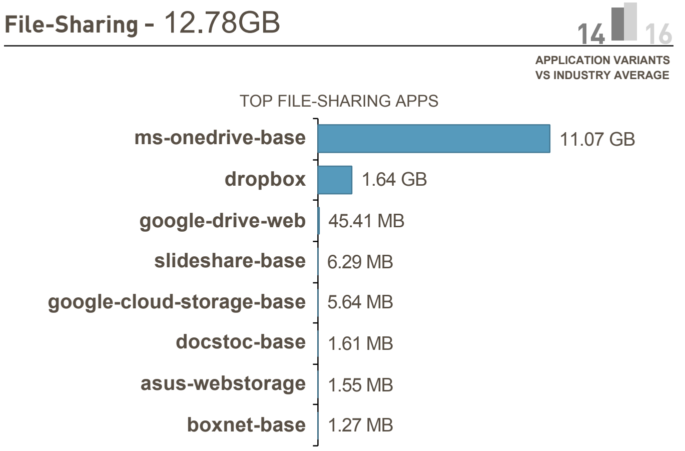
The following displays the number of applications in each application subcategory. This allows you to assess the most used applications organization.

Top SaaS application subcategories by total number of applications

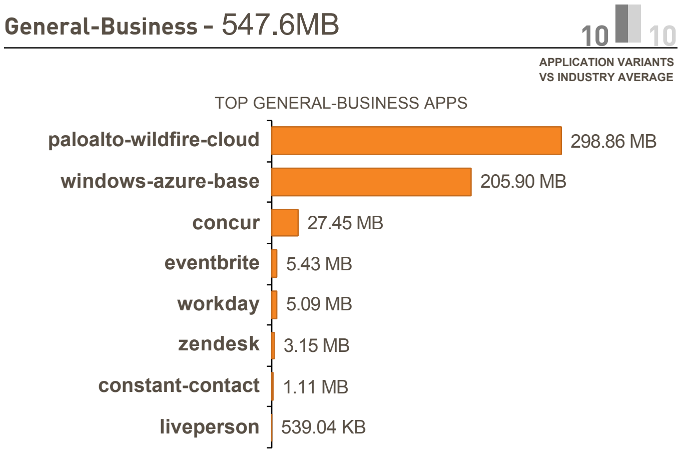


The following shows the top used applications by data movement within the subcategories identified above.

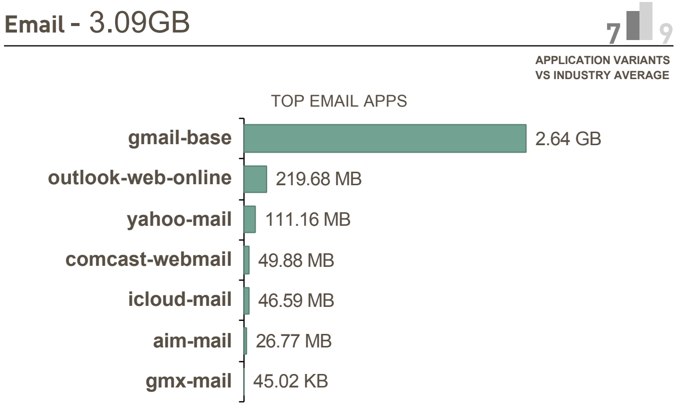
File-Sharing - 12.78GB



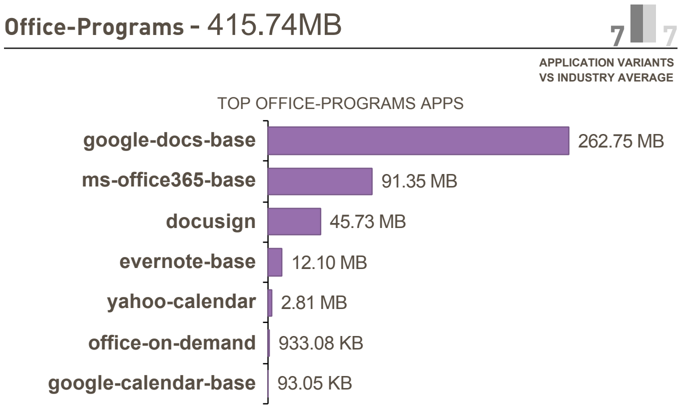
General-Business - 547.6MB



Email - 3.09GB



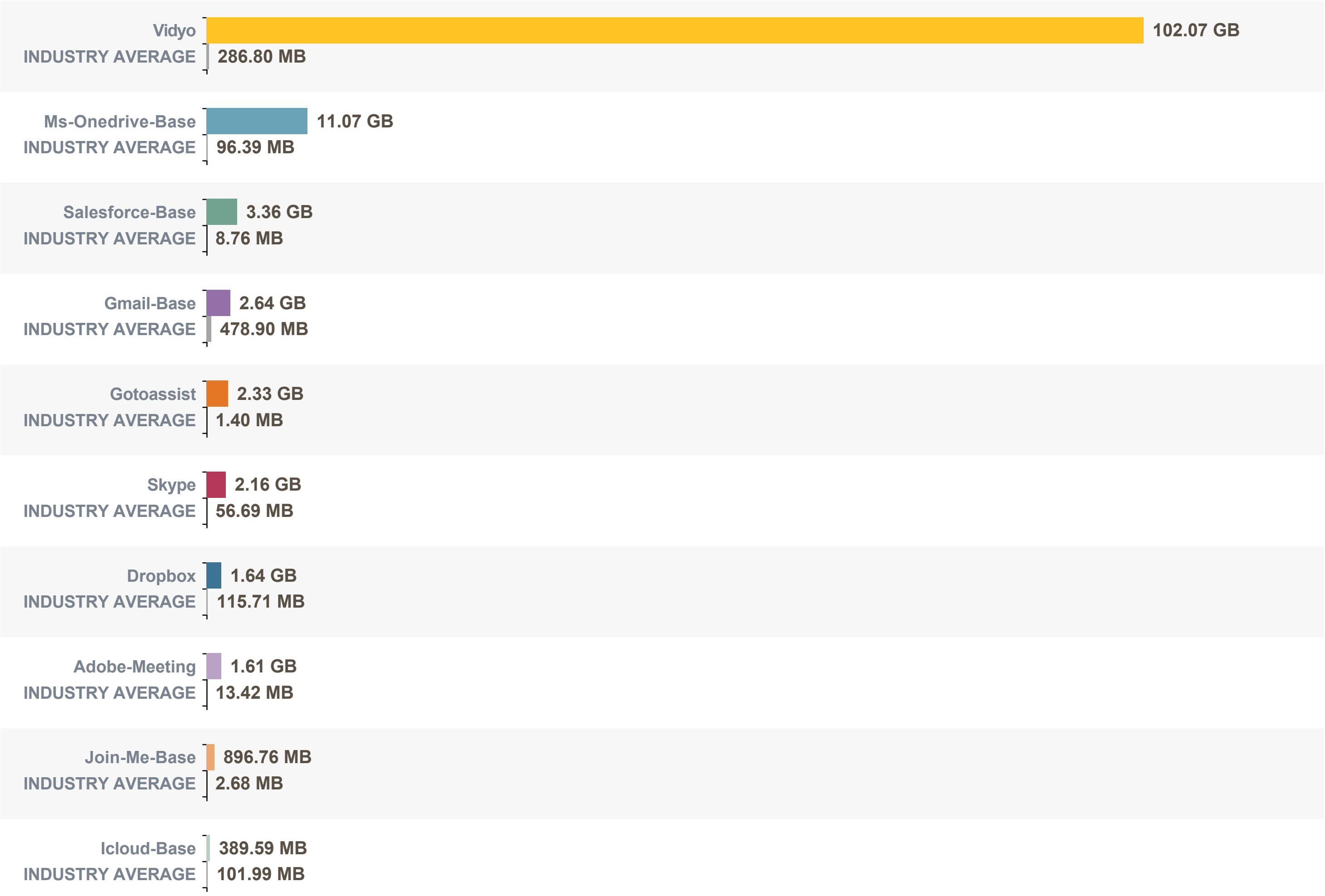
Office-Programs - 415.74MB



TOP SAAS APPLICATIONS

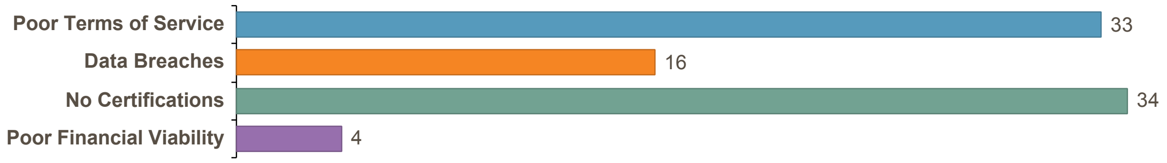
The following displays the top 10 SaaS applications used in your organization and the application usage comparison against your industry peers and all other Palo Alto Networks customers.

Top SaaS Applications by Data Movement



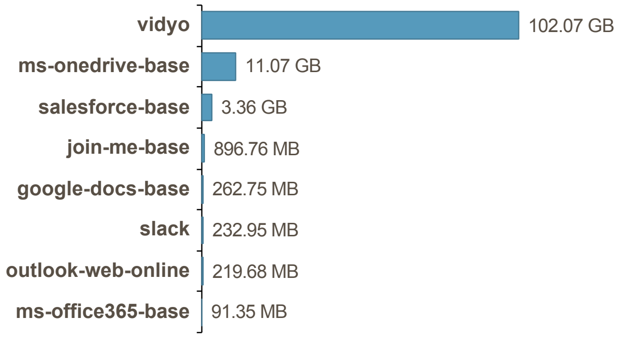
SaaS Applications by Hosting Risk

Based on your SaaS usage, it is imperative to regularly review SaaS applications being accessed, who is accessing them, and how they are being used.
The following chart displays the number of applications by each hosting risk characteristic.

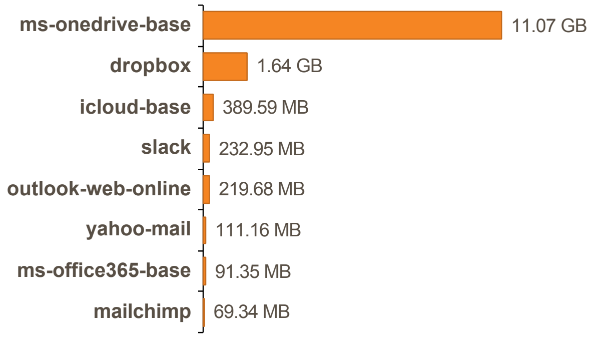


The following charts display the top applications by bandwidth for each hosting risk characteristic.

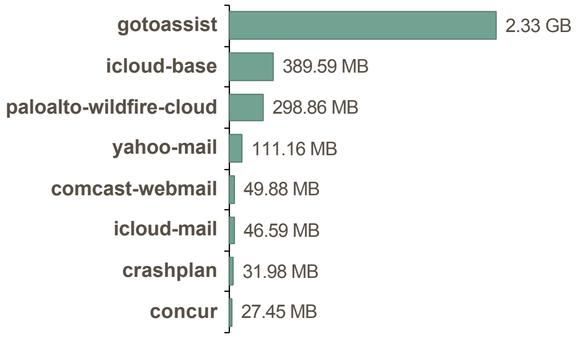
Apps with Poor Terms of Service - 118.53GB



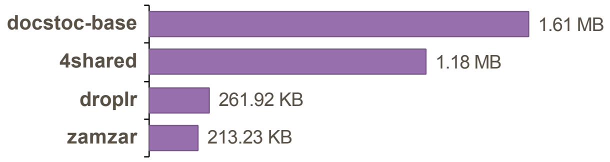
Apps with Data Breaches - 13.88GB



Apps with No Certifications - 3.35GB



Apps with Poor Financial Viability - 3.25MB



URL Activity

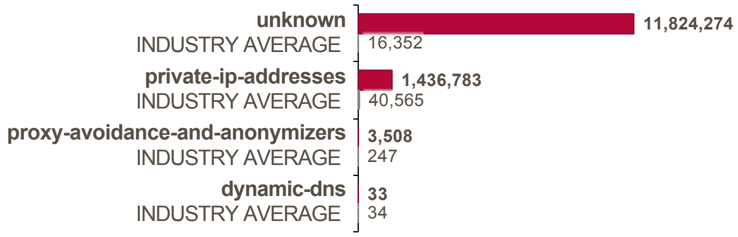
Uncontrolled Web surfing exposes organizations to security and business risks, including exposure to potential threat propagation, data loss, or compliance violations. The most common URL categories visited by users on the network are shown below.

Key Findings:

- High-traffic URL categories were observed on the network, including **web-based-email, unknown and business-and-economy**.
- Users visited a total of **82,005,300** URLs during the report time period across **56** categories.
- There was a variety of personal and work-related Web activity present, including visits to potentially risky websites.

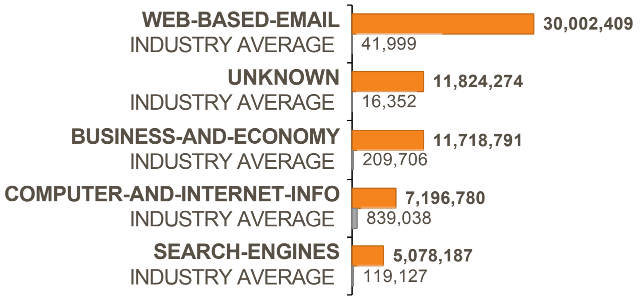
High-Risk URL Categories

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.



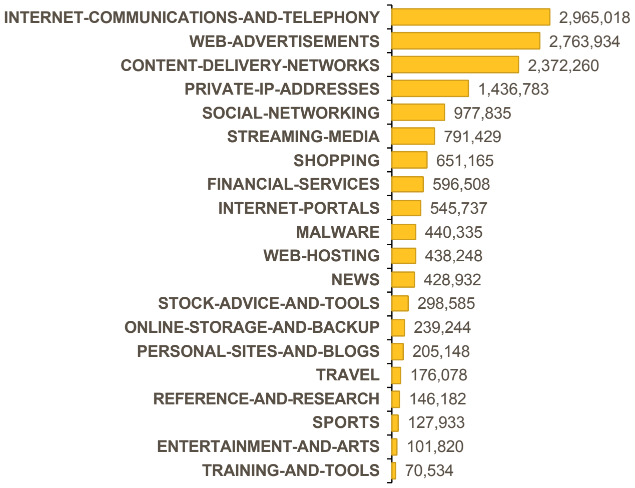
High-Traffic URL Categories

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



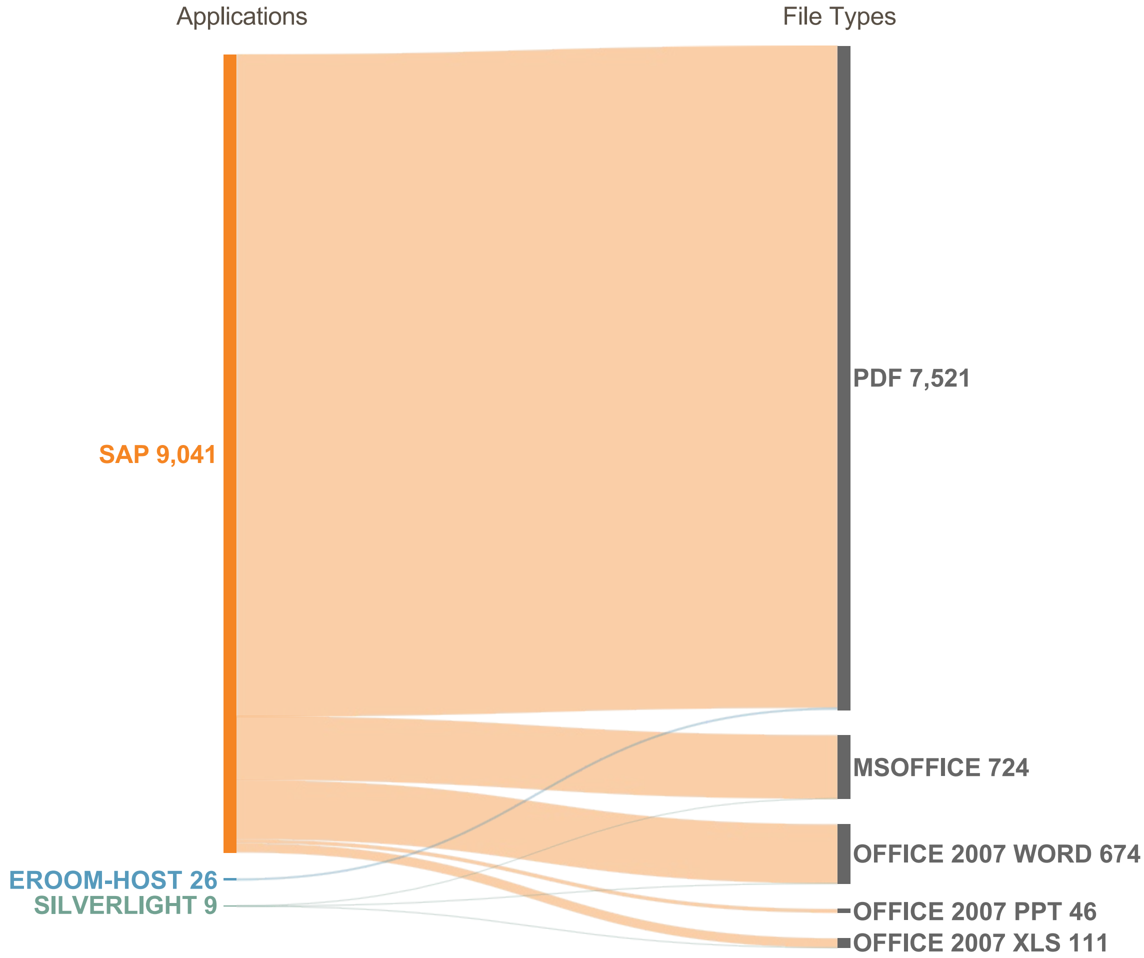
Commonly Used URL Categories

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, **11** file types were delivered via a total of **3** applications. The image below correlates the applications most commonly used to transfer files, along with the most prevalent file and content types observed.



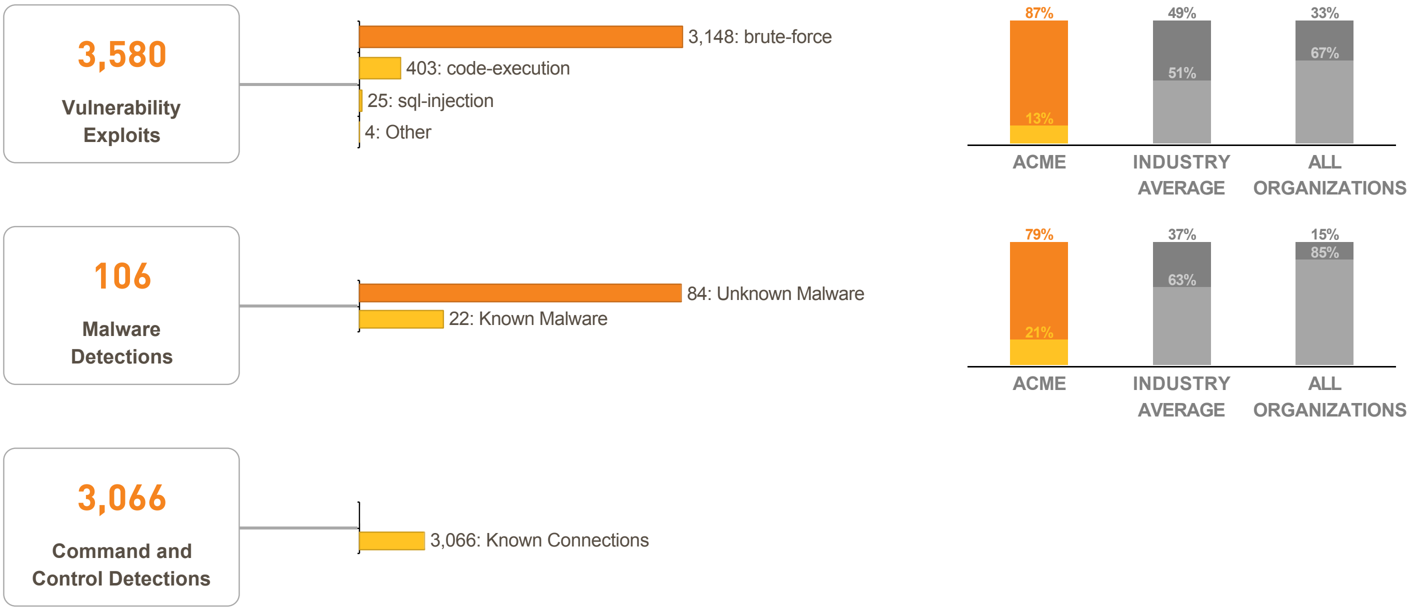
3
Applications
transferred
11
File Types

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.

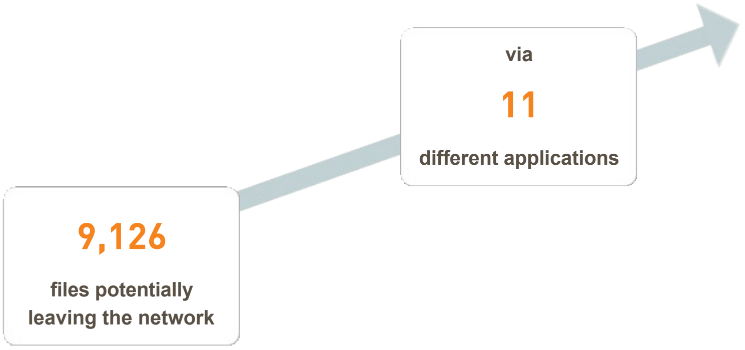
Key Findings:

- **3,580** total vulnerability exploits were observed in your organization, including **brute-force, code-execution and sql-injection**.
- **106** malware events were observed, versus an industry average of **1,346** across your peer group.
- **3,066** total command and control requests were identified, indicating attempts by malware to communicate with 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

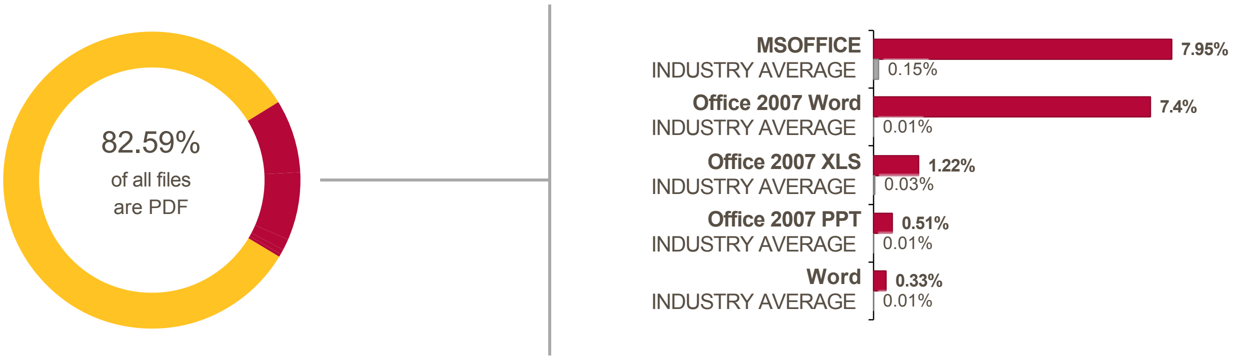
Today's cyber attackers use a variety of file types to deliver malware and exploits, often focusing on content from common business applications present in most enterprise networks. The majority of commodity threats are delivered via executable files, with more targeted and advanced attacks often using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

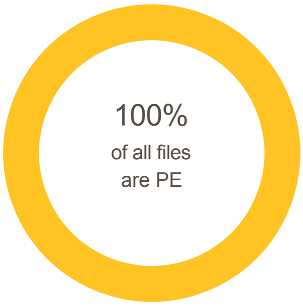
High-Risk File Types

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.

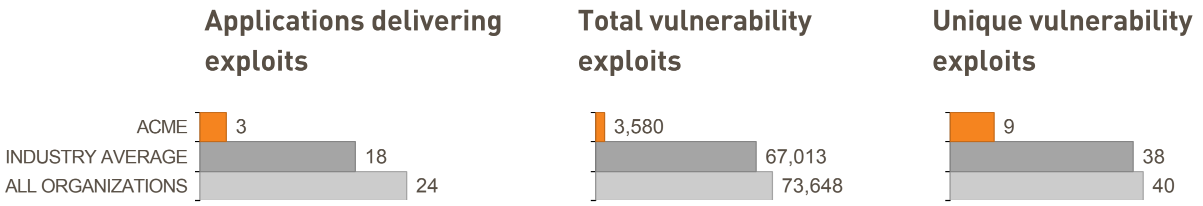


Application Vulnerabilities

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:

- **3** total applications were observed delivering exploits to your environment.
- **3,580** total vulnerability exploits were observed across the following top three applications: **web-browsing, web-browsing and web-browsing**.
- **9** unique vulnerability exploits were found, meaning attackers continued to attempt to exploit the same vulnerability multiple times.



Vulnerability Exploits per Application (top 5 applications with most detections)

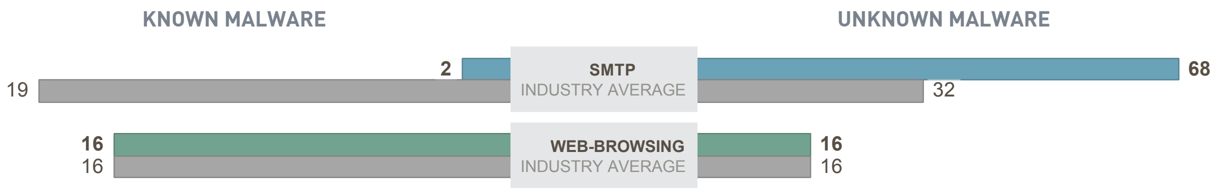
DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY ▾	THREAT TYPE	CVE ID
3,576	**web-browsing**			
9	Microsoft IE GIF Parsing Double Free Vulnerability	Critical	code-execution	CVE-2003-1048
1,573	HTTP Unauthorized Brute Force Attack	High	brute-force	
1,573	HTTP: User Authentication Brute Force Attempt	High	brute-force	
394	Apache Tomcat Windows Installer Default Account Access Vulnerability	High	code-execution	CVE-2011-1889
25	HTTP SQL Injection Attempt	Medium	sql-injection	
1	Microsoft ASP.NET Path Validation Security Bypass Vulnerability	Medium	info-leak	CVE-2004-0847
1	WordPress Cuckootap Theme Arbitrary File Download Vulnerability	Medium	info-leak	
2	**smtp**			
2	QK SMTP Remote Buffer Overflow Vulnerability	Medium	overflow	CVE-2006-5551
2	**ftp**			
2	FTP: login Brute Force attempt	High	brute-force	

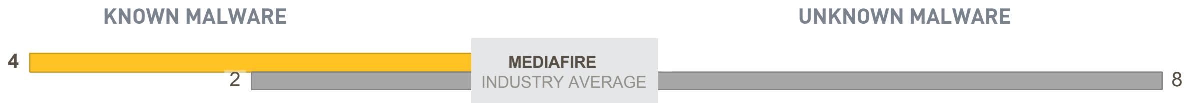
Known and Unknown Malware

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:

- **3** total applications were observed delivering malware to your organization, out of **328** 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.





3

applications found delivering malware

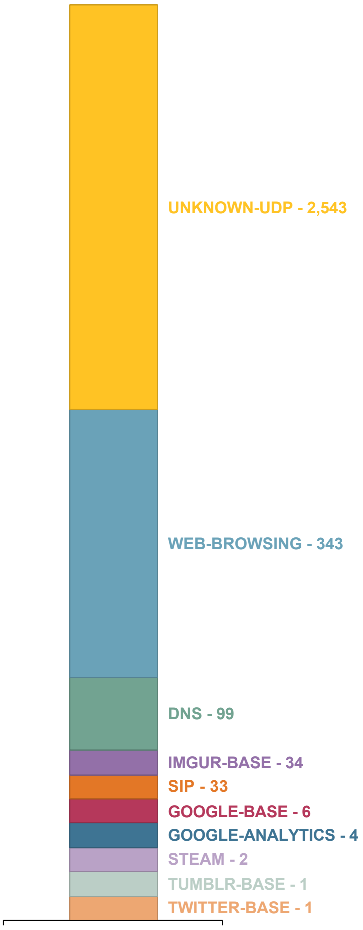
Command and Control Analysis

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

Key Findings:

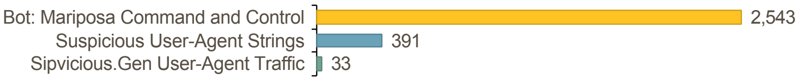
- **10** total applications were used for command-and-control communication.
- **3,066** total command-and-control requests were seen on your network.
- **99** total suspicious DNS queries were observed.

COMMAND AND CONTROL ACTIVITY BY APPLICATION



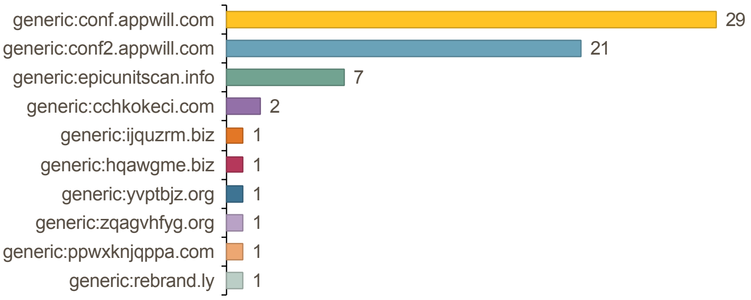
Spyware Phone Home: 2,967

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



Suspicious DNS Queries: 99

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 **photo-video, internet-utility and file-sharing** were observed on the network, which should be investigated due to their potential for abuse.
- **328** total applications were seen on the network across **28** sub-categories, as opposed to an industry average of **224** total applications seen in other **High Technology** organizations.
- **3,580** total vulnerability exploits were observed across the following top three applications: **web-browsing, web-browsing and web-browsing**.
- **106** malware events were observed, versus an industry average of **1,346** across your peer group.
- **10** total applications were used for command and control communication.

328
APPLICATIONS IN USE

75
HIGH RISK APPLICATIONS

6,752
TOTAL THREATS

3,580
VULNERABILITY EXPLOITS

22
KNOWN MALWARE

84
UNKNOWN MALWARE

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.