



SECURITY LIFECYCLE REVIEW

ACME



PREPARED BY:

Acme

The Security Lifecycle Review summarizes the threat exposure and security risks facing **ACME** and the customers connecting to their networks. The data used for this analysis was gathered by Palo Alto Networks during the report time period. The report provides actionable intelligence and risk assessment around the applications, URL traffic, and types of content that are traversing the **ACME** network as well as volume and types of threats and vulnerabilities that are observed. Recommendations are provided that can be employed to reduce the overall risk exposure for both the network operator and their customers.

Report Period: 10 DAYS

Wed, Jan 1, 2020 - Fri, Jan 10, 2020

Confidential Information - Do Not Redistribute



TABLE OF CONTENTS

3 Executive Summary

4 Applications

Applications at a Glance
Applications that Introduce Risk
Applications that Introduce Risk — Detail
SaaS Applications

16 URL Activity

URL Activity

17 File Transfer

File Transfer Analysis

18 DNS Security Analysis

Traffic Distribution
Domains and Destination Distribution
Malicious Traffic Destination Countries and Dns Tunneling Requests
Known Malware and Families

24 Threats

Threats at a Glance
High-Risk and Malicious File Type Analysis
Application Vulnerabilities
Known and Unknown Malware
Command and Control Analysis

31 IoT Security

Device Overview and Analysis
Risk Overview
Alerts Overview
Network Segments With A Mix Of IoT And Non-IoT Devices
Vulnerabilities Overview

39 Summary



Executive Summary For ACME

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.

Confidential Information - Do Not Redistribute

KEY FINDINGS

664

APPLICATIONS IN USE

664 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.

130

HIGH RISK APPLICATIONS

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

211

SAAS APPLICATIONS

211 SaaS applications were observed in your network. To maintain administrative control, adopt SaaS applications that will be managed by your IT team.

121,744

VULNERABILITY EXPLOITS

121,744 total vulnerability exploits were observed in your organization, including **info-leak**, **code-execution** and **brute-force**.

123,285

TOTAL THREATS

123,285 total threats were found on your network, including vulnerability exploits, known and unknown malware, and outbound command and control activity.

74

MALWARE

60 known malware and **14** unknown malware events were observed in your organization.



Applications at a Glance

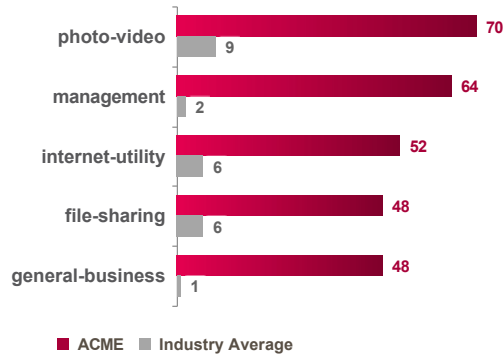
Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision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

KEY FINDINGS

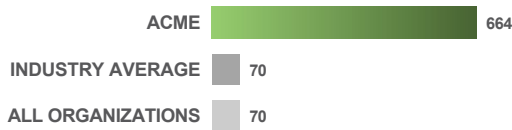
- High-risk applications such as **photo-video, management and internet-utility** were observed on the network, which should be investigated due to their potential for abuse.
- **664** total applications were seen on the network across **28** sub-categories, as opposed to an industry average of **70** total applications seen in other **High Technology** organizations.
- **55.81 TB** was used by all applications, including **networking** with **27.87 TB**, compared to an industry average of **104.54 GB** in similar organizations.

HIGH-RISK APPLICATIONS

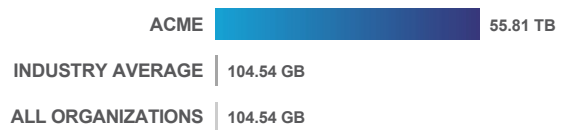
The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.



NUMBER OF APPLICATIONS ON NETWORK

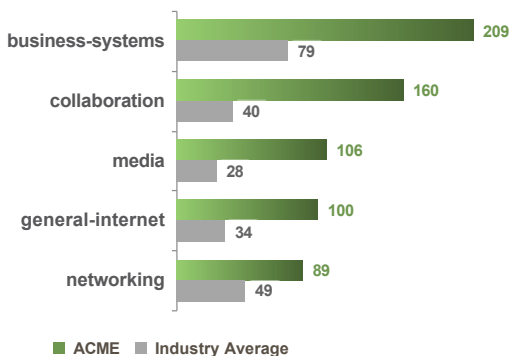


BANDWIDTH CONSUMED BY APPLICATIONS



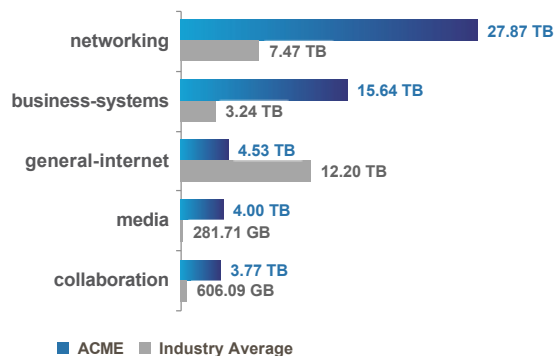
CATEGORIES WITH THE MOST APPLICATIONS

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



KEY FINDINGS

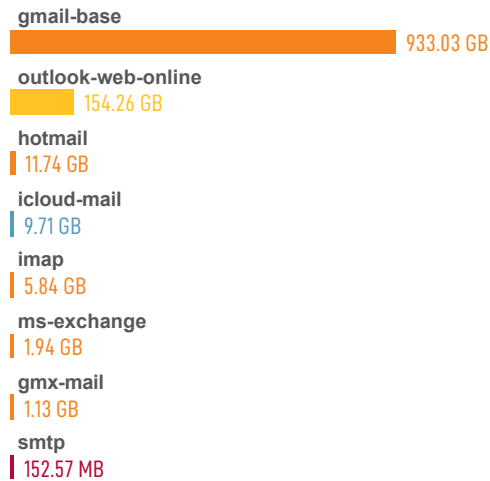
- A total of **664** applications were seen in your organization, compared to an industry average of **70** in other **High Technology** organizations.
- The most common types of application subcategories are **photo-video, management and internet-utility**.
- The application subcategories consuming the most bandwidth are **encrypted-tunnel, storage-backup and infrastructure**.

■ Number of Applications in the subcategory ■ Industry Average



Email 1.12 TB

TOP EMAIL APPS

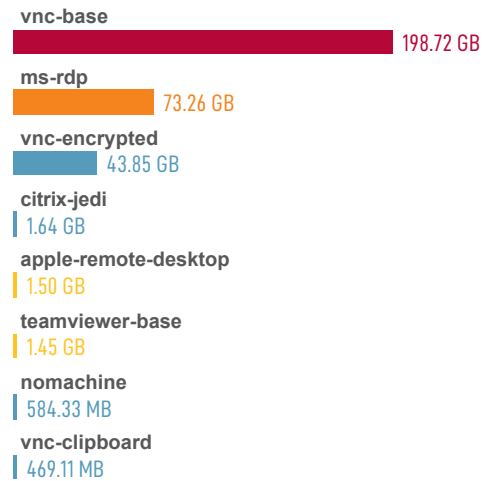


■ Number of Applications in the subcategory ■ Industry Average



Remote-Access 322.41 GB

TOP REMOTE-ACCESS APPS



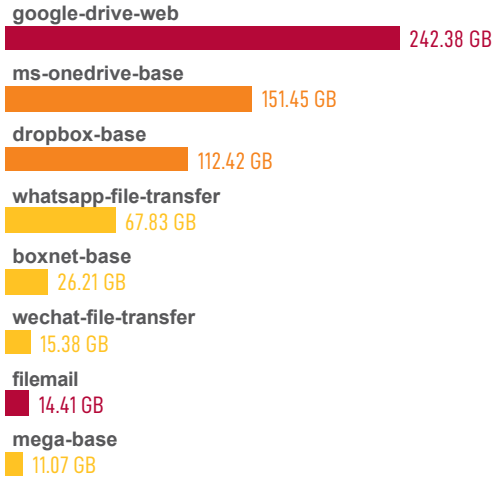


■ Number of Applications in the subcategory ■ Industry Average



File-Sharing 656.12 GB

TOP FILE-SHARING APPS

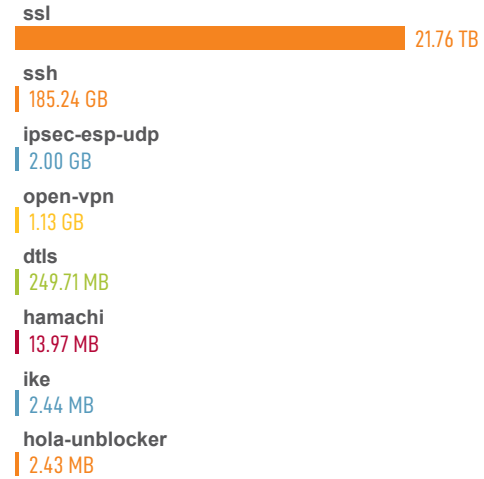


■ Number of Applications in the subcategory ■ Industry Average



Encrypted-Tunnel 21.95 TB

TOP ENCRYPTED-TUNNEL APPS

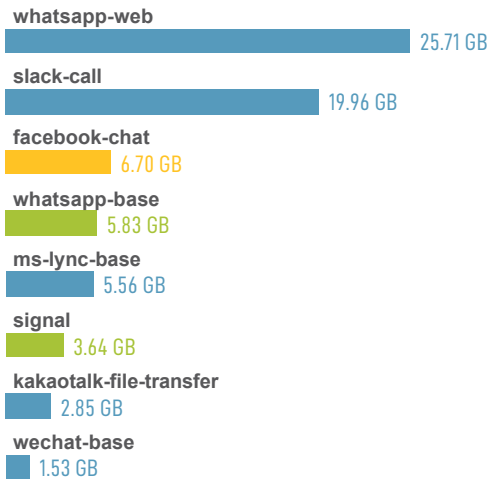


■ Number of Applications in the subcategory ■ Industry Average



Instant-Messaging 75.21 GB

TOP INSTANT-MESSAGING APPS

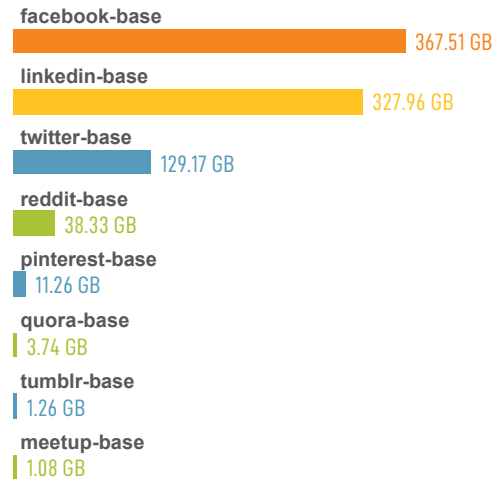


■ Number of Applications in the subcategory ■ Industry Average



Social-Networking 881.8 GB

TOP SOCIAL-NETWORKING APPS



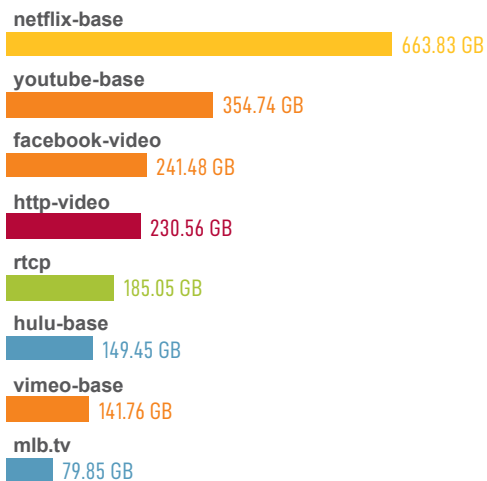


■ Number of Applications in the subcategory ■ Industry Average



Photo-Video 2.27 TB

TOP PHOTO-VIDEO APPS

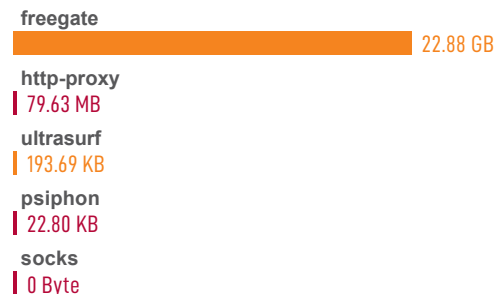


■ Number of Applications in the subcategory ■ Industry Average



Proxy 22.96 GB

TOP PROXY APPS





Applications that Introduce Risk — Detail

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
4	gmail-base	collaboration	email	browser-based	933.03 GB	2370058
3	outlook-web-online	collaboration	email	browser-based	154.26 GB	678133
4	hotmail	collaboration	email	browser-based	11.74 GB	35234
2	icloud-mail	collaboration	email	client-server	9.71 GB	43657
4	imap	collaboration	email	client-server	5.84 GB	9111
4	ms-exchange	collaboration	email	client-server	1.94 GB	666
4	gmx-mail	collaboration	email	browser-based	1.13 GB	5033
5	smtp	collaboration	email	client-server	152.57 MB	719
4	ssl	networking	encrypted-tunnel	browser-based	21.76 TB	80298246
4	ssh	networking	encrypted-tunnel	client-server	185.24 GB	70736
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	2 GB	1785
3	open-vpn	networking	encrypted-tunnel	client-server	1.13 GB	474
1	dtls	networking	encrypted-tunnel	client-server	249.71 MB	128
5	hamachi	networking	encrypted-tunnel	peer-to-peer	13.97 MB	1
2	ike	networking	encrypted-tunnel	client-server	2.44 MB	250
4	hola-unblocker	networking	encrypted-tunnel	client-server	2.43 MB	3437
5	google-drive-web	general-internet	file-sharing	browser-based	242.38 GB	200780
4	ms-onedrive-base	general-internet	file-sharing	client-server	151.45 GB	246374
4	dropbox-base	general-internet	file-sharing	client-server	112.42 GB	185852
3	whatsapp-file-transfer	general-internet	file-sharing	client-server	67.83 GB	24303
3	boxnet-base	general-internet	file-sharing	browser-based	26.21 GB	71887
3	wechat-file-transfer	general-internet	file-sharing	client-server	15.38 GB	26266
5	filemail	general-internet	file-sharing	browser-based	14.41 GB	256
3	mega-base	general-internet	file-sharing	browser-based	11.07 GB	1496
2	whatsapp-web	collaboration	instant-messaging	browser-based	25.71 GB	217978

Notes:



RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
2	slack-call	collaboration	instant-messaging	browser-based	19.96 GB	12383
3	facebook-chat	collaboration	instant-messaging	browser-based	6.7 GB	63930
1	whatsapp-base	collaboration	instant-messaging	client-server	5.83 GB	10139
2	ms-lync-base	collaboration	instant-messaging	client-server	5.56 GB	1588
1	signal	collaboration	instant-messaging	client-server	3.64 GB	56990
2	kakaotalk-file-transfer	collaboration	instant-messaging	client-server	2.85 GB	440
2	wechat-base	collaboration	instant-messaging	client-server	1.53 GB	249783
3	netflix-base	media	photo-video	browser-based	663.83 GB	176141
4	youtube-base	media	photo-video	browser-based	354.74 GB	137595
4	facebook-video	media	photo-video	browser-based	241.48 GB	54741
5	http-video	media	photo-video	browser-based	230.56 GB	38210
1	rtcp	media	photo-video	client-server	185.05 GB	6155
2	hulu-base	media	photo-video	browser-based	149.45 GB	26004
4	vimeo-base	media	photo-video	browser-based	141.76 GB	53115
2	mlb.tv	media	photo-video	browser-based	79.85 GB	1037
4	freegate	networking	proxy	client-server	22.88 GB	36662
5	http-proxy	networking	proxy	browser-based	79.63 MB	58682
4	ultrasurf	networking	proxy	client-server	193.69 KB	9
5	psiphon	networking	proxy	browser-based	22.8 KB	1
5	socks	networking	proxy	network-protocol	0 Byte	0
5	vnc-base	networking	remote-access	client-server	198.72 GB	1045
4	ms-rdp	networking	remote-access	client-server	73.26 GB	8197
2	vnc-encrypted	networking	remote-access	client-server	43.85 GB	1225
2	citrix-jedi	networking	remote-access	client-server	1.64 GB	78
3	apple-remote-desktop	networking	remote-access	client-server	1.5 GB	279

Notes:



RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
3	teamviewer-base	networking	remote-access	client-server	1.45 GB	1585
2	nomachine	networking	remote-access	client-server	584.33 MB	2
2	vnc-clipboard	networking	remote-access	client-server	469.11 MB	38
4	facebook-base	collaboration	social-networking	browser-based	367.51 GB	1046088
3	linkedin-base	collaboration	social-networking	browser-based	327.96 GB	1568579
2	twitter-base	collaboration	social-networking	browser-based	129.17 GB	351163
1	reddit-base	collaboration	social-networking	browser-based	38.33 GB	36584
2	pinterest-base	collaboration	social-networking	browser-based	11.26 GB	98841
1	quora-base	collaboration	social-networking	browser-based	3.74 GB	35123
2	tumblr-base	collaboration	social-networking	browser-based	1.26 GB	6783
1	meetup-base	collaboration	social-networking	browser-based	1.08 GB	737

Notes:



SaaS Applications

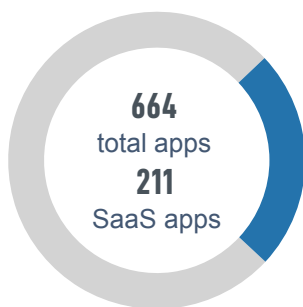
SaaS-based application services continue to redefine the network perimeter. Often labeled “shadow IT,” most of these services are adopted directly by individual users, business teams, or even entire departments. In order to minimize data security risks you need control over SaaS applications used your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

KEY FINDINGS

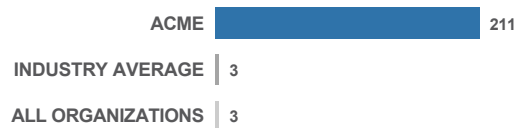
- **file-sharing** subcategory has the most number of unique SaaS applications.
- In terms of data movement, **crashplan** is the most used SaaS application in your organization.

SAAS APPLICATIONS BY NUMBERS

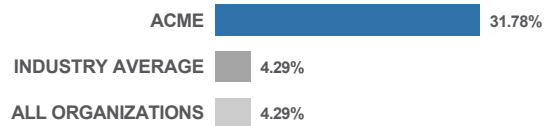
Review the applications being used in your organization. To maintain administrative control, adopt SaaS applications that will be managed by your IT team



NUMBER OF SAAS APPLICATIONS

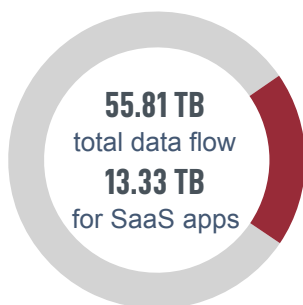


PERCENTAGE OF ALL APPLICATIONS

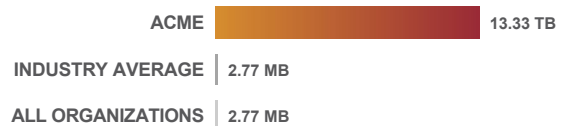


SAAS APPLICATION BANDWIDTH

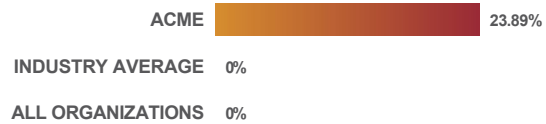
Monitor the volume of data movement to and from SaaS applications. Understand the nature of the applications and how they are being used



SAAS APPLICATION BANDWIDTH



PERCENTAGE OF ALL BANDWIDTH





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



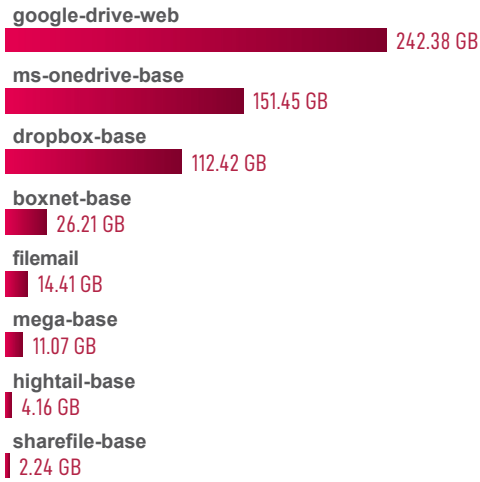
■ Number of Applications in the subcategory ■ Industry Average

■ Number of Applications in the subcategory ■ Industry Average



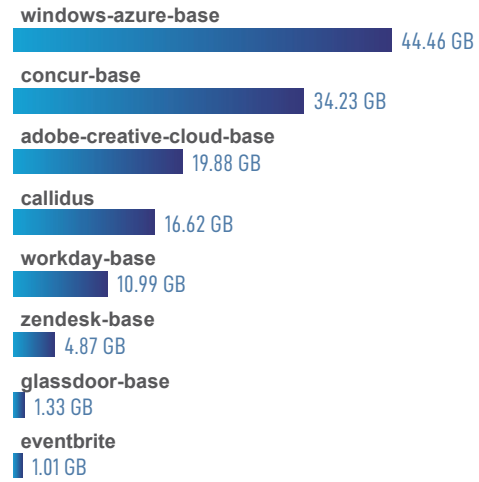
File-Sharing 568.12 GB

TOP FILE-SHARING APPS



General-Business 134.78 GB

TOP GENERAL-BUSINESS APPS



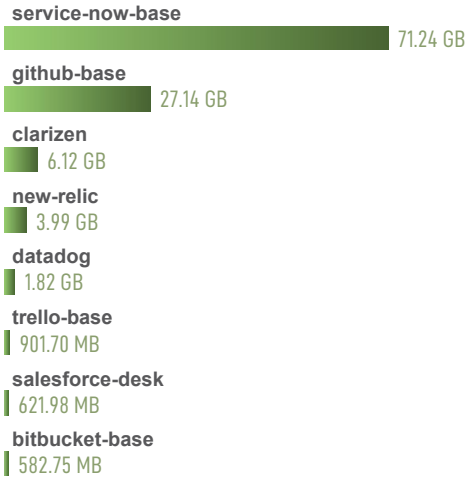


■ Number of Applications in the subcategory ■ Industry Average



Management 112.89 GB

TOP MANAGEMENT APPS

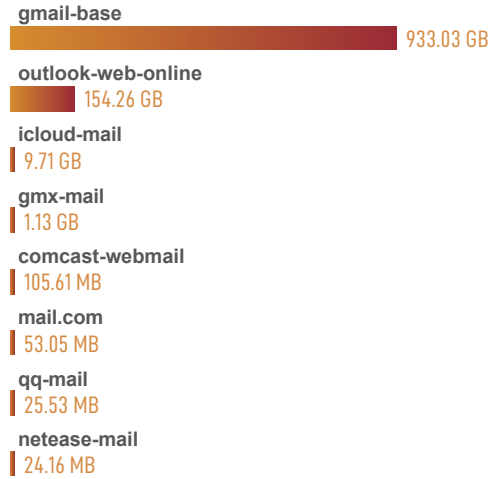


■ Number of Applications in the subcategory ■ Industry Average



Email 1.1 TB

TOP EMAIL APPS

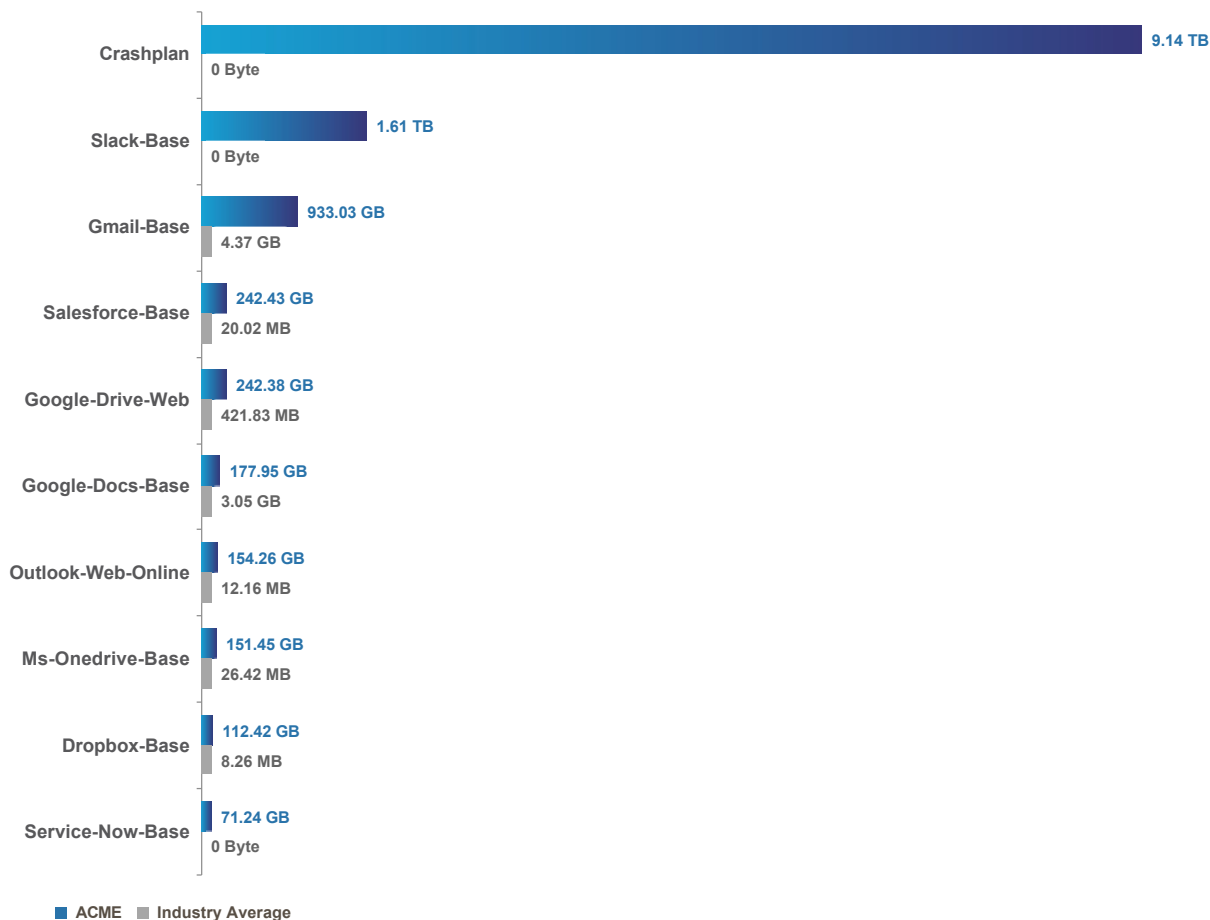




TOP SAAS APPLICATIONS

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

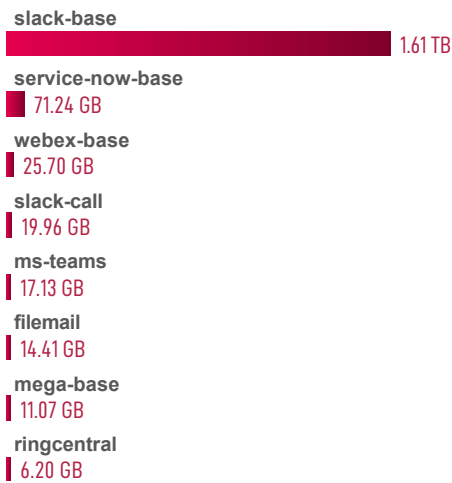
Based on your SaaS usage, it is imperative to regularly review SaaS applications being accessed, who is accessing them, and how they are being used. The following chart displays the number of applications by each hosting risk characteristic.



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

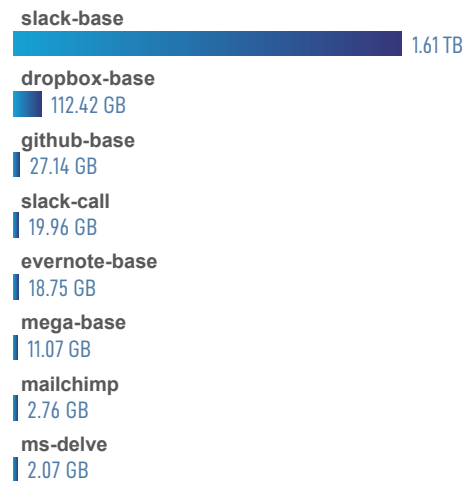
1.8 TB

Apps With Poor Terms Of Service



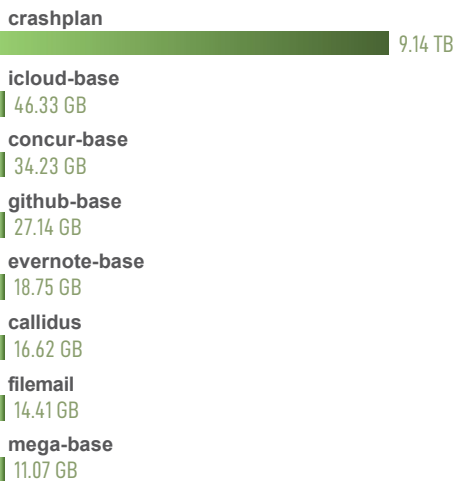
1.8 TB

Apps With Data Breaches



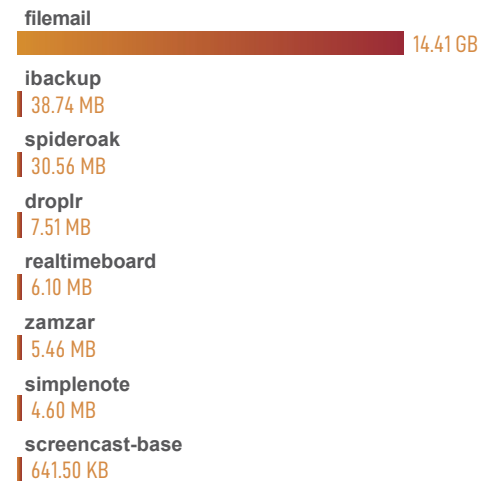
9.36 TB

Apps With No Certifications



14.5 GB

Apps With Poor Financial Viability





URL Activity

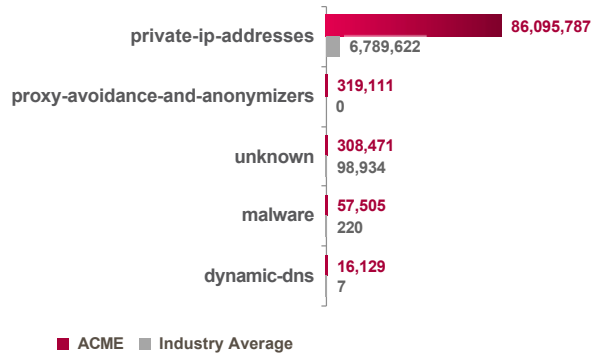
Uncontrolled Web surfing exposes organizations to security and business risks, including exposure to potential threat propagation, data loss, or compliance violations. The most common URL categories visited by users on the network are shown below.

KEY FINDINGS

- High-traffic URL categories were observed on the network, including **Bypass-decrypt-URLs, private-ip-addresses and computer-and-internet-info**.
- Users visited a total of **378,441,817** URLs during the report time period across **80** categories.
- There was a variety of personal and work-related Web activity present, including visits to potentially risky websites.

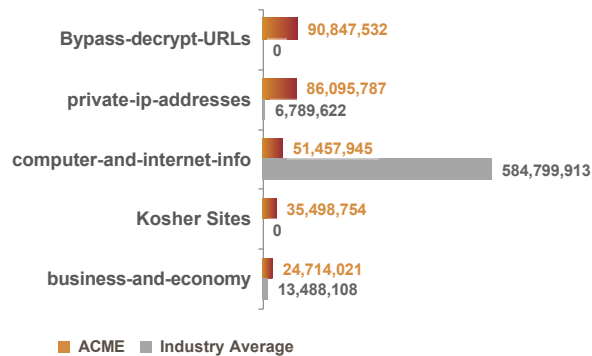
HIGH-RISK URL CATEGORIES

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.



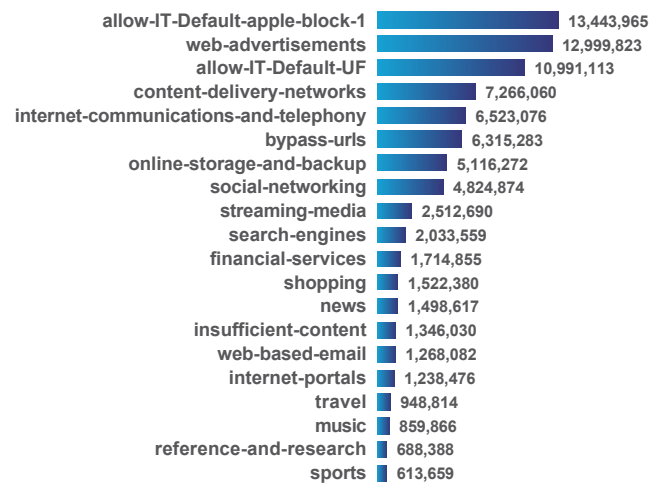
HIGH-TRAFFIC URL CATEGORIES

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



COMMONLY USED URL CATEGORIES

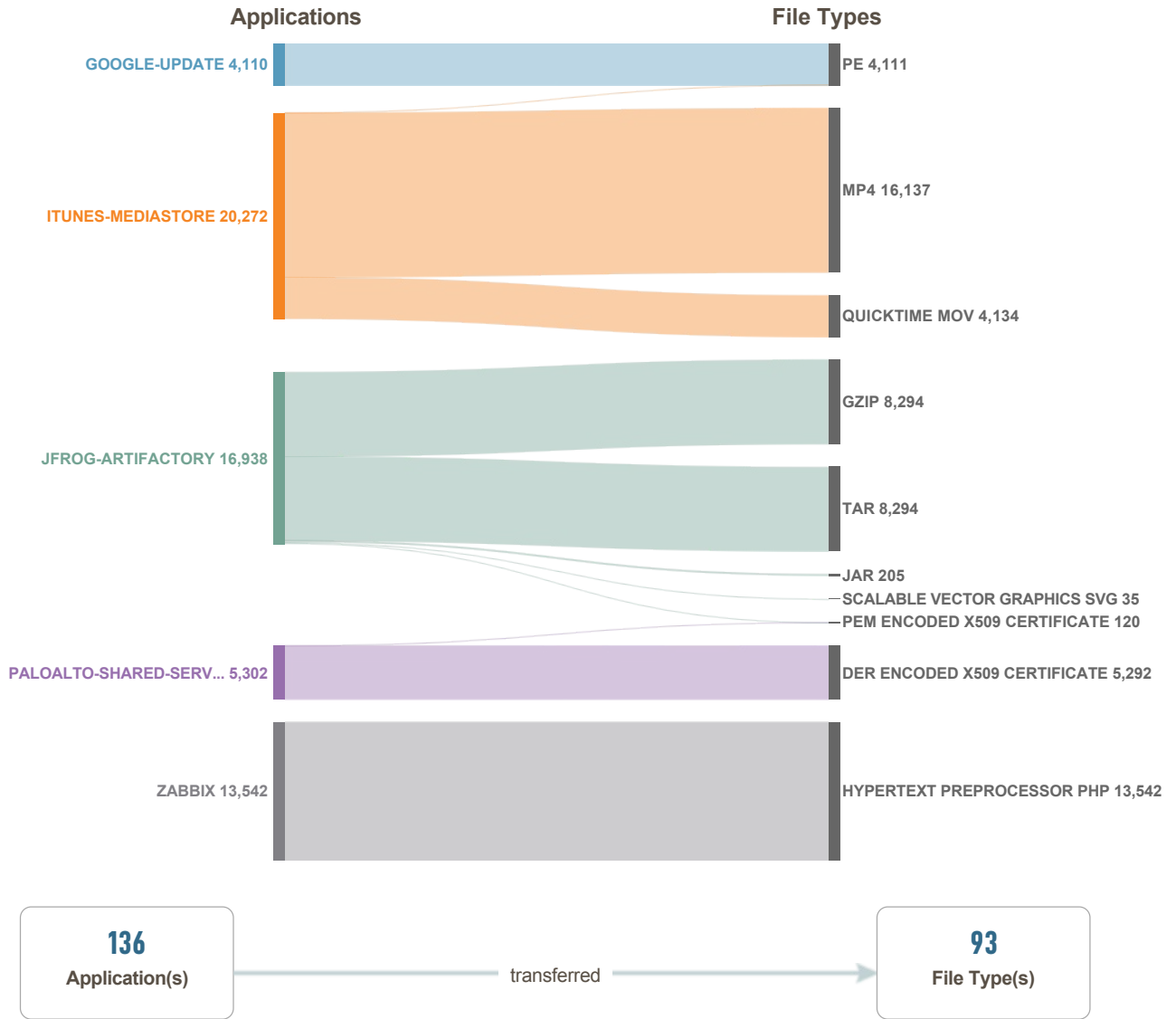
The top 20 most commonly visited URL categories are shown below.





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, **93** file types were delivered via a total of **136** applications. The image below correlates the applications most commonly used to transfer files, along with the most prevalent file and content types observed.





DNS Security Analysis

Fri, Jan 04, 2019 - Sat, Jan 11, 2020

294,412

DNS REQUESTS ANALYZED

The real-time DNS Security service has analyzed **294,412** DNS requests in your network. DNS is an often overlooked attack surface that can be used for malware delivery, command-and-control (C2), or data exfiltration.

1,651

MALICIOUS DOMAINS IDENTIFIED

The DNS Security service has identified **1,651** malicious domains. These domains were used by domain generation algorithms (DGAs), DNS tunneling or malware.

37

MALICIOUS IP ADDRESSES

The DNS Security service has identified **37** malicious IP addresses from malicious domains. These IP addresses can be used as C2 infrastructure to exfiltrate data or deliver malware or remote commands to a system in your network.

10

DESTINATION COUNTRIES HOSTING MALICIOUS DOMAINS

The DNS Security service has identified **10** destination countries that host these malicious domains.

4

MALWARE FAMILIES

The DNS Security service has identified malicious traffic of **4** different malware families.

1,699

MALICIOUS DNS REQUESTS IDENTIFIED

The DNS Security service has identified **1,699** malicious DNS requests in your network.

* Malicious IP addresses resolved from malicious domains are collected from public DNS resolvers and thus not necessarily the same IPs contained in the original DNS responses.

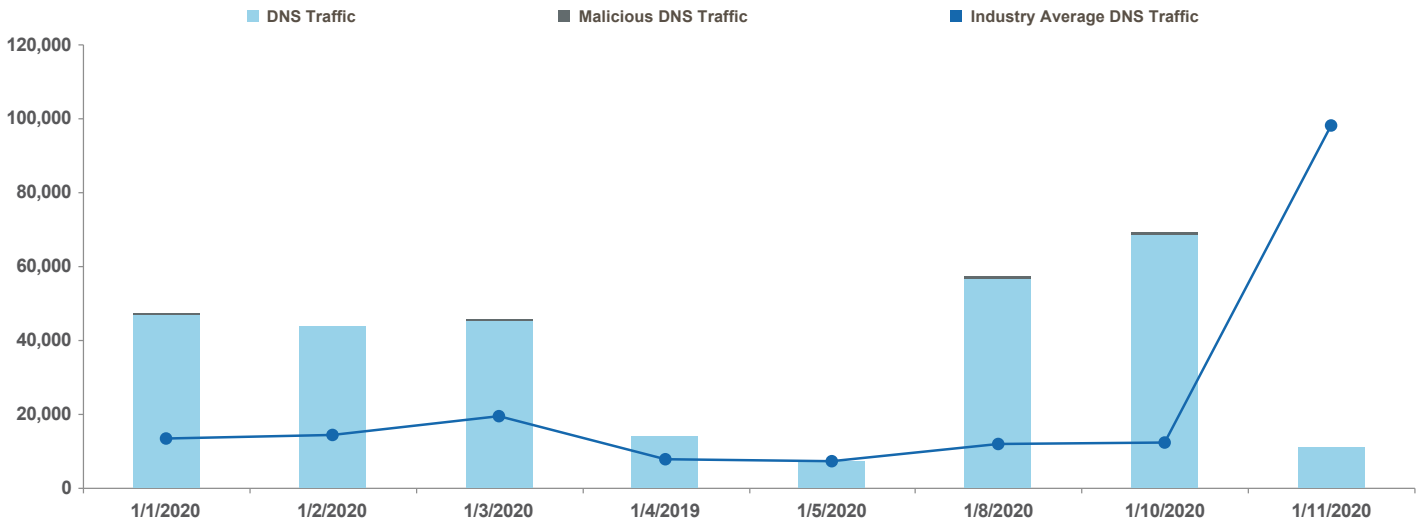


TRAFFIC DISTRIBUTION

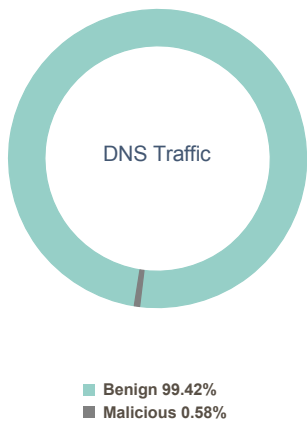
Many security teams don't inspect DNS traffic for threats because they assume queries sent over DNS protocol and port 53 are benign. In addition to how prevalent and easily abused DNS is, the sheer rate and volume of new malicious domains is enormous, and static signatures cannot be created quickly enough to keep up. If a system gets infected, networking and security teams are challenged to quickly identify that system and address the infection. By then, malware may have already spread, or data may have already been stolen.

KEY FINDINGS

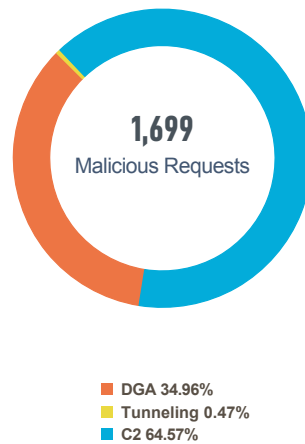
- A total of **294,412** DNS queries were observed on your network
- **1,651** malicious domains were observed including C2, DGA and Tunneling



DNS TRAFFIC DISTRIBUTION



MALICIOUS TRAFFIC DISTRIBUTION

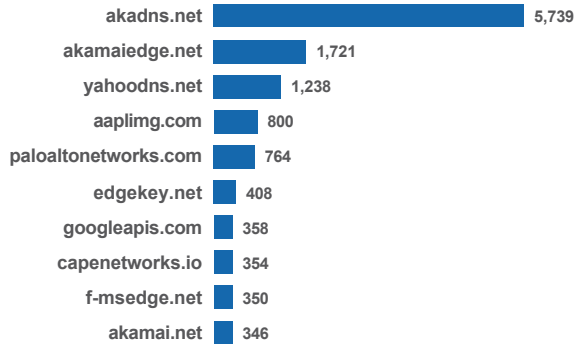




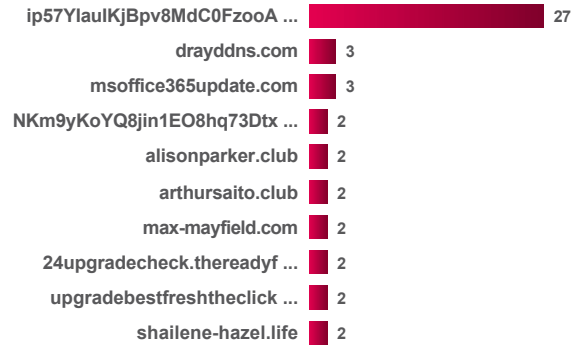
DOMAINS AND DESTINATION DISTRIBUTION

The following charts list the top domains and the top resolvers with the most traffic in your network. Malicious domains in your network should be reviewed to understand the volume of the domain requests, who is accessing those domains, and what malware families are associated with those domains.

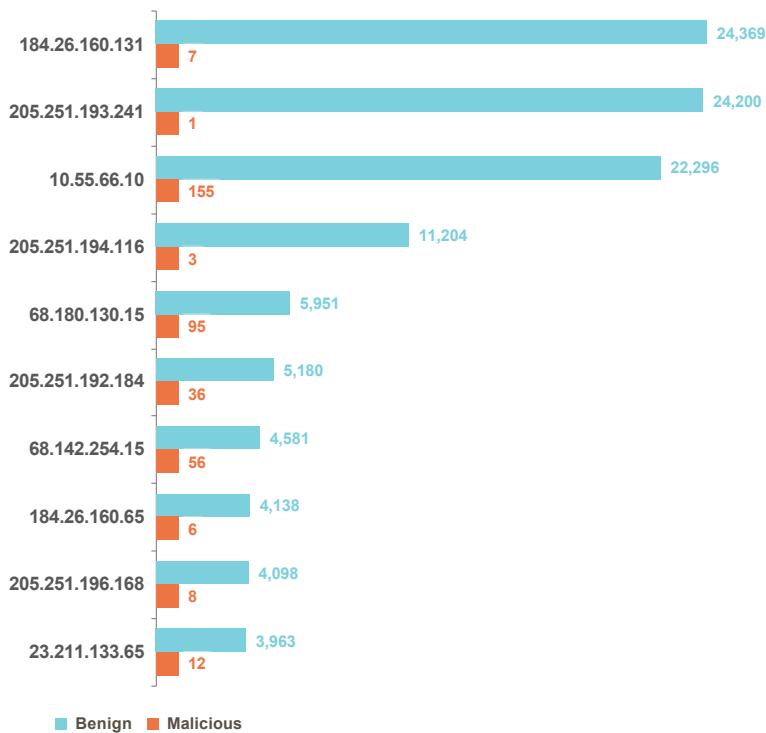
TOP DOMAINS BY TRAFFIC



TOP MALICIOUS DOMAINS BY TRAFFIC



TOP DNS RESOLVERS BY TRAFFIC





MALICIOUS TRAFFIC DESTINATION COUNTRIES AND DNS TUNNELING REQUESTS

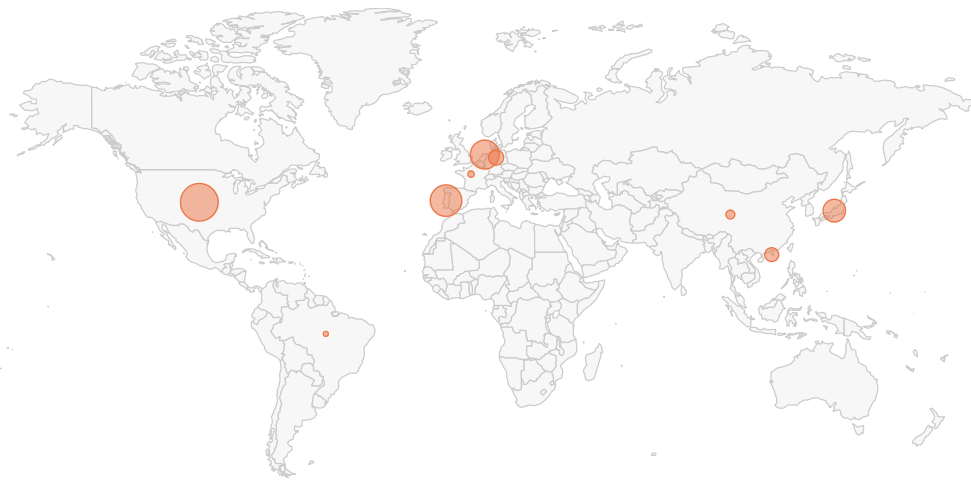
Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. This technique, lets attackers encode their payloads in small chunks within DNS requests to bypass security controls. Once a victim's device is compromised, the infected device sends a request within the DNS traffic. The DNS server is instructed to connect to the cybercriminals' server, establishing a channel through which to steal and transmit data.

With DNS tunneling, DNS requests pass through the normal DNS server, inside and outside a company's firewall. However, tunneled data hidden in the DNS requests goes unnoticed.

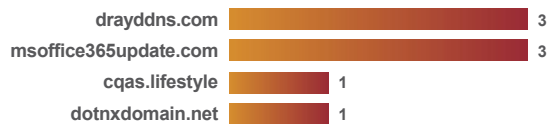
KEY FINDINGS

- **38.53%** of malicious domains are hosted in **United States of America**
- **8** DNS tunneling requests were found in your network
- **648 Bytes** of data was attempted to be sent out from your network through DNS Tunneling

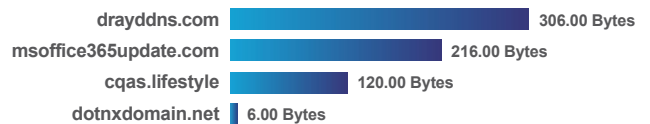
MALICIOUS TRAFFIC DESTINATION COUNTRIES



DNS TUNNELING REQUESTS BY DOMAIN



DNS TUNNELING VOLUME BY DOMAIN





KNOWN MALWARE AND FAMILIES

DNS can be used by malware authors as covert protocol channel that adversaries use for C2, data exfiltration and other nefarious tasks. The table below lists the number of malicious domains and the associated malware families and the corresponding top domains that were found in your network.

Malware Family	Domain Count	Top Domains	Description
corebot	424	<ul style="list-style-type: none"> zuxmq6zj3v.2oht04fdqqtsc7wk36r9.com ff1ezirsv.f6201t2ck46p8tytl0uxh.com pbkawm8j.pvw4q9jwak8k7w0i1qd09.com bben4w3yb8snl.6p3wwjgkm0ad7nb791s1pf o.com 8n53hitm.440h3plgzipn9i1cmrxumqv.com vdrrrzqk7y.9gw2b02ksbio9vmohnq.com 34stqmwg8xb.3o41t3wmqqr4a59tw9c.com 21iyfwq2cwm2.0u94ypjc1rvh98c2tc5mfe.co m rbqk9otr.q4yo6cnmdqqoxuuytyi.com e2sjkxz-z.tnjq7vffhfjlvrov31p.com 	<p>CoreBot's most interesting facility is its plugin system, enabling it to be modular and easily supplemented with new theft capabilities. CoreBot downloads plugins from its command-and-control (C&C) server right after setting its persistence mechanism on the endpoint. It then loads the plugins using the plugininit export function in the plugin's DLL. At present, the main plugin is called Stealer. CoreBot steals passwords, but it is currently incapable of intercepting real-time data from Web browsers. Instead, it steals saved passwords stored in the endpoint's browsers, scanning for passwords on all the most popular browsers. CoreBot further searches an extensive list of FTP clients, mail clients, webmail accounts, cryptocurrency wallets, private certificates and personal data from a list of various desktop applications.</p>
madmax	51	<ul style="list-style-type: none"> kzgnbpded-t.ddix48mepv.com bmsiexy-rhoc.lo8qv6se.com esdilcgea.rbj3qa042j.com 7ii-fz7fuzgj7.hk2emwvwp5.com 5k20kq2-mf-.r8zgbuqk1d.com xhdc4012h-rezryqfhaiy.dkdw1n5tsp.com rka9gednc3fe5.iz0wr3tp6h.com 0ccnmp1rd017.uvfc1nbf6y.com ylvqxqghrur10dk.1aivcvhlpv.com rp8k-mqi0rbqur7yhmq8bgztz.b4x30yypvl.co m 	<p>A targeted malware family which uses a DGA as a backup communications mechanism. Uses extensive obfuscation techniques to defeat static analysis attempts.</p>
rovnix	33	<ul style="list-style-type: none"> -xzhxfllwwz1sll.pwssp1gmj2nrgt7g3q.com 4hdxqomy.dxaqipn9y2pps35bkw.com j0usstgbf.to11ezu5urwhx9wube.com htf10ohutcynzaaiwngud.a7hkwbq3gezr0rz7 wh.com wgztxlamjq3.xy96dsgz7uhxlio4ma.com bwyj279xijma7x-wlxqpkhb.lrb40mqf13z84k3 pwn.com 85am8-dtbn9w.ljncjqv6x2hab0bos.com zvor0gjh6jmz.o685ynhvkw6pju2e5.com sg3jszce1u.wsw0ih1ms53hr47q2m.com 1n2p7kw5lkv03oy-guocb.4mdus62fjpt8asivc n.com 	<p>Rovnix writes malicious rootkit drivers to an unpartitioned space of the NTFS drive. This effectively hides the driver since this unpartitioned space cannot be seen by the operating system and security products.</p>



Malware Family	Domain Count	Top Domains	Description										
	35	<table border="1"> <tr><td>th1sib3stway.com</td></tr> <tr><td>u8e8fydab.6nbfw29txihd.com</td></tr> <tr><td>pezmbdpeu4y7ixv-zb.1nguexf7zpqf.com</td></tr> <tr><td>alm2prwkt9ui8gk2z6.0k5xm82mw80d.com</td></tr> <tr><td>zrwhz8jet4xayb.ba04ia33sq6u.com</td></tr> <tr><td>zgkwnkt0fawzgg9dyox.144bo9fsbrzw.com</td></tr> <tr><td>olnuoaagwosnxeni4v.k02t2kjqwxm6.com</td></tr> <tr><td>038chcugpom3kvm3cl-p.n8wil5110zyf.com</td></tr> <tr><td>vs1g3jajqps.w9gyas5zvplo.com</td></tr> <tr><td>kynewvagno8aj.y30vm6wxuyxc.com</td></tr> </table>	th1sib3stway.com	u8e8fydab.6nbfw29txihd.com	pezmbdpeu4y7ixv-zb.1nguexf7zpqf.com	alm2prwkt9ui8gk2z6.0k5xm82mw80d.com	zrwhz8jet4xayb.ba04ia33sq6u.com	zgkwnkt0fawzgg9dyox.144bo9fsbrzw.com	olnuoaagwosnxeni4v.k02t2kjqwxm6.com	038chcugpom3kvm3cl-p.n8wil5110zyf.com	vs1g3jajqps.w9gyas5zvplo.com	kynewvagno8aj.y30vm6wxuyxc.com	<p>Qadars is an advanced online banking Trojan that comes from a single source. Its source programs all operational components and does not buy injection kits from outsourced developers. When Qadars v3 was detected in the wild, the malware's operators dedicated a new attack configuration to targeting all the major banks in Australia. V3 of Qadars' fraud improvements: Browser hooking (IE, Firefox); Cookie and certificate theft; Form grabbing; Webinjections; FIGrabbers and ATS; Use of the Tor client on the victim's machine to hide malware communications; and Use of domain generation algorithm (DGA) to hide remote malware resources (as of v3). Qadars is capable of in-session fraud, remote-controlling the infected endpoint via virtual network computing (VNC) and performing a fraudulent transaction in real time when the user is logged on. Qadars can also collect victim credentials and use them in account takeover fraud at a later time and from a different device, depending on the targeted bank and the corresponding authentication challenges.</p>
th1sib3stway.com													
u8e8fydab.6nbfw29txihd.com													
pezmbdpeu4y7ixv-zb.1nguexf7zpqf.com													
alm2prwkt9ui8gk2z6.0k5xm82mw80d.com													
zrwhz8jet4xayb.ba04ia33sq6u.com													
zgkwnkt0fawzgg9dyox.144bo9fsbrzw.com													
olnuoaagwosnxeni4v.k02t2kjqwxm6.com													
038chcugpom3kvm3cl-p.n8wil5110zyf.com													
vs1g3jajqps.w9gyas5zvplo.com													
kynewvagno8aj.y30vm6wxuyxc.com													

- Linked to threats that belong to a certain Malware Family

- Part of a larger Campaign of attacks

- A type of Malicious Behavior that indicates that your system has been compromised

- An individual or group that instigates one or more campaigns using malware families

- An attack, usually in the form of a script, that takes advantage of a software or network weakness, bug, or vulnerability to manipulate the behavior of the system

- Public tags are tags shared with the AutoFocus community by your organization and other AutoFocus users. They are visible to all AutoFocus users.

- Unit 42 (alerting) tags are created by Unit 42 (the Palo Alto Networks® threat intelligence and research team) for threats and campaigns that pose a direct security risk.

- Unit 42 creates alerting tags for threats discovered by individuals or organizations outside of Unit 42. These tags have a pointed and marked top right corner.

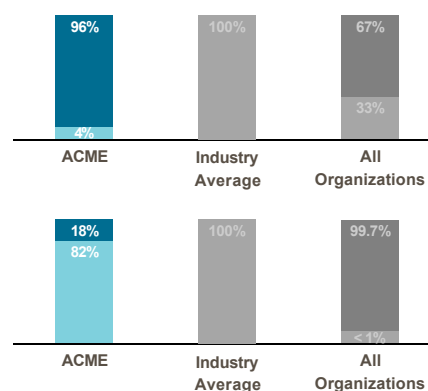
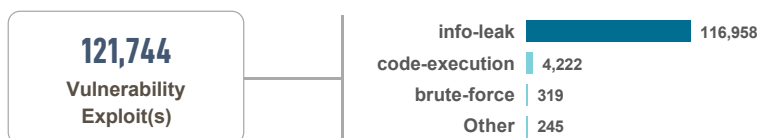


Threats at a Glance

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

- **121,744** total vulnerability exploits were observed in your organization, including **info-leak**, **code-execution** and **brute-force**.
- **74** malware events were observed, versus an industry average of **0** across your peer group.
- **1,467** total command and control requests were identified, indicating attempts by malware to communicate with attackers to download additional malware, receive instructions, or exfiltrate data.





High-Risk and Malicious File Type Analysis

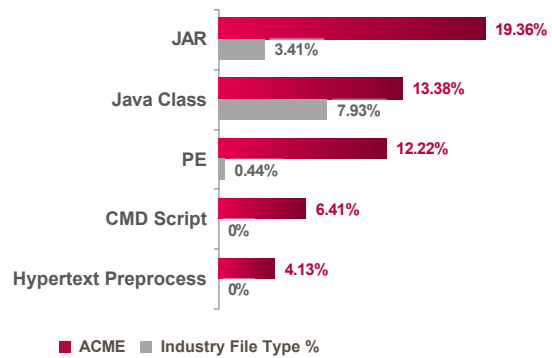
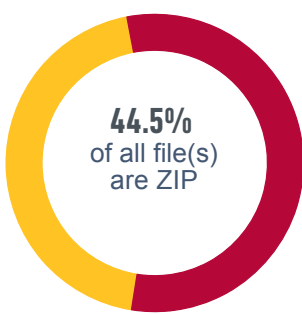
Today's cyber attackers use a variety of file types to deliver malware and exploits, often focusing on content from common business applications present in most enterprise networks. The majority of commodity threats are delivered via executable files, with more targeted and advanced attacks often using 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. Ensuring host prevention solutions perform local and remote analysis of such file types will provide additional protection at the endpoint.

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.





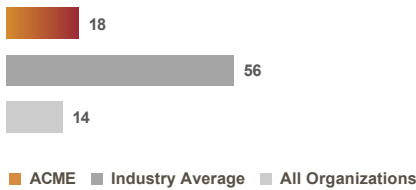
Application Vulnerabilities

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

- 18 total applications were observed delivering exploits to your environment.
- 121,744 total vulnerability exploits were observed across the following top three applications: **netbios-ns**, **ms-ds-smbv2** and **mount**.
- 50 unique vulnerability exploits were found, meaning attackers continued to attempt to exploit the same vulnerability multiple times.

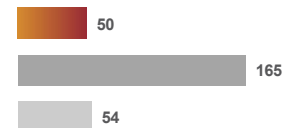
APPLICATIONS DELIVERING EXPLOITS



TOTAL VULNERABILITY EXPLOITS



UNIQUE VULNERABILITY EXPLOITS



■ ACME ■ Industry Average ■ All Organizations

VULNERABILITY EXPLOITS PER APPLICATION

(TOP 5 APPLICATIONS WITH MOST DETECTIONS)

DETECTIONS	EXPLOIT ID	SEVERITY
51,248	Netbios-Ns	
51,248	NetBIOS nbstat query	INFO
39,559	Ms-Ds-Smbv2	
9	Microsoft Windows RPC Fragment Evasion Attempt	MEDIUM
51	Microsoft Windows Registry Read Attempt	LOW
36,078	Windows Local Security Architect Security Identifier Lookup	INFO
2,272	Microsoft Office File with Macros Detected	INFO
768	Microsoft Windows Server Service NetrShareEnum access	INFO
366	Microsoft Windows Server Service NetrServerGetInfo Opnum 21 Access Attempt	INFO
9	Microsoft Windows user enumeration	INFO
3	Windows Local Security Architect LsarQueryInformationPolicy	INFO
2	Adobe PDF File With Embedded Javascript	INFO
1	Microsoft Windows Registry Enumeration	INFO
23,981	Mount	
23,981	UNIX NFS Export Directory Attempt	MEDIUM
4,666	Web-Browsing	
1,041	Bash Remote Code Execution Vulnerability	CRITICAL
298	HTTP /etc/passwd Access Attempt	CRITICAL



DETECTIONS	EXPLOIT ID	SEVERITY ▼
6	Linksys Devices Remote Code Execution Vulnerability	CRITICAL
2	Joomla Component SQL Injection Attempt Vulnerability	CRITICAL
1,894	Microsoft Windows win.ini Access Attempt Detected	HIGH
552	HTTP Cross Site Scripting Attempt	HIGH
317	HTTP Unauthorized Brute Force Attack	HIGH
216	Generic HTTP Cross Site Scripting Attempt	HIGH
50	HTTP Cross Site Scripting Vulnerability	HIGH
6	Webhints Improper URI Sanitization Remote Command Execution Vulnerability	HIGH

1,585 Ms-Ds-Smbv3

1	SMB: User Password Brute Force Attempt	HIGH
36	Windows Local Security Architect Isardelete access	LOW
1,052	Microsoft Windows Server Service NetrServerGetInfo Opnum 21 Access Attempt	INFO
252	Microsoft Windows user enumeration	INFO
124	Microsoft Windows Server Service NetrShareEnum access	INFO
116	Windows Local Security Architect LsarQueryInformationPolicy	INFO
4	Microsoft Office File with Macros Detected	INFO

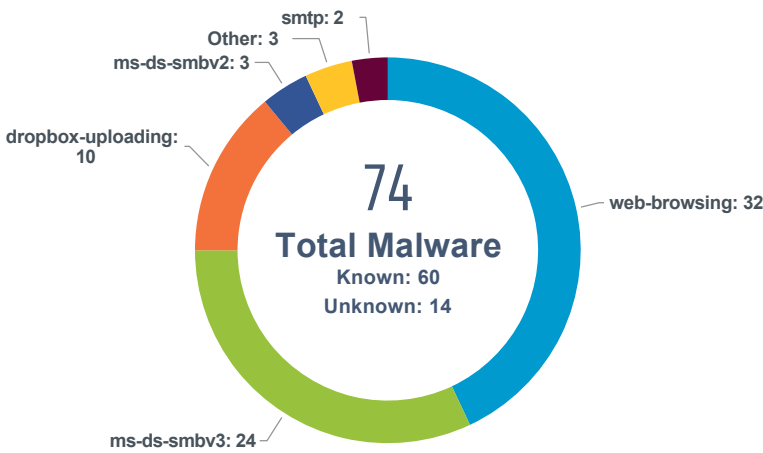


Known and Unknown Malware

Applications are the primary vector 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, or within an endpoint operating system, into which traditional security solutions have little or no visibility.

KEY FINDINGS

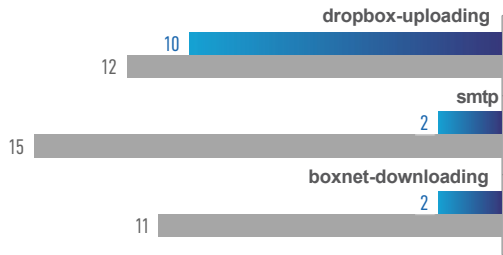
- 7 total applications were observed delivering malware to your organization.
- Many applications delivering malware are required to run your business, which means you need a solution that can prevent threats, while still enabling the applications.
- While most malware is delivered over HTTP or SMTP, advanced attacks will often use other applications, including those on non-standard ports or employing other evasive behavior.
- 7 malware were first detected at the endpoint. Coordinating threat information between network and endpoint security products ensures consistent protection even when devices leave the corporate network and prevents threats through secondary vectors.



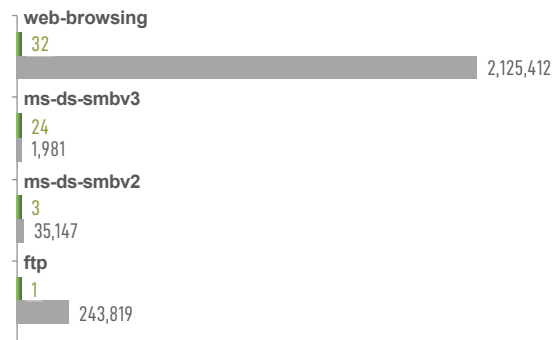
7
Malware sample(s)
first discovered at the endpoint

7
Application(s)
found delivering malware

14 UNKNOWN MALWARE



60 KNOWN MALWARE



■ ACME Unknown Malware ■ ACME Known Malware ■ Industry Average

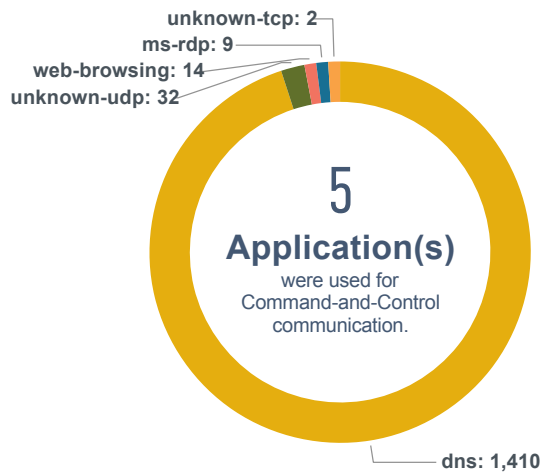


Command and Control Analysis

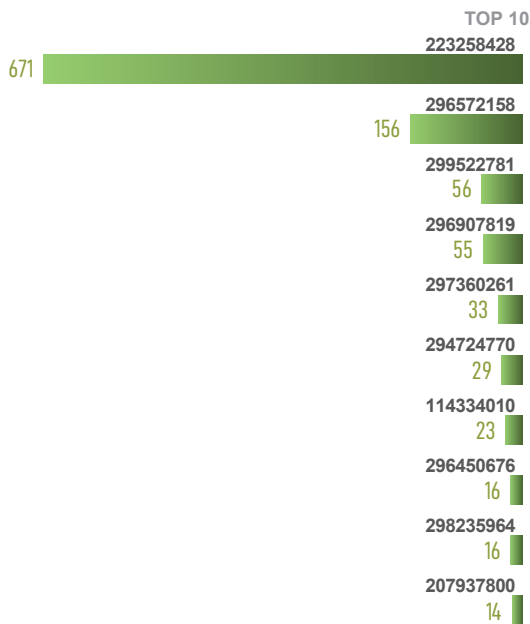
Command-and-control (CnC) activity often indicates a host in the network has been infected by malware, and may be attempting to connect outside of the network to malicious actors, reconnaissance attempts from outside, or other command-and-control traffic. Malware running on managed hosts is evading the active endpoint prevention product that is allowing this activity to occur. Understanding and preventing this activity is critical, as attackers use CnC to deliver additional malware, provide instruction, or exfiltrate data. Detection and response products may provide detail on the malicious network and host activity that has occurred as a result of the identified malware.

KEY FINDINGS

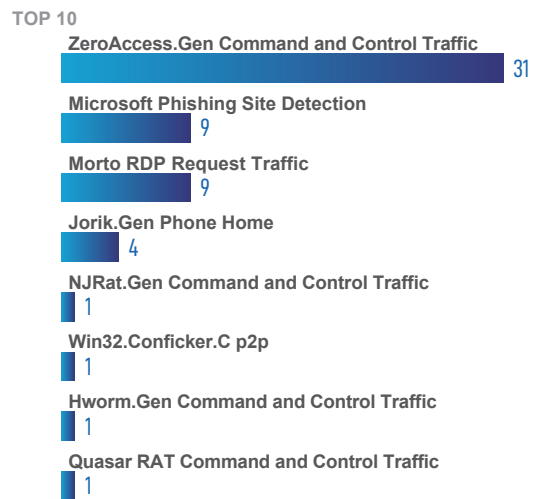
- 5 total applications were used for command-and-control communication.
- 1,467 total command-and-control requests were seen on your network.
- 1,410 total suspicious DNS queries were observed.
- Active command-and-control should be stopped immediately. Endpoint prevention running on managed hosts with this activity should have policies reviewed. Network products with application visibility and awareness of malicious DNS can prevent these communications, however the malware on the host must also be stopped to prevent an adversaries ongoing efforts.



1,410 SUSPICIOUS DNS QUERIES



57 SPYWARE PHONE HOME





Top Malware Family Tags	
Tag	Count
Upatre	129,906
GandCrab	7,102
NJRat	5,830
BlackShades	5,512
GameOverZeus	3,918
VirLock	3,324
Gepys	2,765
VBKrypt	1,683
XtremeRAT	1,653
Tinba	1,220

Top Campaign Tags	
Tag	Count
BlackVine	270
DustySky	75
SilverTerrier	63
FBot	38
OperationBabyCoin	7
OlympicDestroyer	5
TurkishRemcosAttack	3
OperationPotaoExpress	1
Naikon	1
MMCore	1

Top Malicious Behavior Tags	
Tag	Count
IPAddressLookup	25,354
CreateScheduledTask	19,737
ProcessInjection	18,382
UsesDynamicDNS	18,080
ResolveSinkholedDomain	15,565
ModifyWindowsFirewall	14,627
FewIATEntries	12,011
HttpNoUserAgent	11,341
CreateApplnitDll	9,847
InitialSystemDataEnumeration	7,260

- Linked to threats that belong to a certain Malware Family
- Part of a larger Campaign of attacks
- A type of Malicious Behavior that indicates that your system has been compromised
- Public tags are tags shared with the AutoFocus community by your organization and other AutoFocus users. They are visible to all AutoFocus users.
- Unit 42 (alerting) tags are created by Unit 42 (the Palo Alto Networks® threat intelligence and research team) for threats and campaigns that pose a direct security risk.
- Unit 42 creates alerting tags for threats discovered by individuals or organizations outside of Unit 42. These tags have a pointed and marked top right corner.

THREATS BY DESTINATION COUNTRIES



Malware threats sent against **3** countries.
64.10% of malware was destined to **Germany**, a total of **25** malware sessions.



IoT Security

Wed, Jan 01, 2020 - Mon, Mar 23, 2020

Enterprises no longer comprise only traditional IT applications and devices. Enterprises include several purpose-built, Internet-connected devices—devices that help streamline day-to-day operations: Operational Technology (OT) devices and devices broadly known as Internet of Things (IoT). These IoT devices are often unmanaged and pose a huge security risk to organizations because they do not undergo the typical IT lifecycle management from onboarding to ongoing maintenance to eventual retirement. The Palo Alto Networks IoT Security solution uses patented machine learning (ML) algorithms to discover these devices, detect risk, and provide policy recommendations to improve their security posture and help orchestrate their lifecycle management.

KEY FINDINGS

574

IoT DEVICES DISCOVERED

574 IoT devices were discovered in your network. **110** pose a critical risk, **130** are high risk and **160** are medium risk. Device profiles posing the most risk are: **Polycom IP Phone (153)**, **Aruba Instant AccessPoint (107)**, **Polycom Device (106)**, **Polycom Video Conferencing Device (81)** and **Avaya IP Phone (33)**.

4

IoT ALERTS DETECTED

4 alerts were detected on your network. **1** alert is critical, **1** alert is high severity and **1** is medium severity. Top alert types: **anomalous behavior (4)**.

12

IoT VULNERABILITIES DETECTED

12 vulnerabilities were detected on your network. **3** are confirmed vulnerabilities: **2** critical severity and **1** medium severity. **9** are potential vulnerabilities: **6** critical severity, **1** high severity and **2** medium severity.

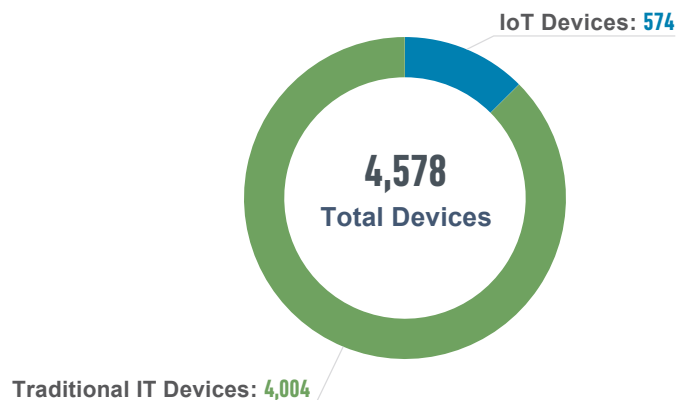


DEVICE OVERVIEW AND ANALYSIS

Unmanaged IoT devices are a threat to any organization. The following chart shows all the devices discovered on your network.

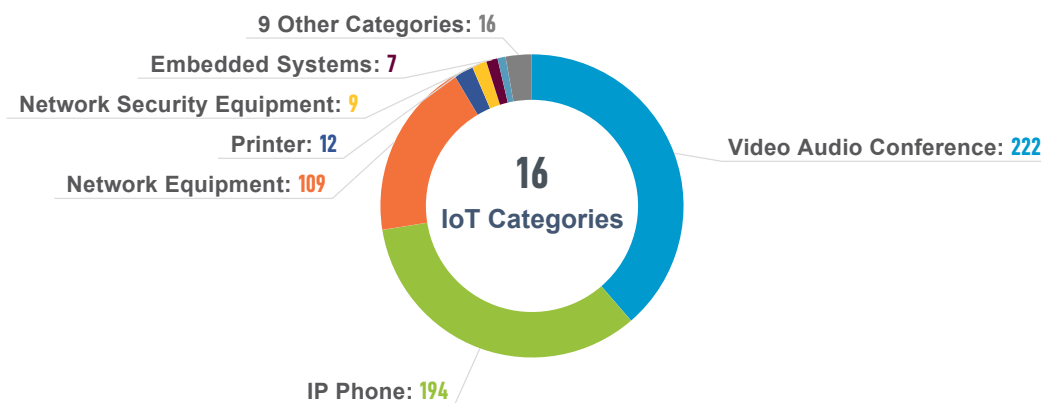
KEY FINDINGS

- **4,578** devices were discovered in your network.
- **574** IoT devices and **4,004** traditional IT devices were discovered.



IoT DEVICE ANALYSIS

Having a smaller number of device types not only helps standardize on device models, it also helps streamline the ongoing management of these devices.



CATEGORIES	DEVICES	% OF DEVICES
Video Audio Conference	222	39%
IP Phone	194	34%
Network Equipment	109	19%
Printer	12	2%
Network Security Equipment	9	2%
Embedded Systems	7	1%
Energy Management	5	1%
Wireless Presentation System	4	1%



CATEGORIES	DEVICES	% OF DEVICES
■ Entertainment	2	1%
■ Smart Building	2	<0.1%
■ Video Gaming	2	<0.1%
■ Wearable	2	<0.1%
■ Office	1	<0.1%
■ Consumer Electronics	1	<0.1%
■ Physical Security	1	<0.1%











RISK OVERVIEW

Risk is the potential security impact posed by alerts, unaddressed device vulnerabilities, and other factors that weaken your security posture. Each of these factors and the severity of their potential impact contribute to the level of risk, which is represented as a device risk score. Devices with a score of 40 and above are considered at risk.

KEY FINDINGS

- Based on the alerts, vulnerabilities, and other risks we track, we calculate a risk score for each monitored device. Devices with a score of 40 and above are considered at risk.
- 400** IoT devices with a risk score of 40 and above have been found in your organization.

SEVERITY	RISK SCORE	DEVICES	RECOMMENDATION
 Critical	90-100	 110	Address issues with these devices immediately
 High	70-89	 130	Address issues with these devices quickly
 Medium	40-69	 160	Address issues with these devices when possible
 Low	0-39	 174	Address issues with these devices when possible







ALERTS OVERVIEW

Alerts are security incidents that happened in your network. They significantly contribute to the risk score of individual devices and the organization as a whole.

KEY FINDINGS

- 4 active alerts in 1 device category were detected.
- Top active alerts ranked by severity are listed below.

SEVERITY	ALERT	ALERT TYPE	IMPACTED DEVICE	DETECTED TIME
	Testing alert CRITICAL	anomalous behavior	tactv-Amsterdam-10-193-30-55	3/19/2020 4:00:01 AM
	Testing alert HIGH	anomalous behavior	tactv-Amsterdam-10-193-30-55	3/19/2020 4:00:01 AM
	Testing alert LOW	anomalous behavior	tactv-Amsterdam-10-193-30-55	3/19/2020 4:00:01 AM
	Testing alert MEDIUM	anomalous behavior	tactv-Amsterdam-10-193-30-55	3/19/2020 4:00:01 AM

 - Critical

 - High

 - Medium

 - Low



NETWORK SEGMENTS WITH A MIX OF IoT AND NON-IoT DEVICES

Network segments with both IoT and non-IoT devices have an increased level of risk. Attackers might compromise a more vulnerable type of device and use it as a base from which to attack other, potentially more valuable devices in the same network segment.

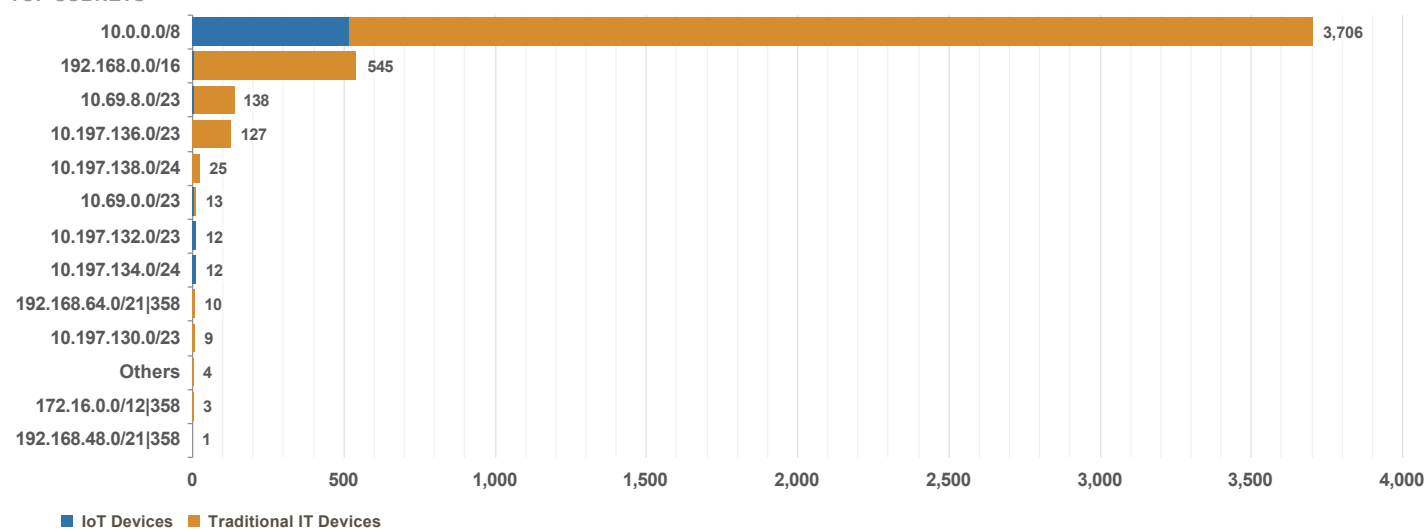
KEY FINDINGS

- 13 network segments have both IoT and non-IoT devices.
- Top network segments by device count are listed below.

DEVICE DISTRIBUTION BY SUBNET

13 TOTAL SUBNETS

TOP SUBNETS





VULNERABILITIES OVERVIEW

Vulnerabilities are flaws built into the software or hardware of devices and pose potential security issues. These flaws can be exploited by attackers to perform unauthorized actions within a computer system. Vulnerabilities contribute to the risk score of individual devices and the organization as a whole. As of **Mar 23, 2020**, there were **1,400** vulnerability instances for **12** different vulnerabilities.

KEY FINDINGS

- **12** vulnerabilities and **1,400** vulnerability instances were discovered in your network.
- **10** vulnerable device profiles were discovered.
- Distribution of vulnerabilities by severity and top device profiles are listed below.




SEVERITY	CVSS	VULNERABILITES	INSTANCES	DEVICE PROFILES
Critical	9.0-10.0	8	220	Apple Device, DTEN Display Board PC Module, Windows Server, NetworkDevice-TrendNet, Airtame Wireless Presentation Device
High	7.0-8.9	1	781	Polycom IP Phone, Polycom Device
Medium	4.0-6.9	3	399	Zebra Label Printer, Polycom Device, Polycom IP Phone
Low	0.1-3.9	0	0	

VULNERABILITIES AND VULNERABILITY TYPES

List of vulnerabilities by severity are listed below.

CVSS	VULNERABILITY NAME	INSTANCES	AFFECTED DEVICE PROFILES
9.8	CVE-2017-15304	45	Airtame Wireless Presentation Device
9.8	CVE-2017-7450	45	Airtame Wireless Presentation Device
9.8	CVE-2019-1181	32	DTEN Display Board PC Module, Windows Server, NetworkDevice-TrendNet
9.8	CVE-2019-1182	32	NetworkDevice-TrendNet, Windows Server, DTEN Display Board PC Module
9.8	CVE-2019-1222	32	NetworkDevice-TrendNet, Windows Server, DTEN Display Board PC Module
9.8	CVE-2019-1226	32	NetworkDevice-TrendNet, DTEN Display Board PC Module, Windows Server
9.8	CVE-2019-11367	1	Apple Device



CVSS	VULNERABILITY NAME	INSTANCES	AFFECTED DEVICE PROFILES
 9.8	CVE-2018-18472	1	Apple Device
 8.8	CVE-2017-12857	781	Polycom IP Phone, Polycom Device
 5.3	CVE-2018-18566	199	Polycom Device, Polycom IP Phone



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, management and internet-utility** were observed on the network, which should be investigated due to their potential for abuse.
- **664** total applications were seen on the network across **28** sub-categories, as opposed to an industry average of **70** total applications seen in other **High Technology** organizations.
- **121,744** total vulnerability exploits were observed across the following top three applications: **netbios-ns, ms-ds-smbv2 and mount**.
- **74** malware events were observed, versus an industry average of **0** across your peer group.
- **5** total applications were used for command and control communication.
- **574** IoT devices were discovered in your network. **110** pose a critical risk, **130** are high risk and **160** are medium risk.

KEY FINDINGS

664

APPLICATIONS IN USE

130

HIGH RISK APPLICATIONS

211

SAAS APPLICATIONS

121,744

VULNERABILITY EXPLOITS

123,285

TOTAL THREATS

74

MALWARE

Known: **60** | Unknown: **14****574**

IoT DEVICES DISCOVERED

Critical: **110** | High: **130** | Medium: **160**

RECOMMENDATIONS

- Implement safe application enablement policies, 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.
- Address command and control communication by examining the network or host source. Detection and response or logging solutions may provide an indication of what occurred.
- 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 and other security products, creating and coordinating new protections for emerging threats, sourced from a global community of other enterprise users.
- Implement managed host policies to restrict file less attack vectors and decrease command-and-control risk by sharing near-real-time threat information across security products.
- When risky IoT devices are detected, consider taking the following actions:
 - Review the risks associated with these devices.
 - Address or mitigate known issues by modifying device configurations or by upgrading or patching their software.
 - Reduce the attack surface by applying policy recommendations.
 - Segment devices to block, limit, or slow attacks.