SECURITY LIFECYCLE REVIEW

BADAN PERTANAHAN NASIONAL

PREPARED BY:

Security Analyst
Palo Alto Networks
www.paloaltonetworks.com

The Security Lifecycle Review summarizes the threat exposure and security risks facing **BADAN PERTANAHAN NASIONAL** and the customers connecting to their networks. The data used for this analysis was gathered by Palo Alto Networks during the report period shown below. The report provides actionable intelligence and risk assessment around the applications, URL traffic, and types of content that are traversing the **BADAN PERTANAHAN NASIONAL** network as well as the 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: 30 DAYS
Wed, Jun 01, 2022 - Thu, Jun 30, 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY FOR BADAN PERTANAHAN NASIONAL

The Security Lifecycle Review summarizes the business and security risks facing **BADAN PERTANAHAN NASIONAL**. 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

184

APPLICATIONS IN USE

184 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.

32

HIGH RISK APPLICATIONS

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

31

SAAS APPLICATIONS

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

23,098,244

VULNERABILITY EXPLOITS

23,098,244 total vulnerability exploits were observed in your organization, including **Other, info-leak, and brute-force**.

23,153,760

TOTAL THREATS

23,153,760 total threats were found on your network, including vulnerability exploits, malware, and outbound command and control activity.

12

MALWARE DETECTED

12 known malware and **0** unknown malware events were observed in your organization.

Applications at a Glance

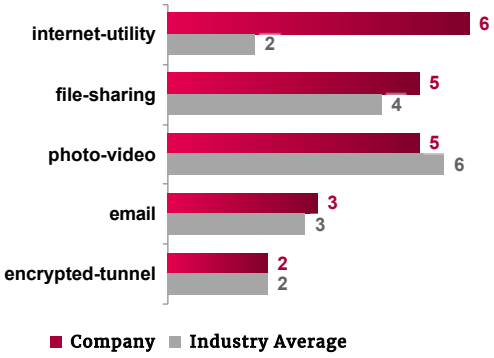
Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision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

KEY FINDINGS

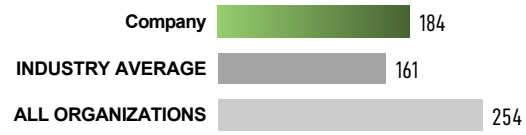
- High-risk applications such as **internet-utility, file-sharing, and photo-video** were observed on the network, which should be investigated due to their potential for abuse.
- **184** total applications were seen on the network across **27** sub-categories, as opposed to an industry average of **161** total applications seen in other **Government - Municipal** organizations.
- **20.24 TB** was used by all applications, including **business-systems** with **16.4 TB**, compared to an industry average of **8.91 TB** in similar organizations.

HIGH-RISK APPLICATIONS

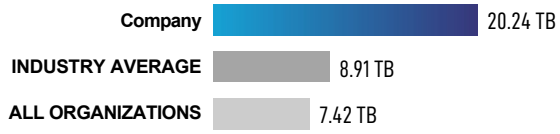
The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.



NUMBER OF APPLICATIONS ON NETWORK

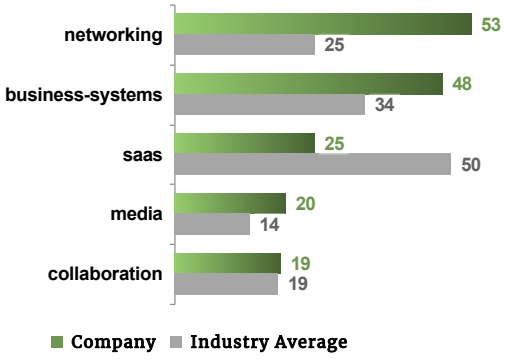


BANDWIDTH CONSUMED BY APPLICATIONS



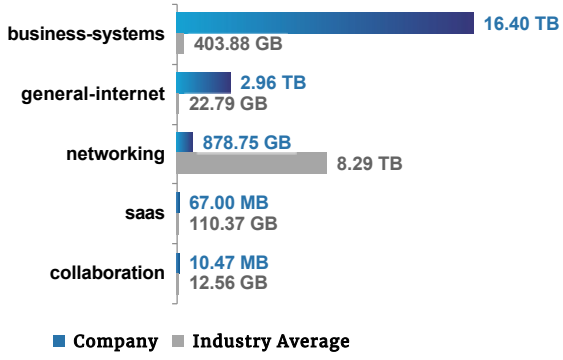
CATEGORIES WITH THE MOST APPLICATIONS

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



CATEGORIES CONSUMING THE MOST BANDWIDTH

Bandwidth consumption 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 **Government - Municipal** organizations. This data can be used to more effectively prioritize your application enablement efforts.

RISK LEVEL

5] – High
4
3
2
1

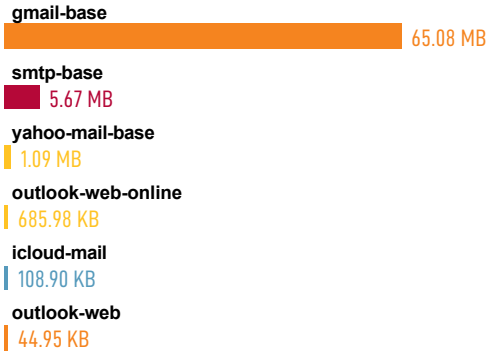
KEY FINDINGS

- A total of **184** applications were seen in your organization, compared to an industry average of **161** in other **Government - Municipal** organizations.
- The most common types of application subcategories are **infrastructure, internet-utility, and photo-video**.
- The application subcategories consuming the most bandwidth are **database, internet-utility, and encrypted-tunnel**.

Number of Applications in the subcategory **Industry Average**

Email 72.68 MB

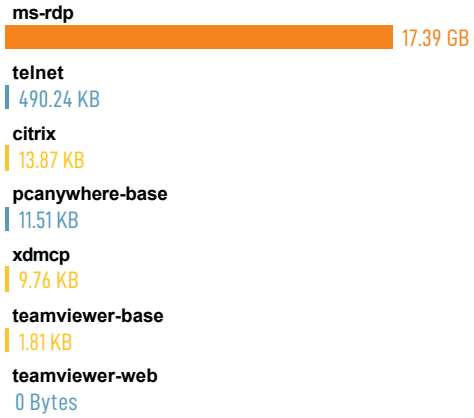
TOP EMAIL APPS



Number of Applications in the subcategory **Industry Average**

Remote-Access 17.39 GB

TOP REMOTE-ACCESS APPS



Number of Applications in the subcategory | Industry Average

File-Sharing 114.74 KB

TOP FILE-SHARING APPS

bittorrent	98.89 KB
tiftp	15.85 KB
boxnet-base	0 Bytes
dropbox-base	0 Bytes
google-drive-web	0 Bytes
ms-onedrive-base	0 Bytes
scribd-base	0 Bytes
whatsapp-file-transfer	0 Bytes

Number of Applications in the subcategory | Industry Average

Encrypted-Tunnel 809.58 GB

TOP ENCRYPTED-TUNNEL APPS

ssl	538.73 GB
ssh	171.34 GB
ipsec-esp-udp	99.28 GB
panos-global-protect	231.02 MB
ike	52.48 KB
dtls	21.31 KB
mobility-xe	2.68 KB
browsec	0 Bytes

Number of Applications in the subcategory | Industry Average

Instant-Messaging 0 Bytes

TOP INSTANT-MESSAGING APPS

google-messages	0 Bytes
qq-base	0 Bytes
telegram-base	0 Bytes
wechat-base	0 Bytes
whatsapp-base	0 Bytes
whatsapp-web	0 Bytes

Number of Applications in the subcategory | Industry Average

Social-Networking 0 Bytes

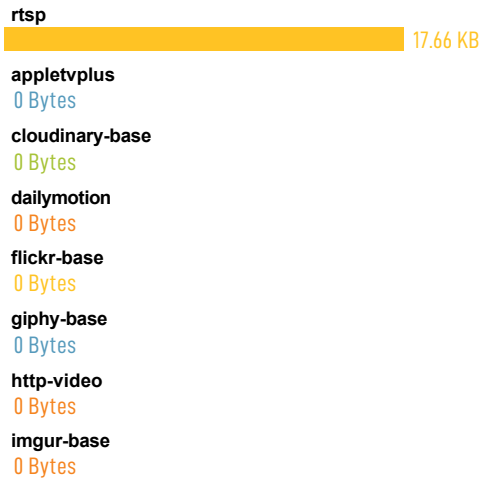
TOP SOCIAL-NETWORKING APPS

google-classroom	0 Bytes
linkedin-base	0 Bytes
mail.ru-base	0 Bytes
quora-base	0 Bytes
reddit-base	0 Bytes

Number of Applications in the subcategory Industry Average

Photo-Video 17.66 KB

TOP PHOTO-VIDEO APPS



Number of Applications in the subcategory Industry Average

Proxy 2.08 GB

TOP PROXY APPS

Applications that Introduce Risk — Detail

RISK	APPLICATION	CATEGORY	SUB CATEGORY	TECHNOLOGY	BYTES	SESSIONS
4	gmail-base	saas	email	browser-based	65.08 MB	14883
5	smtp-base	collaboration	email	client-server	5.67 MB	54
3	yahoo-mail-base	saas	email	browser-based	1.09 MB	27
3	outlook-web-online	saas	email	browser-based	685.98 KB	46
2	icloud-mail	saas	email	client-server	108.9 KB	8
4	outlook-web	collaboration	email	browser-based	44.95 KB	67
4	ssl	networking	encrypted-tunnel	browser-based	538.73 GB	3939426
4	ssh	networking	encrypted-tunnel	client-server	171.34 GB	54365
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	99.28 GB	987
3	panos-global-protect	networking	encrypted-tunnel	client-server	231.02 MB	38775
2	ike	networking	encrypted-tunnel	client-server	52.48 KB	115
1	dtls	networking	encrypted-tunnel	client-server	21.31 KB	73
2	mobility-xe	networking	encrypted-tunnel	client-server	2.68 KB	16
3	browsec	networking	encrypted-tunnel	browser-based	0 Bytes	0
5	bittorrent	general-internet	file-sharing	peer-to-peer	98.89 KB	131
4	tftp	general-internet	file-sharing	client-server	15.85 KB	166
3	scribd-base	general-internet	file-sharing	client-server	0 Bytes	0
5	google-drive-web	saas	file-sharing	browser-based	0 Bytes	0
3	whatsapp-file-transfer	general-internet	file-sharing	client-server	0 Bytes	0
4	dropbox-base	saas	file-sharing	client-server	0 Bytes	0
4	ms-onedrive-base	saas	file-sharing	client-server	0 Bytes	0
3	boxnet-base	saas	file-sharing	browser-based	0 Bytes	0
2	telegram-base	collaboration	instant-messaging	client-server	0 Bytes	0
2	wechat-base	collaboration	instant-messaging	client-server	0 Bytes	0
3	google-messages	collaboration	instant-messaging	browser-based	0 Bytes	0

Notes:

RISK	APPLICATION	CATEGORY	SUB CATEGORY	TECHNOLOGY	BYTES	SESSIONS
1	whatsapp-base	collaboration	instant-messaging	client-server	0 Bytes	0
4	qq-base	collaboration	instant-messaging	client-server	0 Bytes	0
2	whatsapp-web	collaboration	instant-messaging	browser-based	0 Bytes	0
3	rtsp	media	photo-video	client-server	17.66 KB	15
3	netflix-base	media	photo-video	browser-based	0 Bytes	0
4	dailymotion	media	photo-video	browser-based	0 Bytes	0
4	youtube-streaming	media	photo-video	browser-based	0 Bytes	0
2	giphy-base	saas	photo-video	browser-based	0 Bytes	0
4	imgur-base	media	photo-video	browser-based	0 Bytes	0
4	youtube-base	media	photo-video	browser-based	0 Bytes	0
1	kuaishou	media	photo-video	client-server	0 Bytes	0
5	http-proxy	networking	proxy	browser-based	2.08 GB	660602
5	socks	networking	proxy	network-protocol	4.39 KB	10
4	ms-rdp	networking	remote-access	client-server	17.39 GB	201173
2	telnet	networking	remote-access	client-server	490.24 KB	48
3	citrix	networking	remote-access	client-server	13.87 KB	94
2	pcanywhere-base	networking	remote-access	client-server	11.51 KB	109
3	xdmcp	networking	remote-access	client-server	9.76 KB	92
3	teamviewer-base	saas	remote-access	client-server	1.81 KB	4
2	teamviewer-web	networking	remote-access	browser-based	0 Bytes	0
3	linkedin-base	collaboration	social-networking	browser-based	0 Bytes	0
1	quora-base	collaboration	social-networking	browser-based	0 Bytes	0
2	google-classroom	saas	social-networking	browser-based	0 Bytes	0
4	mail.ru-base	collaboration	social-networking	browser-based	0 Bytes	0
1	reddit-base	collaboration	social-networking	browser-based	0 Bytes	0

Notes:

SaaS Applications

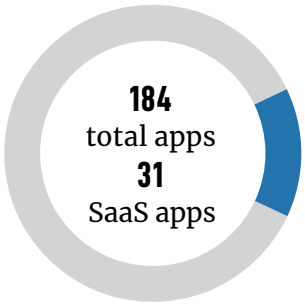
SaaS–based application services continue to redefine the network perimeter. Often labeled "shadow IT," most of these services are adopted directly by individual users, business teams, or even entire departments. To minimize data security risks, you need control over SaaS applications used your network.

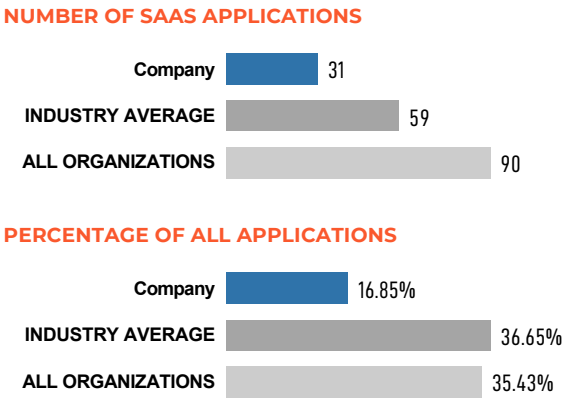
KEY FINDINGS

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

SAAS APPLICATIONS BY NUMBERS

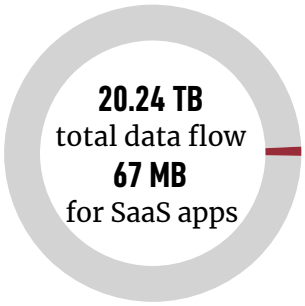
Review the applications being used in your organization. To maintain administrative control, adopt SaaS applications that will be managed by your IT team.

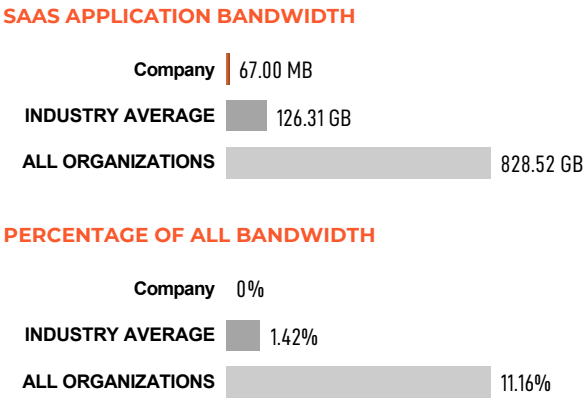




SAAS APPLICATION BANDWIDTH

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

Number of Applications in the subcategory | Industry Average

File-Sharing 0 Bytes

TOP FILE-SHARING APPS

- **boxnet-base**
  0 Bytes
- **dropbox-base**
  0 Bytes
- **google-drive-web**
  0 Bytes
- **ms-onedrive-base**
  0 Bytes
- **scribd-base**
  0 Bytes

Number of Applications in the subcategory | Industry Average

Photo-Video 0 Bytes

TOP PHOTO-VIDEO APPS

- **cloudinary-base**
  0 Bytes
- **flickr-base**
  0 Bytes
- **giphy-base**
  0 Bytes
- **youtube-base**
  0 Bytes
- **youtube-streaming**
  0 Bytes

Number of Applications in the subcategory | Industry Average

Email 66.96 MB

TOP EMAIL APPS

- **gmail-base**
  65.08 MB
- **yahoo-mail-base**
  1.09 MB
- **outlook-web-online**
  685.98 KB
- **icloud-mail**
  108.90 KB

Number of Applications in the subcategory | Industry Average

General-Business 36.51 KB

TOP GENERAL-BUSINESS APPS

- **git-base**
  36.51 KB
- **windows-azure-base**
  0 Bytes
- **zendesk-base**
  0 Bytes

TOP SAAS APPLICATIONS

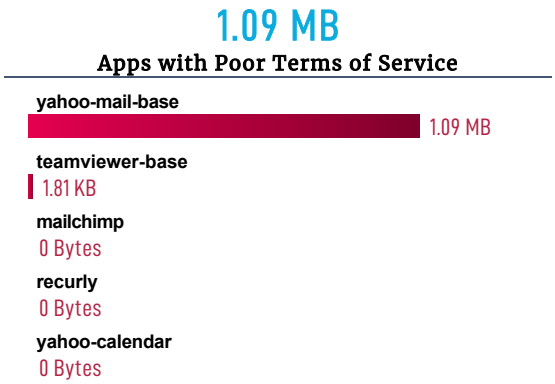
The following displays the top 10 SaaS applications used in your organization and the application usage compared against your industry peers and all other Palo Alto Networks customers.

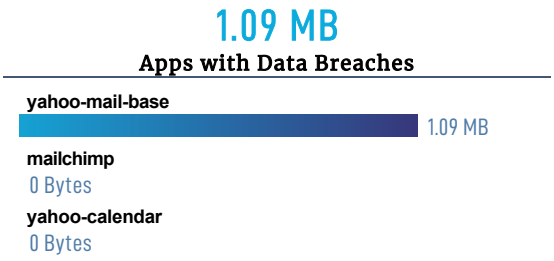
TOP SAAS APPLICATIONS BY DATA MOVEMENT

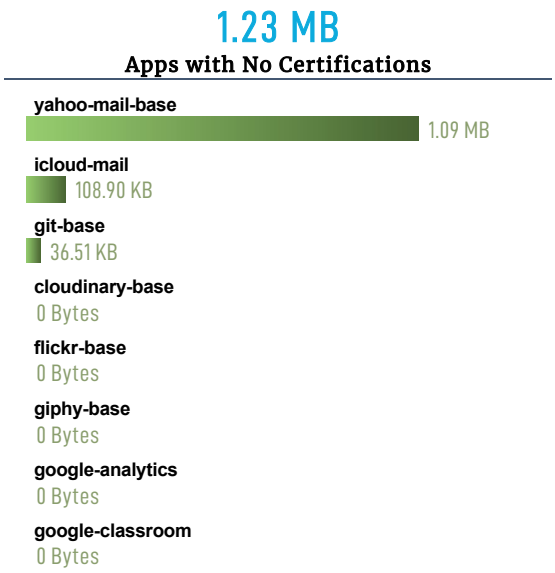
SAAS APPLICATIONS BY HOSTING RISK

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.







Advanced URL Filtering Analysis

Wed, Jun 01, 2022 - Thu, Jun 30, 2022

As applications move to the cloud and people work from anywhere, it's becoming more important—and more difficult—to secure web traffic. Web-based attacks like phishing, command-and-control and other fileless attacks are coming at higher volume, greater speed, and increased sophistication. The Palo Alto Networks Advanced URL Filtering service gives you deep insight into your web traffic, empowers you to control web access through granular policies and enables you to prevent web-based threats in real-time.

1,554,369

TOTAL URL REQUESTS

Advanced URL Filtering has analyzed **1,554,369** URL requests in your network. The Web has become one of the most commonly used attack surfaces and malicious web-pages can be used for malware delivery, command-and-control (C2), or data exfiltration.

20,330

MALICIOUS REQUESTS

Advanced URL Filtering has identified **20,330** malicious requests. These malicious requests include malware, phishing, command and control and grayware.

1,221

MALICIOUS IP ADDRESSES

Advanced URL Filtering has identified **1,221** malicious IP addresses behind these malicious URLs/domains. These IP addresses can be used as C2 infrastructure to exfiltrate data, deliver malware or send remote commands to a system in your network.

TRAFFIC DISTRIBUTION

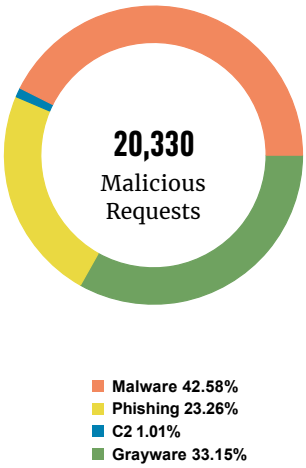
Uncontrolled Web surfing exposes organizations to security and business risks, including exposure to potential cyber-threats, data loss, credential theft or compliance violations. This section will provide visibility into the URL requests in your network, allowing you to make informed decisions regarding potential risk versus business benefit. Malicious URLs and domains in your network should be reviewed to understand who is accessing them, and the potential risk associated with them.

KEY FINDINGS

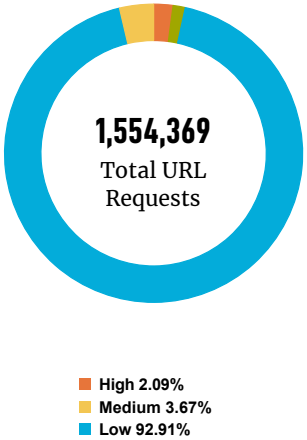
- Users visited a total of **1,554,369** URLs during the report time period across **65** categories.
- **20,330** requests out of that total were to known malicious websites.
- **32,531** high risk and **57,091** medium risk sites were visited.
- **0** malicious requests were analyzed in real-time.

URL REQUEST DISTRIBUTION

MALICIOUS URL REQUEST CATEGORIES



RISK-LEVELS OF URL REQUESTS

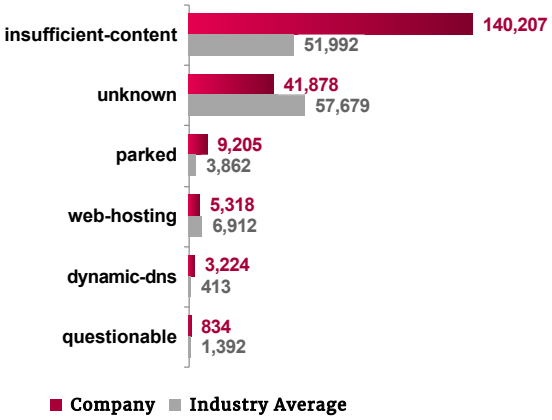


TOP CATEGORIES AND DOMAINS DISTRIBUTION

The following charts list the top visited categories and domains.

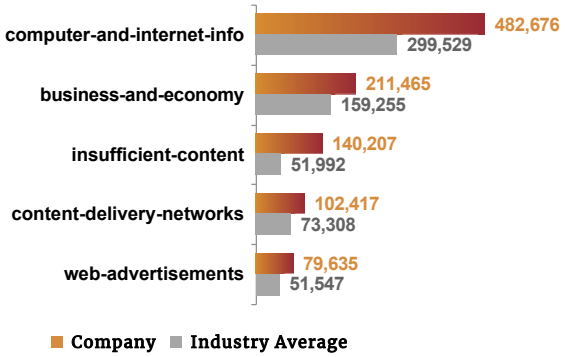
CATEGORIES INTRODUCING POTENTIAL RISK

The Web is a primary attack channel for malicious actors. High risk categories like unknown, insufficient-content, questionable, high-risk, parked, dynamic-dns, web hosting & newly-registered-domain should either be blocked or set for SSL decryption with strict threat control policies to have better visibility and control.



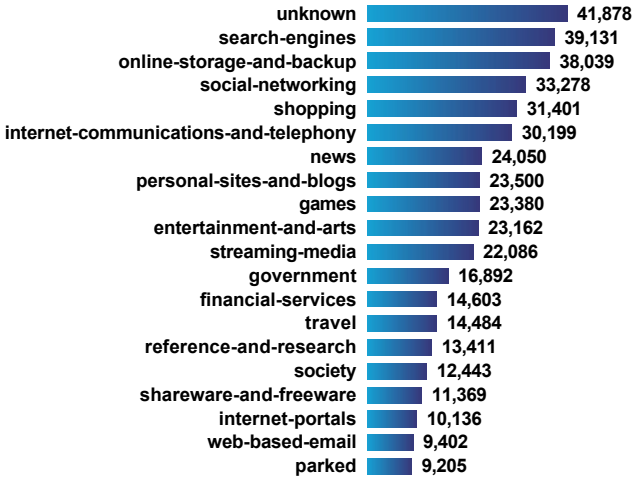
TOP 5 VISITED CATEGORIES

The top 5 most visited URL categories, along with industry benchmarks across your peer group, are shown below. Understanding your web traffic mix over time will help you identify anomalies that may indicate malicious activity.



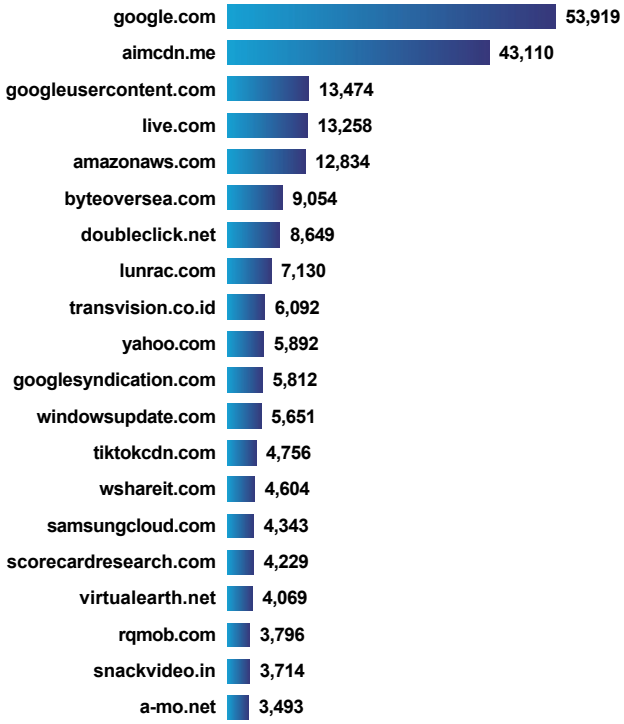
NEXT MOST HIGHLY VISITED CATEGORIES

The next top 20 most visited URL categories are shown below. Understanding your web traffic mix over time will help you identify anomalies that may indicate malicious activity.



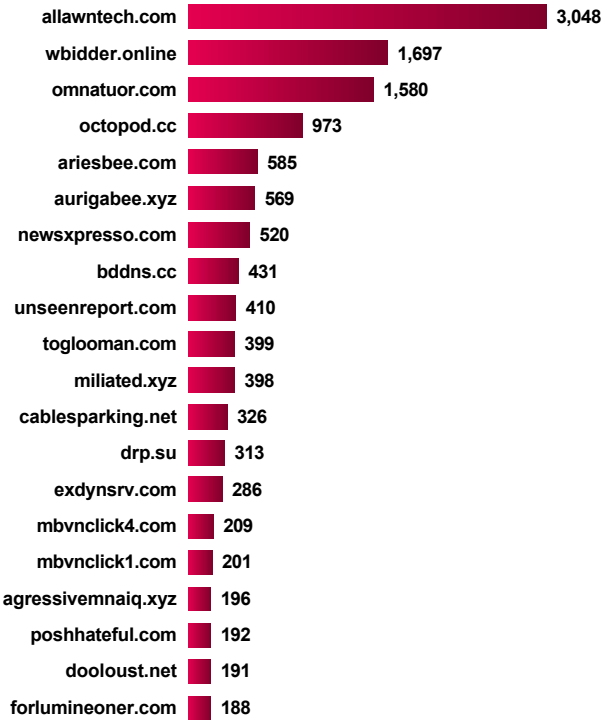
TOP VISITED DOMAINS

The following displays the top 20 visited domains in your network. It is important to regularly view the top visited domains in your network. Understanding your web traffic usage over time will help you identify anomalies that may indicate malicious activity.



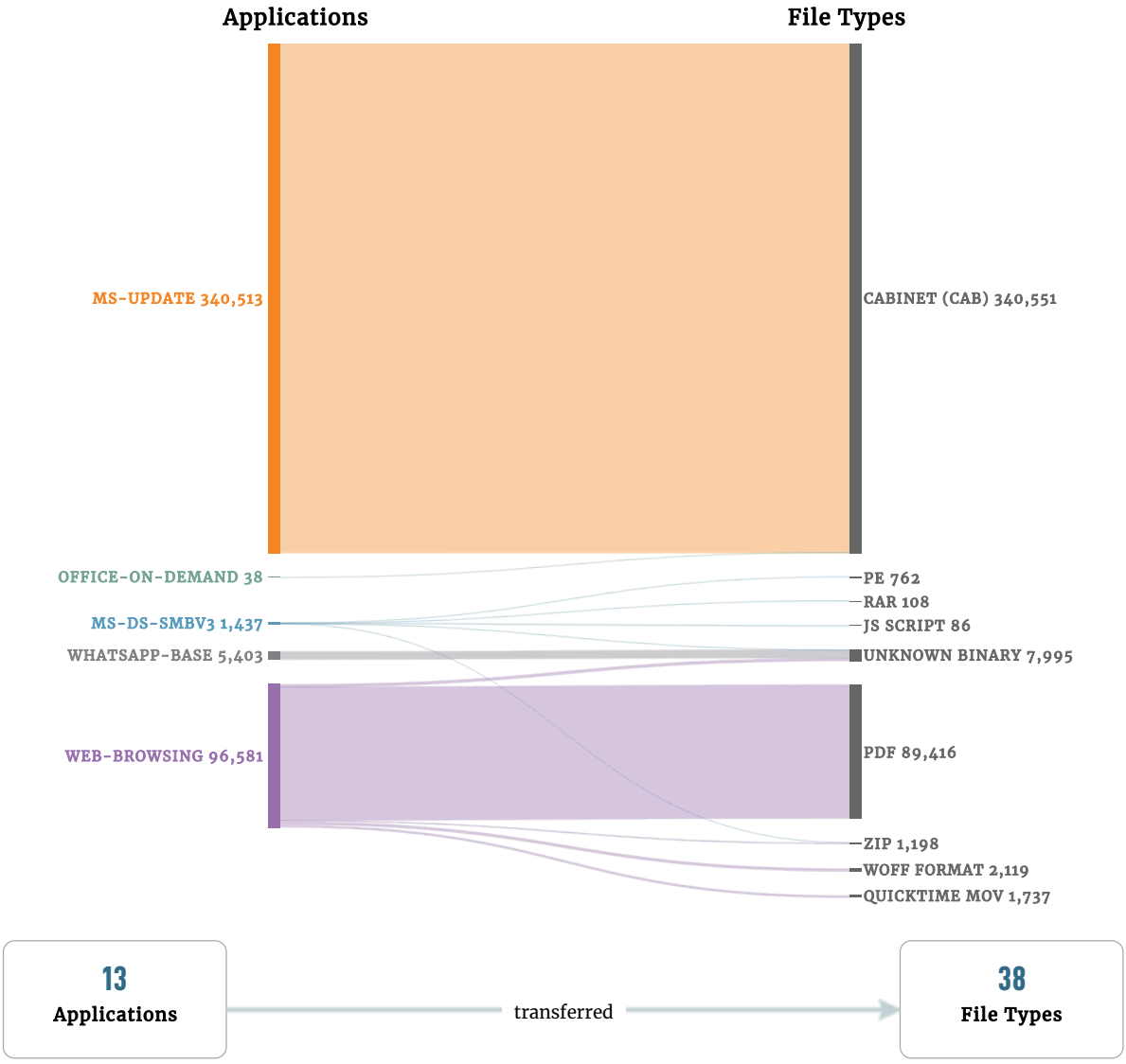
TOP VISITED MALICIOUS DOMAINS

The following displays the top 20 malicious domains visited in your network. Malicious domains 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. Frequent visits to malicious domains from the same machine may indicate an infected endpoint.



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, **38** file types were delivered via a total of **13** applications. The image below correlates the applications most commonly used to transfer files, along with the most prevalent file and content types observed.



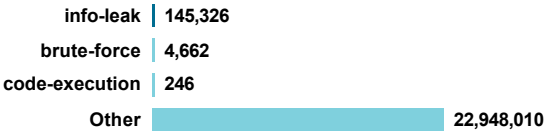
Threats at a Glance

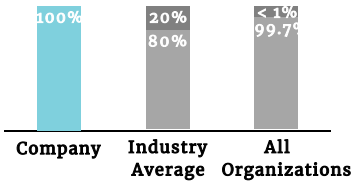
Understanding your risk exposure, and how to adjust your security posture to prevent attacks, requires intelligence on the type and volume of threats used against your organization. This section details the application vulnerabilities, known and unknown malware, and command and control activity observed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

KEY FINDINGS

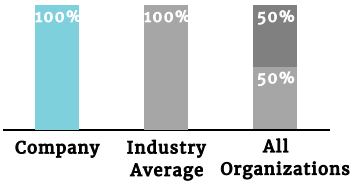
- **23,098,244** total vulnerability exploits were observed in your organization, including **Other, info-leak, and brute-force**.
- **12** malware events were observed, versus an industry average of **0** across your peer group.
- **55,504** total command and control requests were identified, indicating attempts by malware to communicate with attackers to download additional malware, receive instructions, or exfiltrate data.

23,098,244
Vulnerability Exploit(s)

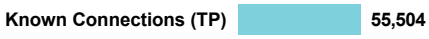




12
Malware Detection(s)



55,504
Command and Control Detection(s)



High-Risk and Malicious File Type Analysis

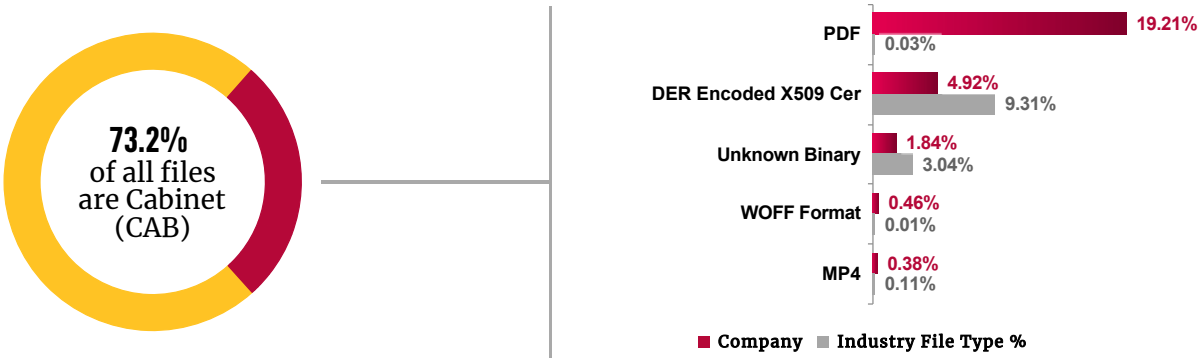
Today's cyber attackers use a variety of file types to deliver malware and exploits, often focusing on content from common business applications present in most enterprise networks. The majority of commodity threats are delivered via executable files, with more targeted and advanced attacks often using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

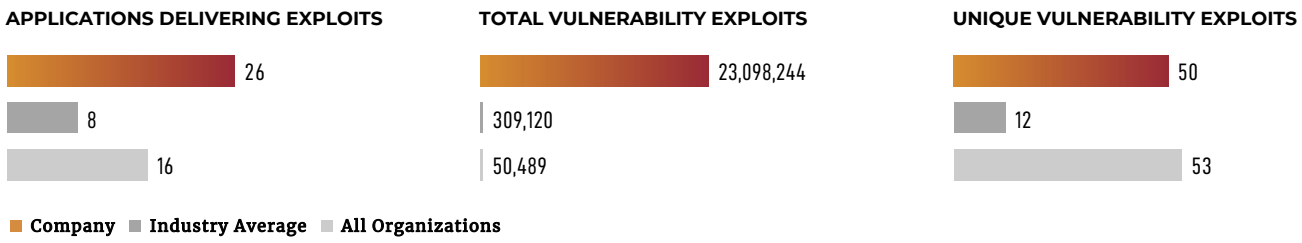


Application Vulnerabilities

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

- **26** total applications were observed delivering exploits to your environment.
- **23,098,244** total vulnerability exploits were observed across the following top three applications: **web-browsing, ssl, and msrpc-base**.
- **50** 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	EXPLOIT ID	SEVERITY	THREAT TYPE	CVE ID
21,053,715	**Web-Browsing**			
97	ThinkPHP Remote Code Execution Vulnerability	CRITICAL		
95	phpunit Remote Code Execution Vulnerability	CRITICAL		
56	Microsoft ASP.Net Information Leak Vulnerability	CRITICAL		
32	MobileIron Core and Connector Remote Code Execution Vulnerability	CRITICAL		
13	Microsoft Exchange Server SSRF Vulnerability	CRITICAL		
11	Apache Struts Content-Type Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2017-5638;CVE-2019-0230
9	Confluence Server OGNL Injection Remote Code Execution Vulnerability	CRITICAL		
9	ZOHOcorp ManageEngine Improper Authentication Vulnerability	CRITICAL		
9	Apache Log4j Remote Code Execution Vulnerability	CRITICAL		
8	Spring Core Remote Code Execution Vulnerability	CRITICAL		
1,080,274	**Ssl**			
2	OpenSSL Handshake Cipher Two More Times Changed Anomaly	LOW	dos	CVE-2004-0079
535,923	Abnormal SSL traffic on port 443	INFO		
484,254	Non-RFC Compliant SSL Traffic on Port 443	INFO		
59,544	SSL TLS CBC Cipher Suite Detection	INFO		
236	OpenSSL SSLv2 Man-in-the-Middle Vulnerability	INFO		
233	SSL Weak Cipher Suite Selection Vulnerability	INFO		
51	Non-RFC Compliant SSL Traffic	INFO		
30	Use of insecure SSLv3.0 Found in Server Response	INFO		

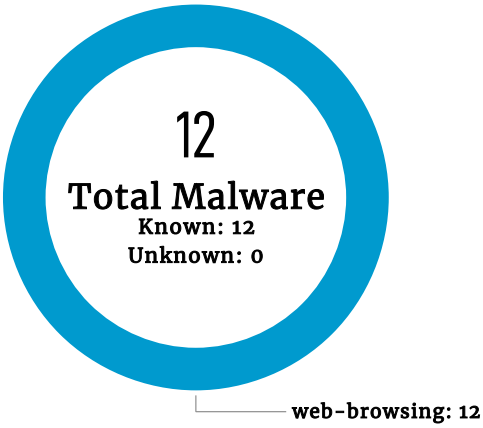
DETECTIONS	EXPLOIT ID	SEVERITY	THREAT TYPE	CVE ID
1	OpenSSL TLS Heartbeat Found	INFO		
600,291	**Msrpc-Base**			
600,291	Microsoft Windows NTLMSSP Detection	INFO		
230,496	**Ms-Ds-Smbv3**			
119,570	Microsoft Windows user enumeration	INFO	info-leak	
110,920	Microsoft Windows NTLMSSP Detection	INFO		
5	Microsoft Windows Server Service NetrShareEnum access	INFO	info-leak	
1	Microsoft Windows Server Service NetrServerGetInfo Opnum 21 Access Attempt	INFO	info-leak	
67,520	**Ldap**			
67,520	Microsoft Windows NTLMSSP Detection	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.

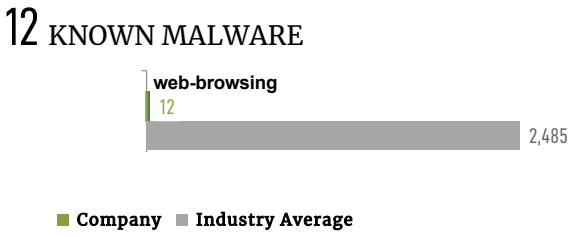
KEY FINDINGS

- **1** 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.
- **1** 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.



1
Malware sample(s)
first discovered at the endpoint

1
Application(s)
found delivering malware

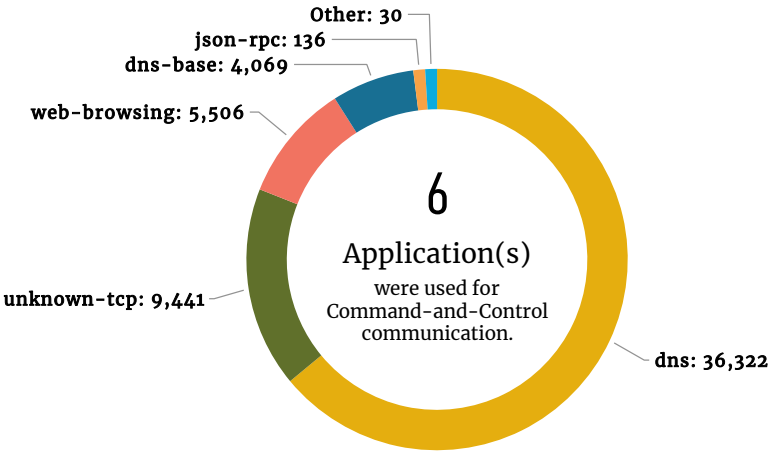


Command and Control Analysis

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.

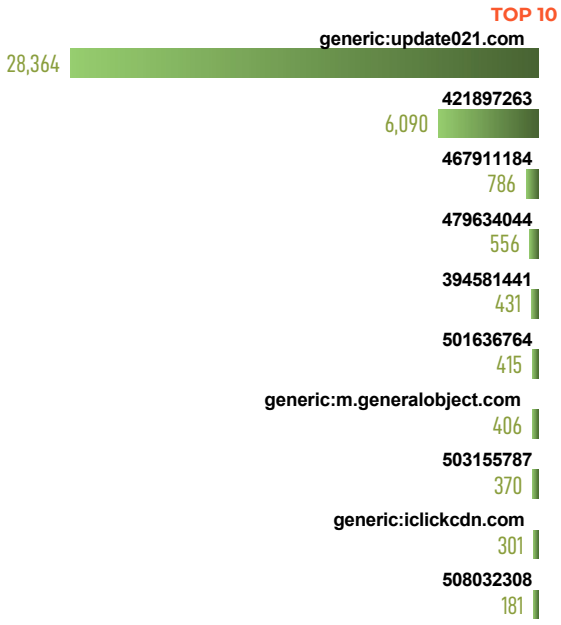
KEY FINDINGS

- **6** total applications were used for command-and-control communication.
- **55,504** total command-and-control requests were seen on your network.
- **40,368** 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.



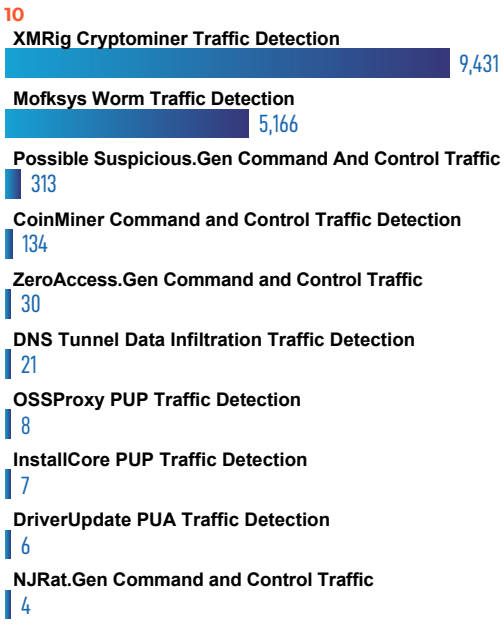
40,368 SUSPICIOUS DNS QUERIES

TOP 10



15,136 KNOWN COMMAND & CONTROL

TOP 10



0 EVASIVE COMMAND & CONTROL

(Inline Cloud Analysis)

Summary: BADAN PERTANAHAN NASIONAL

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 **BADAN PERTANAHAN NASIONAL**. This is 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

- High-risk applications such as **internet-utility, file-sharing, and photo-video** were observed on the network, which should be investigated due to their potential for abuse.
- **184** applications were seen on the network across **27** sub-categories, as opposed to an industry average of **161** applications seen in other **Government - Municipal** organizations.
- **23,098,244** vulnerability exploits were observed across the following top three applications: **web-browsing, ssl, and msrpc-base**.
- **12** malware events were observed, versus an industry average of **0** across your peer group.
- **6** applications were used for command and control communication.

KEY FINDINGS

184 APPLICATIONS IN USE	**32** HIGH RISK APPLICATIONS	**31** SAAS APPLICATIONS
23,098,244 VULNERABILITY EXPLOITS	**23,153,760** TOTAL THREATS	**12** MALWARE DETECTED Known: **12**

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, and encrypted tunnels.
- Investigate 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 the risk of attack.
- 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.