SECURITY LIFECYCLE REVIEW

PREPARED BY
eska.global
Palo Alto Networks
www.paloaltonetworks.com

ESKA

TABLE OF CONTENTS

Итоговый отчет

Обзор жизненного цикла системы безопасности подводит итоговую оценку угроз. Сведения, использованные для данного анализа, были собраны Palo Alto Networks в течение отчетного периода. Данный отчет содержит ценные аналитические сведения о приложениях, трафике URL-адресов, типах содержимого, угрозах безопасности сети, а также о рекомендациях по снижению рисков для организации.

Конфиденциальная информация — распространение запрещено

Основные выводы

325

Используемые приложение

Всего используется приложений: 325. Они представляют определенные проблемы для предприятия и его безопасности. По мере того, как важнейшие функции выходят из-под контроля организации, работники используют приложения, не относящиеся к работе напрямую, а киберпреступники используют такие приложения для создания уязвимостей и кражи данных.

54

Приложения, связанные с высокими рисками

Всего обнаружено приложений с высоким уровнем риска: 54. В их числе приложения, которые представляют собой угрозу или потенциальную опасность, передают файлы за пределы сети, а также устанавливают несанкционированные соединения.

56

Приложение SAAS

Количество приложений SaaS (Программное обеспечение как услуга), обнаруженных в вашей сети: 56. В целях выполнения административного контроля внедрите приложение SaaS, которое будетуправляться вашей IT-командой.

6,060,095

Общее количество угроз

Всего обнаружено угроз в сети: 6,060,095. В их числе программы, использующие уязвимости, известные и неизвестные вредоносные программы, а также операции по отправке исходящих команд и запросов удаленного управления.

6,056,057

Эксплойты

В рамках организации обнаружено программ, использующих уязвимости системы: 6,056,057 (категории уязвимостей: brute-force, info-leak а codeexecution)

Краткая сводка по приложениям

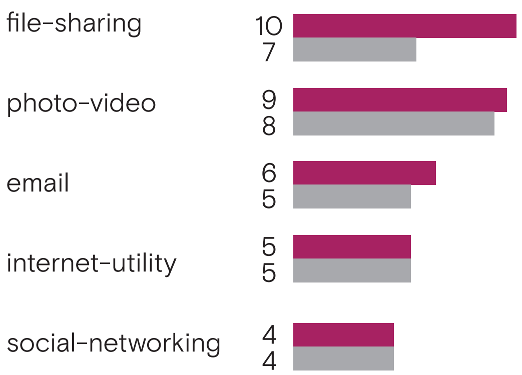
Приложения представляют собой определенный риск, поскольку через них осуществляется отправка данных из сети и несанкционированный доступ, что приводит к снижению продуктивности системы. Кроме того, зачастую такие приложения расходуют общий корпоративный трафик. В этом разделе наглядно описываются основные аспекты работы приложений. Получив всю необходимую информацию, вы сможете принять осознанное решение о снижении рисков без ущерба доходам предприятия.

Основные выводы

- В сети обнаружены приложения с высоким уровнем риска: file-sharing, photo-video а email. Требуется дополнительное изучение этих приложений в связи с потенциальными рисками для системы.
- Всего обнаружено приложений в сети: **325** (sub-categories: 28), при среднем значении для других организаций в отрасли: **246** (Media &Entertainment).
- Трафик, используемый всеми приложениями: **5.93 TB** в том числе: business-systems – **3.34 TB**, при среднем значении для другихорганизаций в отрасли: **4.21 TB**.

Приложения с высоким уровнем риска

Первый шаг к управлению системой безопасности состоит в том, чтобы определить приложения, представляющие собой основную мишень для злоумышленников. Мы рекомендуем пристально изучить приложения в указанных категориях, с тем чтобы минимизировать дополнительные оперативные риски, потенциальное нарушение нормативных требований, а также не допустить угрозы кибератак.



Количество приложений в сети

Company X	325	
Industry average	246	
All organizations	211	

Расход трафика через приложения

Company X	5.93 MB	
Industry average	4.21 TB	
All organizations	5.57 TB	

Категории с максимальным числом приложений

Следующие категории содержат максимальное число видов приложений, которые следует проверить на соответствие целям предприятия.

business-systems	98 74
networking	76
collaboration	58 53
general-internet	51 44
media	42 36

Категории приложений, использующие больше всего трафика

CBandwidth consumed by application category shows Трафик приложений по категориям демонстрирует, где нагрузка максимальна, а также где существует потенциальная возможность снизить потребление оперативных ресурсов.

business-systems	3.34 TB 1.25 TB
networking	2.01 TB 837.00 GB
collaboration	245.60 GB 235.01 GB
general-internet	207.20 GB 1.54 TB
media	123.93 GB 355.05 GB

Приложения, которые представляют собой угрозу

Ниже приведены приложения (расположенные в порядке использования трафика) данной подкатегории, которые представляют собой угрозу. Здесь же указаны стандартные показатели предприятий в данной отрасли (Media & Entertainment). Эти данные можно использовать для более эффективного планирования действий по контролируемому развертыванию приложений в рамках организации.

Основные выводы

- Всего в рамках организации обнаружено приложений: **325**, при среднем значении для других организаций в отрасли: **246** (Media & Entertainment).
- Наиболее распространенные типы подкатегорий приложений: infrastructure, management а internet-utility.
- Подкатегории приложений, использующих больше всего трафика: infrastructure, storage-backup а management.

Risk level

5 High
4 High
3
2
1

Number of Applications in the subcategory
Industry Average

10 9

Email 95.86 GG

TOP EMAIL APPS

ms-exchange
48.37 GB

pop3
42.46 GB

smtp
3.05 GB

gmail-base
1.77 GB

icloud-mail
132.25 MB

outlook-web-online
67.51 MB

yahoo-mail-base
3.38 MB

mail.ru-mail
2.10 MB

Number of Applications in the subcategory
Industry Average

13 8

Remote-Access 18.22 GG

TOP REMOTE-ACCESS APPS

ms-rdp
14.71 GB

windows-remote-management
3.36 GB

teamviewer-base
156.99 MB

apple-remote-desktop
1.19 MB

anydesk
966.07 KB

vnc-encrypted
625.20 KB

splashtop-remote
296.37 KB

pcanywhere-base
7.38 KB

APPLICATIONS

Number of Applications in the subcategory
Industry Average

22 16

File-Sharing 25.1 GG

TOP FILE-SHARING APPS

ftp
18.69 GB

bittorrent
5.75 GB

google-drive-web
350.15 GB

wetransfer
133.70 MB

ms-onedrive-base
96.31 MB

dropbox-base
63.33MB

bittorrent-sync
6.97 MB

google-cloud-storage-download
4.14 MB

Number of Applications in the subcategory
Industry Average

13 7

Encrypted-Tunnel 748.07 GG

TOP ENCRYPTED-TUNNEL APPS

ssl
14.71 GB

ssh
3.36 GB

dtls
431.35 MB

ipsec-esp-udp
88.18 MB

open-vpn
12.33 KB

ipsec-esp
6.05 MB

hola-unblocker
1.62 KB

ikee
1.60 MB

Number of Applications in the subcategory
Industry Average

12 11

Instant-Messaging 10.04 GG

TOP INSTANT-MESSAGING APPS

telegram
7.86 GB

ms-lync-base
1.18 GB

facebook-chat
906.12 MB

whatsapp-base
73.36 MB

ms-lync-online
8.80 MB

qq-base
4.56 MB

snapchat
4.28 MB

wechat-base
965.97 MB

Number of Applications in the subcategory
Industry Average

18 15

Social-Networking 136.92 GG

TOP SOCIAL-NETWORKING APPS

ssl
135.98 GB

ssh
315.23 MB

dtls
231.05 MB

ipsec-esp-udp
135.72 MB

open-vpn
110.00 KB

ipsec-esp
68.34 MB

hola-unblocker
54.18 MB

ikee
9.00 MB

APPLICATIONS

RISK	APPLICATION	CATEGORY	CATEGORY SUB	TECHNOLOGY	BYTES	SESSIONS
4	ms-exchange	collaboration	email	client-server	48.37 GB	56945
4	pop3	collaboration	email	client-server	42.46 GB	42553
5	gmail-base	collaboration	email	browser-based	1.77 GB	27590
4	ssl	networking	encrypted-tunnel	browser-based	745.84 GB	7223713
4	ssh	networking	encrypted-tunnel	client-server	1.68 GB	10246
4	hola-unblocker	networking	encrypted-tunnel	client-server	1.62 MB	398
4	ftp	general-internet	file-sharing	client-server	18.69 GB	99
5	bittorrent	general-internet	file-sharing	peer-to-peer	5.75 GB	2086031
5	google-drive-web	general-internet	file-sharing	browser-based	350.12 MB	1584
5	ms-onedrive-base	general-internet	file-sharing	client-server	96.31 MB	2448
4	dropbox-base	general-internet	file-sharing	client-server	63.33 MB	2403
4	bittorrent-sync	general-internet	file-sharing	client-server	6.97 MB	2041
4	qq-base	collaboration	instant-messaging	client-server	4.56 MB	89
4	youtube-base	media	photo-video	browser-based	43.73 GB	47932
4	facebook-video	media	photo-video	browser-based	34.94 GB	16795
4	http-video	media	photo-video	browser-based	20.93 GB	4434
4	rtmp	media	photo-video	browser-based	9.87 GB	3
4	youtube-uploading	media	photo-video	browser-based	1.63 GB	11
4	freegate	networking	proxy	client-server	63.49 MB	3919
5	http-proxy	networking	proxy	browser-based	33.04 MB	3232
5	socks	networking	proxy	network-protocol	1.01 KB	2
4	ms-rdp	networking	remote-access	client-server	14.71 GB	435
4	facebook-base	collaboration	social-networking	browser-based	135.98 GB	578984
4	vkontakte-base	collaboration	social-networking	browser-based	231.05 MB	48256
4	mail.ru-base	collaboration	social-networking	browser-based	68.34 MB	5247

Приложения SAAS

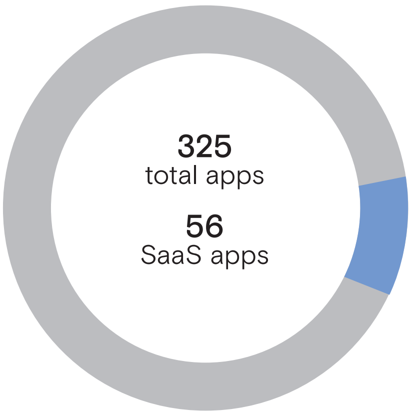
Службы приложений на основе SaaS продолжают переопределять периметр сети. Большинство этих служб, часто называемых теневыми ИТ,выбираются непосредственно отдельными пользователями, рабочими группами или даже целыми отделами. Для уменьшения рисков для безопасности данных требуется контроль над используемыми в сети приложениями SaaS.

Основные выводы

- File-Sharing имеет наибольшее число уникальных приложений SaaS.
- В отношении перемещения данных viber-base— это самое используемое приложение SaaS в вашей организации.

Приложения SAAS по количеству

Проверьте приложения, используемые в вашей организации. Для сохранения административного контроля необходимо выбрать приложения SaaS, которыми будет управлять ваш ИТ-отдел.



Number of SAAS Applications

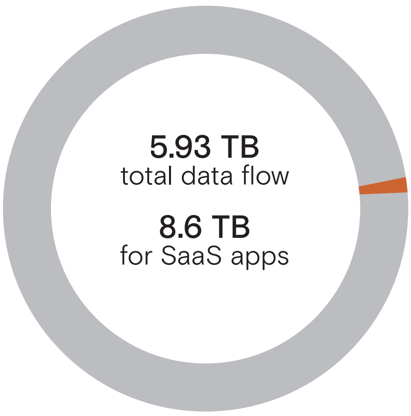
Company X	56
Industry average	61
All organizations	50

Percentage of all Applications

Company X	17.23 %
Industry average	24.8 %
All organizations	23.7 %

Диапазон приложений SAAS

Отслеживание объема перемещаемых данных в приложения SaaS и от них. Понимание природы приложений и их использования.



Number of SAAS Applications

Company X	8.60 GB
Industry average	127.60 GB
All organizations	111.47 GB

Percentage of all Applications

Company X	0.15 %
Industry average	3.97 %
All organizations	2 %

Лучшие подкатегории приложений SAAS

Ниже показано число приложений в каждой подкатегории. Это позволяет оценивать наиболее часто используемые приложения в организации. Лучшие подкатегории приложений SaaS по общему числу приложений Ниже показаны наиболее часто используемые приложения по перемещению данных в указанных выше подкатегориях.

Top SAAS application subcategories by total number of applications

file-sharing	12
office-programs	7
management	5
email	5

Number of Applications in the subcategory
Industry Average

12 16

File-Sharing 656.04 MB

TOP FILE-SHARING APPS

google-drive-web	350.12 MB
wetransfer	133.70 MB
ms-onedrive-base	96.31 MB
wetransfer	133.70 MB
ms-onedrive-base	96.31 MB
dropbox-base	63.33 MB
google-cloud-storage-download	4.14 MB
sourceforge-base	4.02 MB
mega-base	3.82 MB
adobe-cloud	370.88 KB

Number of Applications in the subcategory
Industry Average

7 7

Office-Programs 1.81 GB

TOP OFFICE-PROGRAMS APPS

google-docs-base	1.62 GB
ms-teams	175.90 MB
ms-office365-base	14.69 MB
evernote-base	1.76 MB
ms-delve	1.17 MB
prezi-base	32.03 KB
yahoo-calendar	21.56 KB

SAAS APPLICATIONS

Number of Applications in the subcategory
Industry Average

5 21

Management 102.52 MB

TOP MANAGEMENT APPS

github-base
82.17 MB

new-relic
9.62 MB

trello-base
7.26 MB

bitbucket-base
3.46 MB

helpscout
10.33 KB

Number of Applications in the subcategory
Industry Average

7 7

Email 1.98 GB

TOP EMAIL APPS

gmail-base
1.77 GB

icloud-mail
132.25 MB

outlook-web-online
67.51 MB

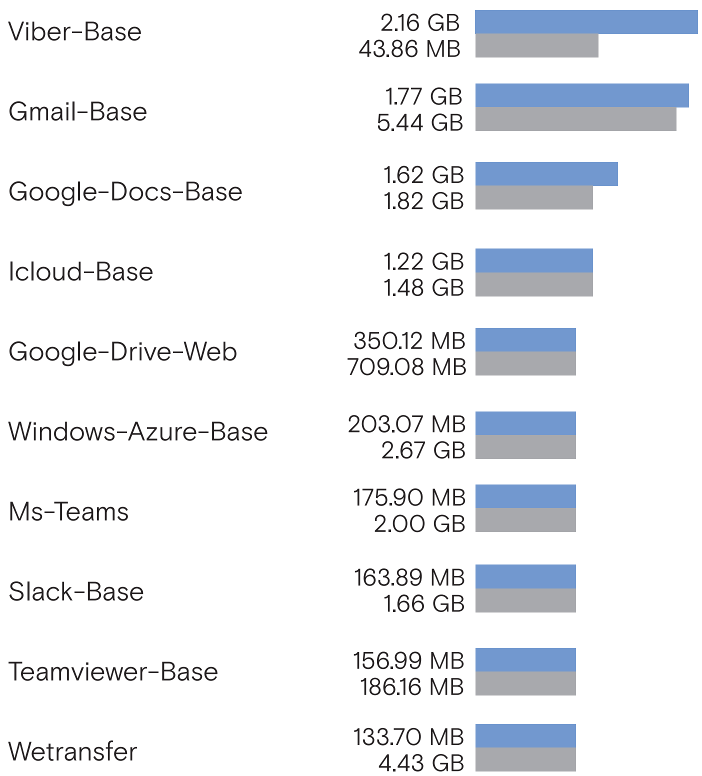
yahoo-mail-base
3.38 MB

mail.ru-mail
2.10 MB

Лучшие приложения SAAS

Ниже показаны 10 лучших приложений SaaS, используемых в вашей организации, и сравнение использования приложений с другими компаниями в отрасли и клиентами Palo Alto Networks.

Top SAAS application by data movement



URL ACTIVITY

Переход по ссылкам

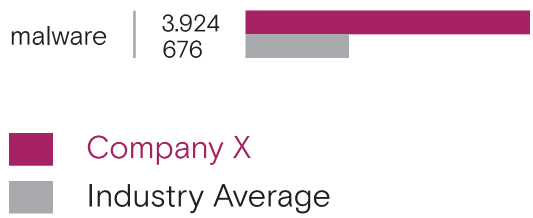
Неконтролируемый просмотр страниц в интернете подвергает предприятие дополнительному риску. Зачастую ссылки служат источником угроз, потери данных и нарушений нормативных стандартов. Ниже приведены наиболее частые категории URL-адресов, посещаемых пользователями в сети.

Основные выводы

- Обнаружены следующие категории URL-адресов, представляющих собой высокий уровень риска: gambling, malware а adult.
- Число посещений страниц пользователями за отчетный период: **15,211** (категорий: **8**).
- Пользователи осуществляют разнообразные действия в интернете, связанные как с работой, так и с личными интересами. В том числе наблюдается посещение веб-сайтов, представляющих определенный риск.

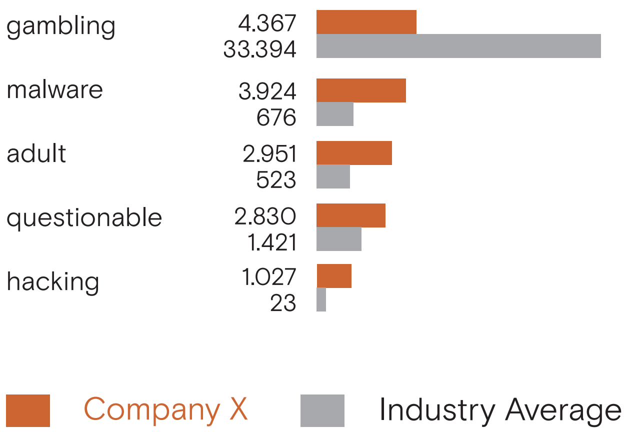
Категории URL-адресов, представляющих собой высокий уровень риска

Сеть представляет собой основную сферу деятельности злоумышленников. При этом потенциально опасные страницы представляют собой наибольшую опасность. Требуется возможность оперативной блокировки нежелательных и вредоносных сайтов, а также поддержка быстрого изучения и классификации неизвестных страниц.



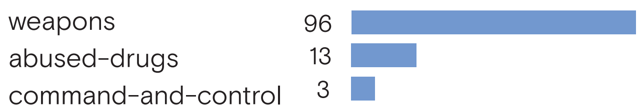
Категории интенсивно посещаемых URL-адресов

Ниже приведены пять наиболее часто посещаемых категорий URL-адресов, а также стандартные показатели для аналогичных предприятий в данной отрасли.



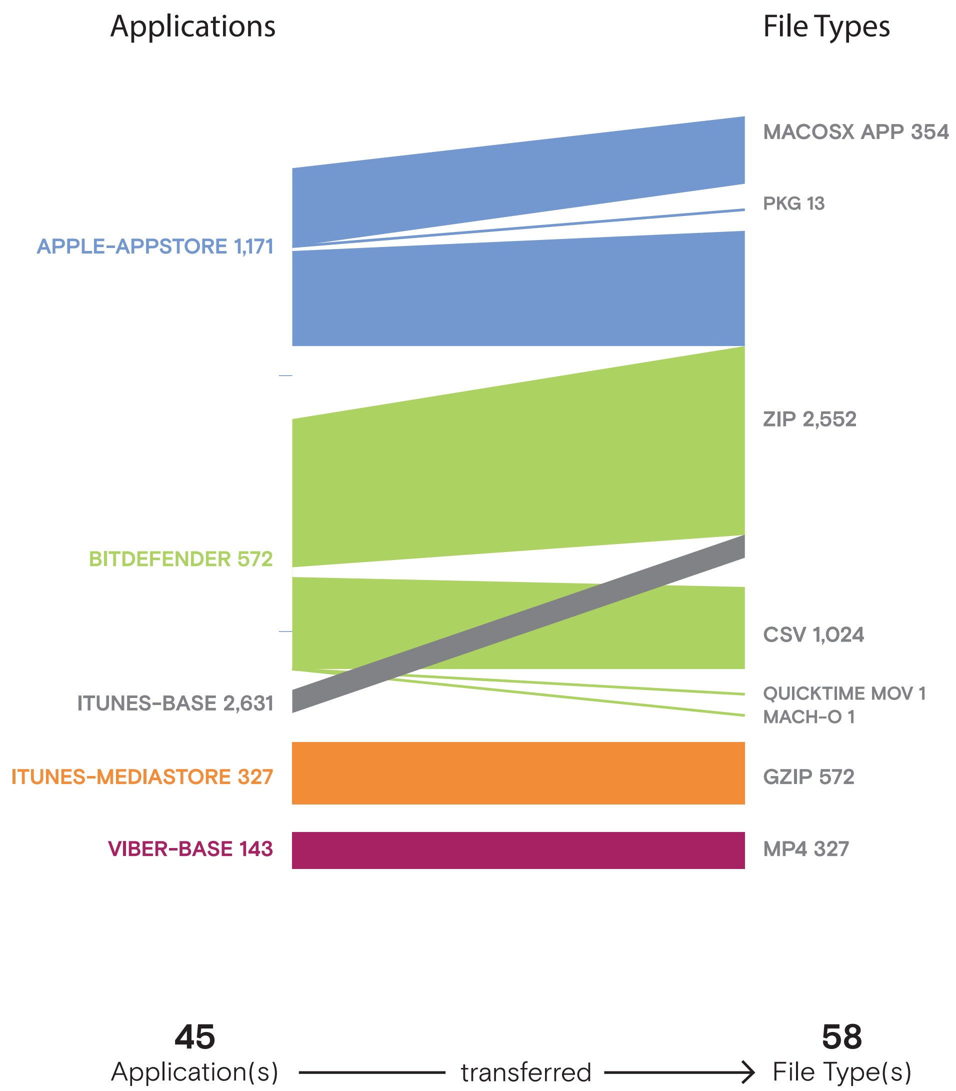
Категории часто используемых URL-адресов

Ниже приведены пятнадцать верхних категорий списка наиболее часто посещаемых URL-адресов.



Анализ передачи файлов

Приложения, осуществляющие передачу файлов, выполняют важные коммерческие функции, но при этом служат лазейкой для киберугроз и открывают доступ к конфиденциальным данным. В рамках вашей организации обнаружено файлов (всего): **866** (типов файлов: 58, используемых для этого приложений: 45) Следующее изображение отражает приложения, наиболее часто используемые для передачи файлов, и соответствующие основные типы передаваемых файлов, а также их содержимое.



Краткая сводка по угрозам

Понимание основных видов угроз, а также методов их устранения требует специальных аналитических сведений о потенциальных опасностях в рамках конкретной организации. В данном разделе приведено описание уязвимостей в приложениях, известных и неизвестных вредоносных программ, операций по отправке исходящих команд и действий удаленного управления, наблюдаемых в сети.

Основные выводы

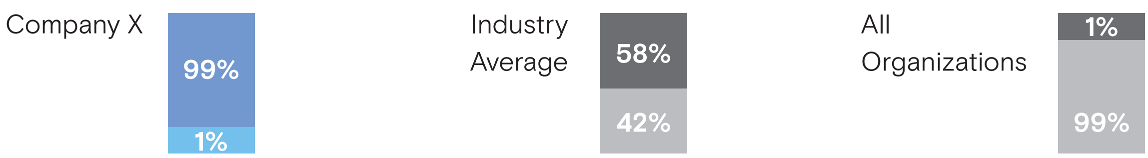
- В рамках организации обнаружено программ, использующих уязвимости системы: **6,056,057** (категории уязвимостей:brute-force, info-leak а code-execution)
- Всего обнаружено вредоносных программ : **0**, при среднем значении для других аналогичных организаций в отрасли: **311**.
- Обнаружено операций по отправке исходящих команд и запросов удаленного управления: **4,038**. Сюда относятся попытки передачи потенциально опасных данных, загрузки дополнительных вредоносных программ, передачи инструкций и получения конфиденциальных данных.

6,056,057
Vulnerability Exploit(s)

brute-force	6,053,034
info-leak	1,463
code-execution	1,171
Other	389

4,038
Command and Control Detection(s)

Known Connections	4,038



Файлы, потенциально способные покидать пределы сети

Transferring files is a required and common part Передача файлов является неотъемлемой составляющей предприятия. При этом следует обеспечивать визуализацию передаваемого содержимого, с тем чтобы контролировать соответствующие приложения и минимизировать потери данных.

101,972 file(s) potentially leaving the network via **19** different application(s)

Анализ типов файлов, представляющих высокий уровень риска, а также небезопасных файлов

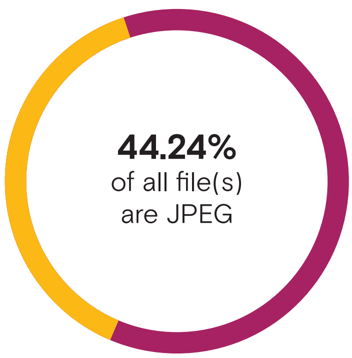
В настоящее время киберпреступники используют в своих целях самые разнообразные типы файлов. Зачастую их целью становятся файлы стандартных корпоративных приложений, которые встречаются на большинстве предприятий. Основным источником угроз служат исполняемые файлы, использующие для проникновения вполне невинное содержимое.

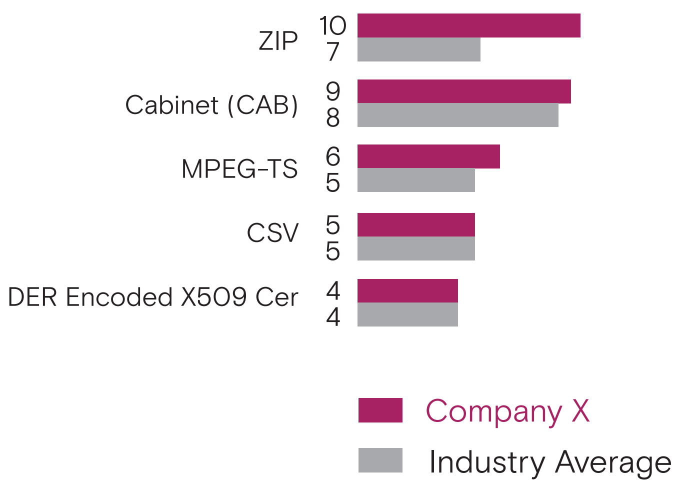
Основные выводы

- В качестве источников угроз используются самые разнообразные типы файлов, и это следует учитывать при определении стратегии борьбы с ними.
- Уменьшить площадь поражения можно, заблокировав типы файлов, представляющие собой максимальную опасность (запрет на скачивание исполняемых файлов, отклонение запросов на скачивание файлов RTF и LNK, которые не являются необходимыми по работе).

Типы файлов, представляющих высокий уровень риска

Приведенные типы файлов особенно опасны для организации, поскольку сочетают в себе обнаружение новых уязвимостей, существующих лазеек и возможность повторного использования в ходе атак.



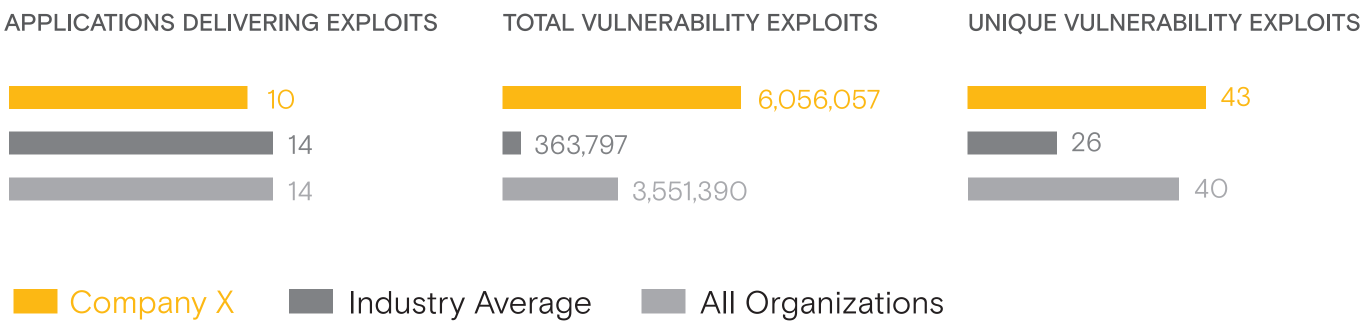


Уязвимости приложений

Уязвимые места приложений позволяют злоумышленникам использовать лазейки в целях заражения и последующего использования атакуемых систем. На этой странице приведены пять верхних позиций в списке приложений, уязвимостями которых злоумышленники пытались воспользоваться в рамках вашей организации. Изучив список, вы выясните, какие приложения представляют собой уязвимые зоны.

Основные выводы

- Всего обнаружено приложений, представляющих собой уязвимости: **10**.
- Всего обнаружено программ, использующих уязвимости системы: **6,056,057** (основные категории: dns, ms-ds-smbv2 а web-browsing).
- Число уникальных уязвимостей: **43**. Это означает, что определенные программы использовались неоднократно.



Попытки использования уязвимостей на приложение

Detections	Exploit ID	Severity	Threat type	CVE ID
6,043,735	**Dns**			
4	PowerDNS Authoritative Server Long qname Denial of Service Vulnerability	HIGH	brute-force	CVE-2016-5426
6,043,731	DNS ANY Queries Brute Force DOS Attack	MEDIUM	brute-force	
9,294	**Ms-Ds-Smbv2**			
9,286	SMB: User Password Brute Force Attempt	HIGH	brute-force	
8	Microsoft Windows RPC Fragment Evasion Attempt	MEDIUM	code-execution	CVE-2008-4250
2,075	**Web-Browsing**			
302	Bash Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2014-6271;CVE-2014-7169;CVE-2014-6277;CVE-2014-6278
230	Apache Struts2 Dynamic Method Invocation Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2016-3081;CVE-2017-12611
83	Apache Struts Content-Type Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2017-5638
27	Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2017-5638
26	Apache Struts 2 Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2010-3749
6	Microsoft Windows HTTP.sys Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2015-1635
4	Spring Data Commons Remote Code Execution Vulnerability	CRITICAL	code-execution	CVE-2013-5331
4	Spring Data Commons Remote Code Execution Vulnerability	CRITICAL	code-execution	
4	Linksys Devices Remote Code Execution Vulnerability	CRITICAL	code-execution	
3	Apache Chunk Encoding Parsing Buffer Overflow Vulnerability	CRITICAL	code-execution	CVE-2002-0392
3	Red Hat JBoss Application Server doFilter Insecure Deserialization Vulnerability	CRITICAL	code-execution	CVE-2017-12149

Анализ команд и запросов удаленного управления

Команды и запросы удаленного управления (CnC) служат признаком того, что сеть поражена вредоносным ПО, которое пытается установить соединение с внешними узлами. Четкое осознание методов предотвращения такого рода атак жизненно необходимо, поскольку они представляют сразу несколько видов опасности: проникновение дополнительных вредоносных программ, извлечение данных и выполнение команд извне.

Основные выводы

- Всего обнаружено приложений, используемых для отправки команд и запросов удаленного доступа: **3**.
- Обнаружено внешних команд и запросов удаленного управления: **4,038**.
- Всего обнаружено подозрительных запросов DNS: **3,992**.

3,992 SUSPICIOUS DNS QUERIES

top 10

generic:sdk.appsflyer.tk 3,894

generic:lucklayed.info 26

generic:tutkryto.su 19

generic:bigdata.adups.com 18

generic:odissey.kiev.ua 6

225125796 5

generic:26.nsmaking.com 5

generic:usd.photios-raj.com 5

generic:track.mialltrack2.com 3

generic:ggmail.com 2

46 SPYWARE PHONE HOME

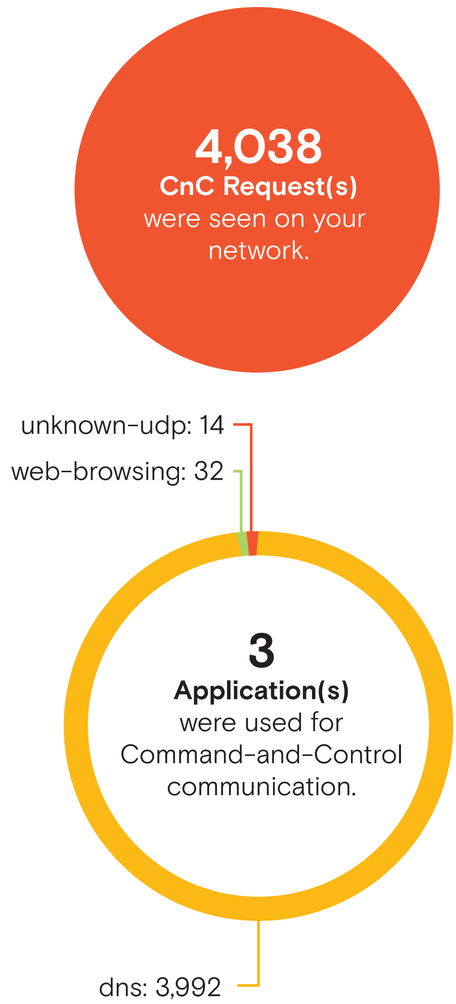
top 10

Suspicious User-Agent Strings 31

ZeroAccess.Gen Command and Control Traffic 11

Win32.Conficker.C p2p 3

CryptoMiner.Gen Malicious Script Detection 1



Сводка Company X

Анализ полученных сведений показал наличие в сети широкого диапазона приложений и кибератак. Такая активность представляет потенциальный риск для безопасности Company X. С другой стороны, это идеальная возможность для внедрения политик безопасного использования приложений и снижения уровня потенциальных угроз, без ограничений для экономического роста организации.

Основные показатели

- В сети обнаружены приложения с высоким уровнем риска: file-sharing, photo-video а email. Требуется дополнительное изучение этих приложений в связи с потенциальными рисками для системы.
- Всего обнаружено приложений в сети: **325** (всего категорий: **28**), при среднем значении для других организаций в отрасли: **246** (Media &Entertainment).
- Всего обнаружено уязвимостей: **6,056,057** (основные категории: dns, ms-ds-smbv2 а web-browsing).
- Всего обнаружено вредоносных программ : **0**, при среднем значении для других аналогичных организаций в отрасли: **311**.
- Всего обнаружено приложений, используемых для отправки команд и запросов удаленного доступа: **3**.

Основные выводы

325	Используемые приложения	6,056,057	Эксплойты
54	Приложения, связанные с высокими рисками	6,060,095	Общее количество угроз
56	Приложения SAAS		

Рекомендации

Необходимо внедрять политики безопасного использования приложений, которые подразумевают применение четко определенных приложений, необходимых для осуществления деятельности предприятия. При этом все остальные приложения должны проходить строгий контроль.

В центре внимания должны находиться приложения с высоким уровнем риска (источники удаленного доступа, обмен файлами, зашифрованные тоннели).

Следует использовать решения, которые способны распознавать и предотвращать источники угроз, известные и неизвестные, а также сводить риски к минимуму.

Оптимальным будет решение, которое автоматически способно перепрограммироваться и создавать новые методы защиты в соответствии с угрозами, возникающими в результате действий корпоративных пользователей.