Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURITY CHECKUP

THREAT ANALYSIS REPORT

Дата

Подготовлено для

Кем подготовлено

Отрасль

Размер компании

Страна

Продолжительность анализа

Анализ сети

Версия шлюза безопасности

Устройство безопасности

Трафик проверялся следующими Программными блейдами Check Point:

Следующий отчет Security Checkup предоставляет результаты оценки безопасности, проведенной в вашей сети. Данный отчет указывает места, где ваша организация может быть подвержена угрозам безопасности, а также предлагает рекомендации по реагированию на данные риски.
Для оценки риска трафик был проверен Check Point для обнаружения ряда угроз безопасности, включая: заражение вредоносным ПО, использование веб приложений высокой степени риска, попытки вторжения, утечка важных данных и т.п.

Интернет доступ высокой степени риска

5 опасных веб-приложений

2.2GB

Потенциальные риски: открытие бекдоров в вашу сеть, сокрытие пользовательской активности, возможность утечки данных или заражения вредоносным ПО.

0 опасные вэб-сайты

0 hits

Потенциальные риски: Подверженность сети к Интернет угрозам и заражению вредоносным ПО. Примеры: СПАМ, зараженные и фишинговые сайты.

0 Облачные приложения

0B

Риск утечки данных и нарушение соответствий требованиям регуляторов и стандартов безопасности. Примеры: Dropbox, Google Drive, OneDrive.

Утечка данных

49 потенциальных утечек данных

7 категорий данных

Отображает информацию, отправленную за пределы сети компании или неавторизованным сотрудникам внутри компании.

Вредоносное ПО и атаки

7 зараженных ботами компьютеров

19 communications with C&C* sites

* C&C - командный центр управления. Если используется прокси-сервер, то число зараженных компьютеров на деле может быть больше.

14 известных вирусов, зашруженных

8 пользователями

14 новых вирусов загружено

Новая модификация вредоносного ПО - это атака 0 □□□ □□□ □□□□□□□□□□□ □□□ неизвестной еще для антивируса сигнатурой.

18 попыток использовать уникальные программные уязвимости

Отображает потенциальные атаки на компьютеры в вашей сети.

Содержимое

Ключевые результаты

USAGE OF HIGH RISK WEB APPLICATIONS

Веб-приложения имеют важное значение для работы каждой организации, но они же создают уязвимость в сфере безопасности. Приложения удаленного администрирования может быть законным, когда используется администраторами и справочной службой, но точно так же некоторые инструменты удаленного доступа могут быть использованы и для кибер-атак. Следующие рискованные веб-приложения были обнаружены в сети, сортированы по категориям, уровню риска и числу пользователей.

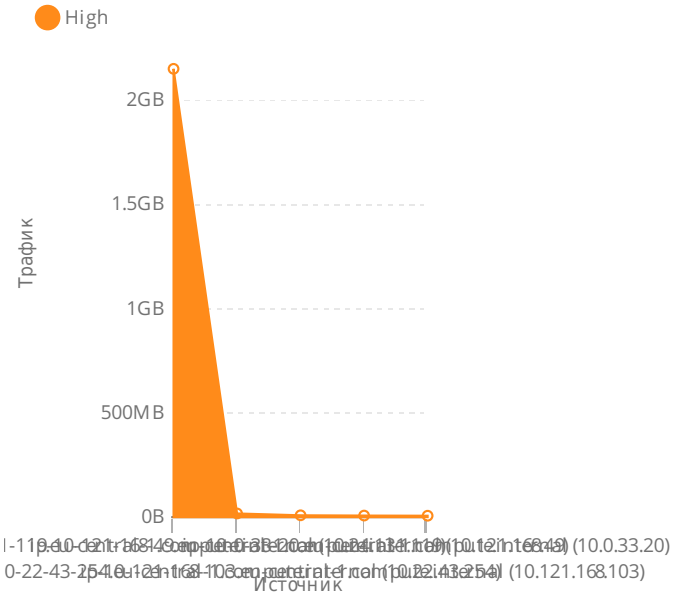
Самые часто используемые веб приложения высокой степени риска (топ 10

Категория приложения	Название приложения	Источник	Опасность приложения*	Трафик
Remote Administration	LogMeIn rescue	ip-10-0-33-20.eu-central-1.com. ip-10-0-33-31.eu-central-1.com. ip-10-0-33-35.eu-central-1.com. ip-10-0-33-68.eu-central-1.com. ip-10-0-33-85.eu-central-1.com. 5 more Источники	4 High	2.2GB
	Remote Desktop Protocol	ip-10-19-239-37.eu-central-1.c... ip-10-22-43-254.eu-central-1.c... ip-10-24-132-101.eu-central-1.c.	4 High	23.2MB
	LogMeIn	ip-10-0-33-105.eu-central-1.co... ip-10-0-34-182.eu-central-1.co... ip-10-19-200-103.eu-central-1.... ip-10-121-168-72.eu-central-1.... ip-10-152-202-81.eu-central-1....	4 High	2.5MB
	Total: 3 Applications	**18 Источники**	**4 High**	**2.2GB**
File Storage and Sharing	Dropbox	ip-10-0-34-162.eu-central-1.co... ip-10-55-248-140.eu-central-1... ip-10-55-248-145.eu-central-1... ip-10-55-248-248.eu-central-1... ip-10-55-249-100.eu-central-1... 4 more Источники	4 High	336.4KB

2.2GB

Общий трафик опасных веб-

5 самых частых источников



*Уровень риска 5 отображает приложения, которые могут обойти систему защиты или скрыть идентификационные данные. Уровень риска 4 отображает приложения, которые способствуют утечке данных или заражению вредоносным ПО без ведома пользователя.

Категория приложения	Название приложения	Источник	Опасность приложения*	Трафик
File Storage and Sharing	**Total: 1 Application**	**9 Источники**	4 **High**	**336.4 KB**
Anonymizer	OpenVPN	ip-10-55-248-71.eu-central-1.compute.internal (10.55.248.71)	5 Critical	22.4KB
	Total: 1 Application	**1 Источник**	5 **Critical**	**22.4 KB**
Total: 3 Categories	**5 Applications**	**28 Источники**	5 **Critical**	**2.2GB**

ИНЦИДЕНТЫ УТЕЧКИ ДАННЫХ

Внутренние данные Вашей компании является одним из наиболее ценных активов. Любая преднамеренная или непреднамеренная утрата может привести к серьезным проблемам. Приведенная ниже информация был послан за пределы компании, или предположительно несанкционированным внутренним пользователям. Потенциально эта информация может быть конфиденциальной, которая должна быть защищена от потери. Ниже представлены характеристики событий потери данных, которые были выявлены в ходе анализа.

Итоги

56 Число сканированых e-mail

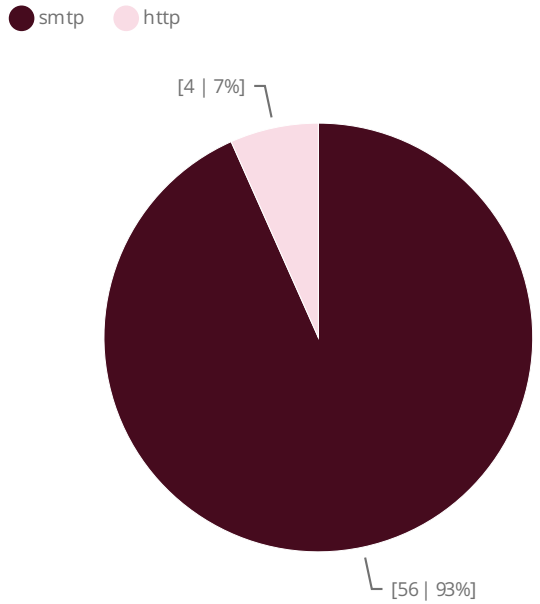
56 Электронные письма с конфиденциальной информацией

4 Инциденты утечки данных через веб-ресурсы

Инциденты утечки данных по типам данных (топ 20)

Тип данных	Пользователи	События	Service
words_dt	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	9	smtp
	ip-10-5-165-178.eu-central-1.compute.internal (10.5.165.178)	6	smtp
	Total: 2 Пользователи	**15**	**1 Service**
hebrew	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	11	smtp
	Total: 1 Пользователь	**11**	**1 Service**
finger	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	6	smtp
	Total: 1 Пользователь	**6**	**1 Service**
ask2	ip-10-5-165-178.eu-central-1.compute.internal (10.5.165.178)	3	smtp

Инциденты по протоколу



Тип данных	Пользователи	События	Service
ask2	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	3	smtp
	Total: 2 Пользователи	**6**	**1 Service**
detect	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	4	smtp
	Total: 1 Пользователь	**4**	**1 Service**
PCI - Cardholder Data	ip-192-168-88-12.eu-central-1.compute.internal (192.168.88.12)	1	http
	ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	1	http
	ip-192-168-15-92.eu-central-1.compute.internal (192.168.15.92)	1	http
	ip-10-16-119-60.eu-central-1.compute.internal (10.16.119.60)	1	http
	Total: 4 Пользователи	**4**	**1 Service**
print	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	3	smtp
	Total: 1 Пользователь	**3**	**1 Service**
Total: 7 Types	**6 Пользователи**	**49**	**2 Services**

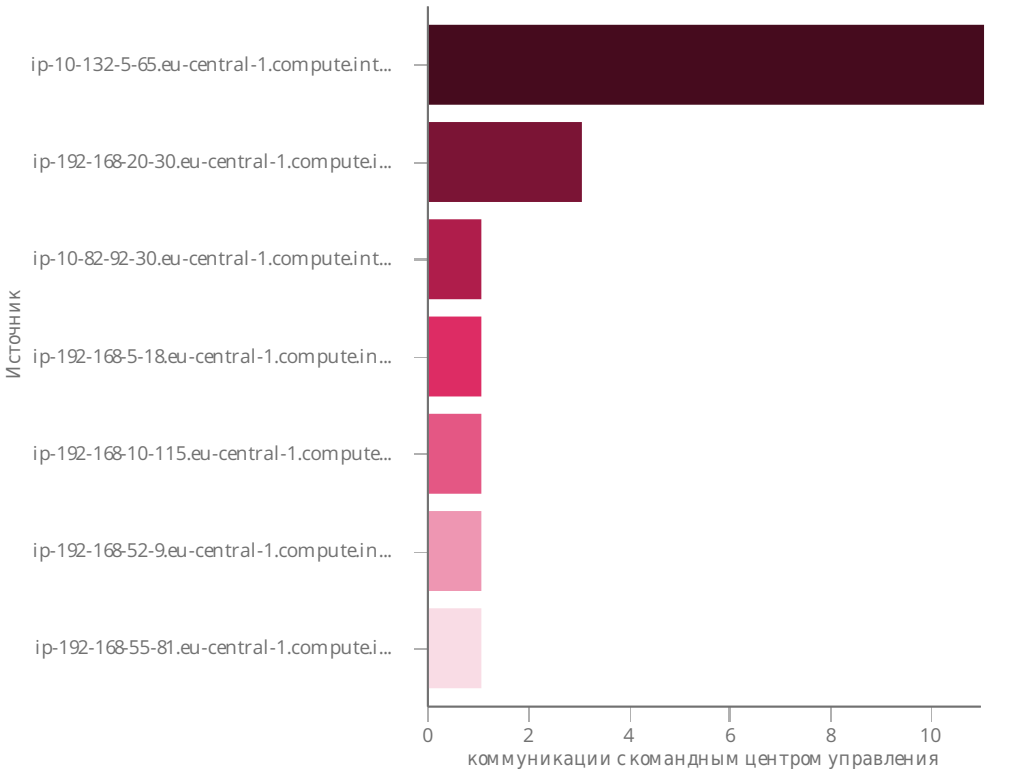
МАШИНЫ, ЗАРАЖЕННЫЕ БОТАМИ

Бот - это вредоносная программа, которая вторгается в ваш компьютер. Боты позволяют преступникам удаленно управлять компьютером для выполнения незаконной деятельности, таких как кражи данных, распространения спама, распространения вредоносного ПО и участия в атаках “отказа в обслуживании» (DOS) без вашего ведома. Боты играют ключевую роль в таргетированных атаках, известных как Advanced Persistent Threats (APTS). В следующей таблице приведены бот семьи и количество зараженных компьютеров, обнаруженных в вашей сети.

Заражение ботами (топ 20 ботов)

Название вредоносного ПО*	Семейство вредоносного ПО	Зараженные компьютеры**	Страна получатель
Backdoor.Win32.Taidoor.A	Taidoor	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	United States Brazil Australia **Total: 3 Countries**
		ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	United States **Total: 1 Country**
		ip-192-168-5-18.eu-central-1.compute.internal (192.168.5.18)	United States **Total: 1 Country**
		ip-10-82-92-30.eu-central-1.compute.internal (10.82.92.30)	Australia **Total: 1 Country**

Топ 10 зараженных машин



* Условное обозначение Check Point вредоносного ПО : <тип вредоносного ПО>.<операционная система>.<семейство вредоносного ПО>.<модификация> Для более подробной информациио отдельном вредоносном ПО, ищите имя вредоносного ПО на сайте www.threat-cloud.com

** Общее число зараженных компьютеров (источников) отображает разные компьютеры

Название вредоносного ПО*	Семейство вредоносного ПО	Зараженные компьютеры**	Страна получатель
Backdoor.Win32.Taidoor.A	Taidoor	ip-192-168-55-81.eu-central-1.compute.internal (192.168.55.81)	United States
			Total: 1 Country
		Total: 5 Компьютеры	**3 Countries**
Total: 1 Вредоносное ПО	**1 Family**	**5 Компьютеры**	**3 Countries**

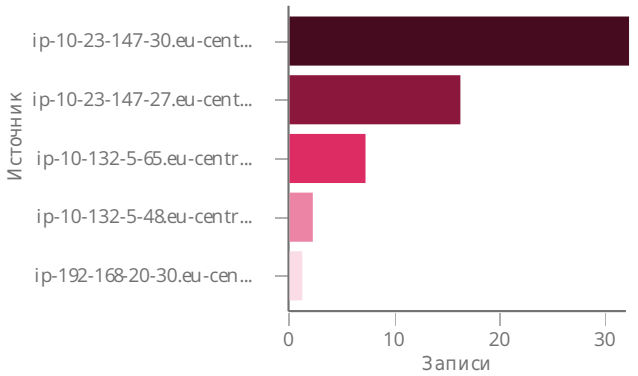
ЗАГРУЗКИ ВИРУСОВ (ИЗВЕСТНЫЕ ВИРУСЫ)

С увеличением сложности кибер-угроз, многие целевые атаки начинаются с использования уязвимостей программного обеспечения в загружаемых файлах и вложениях электронной почты. В ходе анализа безопасности, были обнаружены ряд вредоносных программ, связанных с событиями, которые указывают на загрузку вредоносных файлов. В следующей таблице приведены загрузки известных вредоносных файлов, обнаруженных в вашей сети и количество компьютеров, с которых загрузки производились. Известные вредоносные программы относится к типу вредоносных программ, для которых существуют сигнатуры и, следовательно, должны быть заблокированы системой антивирусной защиты.

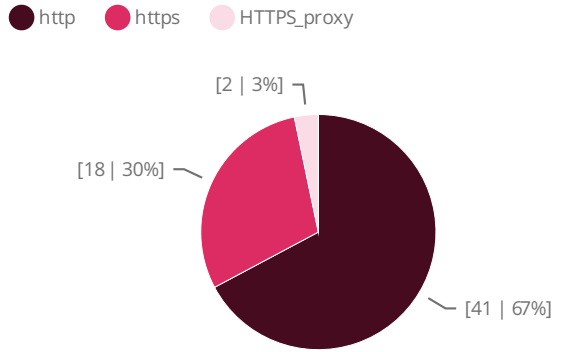
Загрузка вредоносного ПО (топ 20)

Название зараженного файла	Кем загружен	Протокол	MD5*
FileZilla_Server-0_9_45.exe	ip-192-168-160-58.eu-central-1.compute.internal (192.168.160.58)	http	
	ip-192-168-54-130.eu-central-1.compute.internal (192.168.54.130)	http	
	ip-192-168-122-4.eu-central-1.compute.internal (192.168.122.4)	http	
	ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	http	

5 самых частых источников



Загрузки по протоколам



* Вы можете анализировать подозрительные файлы путем копирования и помещения MD5 файлов в онлайн сервис www.virustotal.com

Название зараженного файла	Кем загружен	Протокол	MD5*
FileZilla_Server-0_9_45.exe	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	http	
	Total: 5 Sources	**1 Протокол**	**0 Файлы**
eicar.mod	ip-10-23-147-27.eu-central-1.compute.internal (10.23.147.27)	http https	
	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	https	
	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 3 Sources	**2 Протоколы**	**0 Файлы**
1_level_virus.rar	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
2_level_virus.rar	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
4_level_virus.rar	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
Backdoor.Win32.Bredolab.fzn	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
Virustest.exe	ip-10-132-5-48.eu-central-1.compute.internal (10.132.5.48)	HTTPS_proxy	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
dj.jpg	ip-10-23-147-27.eu-central-1.compute.internal (10.23.147.27)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**

Название зараженного файла	Кем загружен	Протокол	MD5*
Backdoor.MSIL.Agent.ju	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
3_level_virus.rar	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
6_level_virus.rar	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
exe_hash.EXE	ip-10-23-147-27.eu-central-1.compute.internal (10.23.147.27)	https	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
Backdoor.Win32.Bredolab.ggk	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
5_level_virus.rar	ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	http	
	Total: 1 Source	**1 Протокол**	**0 Файлы**
Total: 14 Files	**8 Sources**	**3 Протоколы**	**0 Файлы**

ЗАГРУЗКИ ИЗМЕНЕННЫХ ВИРУСОВ (НЕИЗВЕСТНЫЕ ВИРУСЫ)

В то время как кибер-угрозы становятся все более сложными, продвинутые угрозы часто включают в себя новые варианты вредоносных программ без существующих защит, именуемых APOS. Эти угрозы включают в себя новые (нулевого дня) эксплойты или даже варианты известных эксплойтов, без существующих сигнатур и, следовательно, не обнаруживающихся стандартными решениями. Обнаружение этих типов вредоносных программ требует запуска их в виртуальной песочнице, чтобы обнаружить вредоносное поведение. В ходе анализа безопасности, были обнаружены ряд вредоносных программ, связанных с событиями в вашей сети. В таблице ниже приведены загрузки новых вредоносных вариантов, обнаруженных в вашей сети.

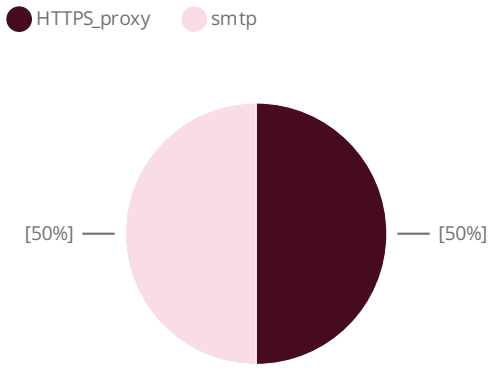
172 Общее количество просканированных файлов

2 Общее количество найденного вредоносного ПО (с использованием технологии песочницы)

Загрузки новых модификаций вредоносного ПО (топ 20)

Имя зараженно... файла	Источник	Действия вредоносного ПО	Загрузки	MD5*	Протокол
Diablo3_Requirements_m.doc	ip-10-5-154-50.eu-central-1.compute.internal (10.5.154.50)	Unexpected Process Crash	1	1f202334fb88c9030ca2f14de16b701f	HTTPS_proxy
Business Offer.pdf	ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	Behaves like a known malware (Gener... Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware activity observed (Exploit.JS.Pd. Unexpected Process Creation Unexpected Process Termination	1	1f202334fb88c9030ca2f14dd16b600f	smtp
Total: 2 Files	**2 Sources**	**8 Действия вредоносного ПО**	**2**	**2 Files MD5**	**2 Services**

Загрузки вредоносного ПО по



Самые часто используемые

Тип файла	Число файлов	Загрузка
pdf	1 Файл	1
doc	1 Файл	1
Total: 2 Types	**2 Файлы**	**2 Загрузки**

* Вы можете анализировать подозрительные файлы путем копирования и помещения MD5 файлов в онлайн сервис www.virustotal.com

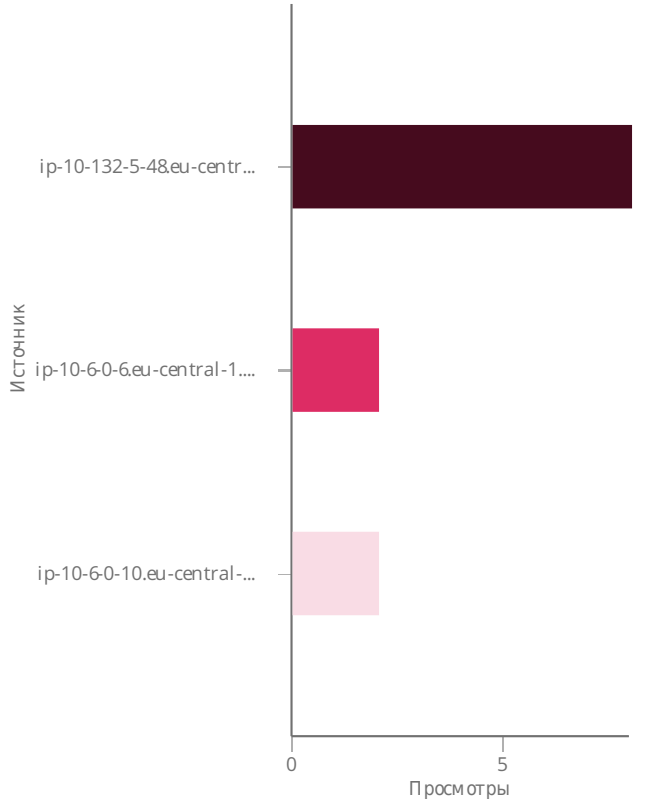
ДОСТУП К САЙТАМ, ПОДОЗРЕВАЕМЫХ В ЗАРАЖЕНИИ

Организации могут заразиться вредоносным ПО путем доступа к вредоносным веб-сайтам во время работы в Интернете, или нажав на вредоносные ссылки, встроенные в полученной электронной почте. Ниже представлен краткий обзор событий, связанных с сайтами, известными содержанием вредоносного программного обеспечения.

Самые часто используемые вредоносные сайты (топ 10)

URL	Просмотры
http://charterbeans.info/	4
	4
http://13131.info/	2
http://66kooum.com/	2
	12

5 самых часто используемых



* Вы можете анализировать подозрительные URL путем копирования и помещения их в онлайн сервис www.virustotal.com

АТАКИ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНЫХ УЯЗВИМОСТЕЙ

В ходе анализа безопасности, были обнаружены атаки и эксплуатируемые уязвимости программного обеспечения на серверах / клиентов. Такие инциденты могут указывать на попытки вторжения, вирусные атаки, атаки DoS или попытки преодолеть безопасность за счет использования уязвимостей программного обеспечения. Ниже приводится краткое описание этих событий.

Самые распространенные атаки и эксплуатируемые программные уязвимости (топ 20)

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
GNU Bash Remote Code Execution	ip-192-168-38-194.eu-central-1.compute.internal (192.168.38.194)	ip-10-38-193-100.eu-central-1.compute.internal (10.38.193.100)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	287
		Total: 1 Destination	**6 References**	**287**
	ip-10-59-1-144.eu-central-1.compute.internal (10.59.1.144)	ip-10-10-82-164.eu-central-1.compute.internal (10.10.82.164)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	195
		Total: 1 Destination	**6 References**	**195**
	ip-192-168-3-4.eu-central-1.compute.internal (192.168.3.4)	ip-10-18-5-90.eu-central-1.compute.internal (10.18.5.90)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	195
		Total: 1 Destination	**6 References**	**195**
	ip-192-168-74-235.eu-central-1.compute.internal (192.168.74.235)	ip-10-63-99-14.eu-central-1.compute.internal (10.63.99.14)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	194

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
GNU Bash Remote Code Execution	ip-192-168-74-235.eu-central-1.compute.internal (192.168.74.235)	**Total: 1 Destination**	**6 References**	**194**
	ip-10-55-118-3.eu-central-1.compute.internal (10.55.118.3)	ip-192-168-9-23.eu-central-1.compute.internal (192.168.9.23)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	77
		Total: 1 Destination	**6 References**	**77**
	Total: 11 Sources	**11 Destinations**	**6 References**	**1.3K**
Ping of Death	ip-10-87-138-4.eu-central-1.compute.internal (10.87.138.4)	ip-10-3-116-1.eu-central-1.compute.internal (10.3.116.1)	CVE-1999-0128	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-10-120-194-78.eu-central-1.compute.internal (10.120.194.78)	ip-10-3-116-1.eu-central-1.compute.internal (10.3.116.1)	CVE-1999-0128	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-10-30-246-47.eu-central-1.compute.internal (10.30.246.47)	ip-10-3-116-1.eu-central-1.compute.internal (10.3.116.1)	CVE-1999-0128	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-10-78-67-122.eu-central-1.compute.internal (10.78.67.122)	ip-10-3-116-1.eu-central-1.compute.internal (10.3.116.1)	CVE-1999-0128	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-10-96-117-81.eu-central-1.compute.internal (10.96.117.81)	ip-10-3-116-1.eu-central-1.compute.internal (10.3.116.1)	CVE-1999-0128	2
		Total: 1 Destination	**1 Reference**	**2**
	Total: 89 Sources	**1 Destination**	**1 Reference**	**178**

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
MIT Kerberos kadmind RPC Library RPCSEC_GSS Authentication Buffer Overflow	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	ip-10-82-92-147.eu-central-1.compute.internal (10.82.92.147)	CVE-2007-3999	6
		ip-192-168-72-190.eu-central-1.compute.internal (192.168.72.190)	CVE-2007-3999	6
		ip-10-7-98-85.eu-central-1.compute.internal (10.7.98.85)	CVE-2007-3999	4
		ip-192-168-55-23.eu-central-1.compute.internal (192.168.55.23)	CVE-2007-3999	3
		ip-10-7-104-26.eu-central-1.compute.internal (10.7.104.26)	CVE-2007-3999	3
		Total: 14 Destinations	**1 Reference**	**32**
	ip-192-168-9-78.eu-central-1.compute.internal (192.168.9.78)	ip-192-168-72-162.eu-central-1.compute.internal (192.168.72.162)	CVE-2007-3999	6
		ip-10-23-147-5.eu-central-1.compute.internal (10.23.147.5)	CVE-2007-3999	6
		ip-192-168-72-40.eu-central-1.compute.internal (192.168.72.40)	CVE-2007-3999	4
		ip-10-23-147-92.eu-central-1.compute.internal (10.23.147.92)	CVE-2007-3999	3
		ip-10-225-243-132.eu-central-1.compute.internal (10.225.243.132)	CVE-2007-3999	3
		Total: 7 Destinations	**1 Reference**	**25**
	ip-10-226-111-7.eu-central-1.compute.internal (10.226.111.7)	ip-10-225-243-132.eu-central-1.compute.internal (10.225.243.132)	CVE-2007-3999	6

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
MIT Kerberos kadmind RPC Library RPCSEC_GSS Authentication Buffer Overflow	ip-10-226-111-7.eu-central-1.compute.internal (10.226.111.7)	ip-10-225-243-64.eu-central-1.compute.internal (10.225.243.64)	CVE-2007-3999	4
		Total: 2 Destinations	**1 Reference**	**10**
	ip-10-132-5-213.eu-central-1.compute.internal (10.132.5.213)	ip-10-7-98-85.eu-central-1.compute.internal (10.7.98.85)	CVE-2007-3999	4
		ip-10-225-243-12.eu-central-1.compute.internal (10.225.243.12)	CVE-2007-3999	2
		Total: 2 Destinations	**1 Reference**	**6**
	ip-10-82-92-88.eu-central-1.compute.internal (10.82.92.88)	ip-192-168-72-71.eu-central-1.compute.internal (192.168.72.71)	CVE-2007-3999	5
		Total: 1 Destination	**1 Reference**	**5**
	Total: 14 Sources	**22 Destinations**	**1 Reference**	**100**
Cisco Unified Communications Manager CTL Provider Heap Overflow	ip-10-82-92-3.eu-central-1.compute.internal (10.82.92.3)	ip-192-168-11-122.eu-central-1.compute.internal (192.168.11.122)	CVE-2008-0027	4
		ip-192-168-72-92.eu-central-1.compute.internal (192.168.72.92)	CVE-2008-0027	1
		Total: 2 Destinations	**1 Reference**	**5**
	ip-10-41-20-115.eu-central-1.compute.internal (10.41.20.115)	ip-192-168-32-80.eu-central-1.compute.internal (192.168.32.80)	CVE-2008-0027	2
		ip-192-168-72-80.eu-central-1.compute.internal (192.168.72.80)	CVE-2008-0027	2
		Total: 2 Destinations	**1 Reference**	**4**

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
Cisco Unified Communications Manager CTL Provider Heap Overflow	ip-10-82-92-54.eu-central-1.compute.internal (10.82.92.54)	ip-192-168-72-80.eu-central-1.compute.internal (192.168.72.80)	CVE-2008-0027	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-10-10-57-2.eu-central-1.compute.internal (10.10.57.2)	ip-192-168-72-92.eu-central-1.compute.internal (192.168.72.92)	CVE-2008-0027	1
		Total: 1 Destination	**1 Reference**	**1**
	Total: 4 Sources	**4 Destinations**	**1 Reference**	**12**
Microsoft Windows RASMAN Service Memory Corruption (MS06-025)	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	ip-192-168-20-92.eu-central-1.compute.internal (192.168.20.92)	CVE-2006-1314	4
		ip-10-23-147-52.eu-central-1.compute.internal (10.23.147.52)	CVE-2006-1314	2
		Total: 2 Destinations	**1 Reference**	**6**
	ip-192-168-54-22.eu-central-1.compute.internal (192.168.54.22)	ip-192-168-33-6.eu-central-1.compute.internal (192.168.33.6)	CVE-2006-1314	1
		ip-10-82-92-4.eu-central-1.compute.internal (10.82.92.4)	CVE-2006-1314	1
		Total: 2 Destinations	**1 Reference**	**2**
	ip-192-168-35-16.eu-central-1.compute.internal (192.168.35.16)	ip-10-23-147-47.eu-central-1.compute.internal (10.23.147.47)	CVE-2006-1314	1
		Total: 1 Destination	**1 Reference**	**1**
	ip-10-225-243-38.eu-central-1.compute.internal (10.225.243.38)	ip-10-82-92-4.eu-central-1.compute.internal (10.82.92.4)	CVE-2006-1314	1
		Total: 1 Destination	**1 Reference**	**1**
	Total: 4 Sources	**5 Destinations**	**1 Reference**	**10**

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
Alt-N Technologies SecurityGateway Username Buffer Overflow	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	ip-192-168-20-92.eu-central-1.compute.internal (192.168.20.92)	None	2
		ip-192-168-20-107.eu-central-1.compute.internal (192.168.20.107)	None	1
		ip-192-168-20-123.eu-central-1.compute.internal (192.168.20.123)	None	1
		Total: 3 Destinations	**1 Reference**	**4**
	ip-10-82-92-38.eu-central-1.compute.internal (10.82.92.38)	ip-192-168-20-87.eu-central-1.compute.internal (192.168.20.87)	None	3
		Total: 1 Destination	**1 Reference**	**3**
	ip-10-82-92-114.eu-central-1.compute.internal (10.82.92.114)	ip-192-168-20-217.eu-central-1.compute.internal (192.168.20.217)	None	1
		ip-192-168-20-45.eu-central-1.compute.internal (192.168.20.45)	None	1
		Total: 2 Destinations	**1 Reference**	**2**
	ip-10-82-92-178.eu-central-1.compute.internal (10.82.92.178)	ip-192-168-20-217.eu-central-1.compute.internal (192.168.20.217)	None	1
		Total: 1 Destination	**1 Reference**	**1**
	Total: 4 Sources	**6 Destinations**	**1 Reference**	**10**
Novell eDirectory HTTP Headers Denial of Service	ip-10-5-3-18.eu-central-1.compute.internal (10.5.3.18)	ip-10-7-210-42.eu-central-1.compute.internal (10.7.210.42)	CVE-2008-0927	1
		ip-10-10-98-42.eu-central-1.compute.internal (10.10.98.42)	CVE-2008-0927	1

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
Novell eDirectory HTTP Headers Denial of Service	ip-10-5-3-18.eu-central-1.compute.internal (10.5.3.18)	**Total: 2 Destinations**	**1 Reference**	**2**
	ip-192-168-9-100.eu-central-1.compute.internal (192.168.9.100)	ip-192-168-72-4.eu-central-1.compute.internal (192.168.72.4)	CVE-2008-0927	1
		Total: 1 Destination	**1 Reference**	**1**
	ip-10-10-87-94.eu-central-1.compute.internal (10.10.87.94)	ip-10-6-11-70.eu-central-1.compute.internal (10.6.11.70)	CVE-2008-0927	1
		Total: 1 Destination	**1 Reference**	**1**
	ip-192-168-54-22.eu-central-1.compute.internal (192.168.54.22)	ip-10-23-147-47.eu-central-1.compute.internal (10.23.147.47)	CVE-2008-0927	1
		Total: 1 Destination	**1 Reference**	**1**
	ip-192-168-33-6.eu-central-1.compute.internal (192.168.33.6)	ip-10-82-92-4.eu-central-1.compute.internal (10.82.92.4)	CVE-2008-0927	1
		Total: 1 Destination	**1 Reference**	**1**
	Total: 8 Sources	**9 Destinations**	**1 Reference**	**9**
Repetitive SMB Login Attempts	ip-10-225-243-77.eu-central-1.compute.internal (10.225.243.77)	ip-10-226-69-14.eu-central-1.compute.internal (10.226.69.14)	None	4
		Total: 1 Destination	**1 Reference**	**4**
	ip-10-225-243-8.eu-central-1.compute.internal (10.225.243.8)	ip-10-226-69-87.eu-central-1.compute.internal (10.226.69.87)	None	3
		Total: 1 Destination	**1 Reference**	**3**
	Total: 2 Sources	**2 Destinations**	**1 Reference**	**7**
ShellShock - GNU Bash Remote Code Execution	ip-192-168-38-194.eu-central-1.compute.internal (192.168.38.194)	ip-10-38-193-100.eu-central-1.compute.internal (10.38.193.100)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	2

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
ShellShock - GNU Bash Remote Code Execution	ip-192-168-38-194.eu-central-1.compute.internal (192.168.38.194)	**Total: 1 Destination**	**6 References**	**2**
	ip-192-168-3-14.eu-central-1.compute.internal (192.168.3.14)	ip-10-64-21-103.eu-central-1.compute.internal (10.64.21.103)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	1
		Total: 1 Destination	**6 References**	**1**
	ip-192-168-19-16.eu-central-1.compute.internal (192.168.19.16)	ip-10-10-41-78.eu-central-1.compute.internal (10.10.41.78)	CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 1 more Reference	1
		Total: 1 Destination	**6 References**	**1**
	Total: 3 Sources	**3 Destinations**	**6 References**	**4**
MS-SQL Server Sp_replwritetovarbin Stored Procedure Buffer Overflow	ip-192-168-13-86.eu-central-1.compute.internal (192.168.13.86)	ip-192-168-9-71.eu-central-1.compute.internal (192.168.9.71)	CVE-2008-5416	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-192-168-35-16.eu-central-1.compute.internal (192.168.35.16)	ip-10-23-147-47.eu-central-1.compute.internal (10.23.147.47)	CVE-2008-5416	1
		ip-10-82-92-4.eu-central-1.compute.internal (10.82.92.4)	CVE-2008-5416	1
		Total: 2 Destinations	**1 Reference**	**2**
	Total: 2 Sources	**3 Destinations**	**1 Reference**	**4**
HP OpenView Products OVTrace Service Stack Buffer Overflow	ip-192-168-9-100.eu-central-1.compute.internal (192.168.9.100)	ip-192-168-72-4.eu-central-1.compute.internal (192.168.72.4)	CVE-2007-3872	3
		Total: 1 Destination	**1 Reference**	**3**

Атака / Эксплойт	Источник	Получатель	Промышленное применение	События
HP OpenView Products OVTrace Service Stack Buffer Overflow	**Total: 1 Source**	**1 Destination**	**1 Reference**	**3**
IMAP Directory Traversal	ip-10-226-69-28.eu-central-1.compute.internal (10.226.69.28)	ip-10-242-54-7.eu-central-1.compute.internal (10.242.54.7)	CAN-2005-1902 CAN-2006-2414	2
		Total: 1 Destination	**2 References**	**2**
	ip-10-226-69-35.eu-central-1.compute.internal (10.226.69.35)	ip-10-242-54-171.eu-central-1.compute.internal (10.242.54.171)	CAN-2005-1902 CAN-2006-2414	1
		Total: 1 Destination	**2 References**	**1**
	Total: 2 Sources	**2 Destinations**	**2 References**	**3**
RealNetworks RealPlayer AVI Parsing Buffer Overflow	ip-10-7-104-66.eu-central-1.compute.internal (10.7.104.66)	ip-10-7-98-132.eu-central-1.compute.internal (10.7.98.132)	CAN-2005-2052	2
		Total: 1 Destination	**1 Reference**	**2**
	ip-10-7-104-98.eu-central-1.compute.internal (10.7.104.98)	ip-10-7-98-19.eu-central-1.compute.internal (10.7.98.19)	CAN-2005-2052	1
		Total: 1 Destination	**1 Reference**	**1**
	Total: 2 Sources	**2 Destinations**	**1 Reference**	**3**
Multiple Vendor SNMPv3 HMAC Handling Authentication Bypass	ip-10-7-104-62.eu-central-1.compute.internal (10.7.104.62)	ip-10-7-98-81.eu-central-1.compute.internal (10.7.98.81)	CVE-2008-0960	1
		Total: 1 Destination	**1 Reference**	**1**
	Total: 1 Source	**1 Destination**	**1 Reference**	**1**
Total: 14 Атаки / Эксплойты	**140 Sources**	**64 Destinations**	**18 References**	**1.7 K**

ИСПОЛЬЗОВАНИЕ КАНАЛА ПРИЛОЖЕНИЯМИ И ВЕБ-САЙТАМИ

Каналы доступа к сети в Организации, как правило, используются для доступа к разнообразным веб-приложениям и сайтам, необходимых сотрудниками. Приложения, использующие много трафика, как например, потоковое мультимедиа, может ограничить полосу пропускания, которая необходима для важных бизнес-приложений. Необходимо понимать важность контроля пропускной способности сети для того, чтобы ограничить потребление канала для приложений, не связанных с бизнесом. Ниже представлен краткий обзор использования пропускной способности вашей организации, отсортированный по потребляемой пропускной способность.

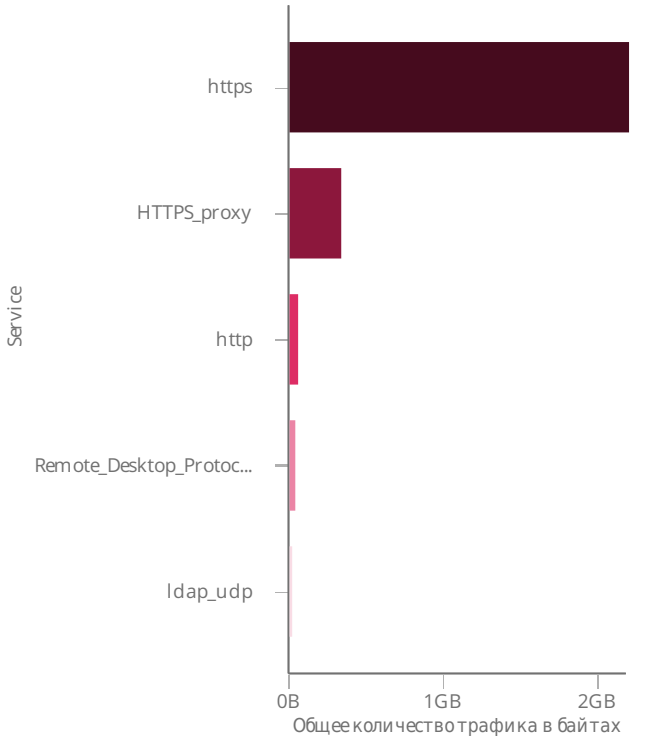
Самые популярные приложения/сайты (топ 30)

Приложение / Сайт	Категории	Уровень риска	Источники	Трафик
LogMeIn rescue	Remote Administration	4 High	10 Источники	2.2GB
YouTube	Media Sharing	2 Low	1 Источник	313.5MB
Remote Desktop Protocol	Remote Administration	4 High	3 Источники	23.2MB
cnn.com/ext/app/redalert/cdaredalert_iframe/0,12639,84-234-208-20,00.html	Search Engines / Portals	— Unknown	1 Источник	22.9MB
Google Search	Search Engines / Portals	2 Low	2 Источники	9.2MB
newmail.aol.com	Search Engines / Portals	— Unknown	1 Источник	3.7MB
LDAP Protocol	Network Protocols	1 Very Low	1 Источник	3.0MB
LogMeIn	Remote Administration	4 High	5 Источники	2.5MB
adobe.com	Computers / Internet	— Unknown	1 Источник	2.2MB
212.235.15.30	Inactive Sites	— Unknown	1 Источник	1.1MB
cdn.stumble-upon.com	Newsgroups / Forums	— Unknown	1 Источник	952.3KB

2.6GB

Общий объем проверенного трафика

Трафик по протоколу



Приложение / Сайт	Категории	Уровень риска	Источники	Трафик
Chartbeat	Business Applications	1 Very Low	1 Источник	655.4KB
server.talkahead.com/scripts	Search Engines / Portals	— Unknown	1 Источник	450.6KB
Dropbox	File Storage and Sharing	4 High	9 Источники	336.4KB
widgets.outbrain.com	Computers / Internet	— Unknown	1 Источник	202.8KB
feeds.delicious.com	Computers / Internet	— Unknown	1 Источник	171.0KB
OpenVPN	Anonymizer	5 Critical	1 Источник	22.4KB
Total: 17 Приложения / Сайты	**10 Categories**	**5 Risks**	**36 Источники**	**2.6GB**

Компьютеры с инцидентами, связанными с Интернет доступом высокого риска и утечкой данных

28

запущенны приложения высокого риска

0

получен доступ к сайтам высокого риска

0

пользователей, запрашиваемых доступ к сомнительным сайтам или к сайтам, не связанных с бизнесом.

6

пользователей, вовлеченных в инциденты с потенциальной утечкой данных

Компьютеры с инцидентами, связанными с вредоносным ПО и атаками

7

заражены вредоносным ПО

8

загружено вредоносное ПО

0

получено писем, содержащих ссылки на зараженный сайт

1

получали доступ с сайтам, известным как зараженные вредоносным ПО

140

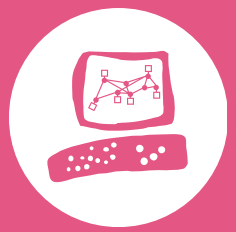
источники атаки

(IP-адрес источника, полученные из IPS событий)

64

жертв атаки

(IP-адреса получателей, взятые из событий IPS)



Программно-определяемая защита

ПРОГРАММНО-ОПРЕДЕЛЯЕМАЯ ЗАЩИТА

В мире с высокими требованиями к IT инфраструктуре и сетям, где периметр уже определен не точно, и где угрозы становятся все более интеллектуальными каждый день, необходимо определить правильный путь для защиты организаций при постоянно меняющемся раскладе угроз безопасности.

Существует тенденция широкого распространения точечных продуктов безопасности, однако эти продукты менее архитектурно ориентированы. Сегодня корпорации нуждаются в единой архитектуре, которая объединяет высокую производительность сетевых устройств безопасности с проактивными технологиями защиты в режиме реального времени. Новая парадигма заставляет защищаться проактивно.

Программно-определяемая защита - это новая практичная архитектура безопасности и методология. Она предлагает инфраструктуру, которая в свою очередь является модульной, гибкой и, что самое главное, БЕЗОПАСНОЙ.

Такая архитектура должна защищать организации любого размера, любого расположения: сетей головных офисов, филиальных отделений, роуминга смартфонов или мобильных устройств, при использовании облачной среды.

Защита должна автоматически адаптироваться к существующим угрозам без необходимости □□□□□□□□□□□ □□□□□□□□ □□□□□□□□□□□□□□□□□ безопасности тысячи рекомендуемых действий. Данные защиты должны прозрачно интегрироваться в большую IT среду и архитектура должна обеспечивать стратегию защиты, которая применяет совместно и внутренние, и внешние интелектуальные источники.

Архитектура программно-определяемой защиты (SDP) разделяет инфраструктуру безопасности на три взаимосвязанных уровня::

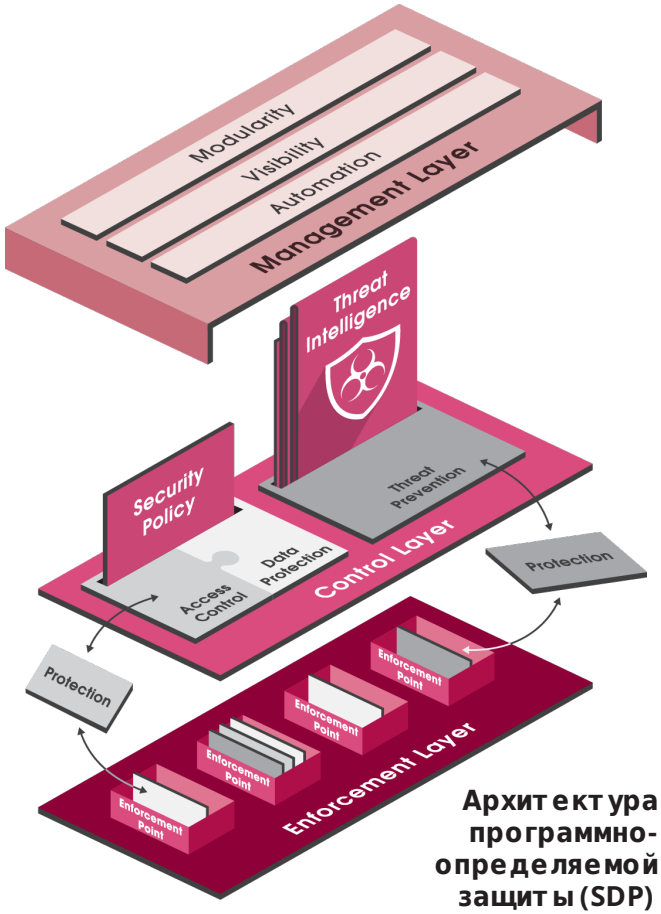
- **Уровень Применения, который основывается на физических**, виртуальных или серверных точках применения безопасности и который разделяет сети в дополнение к выполнению логики защиты в требовательных к производительности средах.

- **Уровень Контроля, который анализирует** различные источники угроз и генерирует защиты и политики для выполнения уровнем Применения.

Уровень Управления который организует инфраструктуру и вносит высокую степень гибкости в общую архитектуру.

Объединяя высокую производительность уровня Применения с быстроразвивающимся и динамическим программным уровнем Контроля, архитектура SDP обеспечивает не только рабочее функционирование, но и проактивное предотвращение инцедентов, связанных с постоянно растущими масштабами угроз безопасности.

Разработанная для того, что быть опережающей, архитектура SDP поддерживает традиционную сетевую безопасность и требования политик контроля доступа, в дополнение к предотвращению угроз, которое включает новые технологии такие, как мобильные вычисления и программно-определяемые сети (SDN).



Архитектура программно-определяемой защиты (SDP)

Программно-определяемая защита Check Point

Check Point □□□□□□□□□□□□ □□□□□ □□□□□□□□□□□ компонентами, необходимыми для внедрения полноценной архитектуры SDP с лучшими в своем классе системами управления и защиты.

Программно-определяемые защиты Check Point обеспечивают гибкость, необходимую для реагирования на новые угрозы, и включают в себя новые технологии. Наши решения генерируют новые и обновленные защиты для известных и неизвестных угроз и проактивно распространяют данные о выявленных угрозах посредством облачного сервиса. Внедрение решений по безопасности компании Check Point, основанное на целостном архитектурном подходе к безопасности, побуждает компании включать качественно новые и надежные решения информационных систем.

CHECK POINT SDP УРОВЕНЬ ПРИМЕНЕНИЯ

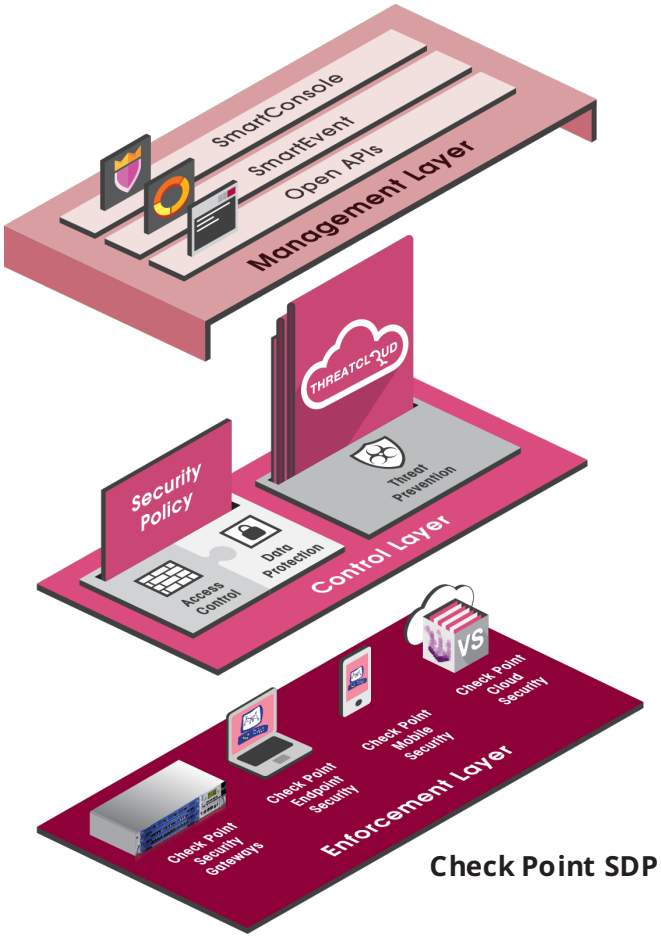
Для защиты границ каждого сегмента Check Point □□□□□□□□□□ □□□□□□□ □□□□□ высокопроизводительных устройств безопасности, виртуальных шлюзов, ПО для рабочих станций и мобильных приложений (Check Point Capsule), □□□□□□□ □□□□□□□□□ □□□ применять защиту не только для корпоративной сети, но и для МУ.

CHECK POINT SDP УРОВЕНЬ КОНТРОЛЯ

Уровень контроля архитектуры Check Point SDP ббазируется на архитектуре программных блейдов Check Point, которая предоставляет заказчикам масштабируемые и эффективные решения безопасности для соответствия именно их требованиям. Заказчики могут выбирать среди 20-ти Программных блейдов, благодаря модульному характеру архитектуры Программных блейдов, тем самым имеют интсрумент для построения необходимого решения безопасности для каждой точки применения и расширения инфраструктуры безопасности.

Предотвращение угроз нового поколения

Check Point □□□□□□□□□□ □□□□□□□□□□□□ контроль над тем, сколько выявлено известных и неизвестных угроз. Решение Check Point по предотвращению угроз (Threat prevention) включает в себя интегрированную систему предотвращения вторжений (IPS) для проактивного предотвращения вторжений, сетевой антивирус для обнаружения и блокирования вредоносного ПО, антибот решение для обнаружения и предотвращения ущерба от действий ботов, песочницу для эмуляции угроз (Threat Emulation) для обнаружения и блокирования неизвестных угроз и атак нулевого дня. Компания Check Point создала уникальный облачный сервис для хранения большого объема информации об угрозах и в тоже время генератор защит Check Point ThreatCloud™. Check Point ThreatCloud позволяет совместно бороться с



Check Point SDP

Межсетевой экран и шлюз безопасного Интернет доступа нового поколения

Контроль доступа Check Point основывается на многочисленных Программных блейдах, которые позволяют создание унифицированной контекстно-ориентированной политики безопасности. Межсетевой экран (Firewall) □□□□□□□□□□□□□ □ □□□□□□□□ □□□□□□ □ □□□□□□□□□, серверам, приложениям и типам подключений. Контроль доступа Интернет приложений (Application Control)□□□□□□□□□□□□□ использование веб2.0 приложений и предотвращает использование приложений высокой степени риска. Фильтрация веб сайтов (URL Filtering) □□□□□□□□□□□□□ □□□□□□ □ □□□□□□□□□□ веб сайтам и предотвращает доступ к сайтам, зараженным вредоносным ПО. Идентификация (Identity Awareness)□□□□□□□□□□ □□□□□□□□□□□□ гранулированный обзор пользователей,компьютеров, групп пользователей и компьютеров, и создавать более детальные политики с использованием идентификационных данных.

Защита данных нового поколения

Решение по защите данных нового поколения охватывает все аспекты для защиты содержимого от попадания его в неправильные руки.. Защита от потери данных (DLP) - составная часть решения по защите данных, помогающего бизнесу незамедлительно защитить конфиденциальную информацию от □□□□□□□□□□□□□□□ □□□□□□; □□□□□□□□ □□□□□□□ технология обучения пользователя тому, как должным образом работать с конфиденциальной информацией. DLP контролирует, чтобы конфиденциальная информацию не покидала пределы сети компании благодаря поддержке Microsoft Exchange.//□□□□□□ □□□□□□□□□□ □□□□□ □□□□ внедрены на всех точках применения безопасности , защищающих конфиденциальные данные от возможного доступа или перемещения на съемный носитель или неавторизованным пользователям.

Check Point Capsule: Расширение Корпоративной Политики Безопасности на Мобильные Устройства

Check Point Capsule □□□□□□□□□ вам расширить защиту Check Point □ □□□□□□□□□ □□ □□ □□□□ мобильные устройства. Такой подход и для корпоративной сети, и для мобильных устройств ваших сотрудников позволяет применять одни и те же защиты против внутренних и внешних угроз. С Check Point Capsule □□ □□□□□□□□ □□□□□□□□ доступ к корпортивной электронной почте, документам и внутренним ресурсам. Личные данные и приложения отделены от бизнес-данных, позволяя безопасно использовать бизнес-ресурсы, не затрагивая личные данные и приложения сотрудника. С помощью Check Point Capsule □□□□□□-□□□□□□□□□ □□□□□□□□ □ □□□□□ месте. защита устанавливается сразу при создании документа и перемещается вместе с ним, гарантируя что конфиденциальная информация полностью защищена от неавторизованного пользователя.

CHECK POINT SDP УРОВЕНЬ УПРАВЛЕНИЯ

Все защиты продуктов и точки применения защиты Check Point управляются из единой унифицированной консоли управления безопасностью. Управление безопасностью Check Point - □□□ □□□□□□□□□□□□□□, обеспечивающее возможность управления десятками и миллионами объектов, поддерживая при этом высокоскоростной пользовательский интерфейс.

Check Point Модульное / Уровневое Управление политикой

Управление безопасностью Check Point поддерживает разделение организации, позволяет администраторам определять политику безопасности для каждого сегмента, разделяя полномочия администраторов. Политики могут быть определены для каждого сегмента. Политики контроля доступа могут быть определены, используя отдельные уровни, которые могут быть назначены на разных администраторов. Многочисленные администраторы могут работать с одной и той же политикой одновременно.

Автоматизаия и Механизмы управления

Управление безопасностью Check Point предоставляет интерфейс командной строки (CLI) □ API □□□ □□□□□□□□, □□□□□□□ □□□□□□□□□ компаниям интегрировать систему управления Check Point □□ □□□□□□□□□□ □□□□□□□□□ □□□□□□, как сетевое управление, CRM, и т.д.

Обзорность, благодаря Check Point SmartEvent

Check Point SmartEvent □□□□□□□□□□ □□□□□□□ большого объема данных и корреляцию событий в режиме реального времени. Данное решение предлагает возможность предоставлять консолидированный и корреляционный просмотр инцидентов на основе информации от многочисленных источников. Анализ событий безопасностисоздает действие, способное информировать в форме индикаторов угроз, которые могут быть распространены через ThreatCloud □□□ □□□□□□□□□□□□□ □□□□□ □ □□□□□□ реального времени.

Для получения более детальной информации о программно-определяемой защите Check Point Software-defined Protection □ □ □□□, □□□ □□□ может помочь в организации ваш инфраструктуры безопасности, посетите:

www.checkpoint.com/sdp

О Check Point

Миссия Check Point Software Technologies' - защита сети Интернет. Компания Check Point была основана в 1993, и с того времени имела в арсенале технологии защиты коммуникаций и операций компаний в сети Интернет.

Check Point □□□ □□□□□□ □ □□□□□□ □□□□□□□, □□□ предложил шлюз безопасности (FireWall-1) и запатентовал технологию Stateful Inspection. Затем Check Point расширил возможности шлюза безопасности, предложив архитектуру Программных блейдов. Динамическая архитектура Программных блейдов предоставляет безопасные, масштабируемые и простые решения, которые можно настроить для соответствия требованиям к защите для любой организации или среды.

Check Point □□□□□□□□□□ □ □□□□□□□□□□□□ широкий выбор как программного обеспечения, так и программно-аппаратных комплексов, и в дополнение сервисов для защиты IT. Мы предлагаем нашим заказчикам обширное портфолио решений по защите сети, данных и рабочих станций, а также возможностей системы управления безопасности. Наши решения работают на базе единой архитектуры безопасности, которая позволяет осуществлять полноценную защиту при использовании одного шлюза безопасности и единого клиента для защиты рабочих станций, которые управляются с единой консоли управления. Данное унифицированное управление позволяет упростить внедрение и централизует контроль над безопасностью.

Наши продукты и сервисы продаются в большие организации, сервисные провайдеры, в компании небольшого и среднего размера. Наша концепция открытой платформы безопасности (Open Platform for Security (OPSEC)) □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ возможности наших продуктов и сервисов, дополняя решениями сторонних фирм. Наши решения продаются, интегрируются и обслуживаются сетью партнеров по всему миру. Заказчики компании Check Point включают десятки тысяч организаций разного размера, включая все компании из списка Fortune 100. Первоклассное решение ZoneAlarm компании Check Point защищает миллионы пользователей от хакеров, шпионского ПО и кражи данных

www.checkpoint.com