CHECK POINT STARS PARTNER

CHECK POINT SandBlast™ ZERO-DAY PROTECTION

ABRIKOS GROUP

Защита от угроз 0-го дня

Сергей Боровиков
Технический директор
sb@abrikos-group.ru

Check Point CCSA R80 Certified Security Administrator CERTIFICATION

Check Point SandBlast Specialist SandBlast Network SPECIALIZATION

Check Point SandBlast Specialist SandBlast Agent SPECIALIZATION

Check Point SandBlast Specialist SandBlast Mobile SPECIALIZATION

Группа компаний «АБРИКОС» – системный интегратор спектра решений и услуг в сфере информационных технологий. Приоритетными направлениями в работе компании являются:

Инфраструктурные решения:

- Вычислительная инфраструктура
- Инфраструктура хранения данных
- Телекоммуникационные решения

Управление ИТ-инфраструктурой

- Виртуализация и облачные сервисы
- Системы резервного копирования и восстановления данных
- Катастрофоустойчивость

Информационная безопасность

- Антивирусная защита
- Безопасность сетевого трафика
- DLP-решения
- Безопасность веб-приложений
- Тестирование на проникновение

Услуги

- ИТ-консалтинг
- ИТ-аутсорсинг. Сопровождение ИТ-инфраструктуры.

ABRIKOS GROUP

CHECK POINT STARS PARTNER

Группа компаний АБРИКОС - **партнёр уровня 2 звезды** компании **Check Point Software Technologies Ltd** крупнейшего в мире поставщика в области информационной безопасности. Решения Check Point защищают как мобильные устройства, так и сети крупных организаций, предотвращая кибератаки и обеспечивая защиту от вредоносного ПО.

Обладаем специализацией **SandBlast**, в штате компании есть обученные и сертифицированные инженеры по продуктам SandBlast, SandBlast Agent и технологии Forensics.

CHECK POINT STARS PARTNER

KASPERSKY lab PLATINUM PARTNER

POSITIVE TECHNOLOGIES

Microsoft Silver Partner

vmware PROFESSIONAL SOLUTION PROVIDER

veeam SILVER pro partner

Acronis Authorized Partner

FUJITSU SELECT Expert

Hewlett Packard Enterprise Business Partner

DELL EMC AUTHORIZED PARTNER

lenovo Business Partner

QTECH МИР ДОСТУПНЕЕ

СДЕЛАНО В РОССИИ

HUAWEI Enterprise Partner Authorized

ABRIKOS GROUP

Наши заказчики

PARMATELECOM ITPS GROUP

МОТОВИЛИХА ПАО «МОТОВИЛИХИНСКИЕ ЗАВОДЫ»

ПЕРМСКИЙ МОТОРНЫЙ ЗАВОД

КОМОС ГРУПП

ЭР·ТЕЛЕКОМ

НОВОМЕТ

КЭС ХОЛДИНГ

АГРОПРОМЫШЛЕННЫЙ ХОЛДИНГ

ФП группа

ПЛФА

НЕДРА

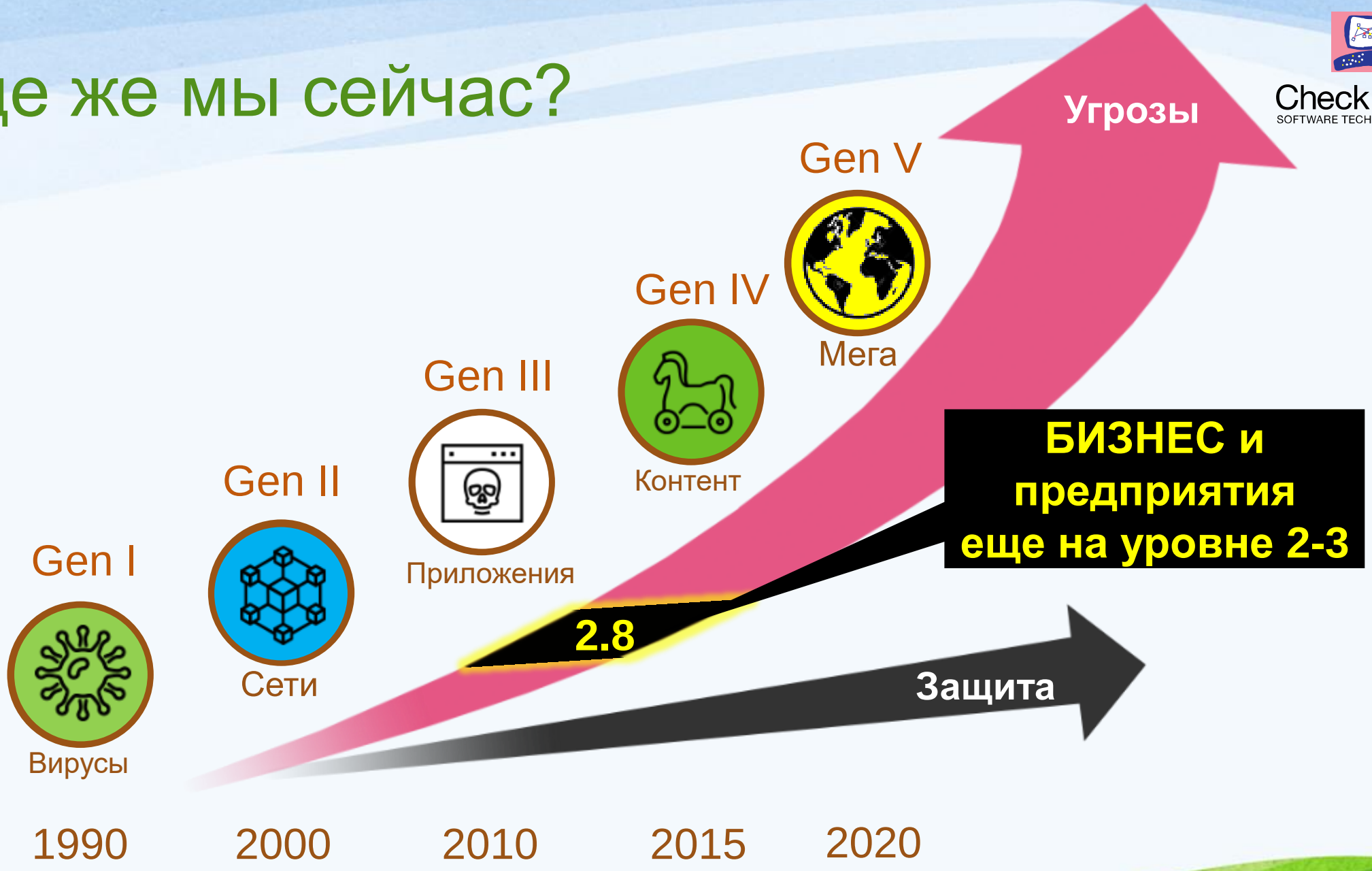
TOYOTA

ЗАКОНОДАТЕЛЬНОЕ СОБРАНИЕ ПЕРМСКОГО КРАЯ

СИБУР

и многие другие предприятия.

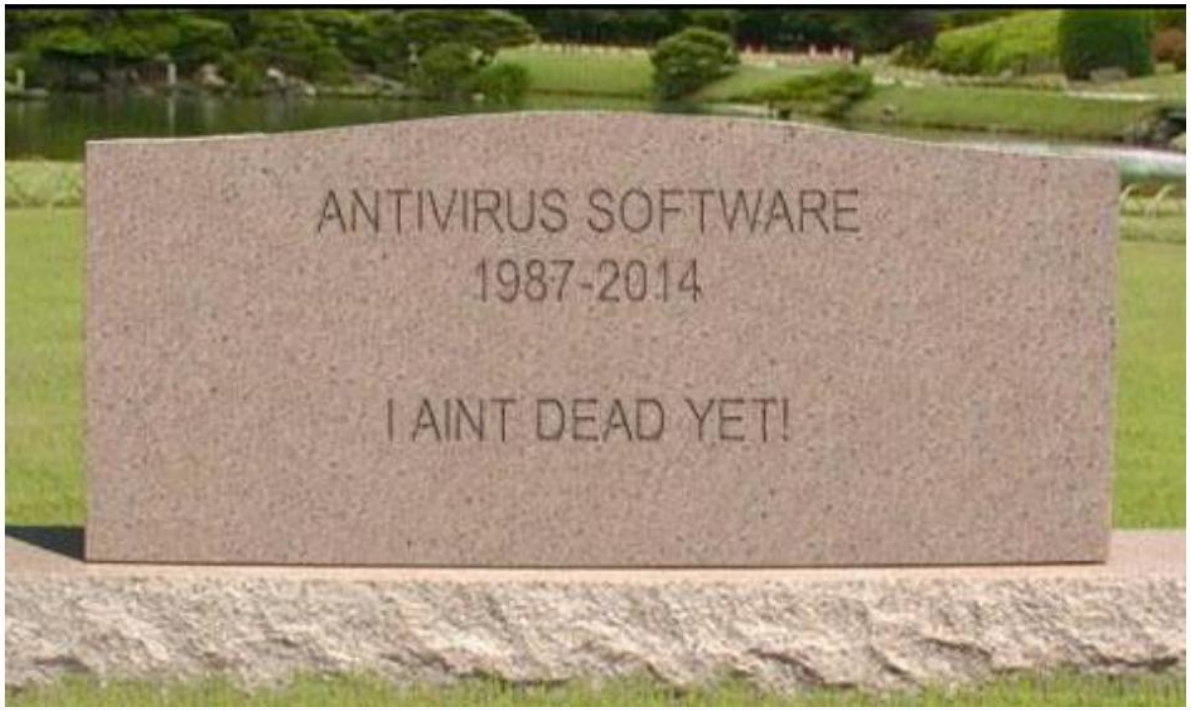
Так где же мы сейчас?



Symantec Says Antivirus Is Dead, World Rolls Eyes

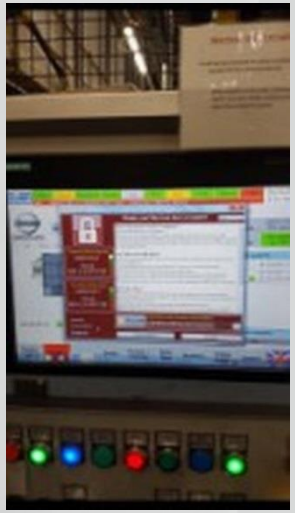
Is AV dead? No. Now it's just not the only weapon in your security arsenal.

By Max Eddy May 7, 2014 11:55AM EST



WannaCry

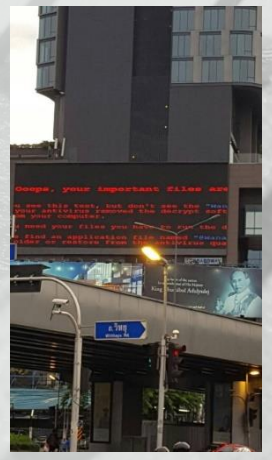
- WannaCry – Зловред-шифровальщик
- В мае 2017 поразил сотни тысяч компьютеров по всей планете



Производственные линии

ЖД Станции

Системы управления



Билборды

Банки

Причин

- Shadow Bro (февраль 2
  - Обнаруже
  - Закрыта М
- Уязвимые С поэтому не
- Использова распростра
  - Другой эко копирован

GitHub - misterch0c/sha

GitHub, Inc. [US] | https://github.com/misterch0c/shadowbroker

https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation

Exploits

- **EARLYSHOVEL** RedHat 7.0 - 7.1 Sendmail 8.11.x exploit
- **EBBISLAND (EBBSHAVE)** root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86.
- **ECHOWRECKER** remote Samba 3.0.x Linux exploit.
- **EASYBEE** appears to be an MDaemon email server vulnerability
- **EASYFUN** EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6
- **EASYPI** is an IBM Lotus Notes exploit that gets detected as Stuxnet
- **EWOKFRENZY** is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2
- **EXPLODINGCAN** is an IIS 6.0 exploit that creates a remote backdoor
- **ETERNALROMANCE** is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)
- **EDUCATEDSCHOLAR** is a SMB exploit (MS09-050)
- **EMERALDTHREAD** is a SMB exploit for Windows XP and Server 2003 (MS10-061)
- **EMPHASISMINE** is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2
- **ENGLISHMANSDENTIST** sets Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users
- **EPICHERO** 0-day exploit (RCE) for Avaya Call Server
- **ERRATICGOPHER** is a SMBv1 exploit targeting Windows XP and Server 2003
- **ETERNALSYNERGY** is a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)
- **ETERNALBLUE** is a SMBv2 exploit for Windows 7 SP1 (MS17-010)
- **ETERNALCHAMPION** is a SMBv1 exploit
- **ESKIMOROLL** is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers
- **ESTEEMAUDIT** is an RDP exploit and backdoor for Windows Server 2003
- **ECLIPSEDWING** is an RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)
- **ETRE** is an exploit for IMail 8.10 to 8.22

Технологии информационной защиты

- **Анти-Вирус**
  - Блокирует **файлы** с **известными** вирусами
- **IPS**
  - Анализирует трафик и блокирует его на основе **известных** шаблонов
- **Анти-Бот**
  - Обнаруживает подозрительный трафик по обновляемым шаблонам

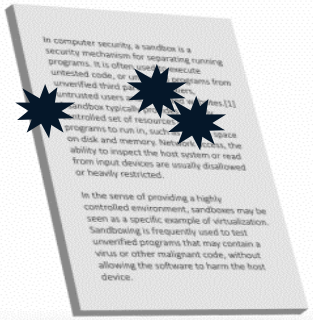
Эффективны, но против ***ИЗВЕСТНЫХ*** *угроз*

СИГНАТУРЫ всегда ОТСТАЮТ, ЧТО ДЕЛАТЬ ?

МЫ ОБЯЗАНЫ ДВИГАТЬСЯ ВПЕРЕД БЫСТРЕЕ!

Эмуляция

Откроем файл в безопасной среде!



Наблюдаем:

- Реестр
- Сетевые соединения
- Действия с файлами
- Действия с процессами

Поведение – вот что выдает зловредное ПО.

Технологии Chek Point SandBlast

CPU-LEVEL

- Human Interaction Simulator
- Network Activity Monitor
- UAC Monitor
- SMEP Detector
- Evasion Detection
- Static Analyzer

PUSH-FORWARD

- FP Guard
- Icon Similarity
- DeepScan
- Virtual Network Service
- Macro Analysis
- Link Scanner

CONTEXT-AWARE

- Image Sanitation
- Dropped File Emulation
- DGA Generator
- Decoys
- Shellcode Detector

Threat Extraction: мгновенная очистка документов

Эмуляция всегда требует времени

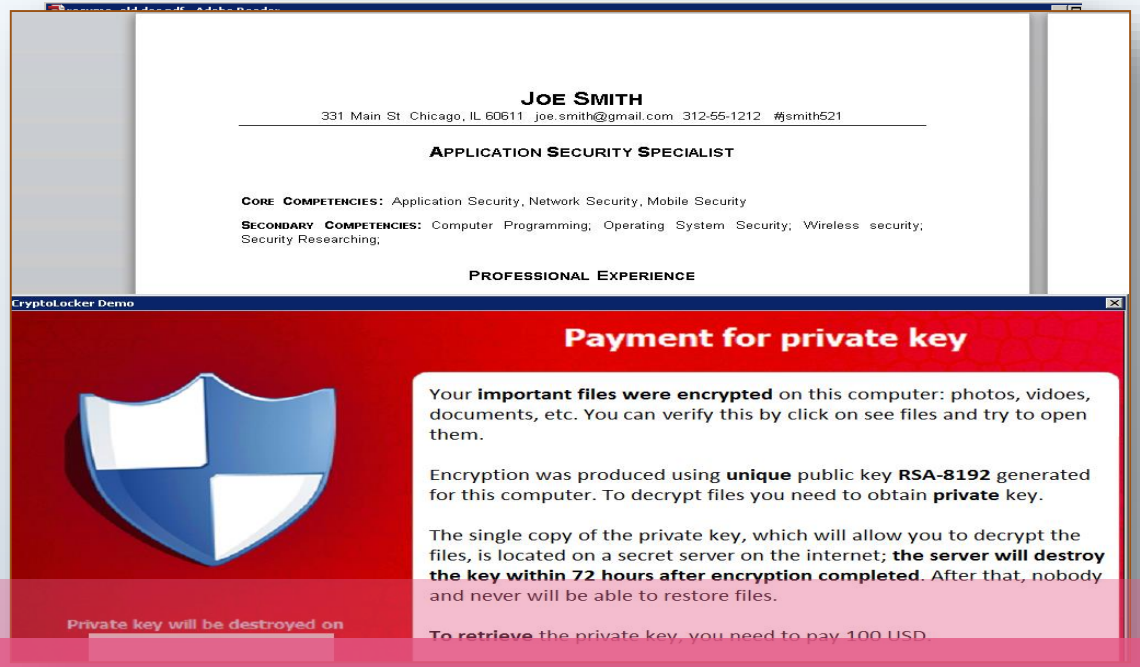
- Поэтому большинство песочниц конкурентов работает в режиме обнаружения, а не предотвращения
- Они пропускают зловред в сеть, тем временем анализируют его в фоновом режиме

SandBlast Threat Extraction

Доставка гарантированно безопасных файлов

ДО

Активация вредоносного ПО



ПОСЛЕ

Вредоносное ПО удалено

Немедленный доступ. Проактивная защита.

Кто-то работает удаленно

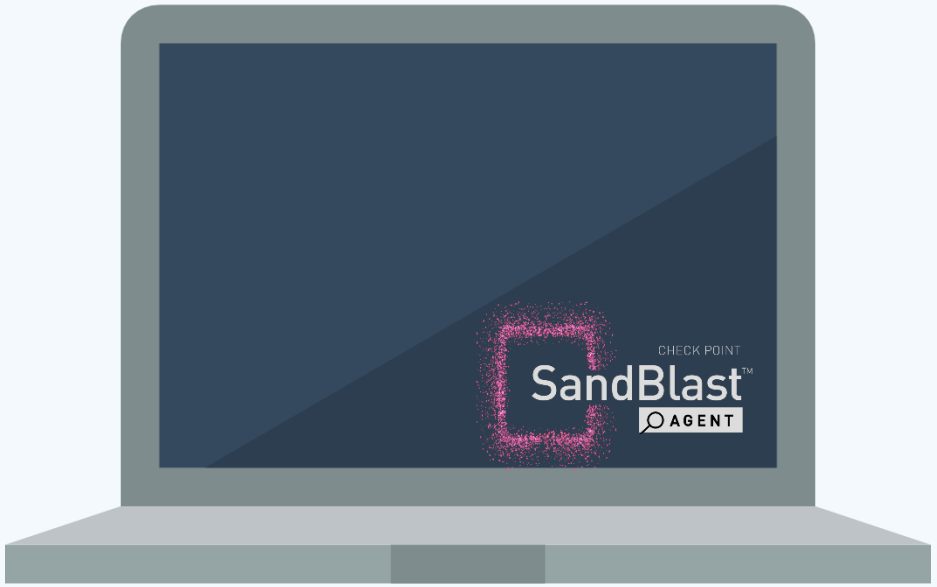
Внешние наколители

Некоторые угрозы можно обнаружить только на рабочей станции

Архивы с паролем, HTTPS

Заражение от другого ПК

Анализ файлов на рабочей станции



SANDBLAST SERVICE

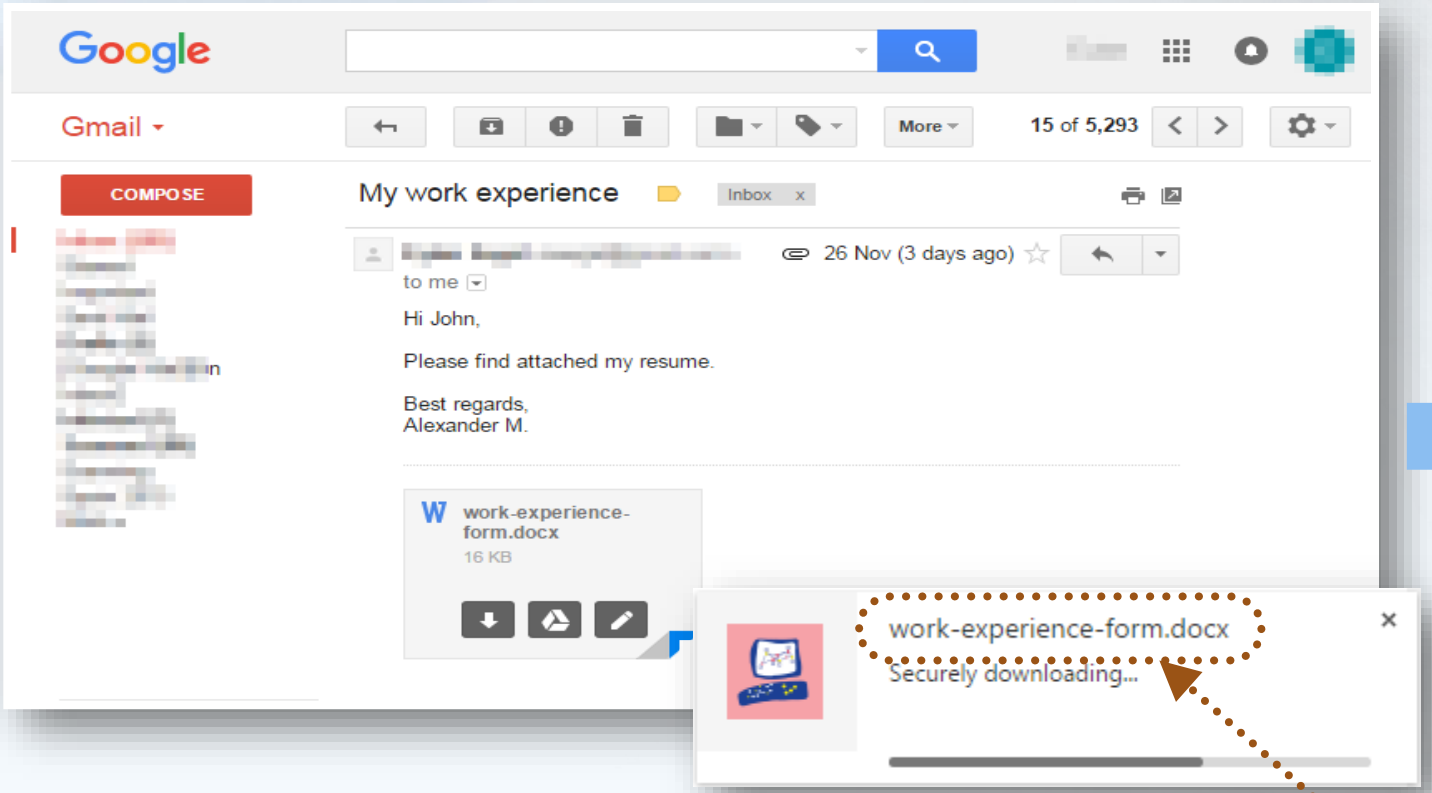
Облако или локально

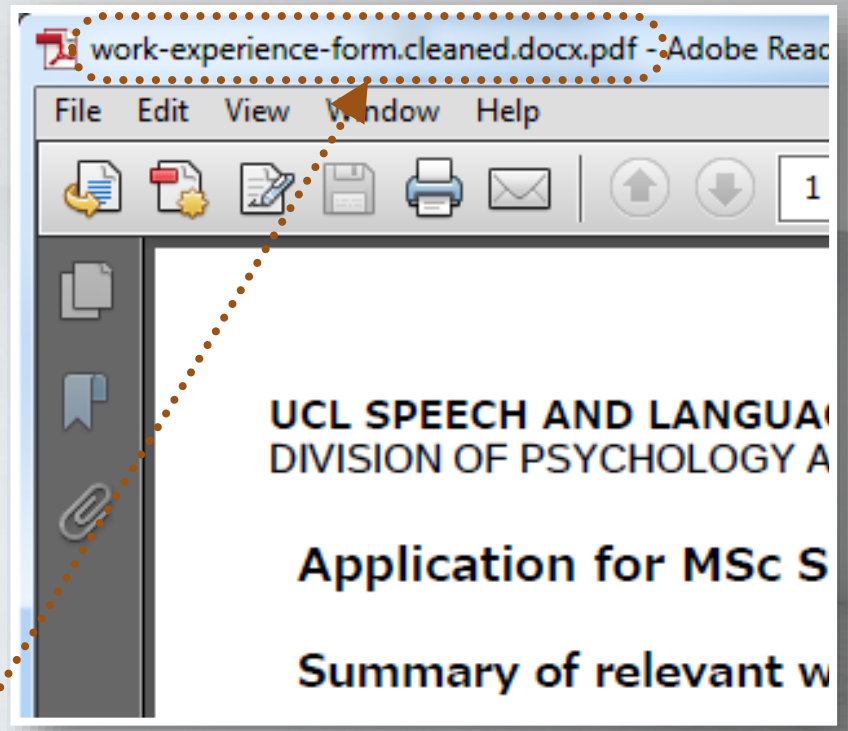
1 Файл отсылается на устройство или облако SandBlast

2 Безопасная копия доставляется мгновенно

3 Оригинал эмулируется

Защита скачиваемых файлов





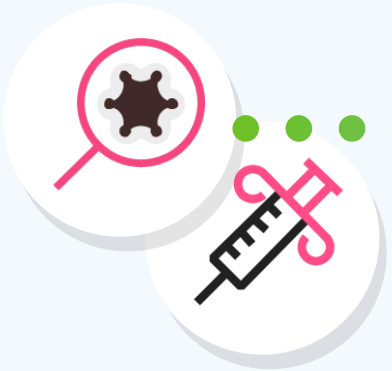
Удаление опасного содержимого и/или конвертация в PDF

Поведенческий анализ и расследование

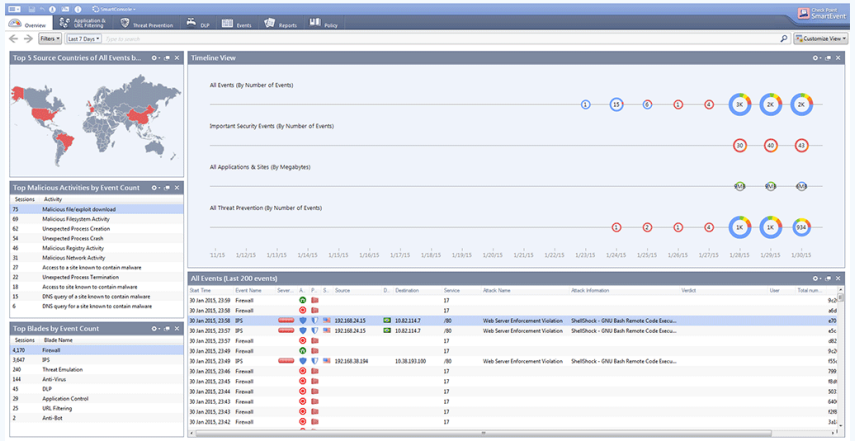
Check Point
SOFTWARE TECHNOLOGIES LTD.

1 **ДАННЫЕ** о системе собираются постоянно от многих источников

2 **ОТЧЕТ** формируется автоматически по срабатыванию локального или внешнего триггера

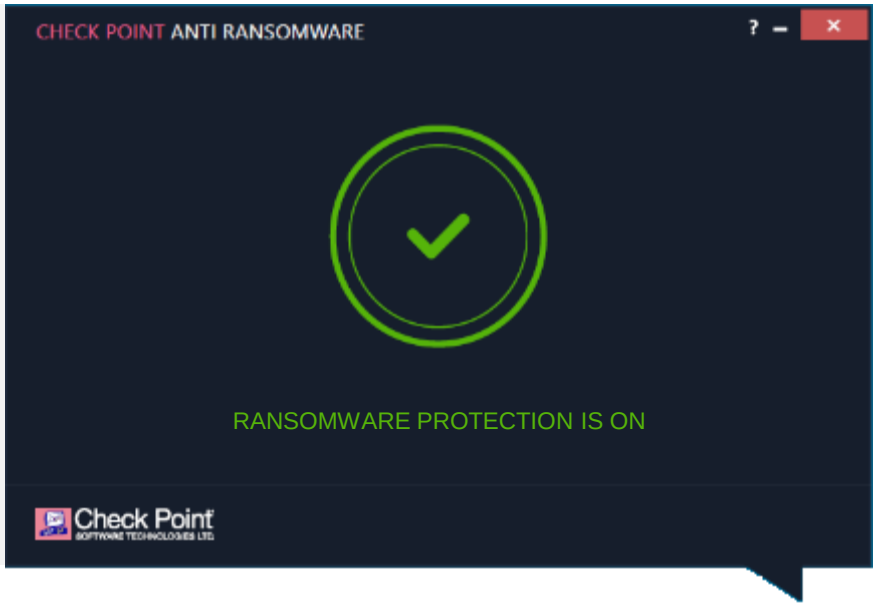


4 **ПОДРОБНЫЙ** отчет формируется на SmartEvent



3 Сырые данные анализируются с помощью сложных алгоритмов

КАК РАБОТАЕТ ANTI-RANSOMWARE



ПОСТОЯННО

АНАЛИЗ ПОВЕДЕНИЯ

Постоянный поиск признаков подозрительной активности

ОБНАРУЖЕНИЕ ШИФРОВАНИЯ

Обнаружение массовой модификации файлов

ВРЕМЕННЫЙ БЕКАП ФАЙЛОВ

Постоянный бекап изменяемых файлов в защищенной области диска

ПОСЛЕ ДЕТЕКТА

КАРАНТИН ЗЛОВРЕДА

Блокировка зловреда, всех его дочерних процессов, расследование активности

ВОССТАНОВЛЕНИЕ ДАННЫХ

Автоматическое устранение последствий и восстановление зашифрованных файлов.

ДЕМО

Check Point SandBlast ZERO-DAY PROTECTION

ПРОДУКТЫ С ТЕХНОЛОГИЕЙ SANDBLAST

NETWORK

- Threat Emulation
- Threat Extraction

AGENT

- Threat Emulation
- Threat Extraction
- Zero Phishing
- Forensics
- Anti-Ransomware

CLOUD

- Threat Emulation
- Threat Extraction

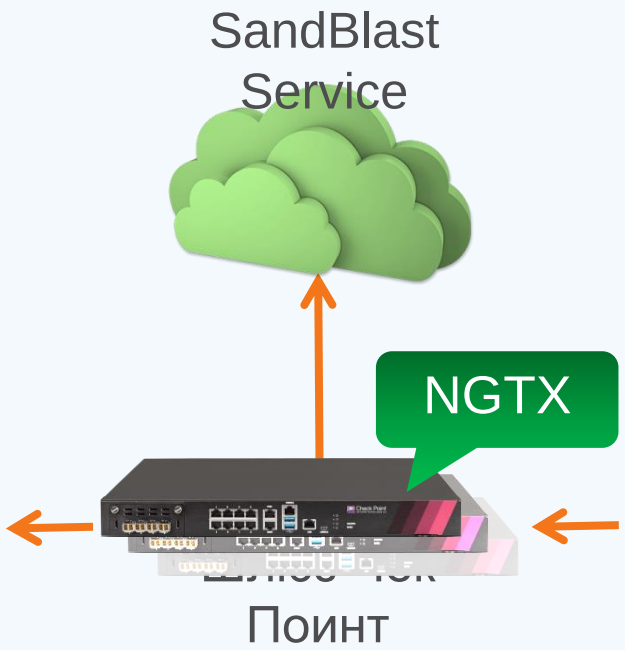
API

- Threat Emulation
- Threat Extraction

©2017 Check Point Software Technologies Ltd.

Варианты развертывания SandBlast

Облачная эмуляция
Шлюз + Сервис SandBlast



Локальная эмуляция
Шлюз + устройство SandBlast

Все в одном
SandBlast сам является шлюзом

Устройство SandBlast:
- Inline
- Span / TAP
- MTA
- ICAP server

Простое правило: NGTX необходим на узле, обрабатывающем трафик для SandBlast

- Шлюз требует NGTX, чтобы использовать SandBlast – при любом способе эмуляции
- В случае использования SandBlast без шлюза, NGTX требуется на само устройство

Лицензирование SandBlast Agent

Features	SandBlast Agent *Complete*	SandBlast Agent NG AV	Endpoint Complete
Deployment	Endpoint Agent	Endpoint Agent	Endpoint Agent
Management	SmartCenter	SmartCenter	SmartCenter
Threat Emulation w/ CPU-level detection	✓	✓	✓
Threat Extraction	✓	✓	✓
Zero Phishing, Credential Protection	✓	✓	✓
Anti-Ransomware, Incident Analysis	✓	✓	✓
Anti-Bot	✓	✓	✓
Automated Forensic Report	✓	✓	✓
Antivirus		✓	✓
Full Disk Encryption, Media Encryption			✓
Firewall, VPN			✓

SBA как часть Endpoint Complete

Check Point
SOFTWARE TECHNOLOGIES LTD.

Endpoint Security

Справка

Обзор

СЕРВИС

Обновить сейчас

Проверить систему сейчас

Отключить от VPN

Дополнительно

Ваш компьютер соответствует политике безопасности организации

Блейд Compliance Применение всех политик. Нет нарушений правил.	Соответствует требованиям
Блейд Anti-Malware Найдены зараженные объекты (14)	Вкл.
Блейд Media Encryption and Port Protection Устройства не обнаружены	Вкл.
Блейды Firewall и Application Control несколько программ (0) и несколько подключений (45795) за...	Вкл.
Блейд Full Disk Encryption Зашифровано 1 устройство.	Зашифровано
Блейд Remote Access VPN Подключено к emea-cp.checkpoint.com	Подключено
Блейд Capsule Docs Блейд Capsule Docs управляется извне	Установлено
Блейд URL Filtering Причина отключения блейда: Отключено политикой конеч...	Выкл.
Блейд Anti-Bot Ведется мониторинг	Вкл.
Блейд Forensics Проанализирован 24 случайв	Вкл.
Блейд эмуляции угроз Найдены зараженные объекты (2)	Вкл.

Подключено к: 192.168.181.137
Версия: E80.70 (80.70.0209)

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
SandBlast
AGENT

Check Point CheckMe – экспресс проверка информационной безопасности (http://www.cpcheckme.com/checkme/)

Сервис CheckMe имитирует различные типы атак, которые могут поставить под угрозу ваш компьютер и информацию о вашей сети. Данный сервис включает в себя серию тестов, которая проверяет ваш компьютер и сеть на уязвимость от вымогателей, фишинга, атак нулевого дня, бот сетей, инъекций кода, использования анонимайзеров и утечки данных.

CheckMe

ARE YOU PROTECTED?

CheckMe runs a series of simulations that test if your existing security technologies can block standard and advanced attacks.

GEN V

CHECK POINT INFINITY

Select Simulation Target(s):

Network	Endpoint	Cloud	Mobile
	*Requires downloading & running an executable	*Requires available infrastructure with internet connectivity	*Requires app download
More	More	More	More

Я не робот

reCAPTCHA

Конфиденциальность - Условия использования

I have read and agreed to Check Point's Terms and Conditions

CHECK SECURITY NOW

КАКИЕ УГРОЗЫ ПРОВЕРЯЮТСЯ?

CheckMe имитирует различные сценарии, которые могли бы стать отправной точкой для следующих векторов атак:

- **ПО для вымогательства** – это вредоносное программное обеспечение, которое шифрует файлы пользователей и требует выкуп за их расшифровку.
- **Кража личных данных/ Фишинговые атаки** – похищение личной информации используя поддельные веб-сайты, которые выглядят как настоящие.
- **Атаки нулевого дня** — использует элемент неожиданности и использует дыру в программном обеспечении, которая неизвестна разработчику.
- **Боты** — выполняют злонамеренные атаки, которые позволяют злоумышленникам получить полный контроль над зараженным компьютером.
- **Атака на браузер** — внедрение вредоносного скрипта на веб-сайты, чтобы украсть cookies жертв с целью выдать себя за жертву.
- **Анонимный веб серфинг** — позволяет пользователям скрывать свою сетевую активность. Он может открывать бреши в сети организации.
- **Утечка данных** — передача секретной или конфиденциальной информации за пределы сети организации путем кражи или случайного воздействия.

CheckMe Instant Security Assessment

CHECKME COMPLETED

GEN V

CHECK POINT INFINITY

9 potential threats were found during the CheckMe assessment

	NETWORK	ENDPOINT
Malware Infection	✗	✓
Command & Control Communication	✗	✗
Zero Day	✗	✗
Browser Exploit	✗	✓
Ransomware	—	✗
Persistent Malware	—	✗
Identity Theft	✗	—
Anonymizer Usage	✗	—
Data Leakage	✗	—

✓ Secure ✗ Vulnerable

GET FULL REPORT

Check Point Security CheckUP

Простой и бесплатный способ проверить безопасность Вашей сети. Получите полноценный отчет, рекомендации по защите, а также аргументированное обоснование необходимости закупки средств защиты.

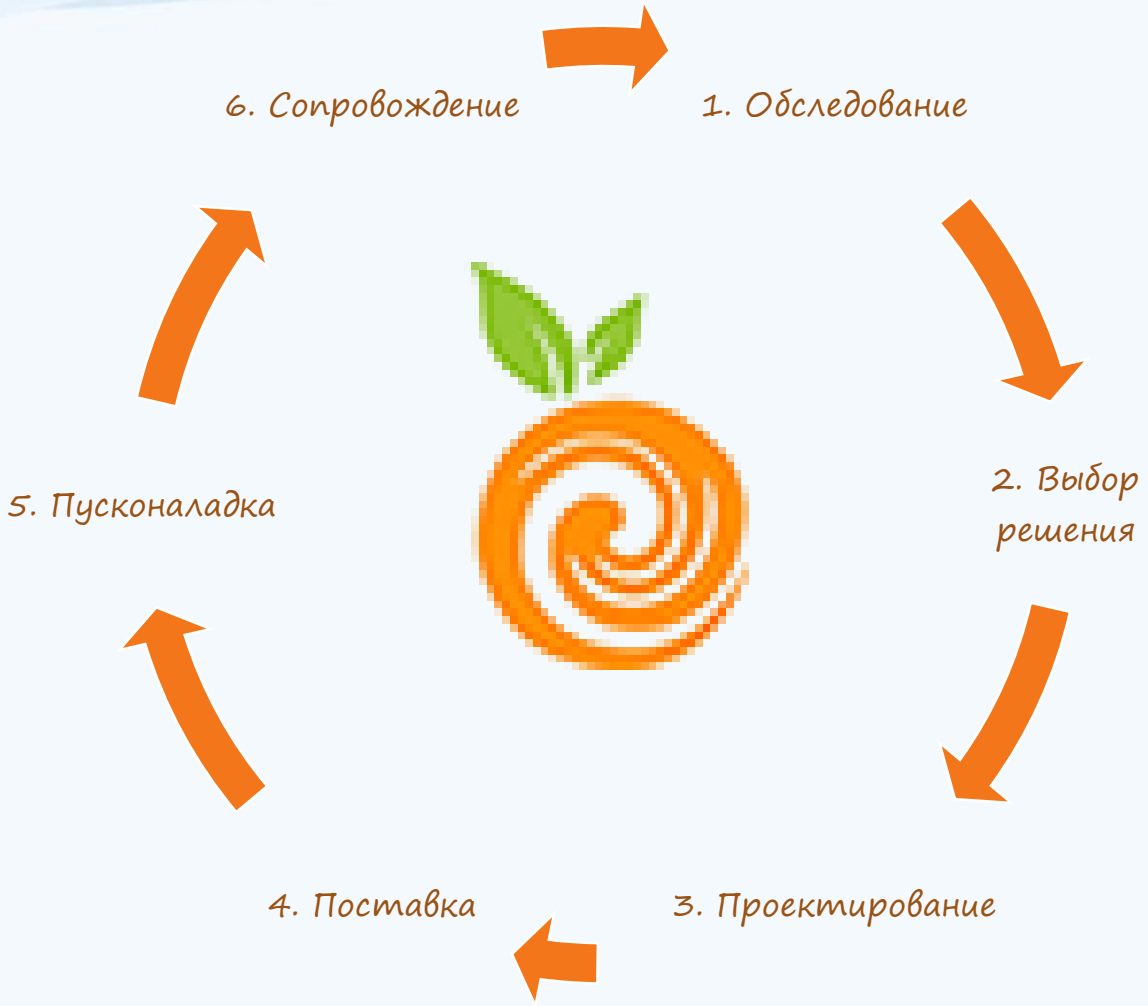
Вы сможете проверить:

- Посещение ресурсов. Какие ресурсы посещают Ваши пользователи (Анонимайзеры, фишинговые сайты и т. д.)
- Использование приложений. Какие приложения используют (Torrent, программы удаленного управления, VPN и т.д.)
- Загруженность интернет-каналов. Чем забит интернет-канал
- Проверка на вирусы. Нет ли инфицированных компьютеров в сети
- Загрузка вредоносного ПО «нулевого дня»
- Утечка данных. Upload в облако из корпоративной сети

Демо-оборудование

- Шлюз безопасности Check Point модели 5200 Next Generation Appliance

- Песочница Check Point модели TE100X SandBlast Appliance


1. Обследование
2. Выбор решения
3. Проектирование
4. Поставка
5. Пусконаладка
6. Сопровождение

ABRIKOS GROUP

НАШЕ КРЕДО

Индивидуальный подход к каждому клиенту. А предложения по внедрению и сопровождению бизнес-решений всегда соответствуют требованиям Вашего бизнеса.

Сергей Боровиков
Технический директор
sb@abrikos-group.ru