

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

# На шаг впереди: Как прекратить рассуждать об обнаружении новых угроз и начать их предотвращать?

**network, endpoint, mobile, cloud**

Алексей Белоглазов  
Руководитель группы инженеров ИБ  
[abeloglazov@checkpoint.com](mailto:abeloglazov@checkpoint.com)  
**+79856478564**





# WannaCry: масштаб бедствия MalwareTech (kill-switch domain sinkhole)

<https://intel.malwaretech.com/botnet/wcrypt/>

152,460  
ONLINE

302,985  
OFFLINE

455,445  
TOTAL

Infection Map (age: 0h 32m 40s)

Oops, your files have been encrypted!

What Happened to My Computer?  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send \$600 worth of bitcoin to this address:  
13AM4VW2dxxYgXeQepoHkHSQuy6NgaEb94

Check Payment Decrypt

интерфакс  
INTERFAX

В России В мире Экономика Спорт Культура Москва Все новости

В РОССИИ → АТАКИ ВИРУСА-ВЫМОГАТЕЛЯ WANNACRY 13:05, 16 мая 2017

**Заражению WannaCry в МВД подверглись только персональные компьютеры сотрудников**

СБЕРБАНК  
Все файлы зашифрованы

## WannaCry 2.0: no kill-switch!

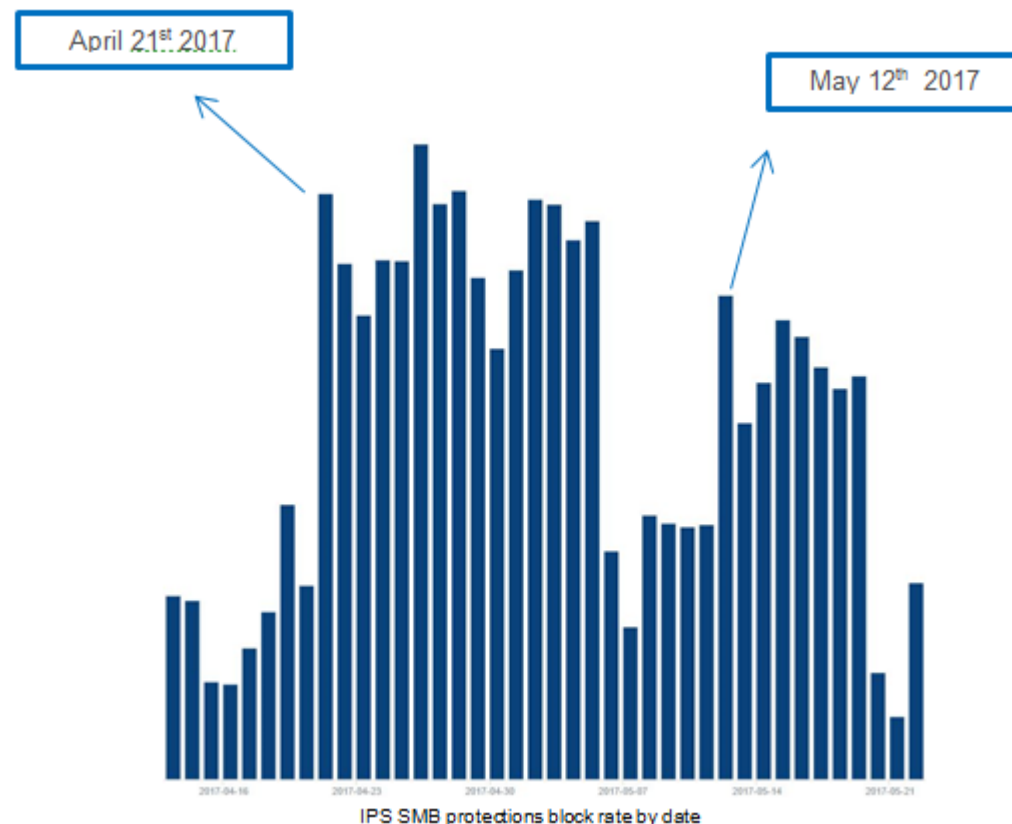
<http://blog.checkpoint.com/2017/05/15/wannacry-new-kill-switch-new-sinkhole/>

# Пример: векторы атаки WannaCry



Check Point  
SOFTWARE TECHNOLOGIES LTD.

1. Червь WannaCryPTOR использует разработки АНБ (утечка через Shadow Brokers):
  - Поиск уязвимых хостов: SMBTouch, ArchiTouch
  - Эксплойты для SMB MS17-10: EternalBlue, EternalChampion, EternalSynergy, EternalRomance
  - Бэкдор: DoublePulsar
2. Фишинговая рассылка:
  - Ссылки в теле письма и документах PDF
  - Архивы ZIP с паролем с PDF
3. Атаки brute-force login на RDP-серверы и установка на них Ransomware



<http://blog.checkpoint.com/2017/05/12/global-outbreak-wanacrypto/>

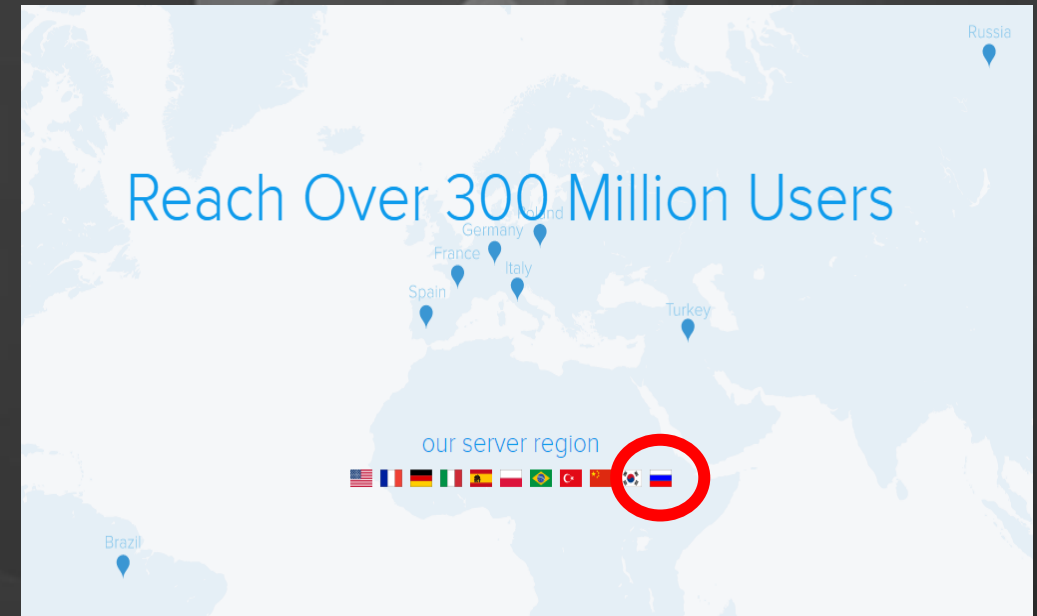
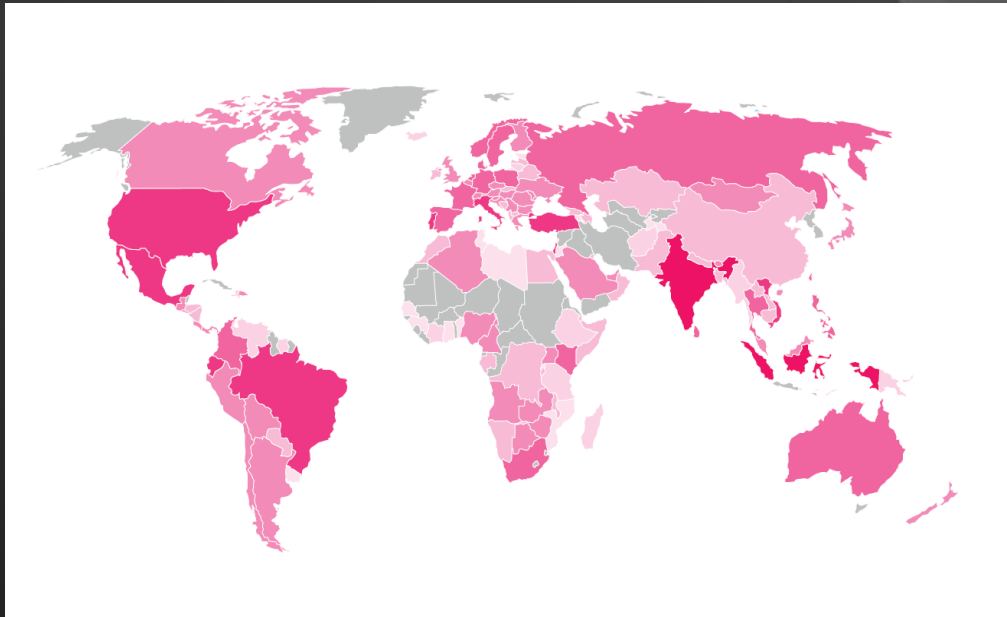
<http://blog.checkpoint.com/2017/05/25/brokers-shadows-analyzing-vulnerabilities-attacks-spawned-leaked-nsa-hacking-tools/>



# FIREBALL – новый китайский вредонос под управлением Rafotech marketing agency (Beijing) 250 млн. зараженных по веб!

Browser hijacking через Wi-Fi / бесплатное ПО

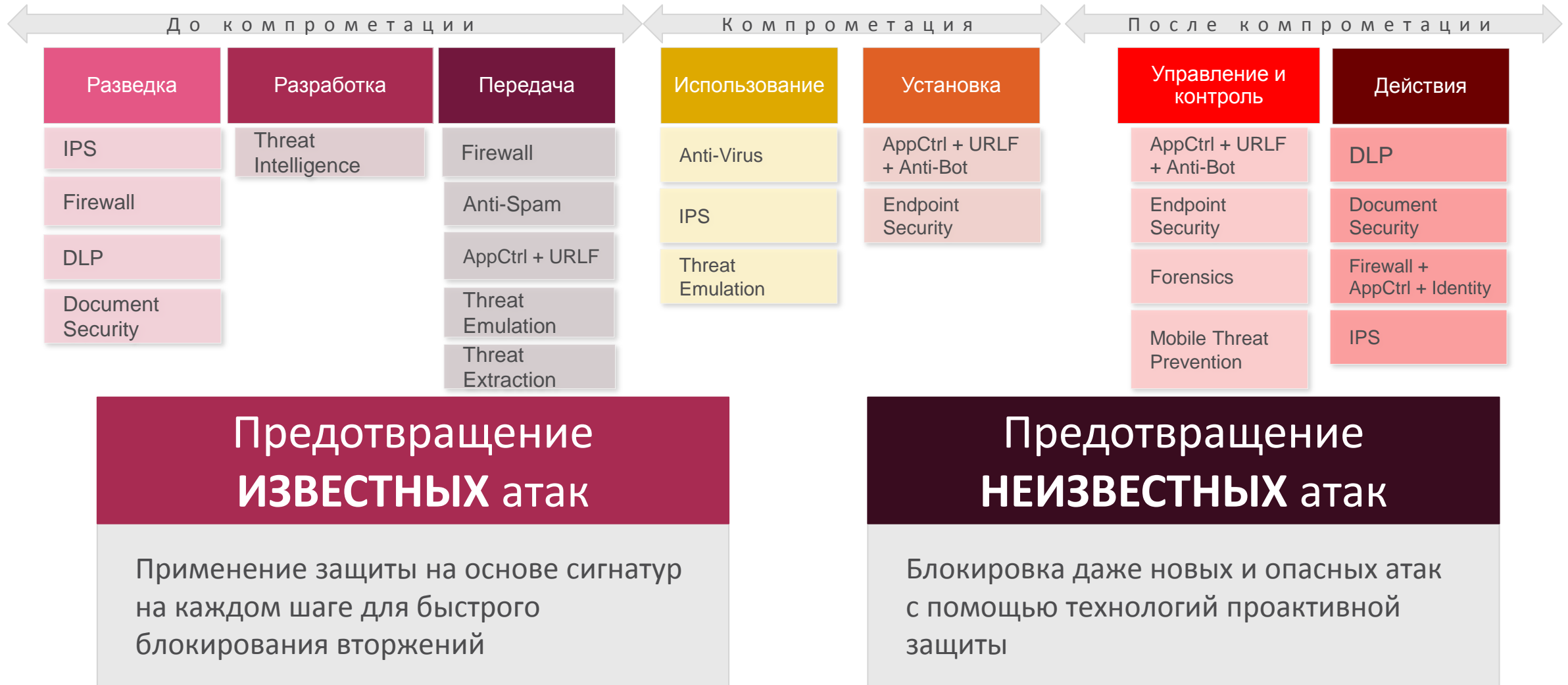
- Фальшивый поисковик с редиректами на настоящие
- Кража данных пользователя, докачивание вредоносного ПО



# УСПЕШНАЯ СТРАТЕГИЯ ЗАЩИТЫ на всех этапах атаки для каждого вектора



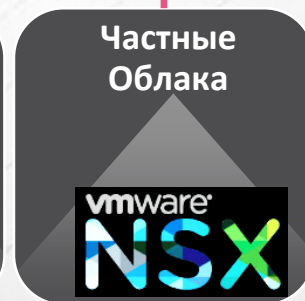
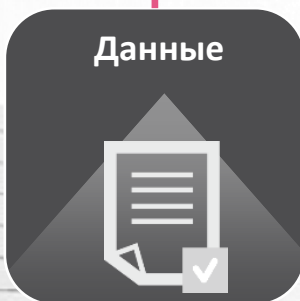
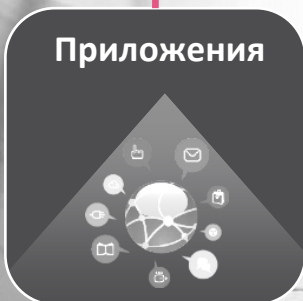
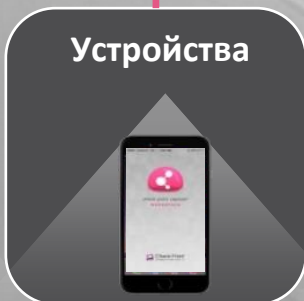
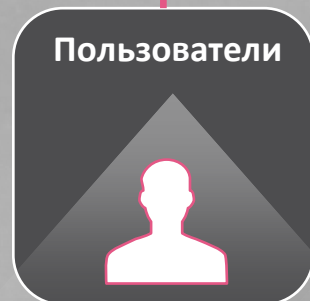
Check Point  
SOFTWARE TECHNOLOGIES LTD.





# R80.10: единая политика контроля доступа

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	* Any	* Any	AccessSubLayer	* Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	* Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800 CapsuleCloud
Access Sensitive Servers	* Any	* Any	* Any	* Any	SensitiveServers	* Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	* Any	Accept	Mobile
Access to Web Server	* Any	WebServer	https	* Any	Accept	AWS VMWare



# Сокращение площади атаки



Check Point  
SOFTWARE TECHNOLOGIES LTD.

- 1) Next-Gen Firewall для сегментации и микросегментации, SDN (vSEC)
- 2) Строгая политика доступа на уровне приложений и групп пользователей
- 3) Расшифрование вх. и исх. SSL с исключениями по категориям
- 4) Предотвращение атак IPS без риска для доступности сервисов

Overview

IPS provides protection from network, application and web attacks.

**IPS in My Organization**

20 Security Gateways are enforcing IPS

2 profiles are configured

Profile	IPS Mode	Activation	Gateways
Default_Protection	Prevent	IPS Poli...	16 GWs
Recommended_Pr...	Prevent	IPS Poli...	4 GWs

Profile Properties - Recommended\_Protection

**Updates Policy**

The IPS Mode is set to Prevent.

Newly downloaded protections will be set to

# Сокращение площади атаки



Check Point  
SOFTWARE TECHNOLOGIES LTD.

5) Блокировка опасного контента (exe, wsf, ...) по формату и способу доставки

Protected Scope	Protection/Site/File/Indicator	Action
SMTPServer	n/a	Recommended Profile
<ul style="list-style-type: none"><li>Anti-Bot Prevent</li><li>Anti-Virus Prevent</li><li>Threat Emulation Prevent</li><li>Threat Extraction Convert To PDF</li></ul>		

File Types Configuration

Specific file types families actions:

Type to Search

Type	Description	Action
msi	Windows Installer file	Block
vb,vbe,vbs	Visual Basic script	Block
jar	Java archive	Block
pif	Windows program info...	Block
cmd	Windows command file	Block
ws,wsc,wsf	Windows script file	Block
js,jse	JavaScript	Block
hta	HTML application	Block
adp,ado	Access project	Inspect
bas	BASIC source code	Inspect
crt	Certificate file	Inspect
inf	Information or Setup file	Inspect
ins,jsp	IIS settings	Inspect
mdb,mde	Access database	Inspect
xsl	XML stylesheet	Inspect

6) Анализ zip, rar, 7zip,...

Блокировка асе, arj, bz2, lzh,...

Fail-close для архивов с паролем

Archive Scanning Configuration

Stop processing archive after 30 seconds.

When maximum time is exceeded Block file.

OK Cancel



# Zero Day Prevention vs. Detection



Большинство «песочниц» выборочно предотвращают в электронной почте и только детектируют в веб.

Они сообщают Вам плохие новости, **когда уже слишком поздно,** и создают много работы.

Сигнатура через X минут – это здорово, но уже не для Вас...

# Обычную песочницу не так сложно обойти

Запуск по таймеру

Ускорение  
таймера

Зловред  
использует  
собственный  
таймер

...

Обнаружение песочницы

Песочница  
эмулирует CPU

Обнаружение  
эмуляции CPU

...

Ожидание действия  
человека

Имитация кликов,  
движения мышки

Обнаружение  
аномалий  
поведения

...

# Эмуляция в SandBlast всегда на шаг впереди



CHECK POINT

## SandBlast<sup>™</sup>

ZERO-DAY  
PROTECTION

CPU Detection Engine

*ДО того, как запустится код обхода...*

*ДО загрузки зловреда....*

Обычная песочница



# Семейство ТЕХНОЛОГИЙ для защиты от таргетированных атак

## THREAT EMULATION

Среда эмуляции  
(Уровни ЦП и ОС),  
устойчивая к  
методикам обхода

## THREAT EXTRACTION

Проактивное  
удаление опасного  
контента при  
доставке

## ENDPOINT FORENSICS

Быстрое понимание  
ситуации  
для лучшей защиты  
и исправления

## ZERO PHISHING

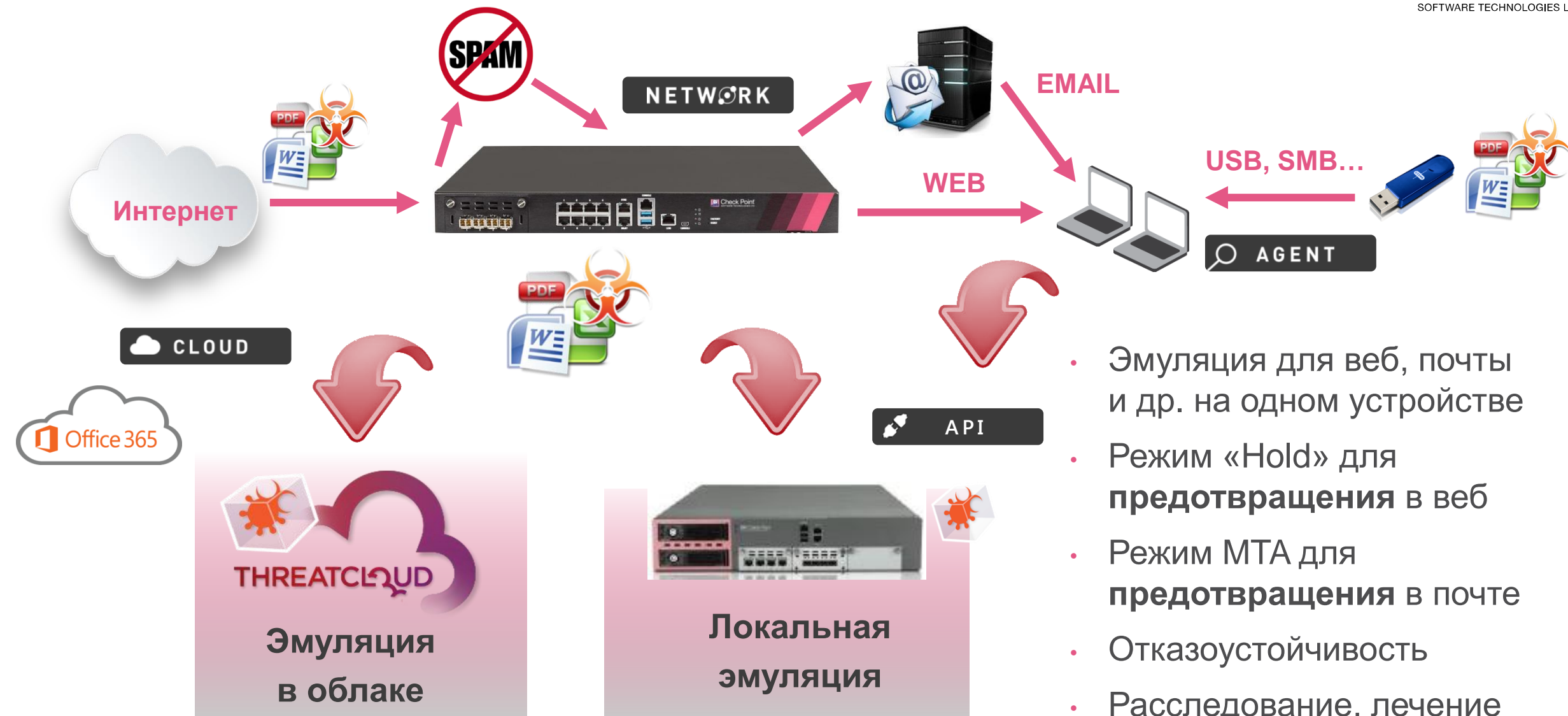
Защита учетных  
записей от кражи  
через фишинговые  
сайты

## ZERO RANSOMWARE

Идентификация и  
восстановление  
после действий  
программы-  
вымогателя



# Предотвращение Zero Day с Check Point

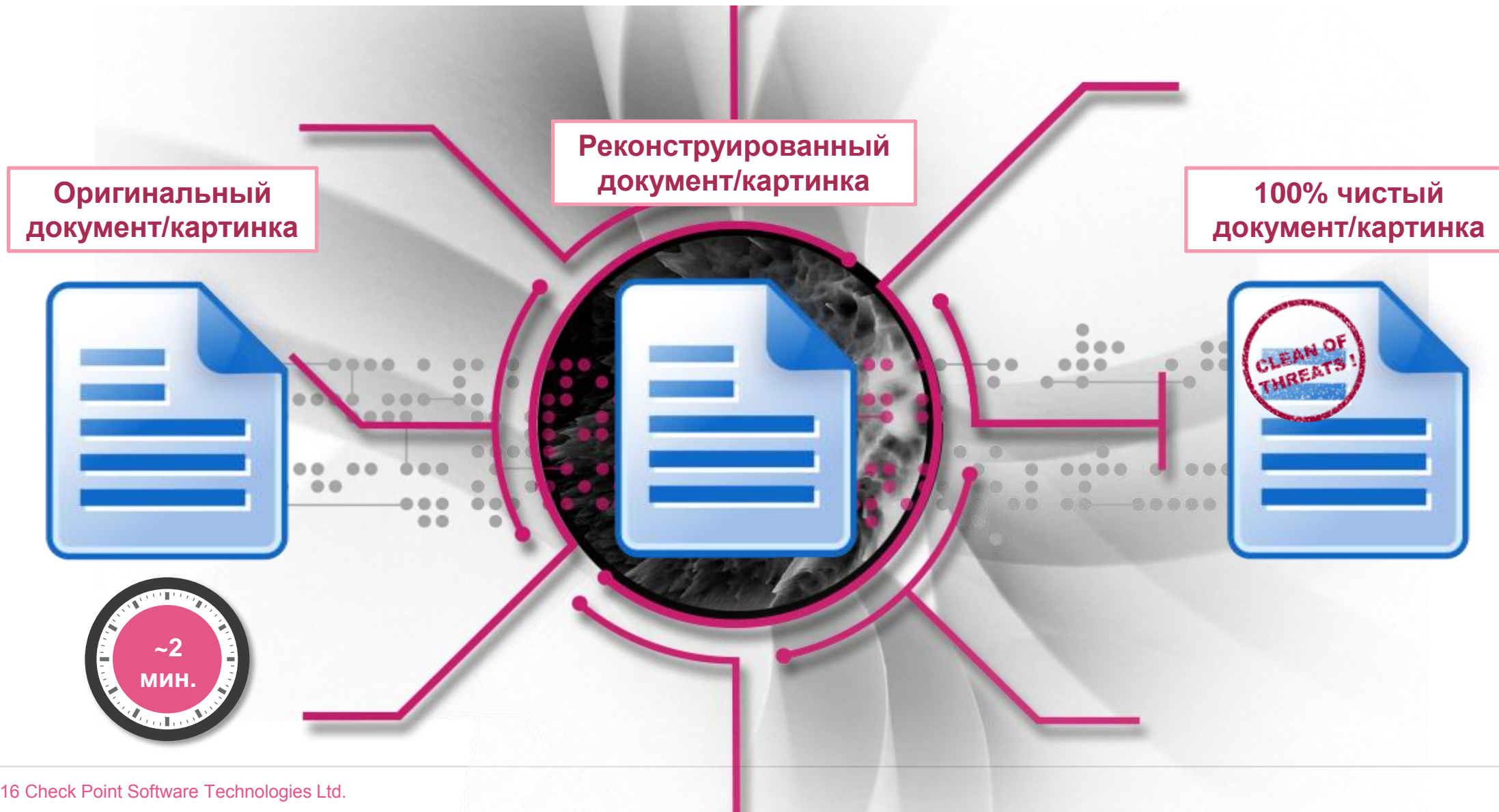





# Sandblast Threat Extraction



Доставка гарантированно безопасных документов и изображений



# Защита конечных точек от Check Point

 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 случай

Вкл.


Блейд эмуляции угроз

Найдены зараженные объекты (2)


Вкл.

Подключено к: 192.168.181.137

Версия: E80.70 (80.70.0209)

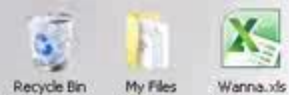


- Универсальный агент
- Модульная архитектура
- Замена AV или
- Совместимость и интеграция с AV
- Защита от APT



©2016 Check Point Software Technologies Ltd.

15



This PC is protected by SandBlast Anti-Ransomware



# Песочница, AV, AB, AR, IoC → Отчет Forensics

SandBlast Agent  
Forensic Analysis

CLEANED

User Name:  
Computer:  
Incident ID:

Entry Point

Accessed [172.217.16.163] in ch

Remediation (32 files)

REPUTATION | FILE NAME

★ @wanadecryptor@.exe

★ @wanadecryptor@.exe

★ @wanadecryptor@.exe

★ @wanadecryptor@.exe

★ @wanadecryptor@.exe

25 more...

Suspicious Activity (1)

SEVERITY | EVENT CATEGORY

Shadow Copy Delet

Tor Communication

Tor Application Dov

File Access Control

Privilege Change (3

Script Execution (1

Dropped File Deleti

8 more...

Business Impact (2 categories, 242 events)

xxxxxxx: wcry\_full\_attack\_analysis1494615803475

These are potentially important

Data Ransom (241 files)

This is a list of user files that

Show 25 ent

Status	File Name
↺	2014-financi
↺	g-example-d
↺	g-finance-ma
↺	g-finance-sta
↺	g-procureme
↺	g-sample-jds
↺	g_budget-worksheet-example.xls
↺	g_cash-flow-forecast.xls

Remediation Details

xxxxxxx: wcry\_full\_attack\_analysis1494615803475

This screen describes all the remediation actions that were taken automatically.

Quarantined Incident Files (3 quarantined)

These are potentially malicious files that have been quarantined.

Reputation	File Name	File Path
★	@wanadecryptor@.exe	c:\users\xxxxxxx\downloads\@wanadecryptor@.exe
★	taskdl.exe	c:\users\xxxxxxx\downloads\taskdl.exe
★	wcry.exe	c:\users\xxxxxxx\downloads\wcry.exe

Terminated Incident Processes (26 terminated)

Remediation Disabled in Policy: Incident Files (3 files)

ssadmin.exe 1676

Low Copy Deletion

wmic.exe 1580

Low Copy Deletion

Decryptor@.exe vs

PID: 2928

Duration: 94ms

Created By PID:

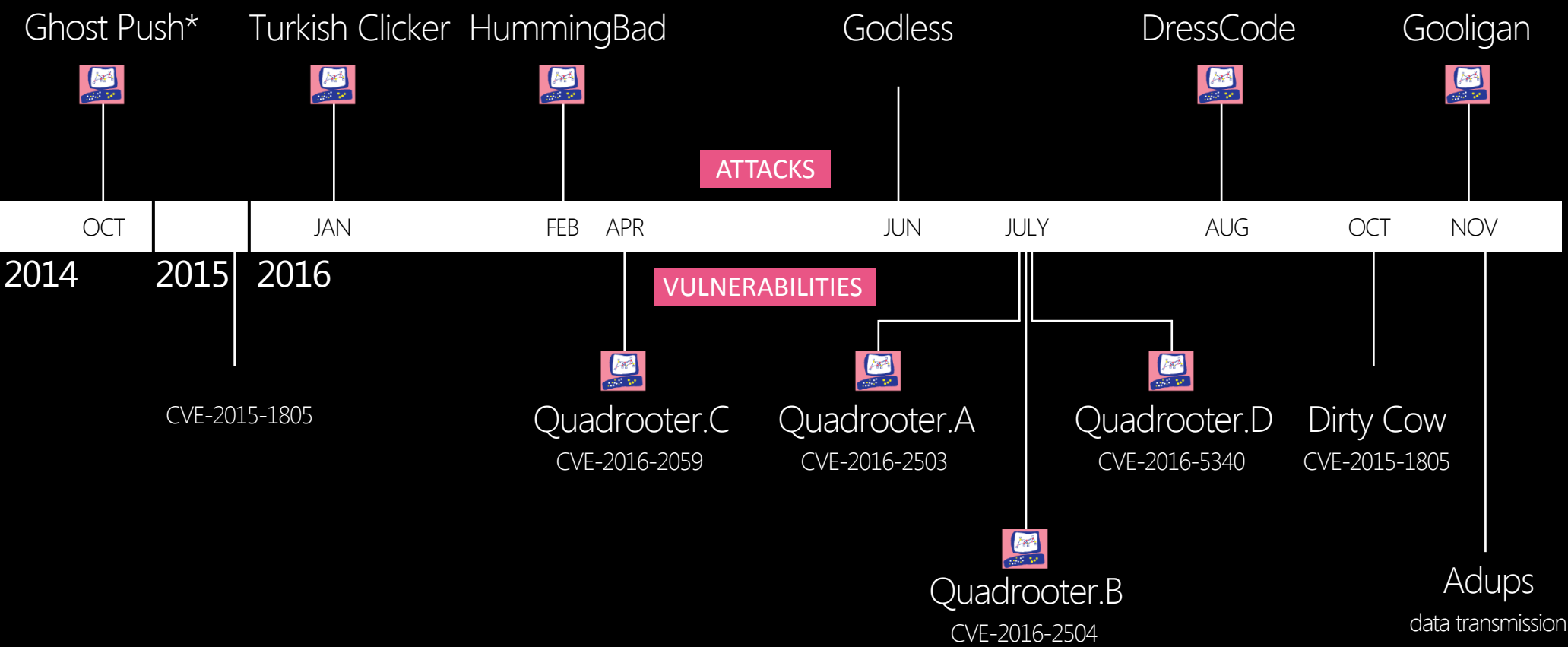
Вылечи

уализация событий



# GOOGLE ANDROID SECURITY 2016 REPORT:

## CHECK POINT ПЕРВЫМ ОБНАРУЖИЛ 70% НОВЫХ УГРОЗ

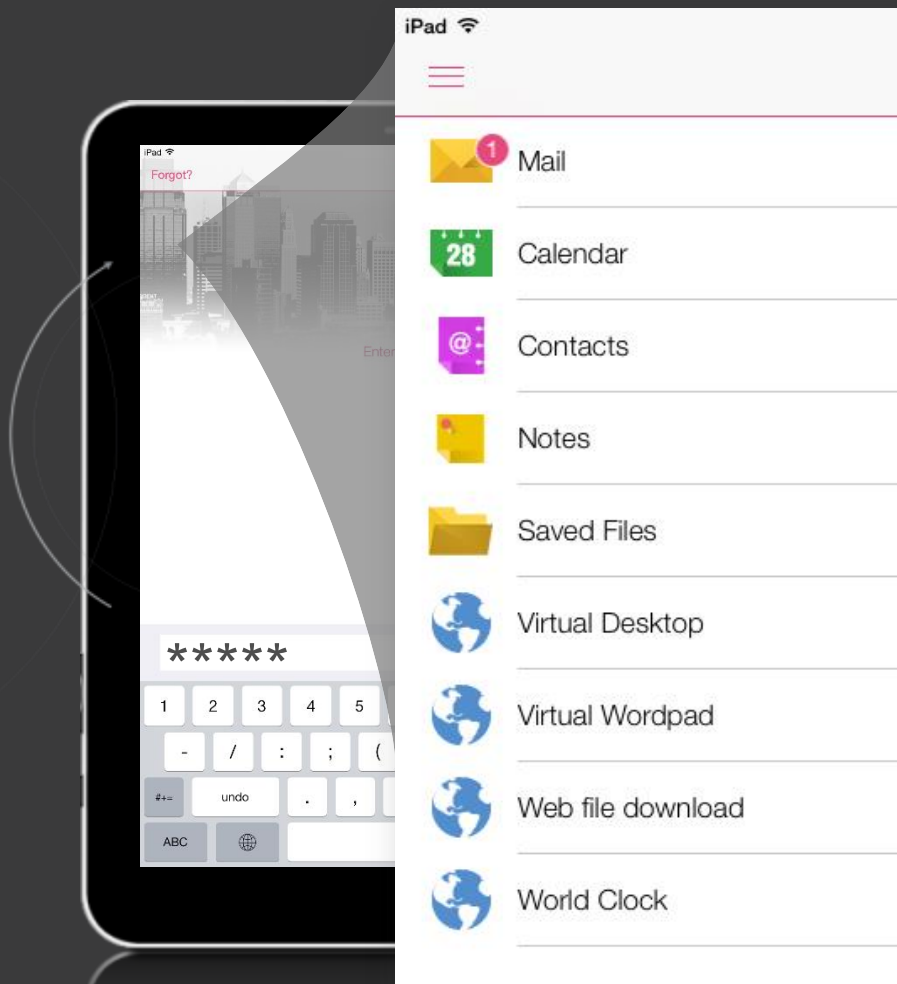


= DISCOVERED BY CHECK POINT

\*Partially Check Point : BrainTest, Sept 2015



# Check Point Capsule: защищенная бизнес-среда



**ЗАЩИЩЕННЫЙ** вход (PIN, Touch-ID)

**ПРОСТОЙ ДОСТУП**  
к опубликованным бизнес приложениям

**ПЕРЕДАЙТЕ** под IT контроль  
**ТОЛЬКО** бизнес информацию (BYOD)

Корпоративные данные защищены **ВЕЗДЕ**



Тест 2017:  
100%



Check Point  
SOFTWARE TECHNOLOGIES LTD.



Check Point  
SOFTWARE TECHNOLOGIES LTD.

# SandBlast Mobile

## ПОВЕДЕНЧЕСКИЙ АНАЛИЗ УГРОЗ

**ЗАЩИТА ОТ  
SMS-ФИШИНГА  
(ПРОВЕРКА ССЫЛОК)**

**СТАТИЧЕСКИЙ И ДИНАМИЧЕСКИЙ  
АНАЛИЗ В ПЕСОЧНИЦЕ ДЛЯ  
ВЫЯВЛЕНИЯ ИЗВЕСТНЫХ И  
НЕИЗВЕСТНЫХ УГРОЗ**



**СЕТЕВАЯ ЗАЩИТА,  
MITM, SS7**

**ЗАЩИТА ОТ УЯЗВИМОСТЕЙ  
НА УРОВНЕ УСТРОЙСТВА  
(ОС)**



<http://blog.checkpoint.com/2017/02/09/smishing-threat-unraveling-details-attack/>

<http://pages.checkpoint.com/miercom-report-on-sandblast-mobile.html>