Check Point
SOFTWARE TECHNOLOGIES LTD.

СОВРЕМЕННЫЙ ВЗГЛЯД НА ЗАЩИТУ ОТ УГРОЗ НУЛЕВОГО ДНЯ

Дмитрий Воронков
Security Consultant Team Lead
dvoronkov@checkpoint.com

Кто стоит за атаками?

УТЕЧКА ТЕХНОЛОГИЙ
e.g. The Shadow Brokers

ИГРОКИ	КРИМИНАЛ	ГОСУДАРСТВА
ЦЕЛИ	ПОЛЬЗОВАТЕЛИ И КОМПАНИИ Массовые заражения	ИНФРАСТРУКТУРА, КОРПОРАЦИИ, C-LEVEL МЕНЕДЖЕРЫ Целенаправленные атаки
МОТИВАЦИЯ	ДЕНЬГИ	ДИВЕРСИИ, ШПИОНАЖ, КИБЕР-ТЕРРОРИЗМ
УГРОЗЫ	ОБЫЧНЫЕ	ZERO-DAY
СЛОЖНОСТЬ	СРЕДНЯЯ	ВЫСОКАЯ, КИБЕР-ОРУЖИЕ
ИНВЕСТИЦИИ	НЕБОЛЬШИЕ	НАЦИОНАЛЬНЫЙ БЮДЖЕТ
ПРИМЕРЫ	АТАКА НА SAN FRANCISCO MTA, НОЯБРЬ 2016	АТАКА НА ЭЛЕКТРОСТАНЦИИ, ДЕКАБРЬ 2015 STUXNET

ПОНЯТНЫ И ОТРАБОТАНЫ БИЗНЕС-МОДЕЛИ

WORMS

KEYLOGGERS

BANKING TROJANS

BOTNETS

Шифровальщики и другое вымогательство

Кража денег со счета

Майнинг

Шпионаж

Отказ в обслуживании

Манипуляция с ценами акций

Сервис...

Функции	BUSINESS	SUPPORT
Шифрование бекапов	Аффилиатные программы	24X7 многоязычная поддержка
Поддержка новых платформ	Ransomware as a Service	Система обработки заявок
Блокирование IoT	Удобные платежи	
	Скидки и акции	

Social Engineering skills:
- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt belive really often.
- Alot of experience with security practices inside big corporations.

What ill do:
Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone
Ruining your opponents, bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.087 ฿	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR = 0.217 ฿	1 X Buy now
Large job which takes a few days or multiple jobs	800 EUR = 0.347 ฿	1 X Buy now

Что делать?

Как защищаться?

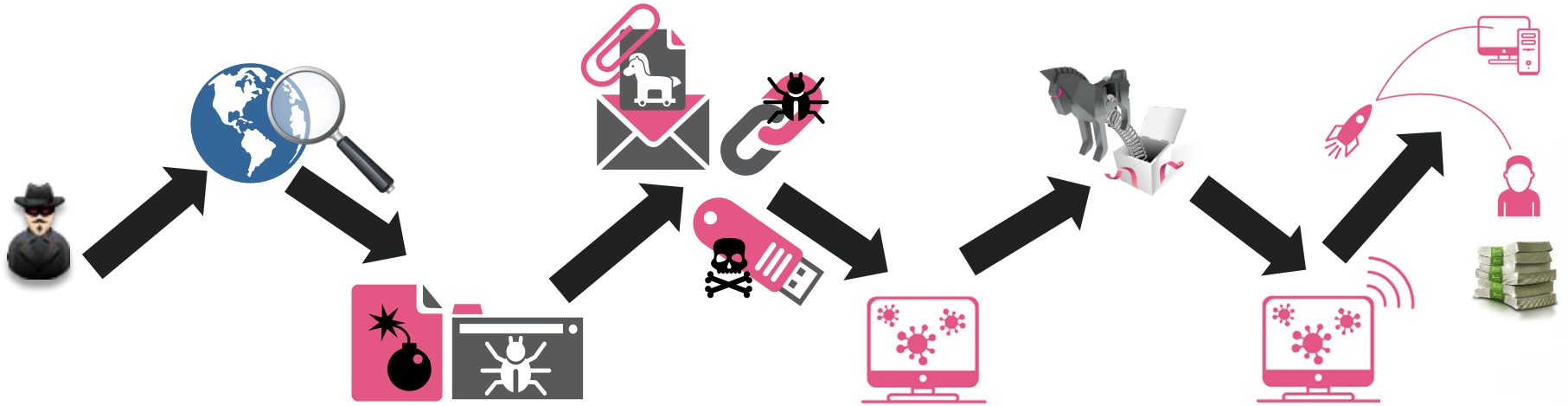
Популярные подходы к защите

- Использование сенсоров в сети
  - Перегрузка персонала
  - Слишком поздно
  - Параллельные маскирующие атаки
- Сканеры на уязвимости
  - 0-day никто не отменял
  - Атака может строиться и без использования уязвимостей
- Несколько разных регулярно обновляемых антивирусов
- «Нам нечего защищать»
  - Конфиденциальные данные все равно есть
  - Использование мощностей компьютеров и серверов

Не помогло...

- Банк в Восточной Европе
  - постепенно защищались от 0-day угроз
  - на момент атаки только часть банкоматов были защищены
  - блокирована работа всего, кроме основного процессинга платежей и защищенных банкоматов
- Группа компаний (металлургия)
  - защищали только рабочие станции (разными решениями)
  - зашифровались тысячи компьютеров
  - машины под защитой SBA (CP EndPoint) не пострадали
- Сеть клиник (республика бывшего СССР)

Продвинутые технологии защиты на каждом этапе атаки



Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

No.	Name	Source	Destination	Services & Applications	Content	Action
Access To Internet (5)						
5	Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Web Control
5.1	DNS server should have access to	DNS Server	ExternalZone	domain-udp-Protoc... domain-tcp-Protoc...	Any	Accept
5.2	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Inappropriate Sites Anonymizer	Any	Drop Blocked Messa...
5.3	HR can acc... network ap...					Inform Access Approval

All | dnscat2

DNSCAT2

DNSCAT2

Primary Category: **Anonymizer** Risk: 5 **Critical**

DNSCAT2 is a dns tunneling tool. DNSCAT2 allows users to implement a tunnel over the dns protocol and to remotely connect to a dns server.

Match By

- Application Signature
- Services:
  - udp/53

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

CLOUD

No.	Name	Source	Destination	Services & Applications	Content	Action	Track
5.3	HR can access to social network applications	HR	Internet	Facebook Twitter	Download Traffic Executable File Archive File Source Code - Shell Scrip	Drop	Log
5.4	HR can access to social network applications	HR	Internet	Facebook Twitter	Any		
5.5	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	YouTube Vimeo	Any		

All | Search...

- Archive File
- CAD-CAM Designs
- Certificate Files
- Certificate Signing Request File
- Certificates and Private Keys
- Credit Card Numbers or IBAN
- CSV File

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

Предотвращение известных угроз

CHECK POINT THREATCLOUD™

NETWORK, CLOUD

ENDPOINT

Сокращение площади атаки и предотвращение ущерба

Check Point SandBlast ZERO-DAY PROTECTION

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

Предотвращение известных угроз

CHECK POINT THREATCLOUD™

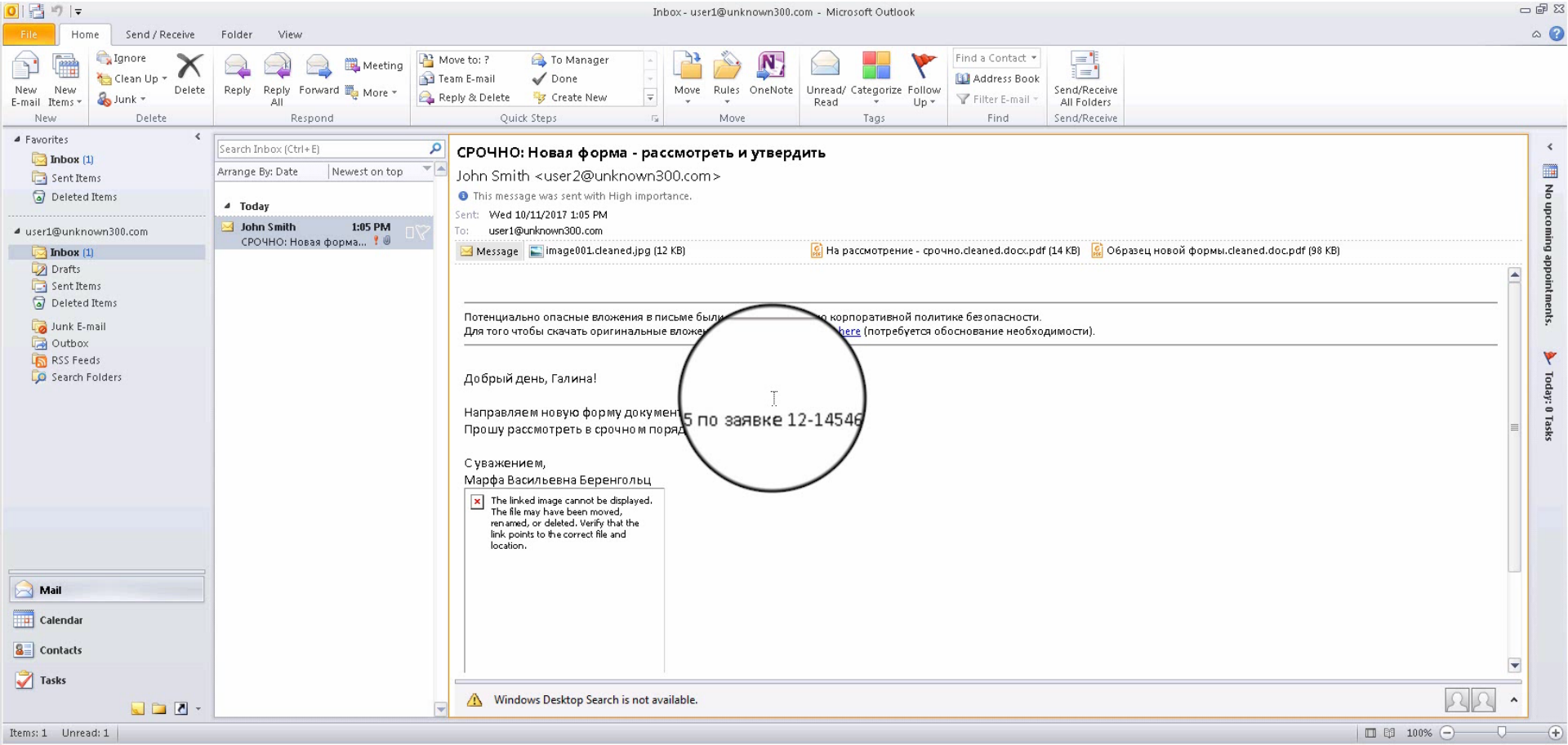
Threat Extraction

Проактивная очистка документов и изображений

NETWORK, CLOUD

ENDPOINT

Threat Extraction – удобная защита для пользователей



Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

Предотвращение известных угроз

Check Point SandBlast ZERO-DAY PROTECTION

Check Point THREATCLOUD

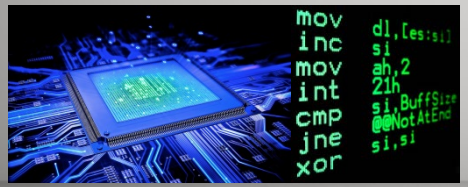
Проактивная очистка документов и изображений

Threat Emulation

Предотвращение неизвестных угроз

NETWORK, CLOUD

ENDPOINT



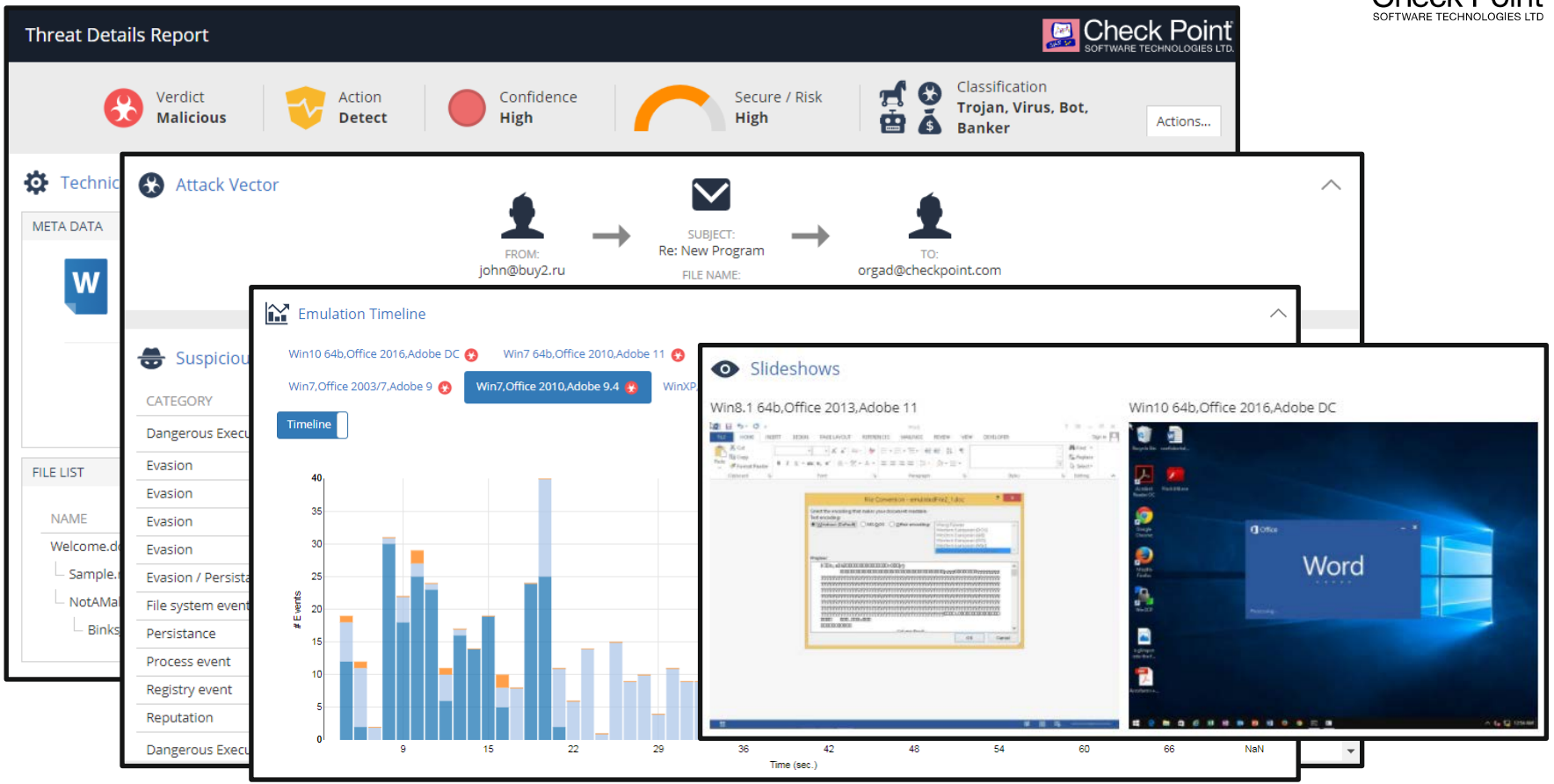
Обнаружение эксплойтов
на уровне ЦПУ
В том числе Meltdown и Spectre!*

Сложные составные веб-атаки
с эксплойтами для Flash

Глубокий анализ
макросов

* https://research.checkpoint.com/detection-meltdown-spectre-vulnerabilities-using-checkpoint-cpu-level-technology/

Детальные отчеты Threat Emulation



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...

SandBlast предотвращает 0-day как в электронной почте, так и в веб-трафике

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

Предотвращение известных угроз

Проактивная очистка документов и изображений

Предотвращение неизвестных угроз

Предотвращение фишинга в веб

NETWORK, CLOUD

ENDPOINT

Check Point SandBlast AGENT

Zero Phishing

- ✓ IP Reputation
- ✓ URL Similarity
- ✓ Title Similarity
- ✓ Visual Similarity
- ✓ Text Similarity
- ✓ Domain Reputation
- ✓ Multiple Top-Level Domain
- ✓ Lookalike Characters
- ✓ Lookalike Favicon
- ✓ Image Only Site

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

Предотвращение известных угроз

CHECK POINT THREATCLOUD™

Проактивная очистка документов и изображений

Check Point SandBlast™ AGENT

Предотвращение неизвестных угроз

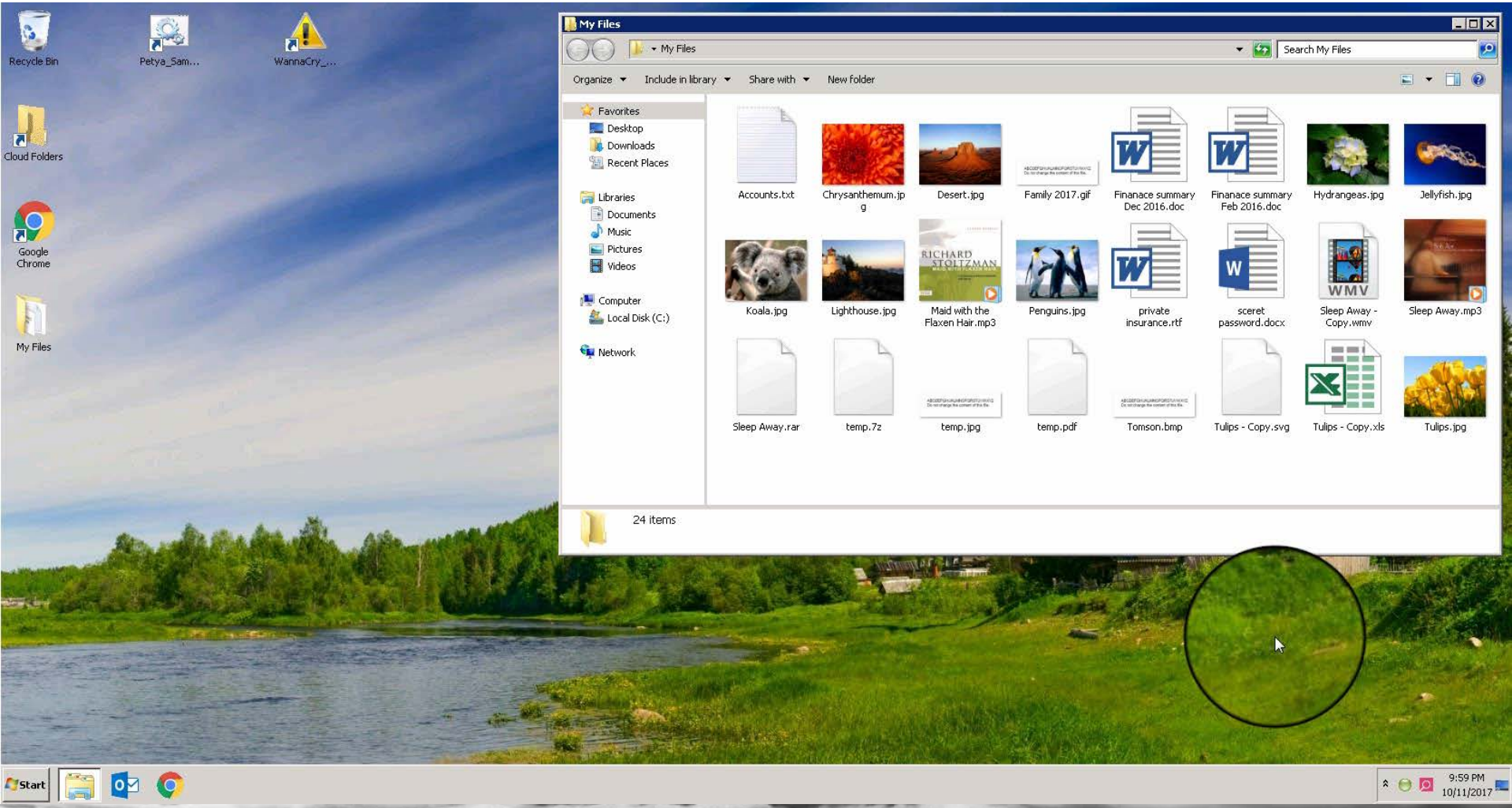
Предотвращение фишинга в веб

Anti-Ransomware

Предотвращение шифровальщиков

NETWORK, CLOUD

ENDPOINT


Recycle Bin
Petya_Sam...
WannaCry_...
Cloud Folders
Google Chrome
My Files
My Files
My Files
Search My Files
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Accounts.txt
Chrysanthemum.jpg
Desert.jpg
Family 2017.gif
Finanace summary Dec 2016.doc
Finanace summary Feb 2016.doc
Hydrangeas.jpg
Jellyfish.jpg
Koala.jpg
Lighthouse.jpg
Maid with the Flaxen Hair.mp3
Penguins.jpg
private insurance.rtf
sceret password.docx
Sleep Away - Copy.wmv
Sleep Away.mp3
Sleep Away.rar
temp.7z
temp.jpg
temp.pdf
Tomson.bmp
Tulips - Copy.svg
Tulips - Copy.xls
Tulips.jpg
24 items
Start
9:59 PM
10/11/2017

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

Предотвращение известных угроз

CHECK POINT THREATCLOUD™

Проактивная очистка документов и изображений

Предотвращение неизвестных угроз

Check Point SandBlast™ AGENT

Предотвращение фишинга в веб

Предотвращение шифровальщиков

NETWORK, CLOUD

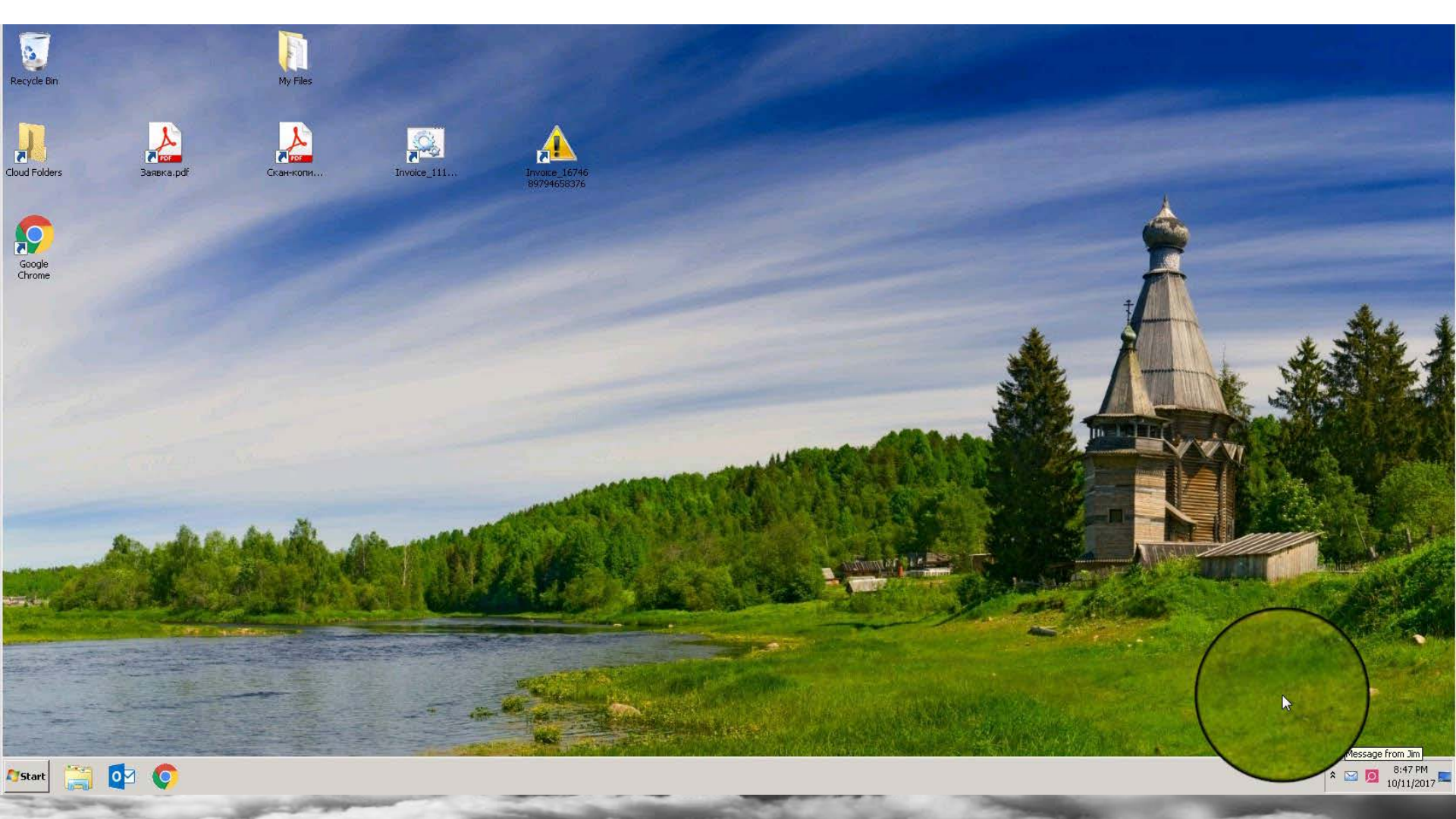
ENDPOINT

Предотвращение атаки

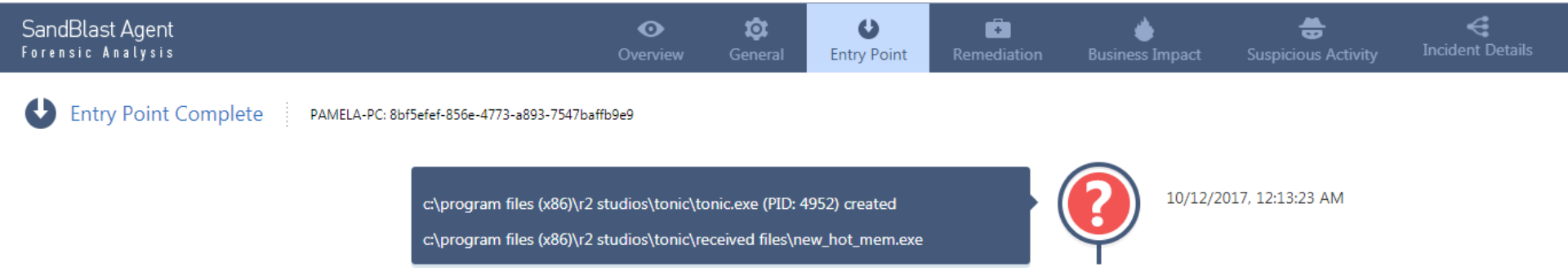
Предотвращение ущерба от атаки

Forensics

Изоляция, лечение, расследование


Recycle Bin
My Files
Cloud Folders
Заявка.pdf
Скан-копи...
Invoice_111...
Invoice_16746
89794658376
Google
Chrome
Start
Message from Jim
8:47 PM
10/11/2017

Forensics: метод доставки вредоноса



Forensics: блокирование угрозы и лечение

Check Point
SOFTWARE TECHNOLOGIES LTD

SandBlast Agent
Forensic Analysis

Overview | General | Entry Point | Remediation | Business Impact | Suspicious Activity | Incident Details

Remediation Details

PAMELA-PC: 8bf5efef-856e-4773-a893-7547baffb9e9

Deleted Incident Files (3 deleted)

These are potentially malicious files that have been removed.

Reputation	File Name	File Path	MD5	Status
?	tonic.exe	c:\program files (x86)\r2 studios\tonic\tonic.exe	5f55b1358f83c2dd50d65573b121802e	⊖
?	new_hot_mem.exe	c:\program files (x86)\r2 studios\tonic\received files\new_hot_mem.exe	f2ed5100d7aca4423d72acd8482e1316	⊖
?	oem86b3.exe	c:\users\administrator.unknown300\documents\oem86b3.exe	b548985699747c0035a89b8494736ab5	⊖

Terminated Incident Processes (7 terminated)

These are active processes related to the incident that have been stopped.

Reputation	PID	Process Name	Process Path	MD5	Status
✓	3608	schtasks.exe	c:\windows\syswow64\schtasks.exe	2003e9b15e1c502b146dad2e383ac1e3	⚙
✓	3272	powershell.exe	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe	92f44e405db16ac55d97e3bfe3b132fa	⚙
✓	3764	cmd.exe	c:\windows\syswow64\cmd.exe	ad7b9c14083b52bc532fba5948342b98	⚙

Forensics: список подозрительных активностей

Check Point
SOFTWARE TECHNOLOGIES LTD

SandBlast Agent
Forensic Analysis

Overview | General | Entry Point | Remediation | Business Impact | Suspicious Activity | Incident Details

Suspicious Activity (7 categories, 22 events)

PAMELA-PC: 8bf5efef-856e-4773-a893-7547baffb9e9

These are suspicious events that can be directly attributed to the attack.

- ▶ Script Execution (1 event)
- ▶ System Security Policy Change (3 events)
- ▶ Dropped File Deletion (1 event)
- ▼ Persistence (6 events)

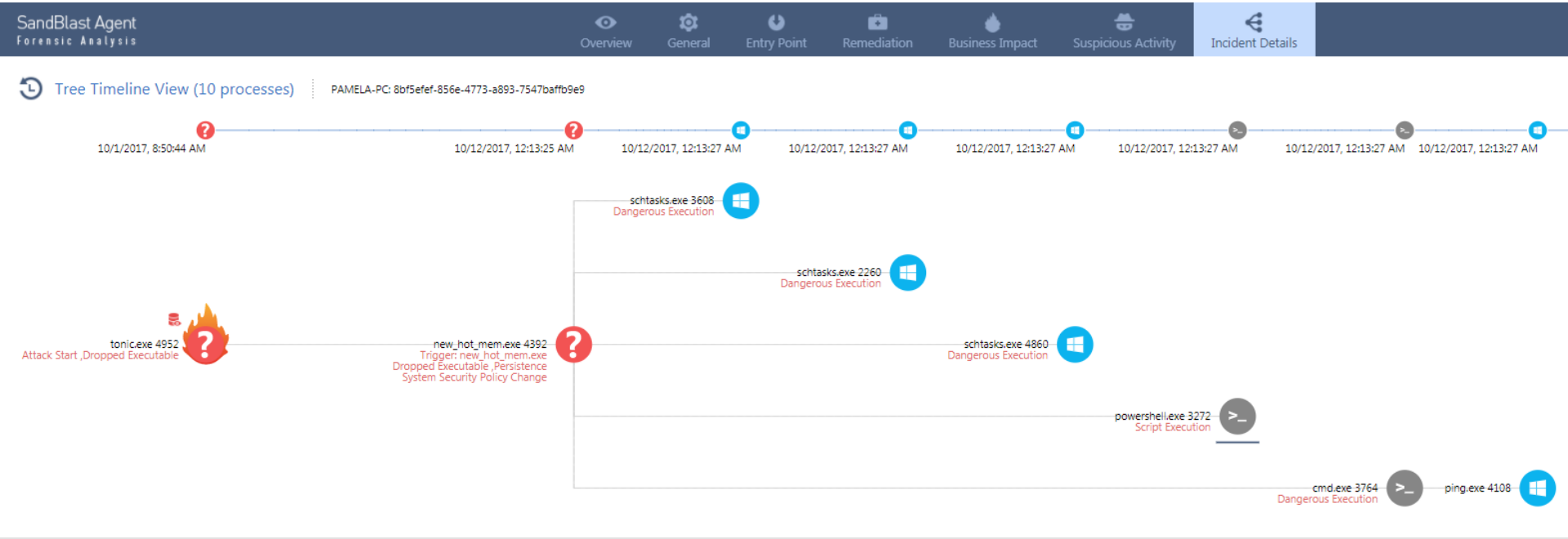
The incident performed persistence actions to ensure execution after system boot. Persistence is performed by setting specific system registry keys or by creating files in specific system folders.

Description
new_hot_mem.exe (PID:4392) modified HKU\s-1-5-21-676522091-3981307122-322411273-500\hkcu\software\microsoft\windows\currentversion\policies\explorer\run\svchost = C:\Users\ADMINI~1.UNK\AppData\Local\Temp\oem86B1.exe
new_hot_mem.exe (PID:4392) modified HKU\s-1-5-21-676522091-3981307122-322411273-500\hkcu\software\microsoft\windows\currentversion\policies\explorer\run\
new_hot_mem.exe (PID:4392) modified HKU\s-1-5-21-676522091-3981307122-322411273-500\software\microsoft\windows\currentversion\runonce\svchost = C:\Users\ADMINI~1.UNK\AppData\Local\Temp\oem86B1.exe
new_hot_mem.exe (PID:4392) modified HKU\s-1-5-21-676522091-3981307122-322411273-500\software\microsoft\windows\currentversion\run\svchost = C:\Users\ADMINI~1.UNK\AppData\Local\Temp\oem86B1.exe
new_hot_mem.exe (PID:4392) created oem86b4.tmp in c:\users\administrator.unknown300\appdata\roaming\microsoft\windows\start menu\programs\startup
new_hot_mem.exe (PID:4392) created oem86b4.exe in c:\users\administrator.unknown300\appdata\roaming\microsoft\windows\start menu\programs\startup

- ▶ Dangerous Execution (5 events)

Forensics: дерево процессов и событий

Check Point
SOFTWARE TECHNOLOGIES LTD



Process Info | Security | Reputation | File Ops (101) | Network Ops (0) | Registry Ops (0) | Injection/Hook Ops (0) | Suspicious Events (1) | Damage (0)

Process Name:	powershell.exe	Arguments:	-c $proc=([wmiclass]'root\cimv2:win32_process').create('c:\users\administrator.unknown300\documents\oem86b3.exe')
Path:	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe	PID:	3272
Start Time:	10/12/2017, 12:13:27 AM	Close Time:	10/12/2017, 12:13:28 AM
Duration:	1s 417ms		
Created By:		Created By PID:	0

Forensics: потенциально украденные данные

Check Point
SOFTWARE TECHNOLOGIES LTD

SandBlast Agent
Forensic Analysis

Overview | General | Entry Point | Remediation | Business Impact | Suspicious Activity | Incident Details

Business Impact (1 category, 21 events)

PAMELA-PC: 8bf5efef-856e-4773-a893-7547baffb9e9

These are potentially important events that have business impact.

▼ Data Loss (21 events)

User files that were likely accessed in the incident.

Search:

File Name	File Path	Action	Event Time
people.gif	c:\program files (x86)\r2 studios\tonic\images\people.gif	Read	10/1/2017, 8:50:45 AM
unknownimage.gif	c:\program files (x86)\r2 studios\tonic\images\unknownimage.gif	Read	10/1/2017, 8:50:45 AM
right.gif	c:\program files (x86)\r2 studios\tonic\messagewindow\default\right.gif	Read	10/12/2017, 12:13:21 AM
bottomleftbubble.gif	c:\program files (x86)\r2 studios\tonic\messagewindow\default\bottomleftbubble.gif	Read	10/12/2017, 12:13:21 AM
bottom.gif	c:\program files (x86)\r2 studios\tonic\messagewindow\default\bottom.gif	Read	10/12/2017, 12:13:21 AM
bottomright.gif	c:\program files (x86)\r2 studios\tonic\messagewindow\default\bottomright.gif	Read	10/12/2017, 12:13:21 AM
companysecret.doc	c:\users\administrator.unknown300\documents\companysecret.doc	Read	10/12/2017, 12:13:28 AM

Showing 1 to 21 of 21 entries

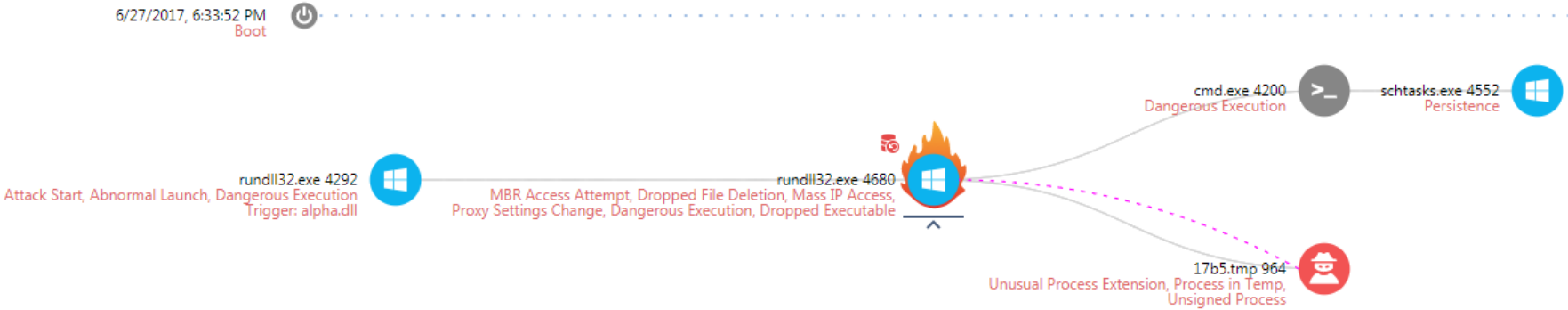
Forensics: горизонтальное перемещение

Check Point
SOFTWARE TECHNOLOGIES LTD

SandBlast Agent
Forensic Analysis

Overview | General | Entry Point | Remediation | Business Impact | Suspicious Activity | Incident Details

Tree View (5 processes) | xxxxxx: Petya-DLL21498581171011

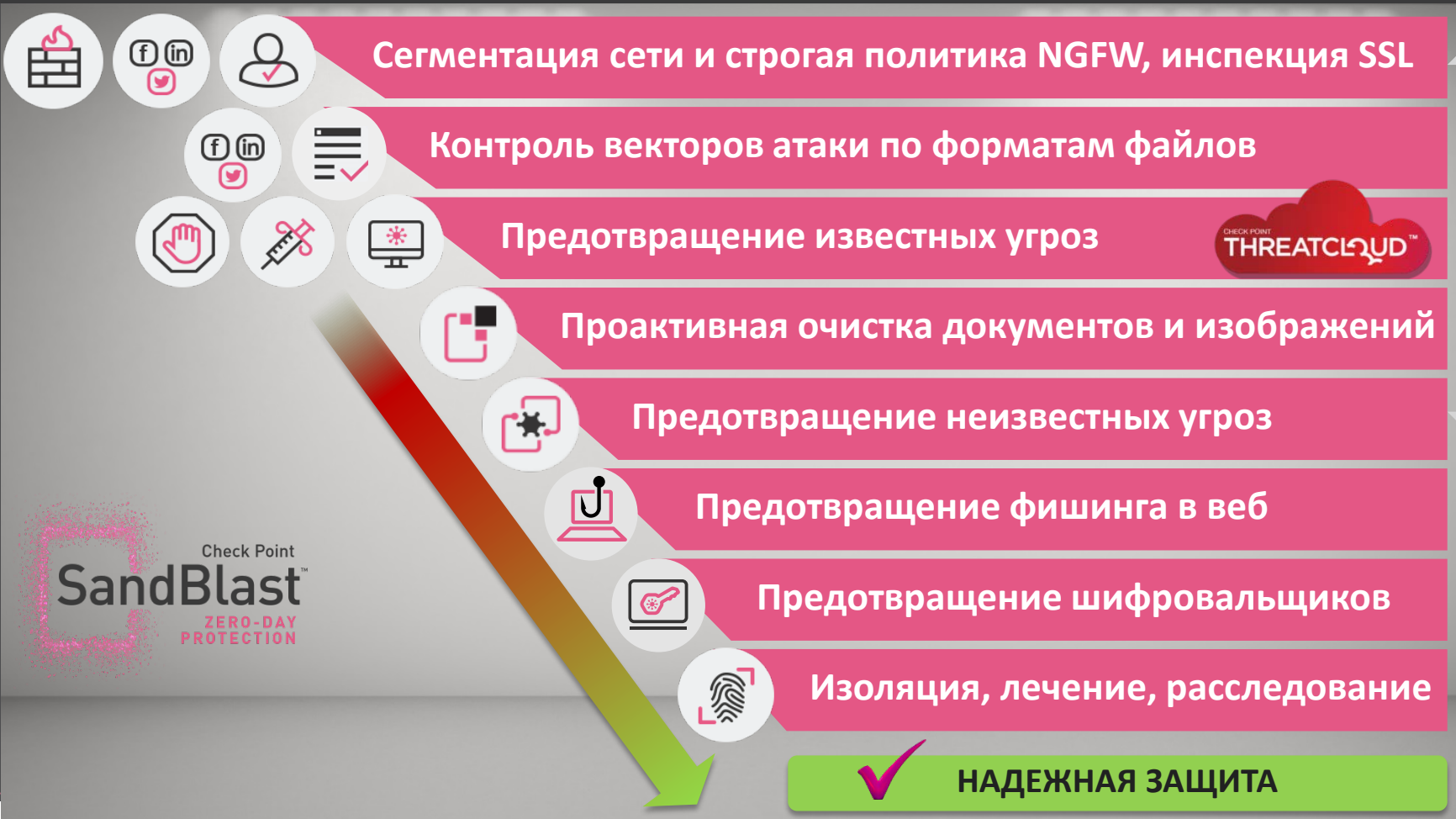


Process Info | Security | Reputation | File Ops (114) | Network Ops (168) | Registry Ops (5) | Injection/Hook Ops (6) | Suspicious Events (9) | Damage (48)

Protocol	Expected App Protocol	Reverse DNS	Dst IP	Dst Port	Src IP	Src Port
TCP	Microsoft-DS Active Directory, Windows shares		192.168.200.0	445	xxxxxx	49850
TCP	Microsoft-DS Active Directory, Windows shares		192.168.200.1	445	xxxxxx	49861
TCP	Microsoft-DS Active Directory, Windows shares		192.168.200.2	445	xxxxxx	49865

*на примере отчета для NotPetya

Комплексная защита Check Point от кибер-атак



Выводы

- Кибер-атаки происходят все чаще, и мы не можем повлиять на факторы этого роста
- Только комплексный многоуровневый подход способен предотвратить атаку
- Архитектура безопасности Check Point и новейшие технологии для защиты от угроз нулевого дня снова доказали свою эффективность

Дмитрий Воронков
Security Consultant Team Lead
dvoronkov@checkpoint.com

СПАСИБО!