



31/05/2018

**Александр
Русецкий**

JET-ПОЛИГОН: ИСПЫТАНИЯ ANTI-ART РЕШЕНИЙ В БОЕВЫХ УСЛОВИЯХ

Руководитель направления по защите от направленных атак
as.rusetskiy@jet.su / +7 926 156-81-25

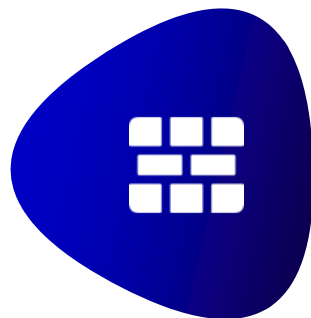
УЧАСТНИКИ JET-ПОЛИГОНА



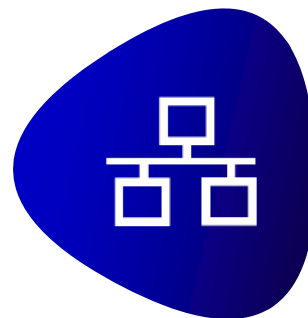
КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ОТ АРТ



Песочница
(SandBox)



NGFW / Proxy



Сетевой
мониторинг



Защита
рабочих станций

ДИНАМИЧЕСКИЙ АНАЛИЗ

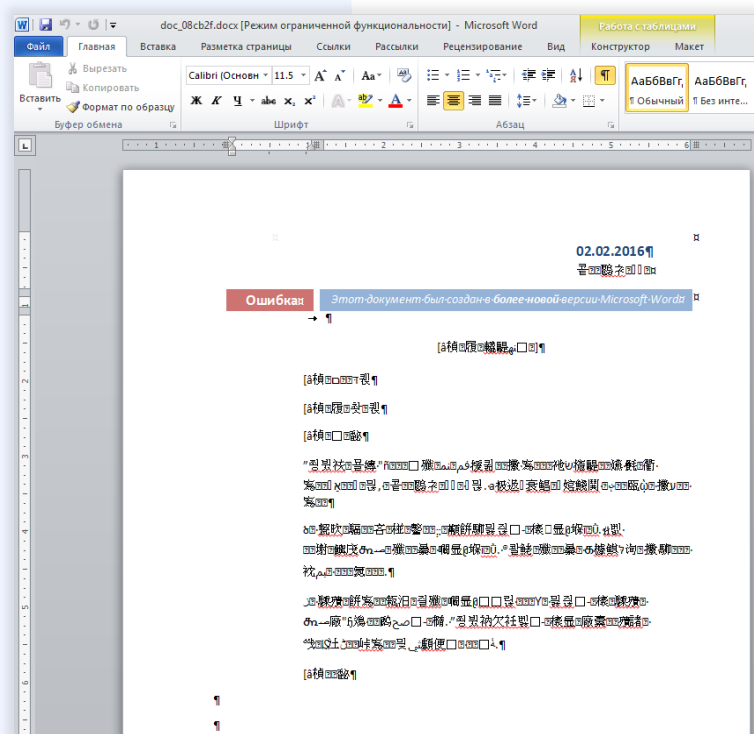
- Обнаружение изменений реестра
- Обнаружение сетевых коммуникаций
- Обнаружение активности процессов
- Обнаружение изменений файловой системы

СТАТИЧЕСКИЙ АНАЛИЗ

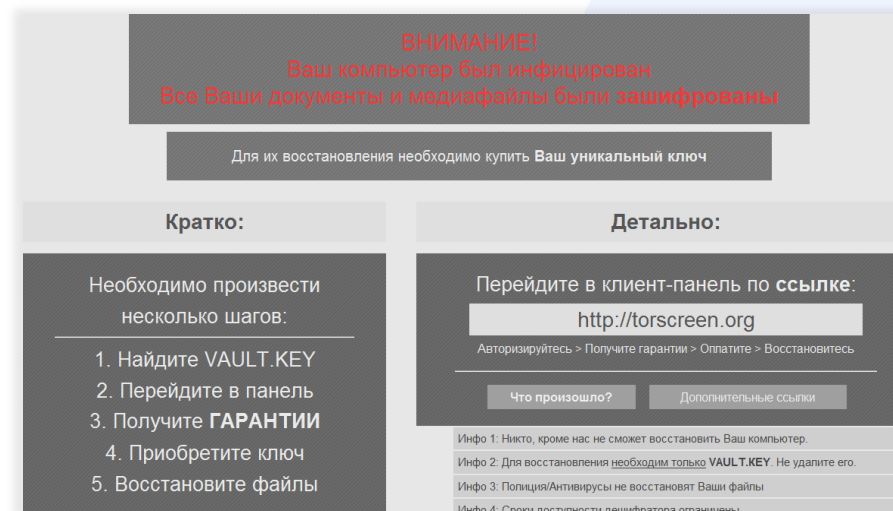
- Распаковка
- Анализ деассемблированного кода
- Анализ пассивного кода
- Обнаружение скрытых логических путей



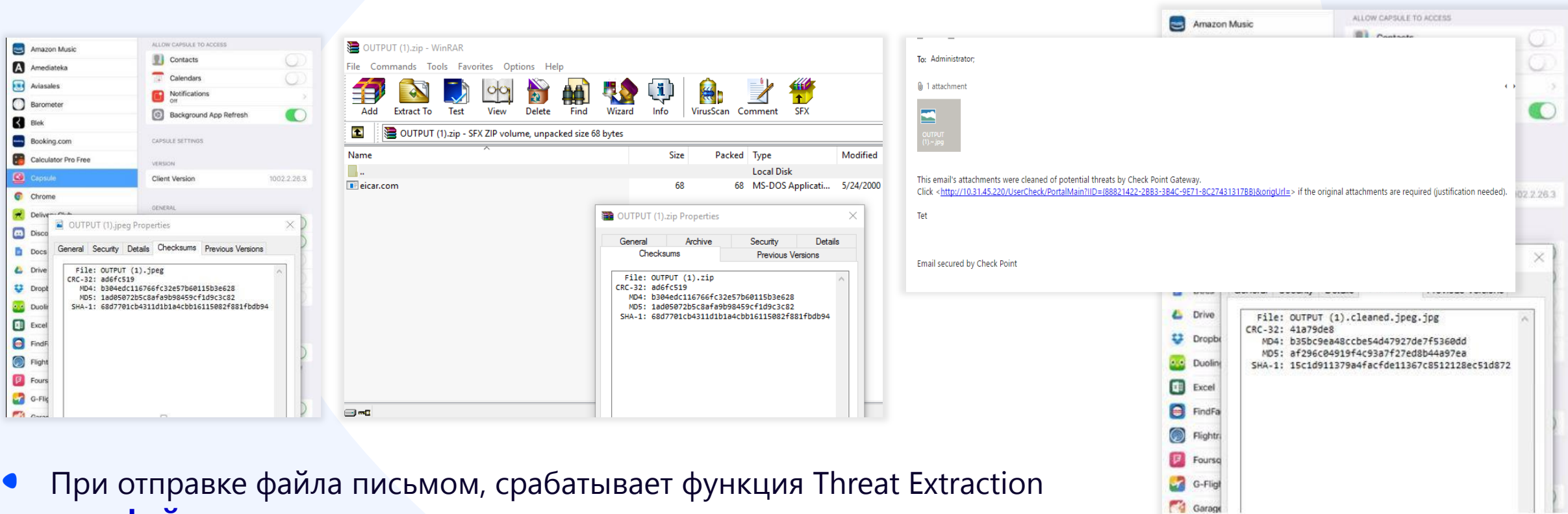
ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ ПОЧТА. ШИФРОВАЛЬЩИК СЕМЕЙСТВА VAULT



- Пересылка письма нескольким адресатам внутри компании
- Не обнаружено установленными СЗИ компании



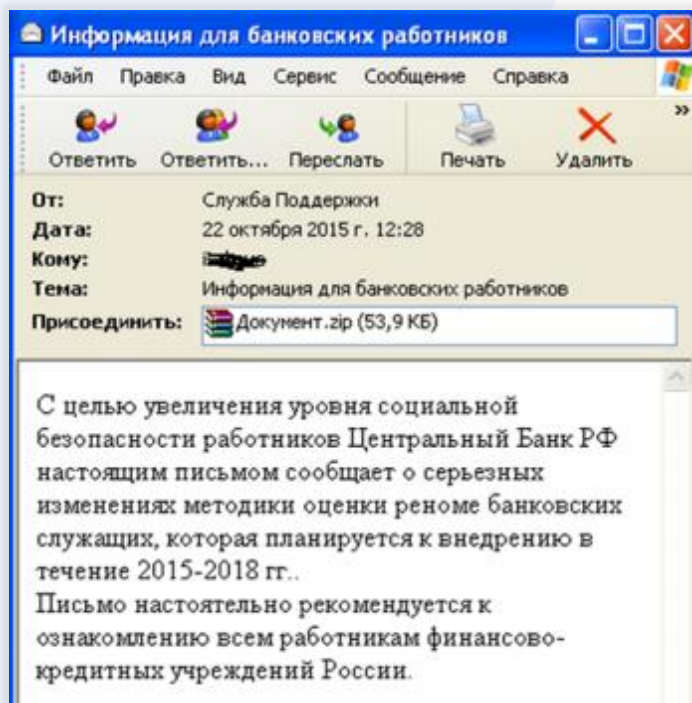
ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ ПОЧТА. ФУНКЦИЯ THREAT EXTRACTION



- При отправке файла письмом, срабатывает функция Threat Extraction и **из файла извлекается все потенциально вредоносное содержимое**
- Полученный файл имеет другую контрольную сумму, по-прежнему открывается как картинка, но уже не может быть открыт как архив

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ПОЧТА. ВРЕДОНОСНОЕ ПО BUHTRAP

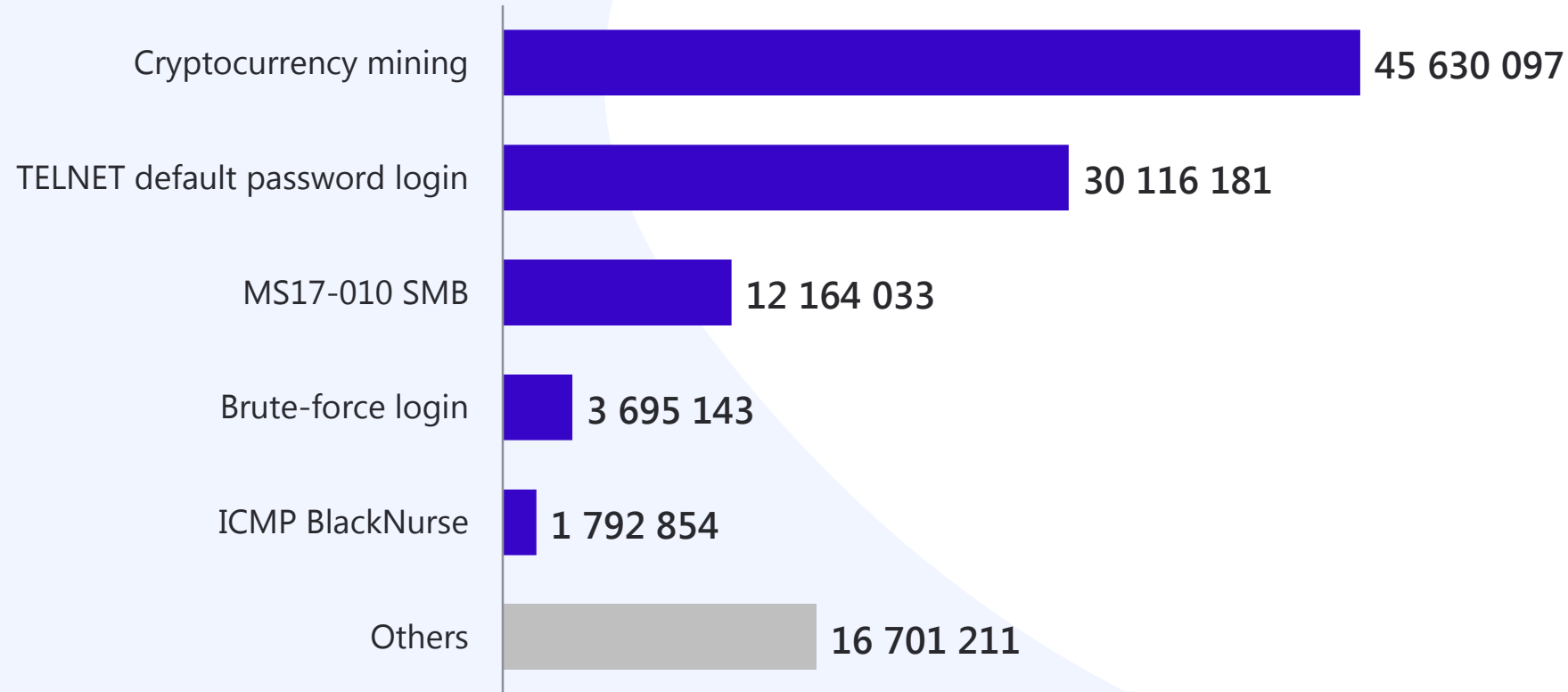


Кастомизированный образ АРМ в песочнице:

- Сбор логинов и паролей от доменных учетных записей
- Поиск систем с ПО АРМ КБР
- Подмена платежных документов в адрес Банка России
- Вывод из строя зараженных ПК

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ПОЧТА. КРИПТОМАЙНИНГ



Статистика Trend Micro™ Smart Network Solution



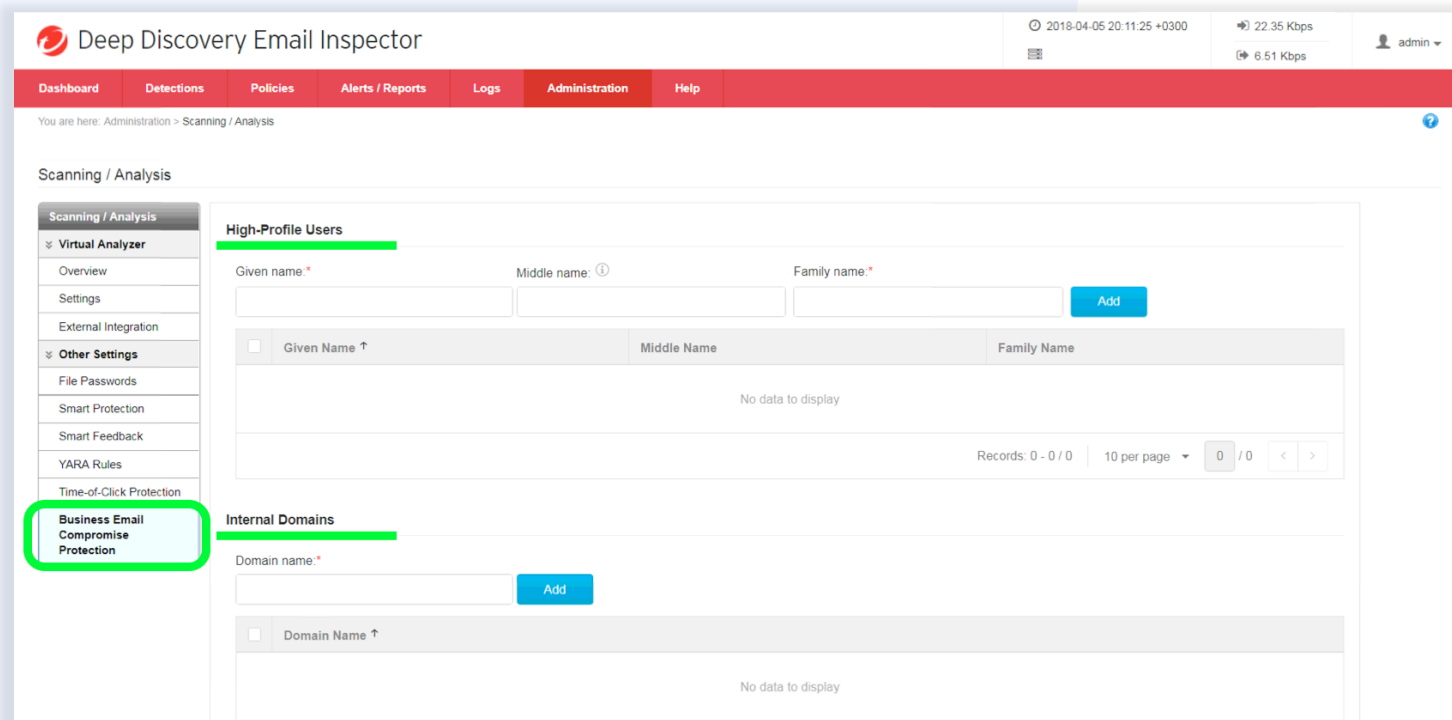
ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ПОЧТА. КОМПЛЕКСНАЯ ЗАЩИТА



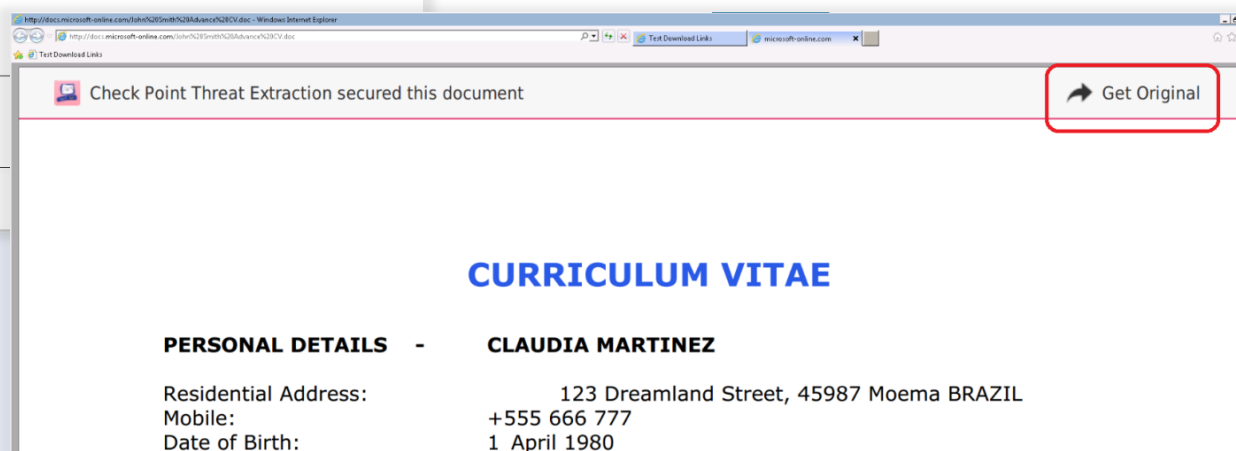
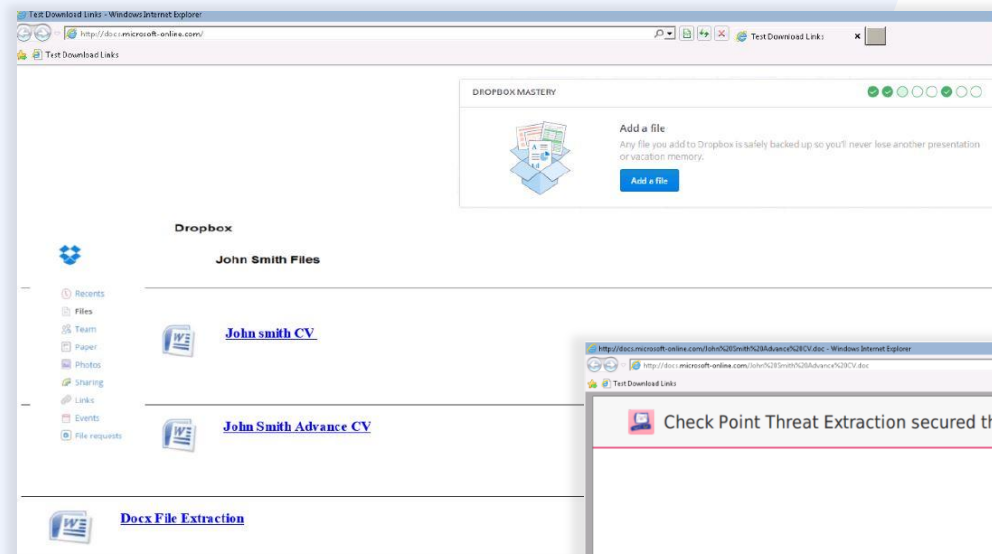
- FortiMail как пограничный шлюз SMTP
- FortiWeb как шлюз для OWA/ActiveSync/MAPI

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ ПОЧТА. ВЕС (BUSINESS EMAIL COMPROMISE)



- Инструменты социальной инженерии
- Компрометация почтового ящика руководителя
- Перевод денежных средств на счет злоумышленника

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ WEB. ПРЕДОТВРАЩЕНИЕ ZERO-DAY БЕЗ ЗАДЕРЖЕК



	Name	Risk
☒	Database Queries	2 Low
☒	Embedded Images	4 High
☒	Embedded Objects	4 High
☒	Fast Save Data	1 Very-Low
☒	Linked Objects	4 High
☒	Macros and Code	5 Critical
☒	PDF 3D Artwork Annotations	3 Medium
☒	PDF GoToR Actions	3 Medium
☒	PDF JavaScript Actions	5 Critical
☒	PDF Launch Actions	4 High
☒	PDF Movie Actions	3 Medium
☒	PDF Sound Actions	3 Medium
☒	PDF Submit Form Actions	4 High
☒	PDF URI Actions	3 Medium
☒	Sensitive Hyperlinks	3 Medium

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ЗАЩИТА ФАЙЛОВЫХ ХРАНИЛИЩ



- Карантин подозрительных файлов
- Возможность сканирования по расписанию
- **Автоматическое переключивание чистых файлов из одного хранилища в другое**

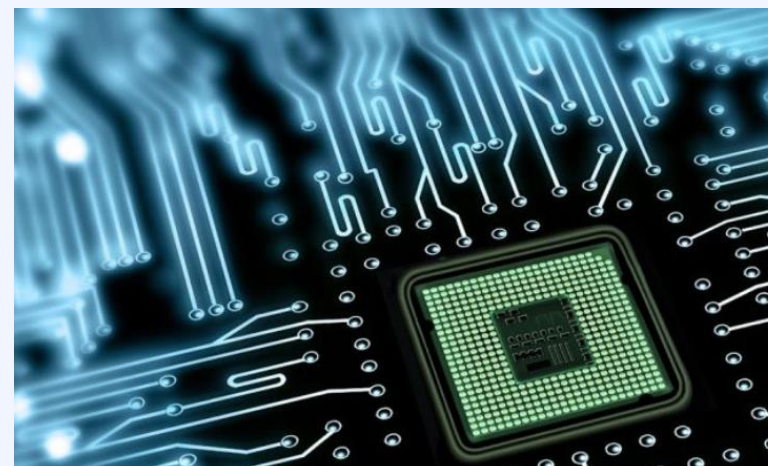
CPU-LEVEL DETECTION: ОБНАРУЖЕНИЕ ЭКСПЛОЙТОВ ДЛЯ INTEL



CVE-2017-5754



CVE-2017-5753,
CVE-2017-5715



Detection of the Meltdown and Spectre
Vulnerabilities

January 8, 2018

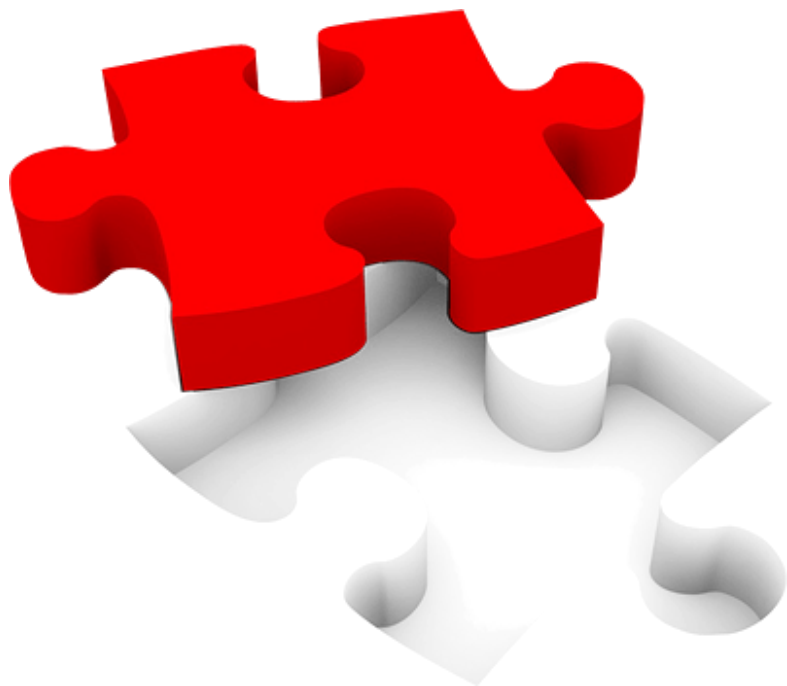
- Детектирование эксплойтов возможно только на уровне ЦПУ (вне ОС)
- Подход к обнаружению в блоге Check Point: <https://research.checkpoint.com/detection-meltdown-spectre-vulnerabilities-using-checkpoint-cpu-level-technology/>

[illegible]

Name	Name
 ..	 ..
 execution_log *	 task0
 internal_tracing_report *	 task1
 pcap *	 task2
 pcap_postproc_report *	 am_bases_version *
	 multitask_result.json *
	 sample *
	 sandbox_config.json *

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

СТОРОННЯЯ ИНТЕГРАЦИЯ



- Поддержка API
- Работа с индикаторами компрометации (IoC)
- Прямая интеграция с сетевыми системами (прокси, МСЭ, IDS/IPS)
- Интеграция с SIEM



TREND
MICRO

FORTINET

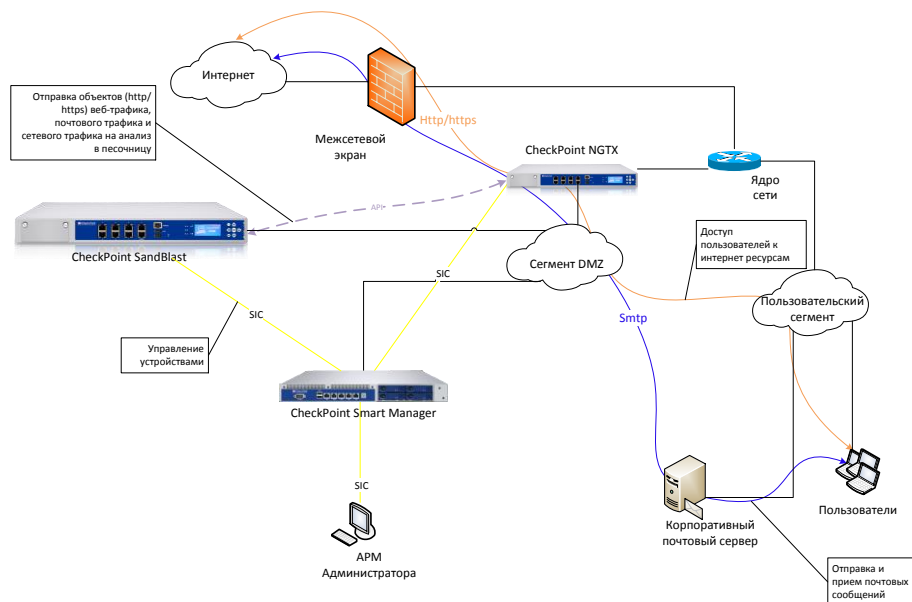
KASPERSKY Lab



Check Point
SOFTWARE TECHNOLOGIES LTD.

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

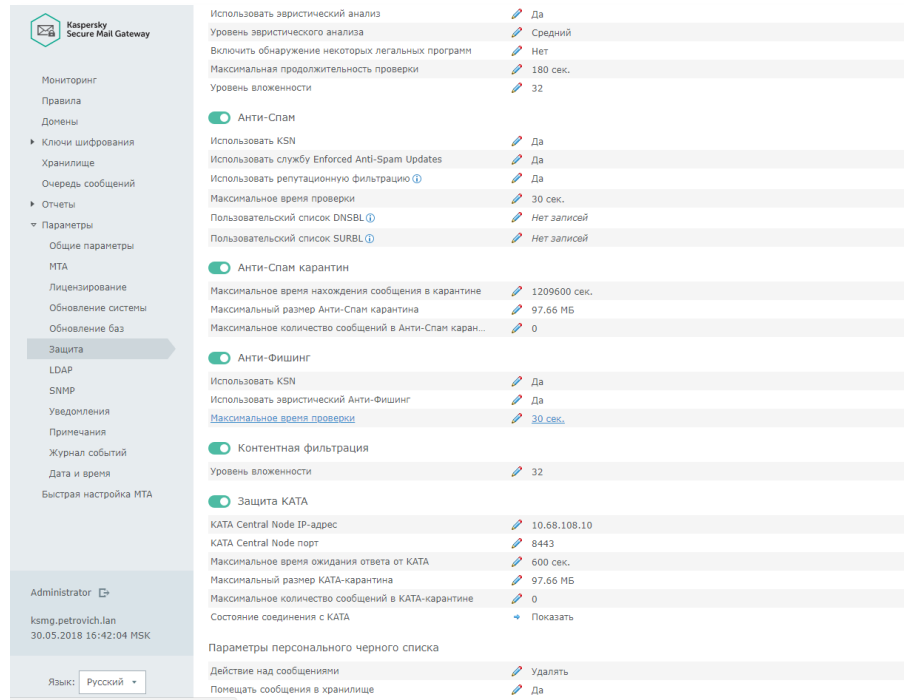
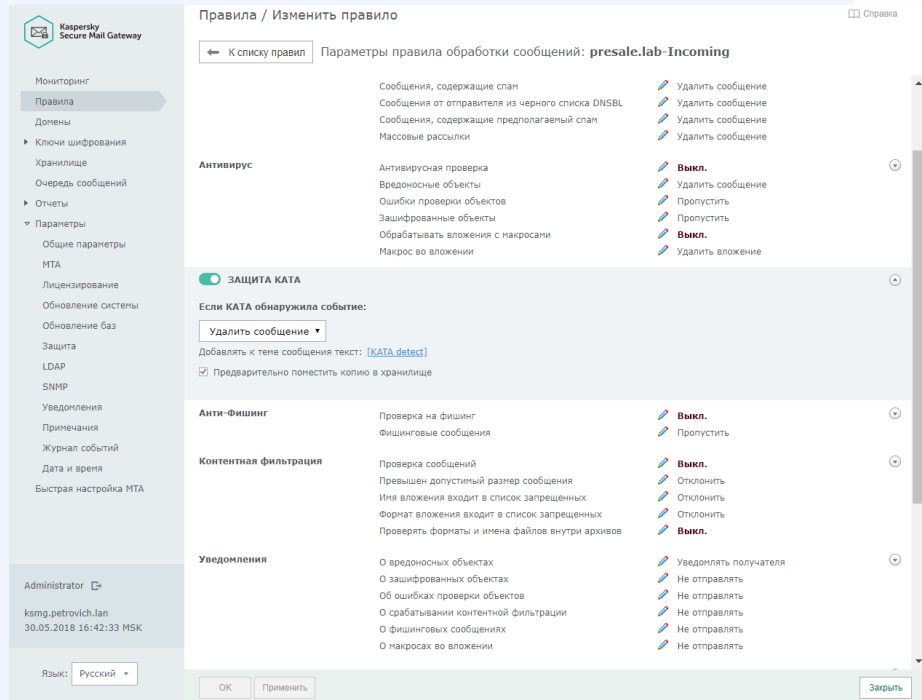
ДОПОЛНИТЕЛЬНЫЕ ПРИМЕРЫ ИНТЕГРАЦИИ



- Шлюз Check Point — «песочница» SandBlast
- Шлюз Check Point — сторонняя «песочница»
- Запуск форенсики SandBlast Agent по внешним событиям
- IoC через API
- От SIEM автоматизация настроек скриптом на шлюзе CP
- Импорт сторонних IoC на шлюз безопасности CP

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ДОПОЛНИТЕЛЬНЫЕ ПРИМЕРЫ ИНТЕГРАЦИИ

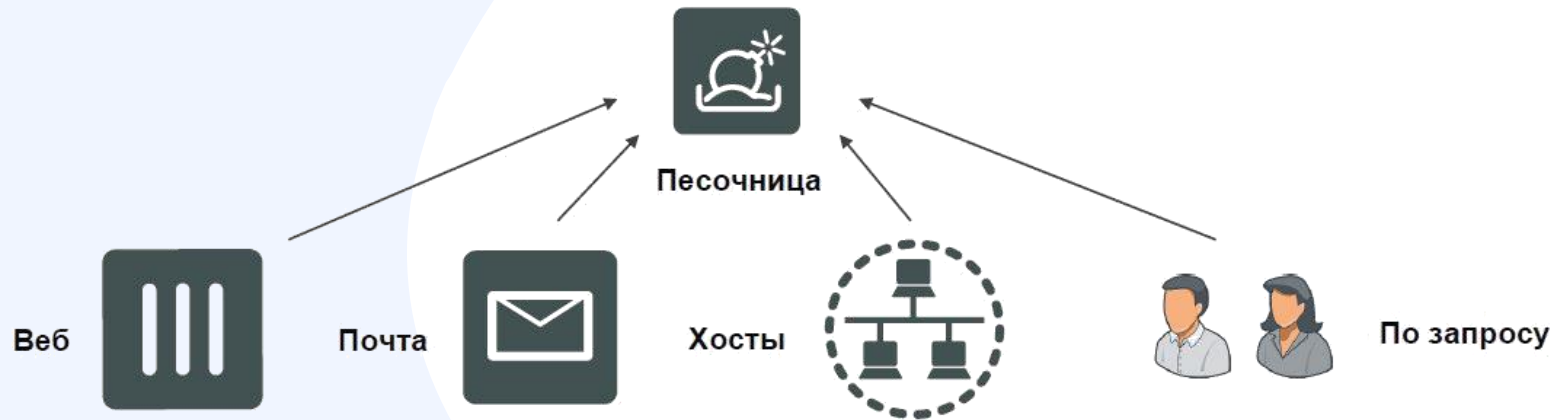


- Интеграция с почтовым шлюзом KSMG
- Интеграция с Kaspersky Security Center
- Интеграция с Kaspersky Private Security Network



ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ДОПОЛНИТЕЛЬНАЯ ИНТЕГРАЦИЯ

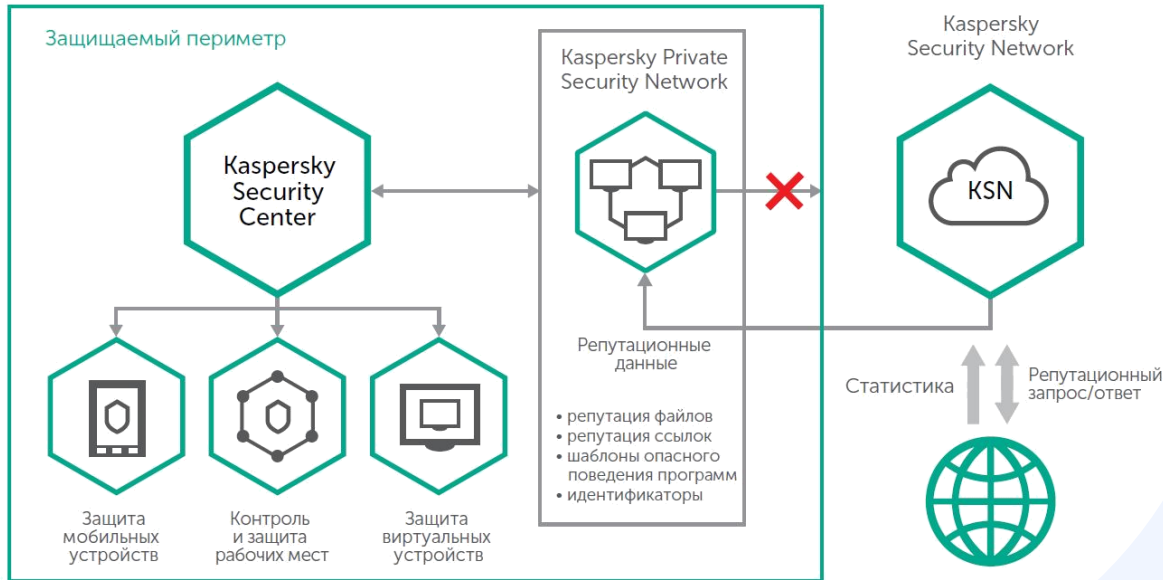


- Поддержка ICAP
- Единая песочница для анализа почты / веб / файловых хранилищ
- Интеграция с SIEM

FORTINET

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ПРИВАТНАЯ ИНСТАЛЛЯЦИЯ БАЗЫ РЕПУТАЦИЙ И СТАТИСТИКИ УГРОЗ



- Размещение репутационной базы внутри защищаемой инфраструктуры
- Выполнение требований регуляторов
- Исключение передачи информации вне контролируемой сети
- Одностороннее получение оперативных обновлений
- Высокая производительность

ANTI-ART: ПРАКТИКА ВНЕДРЕНИЙ

ПРИВАТНАЯ ИНСТАЛЛЯЦИЯ БАЗЫ РЕПУТАЦИИ И СТАТИСТИКИ УГРОЗ



Kaspersky Private Security Network

Мониторинг Серверы Репутационные базы Пользователи

Контроль соответствия

Добавить Удалить

Контроль соответствия

Добавить Удалить Экспорт

Добавление хеша

Доверенный Недоверенный

Хеш*: c42dbce71f2e6b817dcf2e532f98a

Имя файла: test

Описание: test

* — Обязательные поля

Сохранить

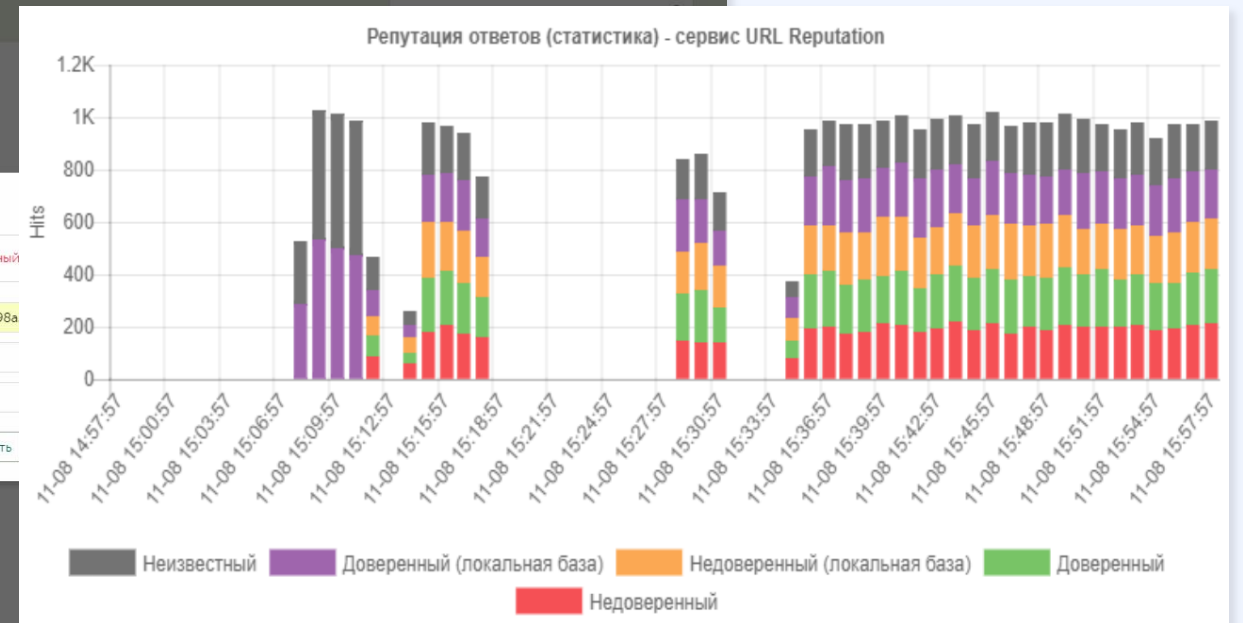
© 1997—2017 Kaspersky Lab

программе

© 1997—2017 Kaspersky Lab

программе

KASPERSKY



Векторы атаки

Защита



Почта

+



WEB

+



Файловые хранилища

+



Рабочие станции

+/-

Обычного антивируса уже недостаточно!



EDR: ENDPOINT DETECTION & RESPONSE

- Анализ поведения рабочей станции
- Инструментарий для проведения расследований
- Устранение последствий заражения
- Блокирование активностей ВПО
- Карантин скомпрометированной станции
- **EDR — дополнение к текущему антивирусу**

SandBlast Agent
Forensic Analysis

Tree Timeline View

10/1/2017, 8:50:44

tonic.exe 4952
Attack Start, Dropped Executable

Process Info

Security

Process Name: powershell.exe

Path: c:\windows\system32\powershell.exe

Start Time: 10/12/2017

Created By:

Parent Chain: new_hot_mem.exe

SandBlast Agent
Forensic Analysis

Suspicious Activity (7)

These are suspicious events that can be associated with this incident.

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

The incident performed persistence actions:

Description
new_hot_mem.exe (PID:4392) m...
new_hot_mem.exe (PID:4392) m...
new_hot_mem.exe (PID:4392) m...
new_hot_mem.exe (PID:4392) m...
new_hot_mem.exe (PID:4392) c...
new_hot_mem.exe (PID:4392) c...

- Dangerous Execution (1 event)
- Dropped Executable (5 events)
- Dropped Script (1 event)

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	⚙️
✓	4108	ping.exe	c:\windows\syswow64\ping.exe	6242e3d67787ccbf4e06ad2982853144	⚙️
✓	676	cmd.exe	c:\windows\syswow64\cmd.exe	ad7b9c14083b52bc532fba5948342b98	⚙️



ЭКСПЕРТИЗА В РЕАЛЬНОМ ВРЕМЕНИ

Kaspersky Anti Targeted Attack Platform

Dashboard Alerts **208** Threat Hunting Tasks Prevention IOC Scanner Storage Endpoint Sensors Reports

Events

Any time

Md5 - "3b5e452d35660a506d03579bd662b233"

Event	Details	Additional	User name	Event time
File created	c:\users\bigoldberg\appdata\local\temp\oice_195290a-c4eb-4539-901a-e959f19c5def\0156d42a72.doc	SHA256 MD5	corplbigoldberg	22/03 13:38:52
File created	c:\programdata\microsoft\windows defender\scans\files\stash\79ccbf-79e5-641f-cbef-703f5057c442_1d3c29321b88c47	SHA256 MD5	unknown\unknown	22/03 13:38:50
File created	c:\users\bigoldberg\downloads\agreement (2).doc	SHA256 MD5	corplbigoldberg	22/03 13:38:49
File created	c:\users\bigoldberg\appdata\local\temp\oice_628f4f3a-3ab6-44bf-ac2e-cbbc41a7a3e3\018c705008.doc	SHA256 MD5	corplbigoldberg	22/03 13:37:28
File created	c:\users\bigoldberg\downloads\agreement (1).doc	SHA256 MD5	corplbigoldberg	22/03 13:37:25
File created	c:\programdata\microsoft\windows defender\scans\files\stash\ebdbbe7e-09fa-42cc-1d8f-b4102ab9fad5_1d3c292ef1758e2	SHA256 MD5	unknown\unknown	22/03 13:37:25
File created	c:\users\bigoldberg\appdata\local\temp\oice_624b3023-2bc7-43f8-b0f3-b670acb48365\01a167d56.doc	SHA256 MD5	corplbigoldberg	22/03 10:07:35
File created	c:\users\bigoldberg\downloads\agreement.doc	SHA256 MD5	corplbigoldberg	22/03 10:07:29
File created	c:\programdata\microsoft\windows defender\scans\files\stash\3a82cba7-6760-0fbf-2c16-62f4356c2a81_1d3c2759b15cc64	SHA256 MD5	nt authority\SYSTEM	22/03 10:07:29
File created	c:\users\admin\appdata\local\temp\oice_0b4625e6-4698-	SHA256 MD5	-	20/03 14:23:37

- Активная «охота» (расследование, инициируемое пользователем)
- Расследование по следам оповещений



ПРИМЕРЫ РЕАГИРОВАНИЯ

cb RESPONSE Sensors

Groups: NEW

Filter by group name:

All Sensors: 2 sensors

Search by computer name:

Show uninstalled sensors: ☐

Computer Name	Domain Name	Status	Activity	OS Version	Node ID
☒ HIGHLEVEL	HighLevel	Online	in a few seconds	Windows 7 Enterprise Service Pack 1, 64-bit	0
☐ MEDIUMLEVEL	MediumLevel	Offline	11 days ago	Windows 7 Ultimate, 64-bit	0

Showing 1-2 of 2

10 Items per Page

Jump to Page: of 1

Filter Export Actions

- Sync
- Restart
- Move to group
- Uninstall
- Isolate
- Remove isolation

Kaspersky Anti Targeted Attack Platform

Dashboard Alerts (208) Threat Hunting Tasks Prevention IOC Scanner Storage Endpoint Sensors Reports

Event details

browser_broker.exe → winword.exe → winword.exe

Events: 5

File created: 5

86d42672.doc

Copy value to clipboard

Find in Events database

Tasks:

- Kill process...
- Delete file...
- Get file...
- Quarantine file...

File created

Event time

File: e959f19c5def0156d42672.doc

MDS: 3b5e452d35660a586d03579b662b233

SHA256: 8ea93e1c81fe840a24fa5a2e182868c5ff6a28bf277fa669585310148f52d04a

Parent process

File: -

MDS: -

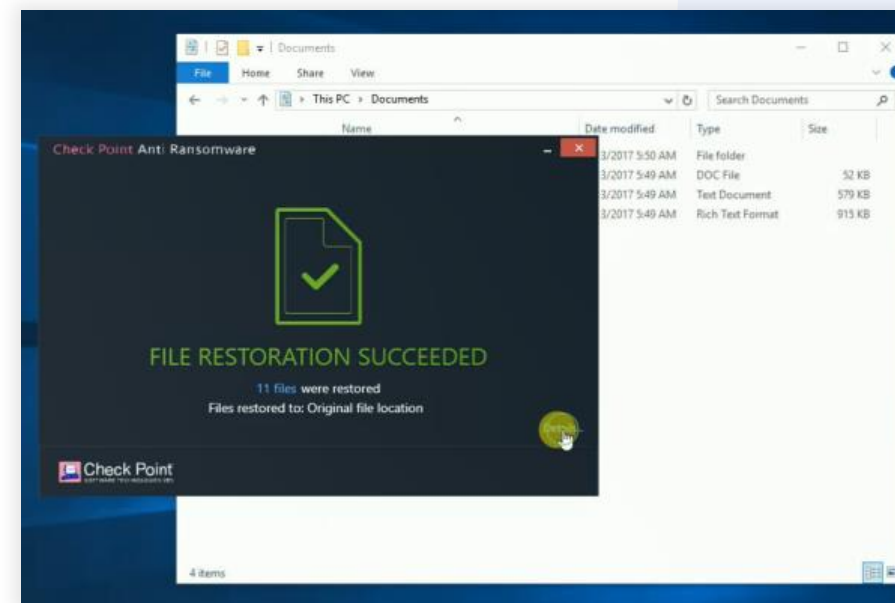
SHA256: -



БОРЬБА С ШИФРОВАЛЬЩИКАМИ



- Постоянный мониторинг специфических признаков шифровальщиков
- Проактивное создание краткосрочных бекапов
- Остановка всех вредоносных процессов
- **Восстановление файлов**
- Запуск форенстики для анализа деталей атаки





ИНТЕГРАЦИЯ С «ПЕСОЧНИЦЕЙ»

PROTECTION 10.31.42.136 Home Reports Assets Rules Tools Alerts: 1 1 1

Files on Computers
Applications
Application Catalog
Applications on Computers
Devices
Device Catalog
Devices on Computers
Certificates

First Seen Name: 4d1015f8f94e64c47fe41d1202ef2438c89e6d2a5fd68e4f01c5b4be943fc43.bin
First Seen Date: Apr 5 2018 05:37 PM
Last Updated: Apr 5 2018 05:32:43 PM
First Seen Path: c:\users\tect\desktop\fresh\
First Seen Computer: WORKGROUP\HIGHLEVEL
First Seen Platform: Windows
Extension: .bin
Global State: Banned
Global State Details: File is globally banned (Manual). Publisher is not present, Certificate is not present
Flags: (none)
Installer / Updater: No
Reputation Enabled: No
File Prevalence: File exists on 1 computer
[View Cb Reputation Data](#)

High Risk Injector

Mark as clean (false positive)
Received: Apr 05 2018 17:11:06
Started: Apr 05 2018 17:11:14+03:00
Status: Done
Rated by: VM Engine
Submit Type: Adapter
Digital Signature: No
Virus Total: Q

More Details

Packers: Microsoft Visual C++ v8.0
File Type: exe
Downloaded From: banker.class.exe
File Size: 1518592 (bytes)
MD5: 5666bbbed1f30ae3418add7f16d13a1
SHA1: 5338b8736cf97682b8914b92e69a32449020bdec
SHA256: 4d1015f8f94e64c47fe41d1202ef2438c89e6d2a5fd68e4f01c5b4be943fc43
ID: 3830036507657511627
Submitted By: ADPBIT1518100141
Submitted Filename: banker.class.exe
Filename: banker.class.exe
Start Time: Apr 05 2018 17:11:14+03:00
Detection Time: Apr 05 2018 17:12+03:00
Scan Time: 358 seconds
Scan Unit: FSAVMOE00009940
Device: ADPBIT1518100141
Launched OS: WIN7X86VMO16E, WIN7X64VM
Infected OS: WIN7X86VMO16E, WIN7X64VM

Suspicious Indicators

- The executable injects code into a process, usually svchost.exe, winlogon.exe, explorer.exe
- The executable seemed to be a keylogger
- The executable tries to inject to system process

Analysis Details

WIN7X86VMO16E

Behavior Chronology Chart

Threat Level

14:26:10 14:26:20 14:26:30 14:26:40 14:26:50 14:27:00 14:27:10 14:27:20 14:27:30 14:27:40 14:27:50

Carbon Black.

Cb Collective Defense Cloud Reputation

MD5 Hash: 5666bbbed1f30ae3418add7f16d13a1
SHA-1 Hash: 5338b8736cf97682b8914b92e69a32449020bdec
SHA-256 Hash: 4d1015f8f94e64c47fe41d1202ef2438c89e6d2a5fd68e4f01c5b4be943fc43
Hash Not Found: This hash was not found in the Carbon Black Collective Defense Cloud Reputation database.
The hash might be:
- non-commercial software (e.g. internally generated)
- less-popular software
- malware
Carbon Black continually updates its databases and uses information about hashes not found to improve coverage. Please fill out the comment below with information about the hash and click Submit. Thank you.
Please enter a comment about this hash and click Submit.
[Submit](#)
Copyright © 2016 Carbon Black, Inc. All rights reserved | [Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#)



CARBON
BLACK
ARM YOUR ENDPOINTS



FORTINET



KASPERSKY lab

KEDR



Kaspersky Anti Targeted
Attack Platform (KATA)

ИНТЕГРАЦИЯ



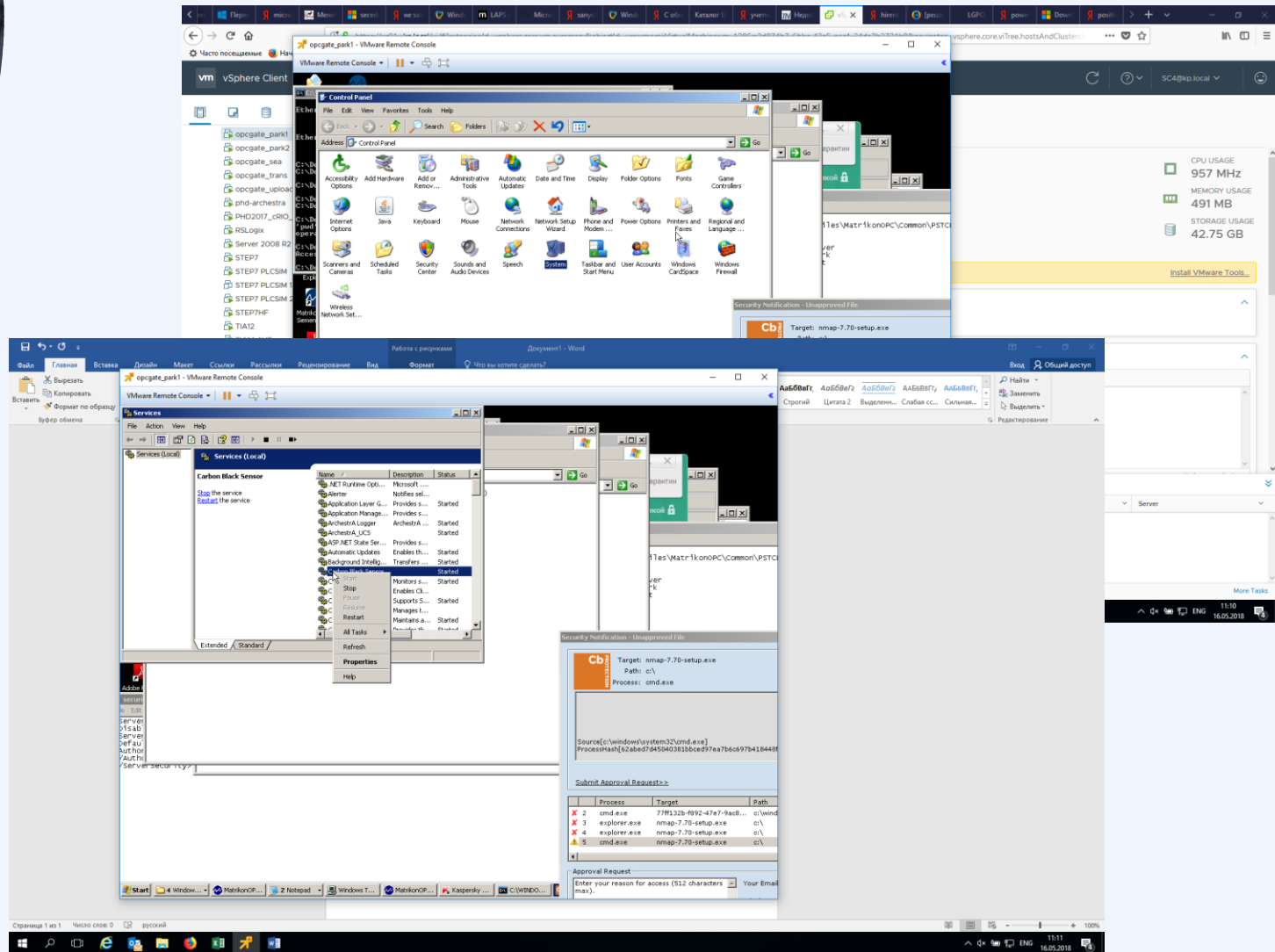
SandBlast
Agent



SandBlast

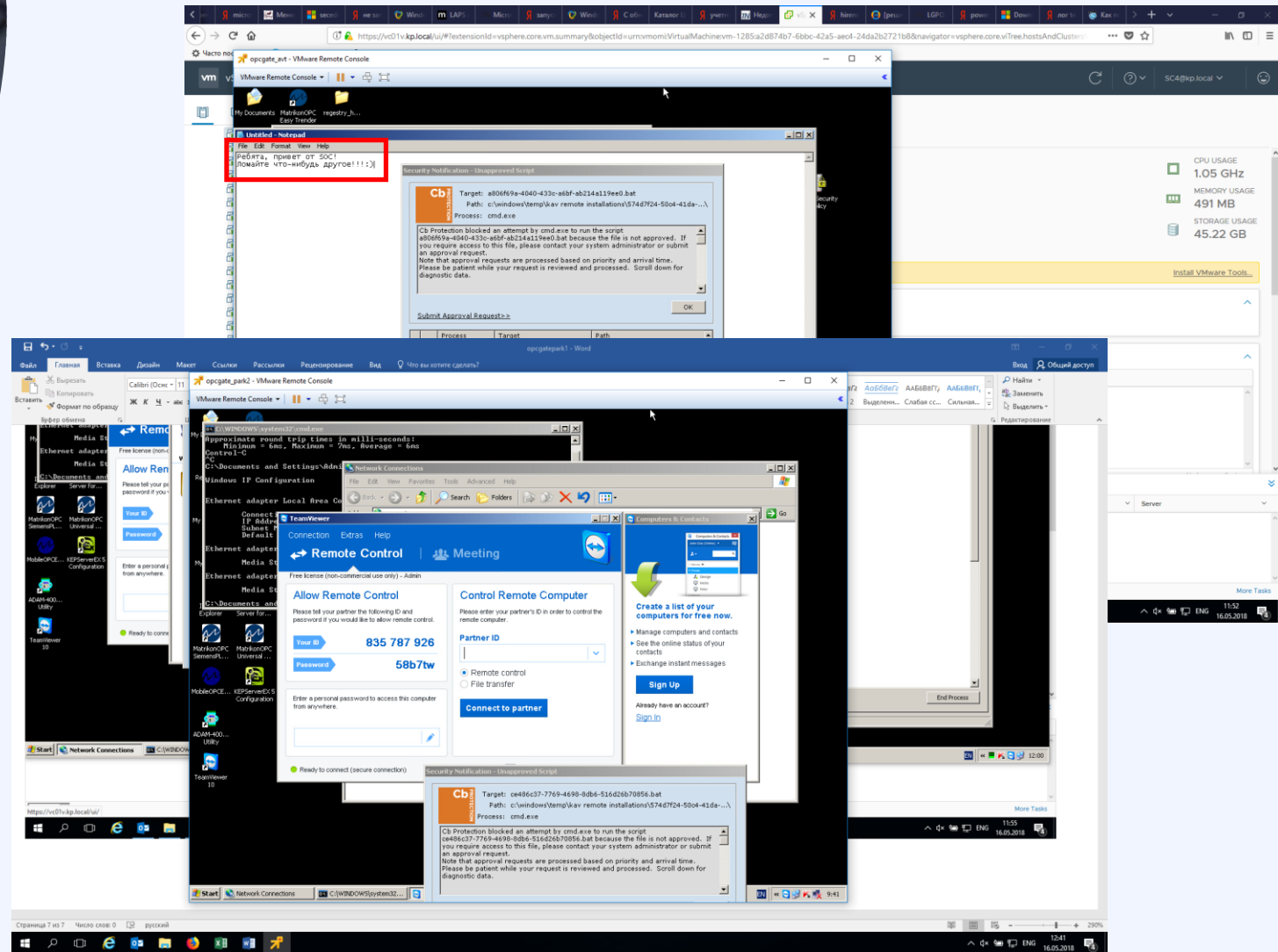


PROOF FROM PHD





PROOF
FROM PHD



ЦИБ: ANTI-APT



Статус 4 Stars Expert Partner от Check Point
Специализация по Check Point SandBlast



Gold Status- Q2 2018



Gold Status



Gold Status
Platinum-2018



Gold Status
IBM-дистрибьютор



Platinum Status

КОРОТКО О ГЛАВНОМ



- К АPT можно отнести довольно много **новых парадигм** (IoT/майнинг/BEC)
- Проблема **нехватки специалистов** в области ИБ
- ANTI-APT — это не только «песочница», а **комплексный проект по ИБ**
- **Своевременное обновление** внедренного решения



31/05/2018

СПАСИБО ЗА ВНИМАНИЕ!

**Александр
Русецкий**

Руководитель направления по защите от направленных атак
as.rusetskiy@jet.su / +7 926 156-81-25