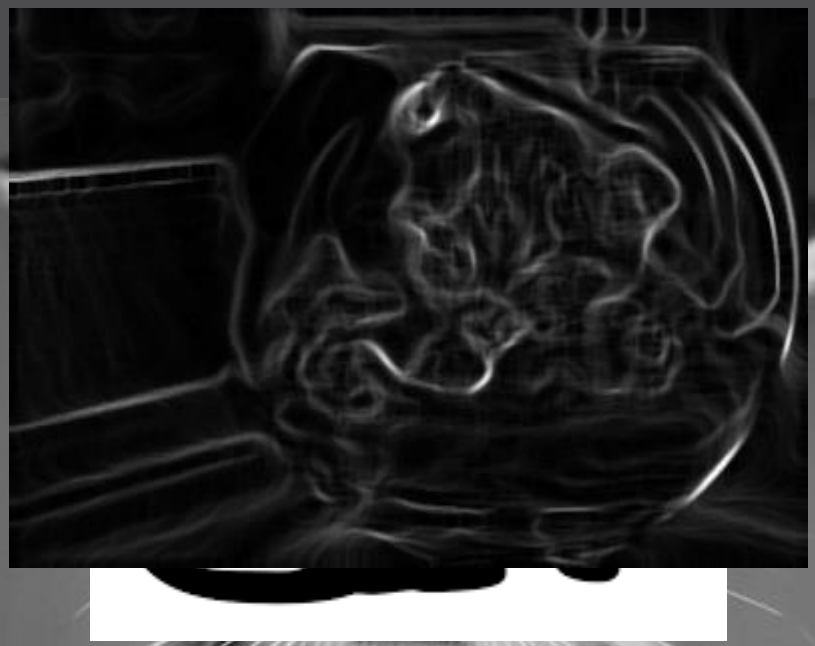
Check Point
SOFTWARE TECHNOLOGIES LTD.

МЕТОДЫ ПРЕДОТВРАЩЕНИЯ ДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА

Anatoly Viklov
Check Point Russia
Check Point. Информационная безопасность: диалог с медиа-рынком

К истокам...

Полиморфизм



Метаморфизм

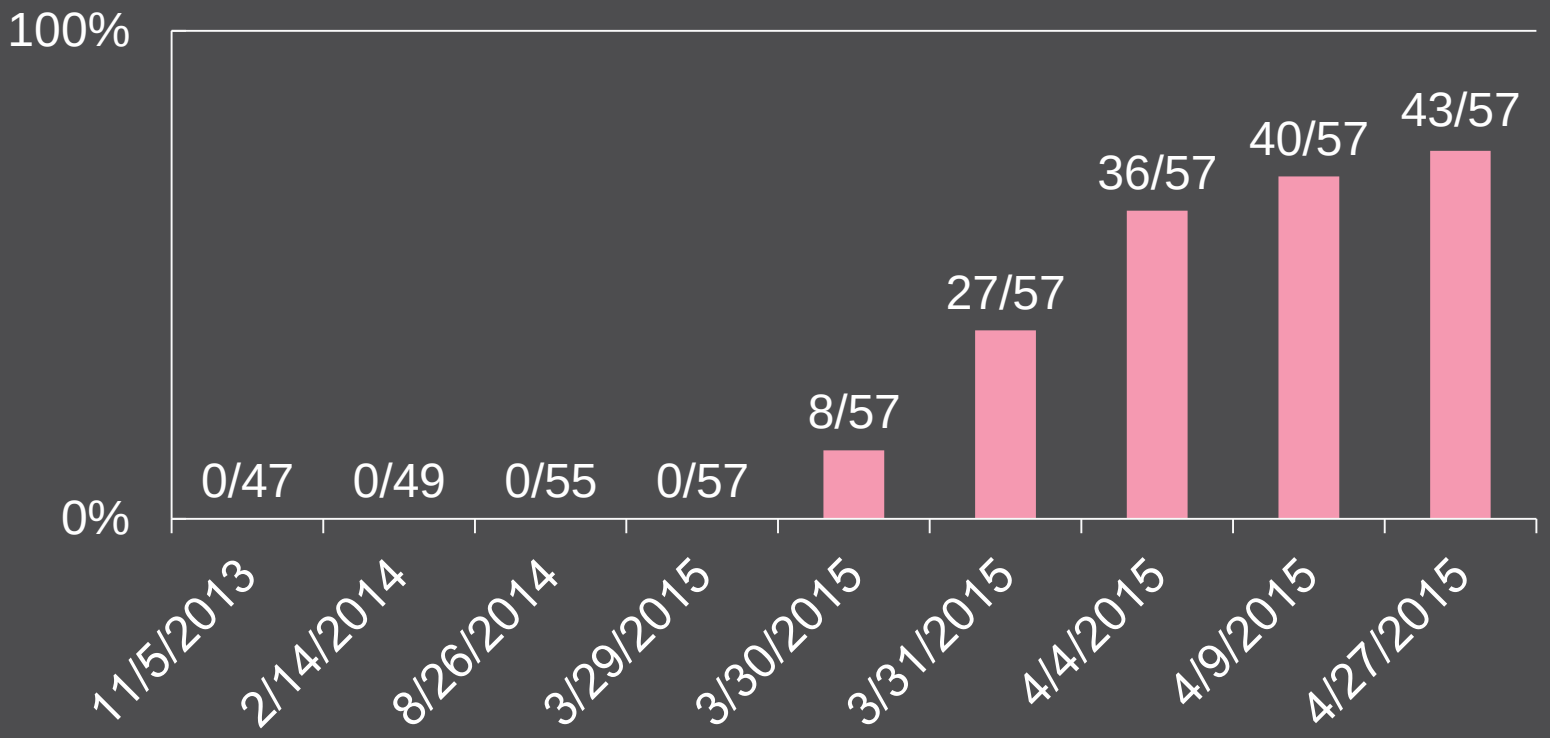
Пример 2015 года: Троян ‘EXPLOSIVE’

- Функционал
  - Цель – операционная система MS Windows
  - Предоставляет атакующему удаленный доступ
  - Автоматическое инфицирование съемных дисков USB
  - Динамически обновляемая информация о C&C серверах
  - Мониторинг CPU и оперативной памяти
- Псевдо-**Метаморфизм**

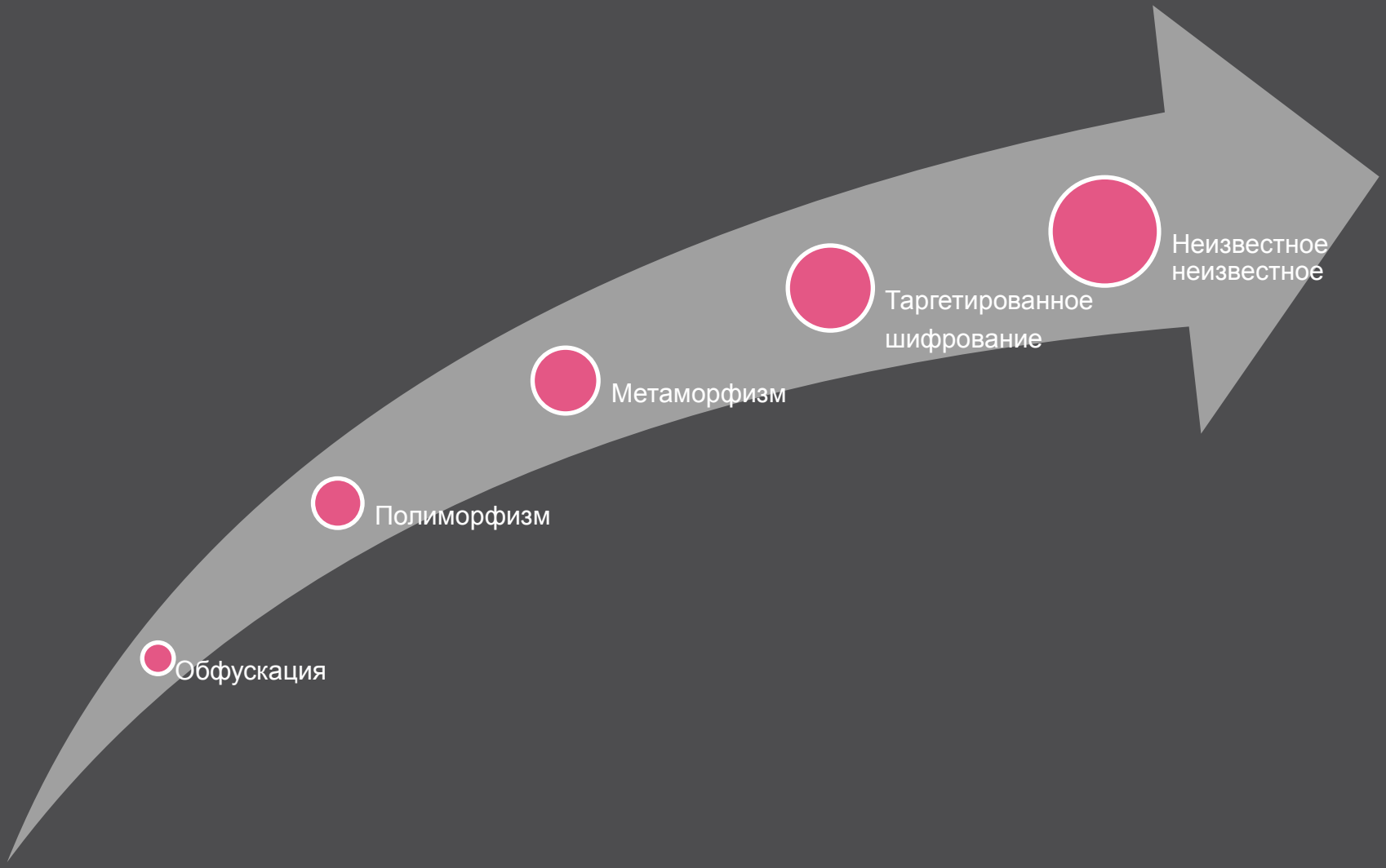
Создан не скрипт-кидди, но и не асами...

Временная шкала детектирования

0008065861f5b09195e51add72dacd3c4bbce6444711320ad349c7dab5bb97fb



Эволюционирование техник обхода вредоносным ПО



Сейчас наиболее эффективное решение -

Песочница

Безопасная среда для исследования ПО

Классическая песочница
Принцип работы

Эмуляция запуска в защищенной среде

Мониторинг:

- Системный реестр
- Сетевые соединения
- Активность файловой системы
- Системные процессы и сервисы

Отслеживание признаков,типичных для вредоносного ПО

Песочницу сложно обойти, НО...

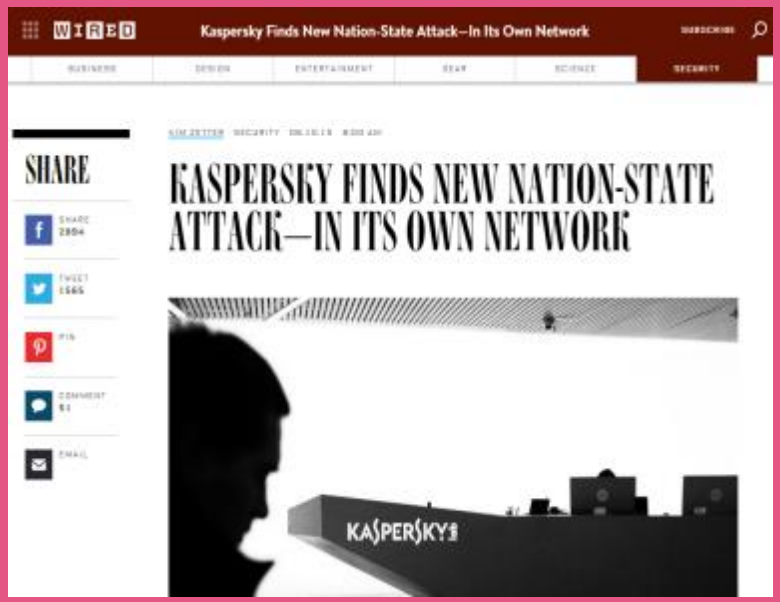
Check Point
SOFTWARE TECHNOLOGIES LTD.

Злоумышленники разрабатывают техники обхода:

- Детектирование вредоносным ПО виртуальных сред
- Задержка атаки…
  по времени или действию пользователя
- Проверка версии ОС и ПО
- Использование защищенных каналов связи

Спрячь на самом видном месте
Пример ЗАО «Лаборатория Касперского»

- Отсутствие вредоносного ПО на жестких дисках зараженных станций
- Размещение кода ТОЛЬКО в оперативной памяти
- После перезагрузки повторное инфицирование с других зараженных станций ЛВС



Source: Wired Magazine

Оставаться на шаг впереди

Представляем

Эффективно **Проактивно** **Управляемо**

Что такое SANDBLAST?

Беспрецедентная защита в реальном времени от неизвестного вредоносного ПО, 0-day уязвимостей и таргетированных атак

CHECK POINT
SandBlast™
ZERO-DAY PROTECTION

Песочница

Устойчивое к попыткам обхода решение

Threat Extraction

Мгновенная доставка гарантированно безопасных вложений

Цепочка атаки

Идентификация на уровне эксплойта - мы на шаг впереди

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT SandBlast™ ZERO-DAY PROTECTION

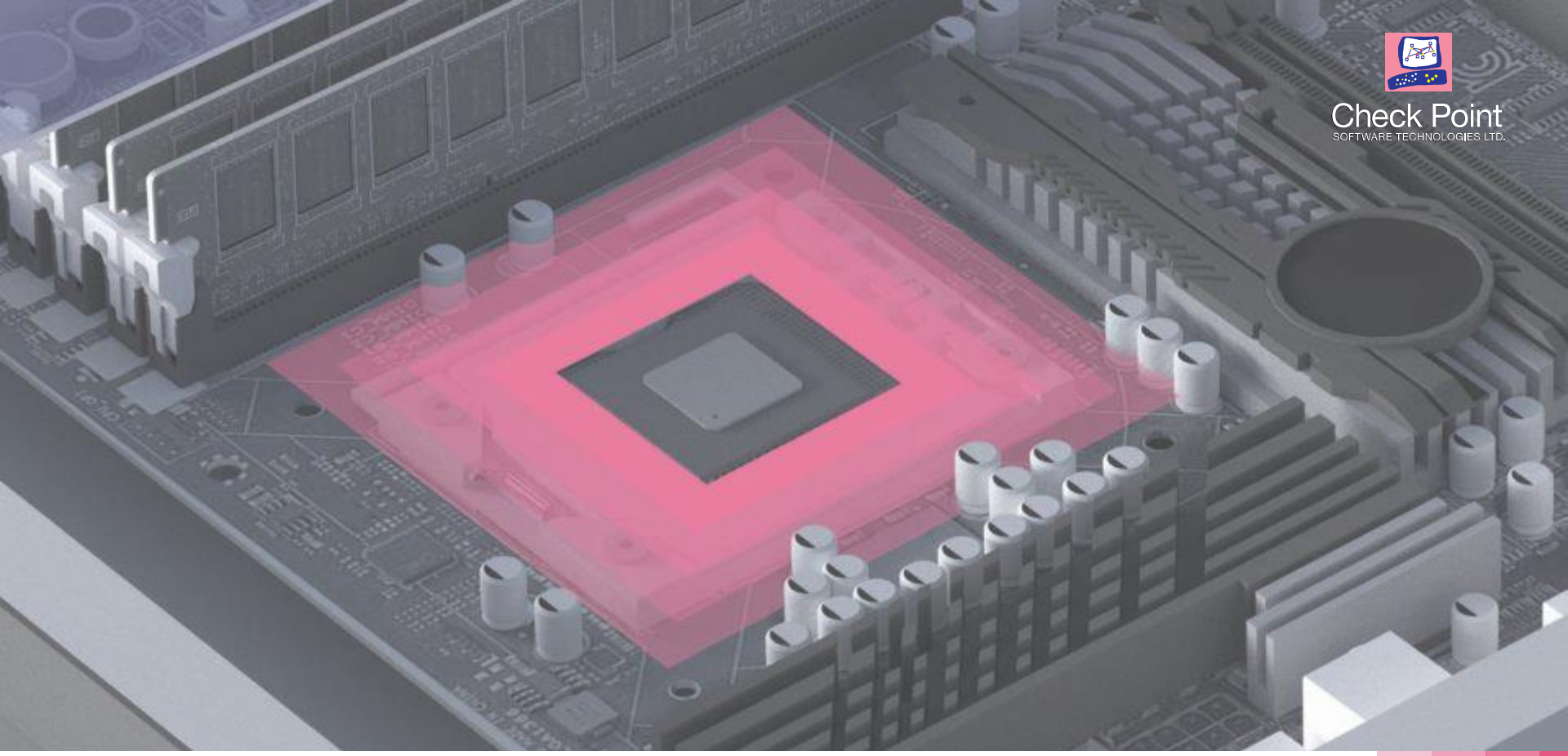
Традиционная песочница

Оставаясь на шаг впереди

Детектирование на уровне CPU

Детект вредоноса до попытки обхода

Что такое гаджет?



Check Point
SOFTWARE TECHNOLOGIES LTD.

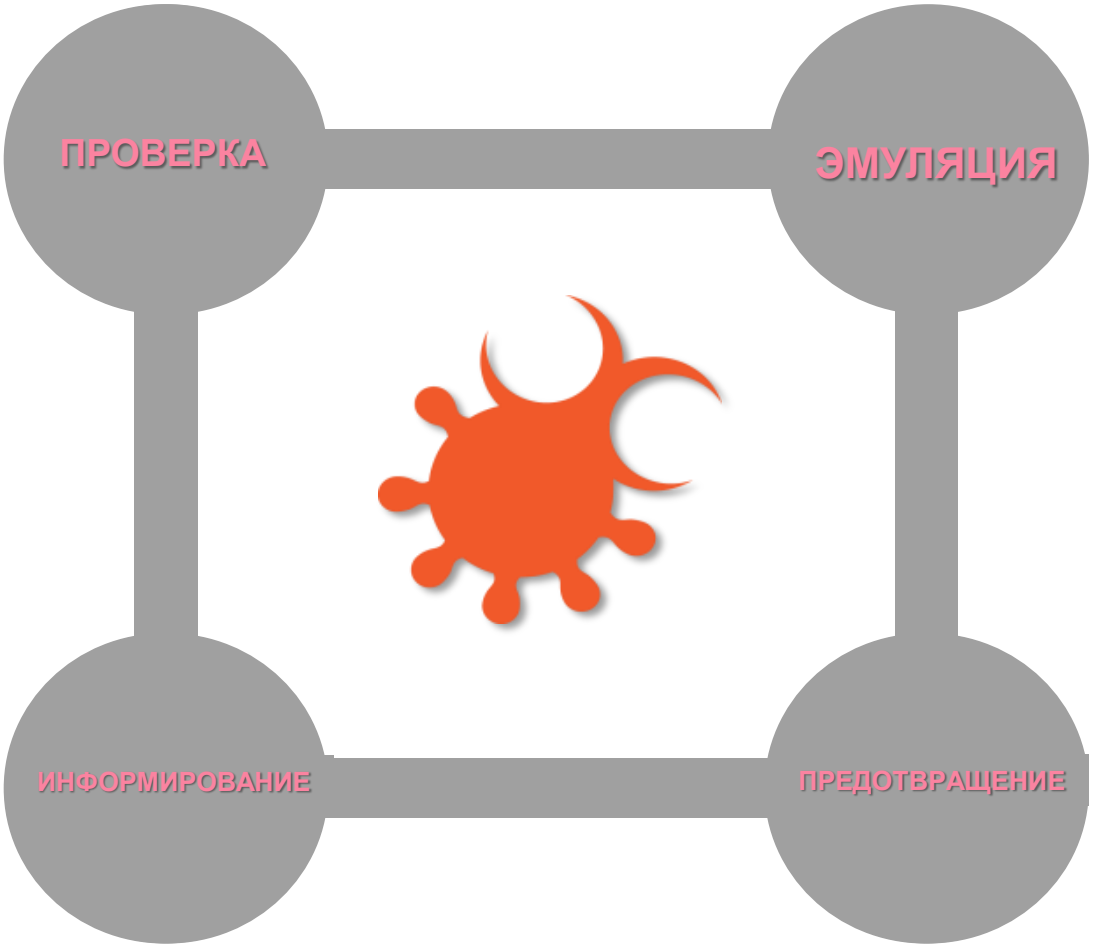
Детект эксплойтов на уровне CPU

- Высочайший уровень детектирования
- Устойчив к обходу
- Эффективен и быстр
- **Только от Check Point!**

THREATCLOUD

Эмуляция в облаке

Эмуляция на устройстве



Check Point
SOFTWARE TECHNOLOGIES LTD.

Защита от неизвестных атак с помощью Check Point Threat Emulation

Определение файлов во вложениях и при скачивании с WEB

Загрузка файлов в виртуальный ПАК (локально или в облаке)

ПРОВЕРКА

exe,pdf,MS Office, flash, jar etc…

Check Point
SOFTWARE TECHNOLOGIES LTD.

Эмуляция файла в разных ОС

Windows XP&7

Файл открывается и происходит анализ поведения

ЭМУЛЯЦИЯ

Мониторинг поведения:

- Файловая система
- Системный реестр
- Сетевые подключения
- Системные процессы

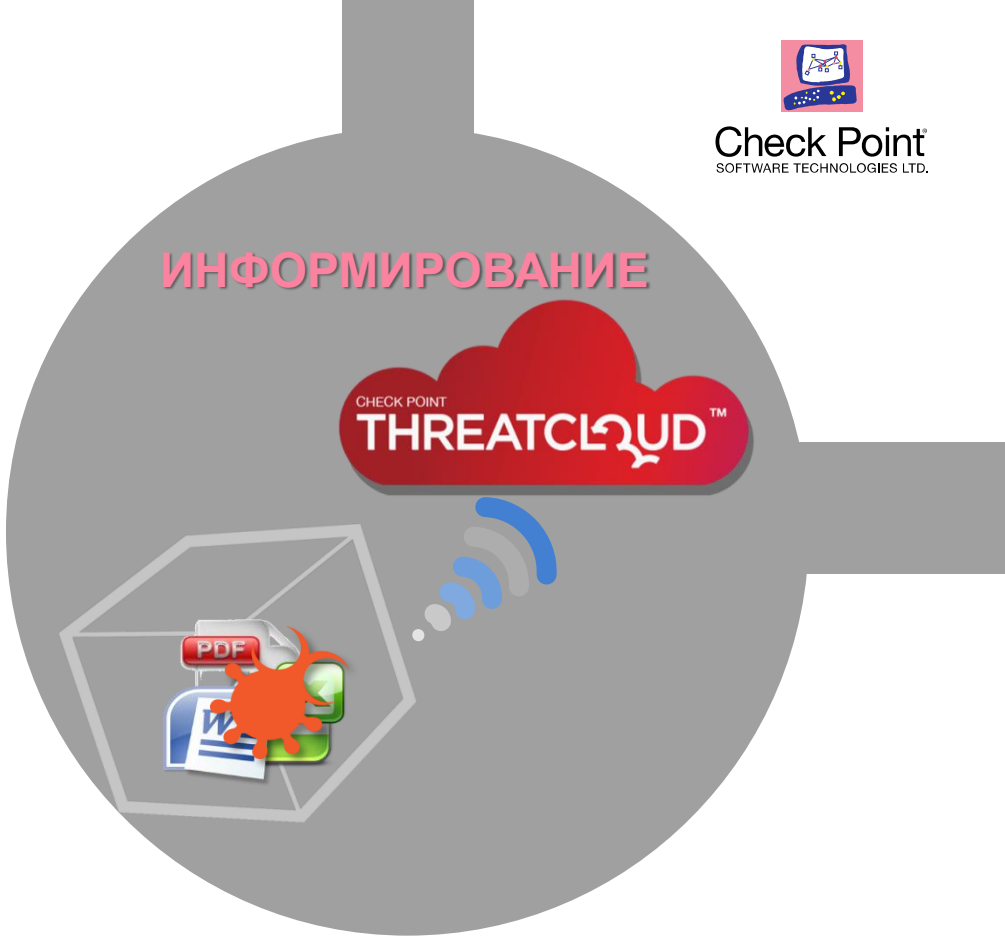
ПРЕДОТВРАЩЕНИЕ

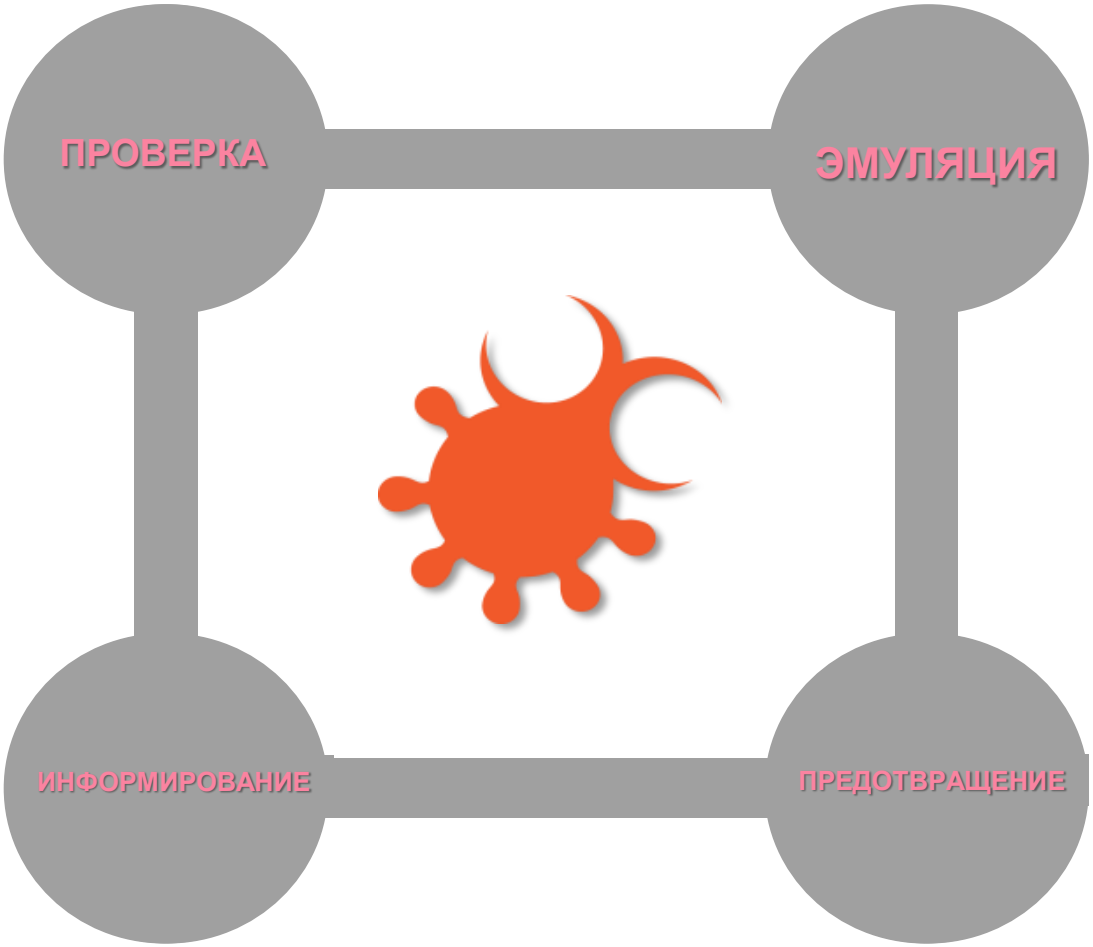
Шлюз безопасности

Уникально

Блокировка вредоносных файлов в реальном времени

Обновление для всех шлюзов

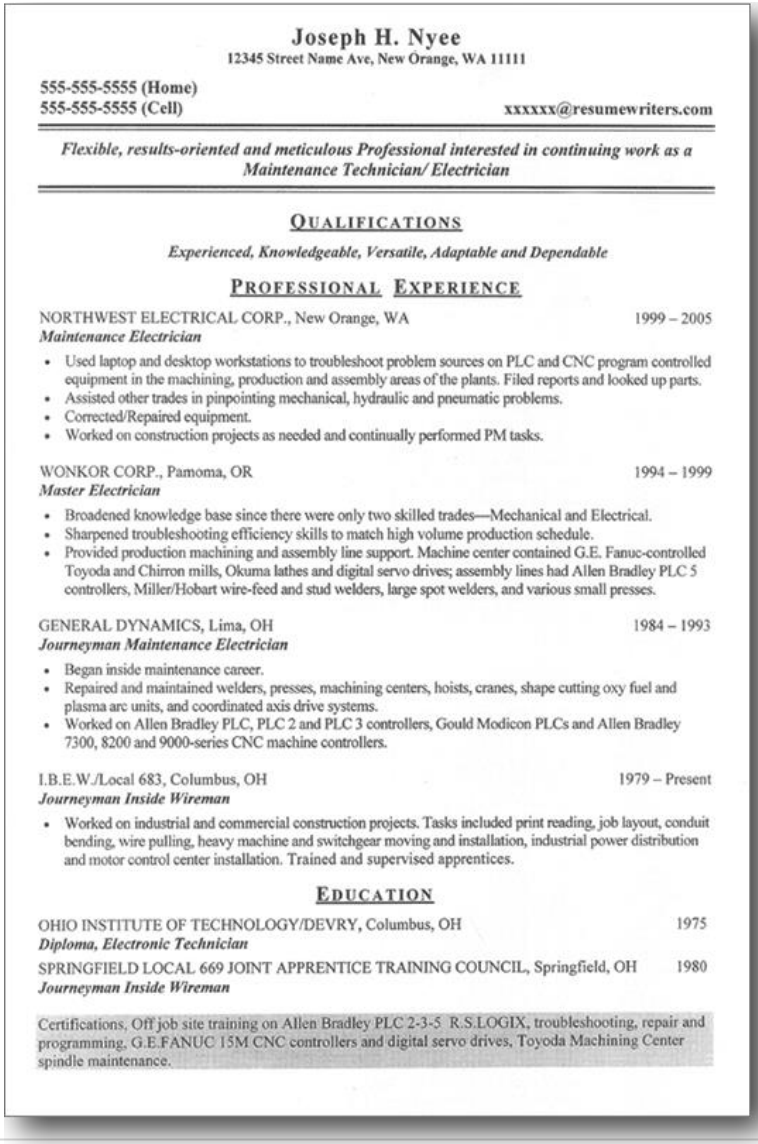




Защита от неизвестных атак с помощью

Check Point Threat Emulation

Threat Emulation за работой



Joseph H. Nyee
12345 Street Name Ave, New Orange, WA 11111

555-555-5555 (Home)
555-555-5555 (Cell)
xxxxxx@resumewriters.com

Flexible, results-oriented and meticulous Professional interested in continuing work as a Maintenance Technician/ Electrician

QUALIFICATIONS

Experienced, Knowledgeable, Versatile, Adaptable and Dependable

PROFESSIONAL EXPERIENCE

NORTHWEST ELECTRICAL CORP., New Orange, WA 1999 – 2005
Maintenance Electrician

- Used laptop and desktop workstations to troubleshoot problem sources on PLC and CNC program controlled equipment in the machining, production and assembly areas of the plants. Filed reports and looked up parts.
- Assisted other trades in pinpointing mechanical, hydraulic and pneumatic problems.
- Corrected/Repaired equipment.
- Worked on construction projects as needed and continually performed PM tasks.

WONKOR CORP., Pamoma, OR 1994 – 1999
Master Electrician

- Broadened knowledge base since there were only two skilled trades—Mechanical and Electrical.
- Sharpened troubleshooting efficiency skills to match high volume production schedule.
- Provided production machining and assembly line support. Machine center contained G.E. Fanuc-controlled Toyoda and Chirron mills, Okuma lathes and digital servo drives; assembly lines had Allen Bradley PLC 5 controllers, Miller/Hobart wire-feed and stud welders, large spot welders, and various small presses.

GENERAL DYNAMICS, Lima, OH 1984 – 1993
Journeyman Maintenance Electrician

- Began inside maintenance career.
- Repaired and maintained welders, presses, machining centers, hoists, cranes, shape cutting oxy fuel and plasma arc units, and coordinated axis drive systems.
- Worked on Allen Bradley PLC, PLC 2 and PLC 3 controllers, Gould Modicon PLCs and Allen Bradley 7300, 8200 and 9000-series CNC machine controllers.

I.B.E.W./Local 683, Columbus, OH 1979 – Present
Journeyman Inside Wireman

- Worked on industrial and commercial construction projects. Tasks included print reading, job layout, conduit bending, wire pulling, heavy machine and switchgear moving and installation, industrial power distribution and motor control center installation. Trained and supervised apprentices.

EDUCATION

OHIO INSTITUTE OF TECHNOLOGY/DEVRY, Columbus, OH 1975
Diploma, Electronic Technician

SPRINGFIELD LOCAL 669 JOINT APPRENTICE TRAINING COUNCIL, Springfield, OH 1980
Journeyman Inside Wireman

Certifications, Off job site training on Allen Bradley PLC 2-3-5 R.S.LOGIX, troubleshooting, repair and programming, G.E.FANUC 15M CNC controllers and digital servo drives, Toyoda Machining Center spindle maintenance.

Выглядит как обычное резюме?

Threat Emulation за работой

Check Point
SOFTWARE TECHNOLOGIES LTD.

Некорректная файловая активность

9 Affected Files

3 Files Created | 8 Files Modified | 1 File Deleted

C:\Documents and Settings\All Users\Application Data\google\googleservic
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googles
C:\Documents and Settings\admin\Application Data\google\googleservice.c

Операции с процессами

4 Affected Processes

4 Processes Created | 1 Process Terminated |

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\googleservice.exe
C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files\Internet Explorer\iexplore.exe

Операции с системным реестром

31 Affected Registry Keys

31 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placemen
HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites
HKCU\Software\Microsoft\Internet Explorer\Toolbar\Locked

Сетевая активность

1 Attempted Network Connections

winssl.dyndns.org

HKCU\Software\Microsoft\Direct3D\MostRecentApplication\Name
HKCU\Software\Microsoft\Internet Explorer\Main\Window_Placement
HKCU\Software\Microsoft\Internet Explorer\Security\P3Sites
winssl.dyndns.org

Файловая активность | Системный реестр | Системные процессы | Сетевые соединения

E-mail От миссис Мира

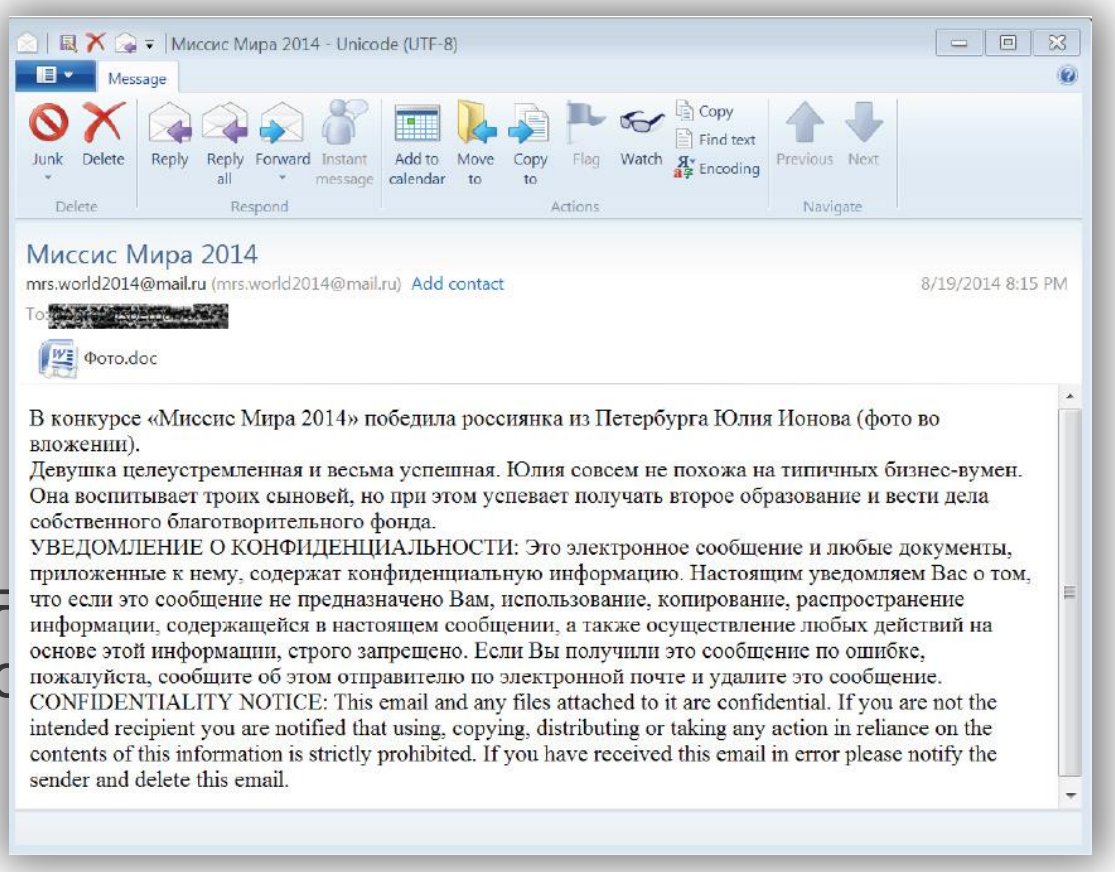
Таргетированная атака 2014 года

ЦЕЛИ:

Российские и европейские организации

МЕТОД:

Точечная фишинговая рассылка с эксплойто в формате MS Word

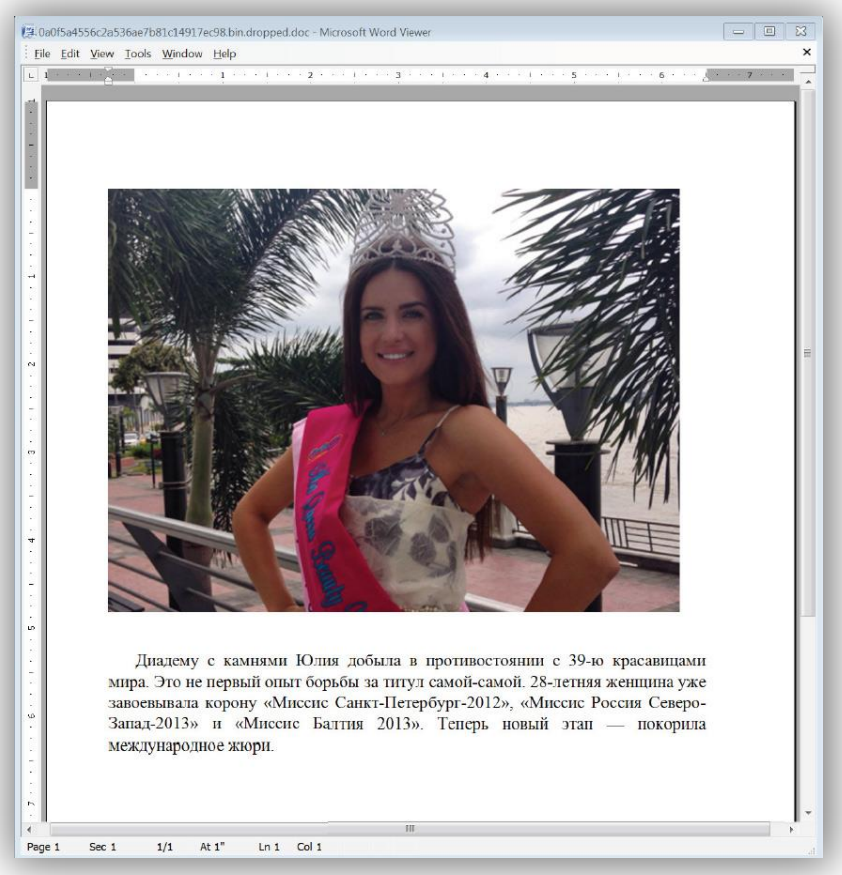


Вредоносный документ

RETURN ORIENTED PROGRAMMING (ROP) EXPLOIT

Использование
новой уязвимости
MS word (CVE-2012-0158)

- Отсылал системную информацию в командный центр
- Скачивал и устанавливал дополнительные модули для управления
- Шифровал и отправлял конфиденциальные данные в командный центр



Традиционная песочница – традиционные задержки

ПРОВЕРКА ЗАНИМАЕТ ВРЕМЯ

- Как результат, во многих инсталляциях песочницы не используются в режиме блокировки
- Вредоносный файл может попасть к пользователю, пока находится в очереди для проверки

SANDBLAST THREAT EXTRACTION

Check Point
SOFTWARE TECHNOLOGIES LTD.

Упреждающая защита

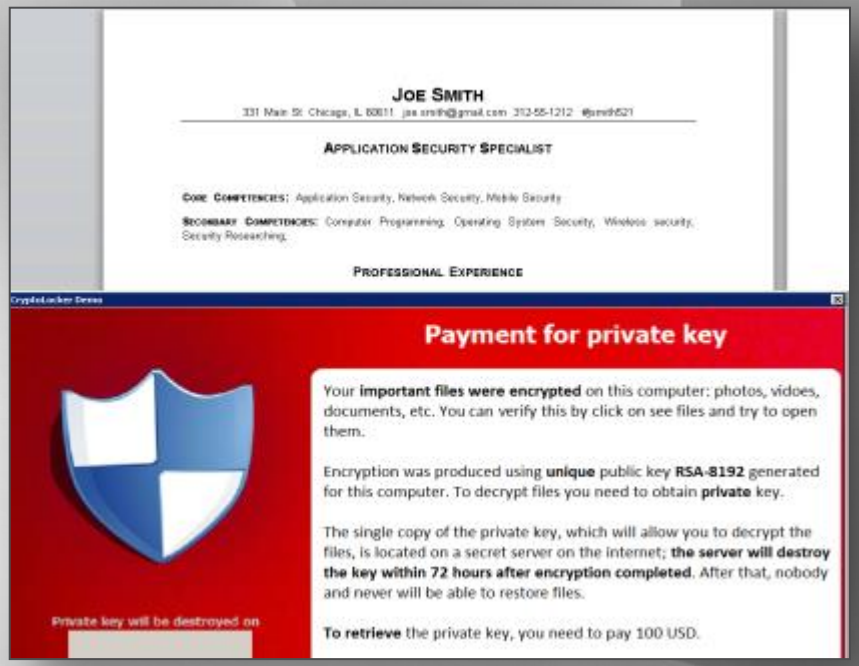
- Немедленный доступ
- Не детект, но упреждающая защита
- Попытки атаки очевидны

Доставляем гарантированно безопасные файлы

Check Point
SOFTWARE TECHNOLOGIES LTD.

Без нас

Инфекция



С нами

Вредоносный код удален

Check Point
SOFTWARE TECHNOLOGIES LTD.

Избавим от будущих заражений уже сейчас!

ВЫСОЧАЙШИЙ УРОВЕНЬ ДЕТЕКТА
МГНОВЕННАЯ ДОСТАВКА БЕЗОПАСНОГО КОНТЕНТА

Check Point
SOFTWARE TECHNOLOGIES LTD.

СПАСИБО!