JET CONFERENCE

# Успешность противостояния комбинированным атакам нулевого дня – есть ли шансы?

Николай Романов / Архитектор решений

# Shadow Brokers launch subscription service for stolen exploits, zero-day leaks

The cyberattackers are demanding $23,000 every month for access to the cache of stolen vulnerabilities.

By Charlie Osborne for Zero Day | May 31, 2017 -- 09:16 GMT (02:16 PDT) | Topic: Security

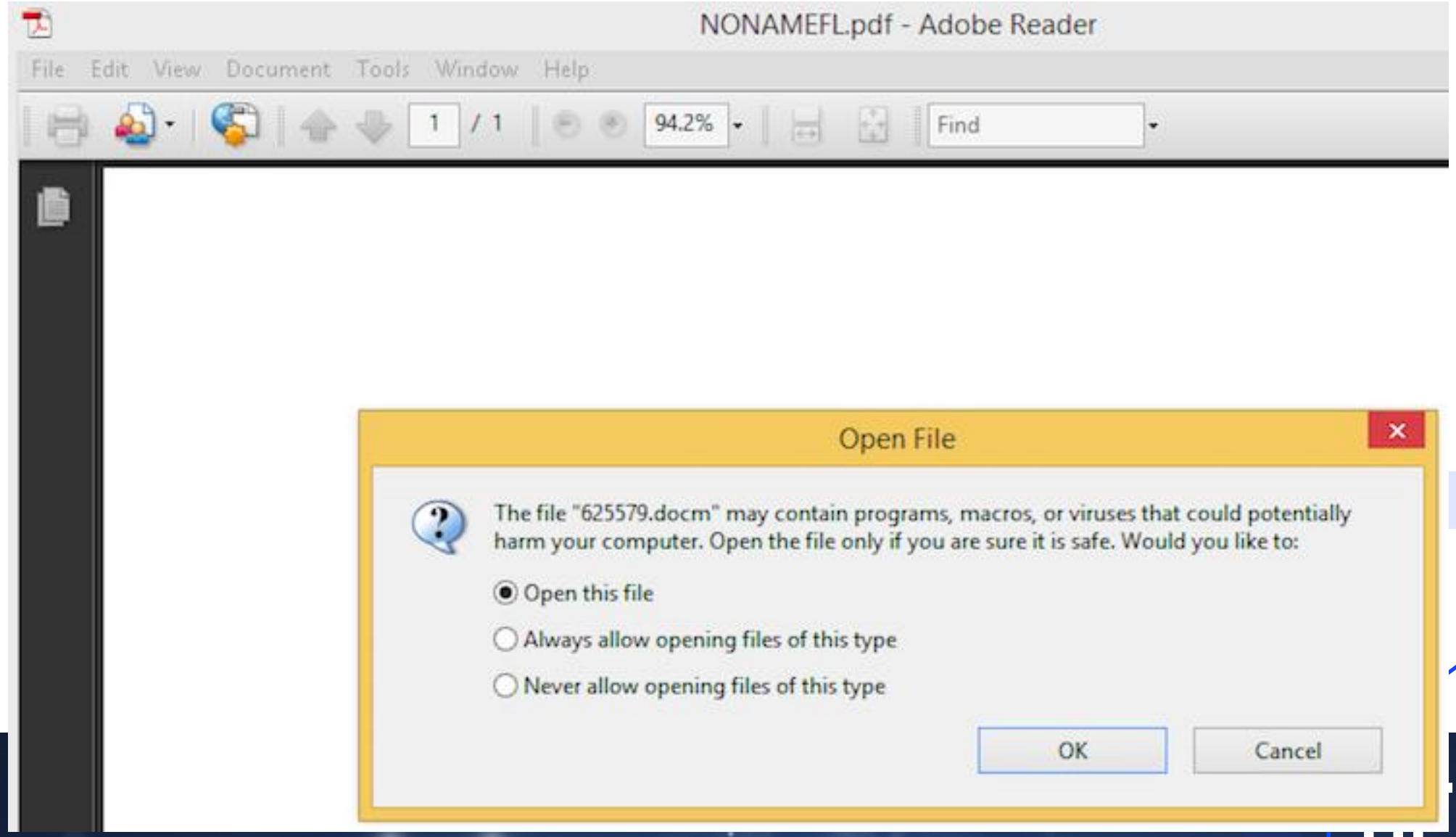
The mysterious group that over the past nine months has leaked millions of dollars' worth of advanced hacking tools developed by the National Security Agency said Tuesday it will release a new batch of tools to individuals who pay a $21,000 subscription fee. The plans, announced in a cryptographically signed post published Tuesday morning, are generating an intense moral dilemma for security professionals around the world.

**Source: ZDNet, Arstechnica**

# Некоторые факты по вымогателям

- **FBI зафиксировал 992 обращений по CryptoWall между апрелем 2014 и июнем 2015.**
  - **Требования варьировались от $200 до $10k**
  - **По статистике Trend Micro требования были в диапазоне $20-600**
- **Что относительно нового зафиксировано**
  - **Teslacrypt: 0-day & exploit kit**
  - **Ransom32: JavaScript**
  - **Petya: нацеленность на MBR**
  - **Jigsaw: игры**
  - **Lucky: DOC в PDF**
  - **Powerware: powershell**

# Некоторые факты по вымогателям – Lucky (Q2'2017)



# Что чаще всего видим..

- Cobalt Strike; Empire Powershell
- Mimikatz
- PS Keylogger
- Утилиты RC
- +некоторые нестандартные инструменты… ☹

# Еще раз про Wcry и PowerShell…

| | | | |
|---|---|---|---|
| CVE-2017-0144 - Remote Code Execution - SMB (Request) | | SMB | High |
| CVE-2017-0144 - Remote Code Execution - SMB (Request) | | SMB | High |
| CVE-2017-0144 - Remote Code Execution - SMB (Request) | | SMB | High |
| CVE-2017-0144 - Remote Code Execution - SMB (Request) | | SMB | High |
| EQUATED - SMB (Response) | | SMB | High |
| EQUATED - SMB (Response) | | SMB | High |
| CVE-2017-0144 - Remote Code Execution - SMB (Request) | | SMB | High |
| Possible HTA PowerShell Empire (Request) | | HTTP | Low |

# Почему PowerShell?...


```
agents          injectshellcode  psinject        sleep
back            jobs             pth             spawn
bypassuac       kill             rename          steal_token
clear           killdate         revtoself       sysinfo
creds           list             sc              updateprofile
download        listeners        scriptcmd       upload
exit            lostlimit        scriptimport    usemodule
help            main             searchmodule    workinghours
info            mimikatz         shell
```

# Предлагаемые меры*

Обнаружение: идентификация неизвестного ВПО/контента **и подозрительной сетевой активности, раскрывающей характерные черты проводимой атаки**

Защита: блокирование целевого фишинга и активностей, связанных с 0-day контентом ну уровне сети (отклики, распространение/перемещение…)

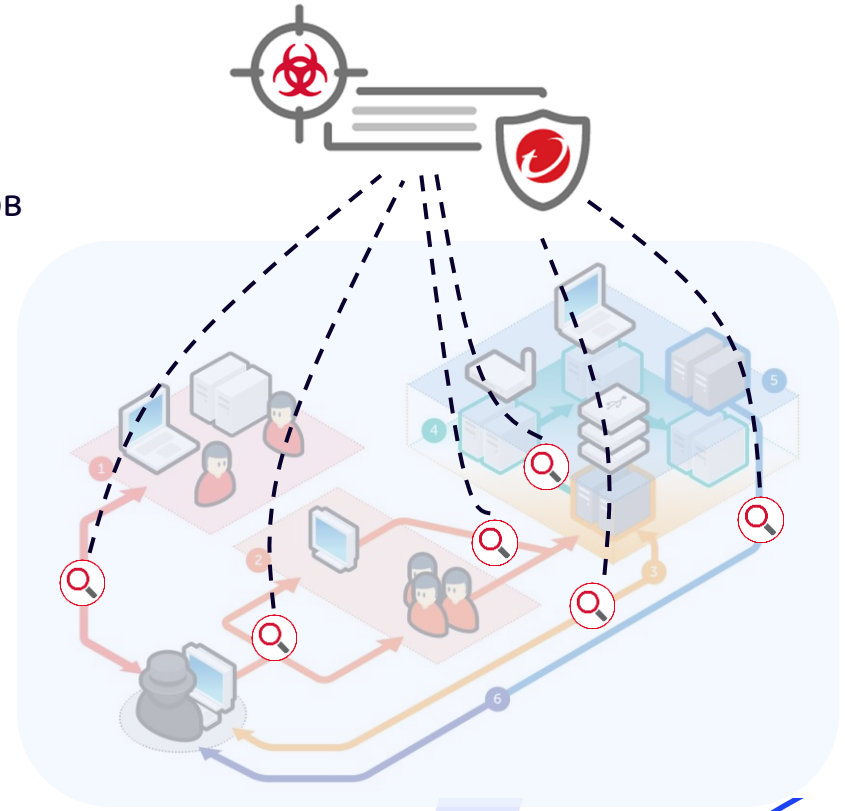
Объединение Threat Intelligence: решение, интегрированное с почтовым шлюзом и другими системами защиты для выявления фишинга и 0-day

ROI: соизмеримые затраты и практическая польза от внедрения (соотношение рисков и их стоимости по отношению к приобретаемому решению)

*Verizon 2016 Data Breach Investigations Report page 33

# Более технически

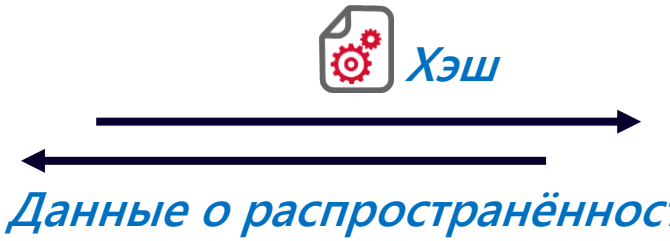
- Идентификация сетевой сессии
  - Выявлять соответствие порта протоколу
  - Отслеживать TCP сессии и пересбор фрагментированных фреймов
- Выявление подозрительной и опасной сетевой активности
  - Известный вредоносный трафик на основе уже имеющихся данных (репутация)
  - Распространение ВПО внутри сети предприятия
  - Выявление использования эксплойтов по сети
  - Подозрительный поток в составе легитимного трафика
- Отслеживание всей цепочки многоэтапной атаки по различным идентификаторам сетевой активности
  - Загрузки/целевой фишинг
  - C&C / отправка данных
  - Внутрисетевое перемещение & и разведка



# Что также учитывать

## 99% ВПО затрагивают менее 10 АРМ

- Зная данные о распространённости и зрелости (сроке жизни) файла, можно сделать определенные выводы
- Чем больше данных (сотни миллионов), тем больше шансов различить ВПО среди новых бинарников
  - Один из способов выявления полиморфов
- Появление неизвестного бинарника может сигнализировать о целевой атаке
- Машинные методы обучения могут использовать эти данные



JET CONFERENCE

1/06/2017

# ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!