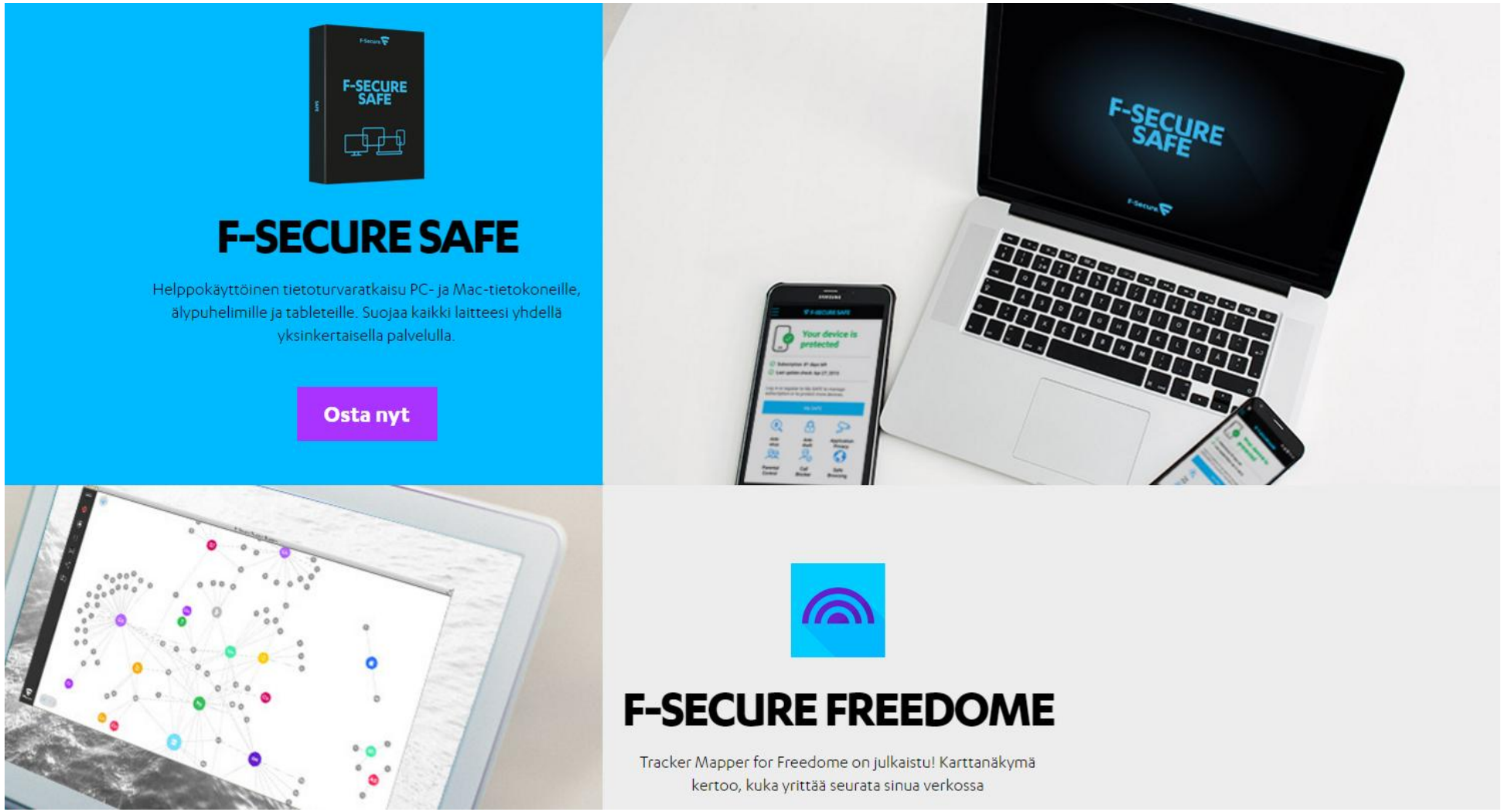
Анатомия APT (Advanced Persistent Threats)

Дмитрий Комашинский

Senior Researcher, F-Secure Labs

Пара слов о моей компании и себе



A: ADVANCED

Сложный, **продвинутый**

Интерпретация:

1. Использование технологически нетривиальных, скрытных методов наблюдения, проникновения и сбора данных;
2. Сложность определения источника атаки, ее заказчика и мотивов;
3. Сложность оценивания последствий атаки и организации дальнейшего противодействия.

P: PERSISTENT

Существующий длительное время

Интерпретация:

1. Длительный период периода наблюдения, сбора и пересылки информации (ergo, вредоносный код «живет» в периметре объекта атаки длительное время);
2. В процессе попыток начального проникновения, объект подвергается постоянно нарастающему давлению со стороны атакующего.

T: THREAT

Угроза, источник опасности

Интерпретация:

1. Вредоносная программа
2. Компьютерный злоумышленник
3. Правительственная или коммерческая организация, нацеленная на скрытный доступ к информации, составляющей государственную или коммерческую тайну

T: THREAT (2)

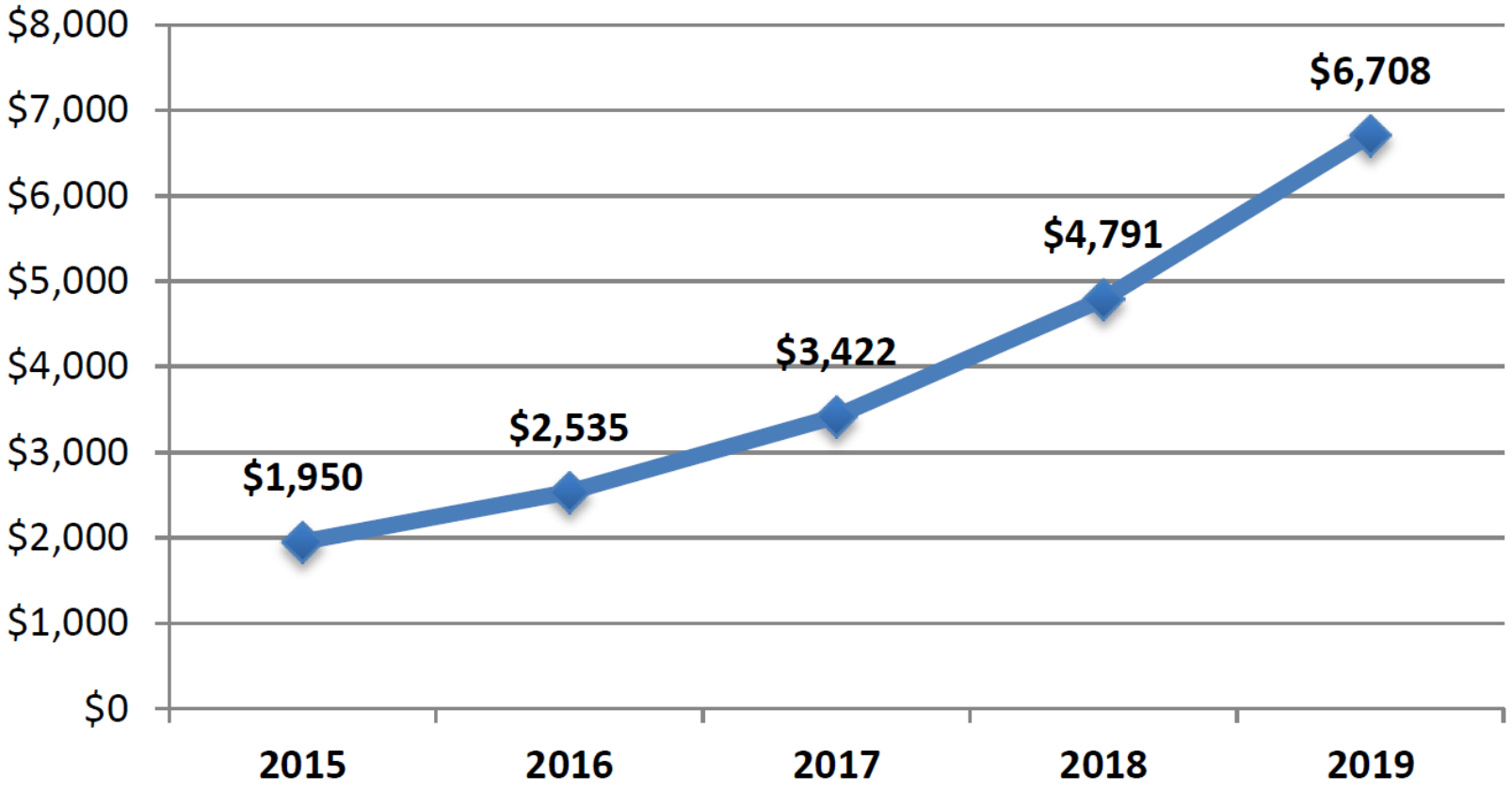
CHINA'S COMPUTER NETWORK OPERATIONS TASKING TO PLA UNIT 61398 (61398部队)

Our research and observations indicate that the Communist Party of China (CPC,中国共产党) is tasking the Chinese People's Liberation Army (PLA,中国人民解放军) to commit systematic cyber espionage and data theft against organizations around the world. This section provides photos and details of Unit 61398 facilities, Chinese references discussing the unit's training and coursework requirements, and internal Chinese communications documenting the nature of the unit's relationship with at least one state-owned enterprise. These details will be particularly relevant when we discuss APT1's expertise, personnel, location, and infrastructure, which parallel those of Unit 61398.

Emblem of the People's Liberation Army

Рынок средств противодействия APT

Финансовый прогноз (млрд. USD)



Рынок средств противодействия APT

Основные требования (1)

- Обнаружение ВП (статический, динамический анализ; оценка репутации, распространенности; эвристические средства);
- Сетевой экран, фильтрация URL;
- Защита почтовых и Web серверов, пользовательских клиентских приложений;
- Сканирование поверх SSL, анализ защищенного трафика;
- Средства форенсики и анализ уязвимостей нулевого дня;
- Изоляция приложений (карантин и песочницы).

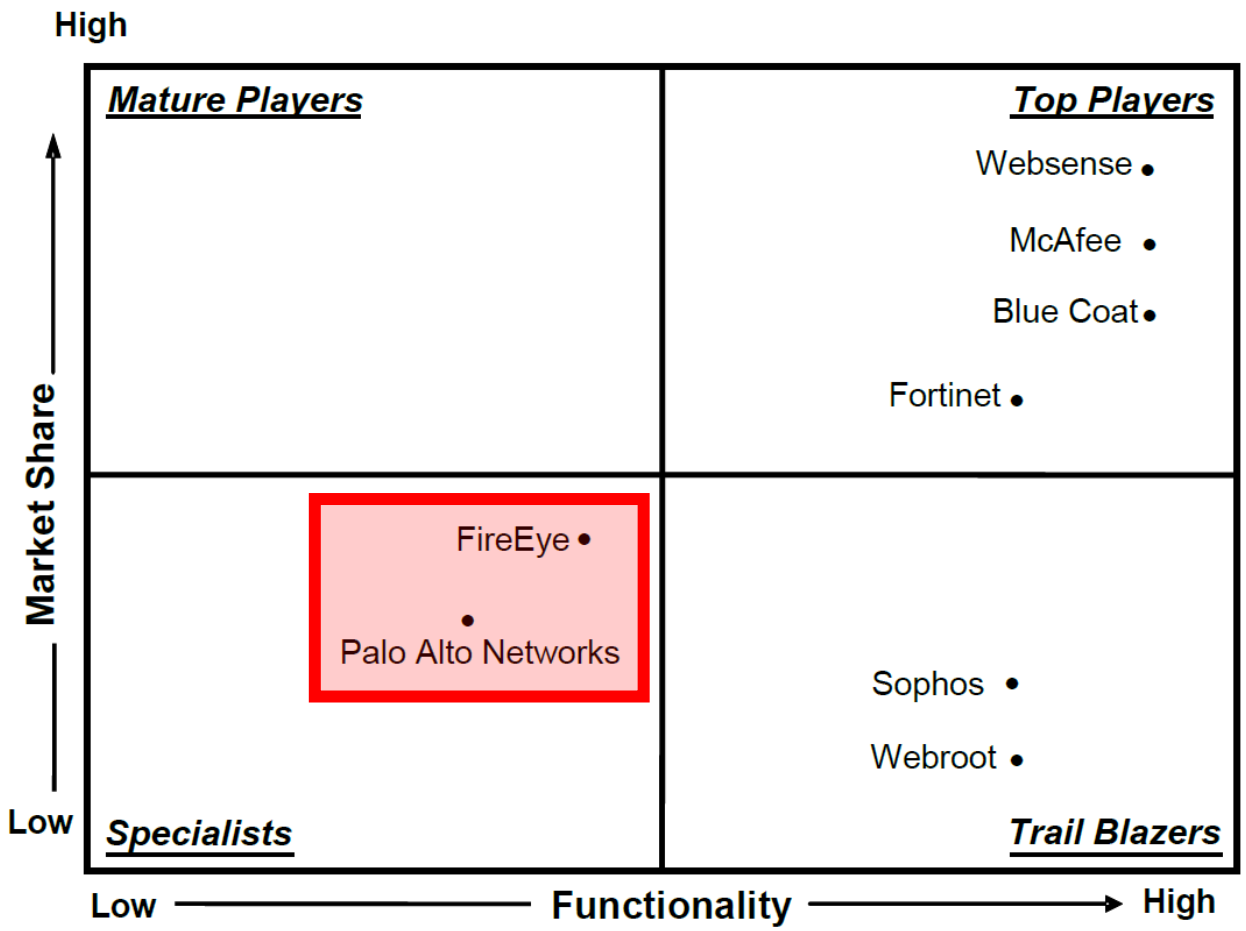
Рынок средств противодействия APT

Основные требования (2)

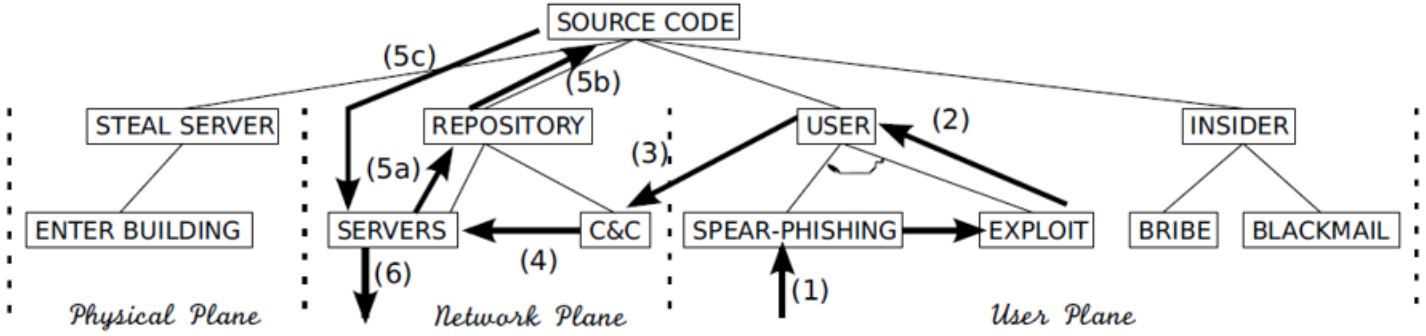
- Интеграция с Active Directory (LDAP);
- Средства противодействия утечкам информации (DLP);
- Защита мобильных устройств;
- Централизованное управление защиты сетевых ресурсов и пользователей;
- Обновления в реальном времени;
- Средства мониторинга и анализа состояния всей вычислительной среды для выявления атак и ее потенциально уязвимых элементов.

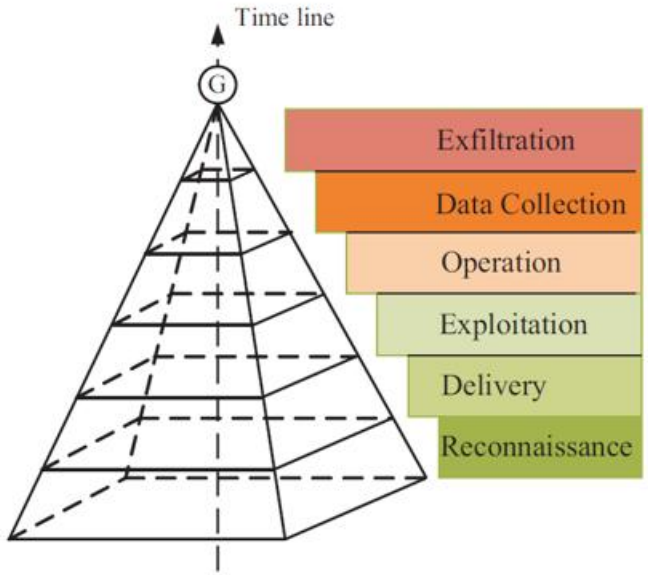
Рынок средств противодействия APT

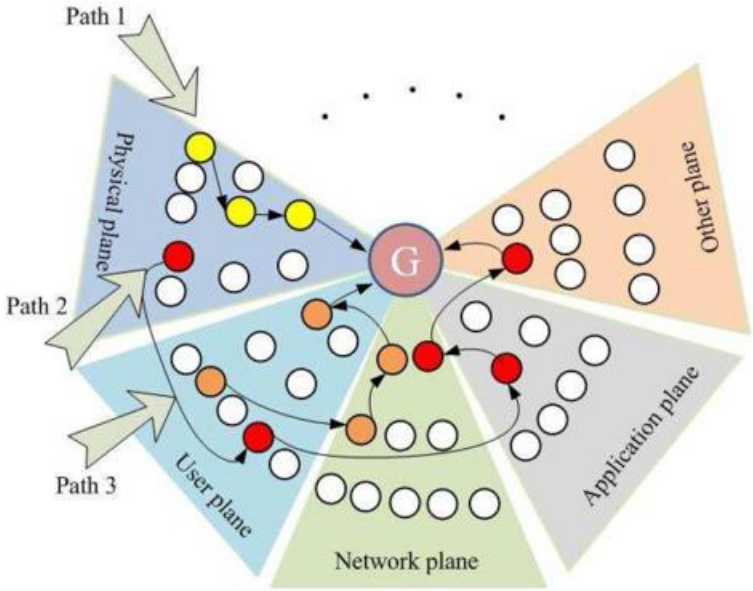
Основные игроки



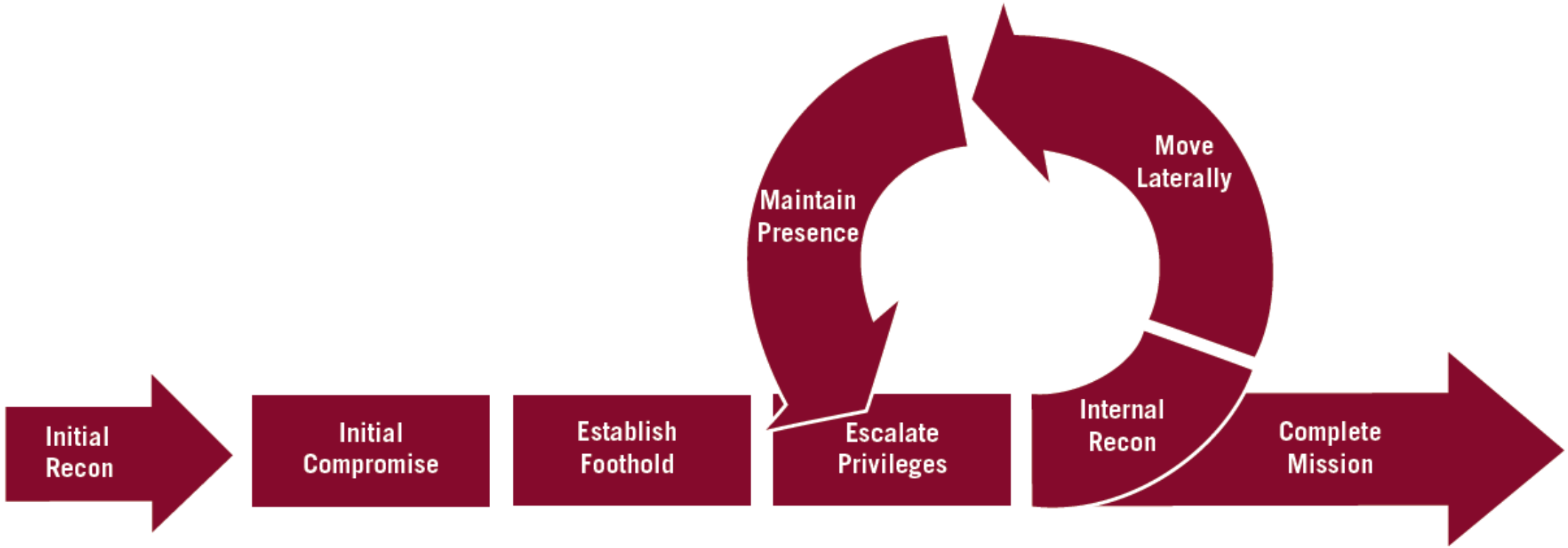
Варианты моделей APT (Giura & Wang)







Варианты моделей APT (FireEye)



Используемая модель APT

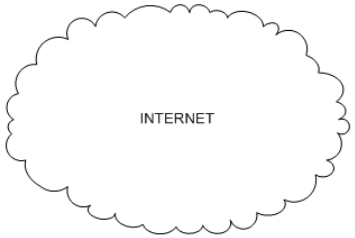
- Наблюдение (Reconnaissance aka Recon)
- Начальное проникновение (Exploit)
- Доставка основного функционала (APT kit delivery)
- Распространение (Lateral movements & privilege escalation)
- Сбор данных (Data collection)
- Копирование данных (Data exfiltration)

В описанной последовательности шагов возможны циклы.

Фаза наблюдения

C&C

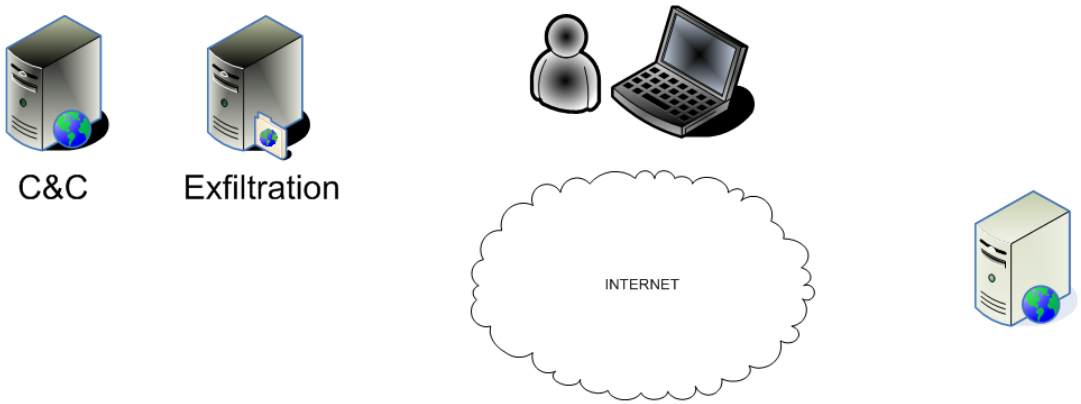
Exfiltration

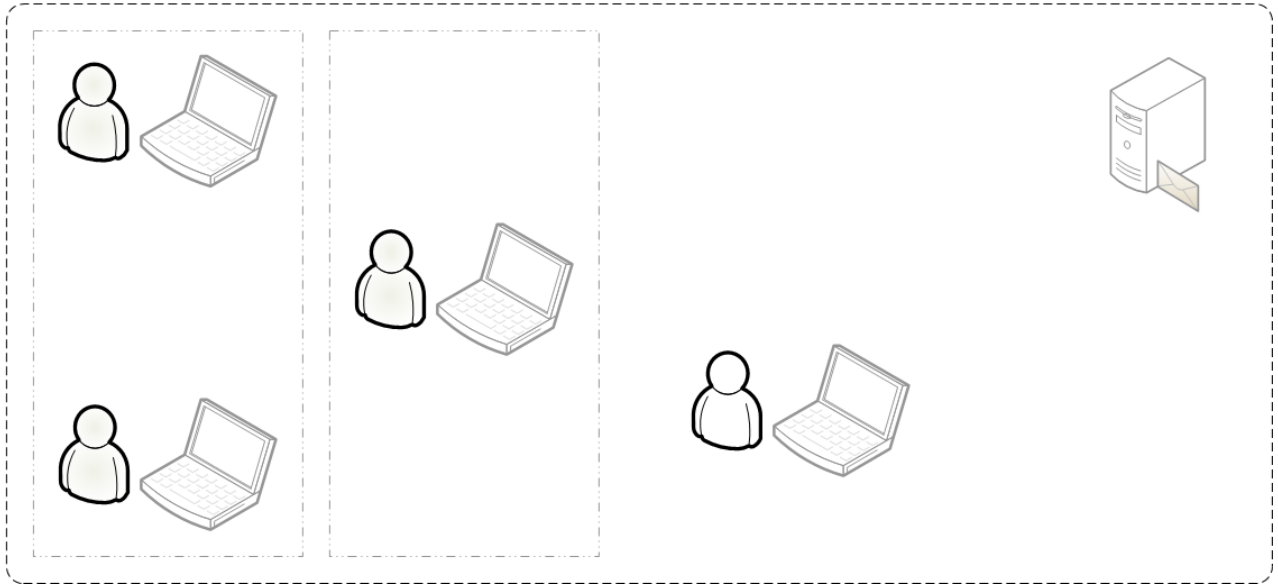


Цели фазы наблюдения

- Получение информации об объекте атаки
  - Данные о бизнес процессах
    - Перечень основных клиентов, субподрядчиков и т.д.
    - Определение ключевых сотрудников, ЛПР и сферы их полномочий
  - Данные о сотрудниках организации
    - Посещаемые ресурсы Internet, почтовые адреса и т.д.
    - Деловые связи, круг знакомых и близких друзей
  - Данные об организационно-штатной структуре организации
  - Данные о вычислительной инфраструктуре организации
    - Сетевая инфраструктура
    - Используемые программные решения

Фаза наблюдения: Итог

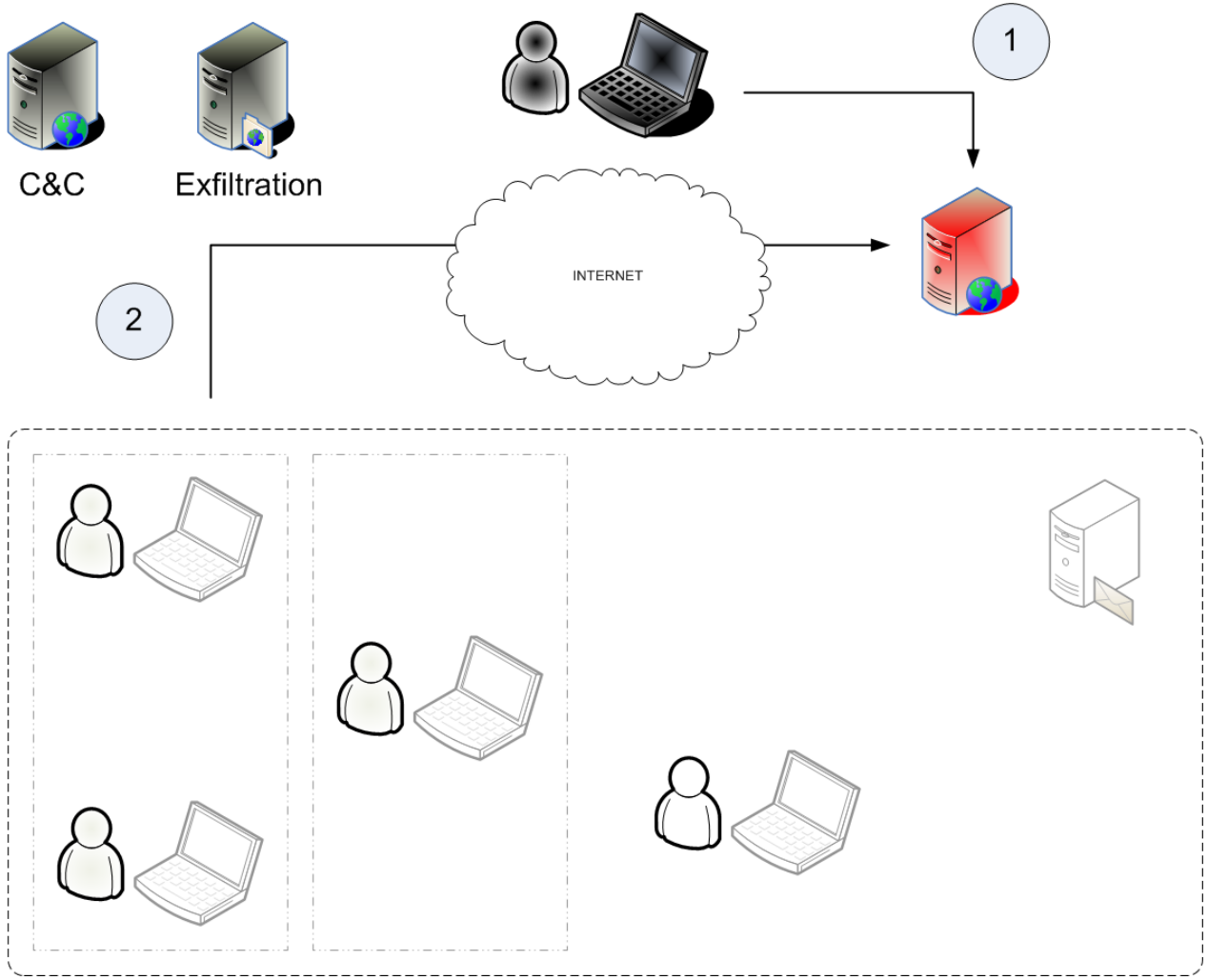




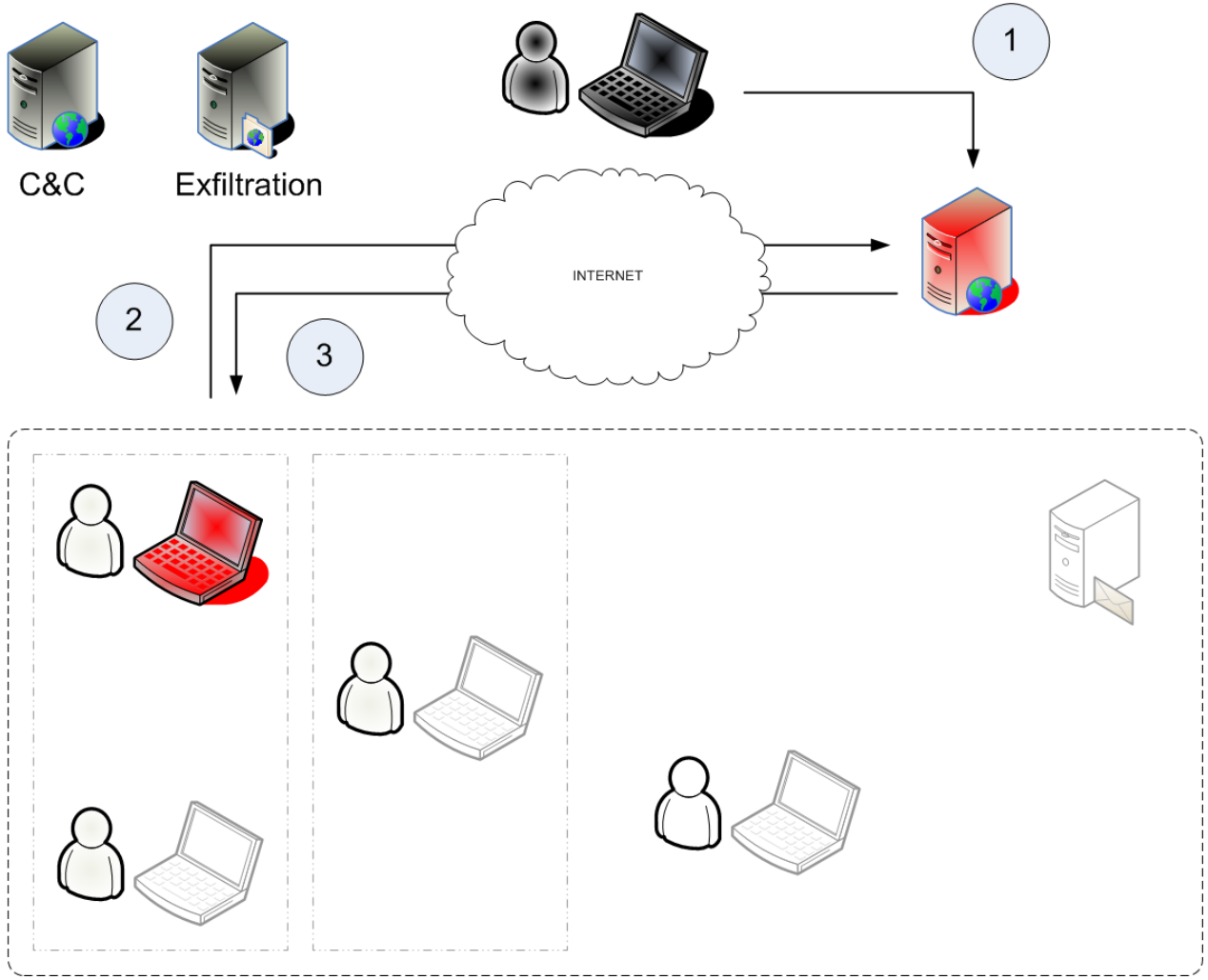
Цели и средства фазы начального проникновения

- Проникновение в сеть организации
  - Средства доставки начальных вредоносных программ
    - «Spear phishing» (вводящие в заблуждение почтовые сообщения)
    - «Watering hole» (временное заражение посещаемых внешних ресурсов)
    - Пользовательские USB sticks
- Успешная установка опорного бэкдора
  - Осуществление запуска
    - Ручной запуск
    - Использование уязвимостей нулевого дня

Фаза начального проникновения



Фаза начального проникновения



«Spear Phishing» и «Watering Hole» атаки

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week
We need to finalize the press release.
Details click here.
```

You have 1 new fax, document 000220964 - Message (Plain Text)

FILE MESSAGE

Fri 27/11/2015 06:25

Interfax <incoming@interfax.net>

You have 1 new fax, document 000220964

To

Message fax000220964.zip (2 KB)

A new fax document for you.

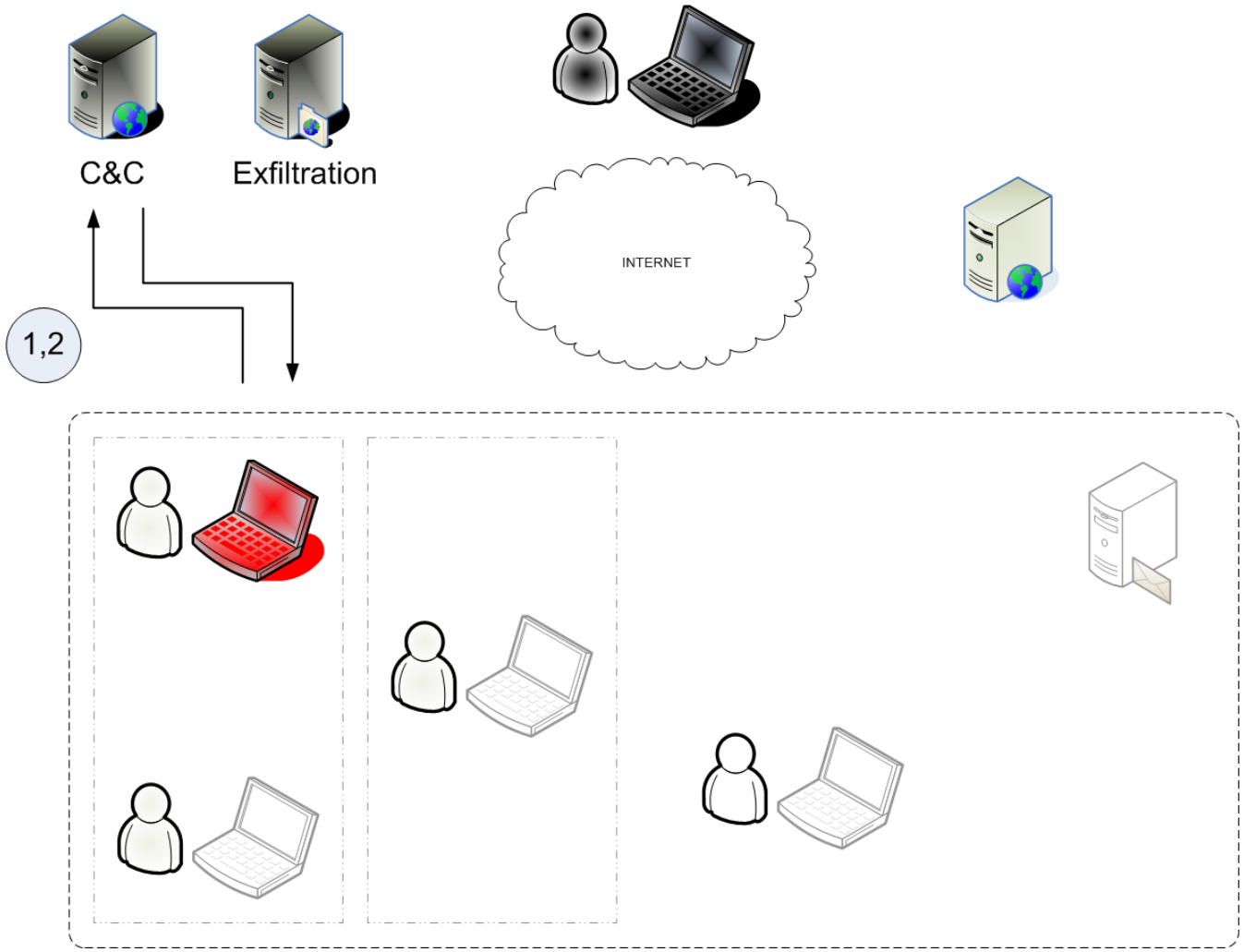
Please check your fax document in the attachment to this e-mail.

Scan duration: 20 seconds
Scanned at: Fri, 27 Nov 2015 04:17:14 +0300
Sender: Jeffrey Bowers
File size: 242 Kb
File name: fax000220964.doc
Scan quality: 100 DPI
Pages sent: 8

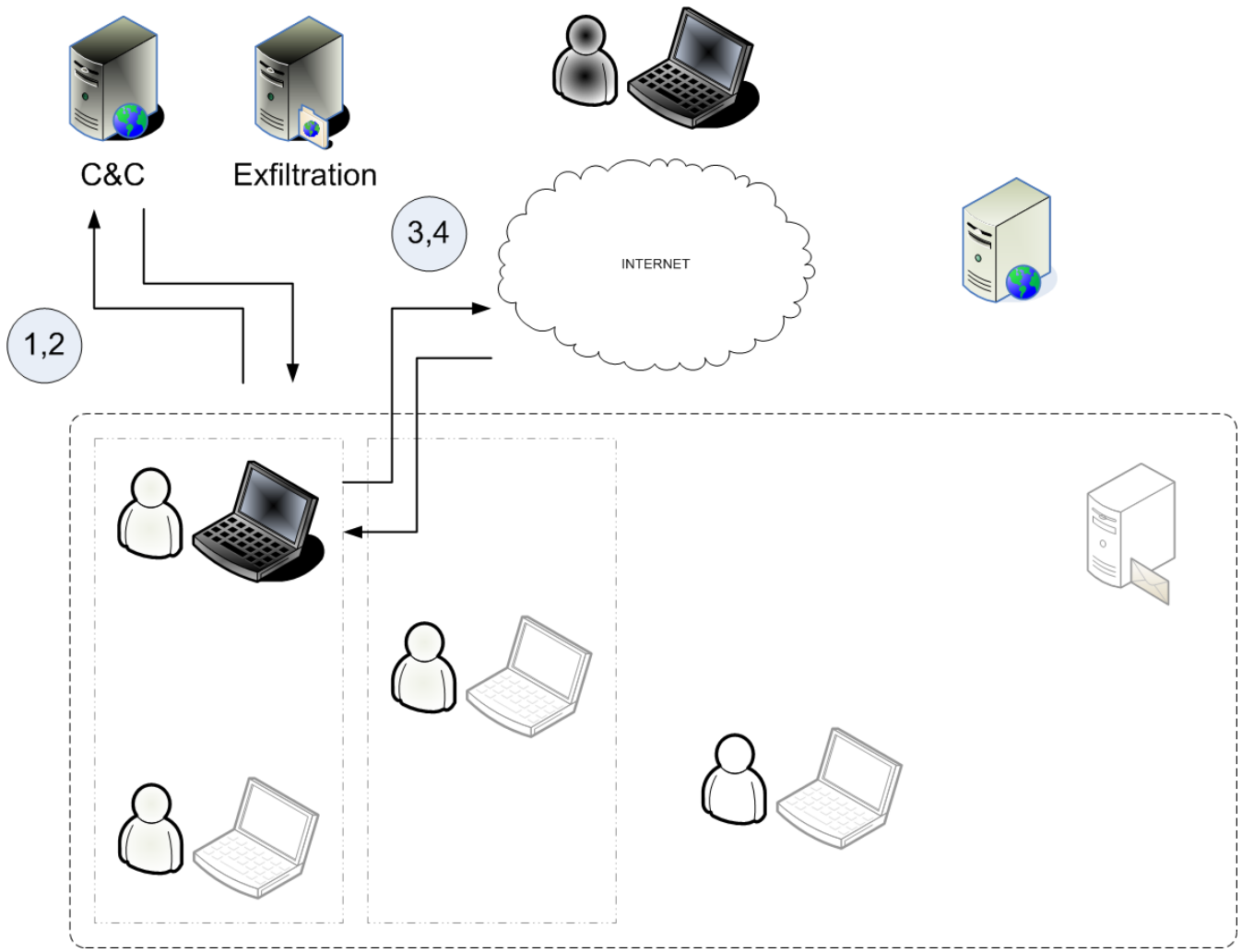
Thanks for using Interfax service!

Interfax No Items

Фаза доставки основного функционала



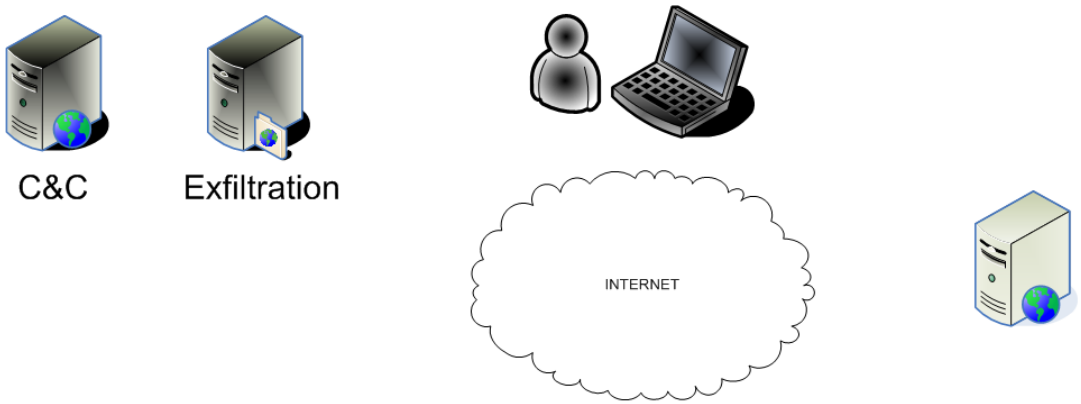
Фаза доставки основного функционала: Итог

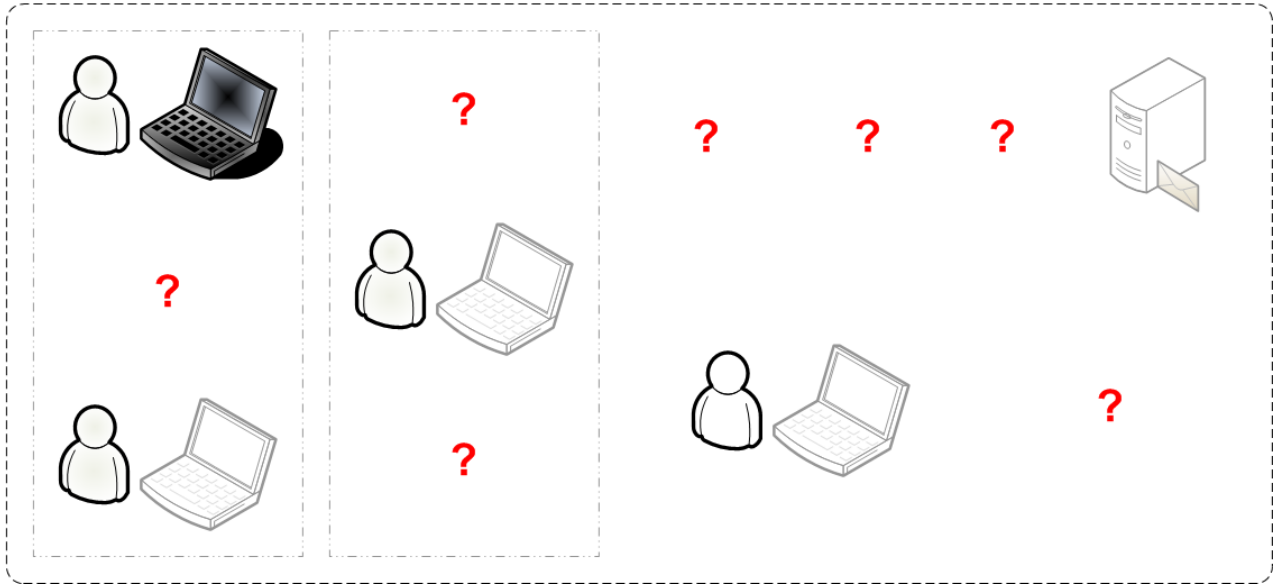


Цели и средства фазы доставки основного функционала

- Определение источника основного функционала
  - Посредством C2 серверов
- Его получение и установка
  - Создание, модификация, удаление и запуск программ
  - Мониторинг клавиатуры и движений мыши
  - Модификация системного реестра
  - Управление процессами
  - Получение и отправка данных по сети
  - Сбор паролей и другой релевантной информации
  - Управление пользовательскими сессиями
  - И т.д.

Фаза распространения





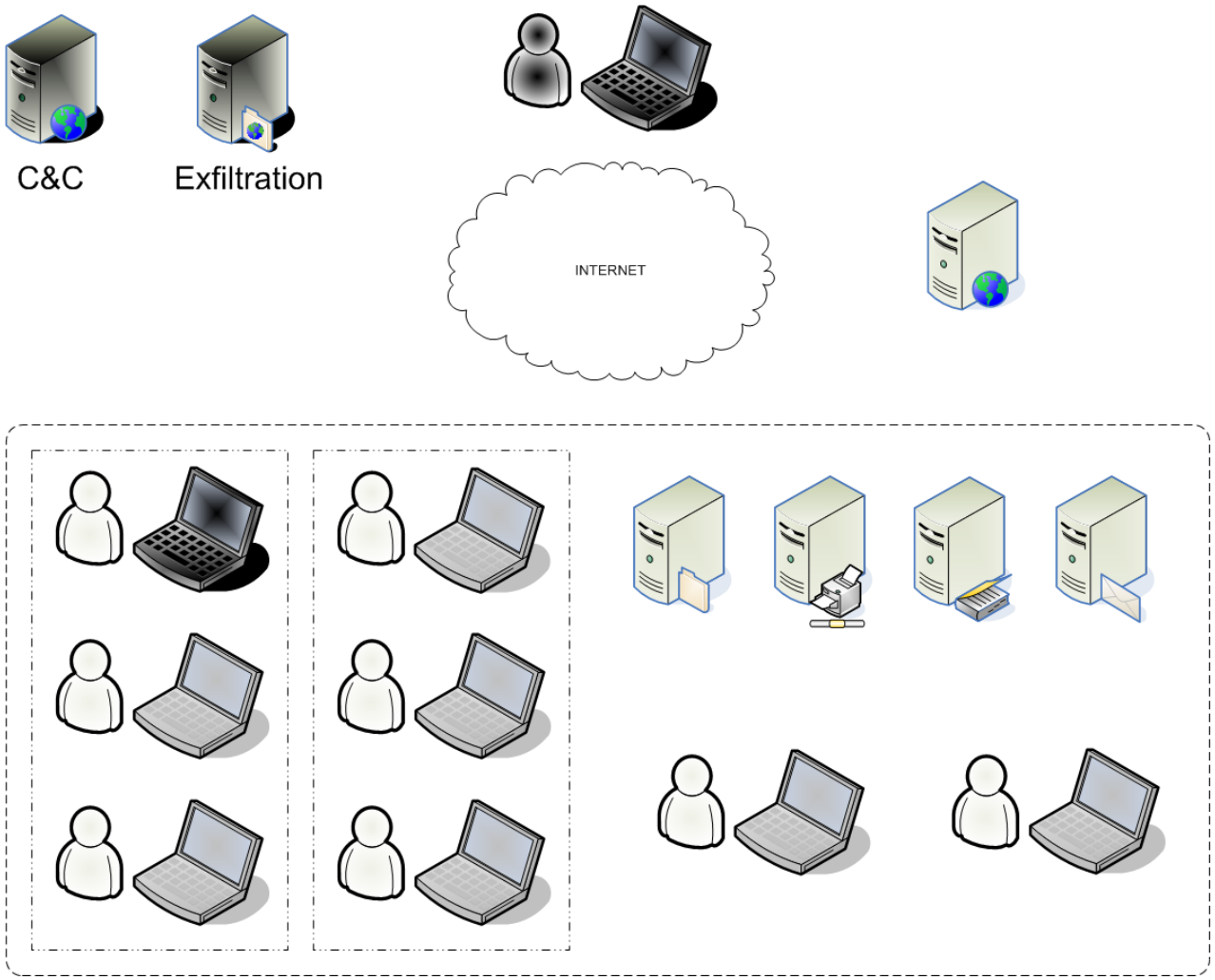
Цели и средства фазы распространения

- Разведка
  - Сбор дополнительных данных о конфигурации сети и правах пользователей
  - Осуществление «горизонтальных» переходов в рамках сетевой инфраструктуры атакуемого объекта
- Получение полномочий администратора атакованной сети
  - Осуществление «вертикальных» переходов в рамках сетевой инфраструктуры атакуемого объекта

Фаза распространения: сбор информации

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

Фаза распространения



Фаза распространения: сбор информации (1)

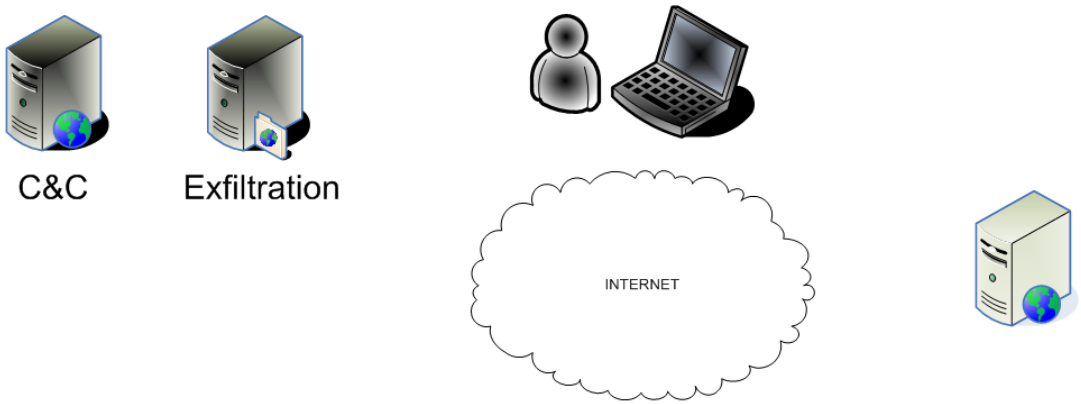
Tool	Command line	GUI	Local	Remote	SAM	NTDS.dit	Password history	
Cain & Abel	No	Yes	Yes	Yes. See notes	Yes (in-memory and from reg files)	Yes (in-memory)	Yes	Yes
pwdump2	Yes	No	Yes	No	Yes (in-memory)	Yes (in-memory)	No	No
pwdump6	Yes. See notes	No	Yes	Yes	Yes (in-memory)	Yes (in-memory)	Yes	No
pwdump7	Yes	No	Yes	No	Yes (from registry files). See notes	No	No	No
Quarks PwDump	Yes	No	Yes	No	Yes (from registry files). See notes	Yes (from NTDS.dit)	Yes	No
PowerDump	Yes	No	Yes	No	Yes (from registry files). See notes	No	No	No
fgdump	Yes	No	Yes	Yes	Yes (in-memory)	Yes (?)	Yes	No
PWDumpX	Yes	No	Yes	Yes	Yes (in-memory)	Yes (in-memory)	Yes	Yes
gsecdump	Yes	No	Yes	No	Yes (in-memory). See notes	Yes (in-memory)	No	Yes

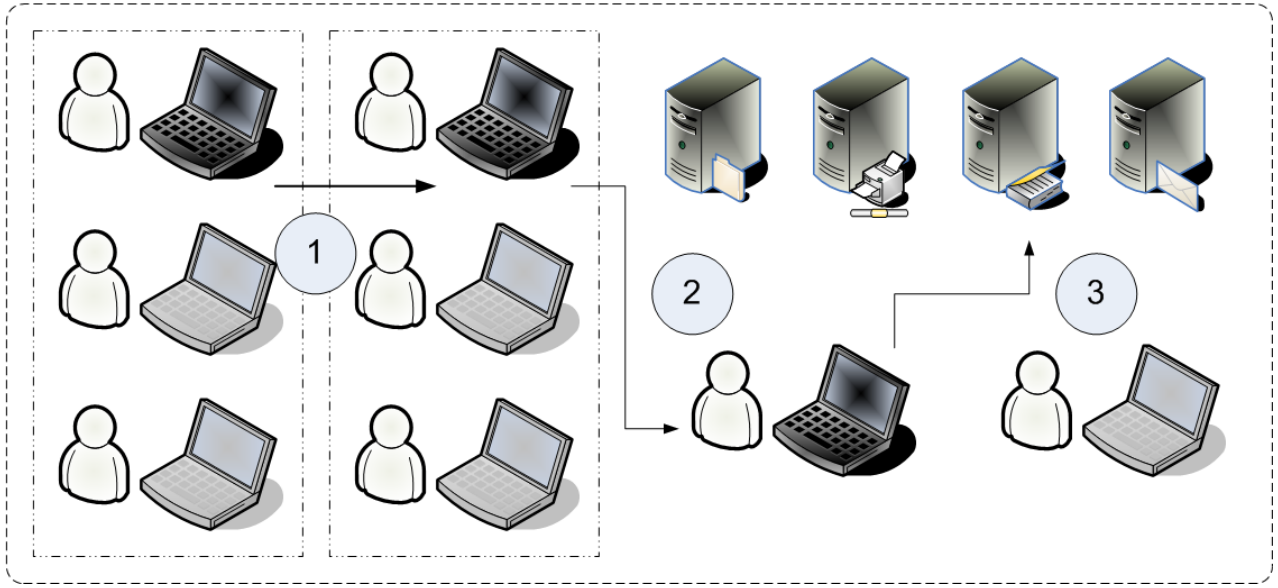
Фаза распространения: сбор информации (2)

mimikatz 2.0 alpha x64

```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 30 2013 23:42:09)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz
  '#####'                                     with  10 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 196180 (00000000:0002fe54)
Session           : Interactive from 1
User Name         : user
Domain            : VM-7x64-test
        msv :
         [00000003] Primary
         * Username : user
         * Domain   : VM-7x64-test
         * LM       : 00000000000000000000000000000000
         * NTLM     : 5058dcdf3965e4cff53994b1302e3174
        tspkg :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        wdigest :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        kerberos :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        ssp :
```

Фаза распространения: Итог

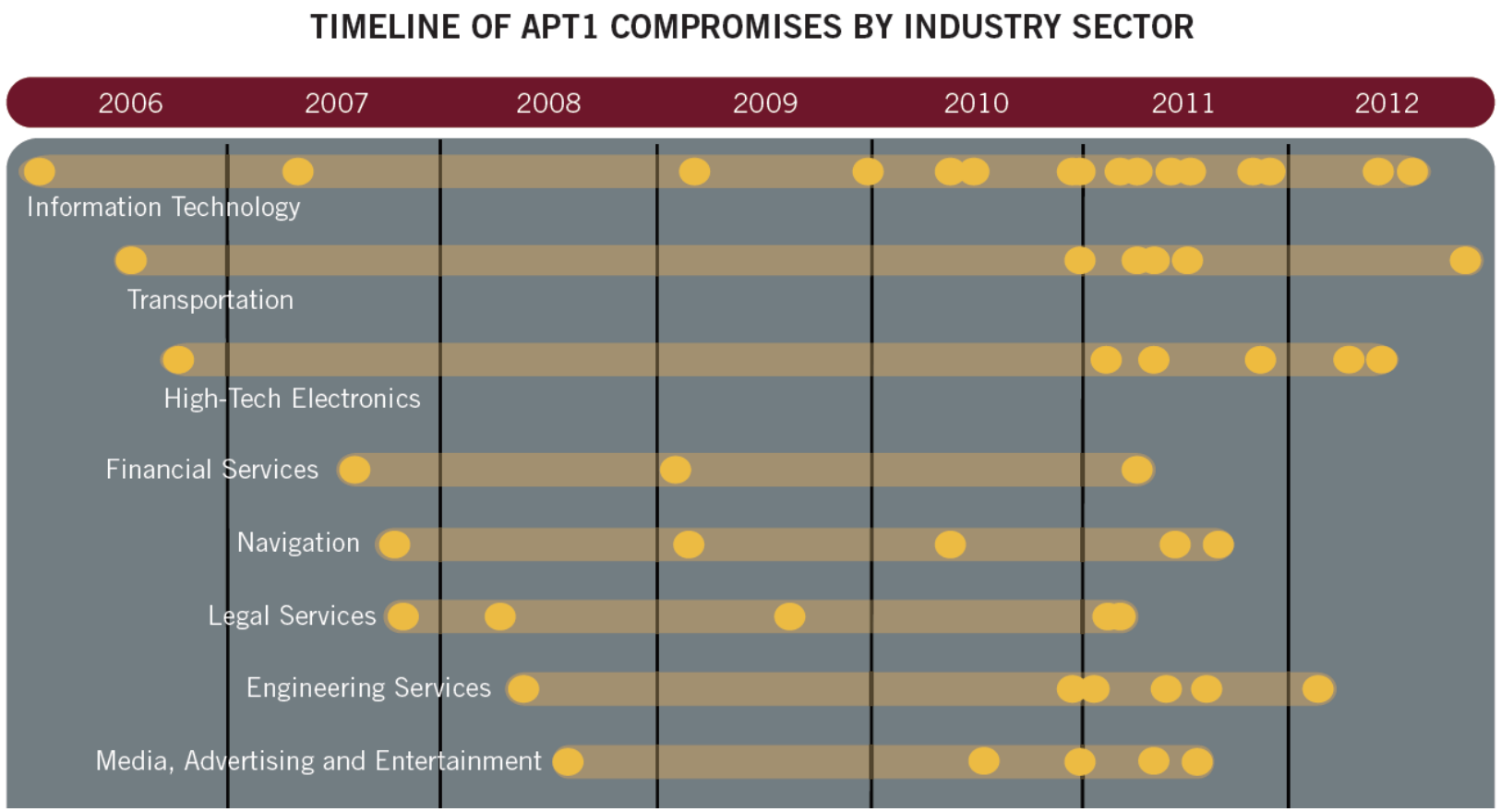




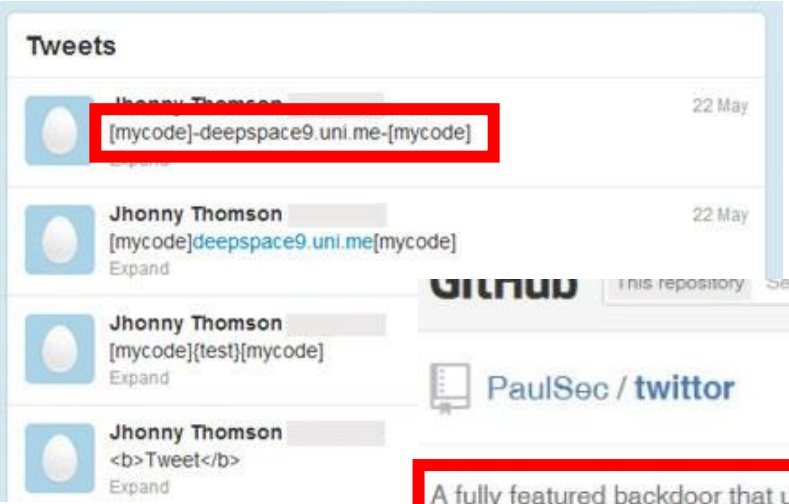
Фазы сбора и копирования данных

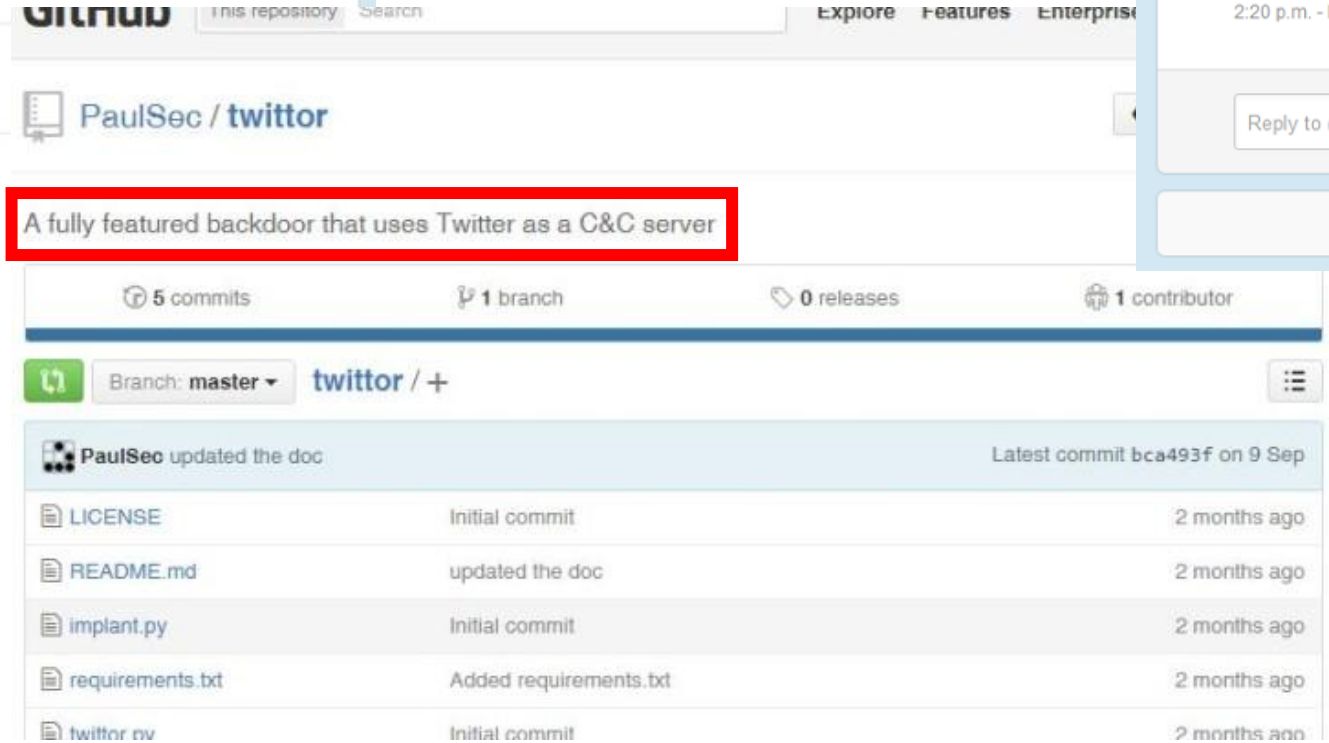
- Сбор и обобщение доступных данных, предварительная обработка, экспертиза
- Формирование информационных блоков, требующих отправки на сторону заказчика атаки
- Шифрование и скрытная пересылка информационных блоков на внешние сервера

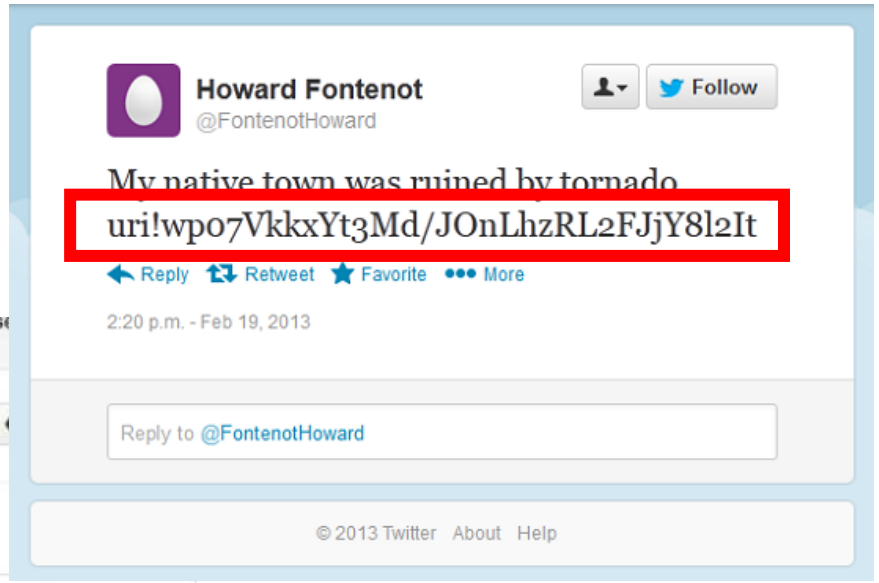
Цели фазы сбора данных



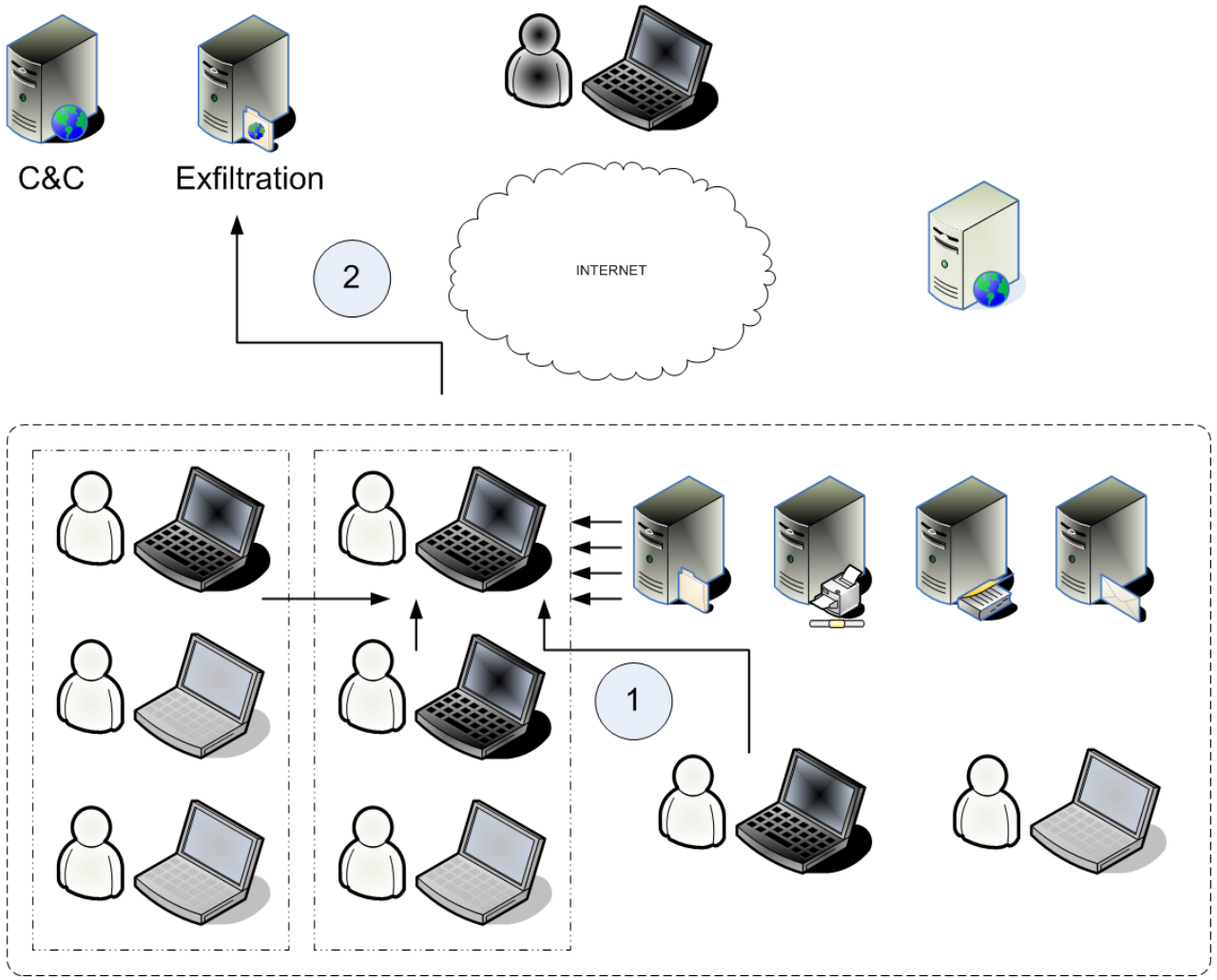
Фаза сбора данных







Фаза копирования данных: Итог



Очевидные контрмеры (1)

- Укрупнение контролируемого контекста
  - Анализ отдельных артефактов (например, файловых объектов) недостаточен
  - Помимо существующих источников информации, требуется включение в контекст ряда дополнительных
    - Сетевая активность
    - События файловой системы
    - Жизненный цикл процессов и изменение их состояния
    - События системного реестра
    - События ОС
  - Необходимо формирование профилей поведения для приложений, пользователей, хостов, сетей, организаций
  - Необходимо обеспечение связи профилей различного типа
- Централизованная обработка информации, поступающей от каждого контролируемого хоста

Очевидные контрмеры (2)

- Адаптивность продукта
  - Уточнение контекста возможной угрозы по запросу оператора
  - Возможность переноса на потенциально зараженный хост дополнительных утилит, подготовленных оператором
- Использование дополнительных источников данных, зачастую весьма неожиданных для традиционной AV индустрии:
  - «Слепки» состояния файловой системы, настроек, установленных обновлений и т.п.
  - Контроль сетевых данных на уровне прикладных сетевых протоколов
  - Отдельные системные журналы
  - Обнаружение противодействия Entropy Checkers

IOC: пример для Stuxnet (Mandiant)


```
- <ioc id="ea3cab0c-72ad-40cc-abbf-90846fa4afec" last-modified="2011-11-04T19:35:05">
    <short_description>STUXNET VIRUS (METHODOLOGY)</short_description>
  + <description></description>
    <keywords>methodology</keywords>
    <authored_by>Mandiant</authored_by>
    <authored_date>0001-01-01T00:00:00</authored_date>
    <links/>
```


Атрибуты PE32


```
- <IndicatorItem id="b9ef2559-cc59-4463-81d9-52800545e16e" condition="contains">
    <Context document="FileItem" search="FileItem/PEInfo/Sections/Section/Name" type="mir"/>
    <Content type="string">.stub</Content>
  </IndicatorItem>
- <IndicatorItem id="156bc4b6-a2a1-4735-bfe8-6c8d1f7eae38" condition="contains">
    <Context document="FileItem" search="FileItem/FileName" type="mir"/>
    <Content type="string">mdmcpq3.PNF</Content>
  </IndicatorItem>
```


Установленные драйвера


```
- <Indicator operator="AND" id="422ae9bf-a1ae-41f2-8e54-5b4c6f3e1598">
  - <IndicatorItem id="e93f1610-daaf-4311-bcf3-3aecef8271c0" condition="contains">
      <Context document="DriverItem" search="DriverItem/DeviceItem/AttachedToDriverName" type="mir"/>
      <Content type="string">fs_rec.sys</Content>
    </IndicatorItem>
  + <IndicatorItem id="72476f35-8dea-4bae-8239-7c22d05d664f" condition="contains"></IndicatorItem>
  + <IndicatorItem id="f98ea5aa-9e23-4f18-b871-b3cf5ba153fe" condition="contains"></IndicatorItem>
  + <IndicatorItem id="32f61140-0f58-43bc-8cdd-a25db75ca6c4" condition="contains"></IndicatorItem>
  </Indicator>
```


Содержимое системного реестра


```
- <Indicator operator="AND" id="d8d9b32c-f648-4552-9805-93c05ed48219">
  - <IndicatorItem id="c08044e7-e88c-433c-b463-763bdddeff82" condition="contains">
      <Context document="RegistryItem" search="RegistryItem/Path" type="mir"/>
    - <Content type="string">
        HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
      </Content>
    </IndicatorItem>
  - <IndicatorItem id="38dfb382-ebbe-4685-bbb7-60675b91bd15" condition="contains">
      <Context document="RegistryItem" search="RegistryItem/Text" type="mir"/>
      <Content type="string">mrxnet.sys</Content>
    </IndicatorItem>
```

IOC: пример для Duqu (Mandiant)


```
– <ioc id="72669174-dd77-4a4e-82ed-99a96784f36e" last-modified="2012-01-05T02:49:14">
    <short_description>DUQU (METHODOLOGY)</short_description>
  + <description></description>
    <authored_by>MANDIANT</authored_by>
    <authored_date>2011-10-21T16:13:31</authored_date>
  + <links></links>
```


Атрибуты электронной подписи (PE32)


```
– <Indicator operator="AND" id="e4deb0af-7558-498e-b953-6e70ec694767">
  – <IndicatorItem id="d5b29cfe-8599-498a-b805-326273fe10c5" condition="contains">
      <Context document="FileItem" search="FileItem/PEInfo/DigitalSignature/CertificateSubject" type="mir"/>
      <Content type="string">C-Media Electronics Incorporation</Content>
    </IndicatorItem>
  – <IndicatorItem id="1ca2947c-0b26-409c-93d2-28f6b364bc0b" condition="contains">
      <Context document="FileItem" search="FileItem/FileName" type="mir"/>
      <Content type="string">cmi4432.sys</Content>
    </IndicatorItem>
  </Indicator>
```


Содержимое системных журналов


```
– <Indicator operator="AND" id="e59031e1-1a15-42be-8cae-198e69c88ced">
  – <IndicatorItem id="0f00f74d-c2ff-4c24-9334-bcfa8430a00b" condition="is">
      <Context document="EventLogItem" search="EventLogItem/type" type="mir"/>
      <Content type="string">Error</Content>
    </IndicatorItem>
  – <IndicatorItem id="a3ae813d-27b1-49d5-8057-04d0702eb3ee" condition="is">
      <Context document="EventLogItem" search="EventLogItem/source" type="mir"/>
      <Content type="string">DCOM</Content>
    </IndicatorItem>
  – <IndicatorItem id="a10fc902-a5fa-4f1a-87a7-ad7855066be1" condition="is">
      <Context document="EventLogItem" search="EventLogItem/EID" type="mir"/>
      <Content type="int">3221235481</Content>
    </IndicatorItem>
```


Состояние адресного пространства процессов


```
– <Indicator operator="AND" id="1bd40f96-b1bc-43ef-b482-5d2e81fa6da7">
  – <IndicatorItem id="2e0bd752-975b-4155-94ad-2ab760a9a53a" condition="is">
      <Context document="ProcessItem" search="ProcessItem/name" type="mir"/>
      <Content type="string">winlogon.exe</Content>
    </IndicatorItem>
  – <IndicatorItem id="174d0bcd-4325-44f6-805d-87dce4c51b47" condition="containsnot">
      <Context document="ProcessItem" search="ProcessItem/SectionList/MemorySection/Name" type="mir"/>
      <Content type="string">winlogon.exe</Content>
    </IndicatorItem>
  – <IndicatorItem id="5215ed3f-7795-4689-801b-13373da473f6" condition="is">
      <Context document="ProcessItem" search="ProcessItem/SectionList/MemorySection/Injected" type="mir"/>
      <Content type="string">TRUE</Content>
    </IndicatorItem>
```

Проблема PCI DSS

Payment Card Industry Data Security Standard, стандарт безопасности информации для индустрии платежных карт.

Конфликт требований защиты данных держателей карт и реализации мер по строгому контролю доступа:

1. Проблема регулярных обновлений;
2. Проблема централизованной обработки информации в системах противодействия APT.

Machine Learning и противодействие APT

splunk>

Splunk Acquires Caspida

Extends Security Analytics Leadership by Adding Behavioral Analytics to Better Detect Advanced and Insider Threats

SAN FRANCISCO - July 9, 2015 - Splunk Inc. (NASDAQ: SPLK), provider of the leading software platform for real-time Operational Intelligence, today announced it has acquired Caspida, Inc., a leading innovator in machine learning and behavioral analytics. Under the terms of the agreement, Splunk has acquired all of the outstanding stock of Caspida for an aggregate purchase price of approximately $190 million, including approximately $127 million in cash and $63 million in restricted Splunk securities.

The combination of Splunk® and Caspida™ technology revolutionizes the security market by unifying world-class breach response with breach detection. Recent high-profile breaches show virtually all attacks happen with compromised credentials, and automated detection leveraging machine learning is the future for detecting known and unknown threats from insider and external attackers. Splunk customers now have out-of-the-box user behavioral analytics to help detect, respond to and mitigate these threats. This combination of Splunk's leading machine data platform with Caspida software provides the most comprehensive security analytics solution available today.

Machine Learning и противодействие APT (2)

10/29/2015
10:30 AM

Simon Crosby
Commentary

Connect Directly

4 COMMENTS
COMMENT NOW

Login
50% 50%

Like 41 Tweet Share 423 G+1 7

Machine Learning Is Cybersecurity's Latest Pipe Dream

Rather than waste money on the unproven promises of ML and AI, invest in your experts, and in tools that enhance their ability to search for and identify components of a new attack.

Related Content Sponsored by Malwarebytes

Resource | Blog | Video | Twitter

Malware removal efficacy: 17 security products tested for malware removal and repair
Strong anti-malware is the backbone of your security strategy. No matter how good the rest of your network's security is...

Tech Brief: An inside view of a zero-day campaign
Cybercriminals work tirelessly to find new vulnerabilities in popular software – sometimes more tirelessly than the actual software developer.

Anti-exploit tools: The next wave of enterprise security
From malware to ransomware to state-sponsored hacks, today's threat landscape is more complex...

Ближайшее будущее APT

В соответствии с прогнозами Лаборатории Касперского и некоторых других AV вендоров, в 2016 году можно будет наблюдать следующие тенденции:

1. Снижение «постоянства» атак
    1. Резидентность
    2. Бестелесность
2. Снижение «продвинутости» атак
    1. Противодействие выявлению источника (заказчика) атаки (сокрытие TTP триады)
    2. Снижение издержек

Основные использованные источники

- The Radicati Group: Advanced Persistent Threat (APT) Protection – Market Quadrant 2015, 2015
- Mandiant: APT1 Exposing One of China's Cyber Espionage Units, 2013
- G. Granadillo et al.: Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats (APTs), 2015
- P. Giura, W. Wang: A Context-Based Detection Framework for Advanced Persistent Threats, 2012
- B. Damele: Dump Windows password Hashes efficiently, http://bernardodamele.blogspot.ru/search/label/dump 2010-2012
- Kaspersky Lab: Kaspersky Security Bulletin. 2016 Predictions, https://securelist.com/files/2015/11/KSB_2016_Predictions_FINAL.pdf , 2015

Вопросы и ответы

?