Опыт противодействия целенаправленным атакам в финансовых организациях

Денис Безкоровайный, CISA, CISSP, CCSK, Аудитор СТО БР ИББС

Руководитель направления по работе с финансовыми организациями Trend Micro

Самая большая проблема – это осознать проблему

Это просто вирус!
Это плохой антиспам!
Это глупый пользователь!

TREND MICRO

Есть средства защиты

- Next-Gen Firewall
- Системы обнаружения атак (IDS)
- Системы IPS
- Антивирус
- Шлюз Email /Web

Известные угрозы

Все это борется только с известными угрозами

Есть средства защиты, но нет защищенности

- Разведка и подготовка
- Целевой email-фишинг
- Неизвестное ВПО
- Новые эксплойты
- Широкий набор уязвимостей
- Динамические C&C-серверы
- BYOD ?

- Next-Gen Firewall
- Системы обнаружения атак (IDS)
- Intrusion Prevention (IPS)
- Антивирус
- Шлюз Email /Web

Традиционную защиту довольно просто обойти

Реальные данные по реальным Заказчикам Обследования с Deep Discovery

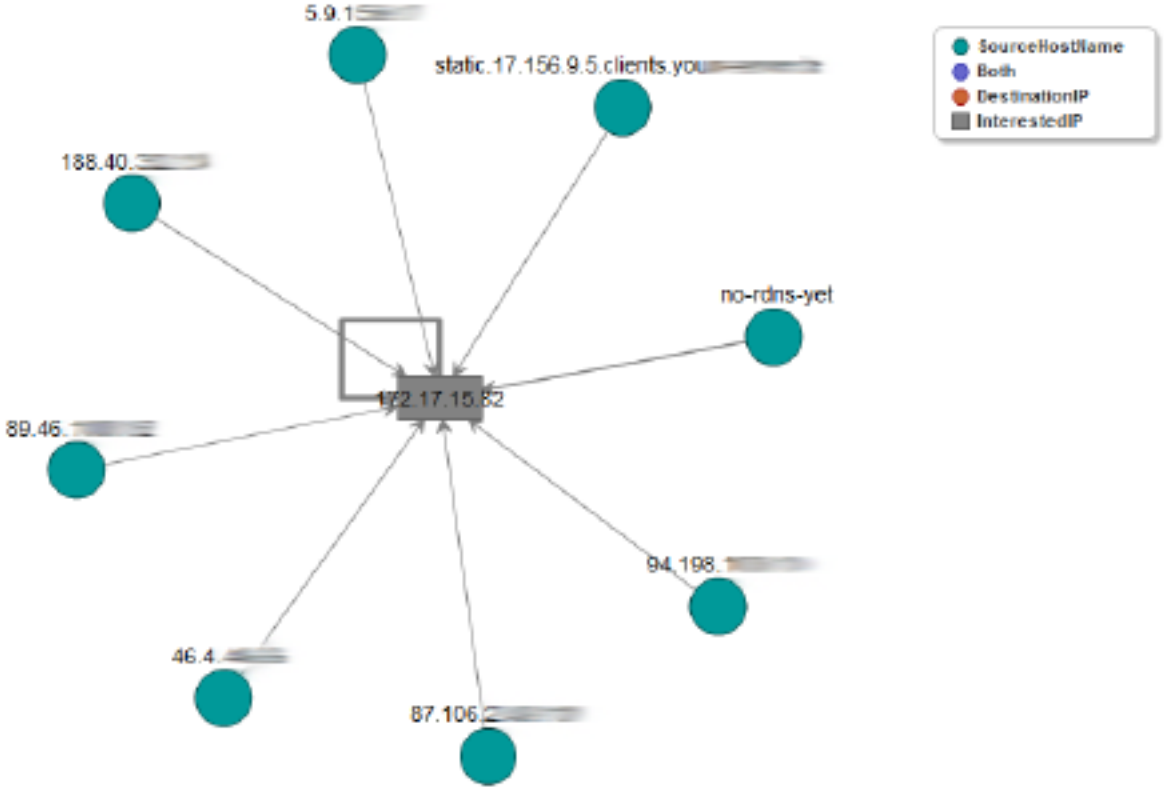
Обнаружено	% компаний
Известное ВПО	98%
Активные ботнеты	94%
Банковское ВПО	75%
Вредоносные документы	75%
ВПО, использующее уязвимости нулевого дня	49%
Сетевые атаки	84%
ВПО для Android	28%

Примеры из банка: клиенты ботнетов

В некоторых банках «живут» десятки зараженных машин

Date/s	Security Site	Number of Occurrences
April 07,2014 - May 05,2014	37.140. (server39.hostin)	247
April 08,2014 - April 08,2014	80.86. (80.86.)	2
April 10,2014 - April 15,2014	83.217. ( )	24
April 18,2014 - May 02,2014	83.238. (83.238.)	4
April 25,2014 - April 25,2014	84.244. (84-244- pppoe.irknet.ru)	7
April 17,2014 - April 17,2014	84.24 (84-244- pppoe.irknet.ru)	90
April 25,2014 - April 30,2014	84.244.17. (84.244.17)	11
April 21,2014 - April 21,2014	87.118.11 (87.118.1)	52
April 15,2014 - April 15,2014	175.214.21 (175.214.2)	4
April 17,2014 - May 05,2014	217.172. (chicago061.start)	14

Примеры из банка:
TOR



TREND MICRO

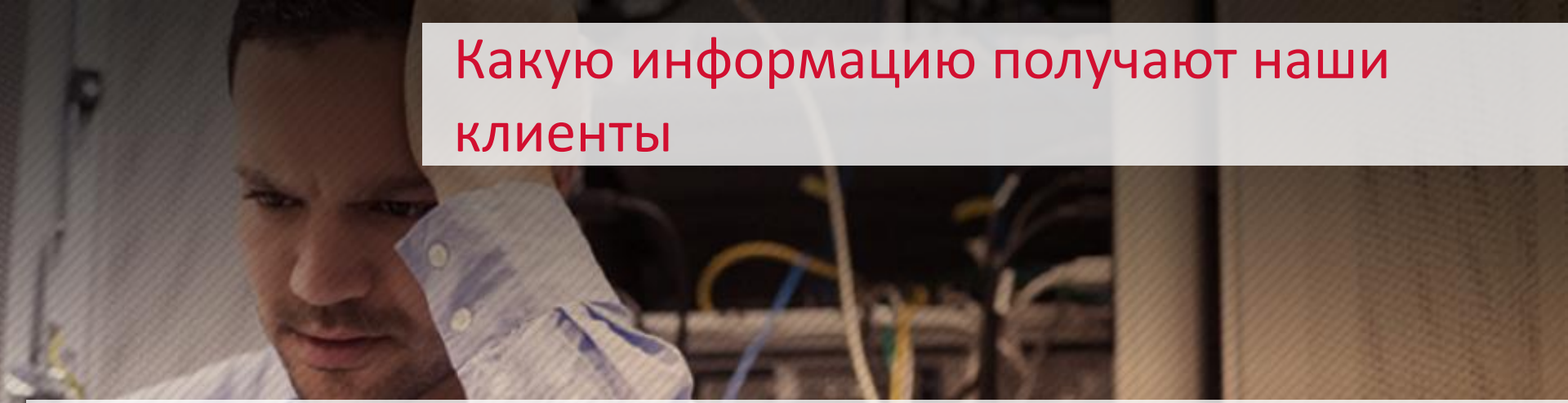
Примеры из банков: прочие признаки атак

- Атаки Drive By Download – автоматическая загрузка вредоносного файла на машину пользователя
- Подтвержденные вредоносные файлы, скачанные из Интернет на рабочие станции
  - прошли через веб-шлюз, не детектировались АВ
- Использование некоторыми машинами нелегитимных DNS-серверов
- Целевой фишинг с вредоносным содержимым
  - прошли через почтовый-шлюз, не детектировались АВ

Примеры из банков: почти всегда

91% атак начинаются с электронной почты

Какую информацию получают наши клиенты



- Откуда атака? Куда выводятся данные?
- Сколько машин/сотрудников скомпрометированы?
- Как давно?
- Атака уникальная или просто мой АВ не справился?
- Как предотвратить?

Внимание, вопрос!

- Какой процент вредоносных программ заражает менее 10 компьютеров?
  - 99%
- Какой процент вредоносных программ заражает только один компьютер?
  - 80%

Как обнаружить *неизвестные* угрозы?

- Продвинутый сетевой анализ
- Динамический анализ угроз («песочницы»)
- Обработка индикаторов компрометации
- Корреляция с глобальной базой угроз

Продвинутый сетевой анализ

- действия атакующего
  - ошибки аутентификации, нестандартные протоколы
  - эксплойты
  - ВПО
- вывод данных
- коммуникации C&C
- выявляются подозрительные файлы для дальнейшего анализа

Windows/Mac OS/Mobile

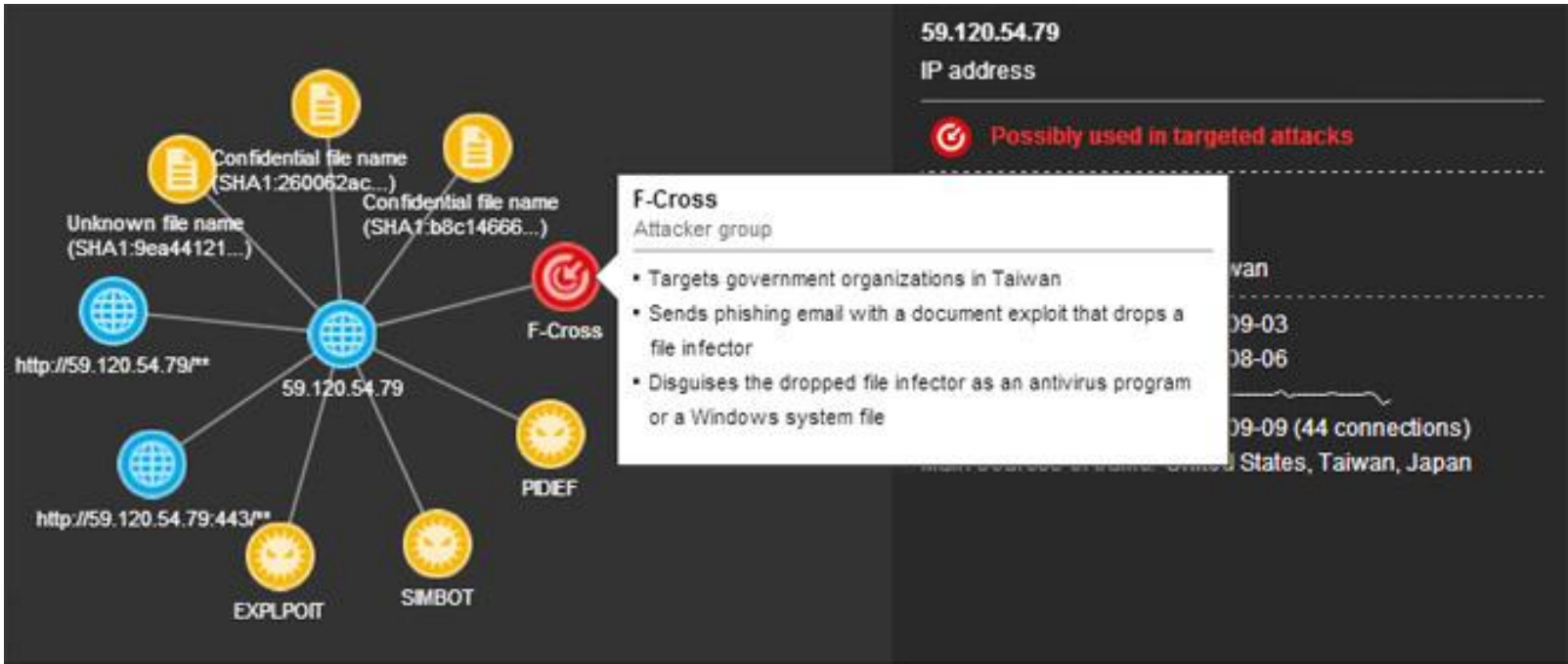
TREND MICRO

Динамический анализ угроз (виртуальные «песочницы»)

Индикаторы компрометации (IoC):

- IP адреса, домены
- Паттерны в URL
- Хеш-суммы файлов
- Email адреса
- X-Mailer
- HTTPUserAgent

Корреляция
с глобальной базой угроз



Интеграция – пример

Что дает Trend Micro Deep Discovery?

Аналитикам ИБ – инструмент анализа и мониторинга угроз

CISO – защита инвестиций в ИБ: возможность по-новой использовать существующие системы защиты, дополнять локальной аналитикой

Живет ли в вашей сети слон?

Вопросы?

Спасибо!

DENIS_BEZKOROVAYNY@TRENDMICRO.COM