QIWI
КИВИ

Опыт взаимодействия QIWI и FinCERT

Опыт взаимодействия QIWI и FinCERT

About

- Александр Секретов
- Эксперт по информационной безопасности, QIWI
- 5 лет в defense
- Reverse-engineering, audit, compliance, automation
- Команда Vulners.com

Анализ вредоносной активности до FinCERT

Опыт взаимодействия QIWI и FinCERT

Анализ вредоносной активности до FinCERT

Входные точки для поиска инцидентов

Произошедшие:
- Аномалии в SIEM
- Сетевые аномалии
- События DLP
- Срабатывания антивирусного ПО

Возможно, еще не произошедшие:
- Вредоносные рассылки

Можно защититься, если проанализировать вложение и удалить письмо из Exchange до того, как его запустит пользователь

Опыт взаимодействия QIWI и FinCERT

Анализ вредоносной активности до FinCERT

- Необходим анализ троянов
- Коллеги из других компаний также тратят время на исследование вредоносного ПО
- Агрегация усилий позволила бы экономить ресурсы и ускорить реакцию на инцидент

Взаимодействие сегодня

Опыт взаимодействия QIWI и FinCERT

Взаимодействие сегодня

- Можно искать письма в Exchange по отправителю/теме/ключевым словам
- Сокращение времени на разбор вредоносных файлов
- Уведомление FinCERT может прийти раньше вредоносной рассылки на вашу компанию
- FinCERT занимается блокировкой вредоносных доменов

Feed с нашей стороны:

- Множество подробных отчетов о вредоносном ПО
- Реакция быстрее, чем обновление антивирусных баз

Опыт взаимодействия QIWI и FinCERT
Реакция на ALERT

- Ретроспективный поиск в SIEM на предмет переходов по указанным IP
- Поиск подробностей троянов

```
https://www.hybrid-analysis.com/sample/[SHA256 файла]
https://www.virustotal.com/en/file/[SHA256 файла]/analysis/
```

*на hybrid-analysis.com часто можно скачать семпл вредоносного файла, если необходимо провести собственное исследование

- Проверка, что на том же IP нет доменов, к которым вам необходим доступ
- Добавление IP в blacklist (Firewall, IPS, …)
- При наличии ПО для контроля целостности – добавление хэш-сумм семпла

Опыт взаимодействия QIWI и FinCERT

Настройка правил в SIEM

Создание отдельных триггеров в SIEM на попытки перехода по заблокированным IP-адресам

При срабатывании:

- Изоляция рабочей станции
- Сброс паролей, отзыв сертификатов пользователя
- Снятие образа
- …

QIWI
КИВИ

Чего хотелось бы?

Опыт взаимодействия QIWI и FinCERT

TODO: IP-reputation на базе DGA

Динамический список IP-адресов для бана на базе DGA*!

*DGA (Domain Generation Algorithm) - механизм генерации доменных имен. Используется в ряде семейств вредоносного ПО вместо статических адресов управляющих центров (C&C).

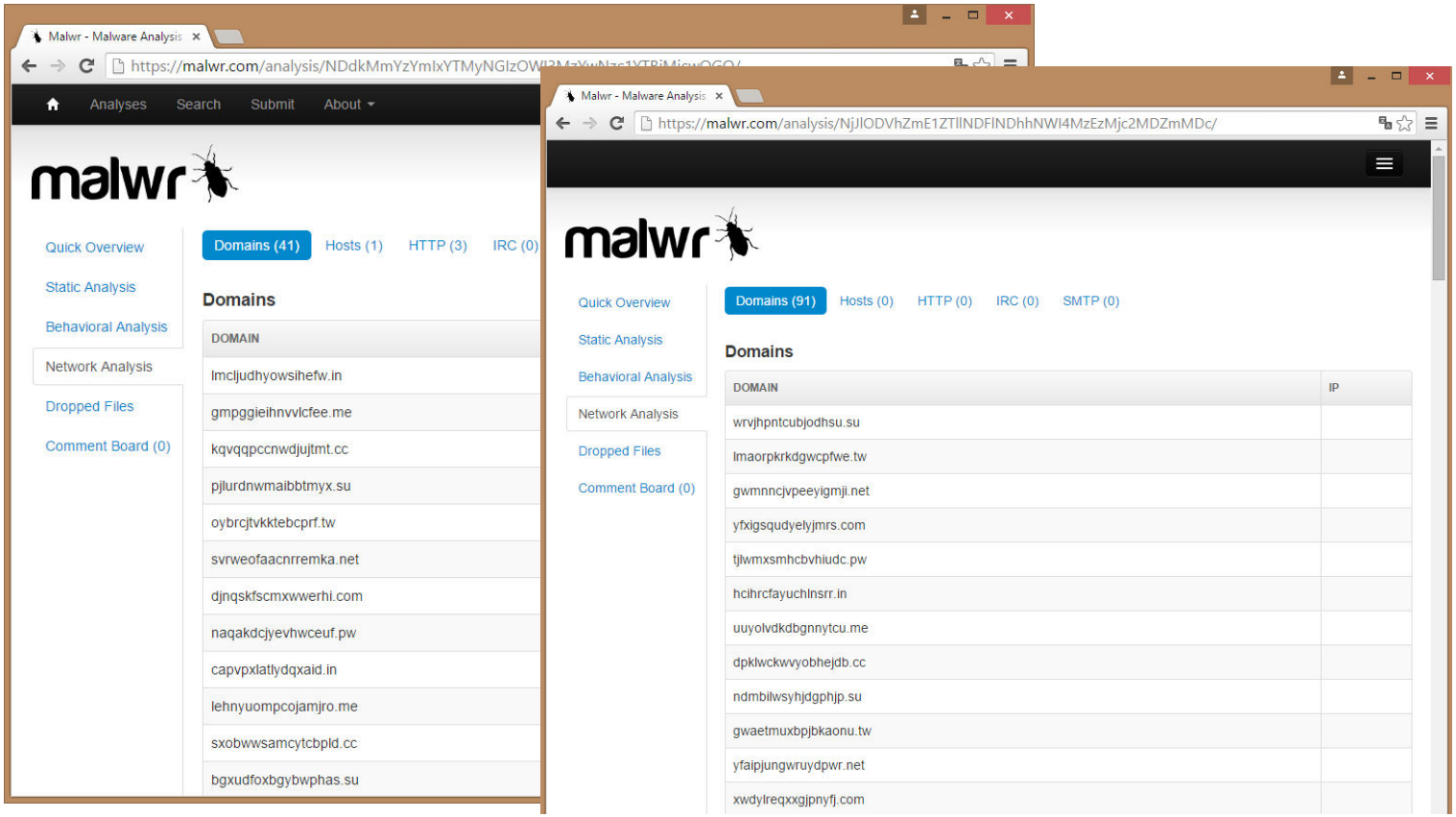
Trojan-Banker.Win32/Ranbyus:

- Используется для атак на банковский сегмент РФ
- Модифицирует JAVA-код в памяти приложения
- Подписывает транзакции с токена
- Содержит DGA

Опыт взаимодействия QIWI и FinCERT

TODO: IP-reputation на базе DGA

Список доменных имен, куда пытается обратиться одна из модификаций Win32/Ranbyus в различные даты



Опыт взаимодействия QIWI и FinCERT

TODO: IP-reputation на базе DGA

Как бороться?

- Подробно проанализировать семпл
- Разобрать механизм DGA
- Реализовать в скрипте аналогичный DGA алгоритм
- Скрипт генерирует список доменных имен и резолвит IP-адреса
- Если найден IP-адрес – он блокируется через API-интерфейс Firewall/IPS

Входные параметры DGA:

- Дата
- Seed (редко меняется, т.к. его смена означает потерю ботов)

Опыт взаимодействия QIWI и FinCERT

TODO: IP-reputation на базе DGA

В итоге:

- Скрипт запускается несколько раз в день
- При появлении, новый управляющий центр C&C трояна будет заблокирован
- Полная автоматизация

```
Generating C&C domains for dates 2015-09-17 00:00:00 - 2015-12-31 00:00:00
2015-9-21 - udvsswdsnwvvrtofx.com - 185.28.193.195 (seed F2C72B14)
2015-9-25 - jwgwqxnwswjudumrd.com - 185.28.193.195 (seed F2C72B14)
2015-9-26 - yuodklkopqmpedujq.net - 54.201.30.58 (seed F2C72B14)
2015-9-28 - gkanpaholwbyshjgs.net - 54.201.30.58 (seed F2C72B14)
2015-10-14 - adislbpahkdstfgpr.in - 208.100.26.234 (seed F2C72B14)
2015-10-19 - tjlwmxsmhcbvhiudc.pw - 92.63.87.21 (seed F2C72B14)
```

Спасибо за внимание!

2016

a.sekretov@qiwi.com