Классический антивирус умер

Что делать и чем заменить ?

Фишман Антон
Group-IB

Слухи о моей смерти несколько преувеличены

(c) Марк Твен


Евгений Касперский
Компьютерные вирусы в MS-DOS
NEW!
Полный каталог вирусов
Методы удаления вирусов
Методы восстановления файлов
Работа с антивирусной программой
92.9.16 · RENAISSANCE


GROUP IB


Е. В. Касперский
Компьютерные вирусы:
OS/2

Вирусология XX в. Vs XXI в.

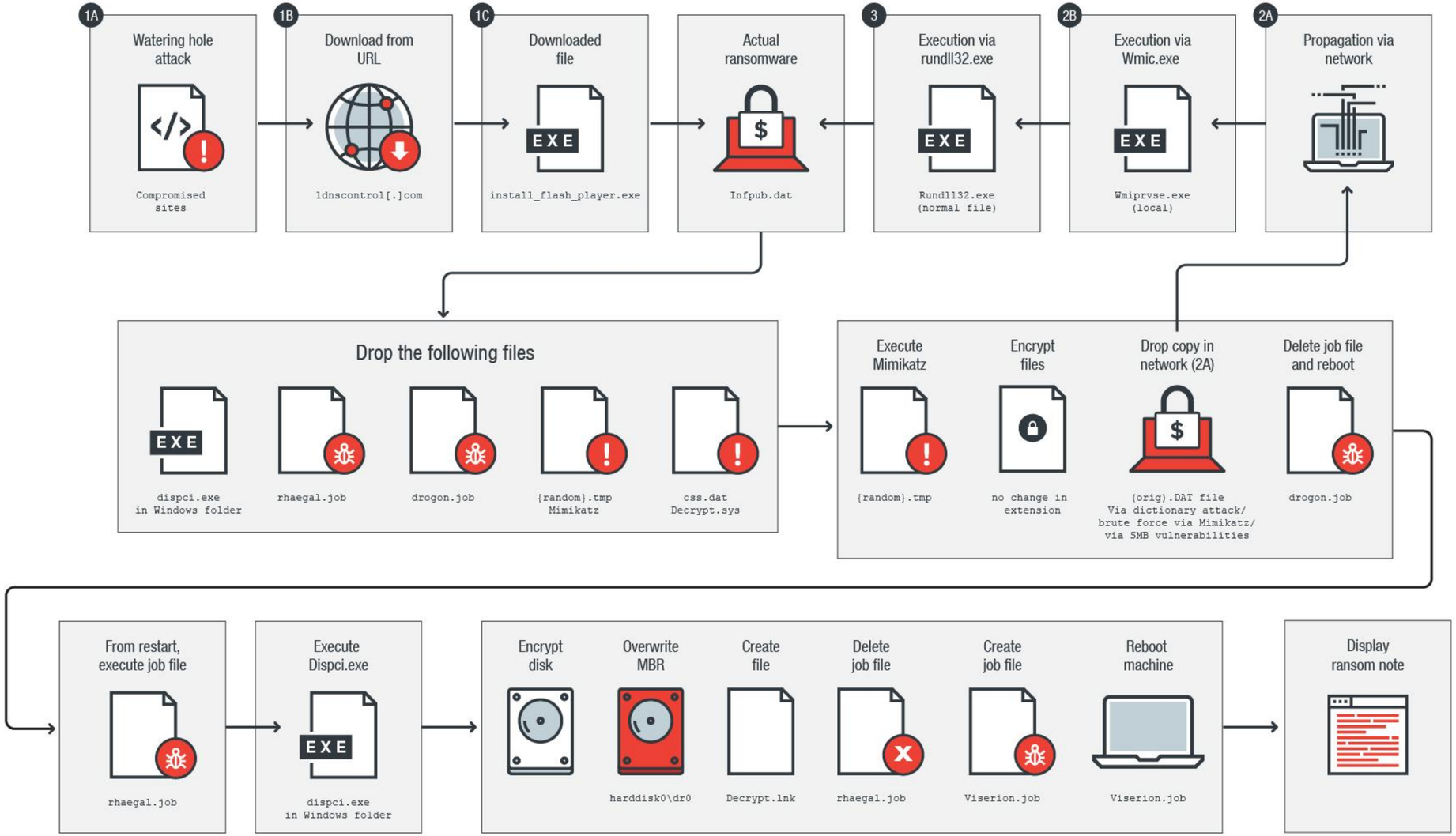
XX

- Worms
- Macro virus
- Stealth virus
- Boot virus
- Polymorphic code
- …

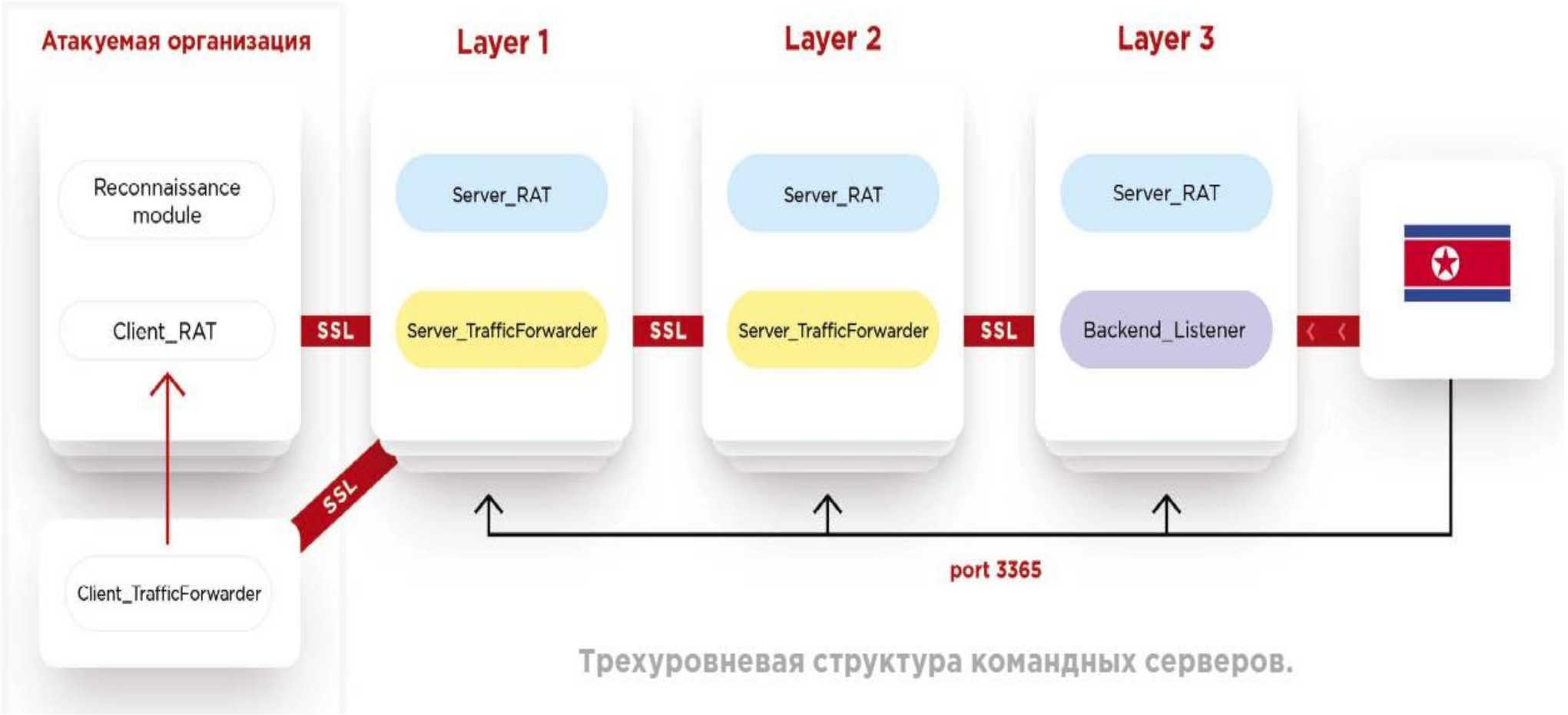
XXI

- Macro virus
- Polymorphic code
- Spread Module
- Exploit
- Shellcode
- Payload
- BackDoor
- Malware
- Trojans/RAT
- Stealer
- Ransomware
- KeyLogger
- Botnet
- …

Bad Rabbit. Взгляд изнутри

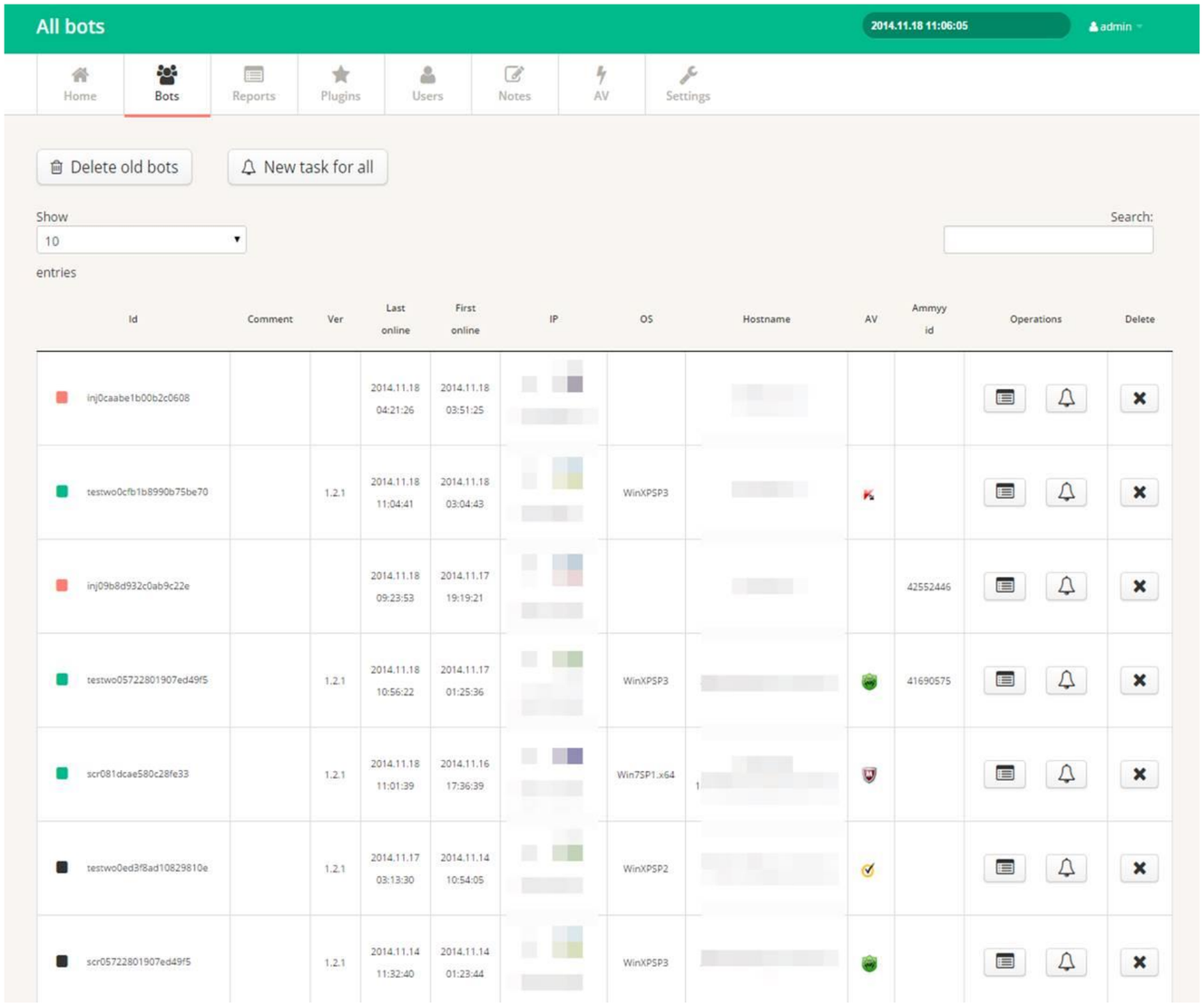


Современная инфраструктура APT атаки Lazarus



Трехуровневая структура командных серверов.

Интерфейс Anunak C&C.



Обход антивирусов

Статический анализ - сигнатурный:

- Шелл-код из Metasploit – обфусцируем.

Статический эвристический анализ:

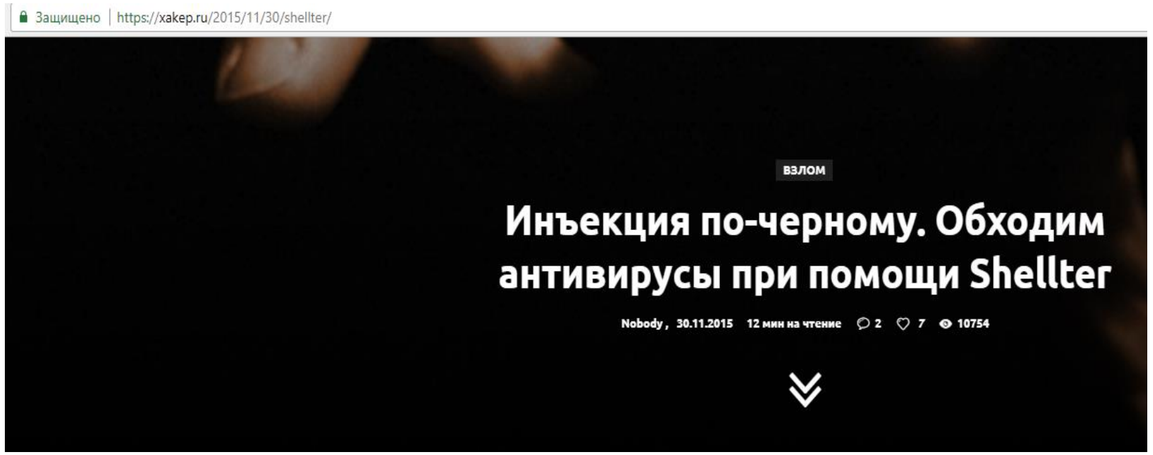
- Шифруем вредоносный код (или просто xor-им)

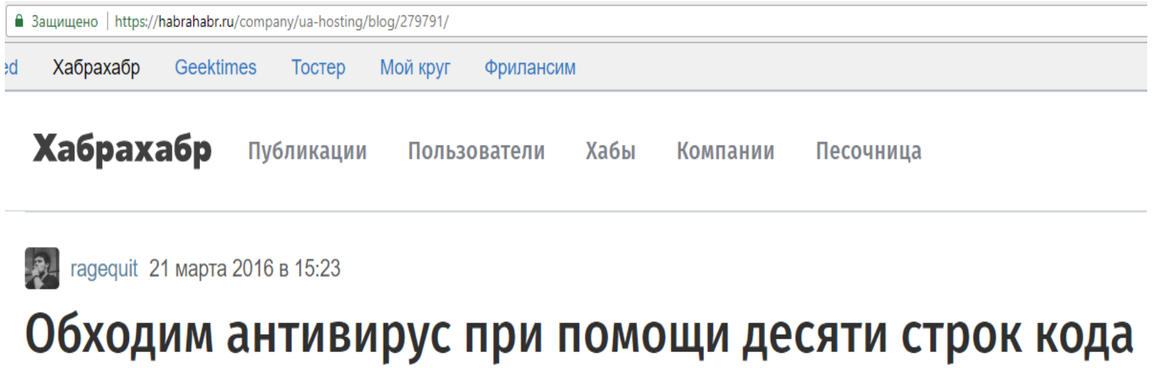
Динамический анализ (эмуляция)

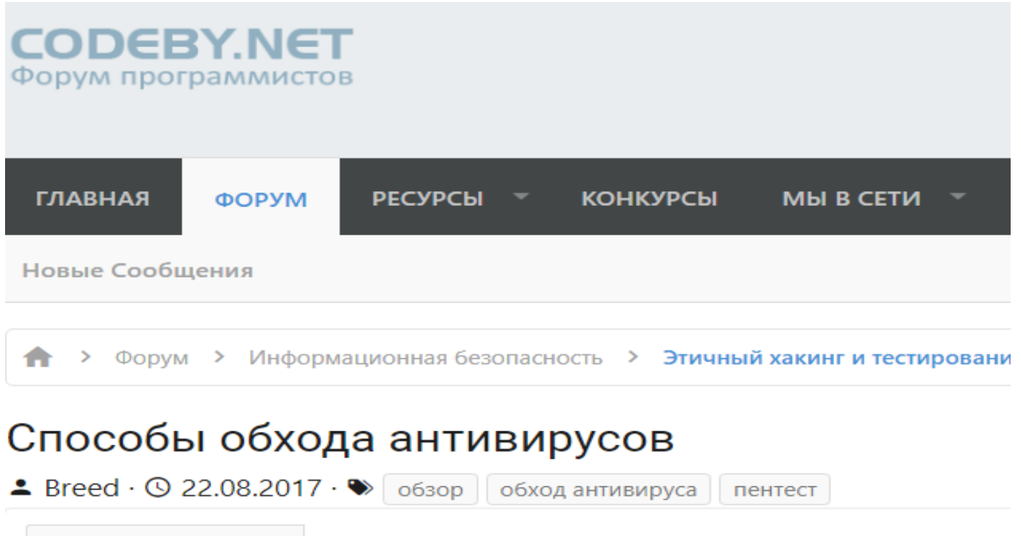
- Проверяем: ресурсы, виртуализацию, ресурсоемкий цикл – проверяем счетчик были ли пропущены операции и тд. Если проверка пройдена расшифровываем

```
#define MAX_OP 100000000
int main() {
int counter = 0;
for( int i =0; i < MAX_OP; i++ ) counter++;
if( counter == MAX_OP ) {
DecryptAndRunPayload();
}
return 0;
}
```

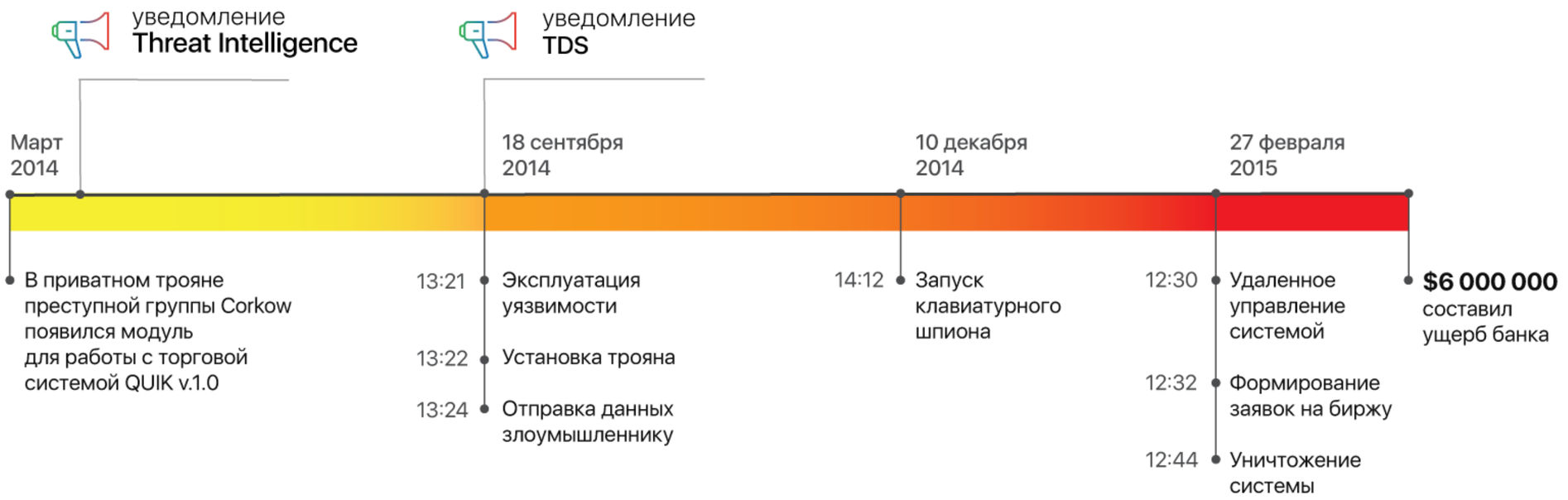
Это все старые техники и они не работают ?







Timeline APT атаки Corkow.

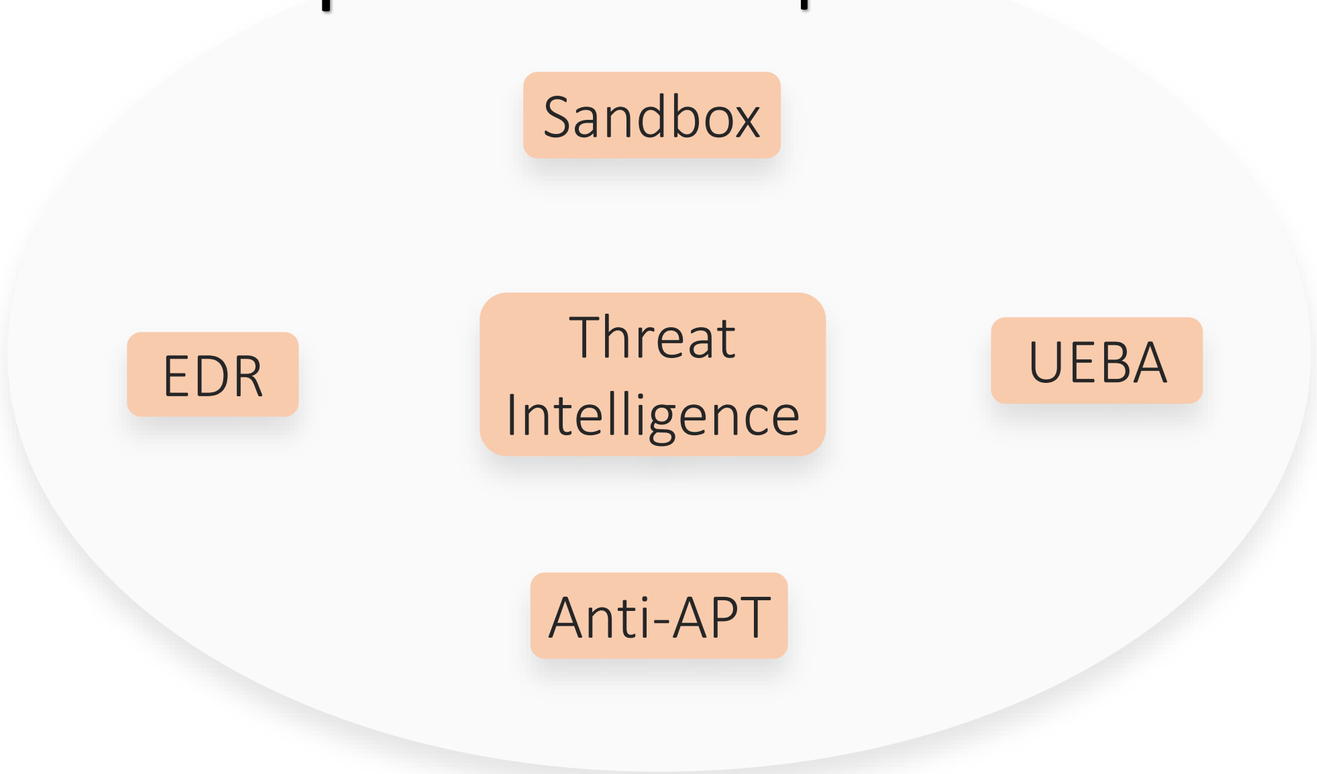


Мобильные устройства

- 2017 – **Maza-in, RATAttack, CopyCat, Gooligan, DressCode** и др
- Ущерб от мобильных банк.троянов превысил ущерб от ПК троянов.
- Архитектура препятствует возможности эффективной защиты в принципе – только сигнатурные методы
- Много зараженных приложений в Apple Store и Google Play.

Как жить в XXI веке?

Время – бесценно!



Защищайтесь правильно!

Фишман Антон
Group-IB