



# Классический антивирус умер

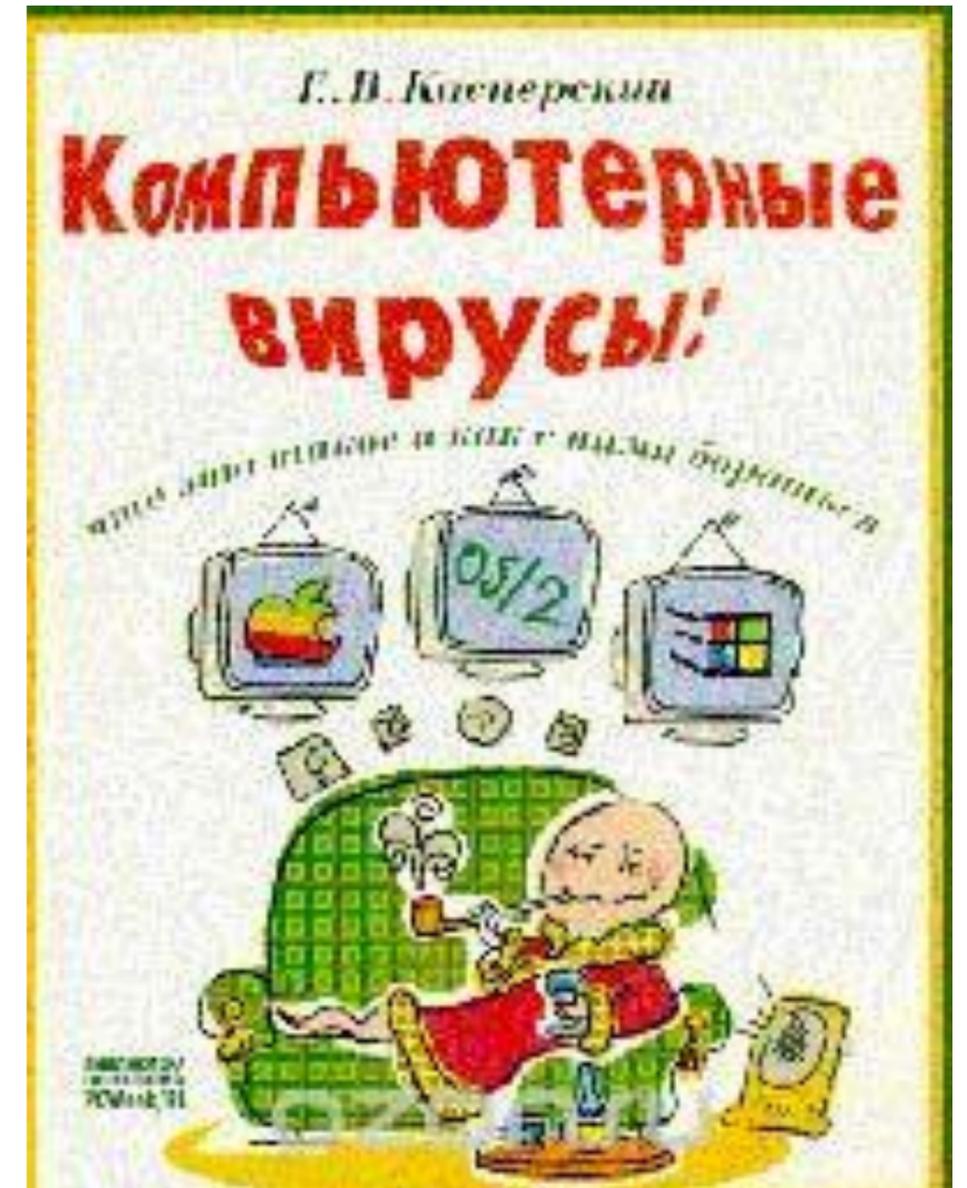
Что делать и чем заменить ?

Фишман Антон  
Group-IB



Слухи о моей смерти несколько преувеличены

(с) Марк Твен





# Вирусология XX в. Vs XXI в.



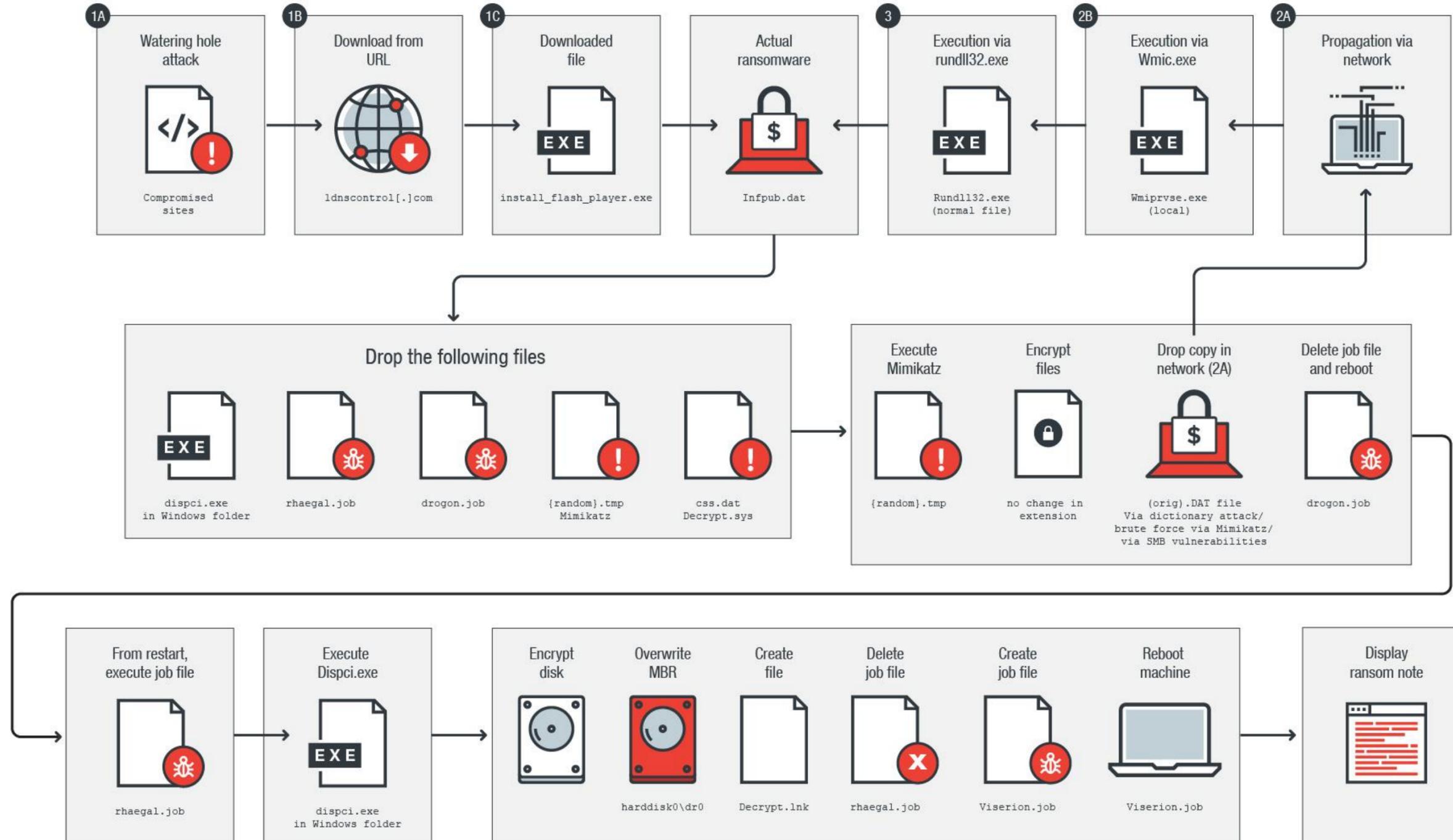
## XX

- 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





# Интерфейс Анубак C&C.



**All bots** 2014.11.18 11:06:05 admin

Home Bots Reports Plugins Users Notes AV Settings

Delete old bots New task for all

Show: 10 entries Search:

| Id                      | Comment | Ver   | Last online            | First online           | IP | OS          | Hostname | AV | Ammy id  | Operations | Delete |
|-------------------------|---------|-------|------------------------|------------------------|----|-------------|----------|----|----------|------------|--------|
| inj0caabe1b00b2c0608    |         |       | 2014.11.18<br>04:21:26 | 2014.11.18<br>03:51:25 |    |             |          |    |          |            |        |
| testwo0cfb1b8990b75be70 |         | 1.2.1 | 2014.11.18<br>11:04:41 | 2014.11.18<br>03:04:43 |    | WinXPSP3    |          |    |          |            |        |
| inj09b8d932c0ab9c22e    |         |       | 2014.11.18<br>09:23:53 | 2014.11.17<br>19:19:21 |    |             |          |    | 42552446 |            |        |
| testwo05722801907ed49f5 |         | 1.2.1 | 2014.11.18<br>10:56:22 | 2014.11.17<br>01:25:36 |    | WinXPSP3    |          |    | 41690575 |            |        |
| scr081dcae580c28fe33    |         | 1.2.1 | 2014.11.18<br>11:01:39 | 2014.11.16<br>17:36:39 |    | Win7SP1.x64 |          |    |          |            |        |
| testwo0ed3f8ad10829810e |         | 1.2.1 | 2014.11.17<br>03:13:30 | 2014.11.14<br>10:54:05 |    | WinXPSP2    |          |    |          |            |        |
| scr05722801907ed49f5    |         | 1.2.1 | 2014.11.14<br>11:32:40 | 2014.11.14<br>01:23:44 |    | WinXPSP3    |          |    |          |            |        |



# Обход антивирусов



## *Статический анализ - сигнатурный:*

- Шелл-код из Metasploit – обфусцируем.

## *Статический эвристический анализ:*

- Шифруем вредоносный код (или просто хог-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 ?



Защищено | <https://xakep.ru/2015/11/30/shellter/>

**ВЗЛОМ**

## Инъекция по-черному. Обходим антивирусы при помощи Shellter

Nobody, 30.11.2015 12 мин на чтение 2 7 10754

⇩

Защищено | <https://www.securitylab.ru/blog/personal/crypto-anarchist/340059.php>

Новости Уязвимости Статьи Софт

[Главная](#) / [Блоги](#) / [Личные блоги](#) / [Криптоанархист](#)

16 Февраля, 2017

## Как обойти антивирус за 5 минут

[Булат Шамсутдинов](#)

Защищено | <https://habrahabr.ru/company/ua-hosting/blog/279791/>

Хабрахабр Geektimes Тостер Мой круг Фрилансим

**Хабрахабр** Публикации Пользователи Хабы Компании Песочница

ragequit 21 марта 2016 в 15:23

## Обходим антивирус при помощи десяти строк кода

**CODEBY.NET**  
Форум программистов

ГЛАВНАЯ **ФОРУМ** РЕСУРСЫ КОНКУРСЫ МЫ В СЕТИ

Новые Сообщения

[🏠](#) > [Форум](#) > [Информационная безопасность](#) > [Этичный хакинг и тестировани](#)

## Способы обхода антивирусов

Breed · 22.08.2017 · обзор обход антивируса пентест



# Timeline APT атаки Corkow.





# Мобильные устройства



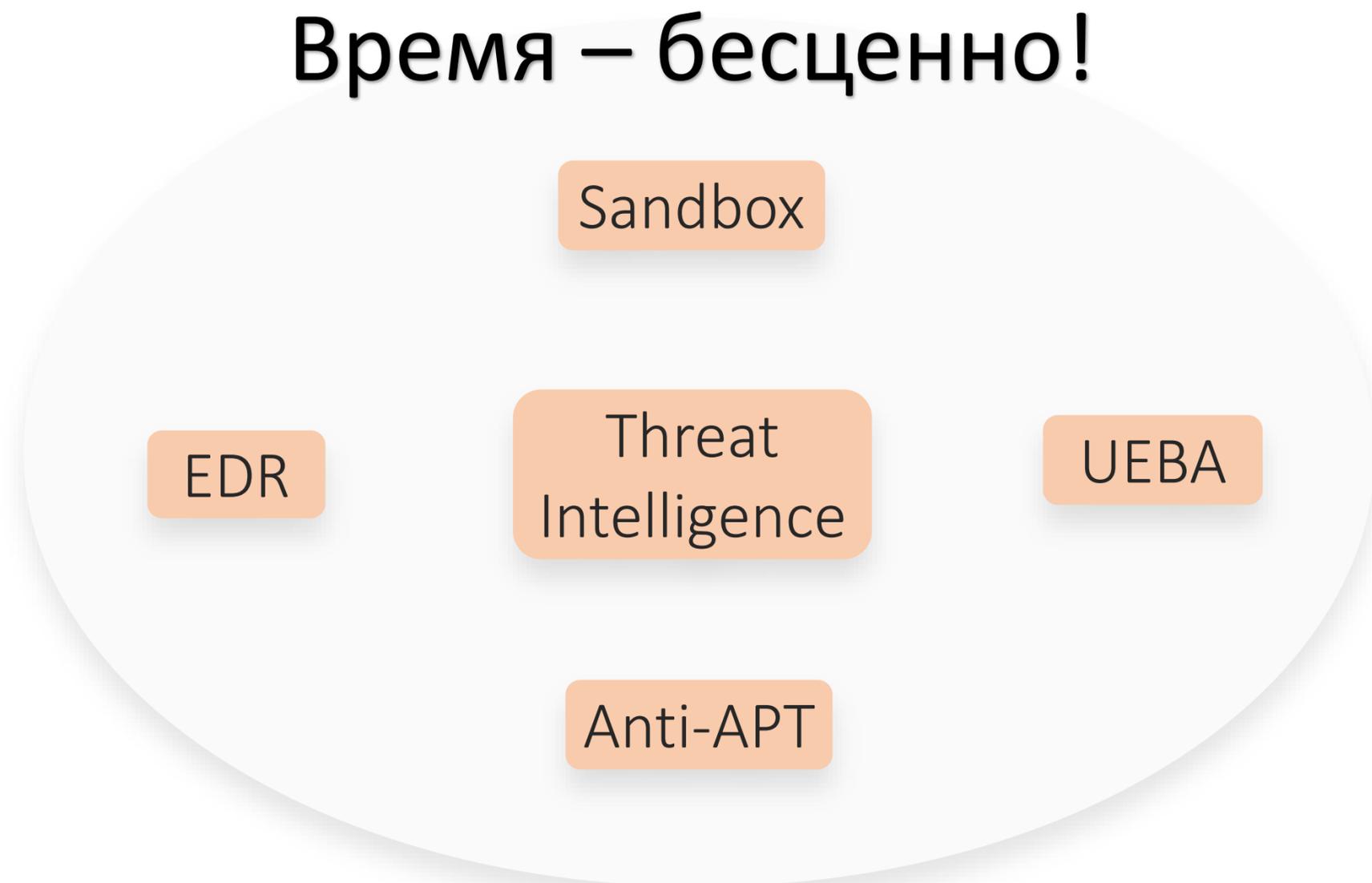
- 2017 – Maza-in, RATAttack, CopyCat, Gooligan, DressCode и др
- Ущерб от мобильных банк.троянов превысил ущерб от ПК троянов.
- Архитектура препятствует возможности эффективной защиты в принципе – только сигнатурные методы
- Много зараженных приложений в Apple Store и Google Play.

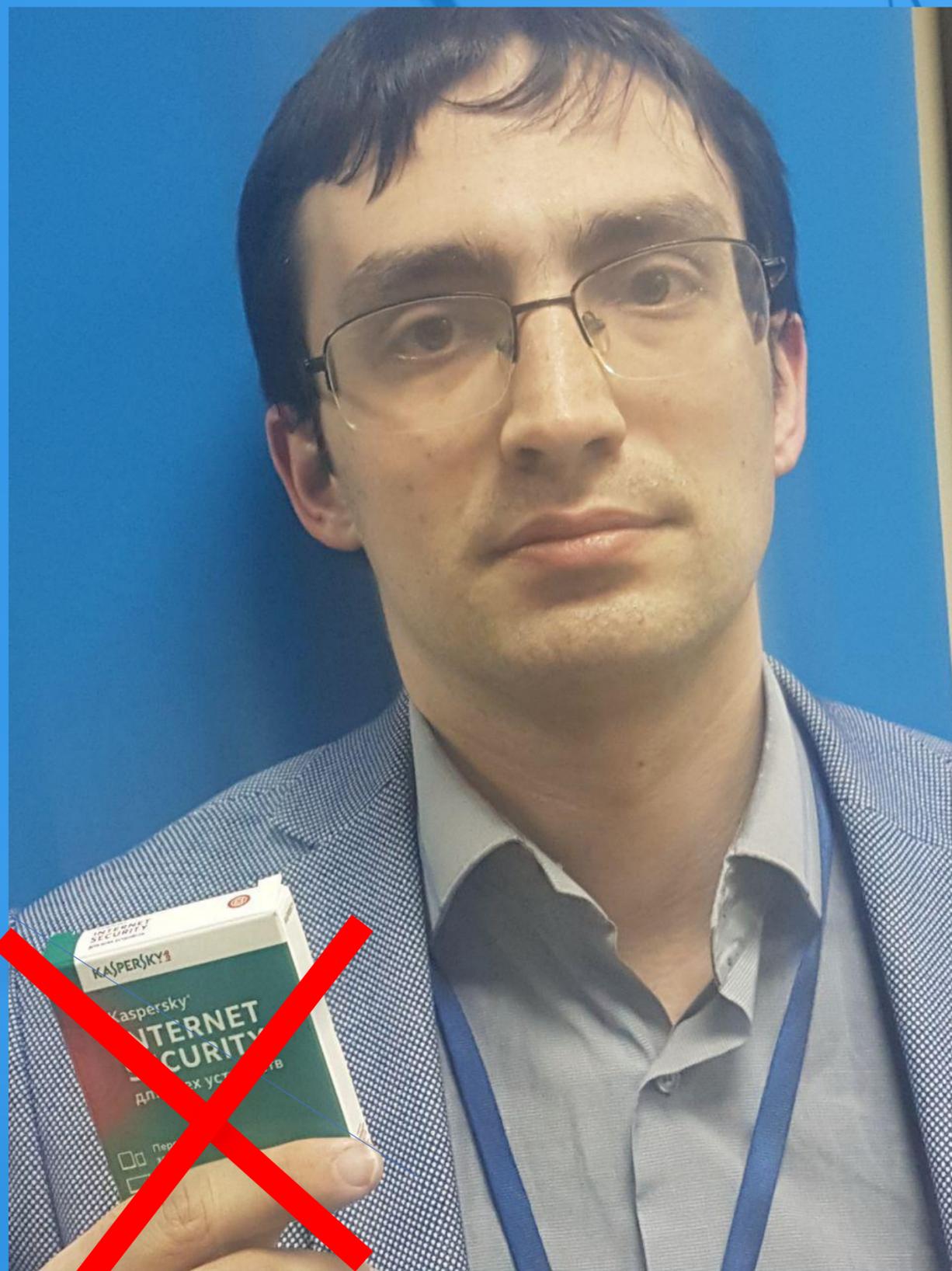


# Как жить в XXI веке?



## Время – бесценно!





Защитайтесь  
правильно!

Фишман Антон  
Group-IB