Трояны-вымогатели и применяемые ими криптографические средства

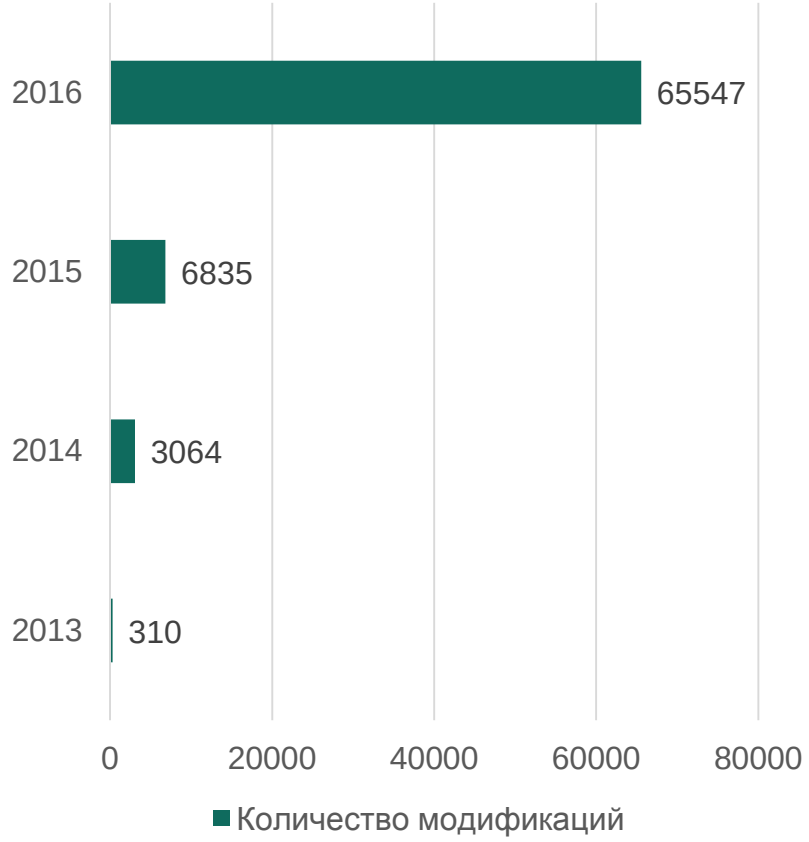
Федор Синицын, Лаборатория Касперского

KASPERSKY lab

Трояны-вымогатели

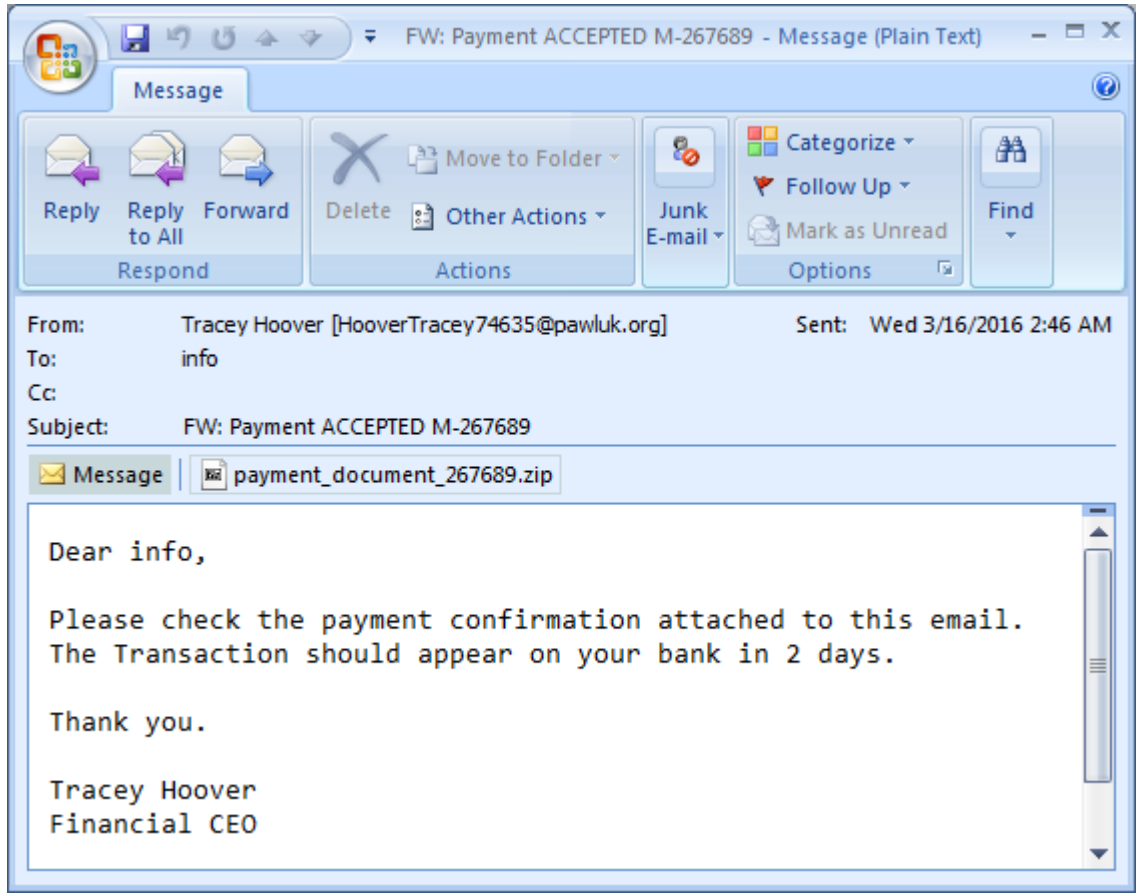
- Без ведома пользователя блокируют ПК, браузер или шифруют файлы/целые разделы
  - Блокировщики экрана
  - Блокировщики MBR
  - Шифровальщики
- Требуют деньги за разблокировку / расшифровку

Шифровальщики



Трояны-шифровальщики. Распространение

- Спам-рассылки
  - Сам шифровальщик в аттаче
  - Загрузчик в аттаче (PE, js, doc с макросами)
  - Ссылка на шифровальщик/загрузчик в теле
- Эксплоит-паки
- Заражение злоумышленниками вручную



Что шифруют?

- Файлы на локальных дисках
  - Целиком
  - Частично (заголовок/всё кроме заголовка/случайные области)
- Файлы на сетевых дисках
- Разделы локальных дисков целиком
- Системные области дисков и разделов (MBR, MFT)

Чем шифруют?

Были обнаружены трояны, использующие:

- Самописные симметричные шифры
- Стандартные симметричные шифры
- Стандартные асимметричные шифры
- Комбинации

Реализация шифров почти всегда библиотечная (CryptoAPI, OpenSSL, mbedtls, axTLS, LibTomCrypt и т.д.)

Схемы распределения ключей

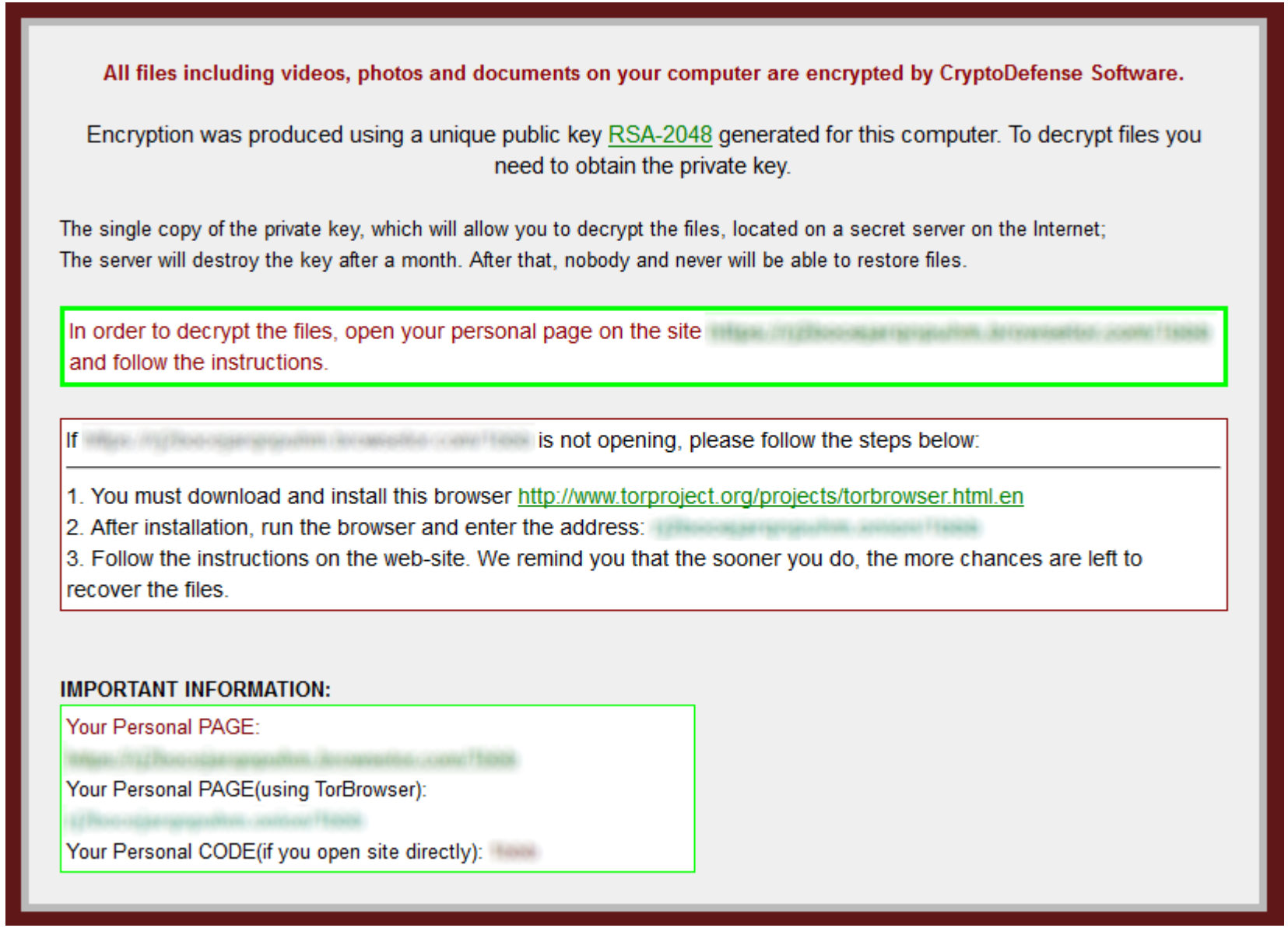
- Ключ один на всех жертв, содержится в теле трояна
- Ключ генерируется на C&C и отправляется трояну по запросу
- Ключ генерируется на зараженном ПК и отправляется на C&C
- Ключ генерируется на зараженном ПК, шифруется и сохраняется

Примеры из реальной жизни

KASPERSKY lab

CryptoDefense

- RSA-2048
- MS CryptoAPI



CryptoDefense

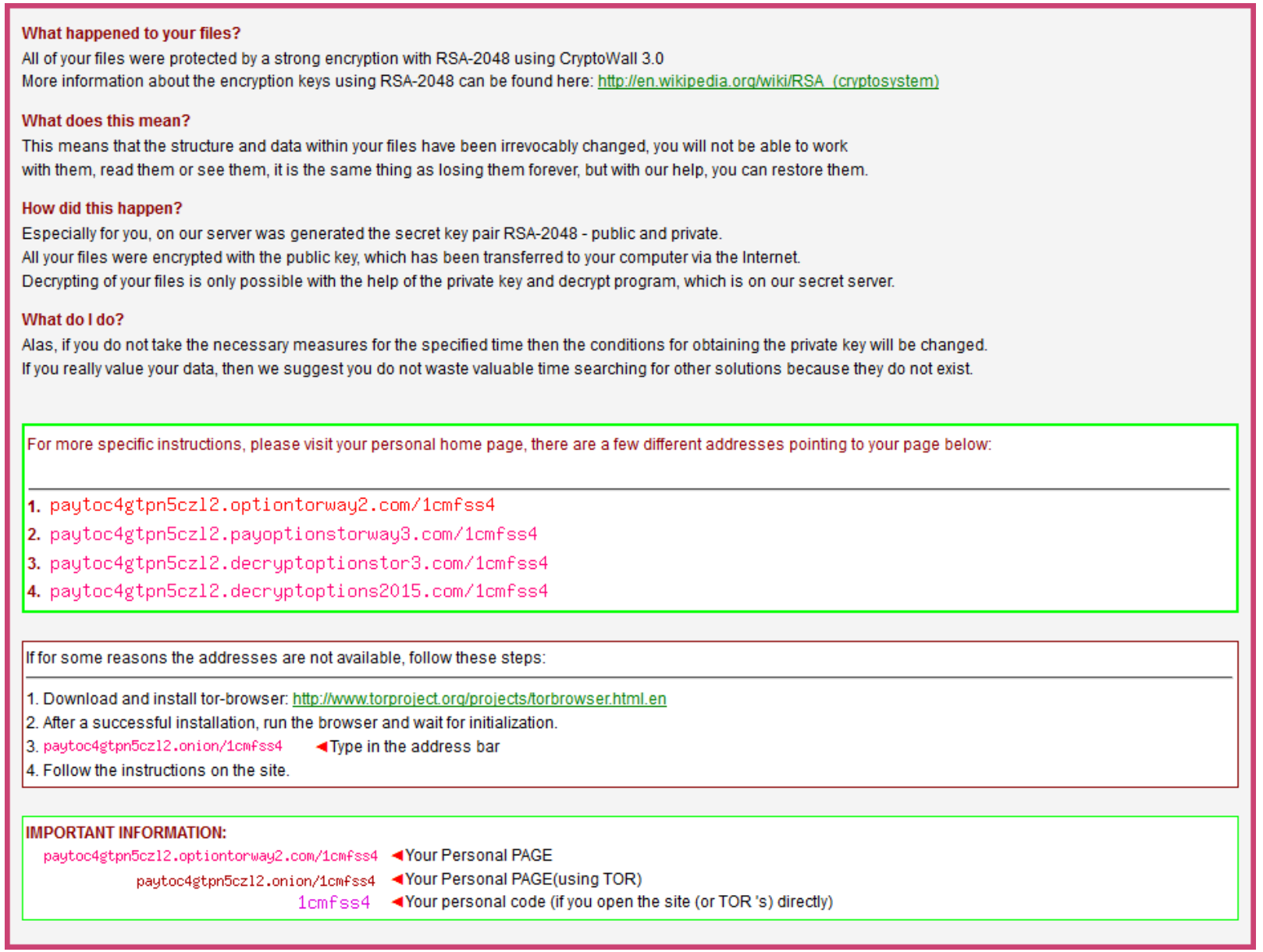
- При заражении генерирует RSA_{pub} + RSA_{priv}
- Отправляет RSA_{priv} на C&C
- Шифрует файлы целиком на RSA_{pub}

Слабости:

1. Можно перехватить трафик с RSA_{priv}
2. Ошибка при использовании CryptoAPI – не удаляет за собой RSA_{priv} на зараженном ПК

CryptoWall

- «Улучшенная» версия CryptoDefense
- AES-256 CBC
- RSA-2048



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. paytoc4gtpn5czl2.optiontorway2.com/1cmfss4
2. paytoc4gtpn5czl2.payoptionstorway3.com/1cmfss4
3. paytoc4gtpn5czl2.decryptoptionstor3.com/1cmfss4
4. paytoc4gtpn5czl2.decryptoptions2015.com/1cmfss4

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. paytoc4gtpn5czl2.onion/1cmfss4 ◄Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
paytoc4gtpn5czl2.optiontorway2.com/1cmfss4 ◄Your Personal PAGE
paytoc4gtpn5czl2.onion/1cmfss4 ◄Your Personal PAGE(using TOR)
1cmfss4 ◄Your personal code (if you open the site (or TOR 's) directly)

CryptoWall

Комбинированная схема AES+RSA

- Получает публичный ключ RSA-2048 от C&C
- Уникальный ключ AES-256 на каждый файл (CryptGenKey)
- Файлы шифрует целиком AES-256 CBC, iv = 0, PKCS5 padding
- Шифрует им ключи AES, помещает результат в зашифрованные файлы

CTB-Locker

- AES-256 ECB
- Диффи-Хеллман на эллиптической кривой (ECDH)
- Кривая Curve25519

CTB-Locker

- В теле трояна содержится $EC_{master}pub$
- При заражении генерирует: $EC_{session}priv$ + $EC_{session}pub$
- K_S = ECDH($EC_{master}pub$, $EC_{session}priv$)
- $EC_{session}priv$ шифрует AES с ключом SHA256(K_s) и отправляет на сервер
- $EC_{session}pub$ отправляет на сервер в открытом виде
- На каждый файл:
  - Новая пара $EC_{file}priv$ + $EC_{file}pub$
  - K_f = ECDH($EC_{session}pub$, $EC_{file}priv$)
  - Шифрует файл AES с ключом SHA256(K_f)

TorLocker

- AES-256 ECB
- RSA-2048

TorLocker

- В теле трояна содержатся 128 публичных ключей RSA-2048
- Использует 1 из них, выбор по формуле на основе имени ПК, серийного номера системного диска
- На каждый файл генерирует ключ K (256 бит, CryptGenRandom)
- Шифрует максимум 512Мб файла AES-256 ECB с ключом K
- В конец файла помещает RSA(K)

Слабости:

1. Малые публичные экспоненты (3, 5, 7)
2. Шифрует RSA без паддинга

Rack (ранняя модификация)

aka TorrentLocker, Teerac, Racketeer

- AES-256 CTR
- RSA-2048
- LibTomCrypt

Rack (ранняя модификация)

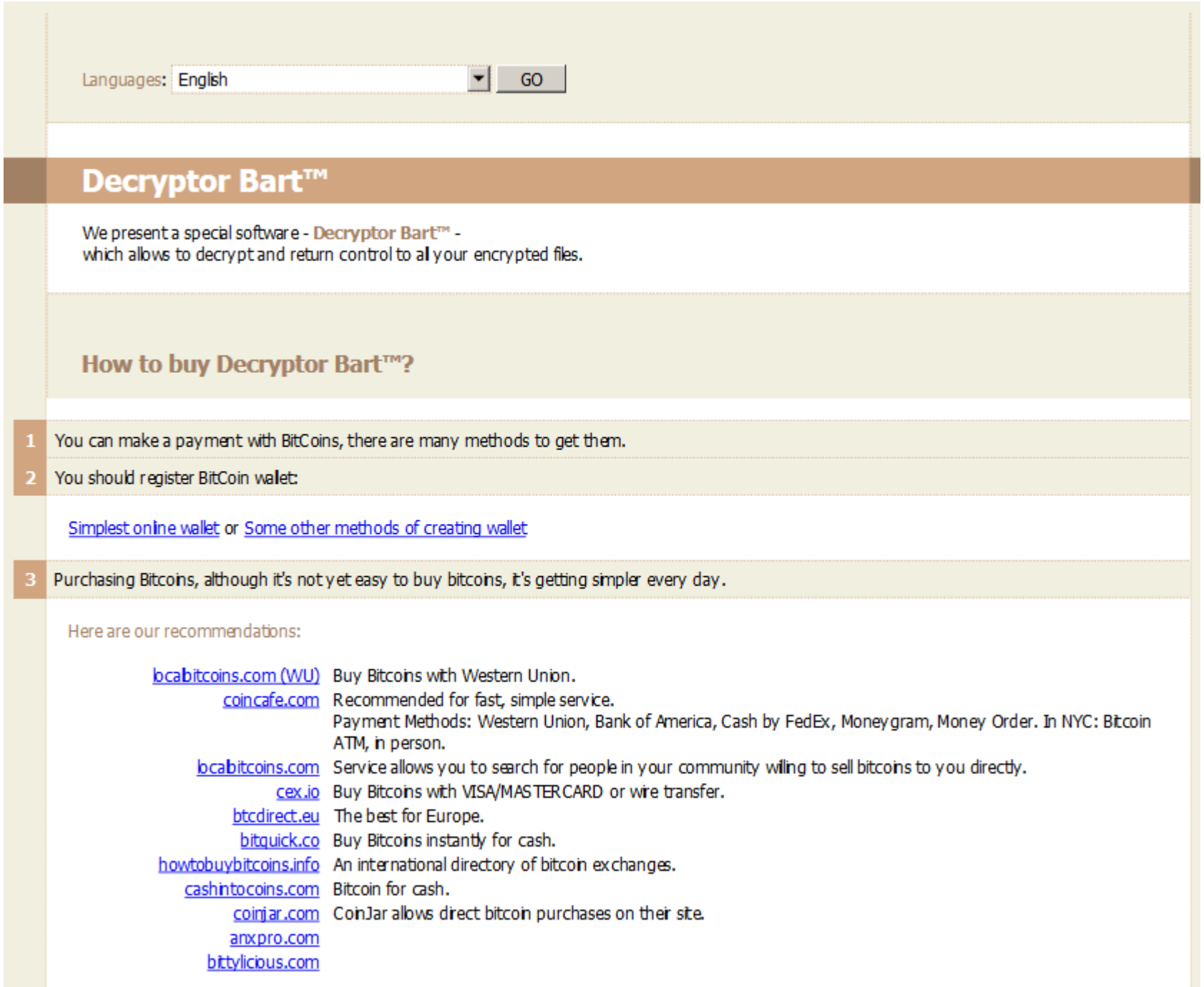
- В теле трояна содержится публичный ключ RSA-2048
- Генерирует ключ K (256 бит) – один на все файлы. ГПСЧ Yarrow
- В реестре сохраняет RSA(K)
- Шифрует первые 2Мб файла AES-256 CTR с ключом K, nonce фиксированный на все файлы

Слабость:

Один ключ и nonce на все файлы + режим CTR

Bart

- Запароленные zip-архивы
- ECDH
- Кривая secp256r1



Bart

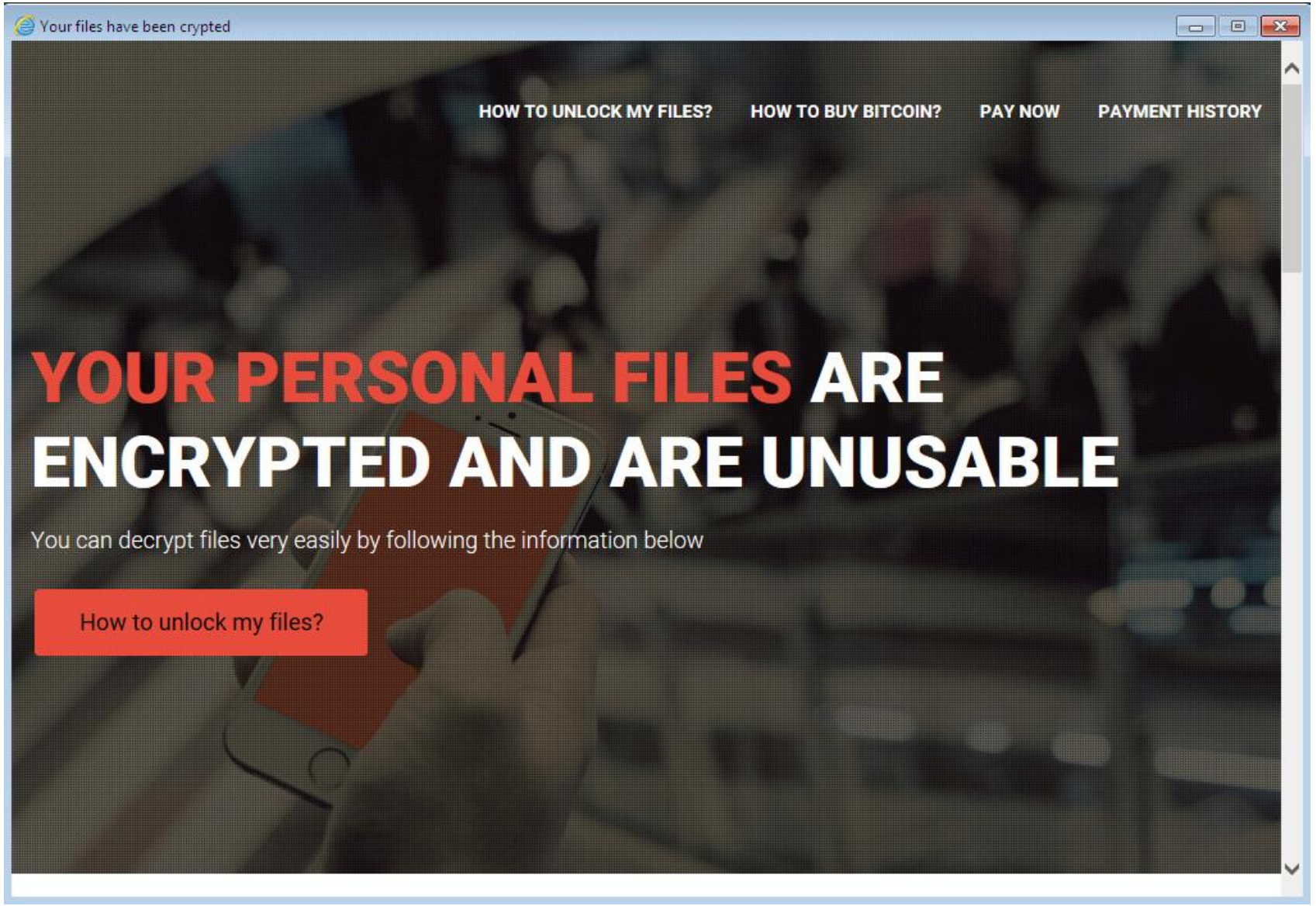
- В теле трояна содержится $EC_{master}pub$
- При заражении генерирует: $EC_{session}priv$ + $EC_{session}pub$
- K_S = ECDH($EC_{master}pub$, $EC_{session}priv$)
- Сжимает файлы в zip-архивы с паролем: base64(K_s)
- В тексте требований сохраняет: base64($EC_{session}pub$)

Слабости:

1. Удаляет оригинальные файлы без перезаписи
2. Слабый шифр ZipCrypto поддается атаке KPA

Goopic

- RC4
- ¯_(ツ)_/¯


Your files have been crypted
HOW TO UNLOCK MY FILES?
HOW TO BUY BITCOIN?
PAY NOW
PAYMENT HISTORY
YOUR PERSONAL FILES ARE ENCRYPTED AND ARE UNUSABLE
You can decrypt files very easily by following the information below
How to unlock my files?

Goopic

- Генерирует K (2048 бит), отправляет его на сервер C&C
- Шифрует файлы модифицированным RC4

Слабости:

1. Можно перехватить трафик
2. Один ключ RC4 на все файлы => KPA
3. Нестойкий ГПСЧ rand() из C stdlib

$X_{n+1} = 214013 * X_n + 2531011 \pmod{2^{31} - 1}$

KASPERSKY lab

Итоги

- Разработчики троянов порой допускают ошибки
- Даже если реализовано всё верно, иногда расшифровать удается благодаря содействию с правоохранительными органами

https://nomoreransom.org

Защита и предотвращение:

- Резервное копирование
- Обучение персонала, обновление ПО
- Стойкие пароли на системах удаленного доступа
- Защитные решения с проактивным детектированием

Вопросы и ответы

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab