

Трояны-вымогатели и применяемые ими криптографические средства

Федор Синицын, Лаборатория Касперского

Трояны-вымогатели

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

ВНИМАНИЕ!

Ваша операционная система заблокирована за нарушение использования сети интернет.
Обнаружены следующие нарушения:
Посещение сайтов порнографического содержания с элементами детской порнографии, насилия, зоофилии.
Данная блокировка предпринята для устранения возможности распространения данных материалов с Вашего ПК в сети Интернет.
Для разблокировки операционной системы вам необходимо оплатить 400 рублей.

ОПЛАТА С ВАШЕГО МОБИЛЬНОГО ТЕЛЕФОНА:

- Если Вы абонент Билайн, отправьте СМС с текстом: 9629065326 400 на номер 3116
В ответном сообщении подтвердите Ваш платеж.
После оплаты, в ответном СМС придет код доступа к системе.
- Если Вы абонент Мегафон, отправьте СМС с текстом: 9629065326 400 на номер 84444
В ответном сообщении подтвердите Ваш платеж.
После оплаты, в ответном СМС придет код доступа к системе.

Если Вы абонент МТС, введите команду *115#

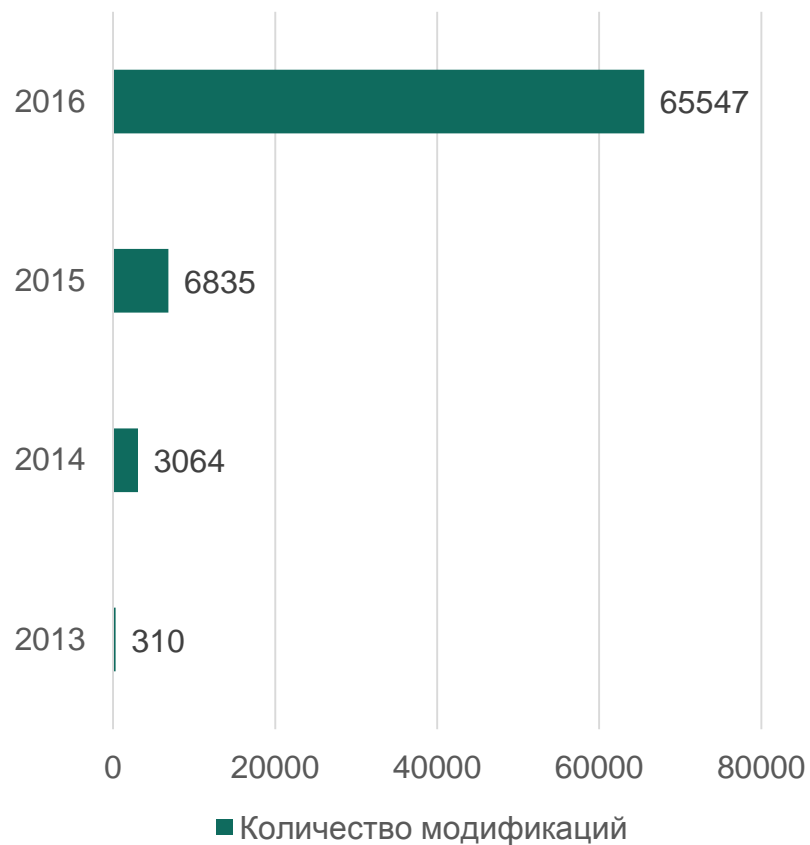
Далее выберите "Связь"."Билайн".номер телефона 9629065326 сумма 400 рублей.
В ответном сообщении подтвердите Ваш платеж.

ОПЛАТА ЧЕРЕЗ ТЕРМИНАЛ ДЛЯ ОПЛАТЫ СОТОВОЙ СВЯЗИ:

Пополните номер абонента Билайн № 9629065326 на сумму 400 рублей
На выданном чеке будет написан код доступа к системе. Введите его в форму ниже.

Ввести код

Шифровальщики



Троянцы-вымогатели

2016 год в цифрах

Появилось

62

новых семейств
троянцев-
вымогателей



Один атакованный пользователь

1 Кв. каждые 20 секунд

3 Кв. каждые 10 секунд

Одна атакованная компания

1 Кв. каждые 2 минуты

3 Кв. каждые 40 секунд

Количество новых модификаций вымогателей выросло

в 11 раз

2,900
1 Кв.

32,091

3 Кв.



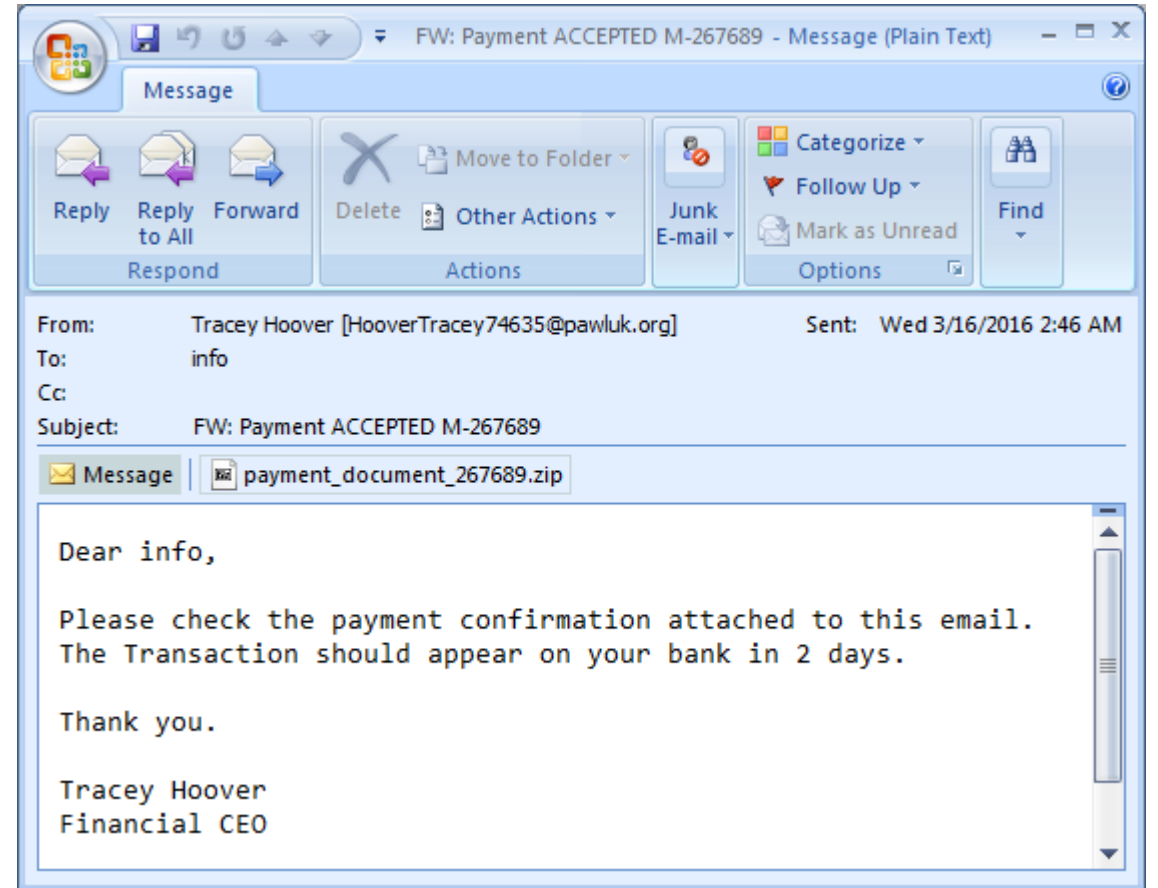
1 из 5 СМБ компаний
заплативших выкуп, так и не
получила доступ к своим
данным

Все статистические данные получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN)

© 2016 АО Kaspersky Lab. All Rights Reserved.

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 (заголовки/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 С&С и отправляется трояну по запросу
- Ключ генерируется на зараженном ПК и отправляется на С&С
- Ключ генерируется на зараженном ПК, шифруется и сохраняется

Примеры из реальной жизни

CryptoDefense

- RSA-2048
- MS CryptoAPI

All files including videos, photos and documents on your computer are encrypted by CryptoDefense Software.

Encryption was produced using a unique public key [RSA-2048](#) generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; The server will destroy the key after a month. After that, nobody and never will be able to restore files.

In order to decrypt the files, open your personal page on the site [https://123kasperdefense.com/123456](#) and follow the instructions.

If [https://123kasperdefense.com/123456](#) is not opening, please follow the steps below:

1. You must download and install this browser <http://www.torproject.org/projects/torbrowser.html.en>
2. After installation, run the browser and enter the address: [https://123kasperdefense.com/123456](#)
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

IMPORTANT INFORMATION:

Your Personal PAGE:

[https://123kasperdefense.com/123456](#)

Your Personal PAGE(using TorBrowser):

[https://123kasperdefense.com/123456](#)

Your Personal CODE(if you open site directly): [123456](#)

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_\(cryptosystem\)](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. paytoc4gtpn5cz12.optiontorway2.com/1cmfss4
2. paytoc4gtpn5cz12.payoptionstorway3.com/1cmfss4
3. paytoc4gtpn5cz12.decryptoptionstor3.com/1cmfss4
4. paytoc4gtpn5cz12.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. paytoc4gtpn5cz12.onion/1cmfss4 ◀ Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

- paytoc4gtpn5cz12.optiontorway2.com/1cmfss4 ◀ Your Personal PAGE
- paytoc4gtpn5cz12.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

Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 92 18 34 Next >>

СТВ-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

唐澤タカヒロッカー

警告



日本の法律に違反するファイルがお使いのパソコンから検出されたため、パソコンをロックしました。

ロックの解除をには、左に表示されている日時までに罰金として三十万円をBitcoinで支払わなければならない。

この日時までに誠意ある対応なき場合は、ロックが解除されることは永遠にありません。

俺は君に人を傷付けるのではなく人を助ける人間になってほしい

俺は君の20年後を見ている

※このソフトウェアを削除したり、ウイルス対策ソフトで駆除を行っても、問題は解決しません。

2/ 4/2015
23:00:00

残り時間
71:59:29

この件に関するお問い合わせ

恒心綜合法律事務所
東京都港区虎ノ門3丁目16番7号
ピュア虎ノ門4階
TEL: 03-6435-8073
takahiro.karasawa@koushin-lawfirm.jp

ロックされたファイル

次へ

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

Languages:

Decryptor Bart™

We present a special software - **Decryptor Bart™** - which allows to decrypt and return control to all your encrypted files.

How to buy Decryptor Bart™?

- 1 You can make a payment with BitCoins, there are many methods to get them.
- 2 You should register BitCoin wallet:
[Simplest online wallet](#) or [Some other methods of creating wallet](#)
- 3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

locabitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
locabitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bitylicious.com	

Bart

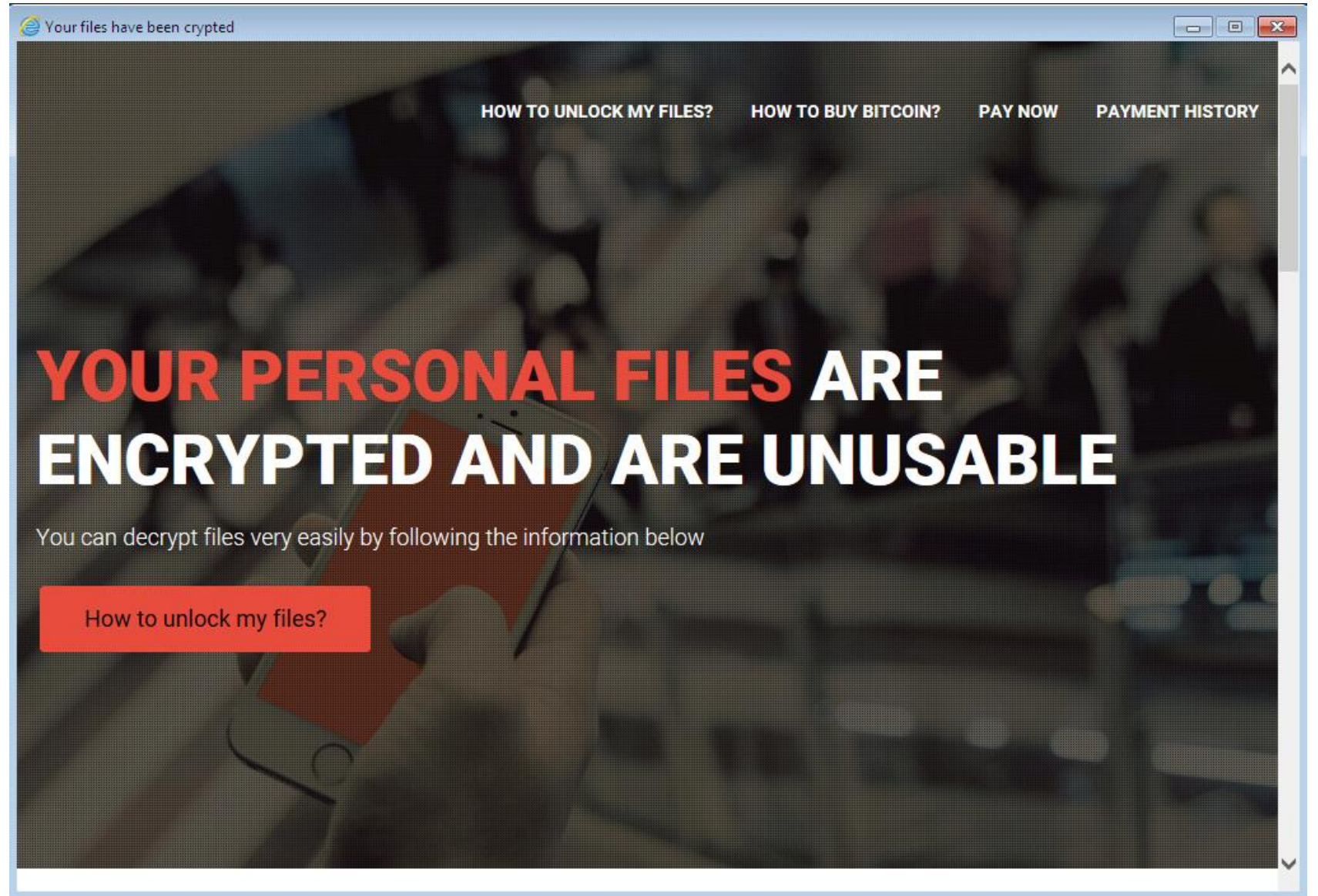
- В теле трояна содержится $EC_{\text{master}}\text{pub}$
- При заражении генерирует: $EC_{\text{session}}\text{priv} + EC_{\text{session}}\text{pub}$
- $K_S = \text{ECDH}(EC_{\text{master}}\text{pub}, EC_{\text{session}}\text{priv})$
- Сжимает файлы в zip-архивы с паролем: $\text{base64}(K_S)$
- В тексте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

Слабости:

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

Goopic

- RC4
- _(ツ)_/



Goopіc

- 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 => КРА
3. Нестойкий ГПСЧ rand() из C stdlib

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

Итоги

- Разработчики троянов порой допускают ошибки
- Даже если реализовано всё верно, иногда расшифровать удастся 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 