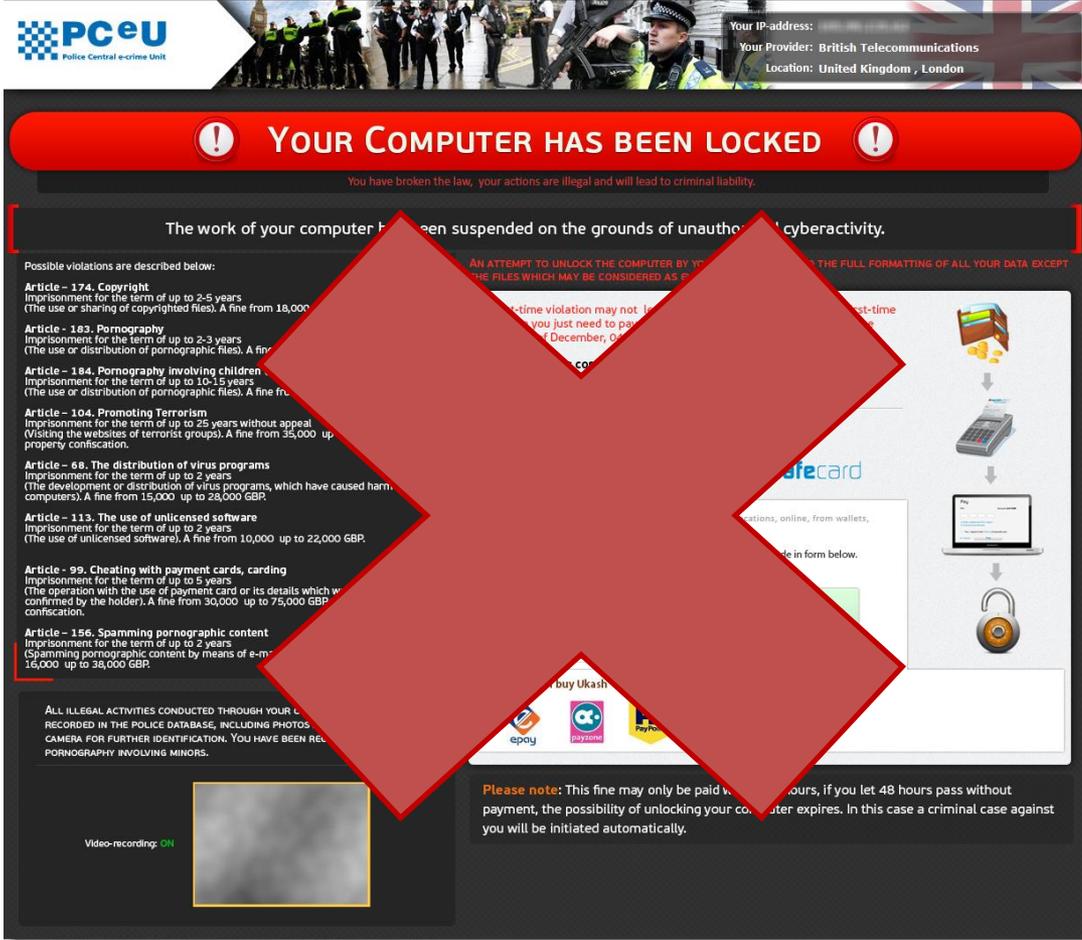


Dead and Buried in Their Crypts: Defeating Modern Ransomware



Samir Mody
Gregory Panakkal

Screen Lockers not Covered



PCEU
Police Central e-crime Unit

Your IP-address:
Your Provider: British Telecommunications
Location: United Kingdom, London

! YOUR COMPUTER HAS BEEN LOCKED !

You have broken the law, your actions are illegal and will lead to criminal liability.

The work of your computer has been suspended on the grounds of unauthorised cyberactivity.

Possible violations are described below:

- Article - 174. Copyright**
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files). A fine from 18,000
- Article - 183. Pornography**
Imprisonment for the term of up to 2-3 years
(The use or distribution of pornographic files). A fine from
- Article - 184. Pornography involving children**
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files). A fine from
- Article - 104. Promoting Terrorism**
Imprisonment for the term of up to 25 years without appeal
(Visiting the websites of terrorist groups). A fine from 35,000 up to property confiscation.
- Article - 68. The distribution of virus programs**
Imprisonment for the term of up to 2 years
(The development or distribution of virus programs, which have caused harm to computers). A fine from 15,000 up to 28,000 GBP.
- Article - 113. The use of unlicensed software**
Imprisonment for the term of up to 2 years
(The use of unlicensed software). A fine from 10,000 up to 22,000 GBP.
- Article - 99. Cheating with payment cards, carding**
Imprisonment for the term of up to 5 years
(The operation with the use of payment card or its details which was confirmed by the holder). A fine from 30,000 up to 75,000 GBP confiscation.
- Article - 156. Spamming pornographic content**
Imprisonment for the term of up to 2 years
(Spamming pornographic content by means of e-mail). A fine from 16,000 up to 38,000 GBP.

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER ARE RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS TAKEN BY A CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN RECORDED FOR PORNOGRAPHY INVOLVING MINORS.

Video-recording: ON

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires. In this case a criminal case against you will be initiated automatically.

Our Targets – File Encryptors

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. NO INSTRUCTION.

[View](#)

tion with RSA-2048 using CryptoWall.

RSA-204

r files hav
thing as

the secret

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

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 only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files press button to open your personal page [File decryption site](#) and follow the instruction.

In case of "File decryption button" malfunction use one of our gates:
<http://34r6hq26q2h4jkzj.42k2b14.net>
<https://34r6hq26q2h4jkzj.tor2web.fi>

Use your Bitcoin address to enter the site:
1MDvLuSwqrLDeszkhX41sWBHGDTAC5jnXg
[Click to copy address to clipboard](#)

If both button and reserve gate not opening, please follow the steps:
 You must install this browser www.torproject.org/projects/torbrowser.html.en
 After installation, run the browser and enter address 34r6hq26q2h4jkzj.onion
 Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

[Click for Free Decryption on site](#)

[Show files](#) [Enter Decrypt Key](#)

CryptoLocker Your Personal files are encr

Your personal files encryption produced on this computer documents, etc. Encryption was produced using a unique generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to dec a secret server on the Internet; the server will destroy th specified in this window. After that nobody and never will

To obtain the private key for this computer, which will aut you need pay 1 Bitcoin (~237 USD)

You can easily delete this software, but you must know th never be able to get your original files back.

Disable your antivirus to prevent the removal of this so

For more information on how to buy and send bitcoins, clic open a list of encoded files, click: 'Show Files'.

Do not delete this list, it will be used for decryption. And d

Private key will be destroyed on 8/3/2011 5:22:30 PM

Time left: 165:44:23

Received: 0.00 BTC
Checking wallet.

[Show Files](#) [Pay with Bitcoin](#)

chang
If you
exist.

For n
below

1. <http://www.torproject.org/projects/torbrowser.html.en>
2. <http://34r6hq26q2h4jkzj.onion>
3. <https://1MDvLuSwqrLDeszkhX41sWBHGDTAC5jnXg>

are a few different addresses pointing to your page

Once Bitten...

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.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://ohmva4gbywokzqso.onion.cab> or <http://ohmva4gbywokzqso.tor2web.org> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from <http://torproject.org/>
2. In the Tor Browser open the <http://ohmva4gbywokzqso.onion/>
Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

Write in the following public key in the input form on server. Avoid missprints.

```
F35VL7O-PD7NK3J-56CMMX4-2LB53Z6-64PPAXM-LVKW6XG-JUWBDNP-PCUHQAE  
FRGC7L3-65LKSAD-YJ5CVLZ-T5MNYXN-UUV2NSA-FY56ULM-BXNSTD5-DMYF2YR  
IHDT5QB-O5S3LUP-PUVJHYY-CBBYTWH-MZ3MZAk-2RTM25V-KRZCSYK-HXG4OCO
```

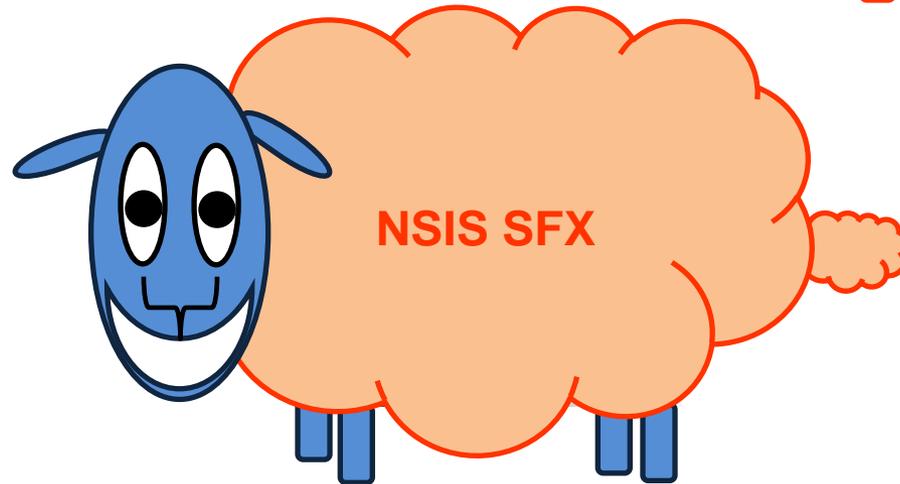
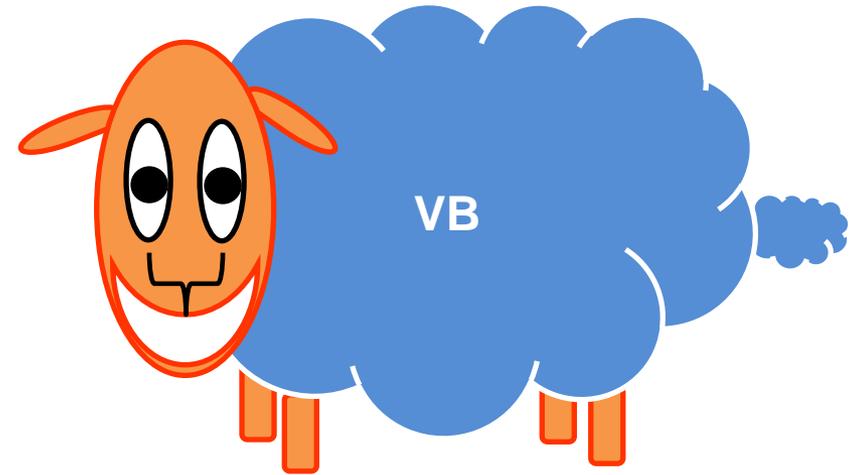
Follow the instructions on the server.

These instructions are also saved to file named DecryptAllFiles.txt in Documents folder. You can open it and use copy-paste for address and key.

...Revenge is Best Served Cold



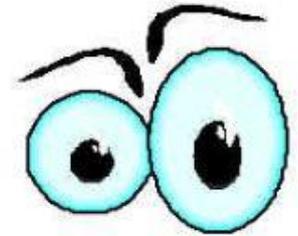
Static Detection Difficult – Packer Obfuscation



Process Injection – Implications for Dynamic Blocking

Into spawned non-OS process

- Potential loss of process context - complicates behaviour tracking and blocking

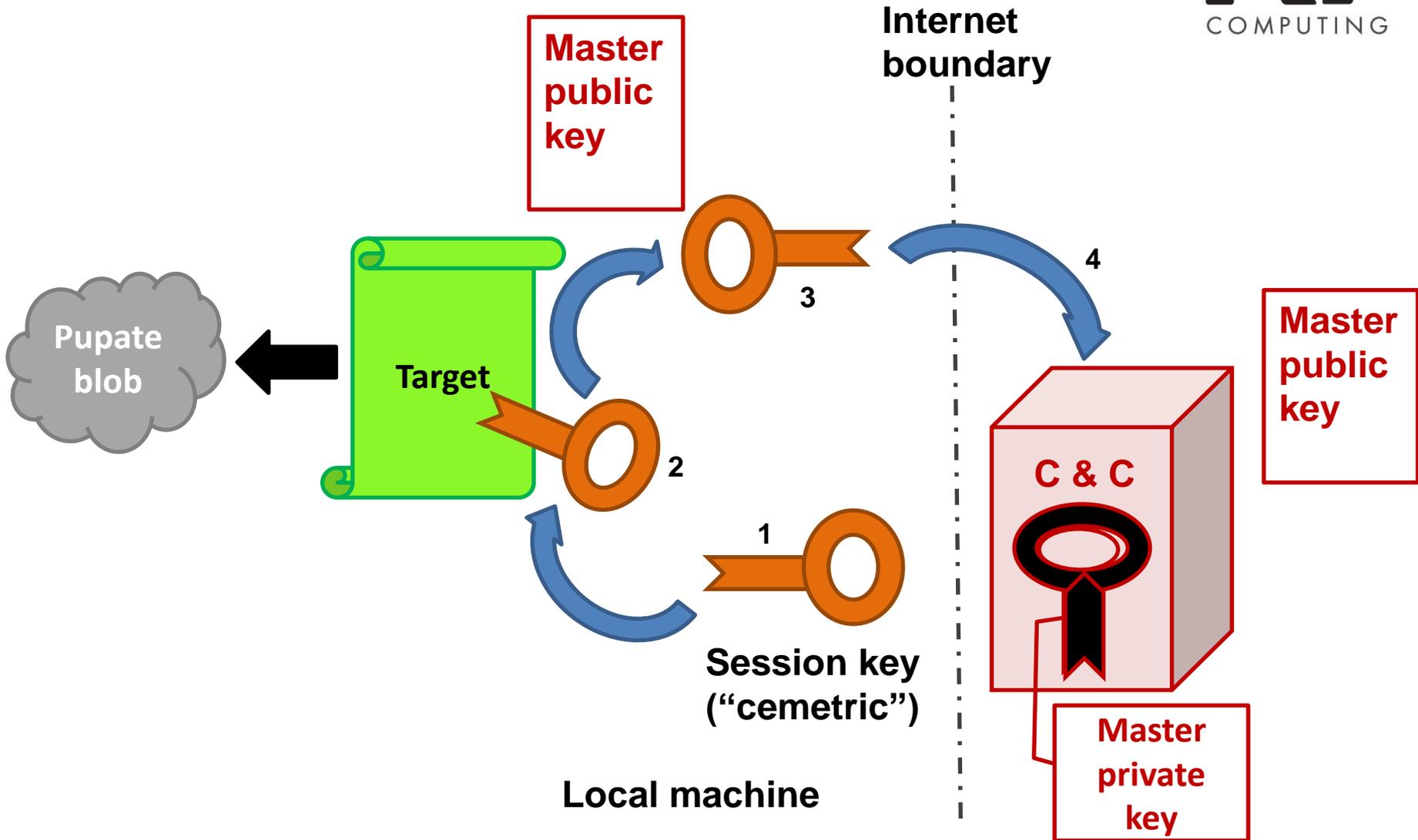


Into spawned or running OS process – an opportunity

- Untrusted process injecting into explorer.exe or svchost.exe, etc.
- OS process encryption-writes to target files
- Presence of encryption/hash algorithm artefacts in OS process space



Typical Encryption Lifecycle



Assumptions



Ransomware bypass first-line defences



OS privilege-control features do not abort the infection



Ransomware EXEs come from untrusted sources



Only user mode components are involved

Modus Operandi



**LOCATE
TARGET**

**TAKE
HOSTAGE**



**DEMAND
RANSOM**

S E n d
y O u R

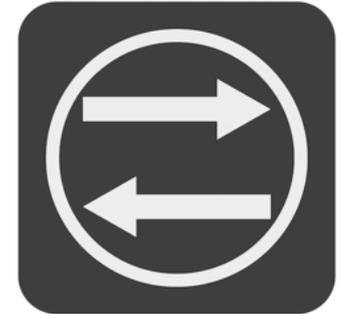
m E A L L
m O n E Y



Generic Ransomware Tracking

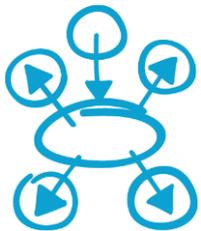
Interception Points

- IRP_MJ_CREATE
 - IRP_MJ_DIRECTORY_CONTROL
 - IRP_MJ_WRITE
 - IRP_MJ_CLOSE / IRP_MJ_CLEANUP
-
- PoC intercepts using Filesystem Minifilter architecture.



Of Triggers & Contexts..

- Trigger Point : Dir Enumeration
- Process-Level Context ?
 - Few Inject code into OS Processes
 - Insufficient..
- Thread-Level Context ?
 - CTB Locker - Multiple Threads split work
 - Insufficient..
- Code-Block Level Context ?
 - Threads originate from same code-block
 - Sufficient to track & prove intent

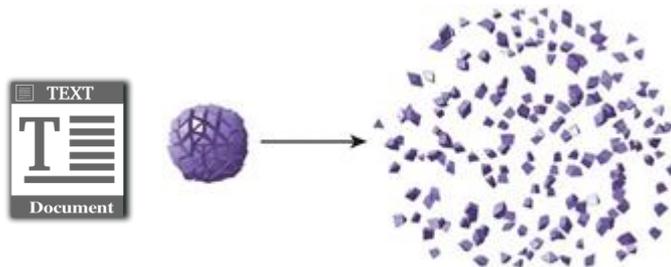


Nail in the Coffin

- Write Monitoring – For Encryption
- Known Binary File Type
 - Change to Unknown file-type detected



- Unknown/Text File Type
 - Increase in entropy detected



Minimizing the Damage



- I/O Buffering (In-Memory Backup)
 - Handle based on detection



- Maintaining Journal
 - Most Ransomware move the encrypted content to <FileName>.<RandomExtn>
 - Maintain rename/move actions history
 - Revert changes post-detection



DEMO

Mitigating the Risk



oops False positives

Performance slowdown



Tighten process context:

- Executables from external sources, e.g. Internet
- Untrusted exec path, e.g. NOT from Program Files
- Exclusions based on Digital Signature, etc.

What about Android Ransomware Encryptors?



Simplelocker

Внимание Ваш телефон заблокирован!
Устройство заблокировано за просмотр и распространение детской порнографии, зоофилии и других извращений.

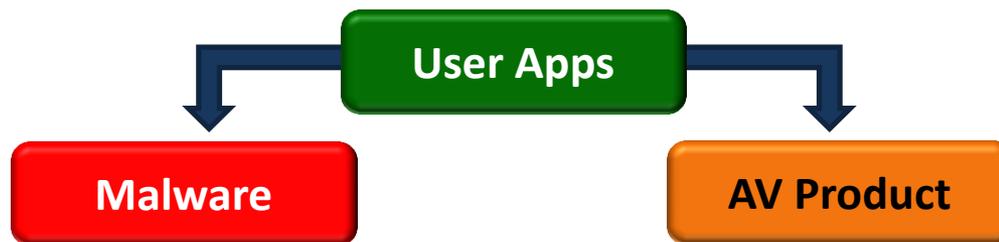
Для разблокировки вам необходимо оплатить 260 Грн.

1. Найдите ближайший терминал пополнения счета.
2. В нем найдите МонеХу.
3. Введите 380982049193.
4. Внесите 260 гривен и нажмите оплатить.

Не забудьте взять квитанцию!
После поступления оплаты ваше устройство будет разблокировано в течении 24 часов.
В СЛУЧАЙ НЕ УПЛАТЫ ВЫ ПОТЕРЯЕТЕ НА ВСЕГДА ВСЕ ДАННЫЕ КОТОРЫЕ ЕСТЬ НА ВАШЕМ УСТРОЙСТВЕ!

Same detection framework applicable
... in theory

In practice however...



Low-level interception not possible

```
"android.permission.RECEIVE_BOOT_COMPLETED"
```

Windows Ransomware Encryptors Must Die

