K7 COMPUTING™

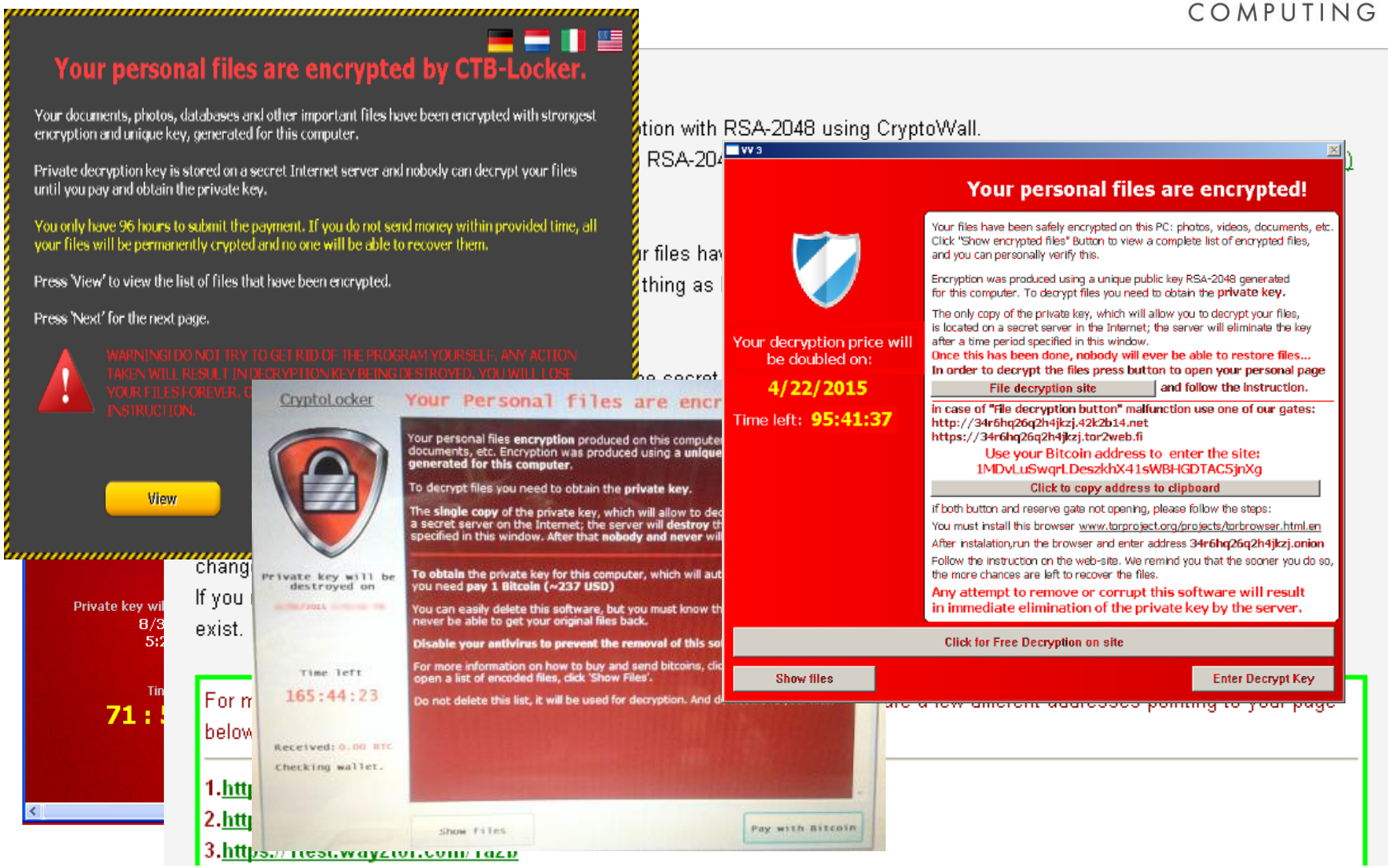
Dead and Buried in Their Crypts:
Defeating Modern Ransomware

Samir Mody

Gregory Panakkal

Screen Lockers not Covered

Our Targets – File Encryptors



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. Overwise, 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.

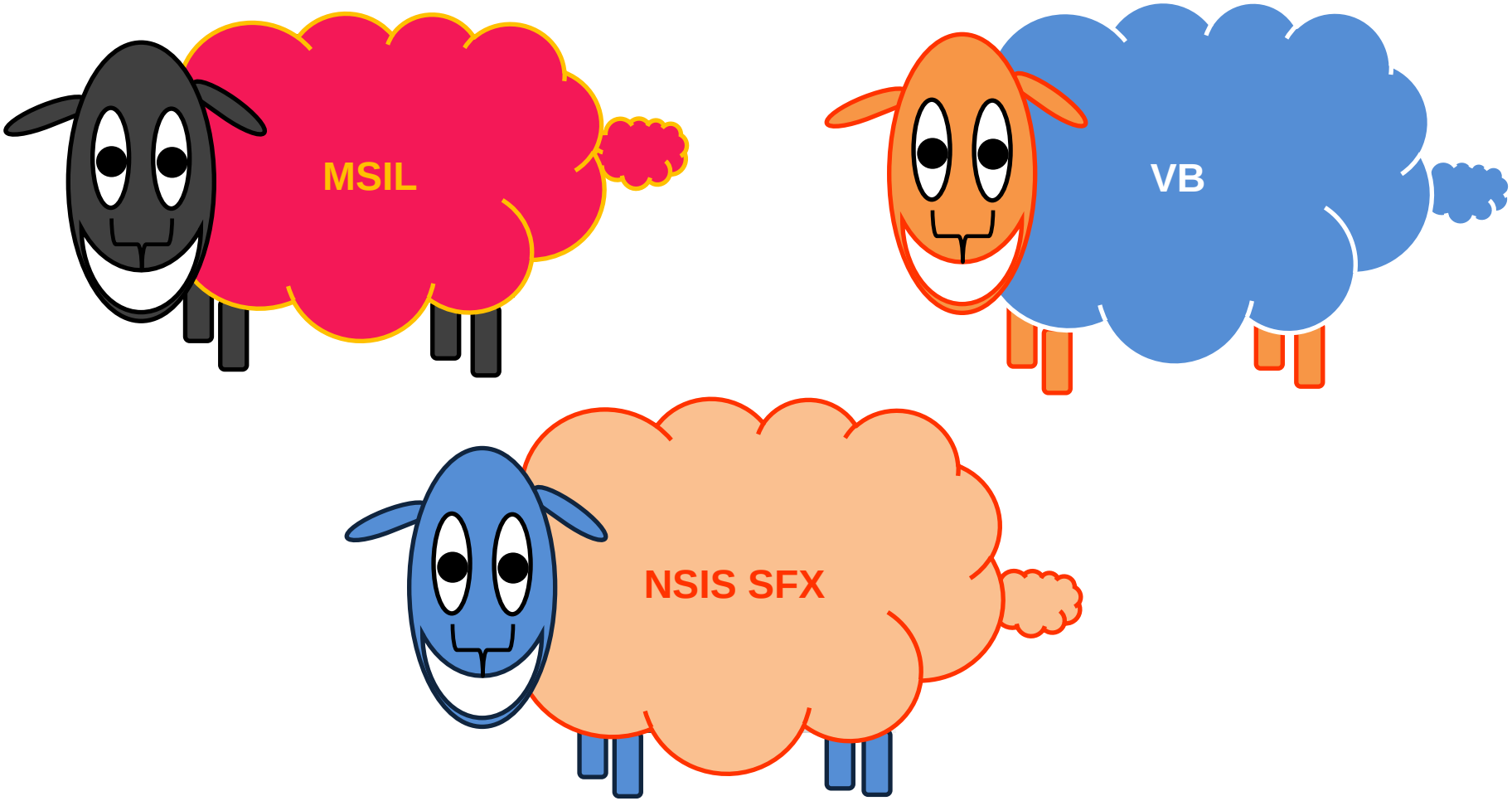
```
F35VL7O-PD7NK3J-56CMMX4-2LB53Z6-64PPAXM-LVKW6XG-JUWBDNP-PCUHQAE
FKGC7L3-65LKSAD-YJ5CVLZ-T5MNYXN-UUV2NSA-FY56ULM-BXNSTD5-DMYF2YR
IHDT5QB-O5S3LUP-PUVJHYY-CBBYTWH-MZ3MZAK-2RTM25V-KRZCSYK-HXG4OCO
```

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

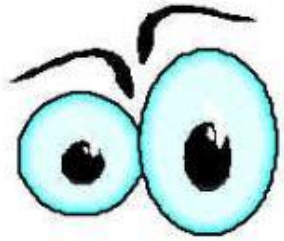
Static Detection Difficult – Packer Obfuscation



Process Injection – Implications for Dynamic Blocking

Into spawned non-OS process

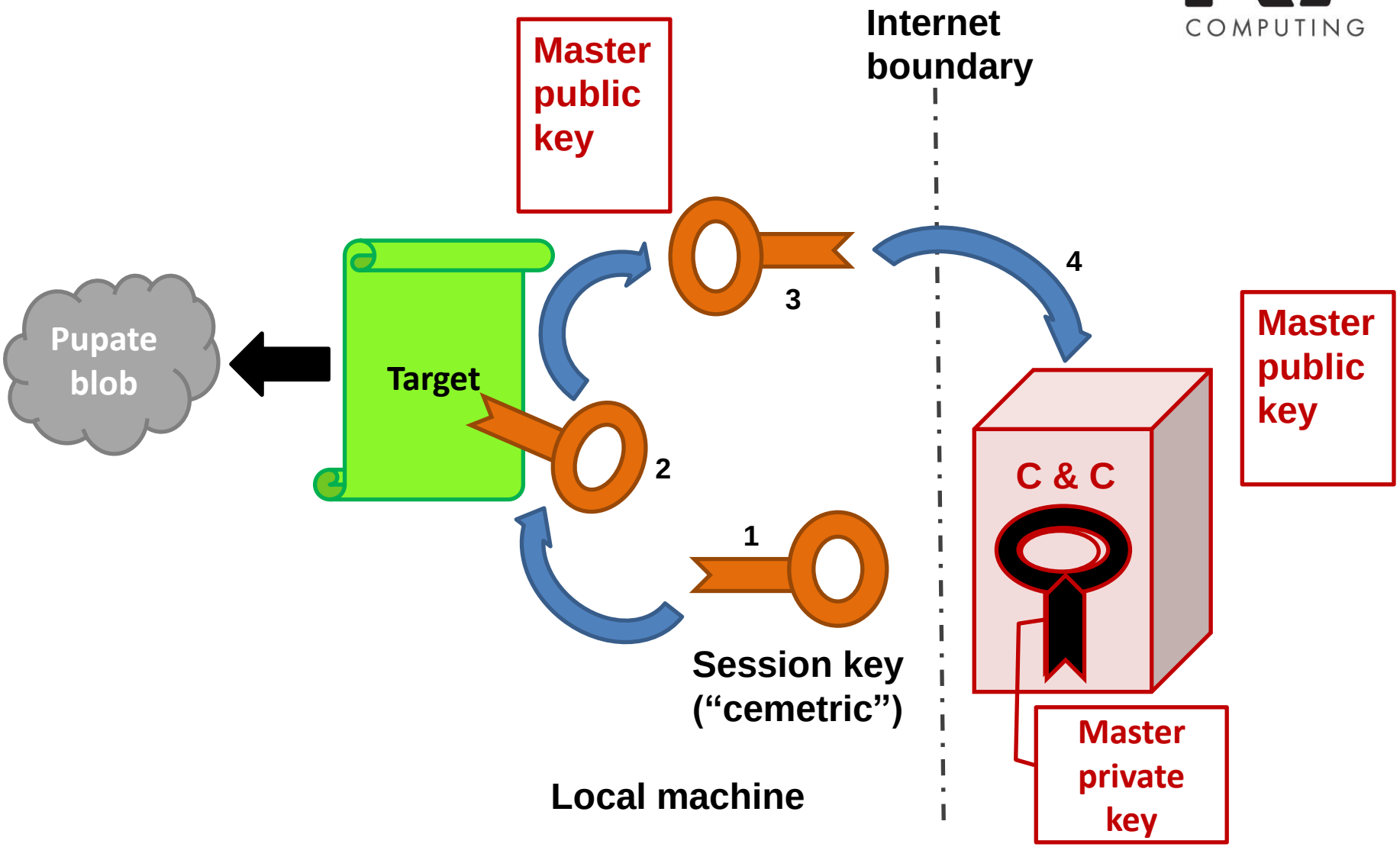
- Potential loss of process context - complicates behaviour tracking and blocking



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

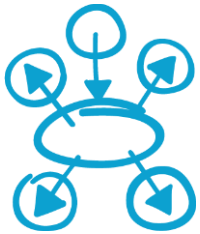
Generic Ransomware Tracking

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..

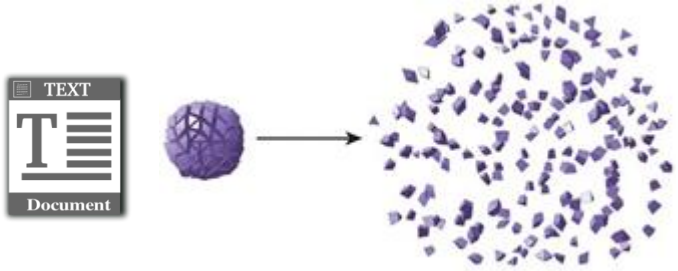


- Trigger Point : Dir Enumeration
- Process-Level Context ?
  - Few Inject code into OS Processes
  - Insufficient..
- Thread-Level Context ?
  - CTB Locker - Multiple Threads split work
  - Insufficient..
- Code-Block Level Context ?
  - Threads originate from same code-block
  - Sufficient to track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

K7 COMPUTING™

DEMO

Mitigating the Risk

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

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

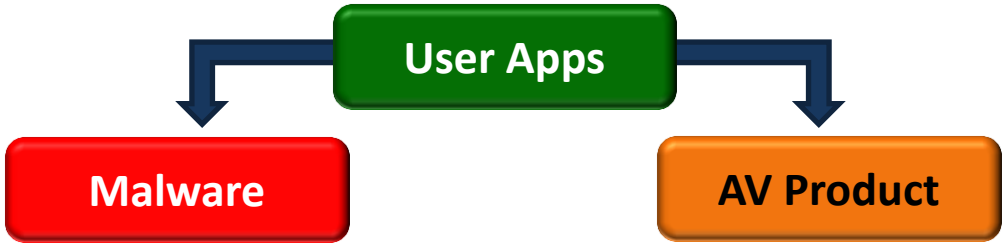
Для разблокировки вам необходимо оплатить 260 Грн.
1. Найдите ближайший терминал пополнения счета.
2. В нем найдите MoneXy.
3. Введите 380982049193.
4. Внесите 260 гривен и нажмите оплатить.

Не забудте 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 УСТРОЙТВЕ!

Same detection framework applicable

... in theory

In practice however...



Low-level interception not possible

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

Windows Ransomware Encryptors Must Die