UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

CONCINNITYRISKS

2018 hack.lu

Come to the dark side!
We have radical insurance groups & ransomware.

Ankit Gangwal
Department of Mathematics,
University of Padua, Italy
ankit.gangwal@phd.unipd.it

Éireann Leverett
Cambridge Judge Business School,
University of Cambridge,
e.leverett@jbs.cam.ac.uk

Oct 16, 2018

Table of contents

1. Who we are
2. Insurance != Capitalism
3. Fun facts
4. Ransomware & its life cycle
5. Payments analysis
6. Payments != The full cost to society
7. Frequency and severity
8. References & tools

Who are we

...a chance MISP correlation brought us together...

- Éireann Leverett:
  - A bitshifter and lifelong scholar
  - A Senior Risk Researcher at Cambridge Centre for Risk Studies
  - A Founder at Concinnity Risks
  - A Free and Open Source Software for DFIR developer

- Ankit Gangwal:
  - A PhD student at the University of Padua, Italy.
  - Current research interest: cryptocurrency and cryptomining.
  - Believe in reproducible research and tend to publicly release the source code as well as the data set of my projects (sometimes, even before the paper is accepted).

Insurance != Capitalism

Free transport radicals introduce us to quantitative risk

STEP 1: IS IT LEGAL?

STEP 2: START ON A SMALL SCALE...

STEP 3: DO THE MATH!

Insurance != Capitalism

Mutuals and Risk Captives

- If you don’t insure, you self insure.
- You reckon your risk model is better, which is probably true, so let’s verify that.
- Ask the price on insurance and what capacity coverage you get.
- Now ask your team if this is their budget and they have this capacity if something goes wrong.
- Don’t let them include PREVENTION spending in this budget. Only RESPONSE spending.
- In other words, what you spend on firewalls is PREVENTION, what we’re asking, is how much you have in reserve for that bad day when your team comes and says “we’re breached.”

Ransomware

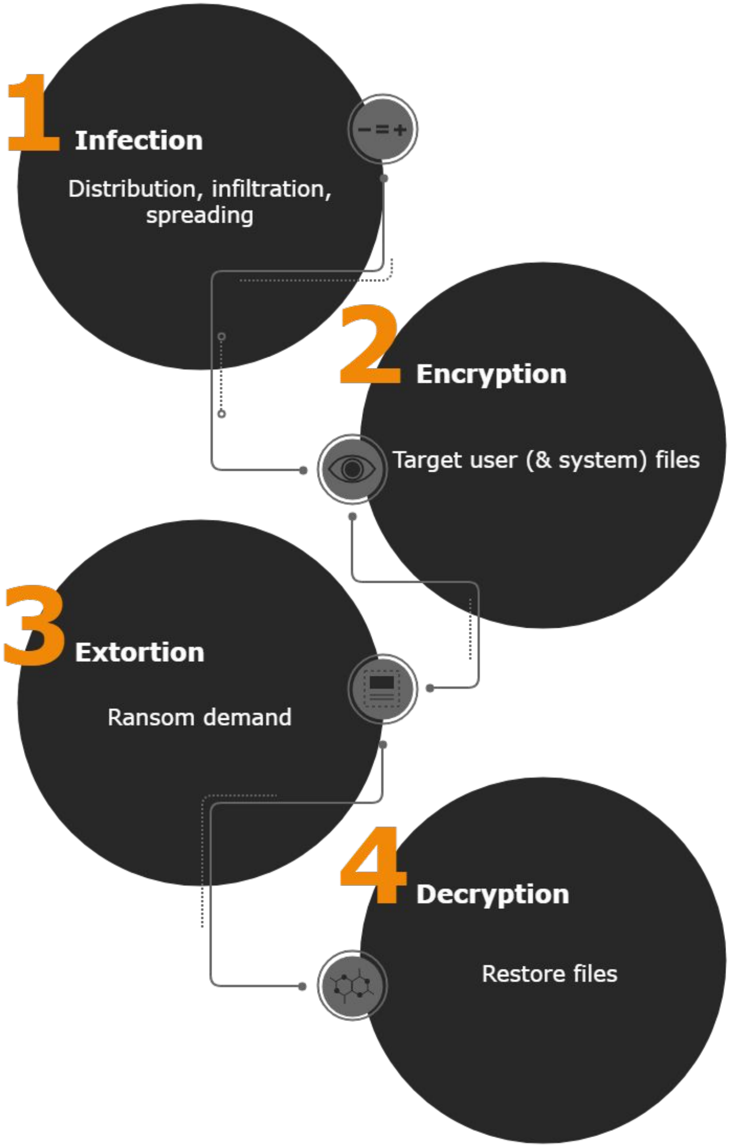
What is a ransomware?

- Ransomware is a class of malware that restricts access to the system it infects until the victim pays the demanded ransom.

Image by: Courtesy graphic

Ransomware

Life cycle



1 **Infection**

Distribution, infiltration, spreading

2 **Encryption**

Target user (& system) files

3 **Extortion**

Ransom demand

4 **Decryption**

Restore files

Ransomware: Life cycle

Infection (1/2)

1. Spam emails (e.g., CryptoLocker)
   - Customer complaints, order confirmations, invoices, urgent message for unpaid balances.

2. Drive-by downloads (e.g., CryptoWall)
   - "Missed-fax" decoy, messages from govt. agencies/banks that included links to malicious payload hosted over popular cloud services Dropbox, MediaFire, Cubby.

3. Software update (e.g., NotPetya)
   - Distributed as an update to *MeDoc* accounting software in Ukraine.

Ransomware: Life cycle

Infection (2/2)

4. Backdoors (e.g., WannaCry)
   - Exploited *DoublePulsar* backdoor.

5. Installers (e.g., Bad Rabbit)
   - Distributed it via as a dropper-file named "install flash player.exe".

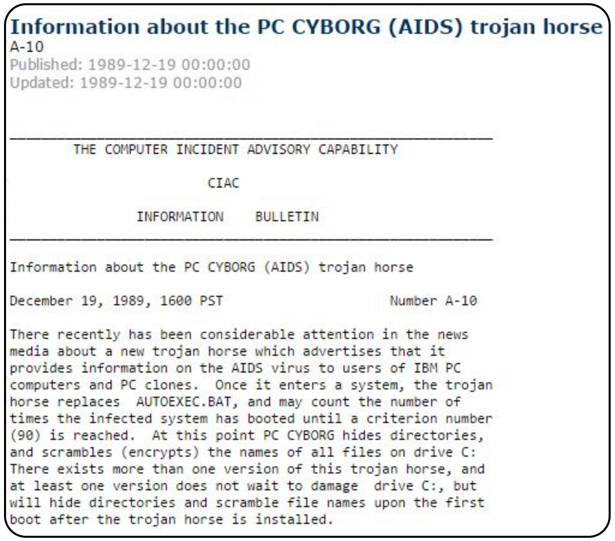
6. Affiliate program (e.g., Mischa/GoldenEye/Petya)
   - The cybercriminals offered profits through their own affiliate program and introduced RaaS [1].

[1] www.bleepingcomputer.com/news/security/the-petya-and-mischa-ransomwares-part-of-a-new-affiliate-service/

Fun facts (1/3)

From our research

- First known ransomware virus was written by an AIDS researcher, called Dr. Joseph Popp, in 1989.



Information about the PC CYBORG (AIDS) trojan horse

A-10
Published: 1989-12-19 00:00:00
Updated: 1989-12-19 00:00:00

```
_____________________________________________________________________
         THE COMPUTER INCIDENT ADVISORY CAPABILITY

                          CIAC

                   INFORMATION     BULLETIN
_____________________________________________________________________

Information about the PC CYBORG (AIDS) trojan horse

December 19, 1989, 1600 PST                         Number A-10

There recently has been considerable attention in the news
media about a new trojan horse which advertises that it
provides information on the AIDS virus to users of IBM PC
computers and PC clones.  Once it enters a system, the trojan
horse replaces  AUTOEXEC.BAT, and may count the number of
times the infected system has booted until a criterion number
(90) is reached.  At this point PC CYBORG hides directories,
and scrambles (encrypts) the names of all files on drive C:
There exists more than one version of this trojan horse, and
at least one version does not wait to damage  drive C:, but
will hide directories and scramble file names upon the first
boot after the trojan horse is installed.
```

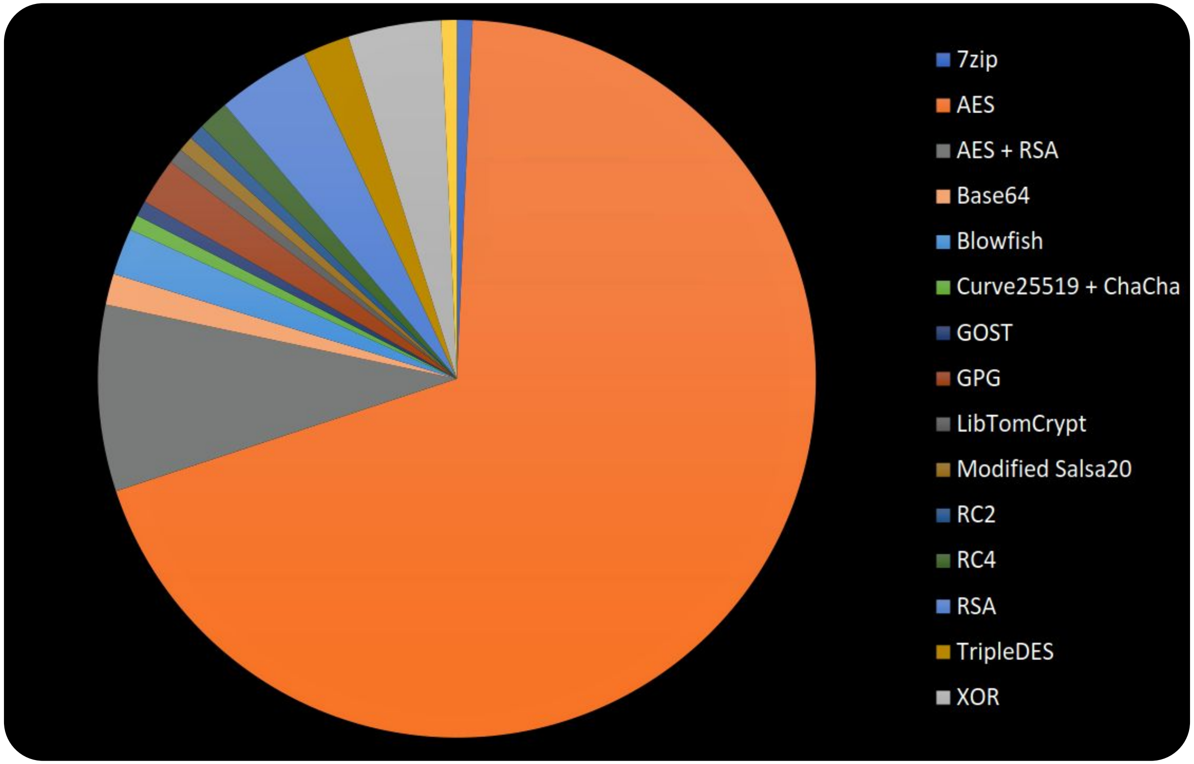
- The “first” cashout we found in the blockchain was from CryptoLocker, in 1972, before the blockchain EXISTED!

Screenshot by: Security Focus

Ransomware: Life cycle

Encryption (1/3): Symmetric or asymmetric?

- AES is the most popular cipher choice for ransomware

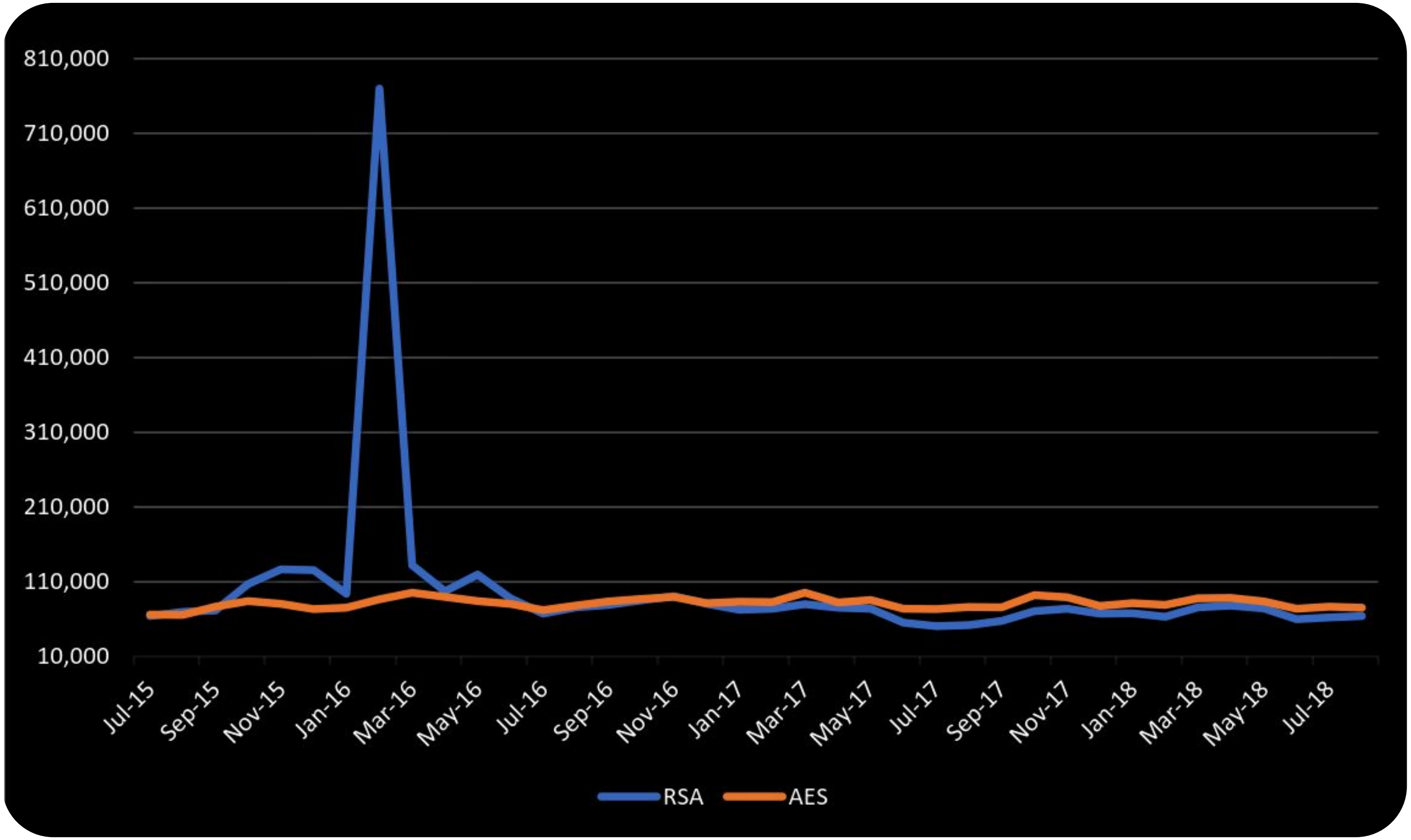


Source: Wikipedia

Ransomware: Life cycle

Encryption (2/3): Symmetric or asymmetric?

- Yet there was a time when RSA still dominated!



Source: Wikipedia

Ransomware: Life cycle

Encryption (3/3): Symmetric, asymmetric, or both?

- Typically symmetric + asymmetric
  - Faster encryption + superior protection
  - E.g., CryptoWall 3.0 used AES-256 (symmetric) key for file encryption. The symmetric key is then encrypted using a unique RSA-2048 (asymmetric) key generated by the C&C server.

Ransomware: Life cycle

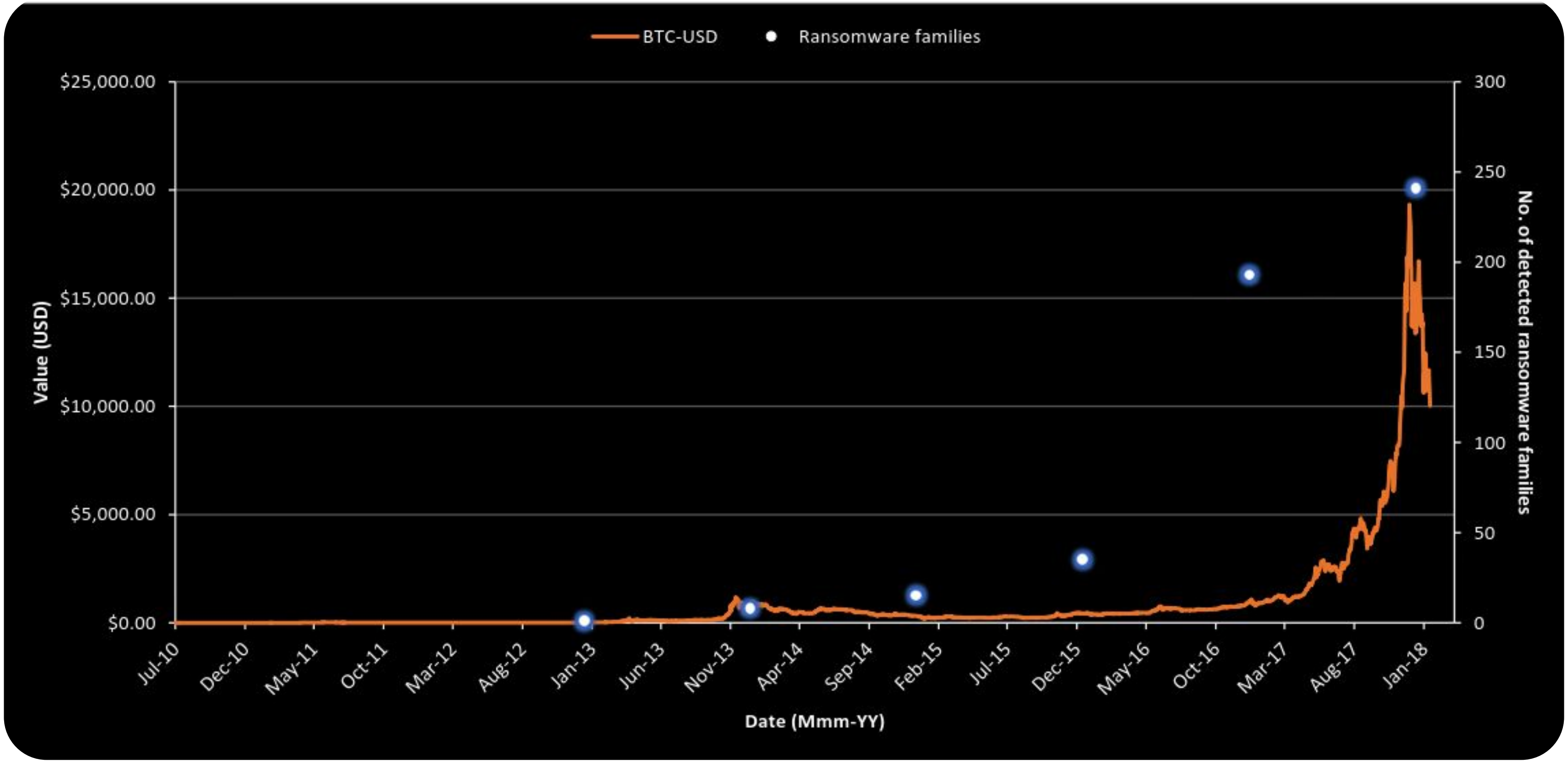
Extortion (1/2)

- Ransom payment
  - cashU, Ukash, paysafecard, MoneyPak, Litecoin, Bitcoin, etc.
    - ➢ All these payments methods are anonymous (or at least pseudo-anonymous), which makes it difficult to track the payer and the payee.
      - ○ Tor network for anonymity.

Ransomware: Life cycle

Extortion (1/2)

- Ransom payment
  - cashU, Ukash, paysafecard, MoneyPak, Litecoin, Bitcoin, etc.



Source for ransomware families: 2017 F-Secure State of Cyber Security & Trend Micro 2016 Security Roundup

Ransomware: Life cycle

Extortion (2/2)

- Deadline for the payment
  a. Few days (counted in hours) to maximum a week
  b. Extensions

- Payment address
  a. Single address (e.g., NotPetya)
     ➢ 1-to-1 (Binary-to-address)
     ➢ Many-to-1 (Binaries to address)
  b. Hardcoded (e.g., WannaCry)
     ➢ 1-to-1
     ➢ 1-to-many
     ➢ Many-to-many
  c. On-the-fly (e.g., CryptoWall)
     ➢ 1-to-1
     ➢ 1-to-many

Fun facts (2/3)

From our research

- CTB-Locker targeted websites
  - Are backed-up regularly
    - ➢ Webmasters restored a sites without paying the ransom.

- Ransomware is a full-fledged business model that offers "discounts" on ransoms and "better" customer support, e.g., TeslaCrypt [2].

- New pressure tactics, e.g., Chimera used doxing.
  - Leverage using GDPR???

[2] Nart Villeneuve, Fireeye. (2015) "TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware." www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html

Ransomware: Life cycle

Decryption

- Decrypt and restore the encrypted files.

Ransomware: Life cycle

Decryption

- Decrypt and restore the encrypted files.
- There's no guarantee!
  - But some say “yes, they decrypt.”
    - The short answer is: “it depends.”
    - Kansas Heart Hospital [3] Power Worm [4].

[3] www.techspot.com/news/64954-hackers-demand-ransom-payment-kansas-heart-hospital-files.html
[4] news.softpedia.com/news/epic-fail-power-worm-ransomware-accidentally-destroys-victim-s-data-during-encryption-495833.shtml

Fun facts (3/3)

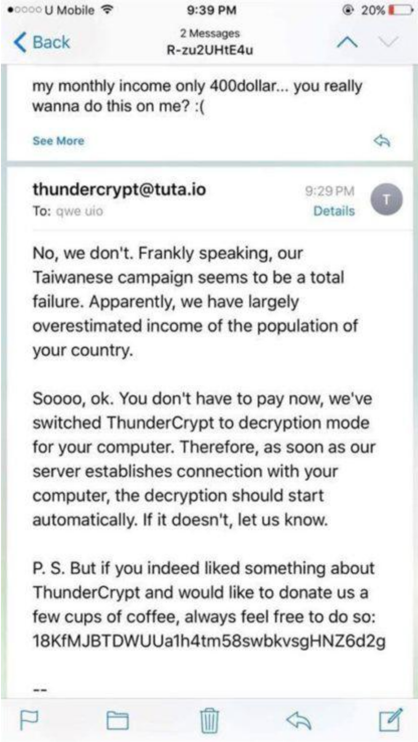
From our research

- Rival ransomware developers leaked [5] private keys of Chimera.

- Prove authenticity, e.g., CTB-Locker allowed victims to decrypt five files for free and do test transaction of 0.0001 BTC.

- Publicly release the master key, TeslaCrypt [6].

- Ask for tip, e.g., ThunderCrypt[7].



my monthly income only 400dollar... you really wanna do this on me? :(

thundercrypt@tuta.io 9:29 PM

To: qwe uio

No, we don't. Frankly speaking, our Taiwanese campaign seems to be a total failure. Apparently, we have largely overestimated income of the population of your country.

Soooo, ok. You don't have to pay now, we've switched ThunderCrypt to decryption mode for your computer. Therefore, as soon as our server establishes connection with your computer, the decryption should start automatically. If it doesn't, let us know.

P. S. But if you indeed liked something about ThunderCrypt and would like to donate us a few cups of coffee, always feel free to do so: 18KfMJBTDWUUa1h4tm58swbkvsgHNZ6d2g

--

[5] https://twitter.com/JanusSecretary/status/757951375561072640
[6] www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/
[7] wccftech.com/thundercrypt-ransomware-taiwanese-man/

Ransomware

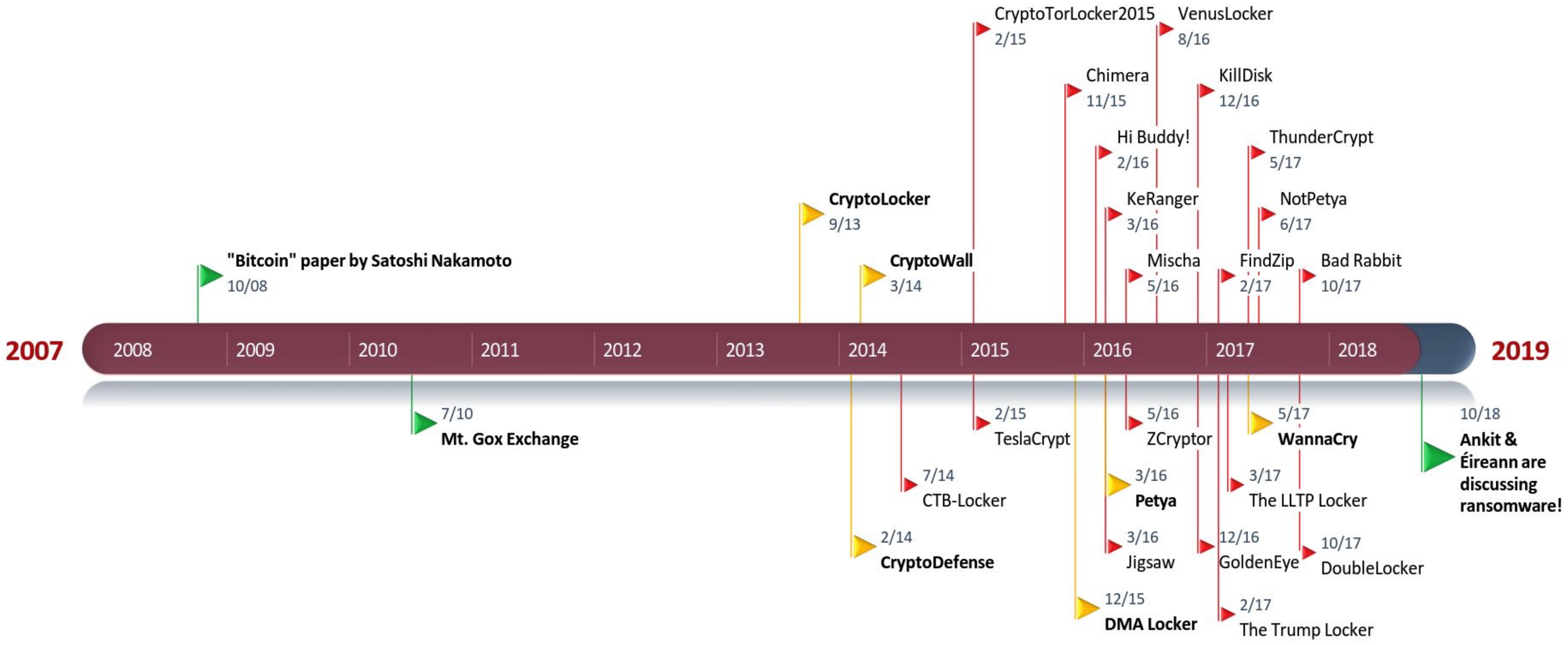
Affected OSes

- Microsoft Windows (e.g., CryptoLocker, CryptoDefense)
- Linux (e.g., KillDisk)
- macOS (e.g., KeRanger, FindZip)
- Android (e.g., DoubleLocker)

Occurrence of Bitcoin ransomware

We'll get to the insurance part slowly...

- We studied [8] all the recent ransomware:
  - that used Bitcoin as at least one mode of ransom payment, and
  - for which at least one Bitcoin address is publicly known.



[8] Mauro Conti, Ankit Gangwal, Sushmita Ruj. "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective." In (Elsevier) Computers & Security, 79: 162-189, 2018. DOI: 10.1016/j.cose.2018.08.008, ISSN: 0167-4048.

Payments analysis

- Ransom identification framework:
  - Module 1: Identification of ransomware addresses
    - github.com/Concinnity-Risks/RansomCoinPublic
  - Module 2: Data collection and database generation
  - Module 3: Classifying a payment as ransom

Payments analysis

Module 1: Identification of ransomware addresses (1/2)

A. Collect initial addresses

- Ransomware binary
- Knowledge base (e.g., ESET, Symantec)
- Reports from Counter Threat Units (CTU) & Incident Responses (IR)
- Online fora (e.g., Reddit) where victims and researchers post
- Screenshots of ransomware available in different image search engines (e.g., Google, Yahoo)
- Ransomware removal guides and “How To” videos on YouTube

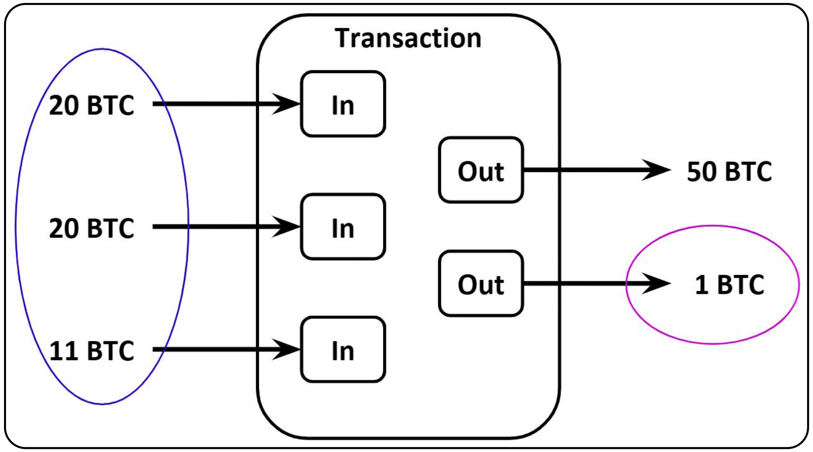
Payments analysis

Module 1: Identification of ransomware addresses (2/2)

B. Find associated Bitcoin addresses

   i. Multi-input transactions

   ii. Shadow/change address



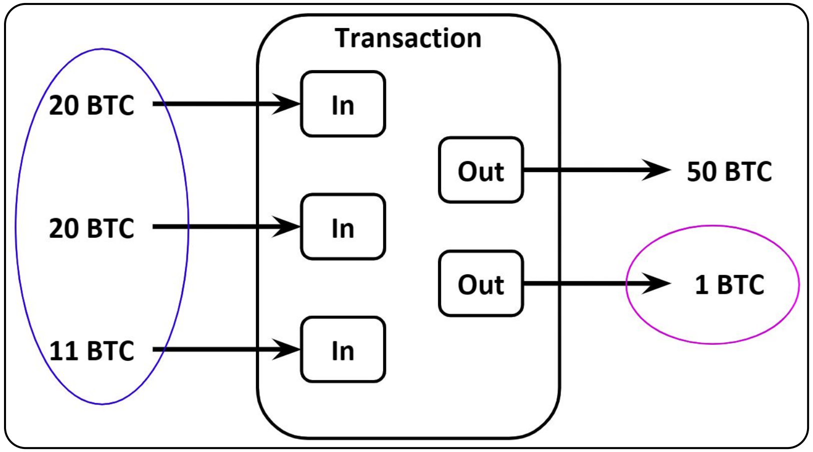
Payments analysis

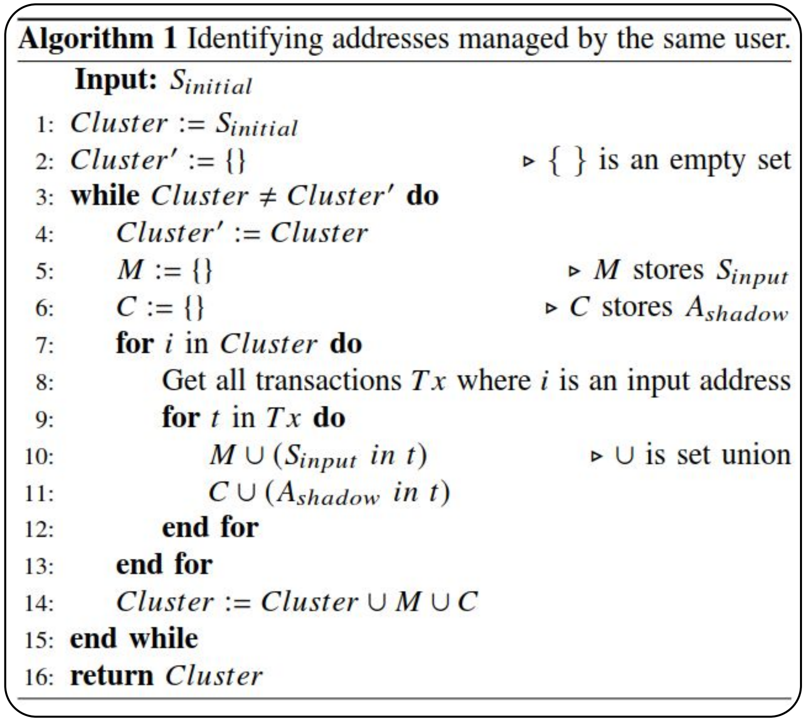
Module 1: Identification of ransomware addresses (2/2)

B. Find associated Bitcoin addresses

   i. Multi-input transactions

   ii. Shadow/change address





Algorithm 1 Identifying addresses managed by the same user.

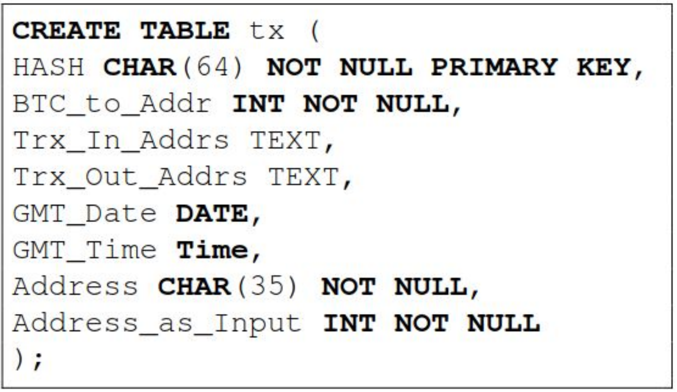
```
Input: $S_{initial}$
$Cluster := S_{initial}$
$Cluster' := \{\}$                              ▷ { } is an empty set
while $Cluster \neq Cluster'$ do
    $Cluster' := Cluster$
    $M := \{\}$                                 ▷ $M$ stores $S_{input}$
    $C := \{\}$                                 ▷ $C$ stores $A_{shadow}$
    for $i$ in $Cluster$ do
        Get all transactions $Tx$ where $i$ is an input address
        for $t$ in $Tx$ do
            $M \cup (S_{input}\ in\ t)$         ▷ ∪ is set union
            $C \cup (A_{shadow}\ in\ t)$
        end for
    end for
    $Cluster := Cluster \cup M \cup C$
end while
return $Cluster$
```

Payments analysis

Module 2: Data collection and database generation

- Download entire blockchain?
    - Over 500K blocks, not a good idea (bandwidth, storage).

- We use Blockchain Data API [9] to crawl and parse transactions associated only with the address(es) of interest.



```
CREATE TABLE tx (
HASH CHAR(64) NOT NULL PRIMARY KEY,
BTC_to_Addr INT NOT NULL,
Trx_In_Addrs TEXT,
Trx_Out_Addrs TEXT,
GMT_Date DATE,
GMT_Time Time,
Address CHAR(35) NOT NULL,
Address_as_Input INT NOT NULL
);
```

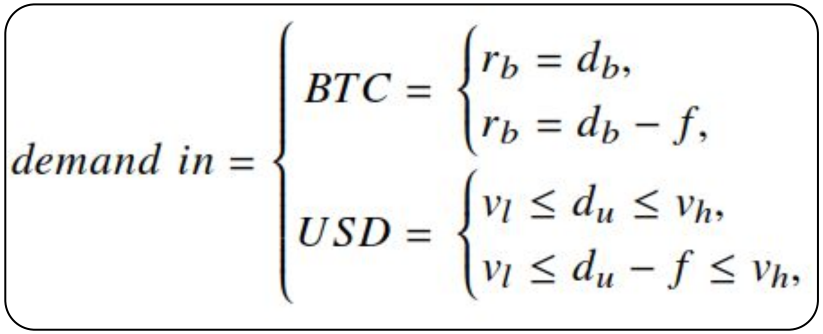
Listing 1: SQL statement for creating our database

[9] www.blockchain.com/api/blockchain_api

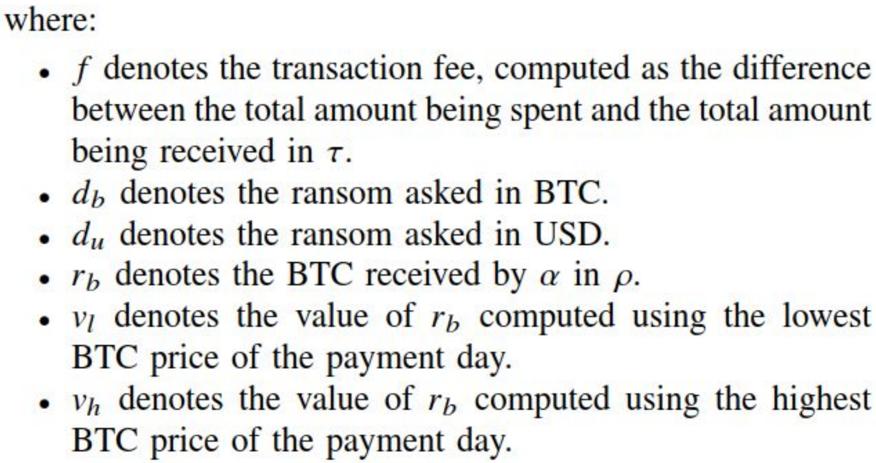
Payments analysis

Module 3: Classifying a payment as ransom

- A BTC trx involves two varying factors:
    i. Bitcoin price (fluctuates)
        ➢ Both the day-to-day lowest and highest price of Bitcoin
    ii. Transaction fee (payer's dilemma)



$$demand\ in = \begin{cases} BTC = \begin{cases} r_b = d_b, \\ r_b = d_b - f, \end{cases} \\ USD = \begin{cases} v_l \leq d_u \leq v_h, \\ v_l \leq d_u - f \leq v_h, \end{cases} \end{cases}$$



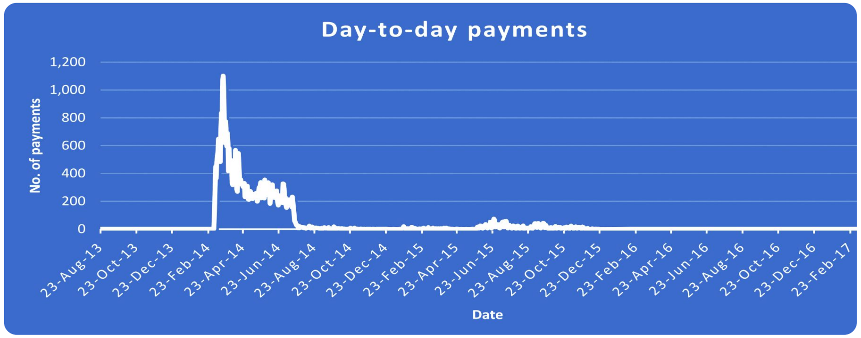
where:

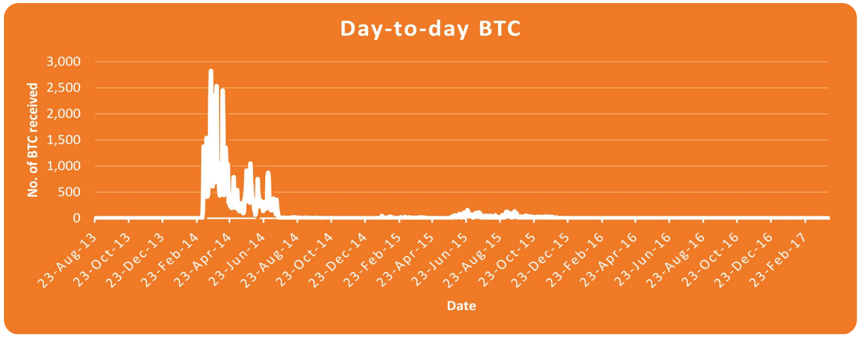
- f denotes the transaction fee, computed as the difference between the total amount being spent and the total amount being received in τ.
- d_b denotes the ransom asked in BTC.
- d_u denotes the ransom asked in USD.
- r_b denotes the BTC received by α in ρ.
- v_l denotes the value of r_b computed using the lowest BTC price of the payment day.
- v_h denotes the value of r_b computed using the highest BTC price of the payment day.

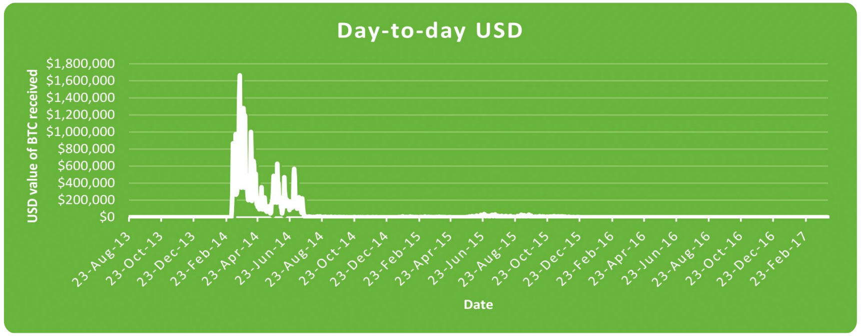
Payments analysis

Most people obsessed with payment size….

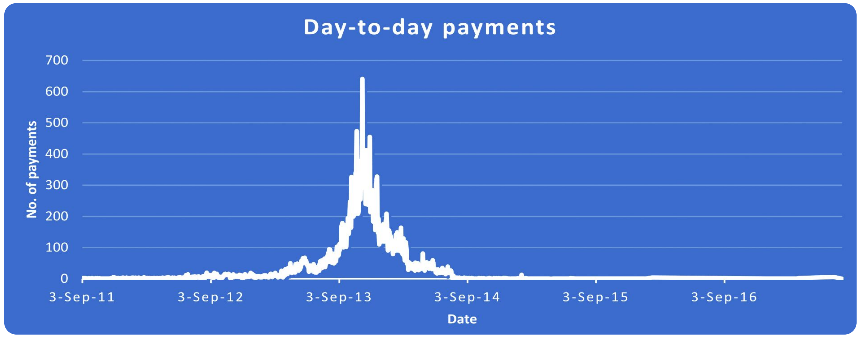
CryptoWall

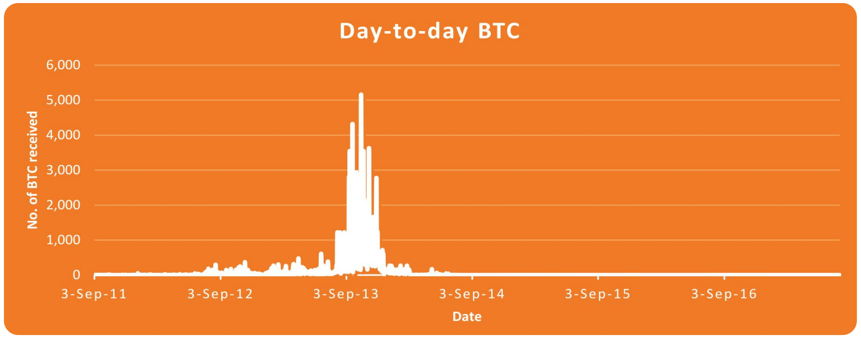


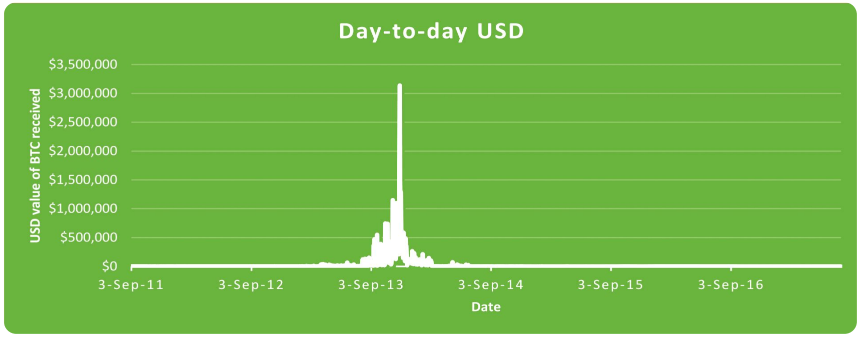




CryptoLocker



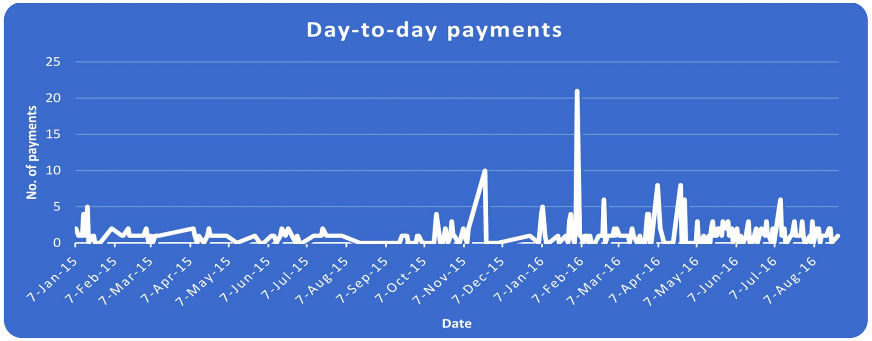


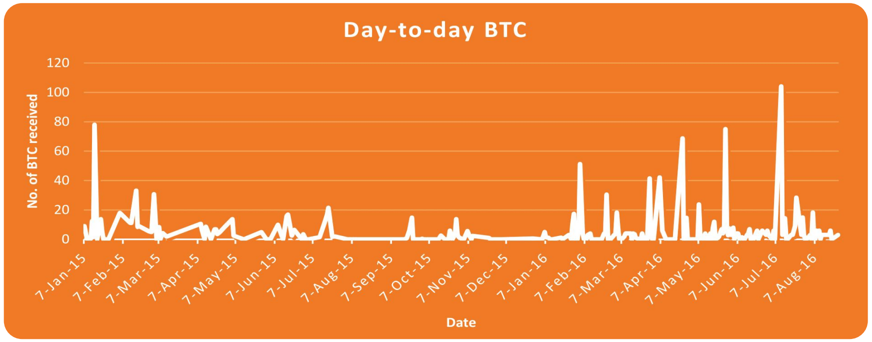


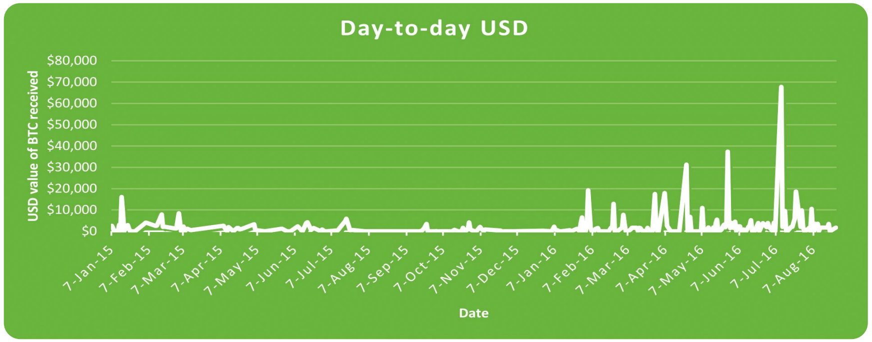
Payments analysis

Most people obsessed with payment size….

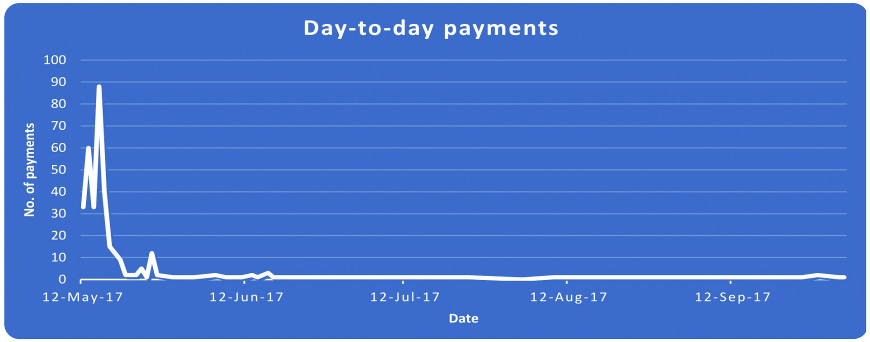
DMA Locker

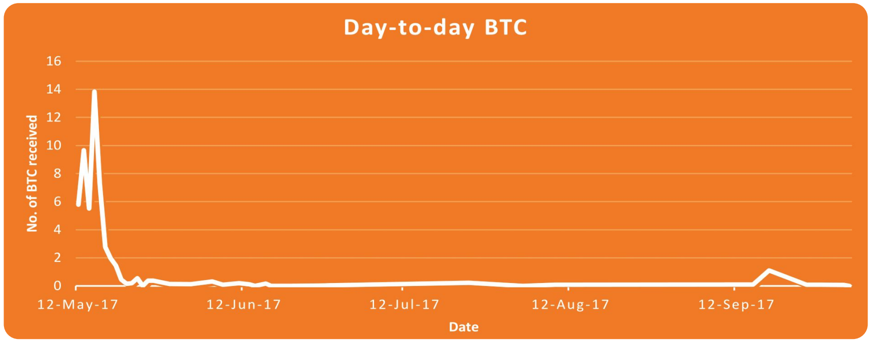

Day-to-day payments

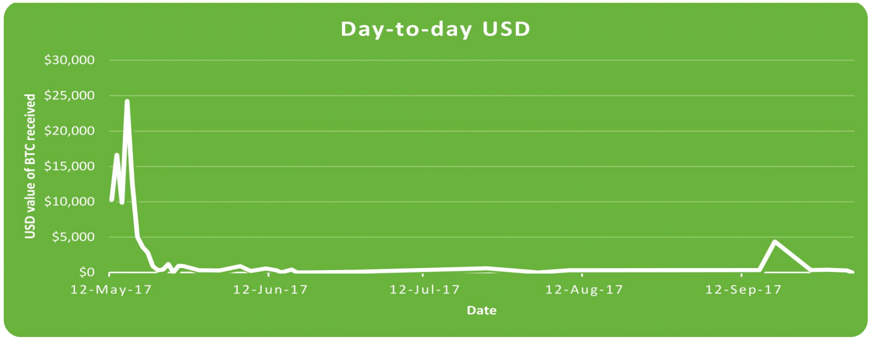

Day-to-day BTC


Day-to-day USD

WannaCry


Day-to-day payments

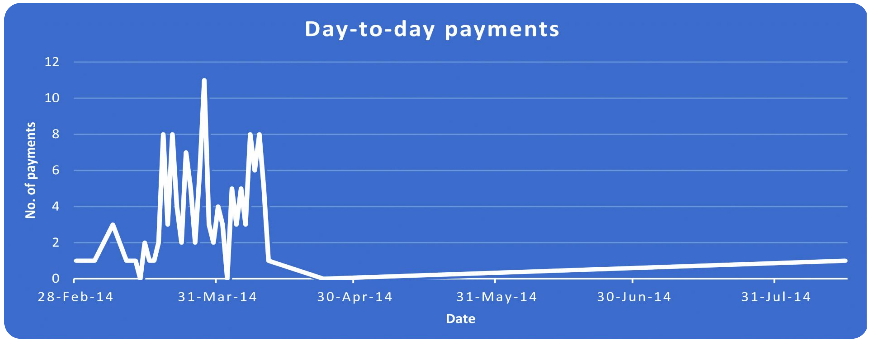

Day-to-day BTC

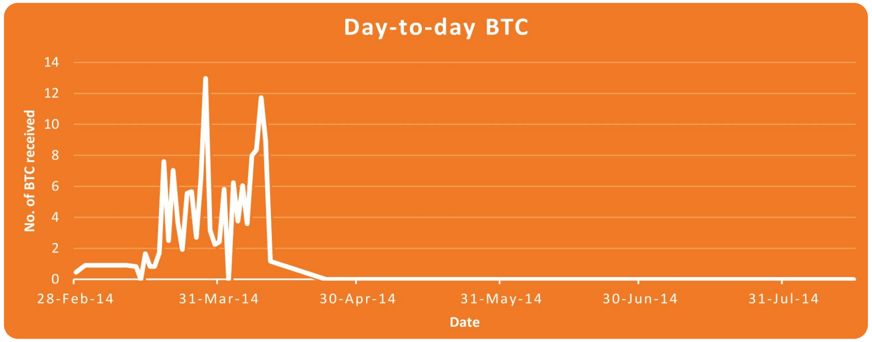

Day-to-day USD

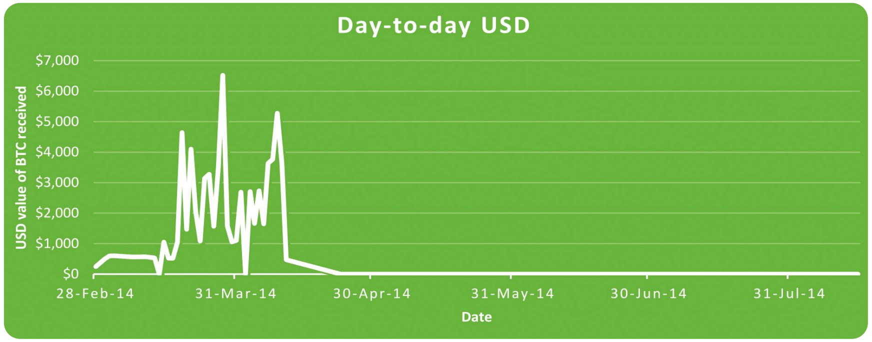
Payments analysis

Most people obsessed with payment size….

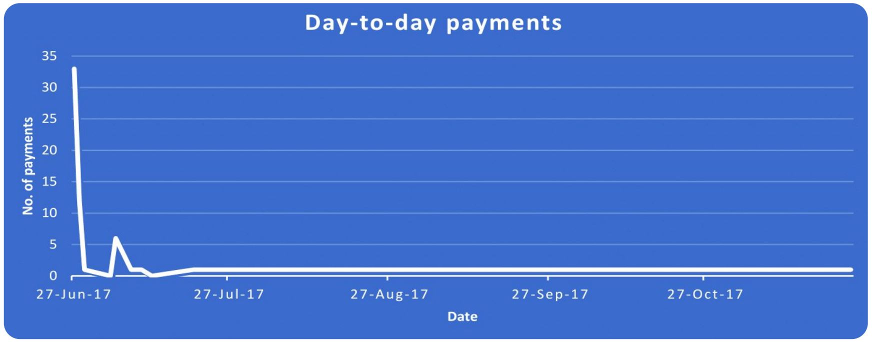
CryptoDefense

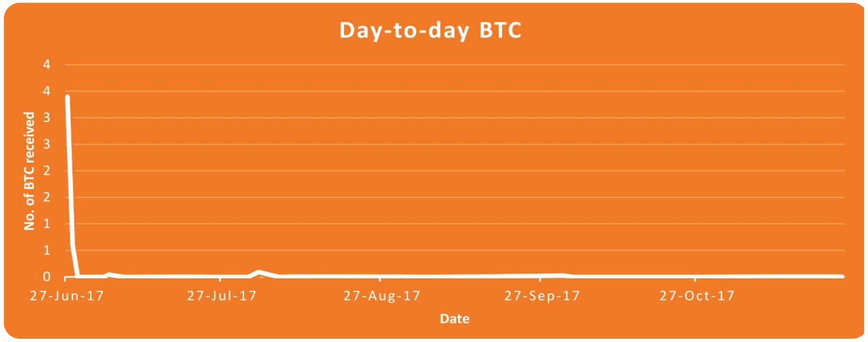


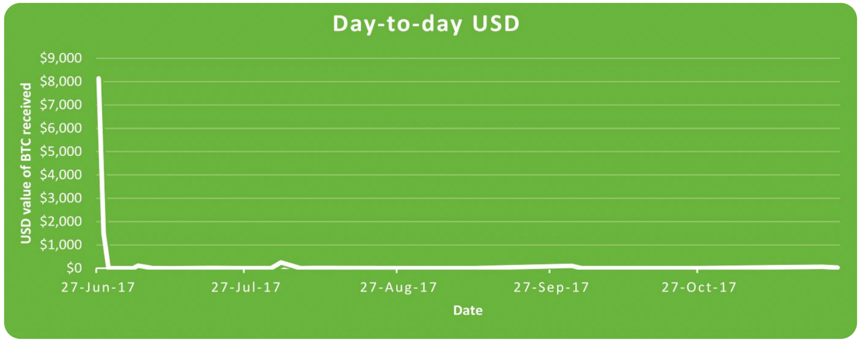




NotPetya







Payments analysis

Summary

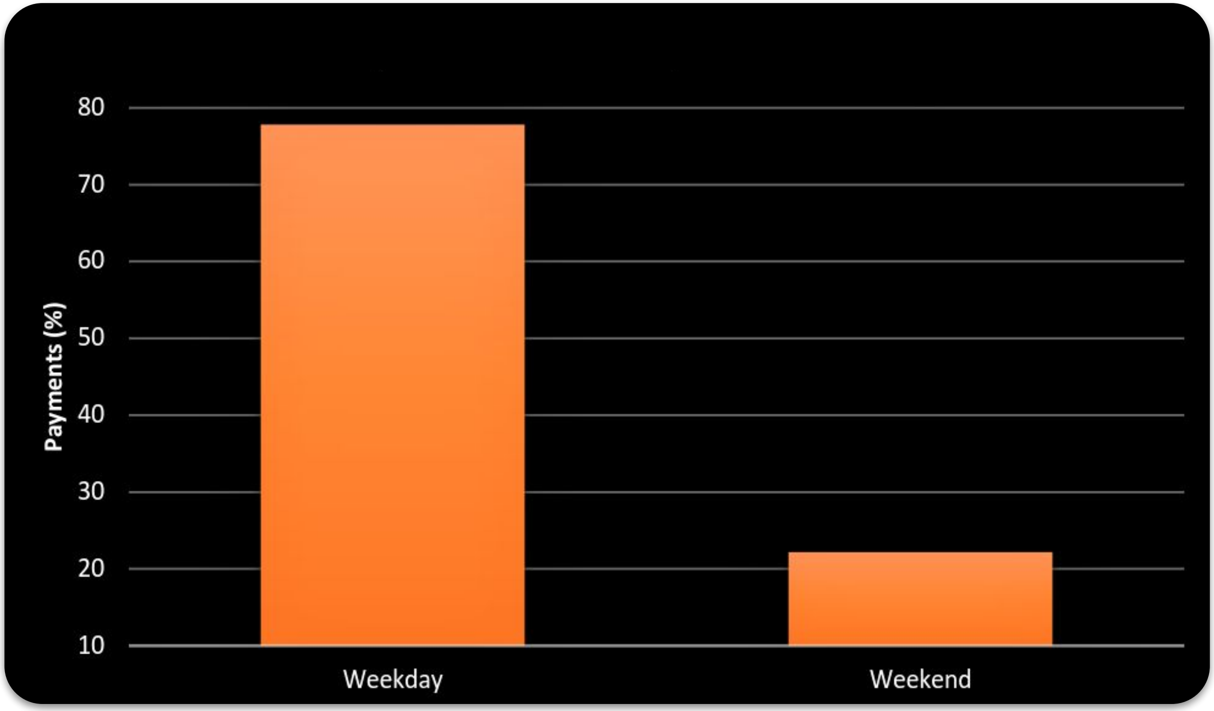
- Overall-minimum payments.

Ransomware	No. of payments	BTC	USD (Avg.) Value
CryptoWall	51,278	87,897.8510	45,370,589.00
CryptoLocker	51,766	133,045.9960	42,292,191.20
DMA Locker	298	1,433.3463	580,763.95
WannaCry	341	53.2906	99,549.05
CryptoDefense	128	138.3223	70,113.41
NotPetya	70	4.1787	10284.42
Total	103K	222K	88.4M

Payments analysis

Neat!

- Payments on weekdays vs. weekends



Payments analysis

We get back to our main story line of (re)insurance

- Reinsurance
  - Key insight here is number of payments is more important than USD/BTC amounts.
  - The cost to clean up each computer for the Govt. is ~66 cents [10].
  - Let’s replace Govt. with Reinsurer, and conservatively estimate it’s $66.

- Estimated cost to society: 103881 x 20 x 66 = $137,122,920

- We think this is a calculable risk, and maybe even a predictable one.

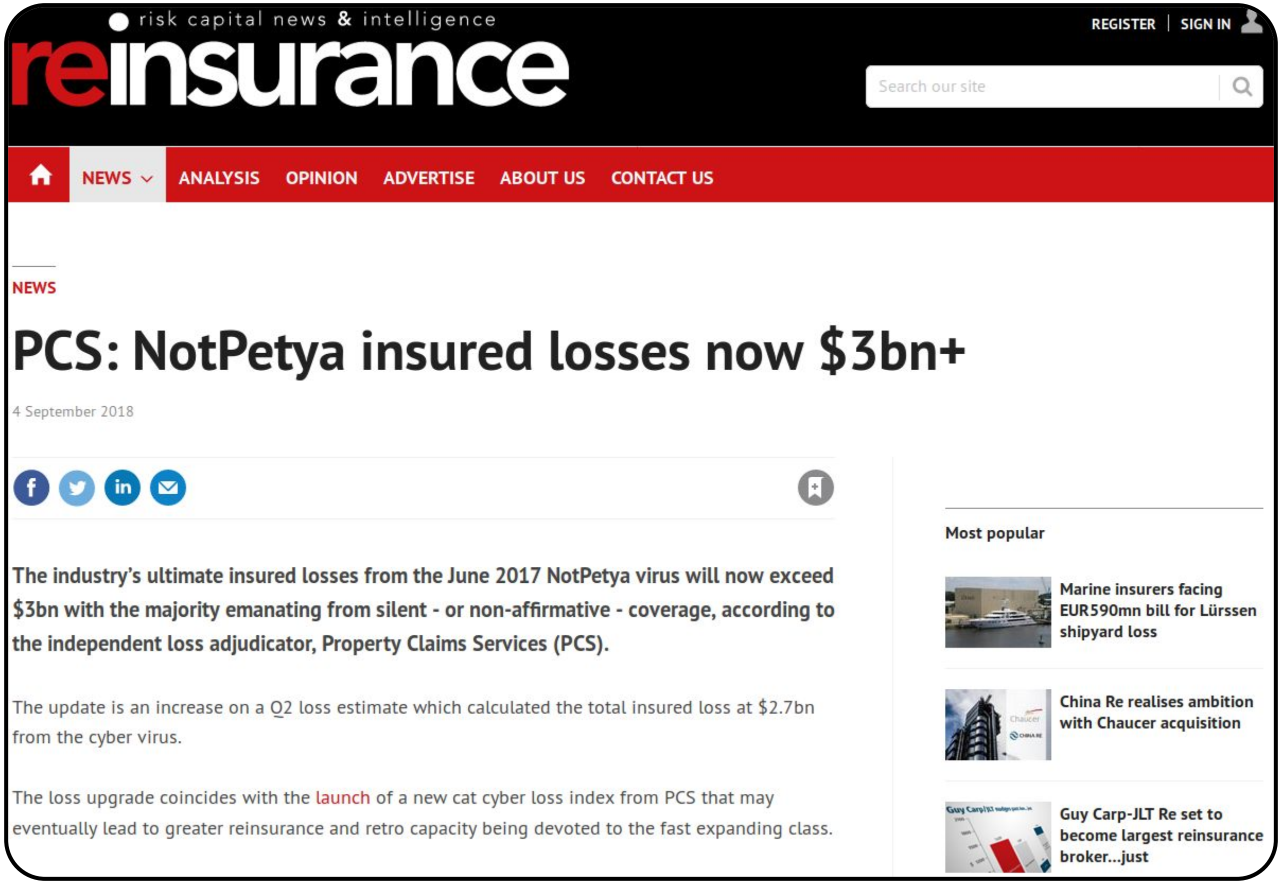
- E.g., You could make a “national health service” for malware if you were serious.

- You could create “not for profit” insurance clubs A.K.A. Mutuals.

[10] Clayton, Richard. "Might governments clean-up malware?." (2011).

Payments != The full cost to society

- Total amount of ransom ~= $88.4 Million
- PCS’s estimated losses from NotPetya in 2017 ~= $3 Billion
- Suggests….insurance pays out ~= 34 x the ransoms


risk capital news & intelligence
reinsurance
REGISTER | SIGN IN
Search our site
NEWS
ANALYSIS
OPINION
ADVERTISE
ABOUT US
CONTACT US
Most popular
Marine insurers facing EUR590mn bill for Lürssen shipyard loss
China Re realises ambition with Chaucer acquisition
Guy Carp-JLT Re set to become largest reinsurance broker...just

NEWS

PCS: NotPetya insured losses now $3bn+

4 September 2018

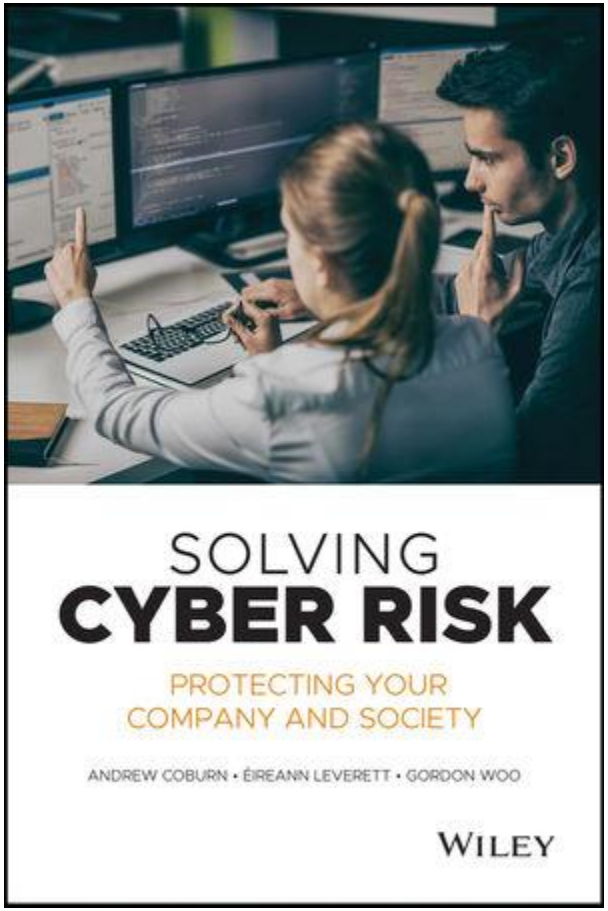
The industry’s ultimate insured losses from the June 2017 NotPetya virus will now exceed $3bn with the majority emanating from silent - or non-affirmative - coverage, according to the independent loss adjudicator, Property Claims Services (PCS).

The update is an increase on a Q2 loss estimate which calculated the total insured loss at $2.7bn from the cyber virus.

The loss upgrade coincides with the launch of a new cat cyber loss index from PCS that may eventually lead to greater reinsurance and retro capacity being devoted to the fast expanding class.

Questions?

Éireann has a book out in December



SOLVING
CYBER RISK

PROTECTING YOUR
COMPANY AND SOCIETY

ANDREW COBURN • ÉIREANN LEVERETT • GORDON WOO

WILEY

Payments analysis

What we discovered

- Ransomware campaigns are increasing day-by-day. Moreover, they are launched by even novice users.
- Insurance - a need or mandate?
- Why can’t you just ban encryption on machines?
- Examples of risk to small organisation, a large business, or a country.

Thank you!

spritz.math.unipd.it/projects/btcransomware/