

Research at 

Tracking desktop ransomware payments

Elie Bursztein, Kylie McRoberts, Luca Invernizzi

with the help of many people from UCSD, NYU, and Chainalysis





Only **37%** of users backup their data

Privacy & Security

WannaCry highlights worst nightmare in medical device security

Among the many lessons that will come out of the massive cyberattack might be a rethink of common patching practices.

May 15, 2017 | 03:17 PM



SAN FRANCISCO — The sprawling WannaCry ransomware attacks have healthcare

Forbes / Security / #CyberSecurity

Ransomware Decrypts Your Files For Free If You Infect Your Friends

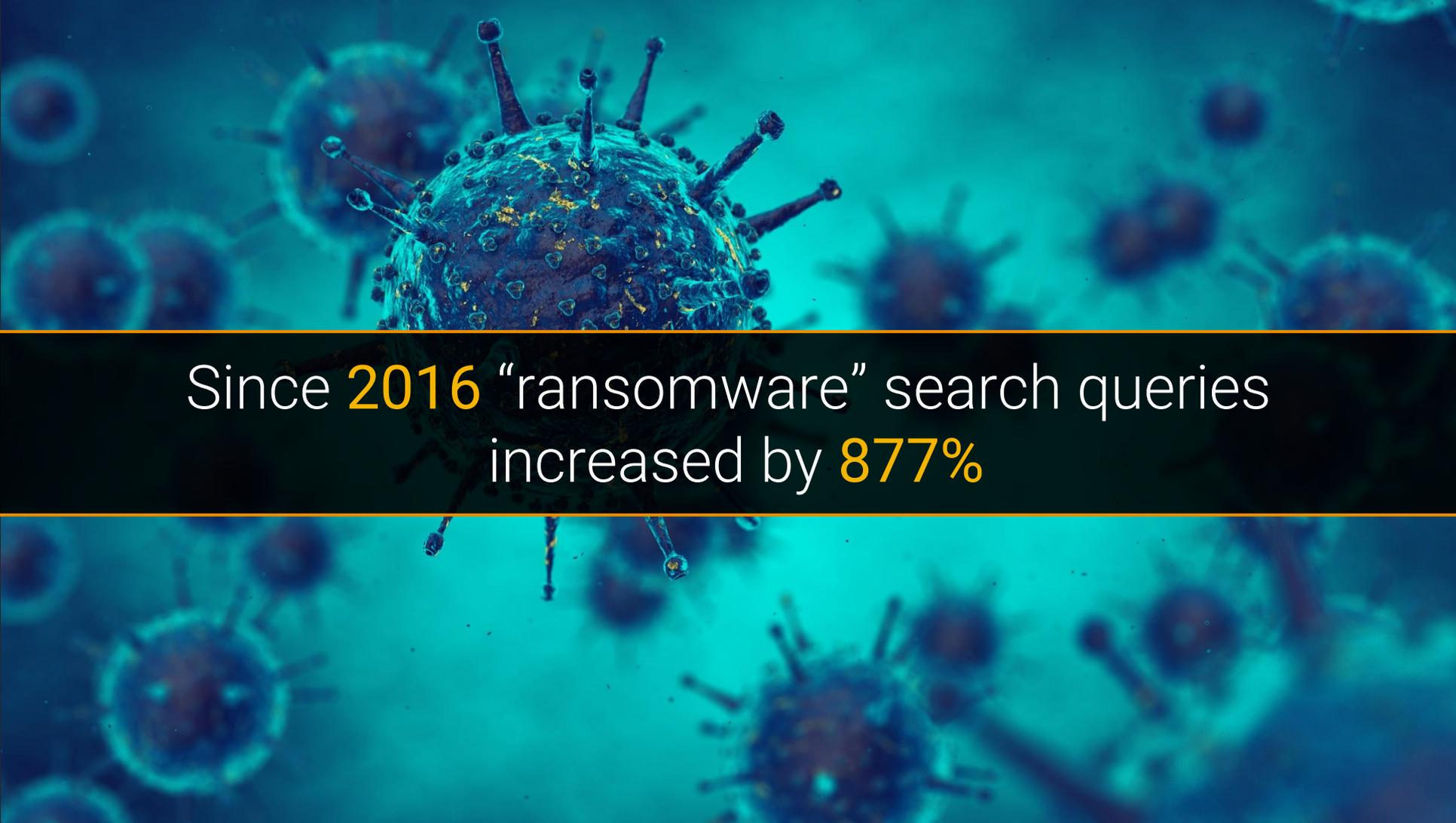


ARE YOU FEELING LOCKY? —

Locky ransomware uses decoy image files to ambush Facebook, LinkedIn accounts



Unbreakable Locky ransomware is on the march again



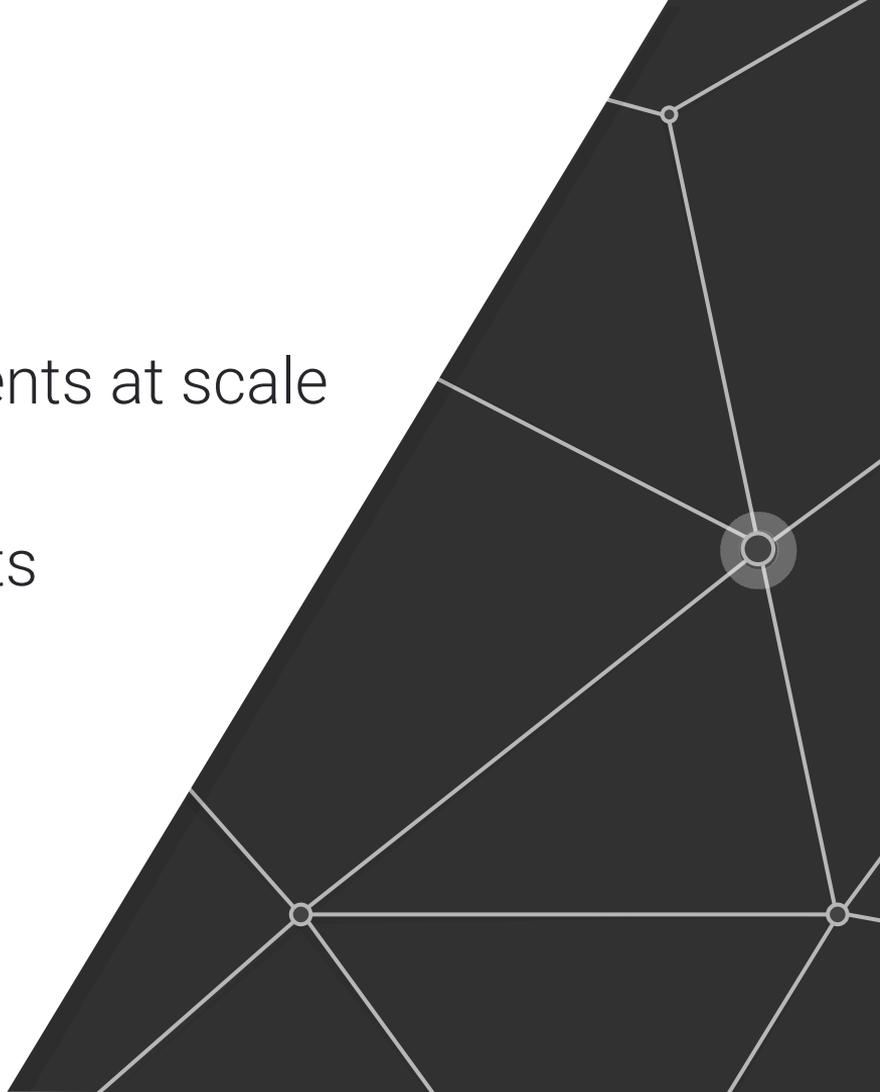
Since **2016** “ransomware” search queries increased by **877%**

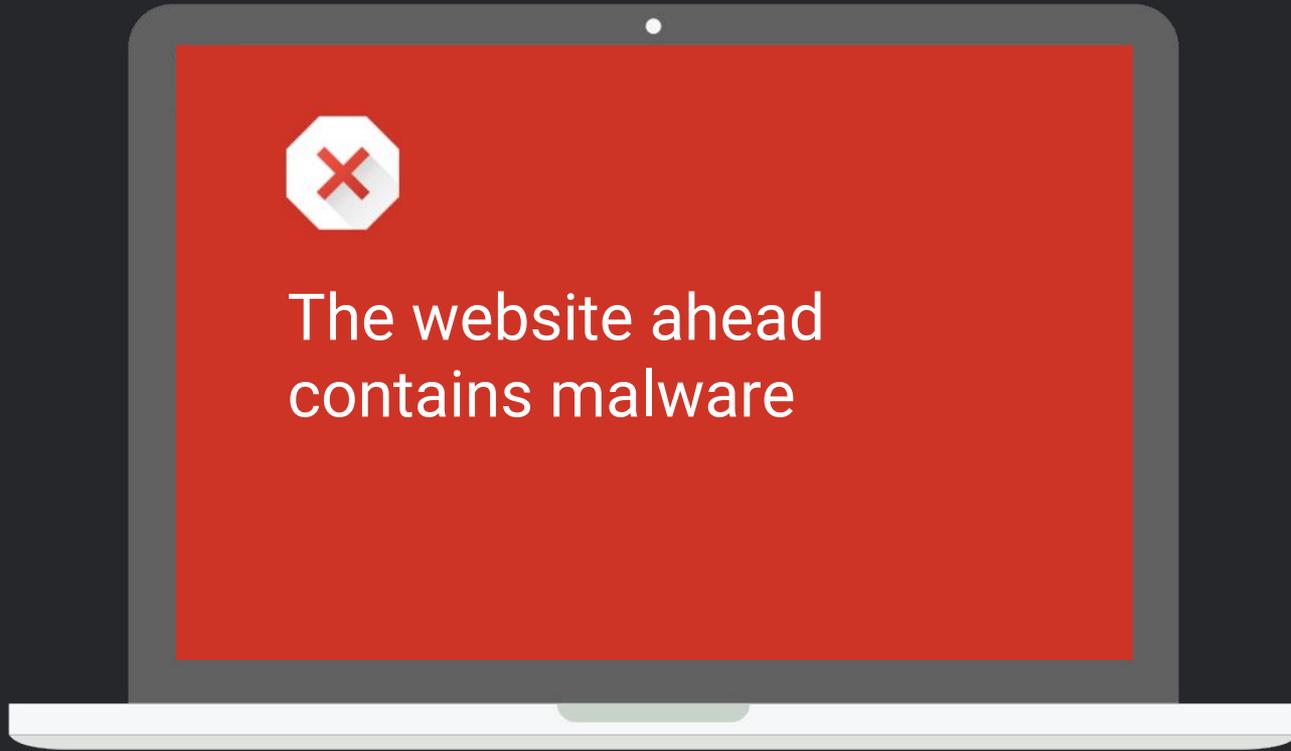


How **profitable** is ransomware?

Agenda

1. How we **trace** ransom payments at scale
2. **Revenue** & ecosystem insights
3. The **kingpins** and the fads





Keeping users safe

The team



Google



Chainalysis



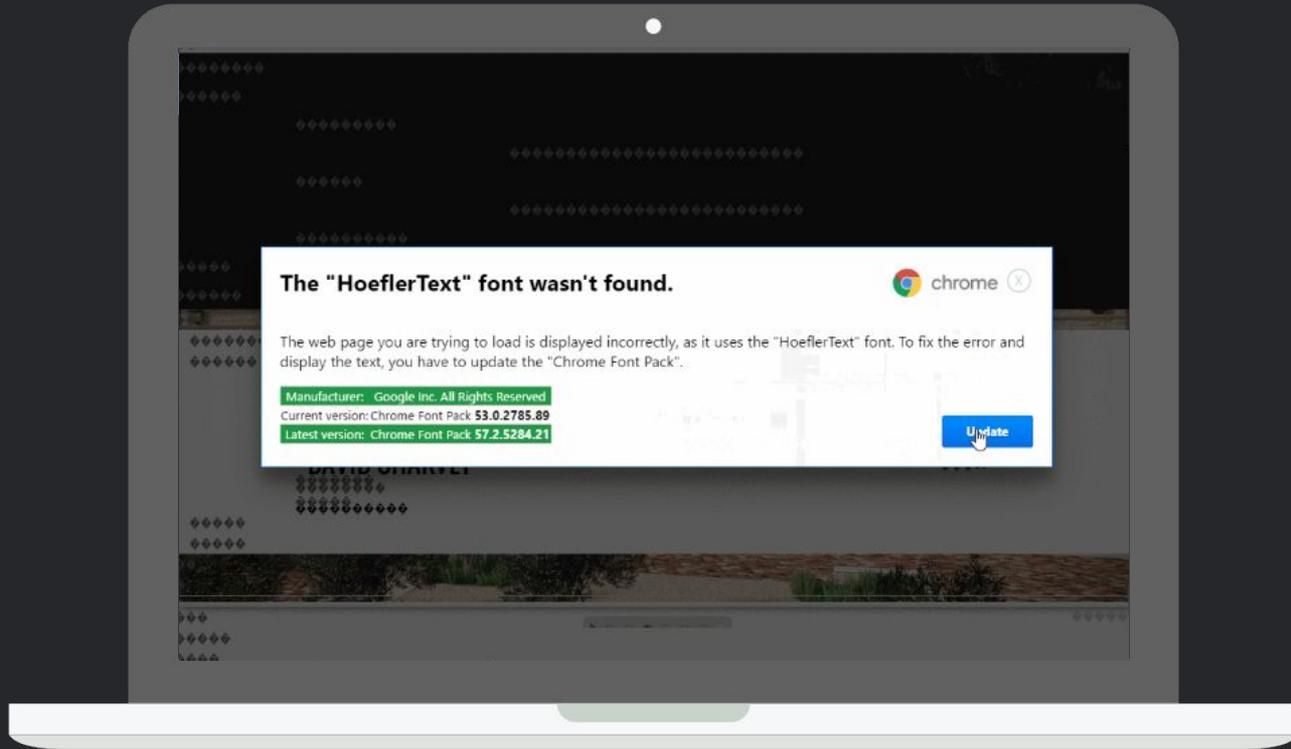
University of
California,
San Diego



New York
University



Life of a ransomware infection



Victim gets infected

CERBER RANSOMWARE

Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

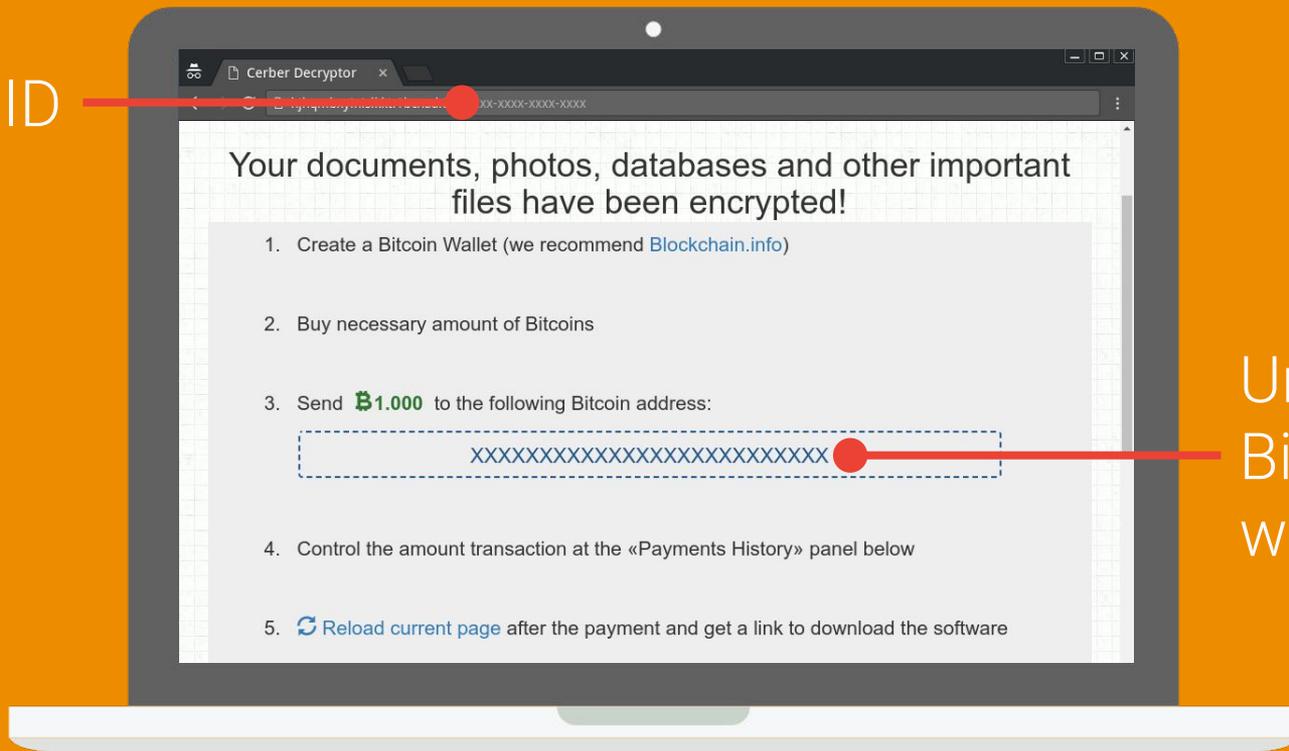
You can proceed with purchasing of the decryption software at your personal page:

<http://hjqmbyinislkk.1d8y5e.top/>

Payment URL

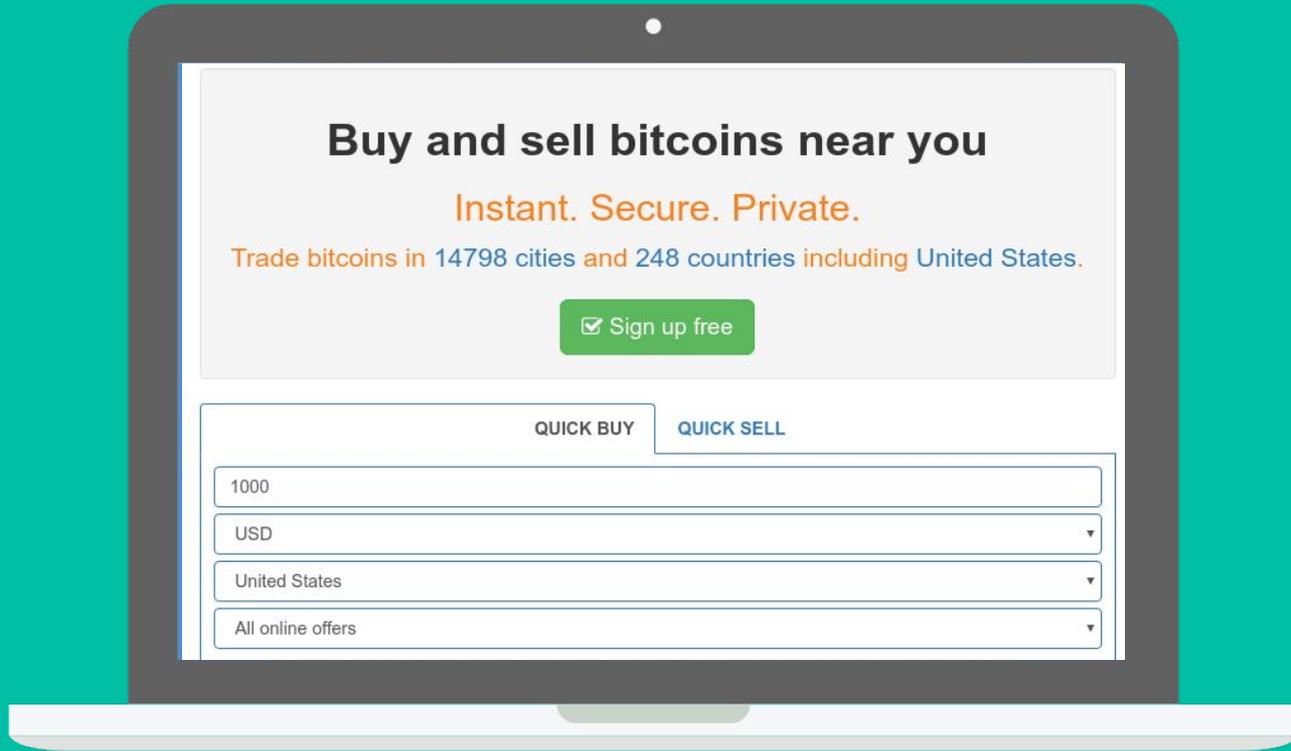
Victim is shown ransom note

Victim ID



Unique
Bitcoin
wallet

Victim visits payment site via Tor



Victim buys bitcoin at *exchange*

Why Bitcoin?



Pseudonymous

No need to show ID card to create wallets

Fully Automatable

Allows scalable payment processing

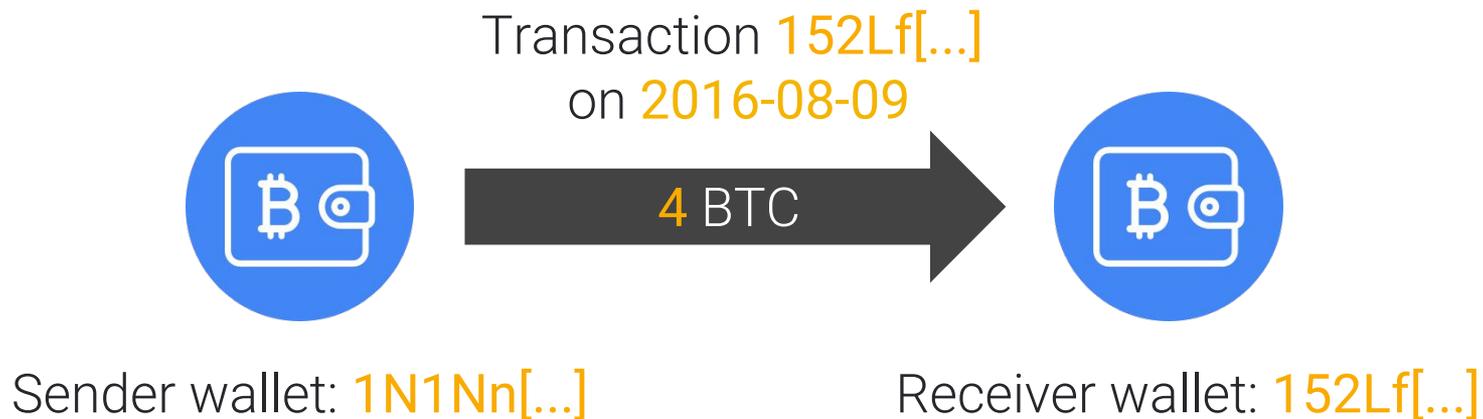
Irrefutable

Transactions can't be reverted

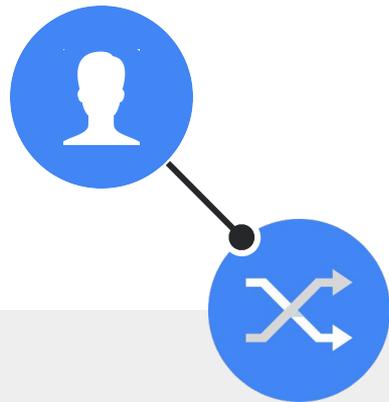
Fungible

Bitcoins are easily converted into cash

Bitcoin transactions are public

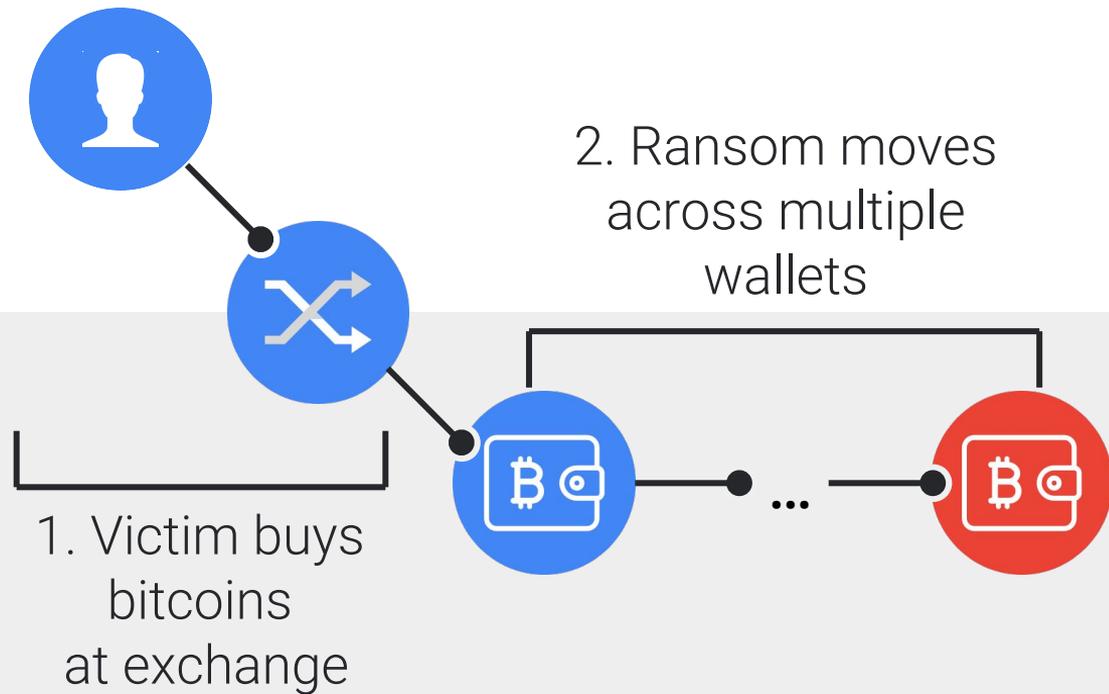


Life of a ransom payment

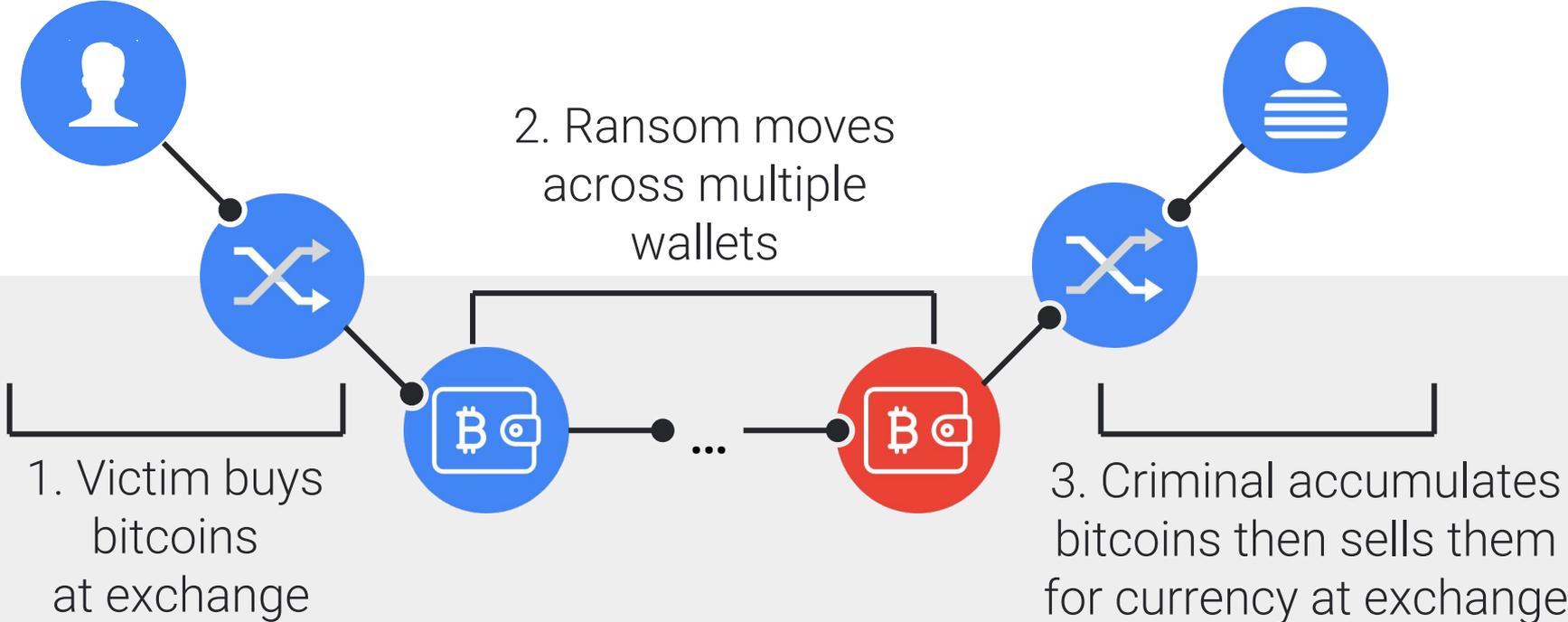


1. Victim buys
bitcoins
at exchange

Life of a ransom payment



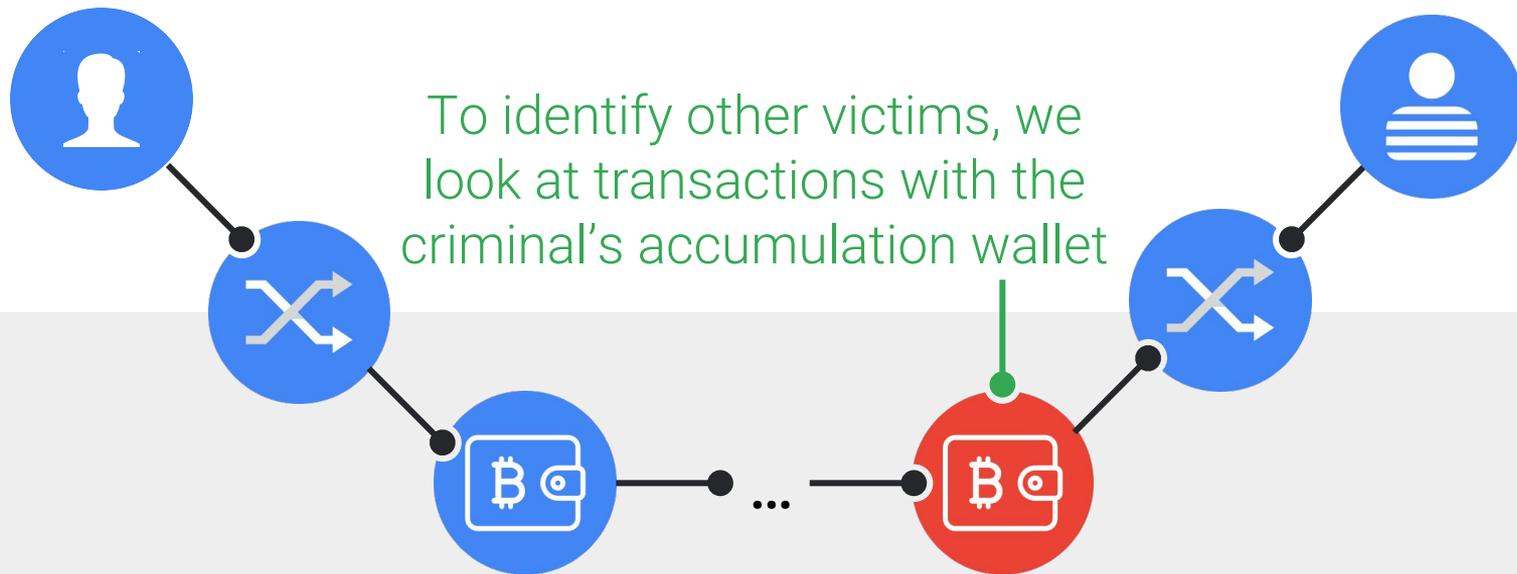
Life of a ransom payment



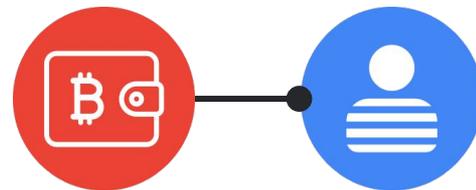


Measuring revenue

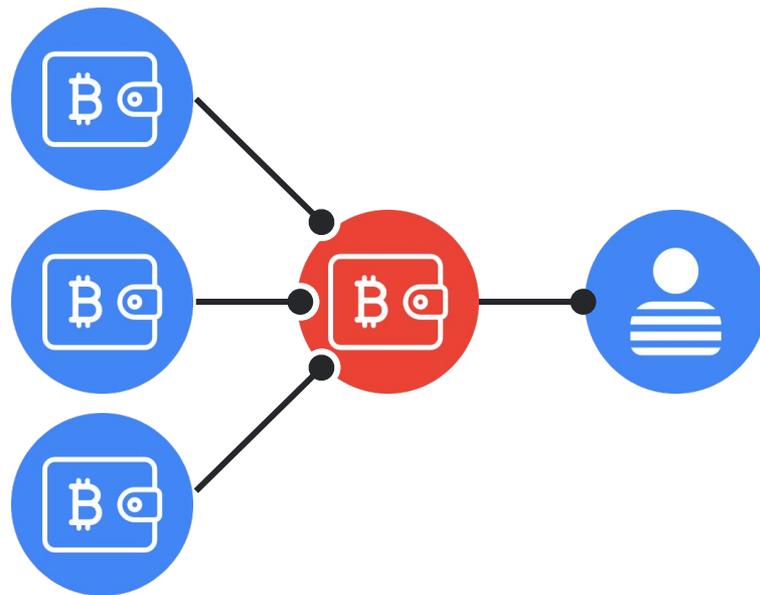
Identifying victims



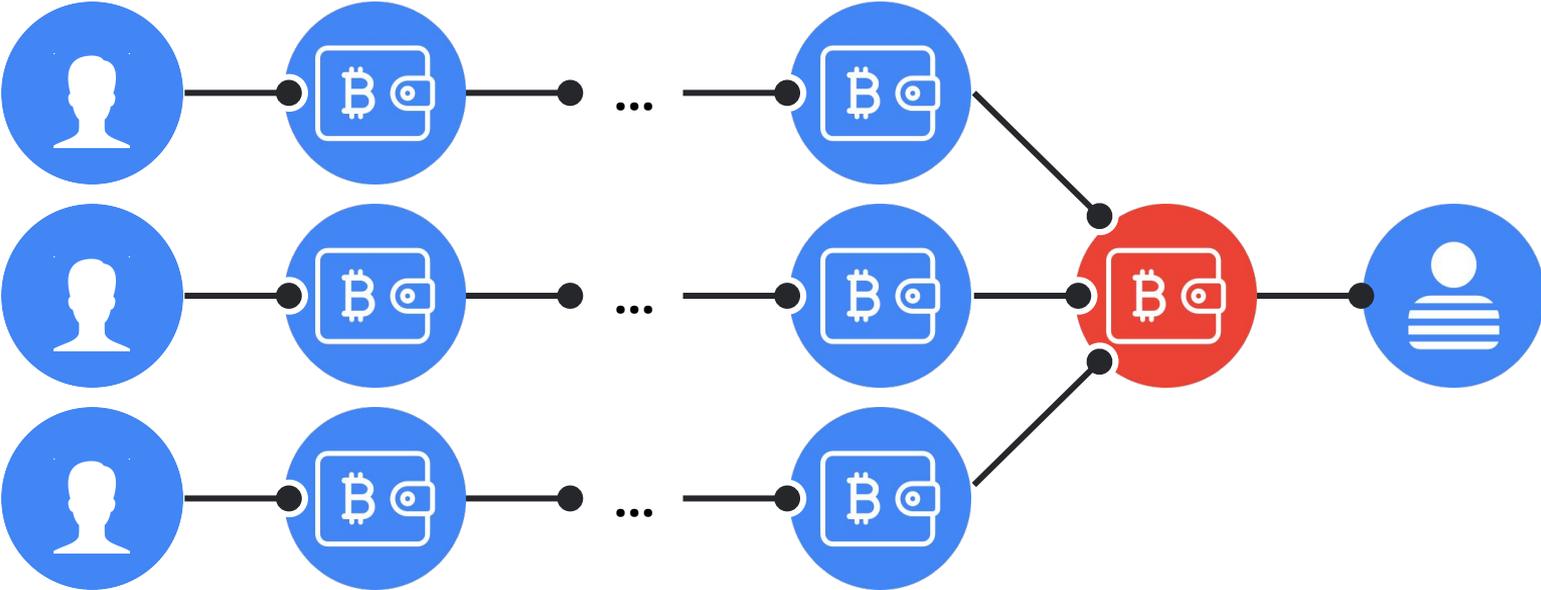
Discovering payment network



Discovering payment network



Discovering payment network



Gathering seed bitcoin transactions

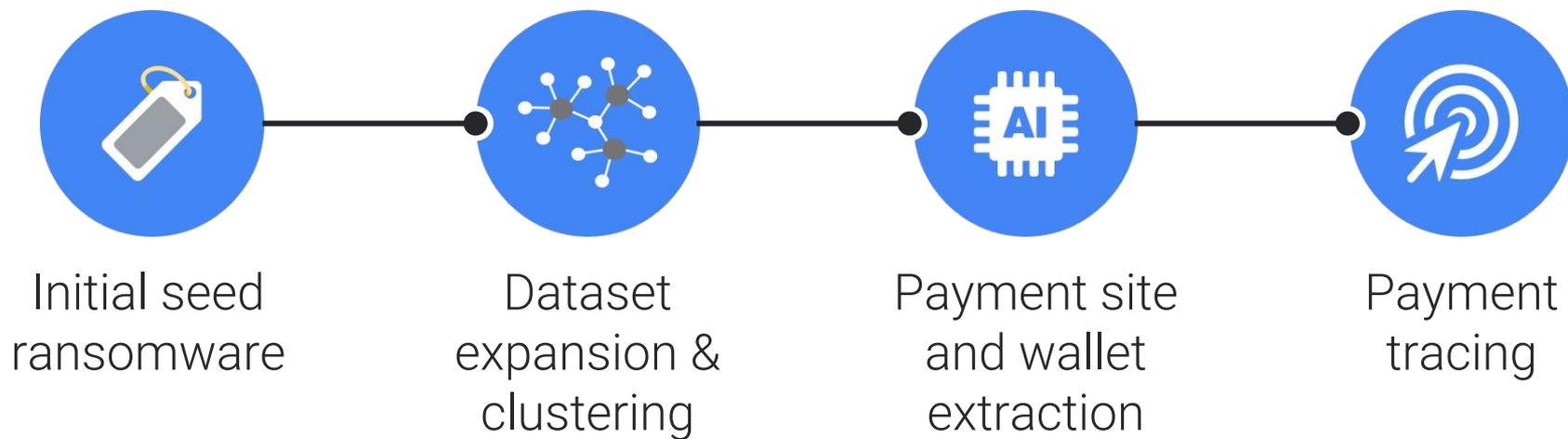


Victim reports

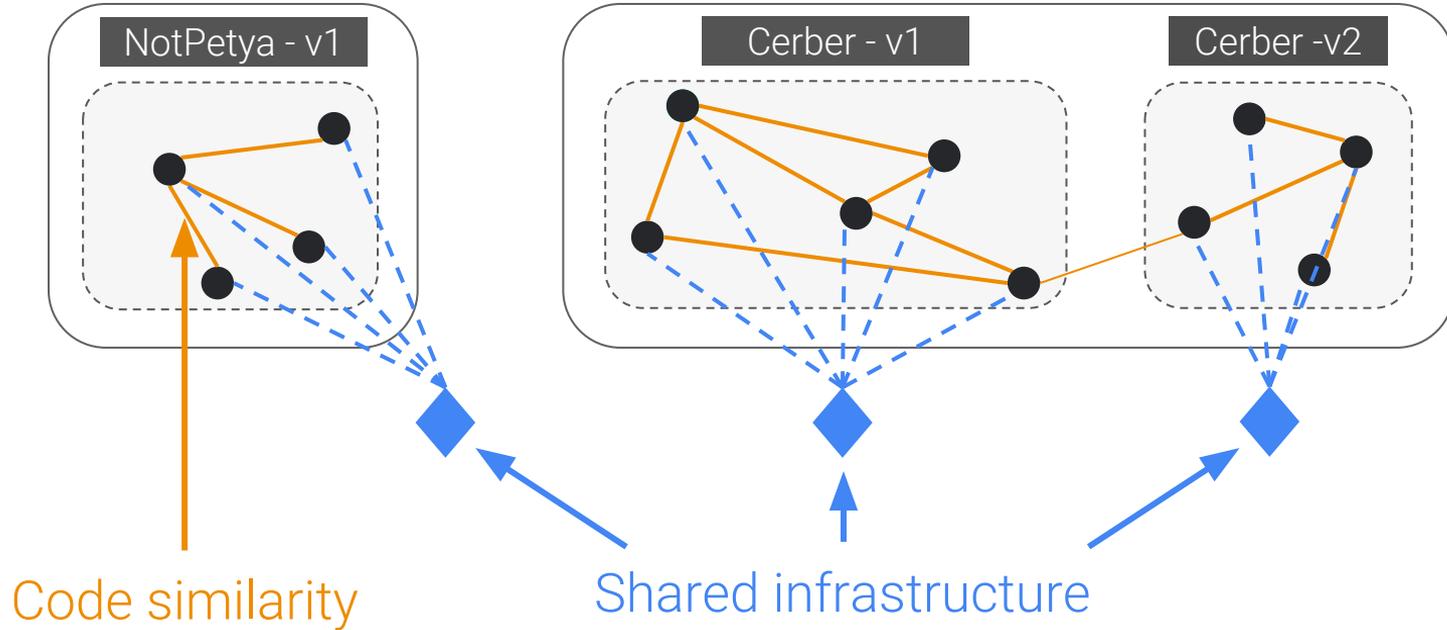


Synthetic “victims”

Automating payment tracing



Using clustering for dataset expansion



Expanded dataset 301,588 binaries

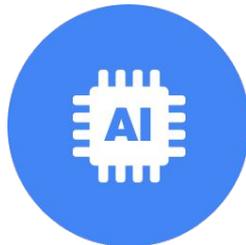
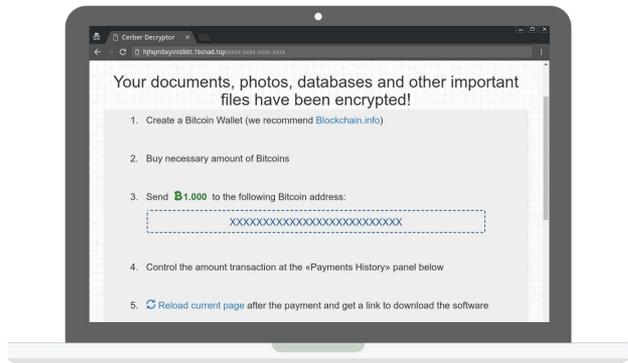
154,227

Seed dataset

147,361

Additional binaries

Automatically identifying payment sites at scale



Tor proxy URL

hjhqmbxyinislkkt.1a58vj.top/XXXX

Found in 4 files and 1 screenshot



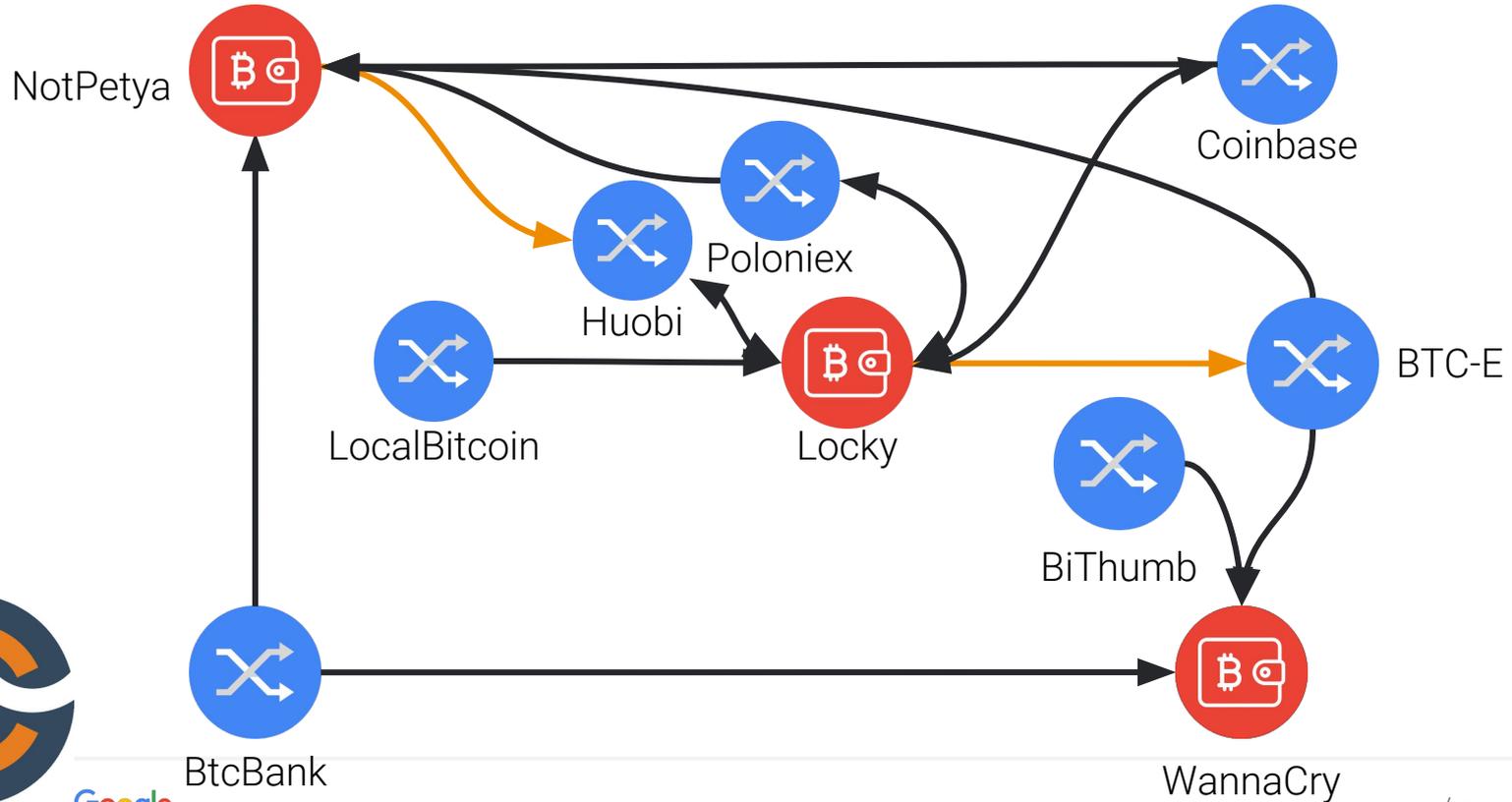
Bitcoin wallet

1AZvk[...]

Found in 16 files and 1 screenshot



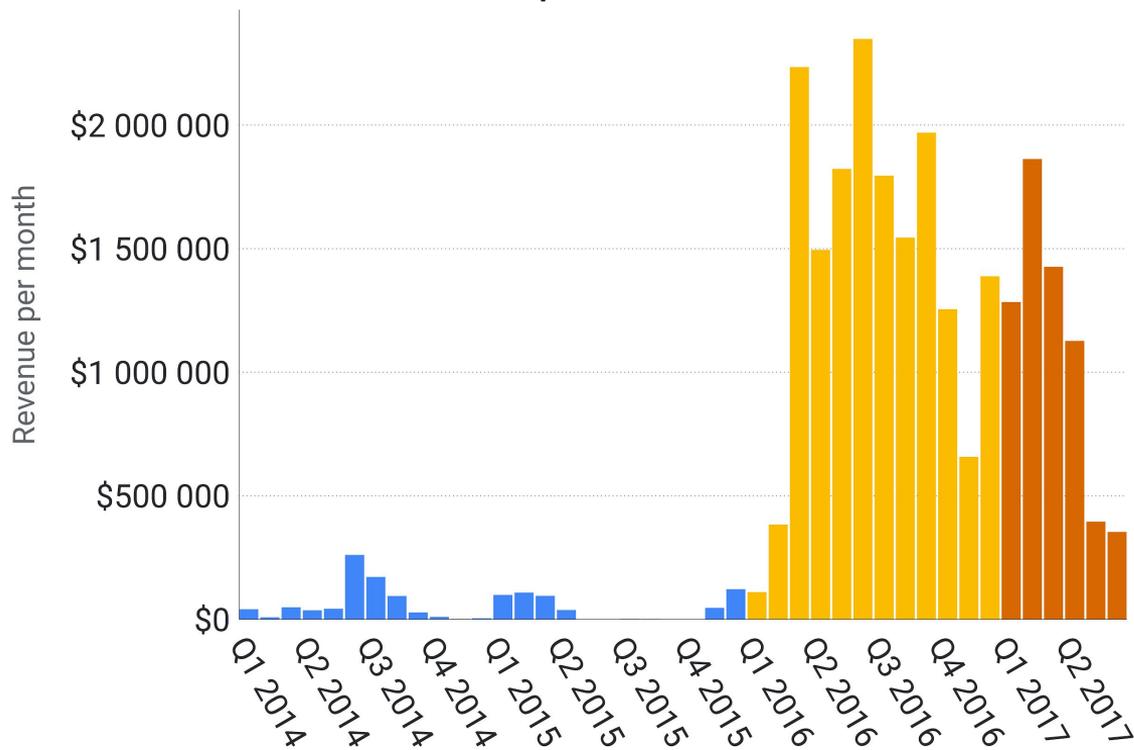
Tracing payments through the bitcoin chain



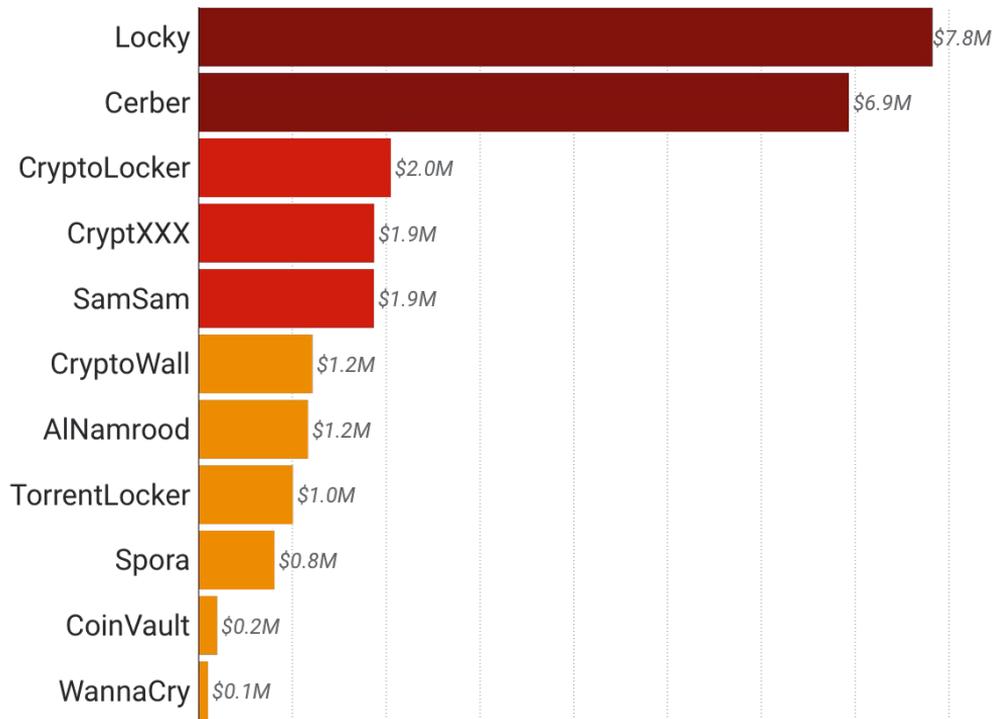
Market insights

\$25,253,505

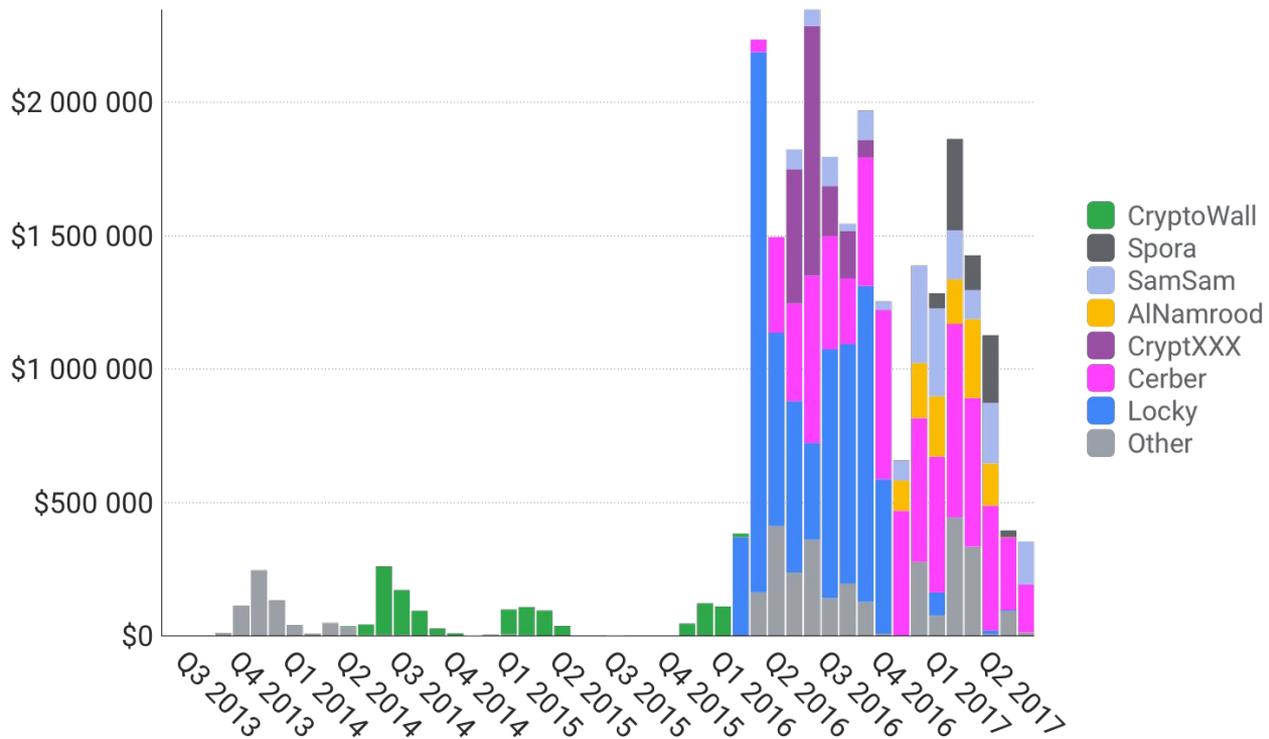




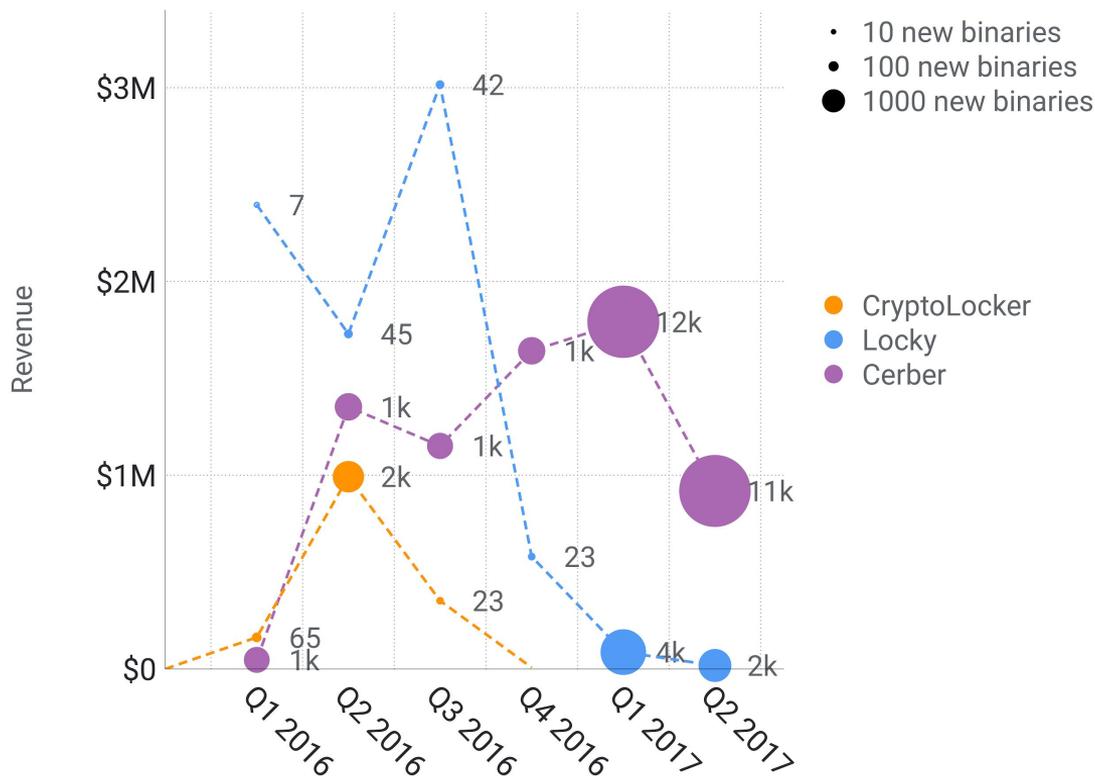
In 2016 ransomware became a multi-million \$ business



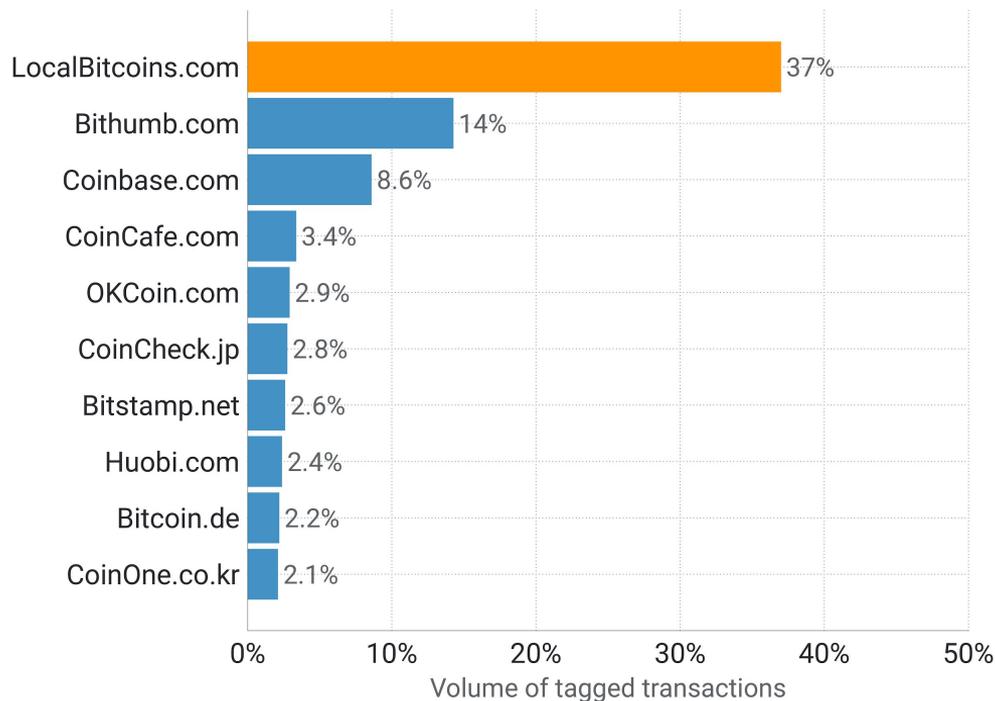
The ecosystem is dominated by a few kingpins



A fast changing market



In 2017 ransomware increased binary diversity to evade AVs



LocalBitcoins.com

Buy and sell bitcoins near you

Instant. Secure. Private.

Trade bitcoins in 14815 cities and 248 countries including United States.

[Sign up free](#)

QUICK BUY **QUICK SELL**

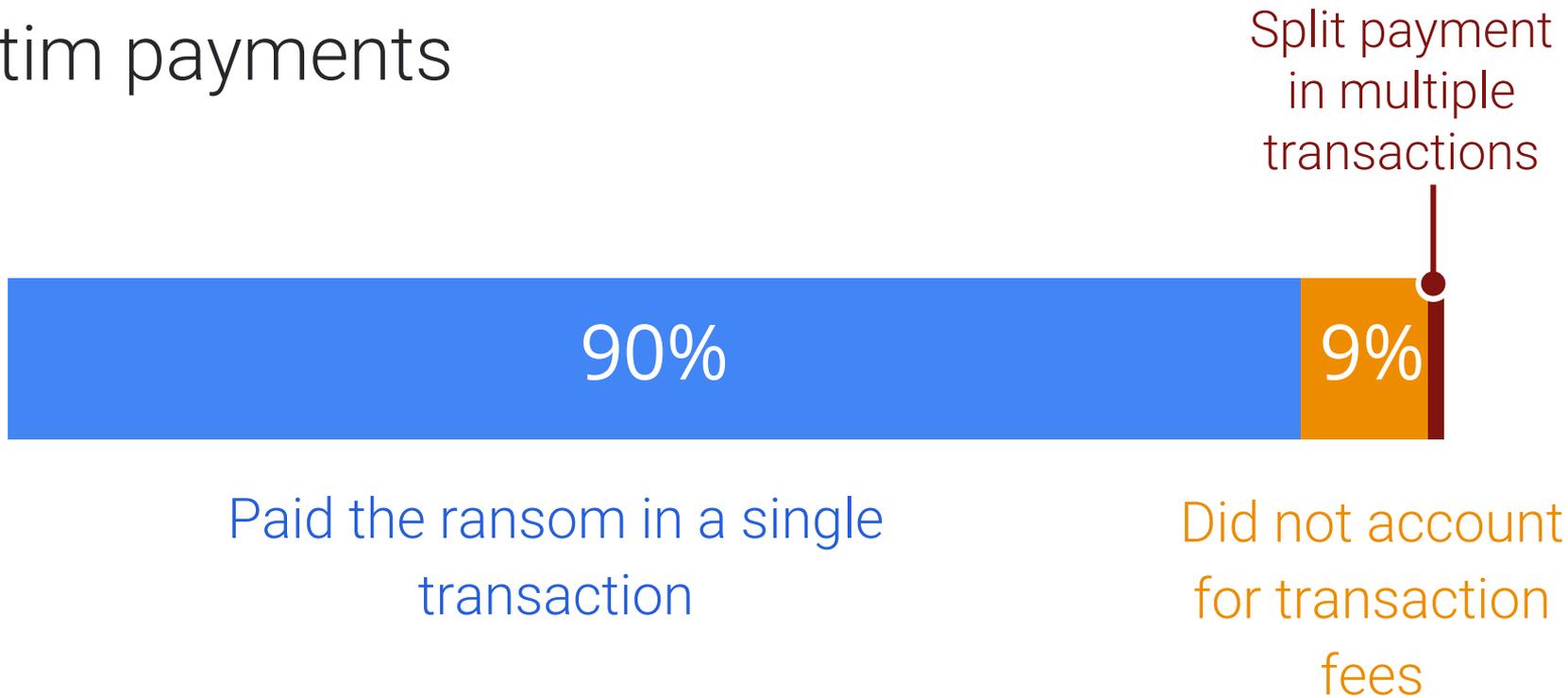
Amount

USD

United States

Many victims buy Bitcoins through the “Craigslit of Bitcoin”

Victim payments



95%

traced ransoms cashed out
via BTC-E

Cashout list available on request

The screenshot shows the BTC-E website interface. At the top, it displays the BTC logo and market statistics: Last Price: 1072.532 USD, Low: 1040 USD, High: 1270 USD, Volume: 14324 BTC / 17073828 USD, and Server Time: 11.03.17 00:23. There are login fields for E-Mail and Password, and links for Login, Sign up, and Lost password.

The main navigation bar includes Trade, Bitcoin Betting, News, PAMM, and Support. The "Latest news" section shows two items: "25/02/17 CloudFlare parser bug" and "10/02/17 Bitcoin Betting".

A central market data table lists various cryptocurrencies and their prices in USD and EUR. Below the table is a candlestick chart showing price fluctuations over a 24-hour period.

On the left side, there are "Buy BTC" and "Sell BTC" forms. The "Buy BTC" form shows a balance of 0 USD, a lowest ask price of 1083.732 USD, and a price per BTC of 1083.732 USD. The "Sell BTC" form shows a balance of 0 BTC, a highest bid price of 1081.91 USD, and a price per BTC of 1081.91 USD.

At the bottom, there are "Sell orders" and "Buy orders" sections. The "Sell orders" table shows a total of 2743.42 BTC with two orders: one at price 1083.732 BTC / 1.50850075 USD, and another at price 1083.733 BTC / 12.82814752 USD. The "Buy orders" table shows a total of 11594947.37 USD with three orders: one at price 1081.91 BTC / 11.48659612 USD / 12427.46320818 USD, one at price 1080.088 BTC / 1.56420284 USD / 1689.47671704 USD, and another at price 1080.088 BTC / 1.56420284 USD / 1689.47671704 USD.

On the right side, there is a "Tweets" section by @btcecom, featuring a tweet from @btcecom about a Tor browser login problem and a retweet from @xBTCe about a desktop terminal release.



Ransomware notable actors



Lucky

*Bringing ransoms to
the masses*

Ransomware infections are surging as 'Locky' evolves into an effective cyberweapon



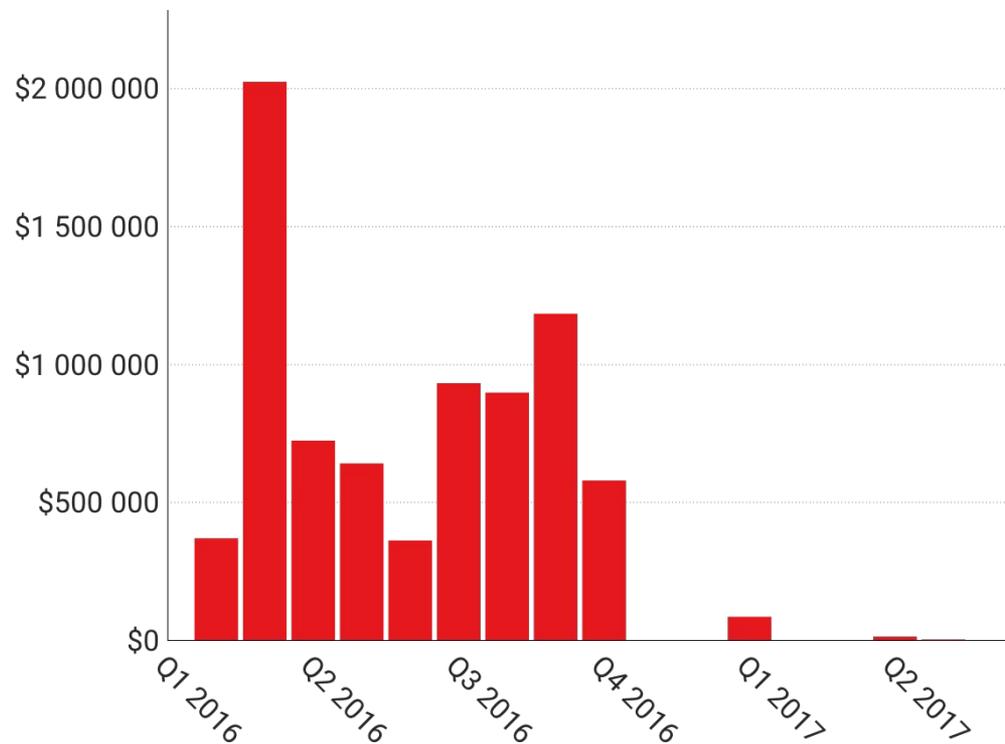
Security experts have warned that 'Locky' is quickly evolving into an effective piece of ransomware (iStock)



Locky ransomware is back, this time via Necurs



The godfather of ransomware returns: Locky is back and sneakier than ever

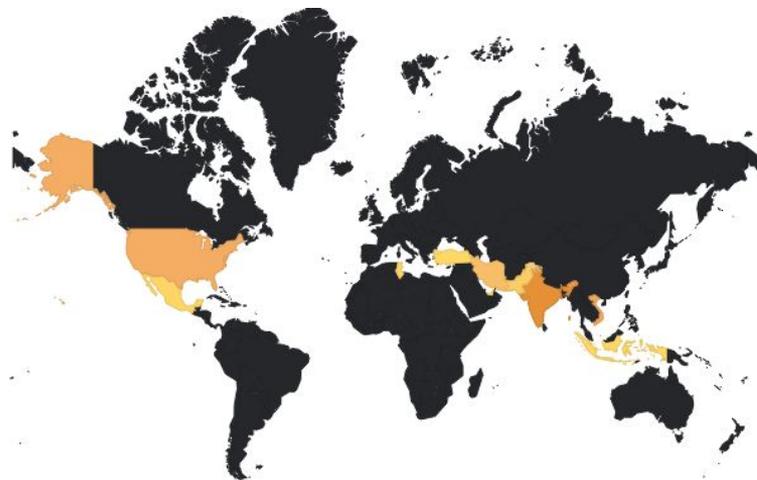


The first ransomware to make >\$1M per month

Renting-out cybercriminal infrastructure



Dridex



Locky

Dridex, Locky, Cerber are distributed via the Necurs botnet

Cerber

*Rise of ransomware
as service*



The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security 5

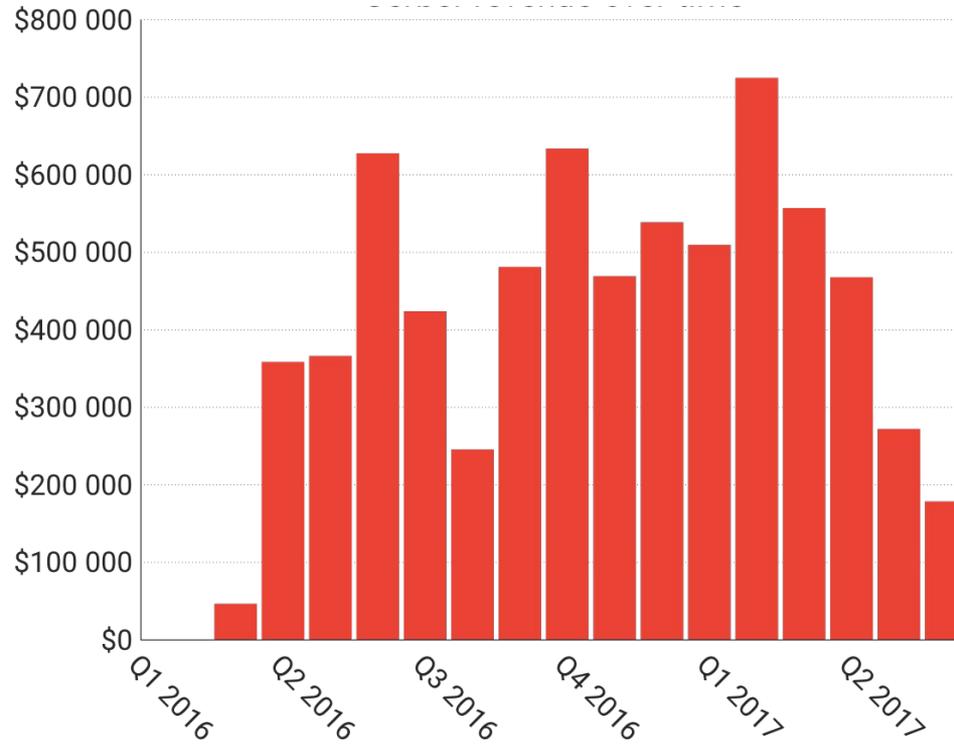
Cerber surpasses Locky to become dominant ransomware menace

Ransomware-as-a-Service is a hit with the tech illiterate

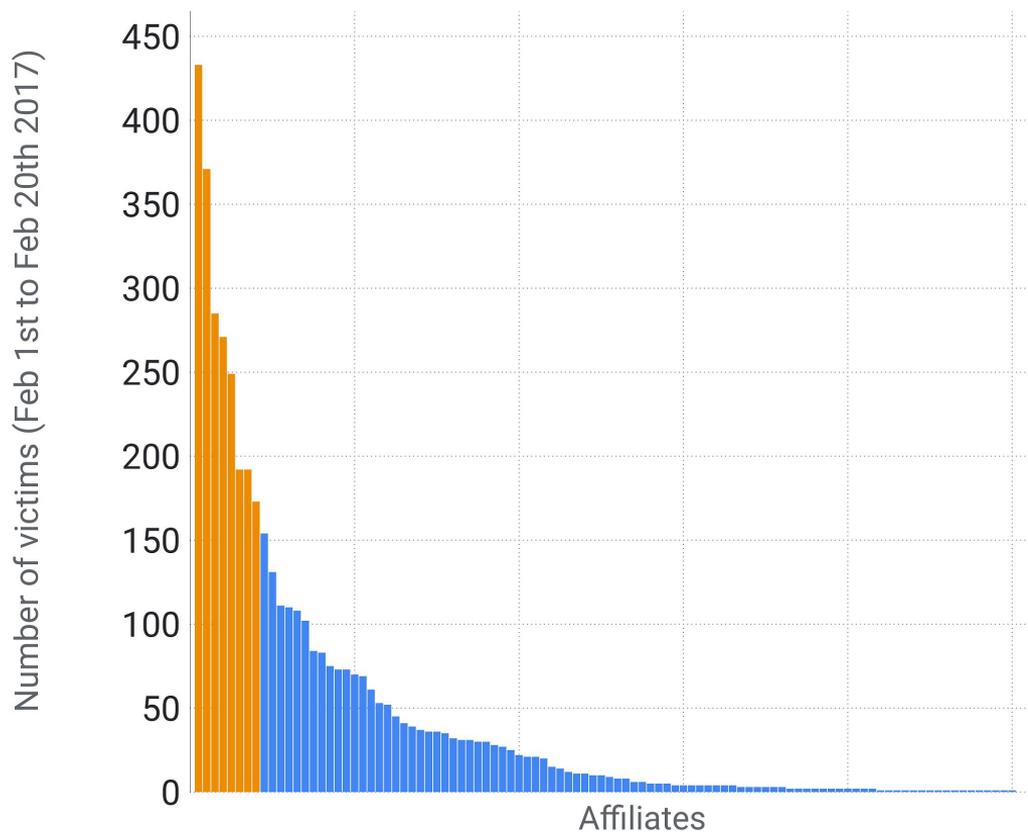
By [John Leyden](#) 13 Apr 2017 at 16:30 SHARE ▼



Enrolling low tech criminals made Cerber the new king of the hill in 2017



Consistent income - \$200k per month for over a year



8 affiliates are responsible for 50% of the infections



1AzkuxChzMB4[...]

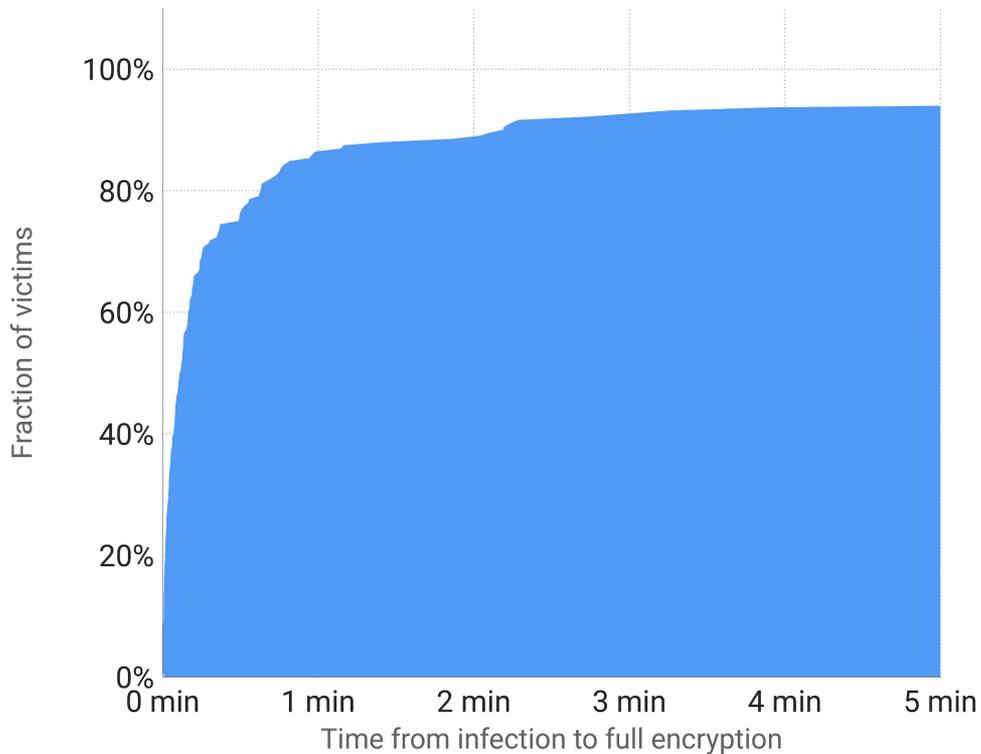


1Azkux.top

Embedding ransom site in the blockchain

Hardcoded wallet transacts with new wallets periodically.

Cerber derives ransom site from these wallets.



From infection to full encryption in under a minute



Spora

*Ransomware business
model refined*

My Purchasings

79\$ FULL RESTORE	50\$ IMMUNITY	20\$ REMOVAL	30\$ FILE RESTORE	2 FREE FILE RESTORE
----------------------	------------------	-----------------	----------------------	------------------------

Reference: You full decrypt price is 79 USD.

Available Payments

Current Balance: 0.00 USD



BitCoin
accepted here



Need Help?

Discount



Payment



Deadline



Welcome

Block Date: 10.01.2017
Username: NULL



Public Communication

Messages: 5

Greetings to all

Type your message..

Send

My Transactions

Date	Task	Balance
------	------	---------

No transactions yet..



Wannacry notPetya

Rise of the impostors



Ooop

If you see
when your
it from yo

If you see

Please fin
any folder

Run and fo

Wana Decrypt0r 2.0



Ooops, your files have been encrypted!

English

Payment will be raised on

5/18/2017 15:01:24

Time Left

00:00:00:00

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t8YDPgwueZ9NyMgw519p7AA8jsr6SMw

Copy

Check Payment

Decrypt

ted.

or" window,
you deleted

ftware.

.exe" in





▶ 0:00 ⌵

Massive cyberattack targeting 99 countries causes sweeping havoc

WannaCry now claiming 159 traffic cameras in Victoria

7,500 fines have already been cancelled across the state in the wake of the WannaCry ransomware.



A SCARY NEW RANSOMWARE OUTBREAK USES WANNACRY'S OLD TRICKS

The (low) bottom line



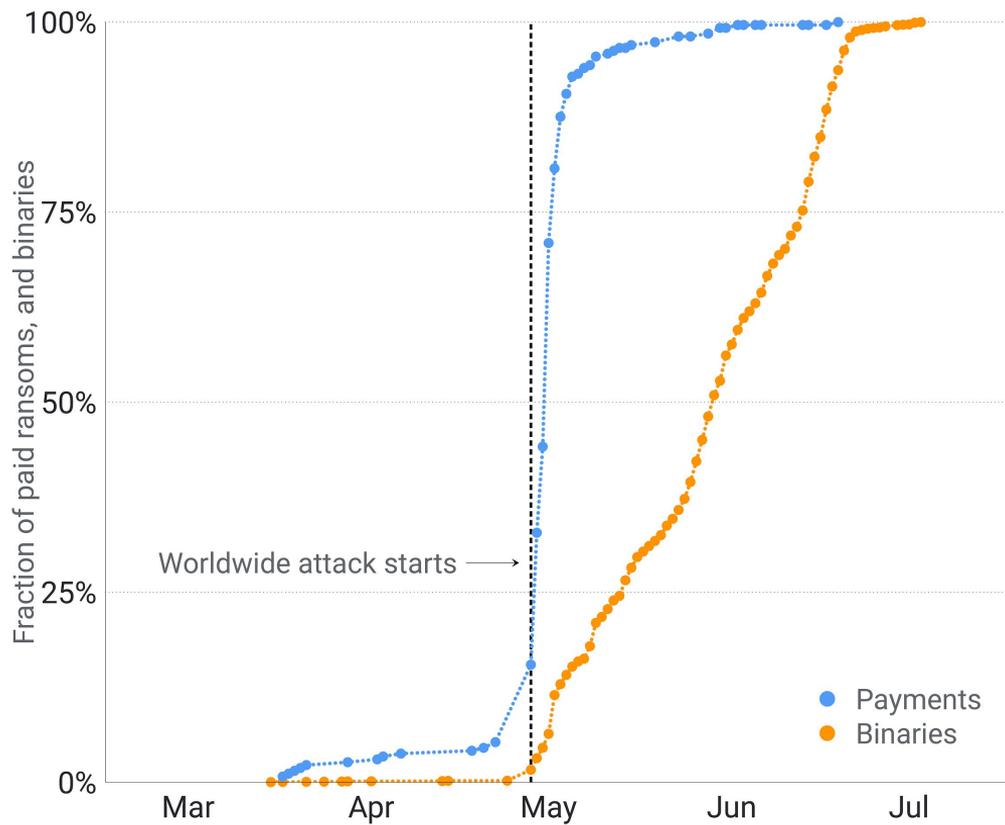
56 BTC
revenue



5
bitcoin wallets



\$0
cashed-out



Testing out the malware, then unleashing it at once

SECURELIST

ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

After an analysis of the encryption routine of the malware used in the [Petya/ExPetr attacks](#), we have thought that the threat actor cannot decrypt victims' disk, even if a payment was made.

```
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
```

```
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
```

```
Please follow the instructions:
```

```
1. Send $300 worth of Bitcoin to following address:
```

```
1Mz7153HMuxXTuR2R1t78mGSdzaftNbbHX
```

```
2. Send your Bitcoin wallet ID and personal installation key to e-mail nomsmith123456@posteo.net. Your personal installation key:
```

```
BSEHwb-CPccj7-Swa iAC-9UP1eg-KA3Hyu-ND9fd8-sUq54i-TAxTS8-MZoaT6-6A0SbF
```

```
If you already purchased your key, please enter it below.
```

```
Key: _
```

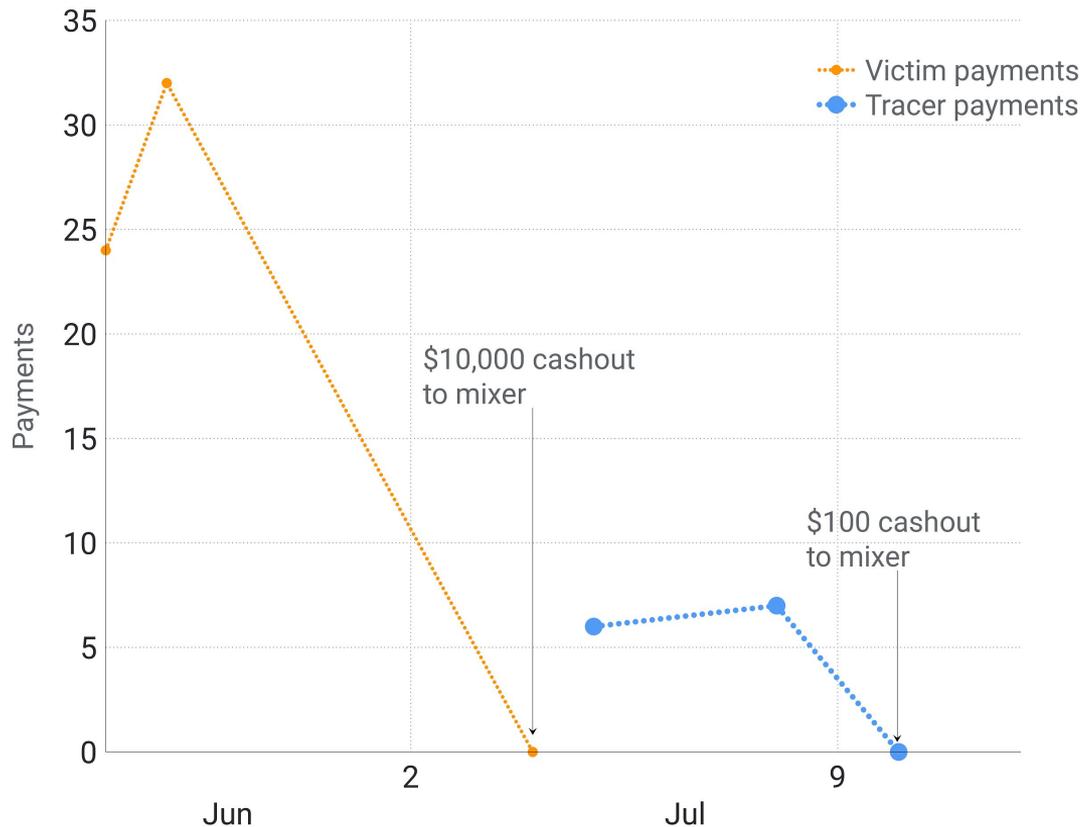
≡ Forbes

The NotPetya Ransomware May Actually Be A Devastating Cyberweapon



Latest ransomware twist: A demand for \$250,000

Following last week's NotPetya outbreak, a new ransom note demands bitcoin in exchange for a security key that decrypts locked files.



No early warning - Activity start on the day of the outbreak

Takeaways

Multi-million dollar black market

Ransomware generates tens of millions of revenue for criminals

RaaS is the new black

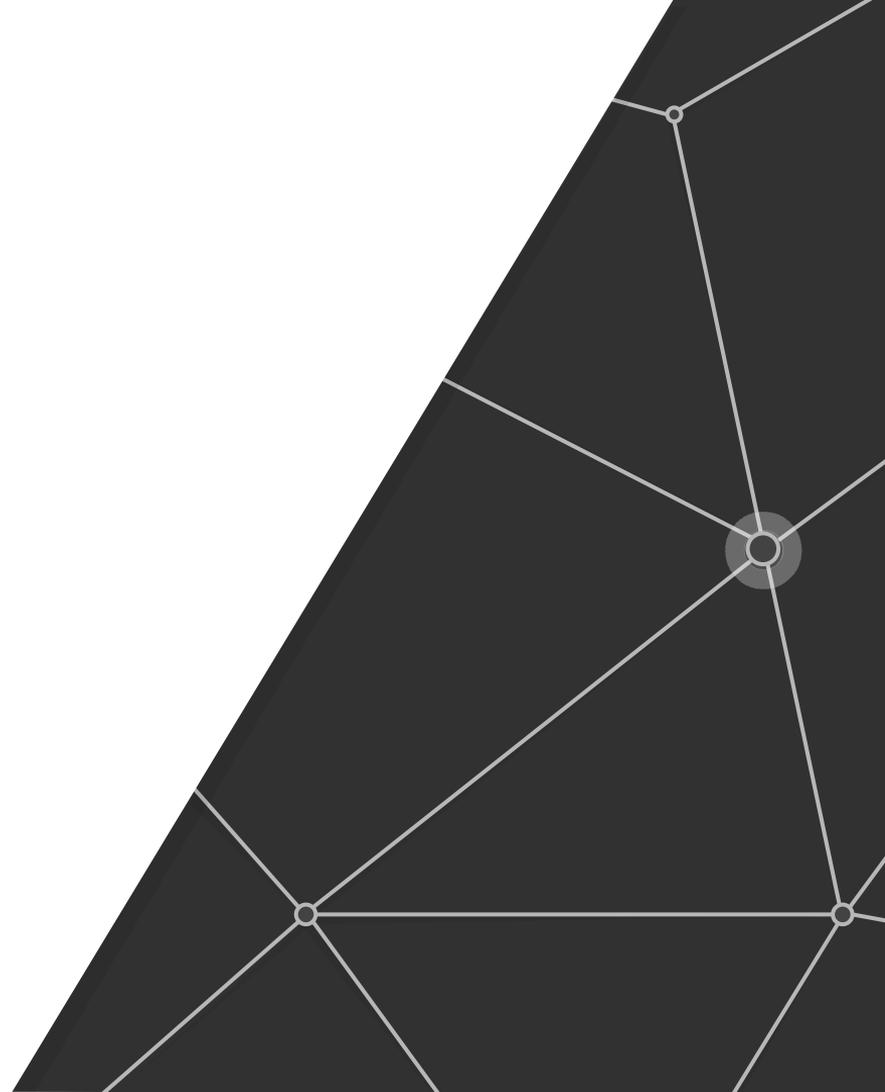
Cerber's affiliate model is taking the world by storm

Rise of the impostors

Wipeware pretending to be ransomware is on the rise

Questions?

Join us tomorrow 12pm | South Seas CD
Attacking encrypted USB keys
the hard(ware) way





Research at Google

Thank you

g.co/research/protect