

Research at **Google**

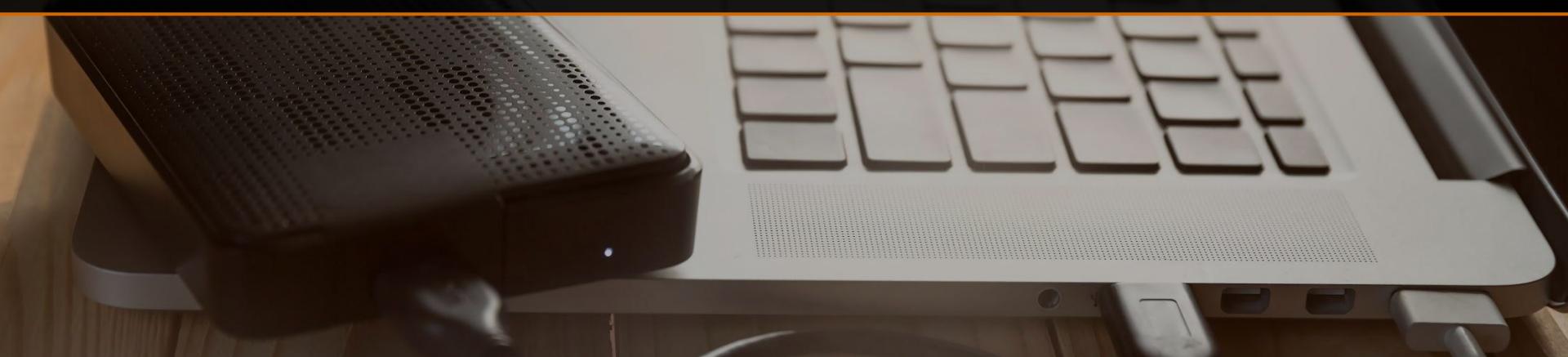
# Tracking desktop ransomware payments

**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



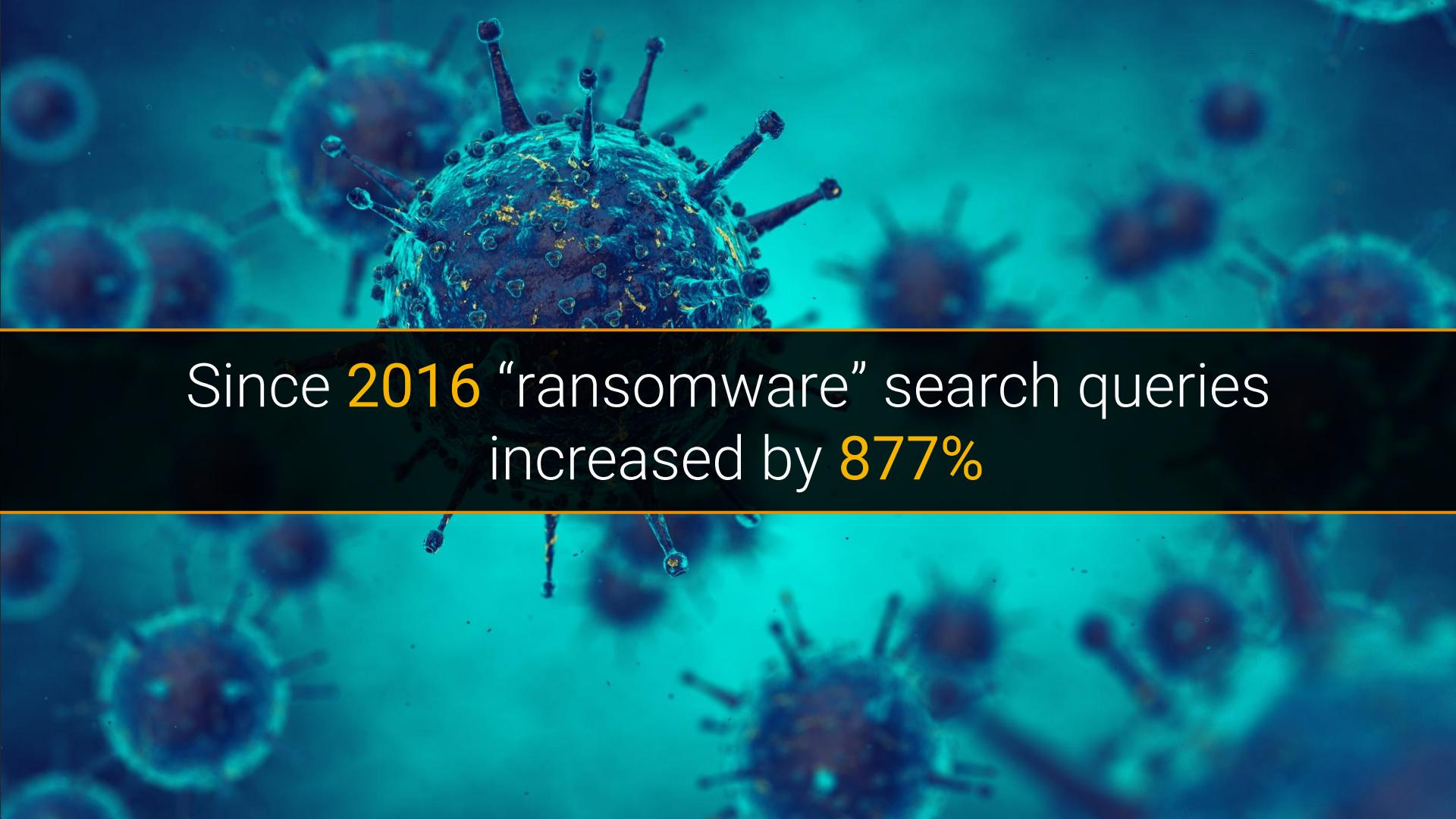
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

ARE YOU FEELING LOCKY? —

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



## Unbreakable Locky ransomware is on the march again



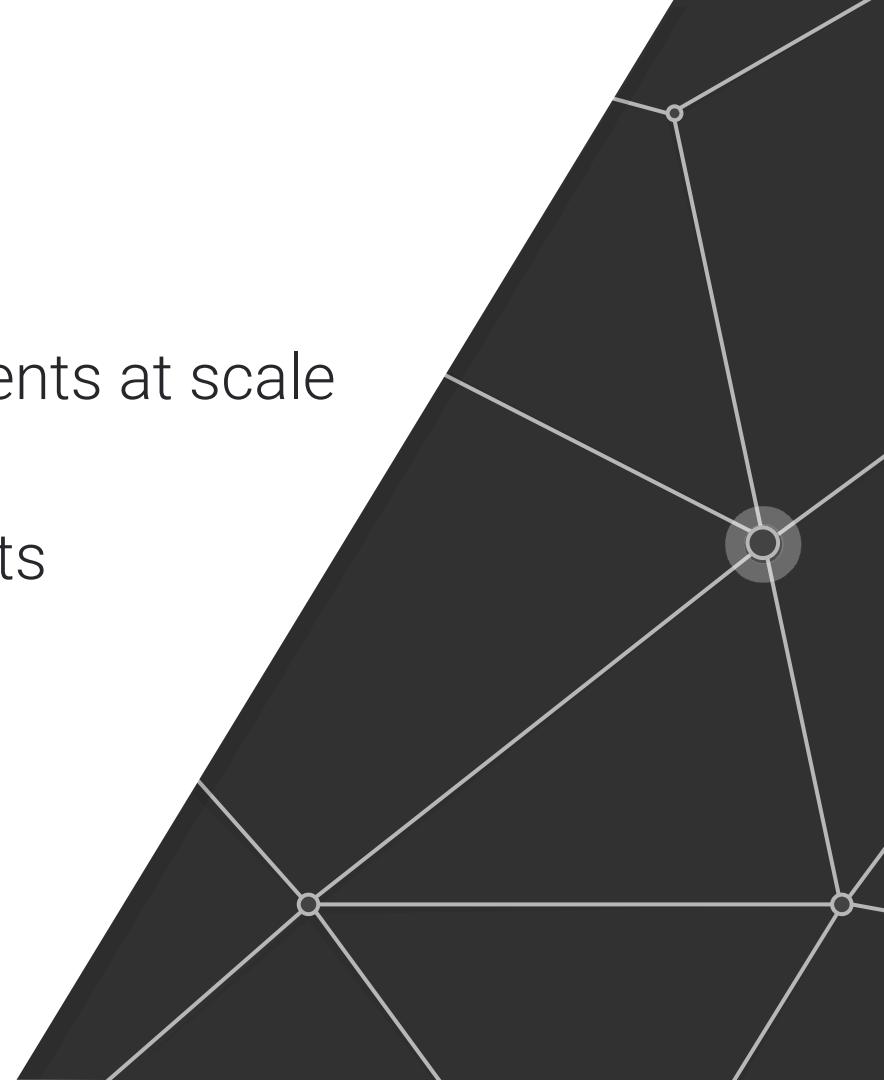
Since 2016 “ransomware” search queries increased by **877%**

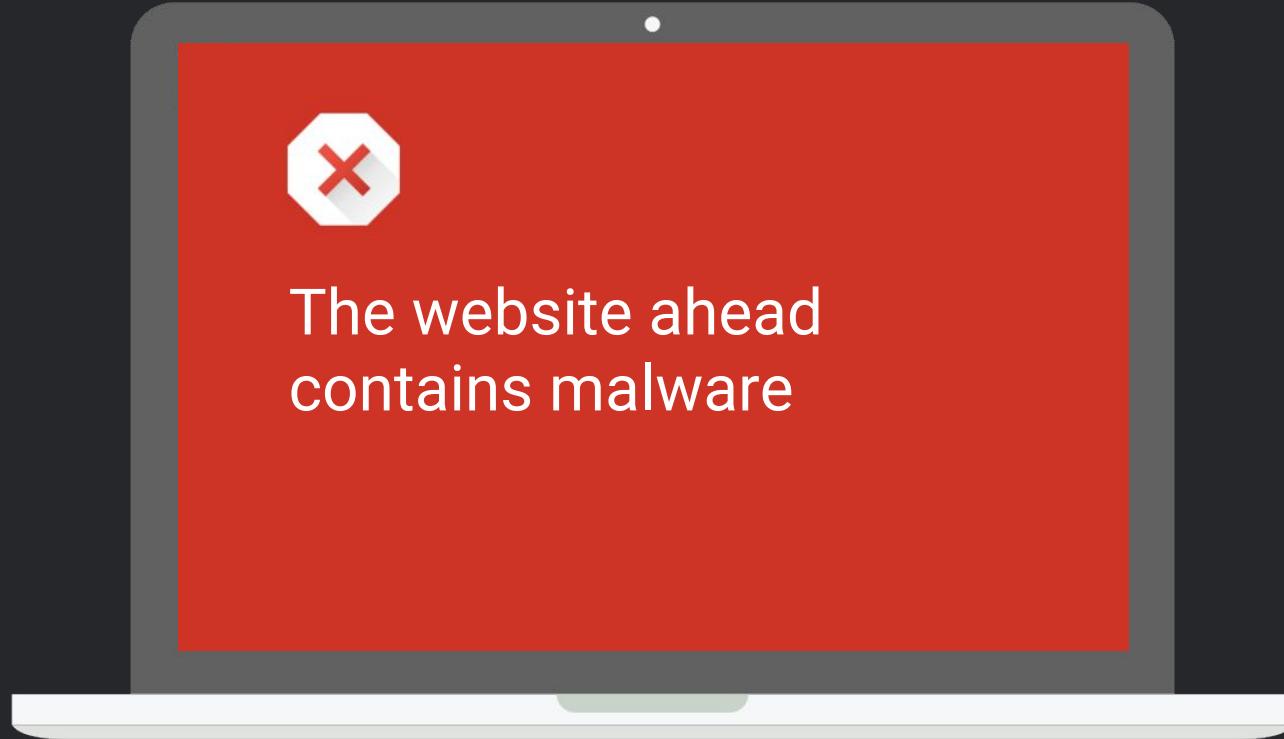


How **profitable** is ransomware?

# 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



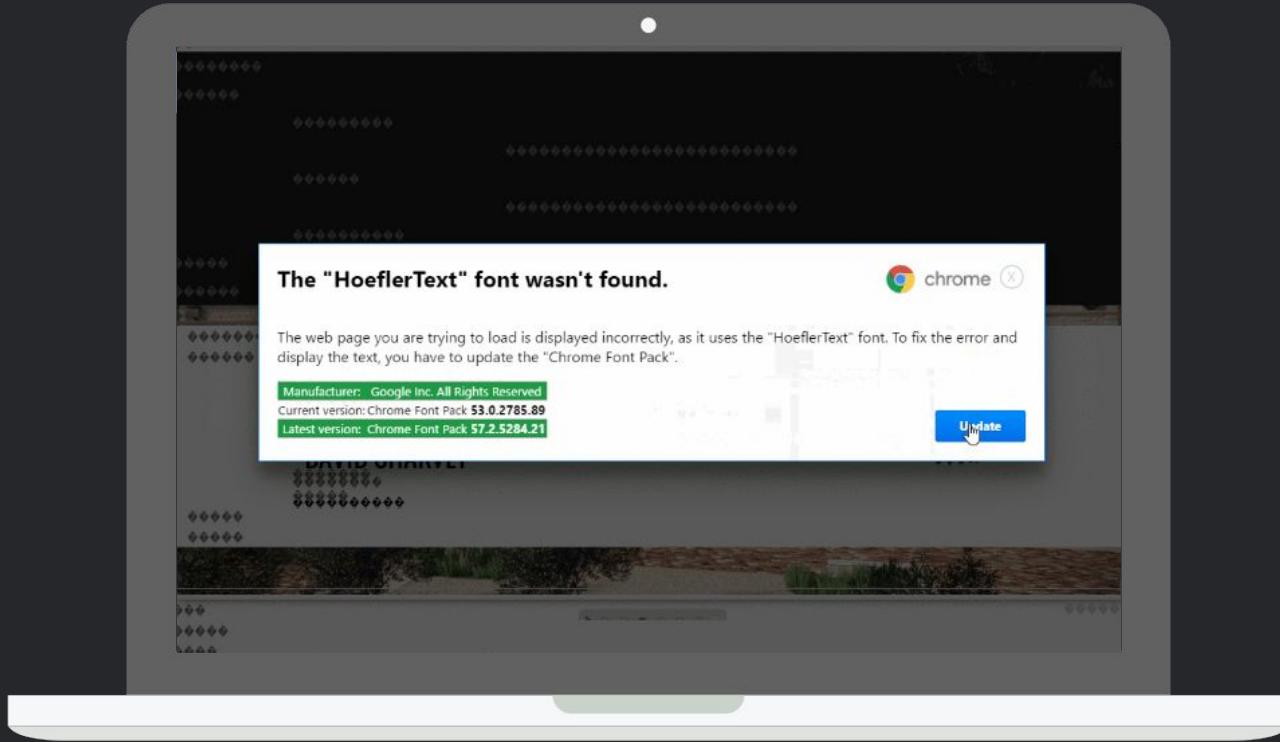
New York  
University



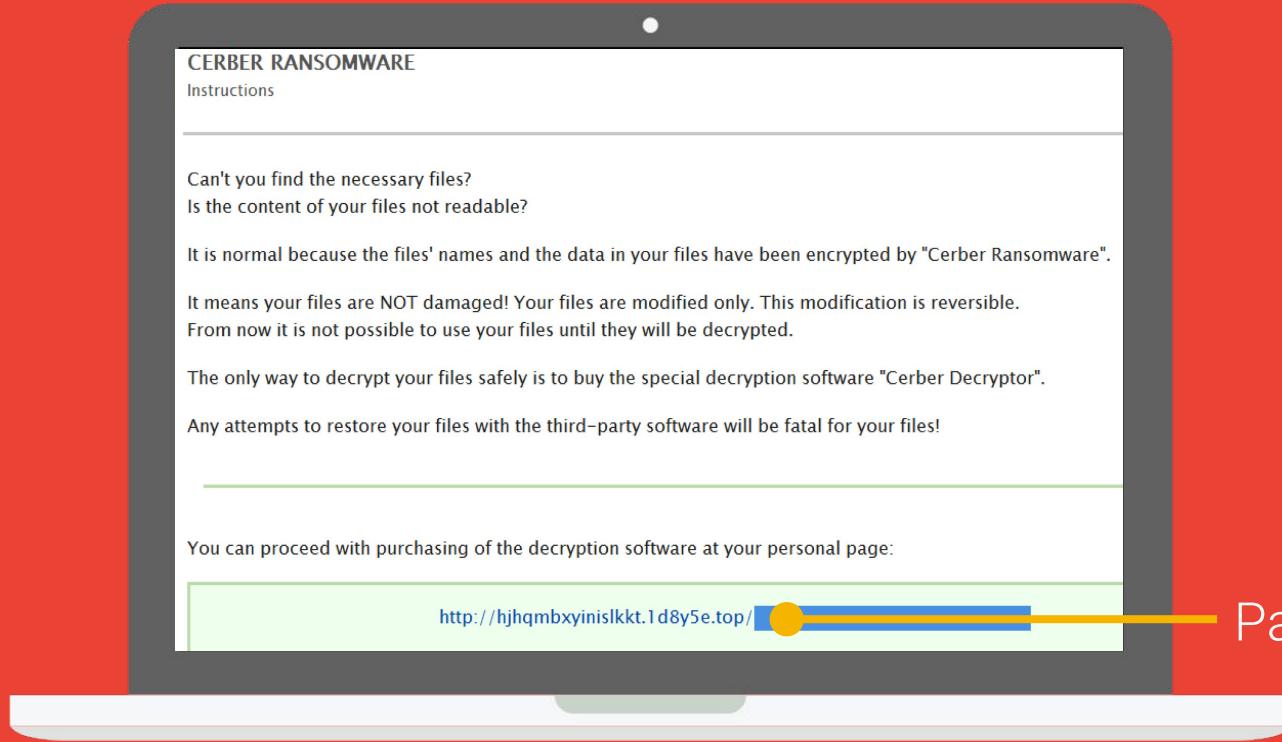
---

Life of a ransomware infection

---

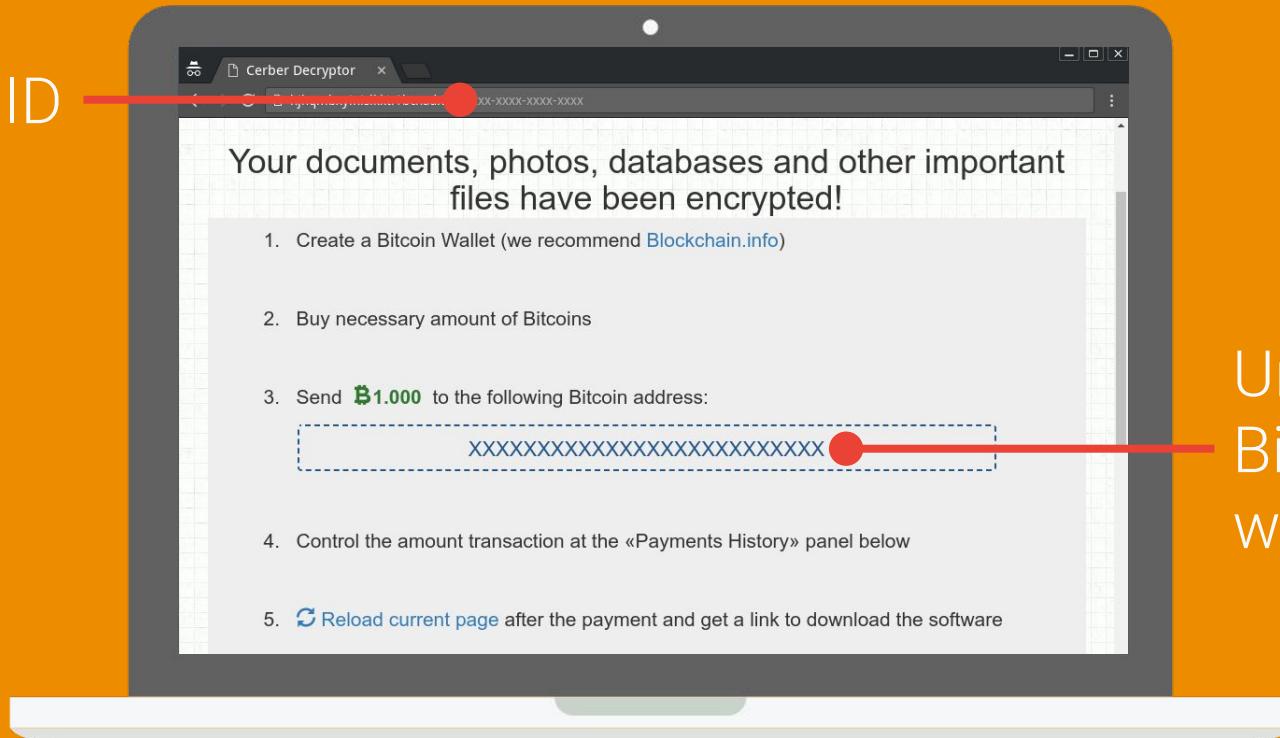


Victim gets infected



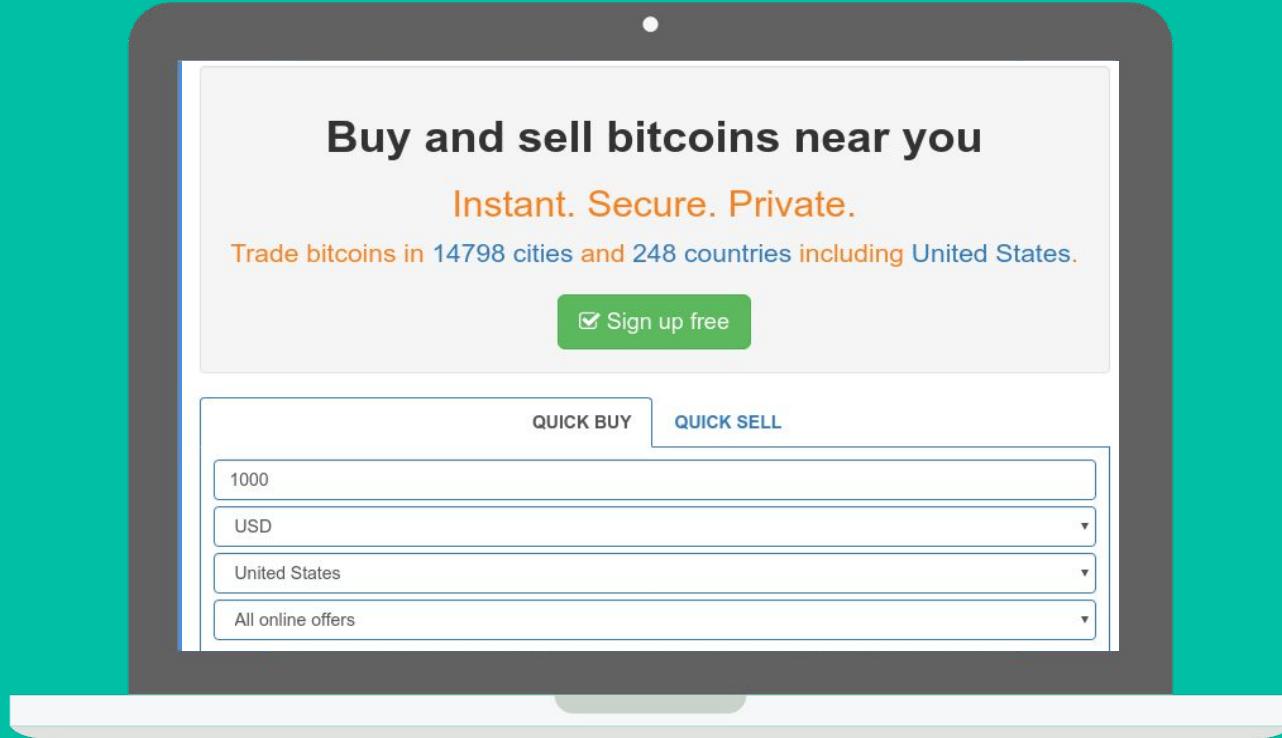
Victim is shown **ransom note**

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

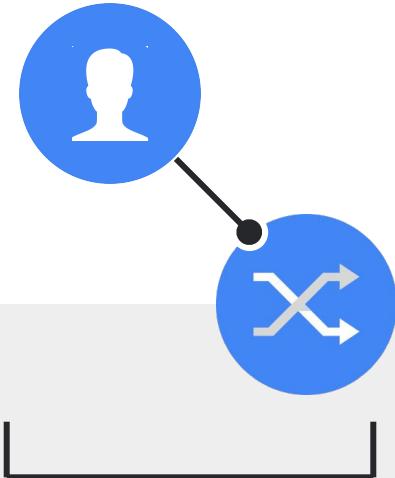
## Fungible

Bitcoins are easily converted into cash

# Bitcoin transactions are public

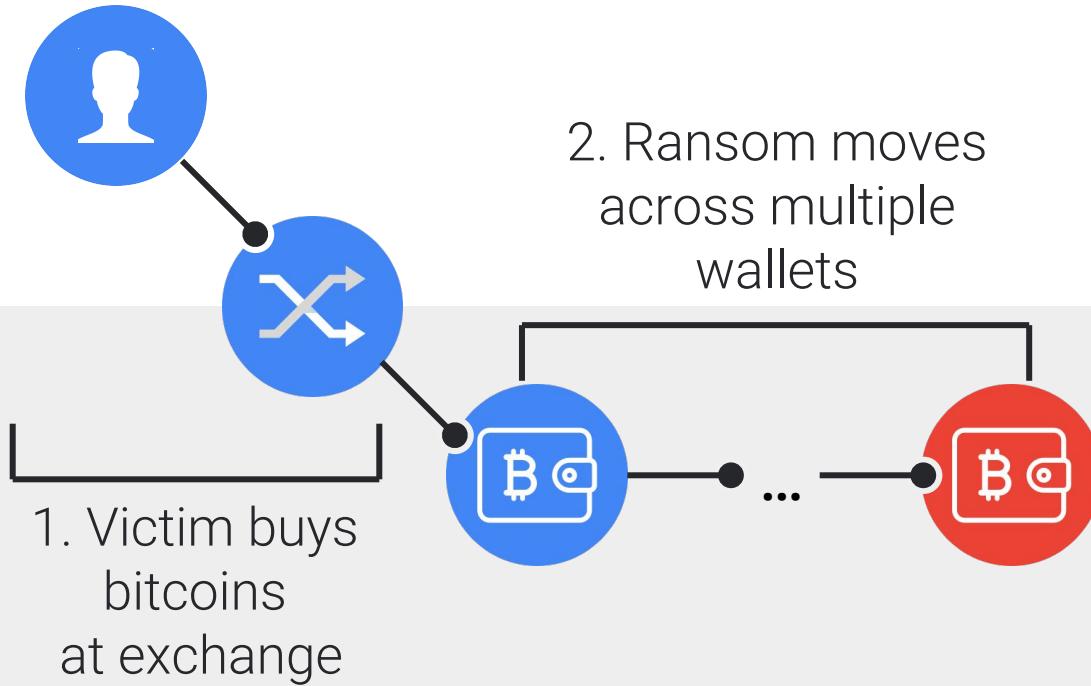


# Life of a ransom payment

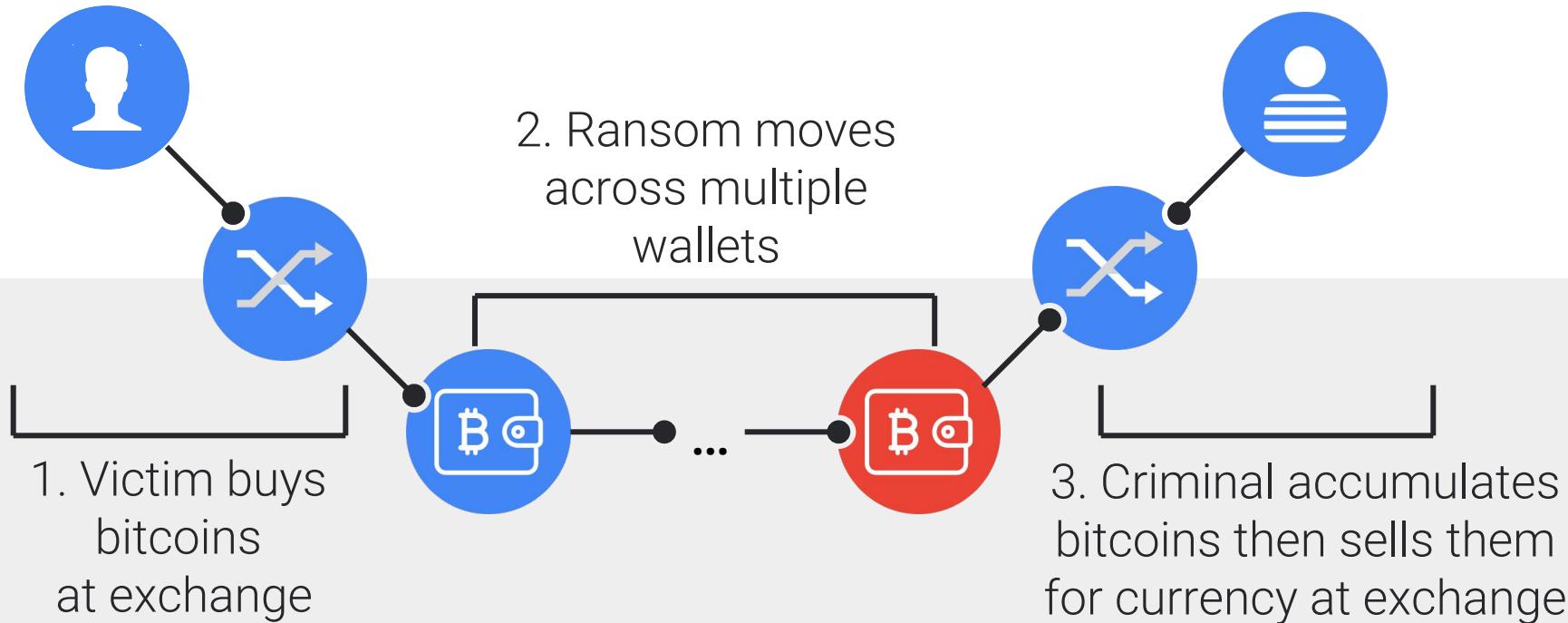


1. Victim buys bitcoins at exchange

# Life of a ransom payment



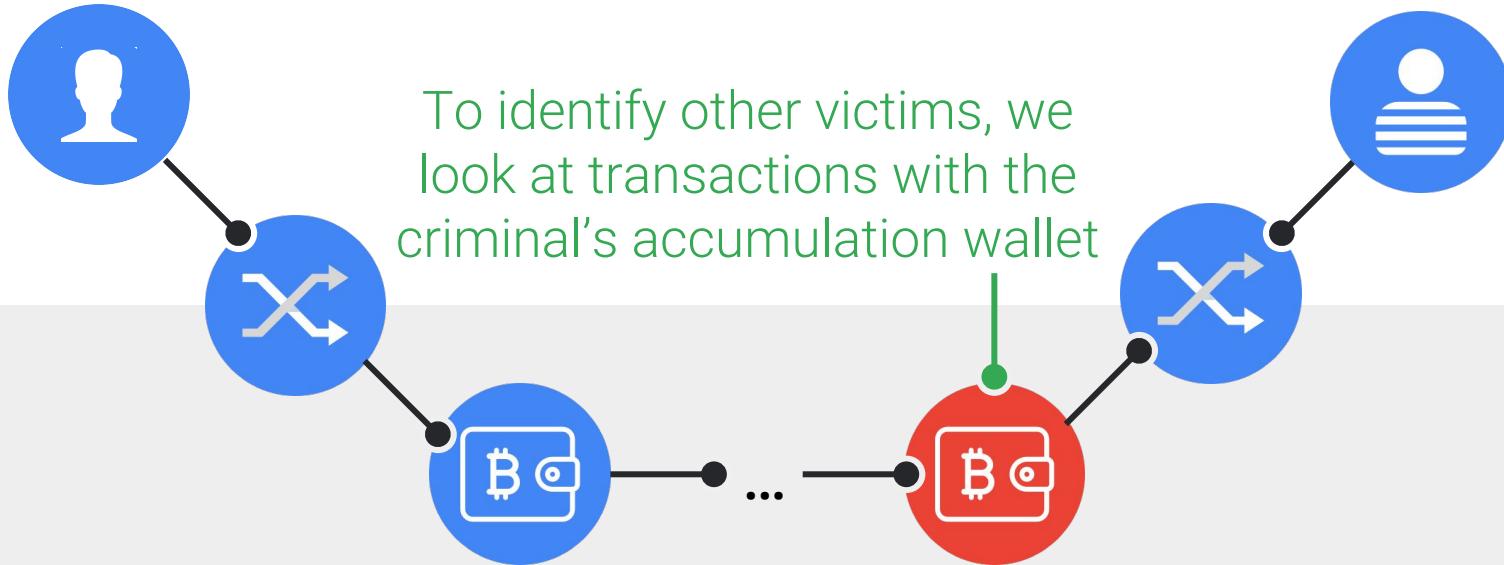
# Life of a ransom payment



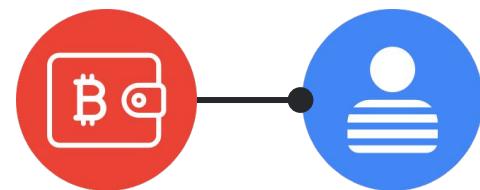
The background features abstract geometric shapes composed of blue lines and glowing blue dots, resembling molecular or network structures, set against a dark blue gradient.

# Measuring revenue

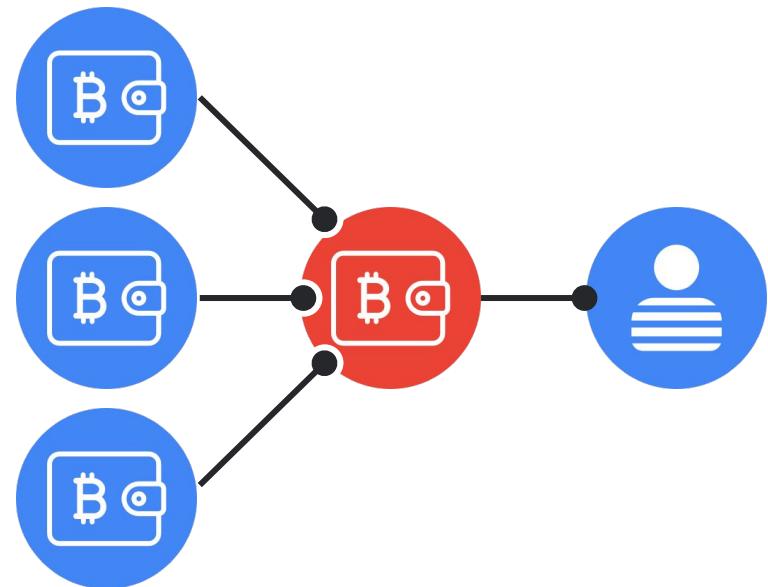
# Identifying victims



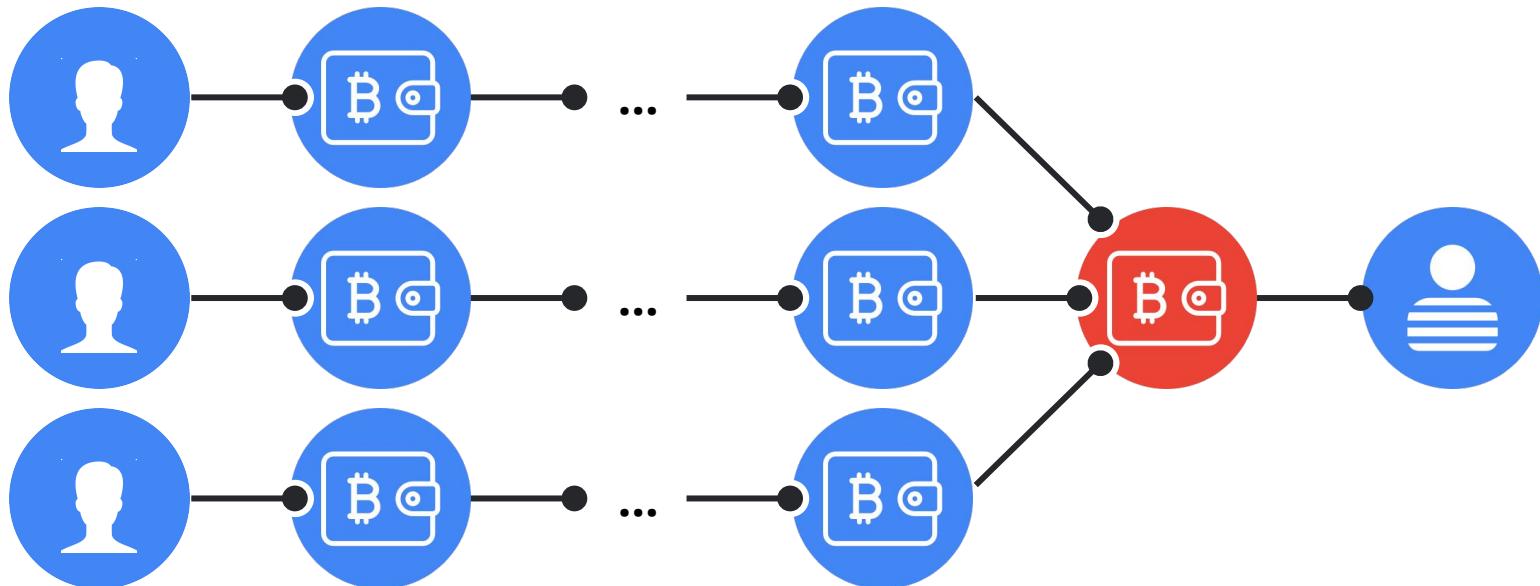
# Discovering payment network



# Discovering payment network



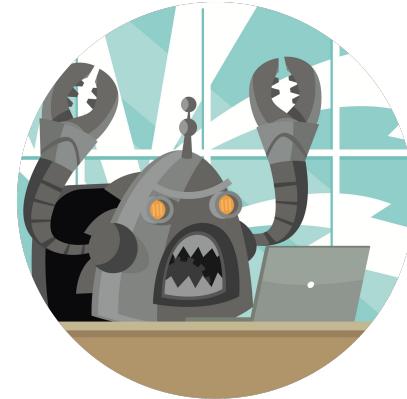
# Discovering payment network



# Gathering seed bitcoin transactions

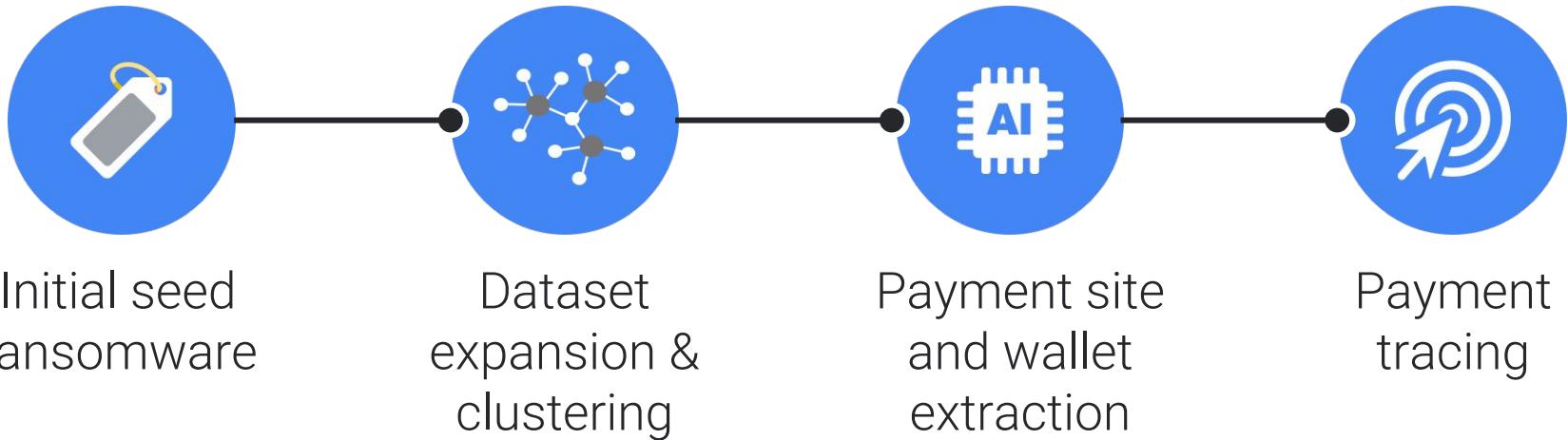


Victim reports



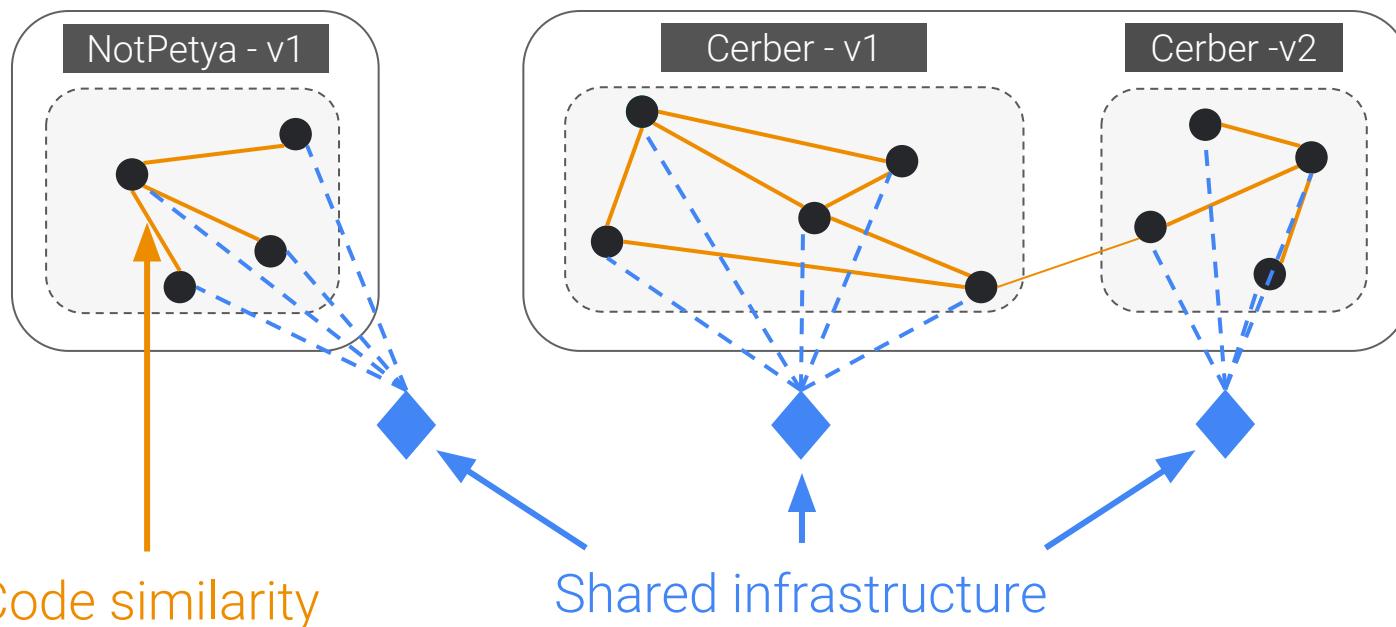
Synthetic “victims”

# Automating payment tracing



Initial dataset: 34 families, 154k binaries

# Using clustering for dataset expansion



# Expanded dataset 301,588 binaries

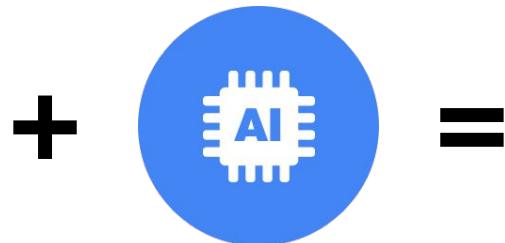
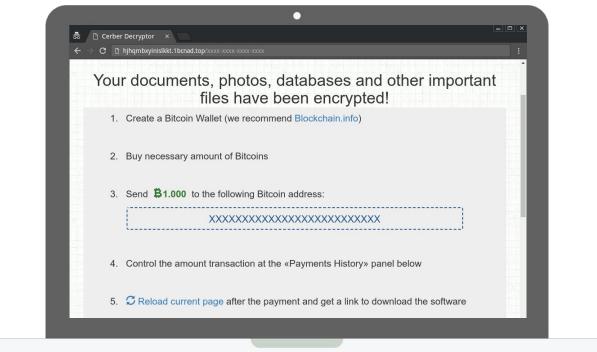
154,227

Seed dataset

147,361

Additional binaries

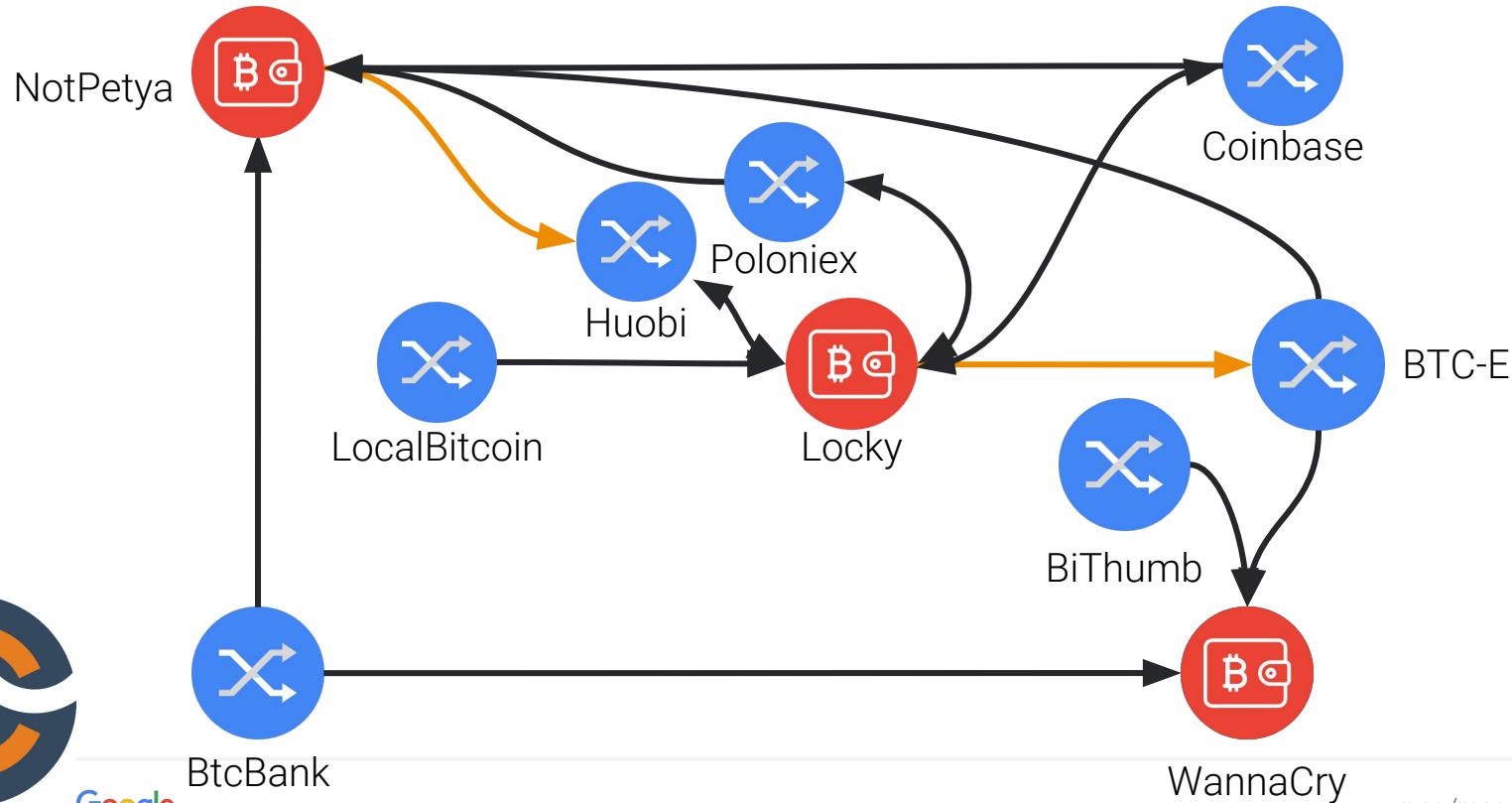
# Automatically identifying payment sites at scale



**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



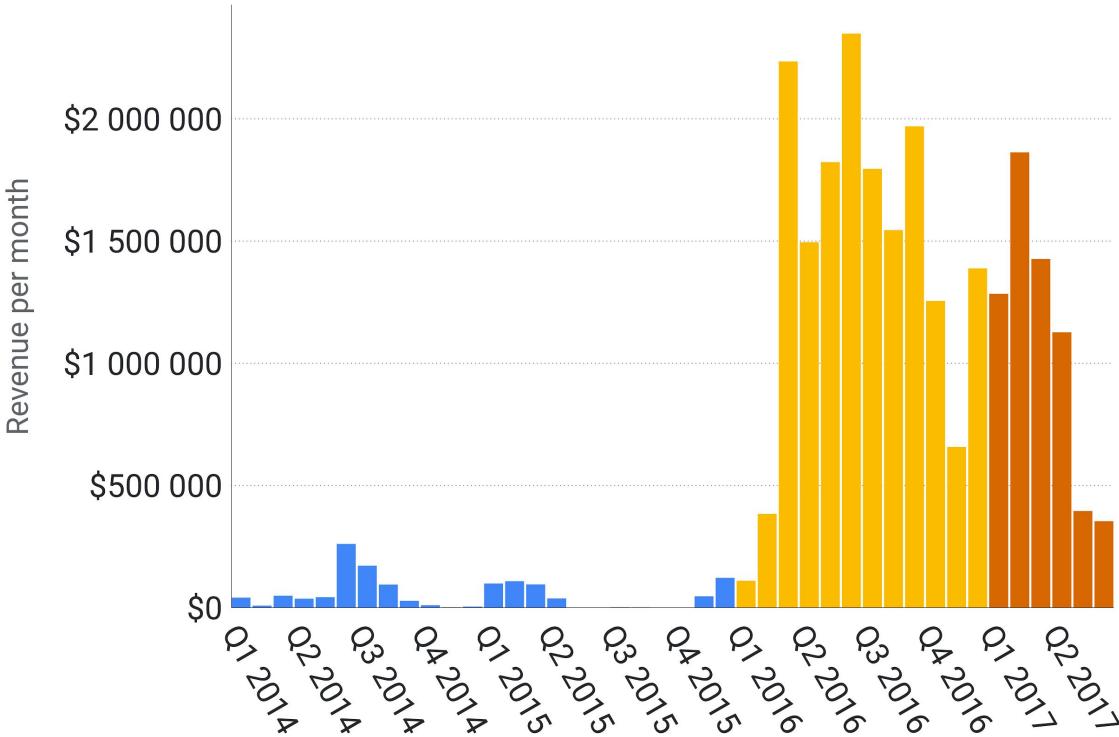
BtcBank

[g.co/research/protect](https://g.co/research/protect)

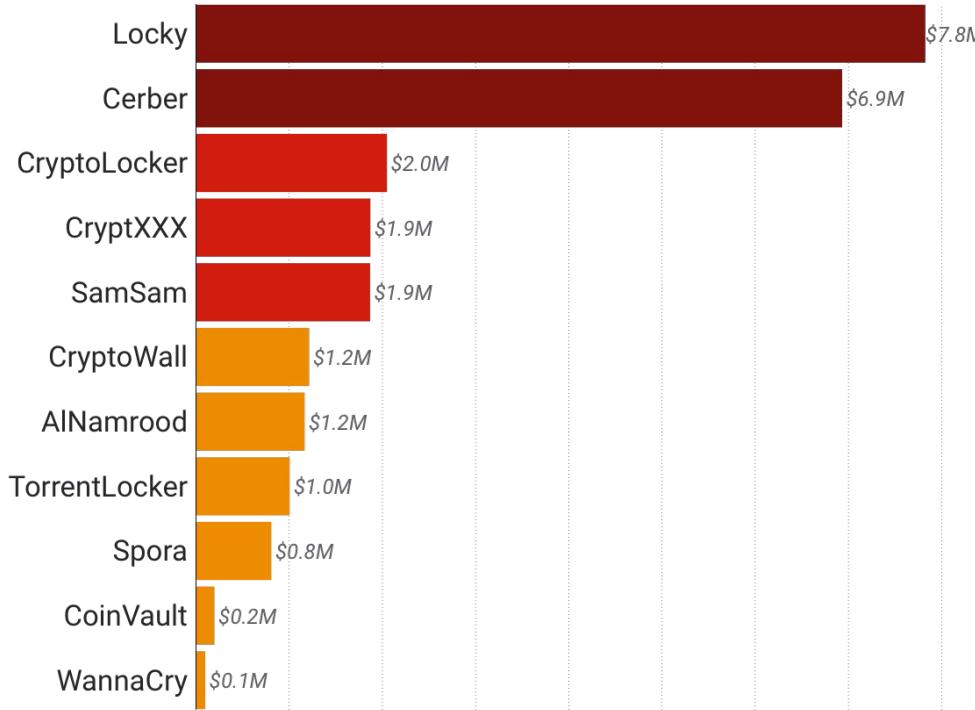
# Market insights

# \$25,253,505

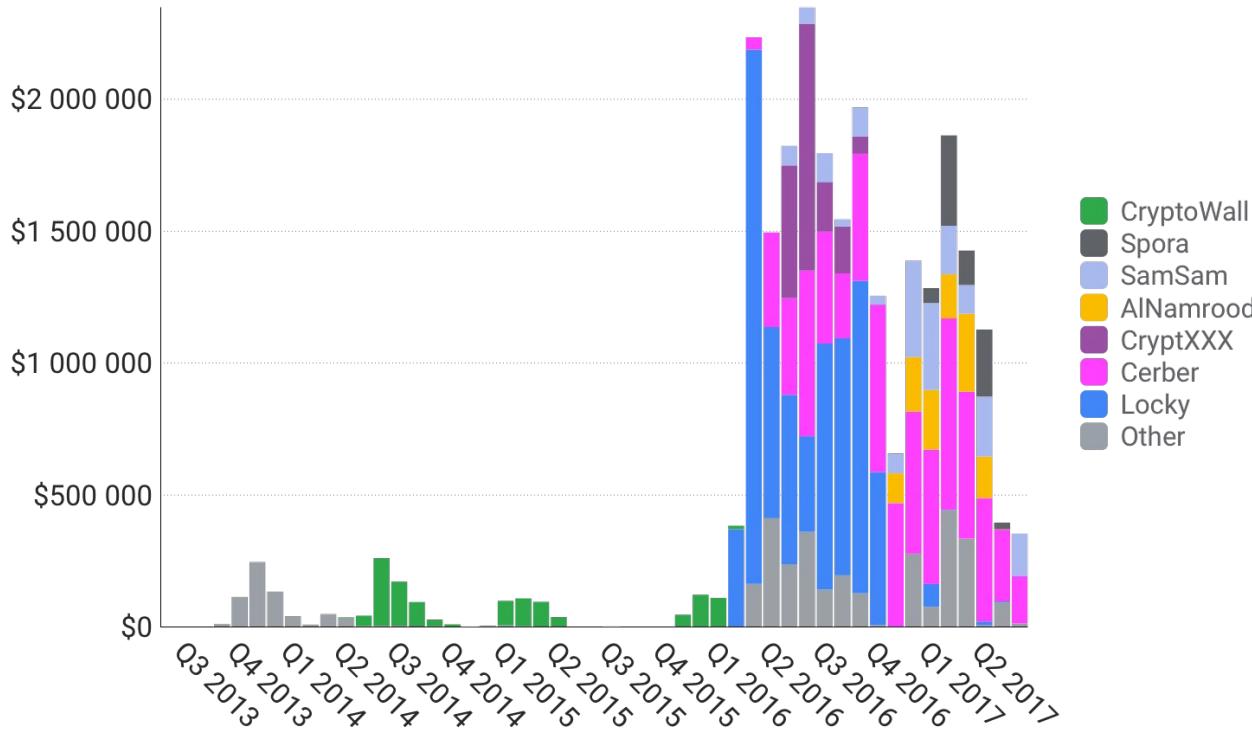




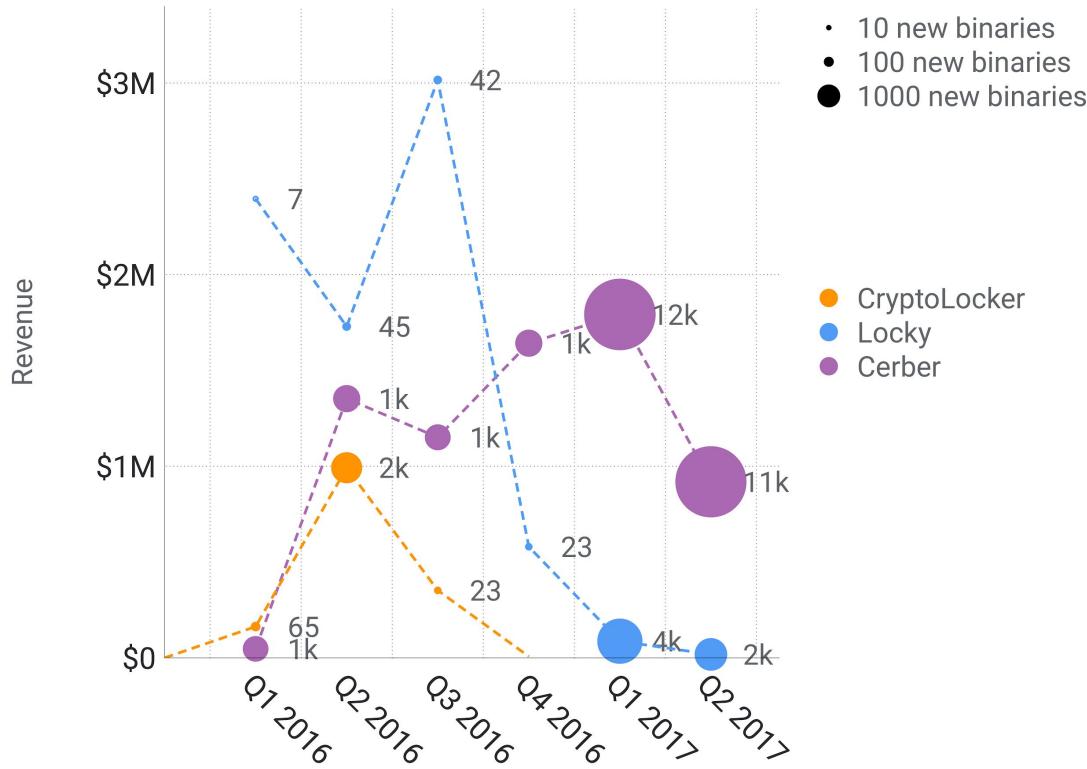
In 2016 ransomware became a multi-million \$ business



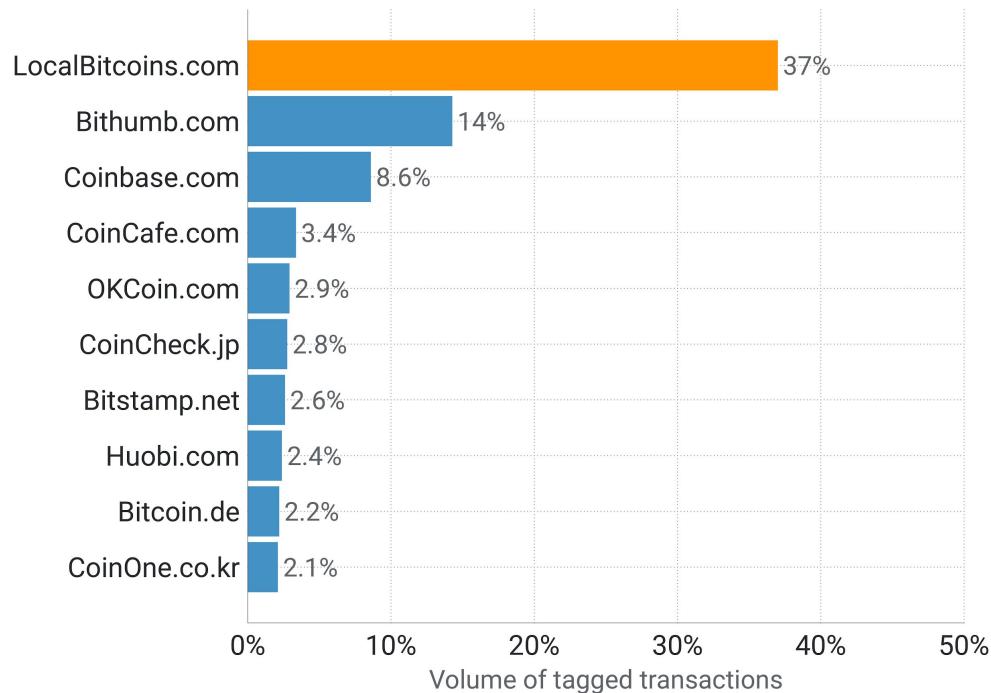
The ecosystem is dominated by a few kingpins



A fast changing market



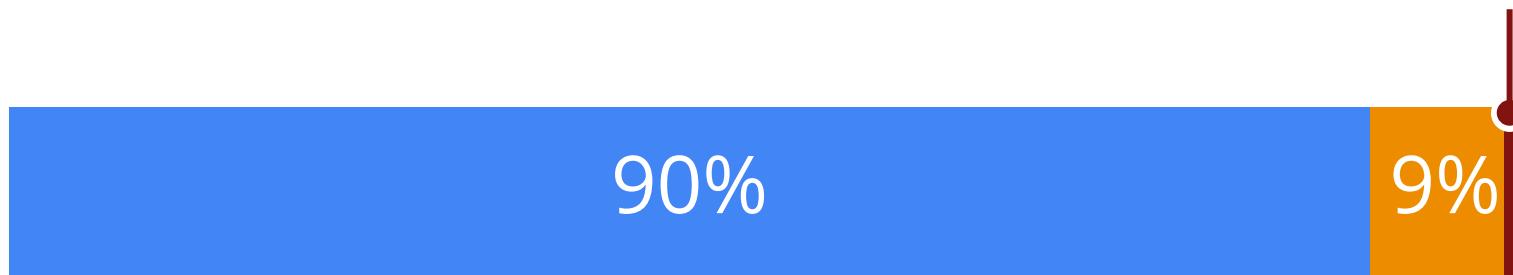
In 2017 ransomware increased binary diversity to evade AVs



The screenshot shows the LocalBitcoins.com homepage. At the top, the logo and navigation menu are visible. Below, a main banner features the text "Buy and sell bitcoins near you" and "Instant. Secure. Private." in bold. It also mentions "Trade bitcoins in 14815 cities and 248 countries including United States." A green "Sign up free" button with a checkmark is prominently displayed. Below the banner, there's a form with fields for "Amount", "USD", and "United States". Two buttons, "QUICK BUY" and "QUICK SELL", are shown above the form.

Many victims buy Bitcoins through the “Craigslist of Bitcoin”

# Victim payments



Paid the ransom in a single transaction

Did not account for transaction fees

# 95%

traced ransoms cashed out  
via BTC-E

Cashout list available on request

Last Price: **1072.532 USD** Low: **1040 USD** High: **1270 USD**  
Volume: **14324 BTC / 17073828 USD** Server Time: **11.03.17 00:23**

E-Mail  
Password  
Login | Sign up | Lost password

Trade Bitcoin Betting News PAMM Support

Latest news:

**25/02/17** CloudFlare parser bug 0  
**10/02/17** Bitcoin Betting 0

BTC/USD 1072.537 BTC/RUR 65192.9184 BTC/EUR 0.03000001 LTC/BTC 0.00346 LTC/USD 3.6949 LTC/RUR 215.80888 LTC/EUR 3.563 NMC/BTC 0.000928 NMC/USD 0.307 NMC/BTC 0.000811

NVC/USD 0.882 USD/RUR 58.6727 EUR/USD 1.39325 EUR/RUR 66.36619 PPC/BTC 0.00035 PPC/USD 0.38 DSH/BTC 0.94337 DSH/USD 46.69385 DSH/RUR 272.795 DSH/EUR 45.469

DSH/LTC 12.773 DSH/ETH 2.658 ETH/BTC 0.01648 ETH/USD 17.63572 ETH/EUR 17.02182 ETH/LTC 4.66367 ETH/RUR 1029.46589



Buy BTC Your balance: **0 USD** Lowest ask Price **1083.732 USD**

Amount BTC:  Price per BTC:  USD Total: **0 USD** Fee: **0 BTC**

Click to sum your order.

Calculate Buy BTC

Sell BTC Your balance: **0 BTC** Highest Bid Price **1081.91 USD**

Amount BTC:  Price per BTC:  USD Total: **0 USD** Fee: **0 USD**

Click to sum your order.

Calculate Sell BTC

Buy orders Total: 11594947.37 USD

price	BTC	USD
1081.91	11.48659612	12427.46320818
1080.088	1.56420284	1689.47671704

Sell orders Total: 2743.42 BTC

price	BTC	USD
1083.732	0.00139195	1.50850075
1083.733	0.011837	12.82814752

Tweets by @btcacom

BTC-E @btcacom Tor browser login problem goo.gl/FqGwi btc...

xBTCE @xbtce\_info Desktop Terminal released @ xBTCE!

Embed View on Twitter

# Ransomware notable actors



# Locky

*Bringing ransoms to  
the masses*



International Business Times



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



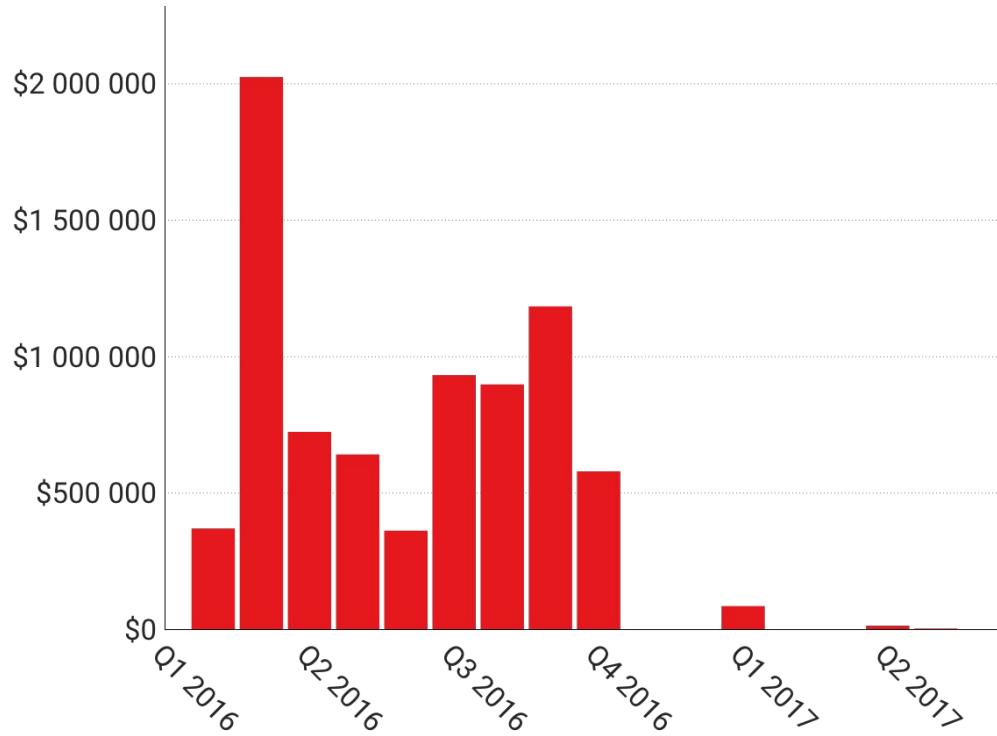
Security experts have warned that 'Locky' is quickly evolving into an effective piece of ransomware (iStock)



## Locky ransomware is back, this time via Necurs

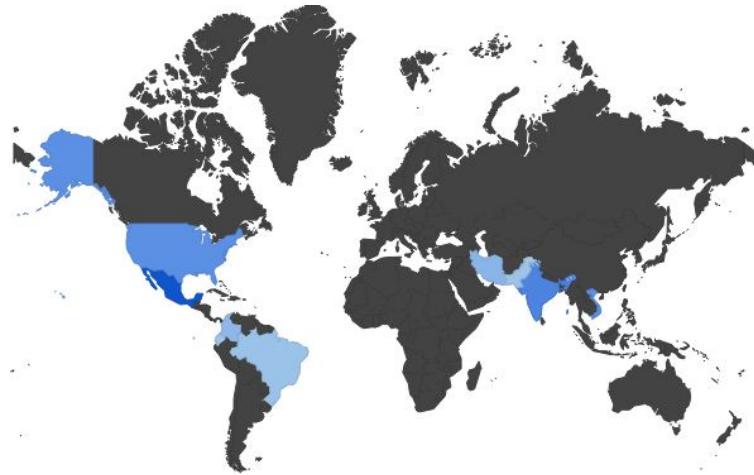


## The godfather of ransomware returns: Locky is back and sneakier than ever

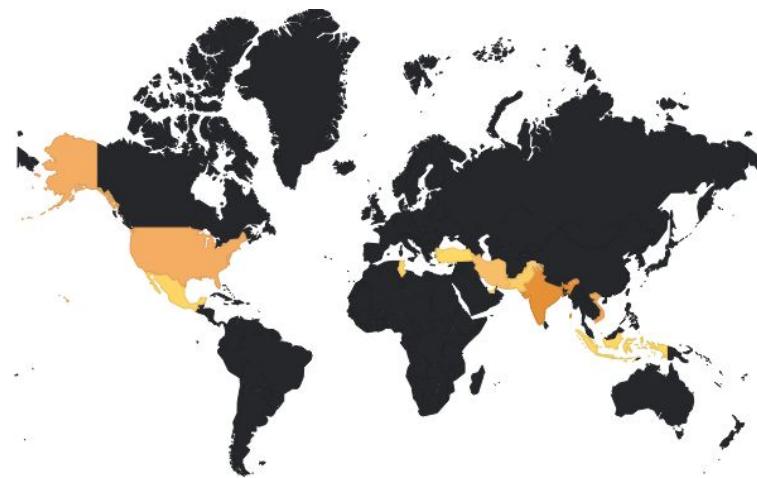


The first ransomware to make >\$1M per month

# 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*

A DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

**Security**

**Cerber surpasses Locky to become dominant ransomware menace**

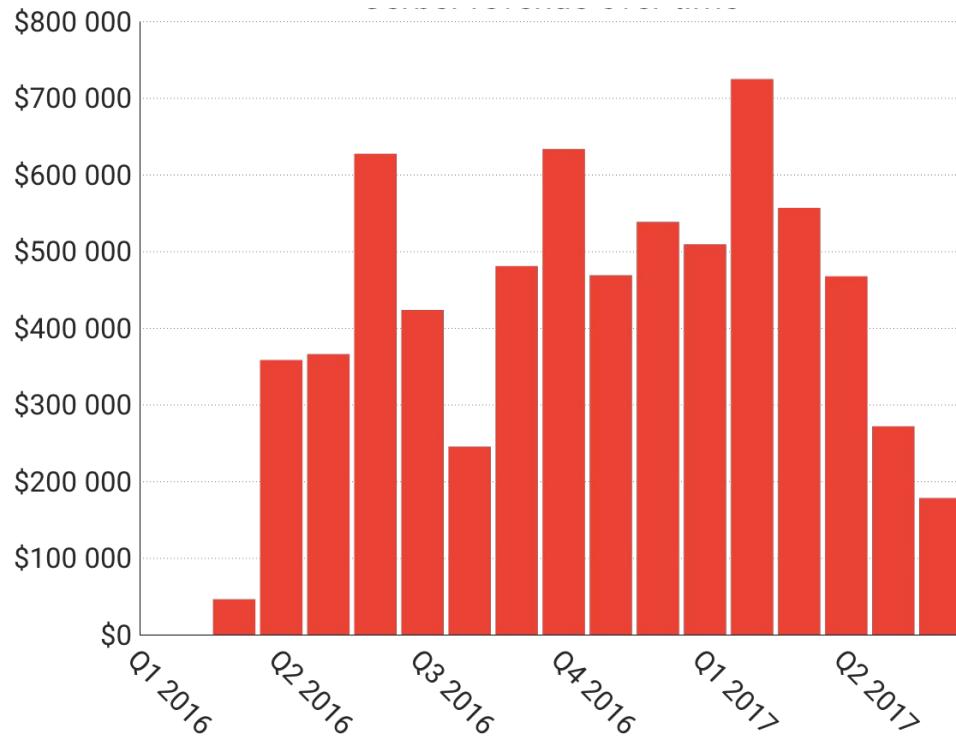
Ransomware-as-a-Service is a hit with the tech illiterate

By John Leyden 13 Apr 2017 at 16:30

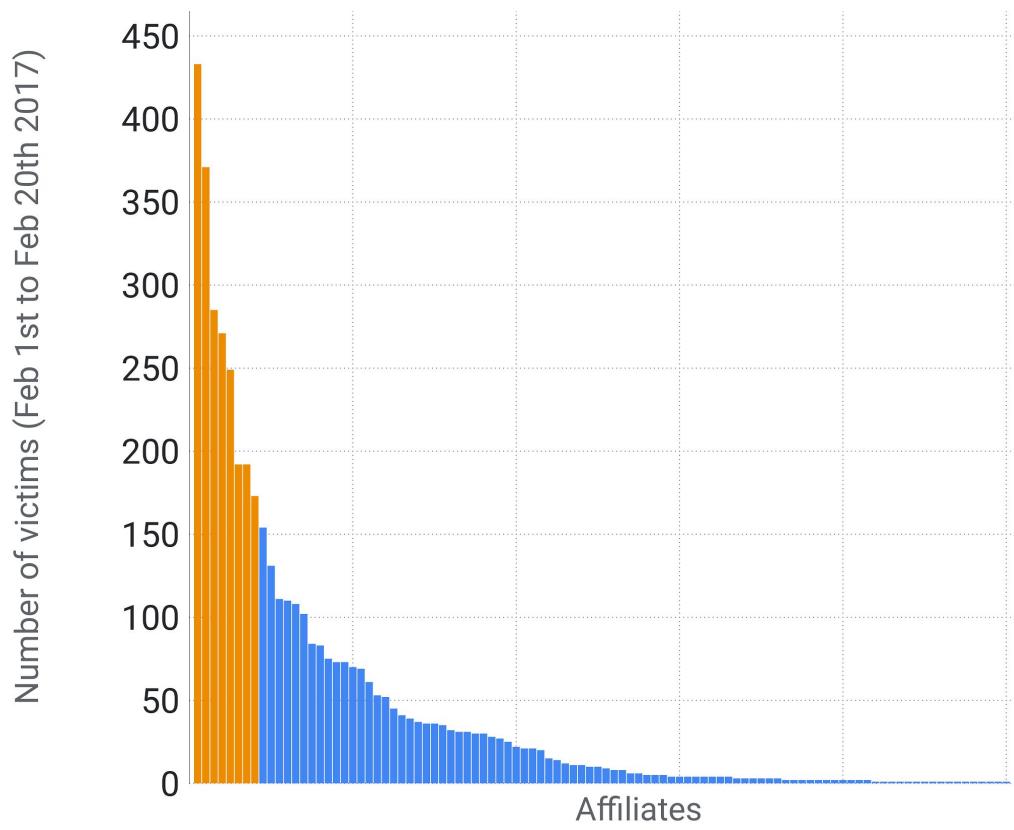
SHARE ▾



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



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





1AzkuxChzM**B**4[...]

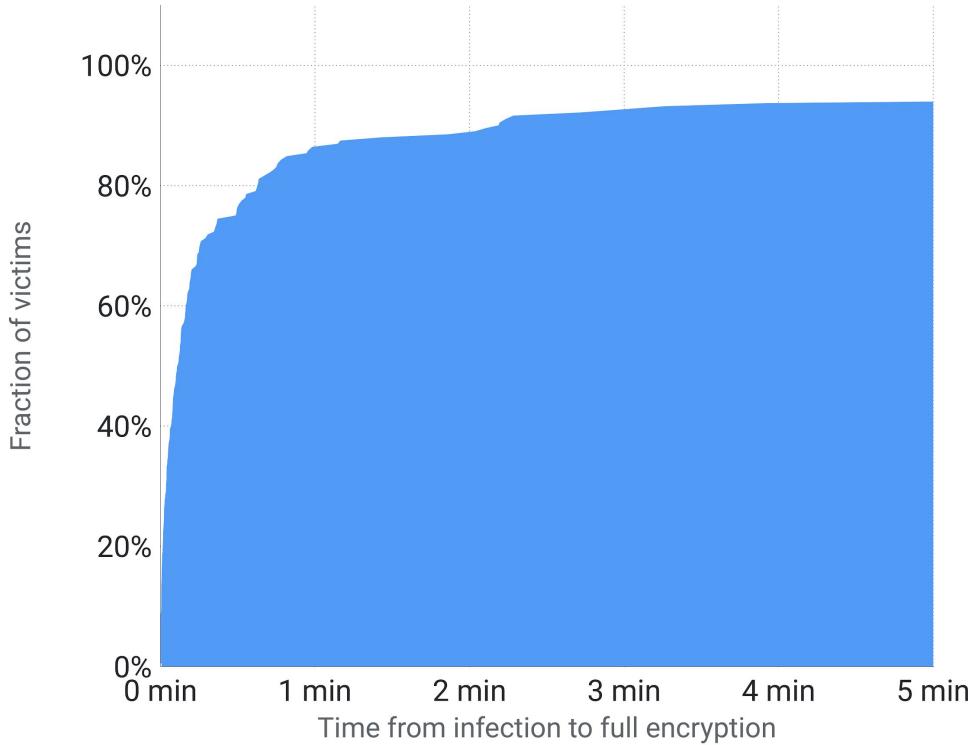


1Azkux.**top**

## 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

A close-up photograph of a highly ornate Venetian-style mask. The mask is primarily light blue with intricate gold-colored patterns and designs. It features a large, detailed lion's head at the top of the strap. Small silver bells hang from the strap. The mask is set against a dark, textured background.

# Spora

*Ransomware business  
model refined*

ID: Redacted

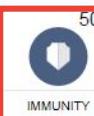
Balance: 0.00 USD Refill Exit Language

### 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*



Recycle Bin



Acrobat Reader DC



Google Chrome



Mozilla Firefox

Ooop  
If you see  
then your  
it from yo  
@WanaDec...

If you nee  
Please fin  
any folder

Run and fo



Test Mode  
Windows 7  
Build 7601

3:01 PM  
5/15/2017



▶ 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



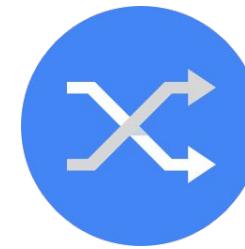
56 BTC

revenue



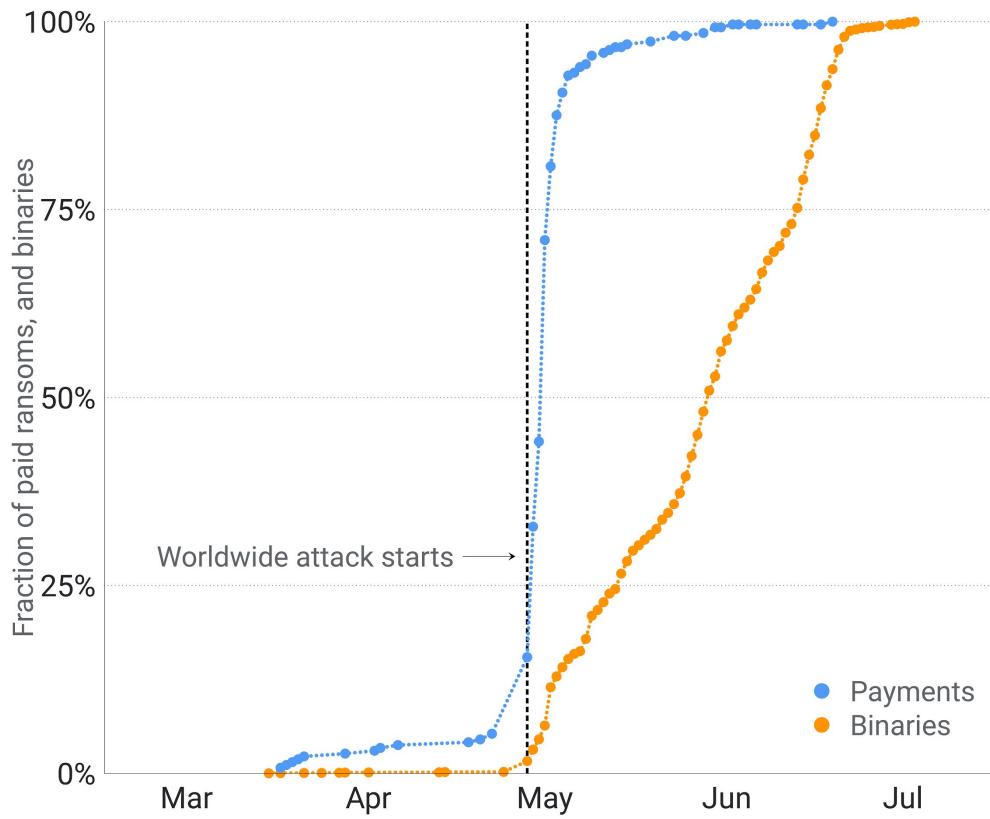
5

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:

1Mz7153HMuXTuR2R1t78hGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

BSENmb-CPccj7-SwaiAC-9UP1eg-KA3Hyw-ND9fd8-sUq54i-TAxTS8-MZoaT6-6ABSBf

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

Key:

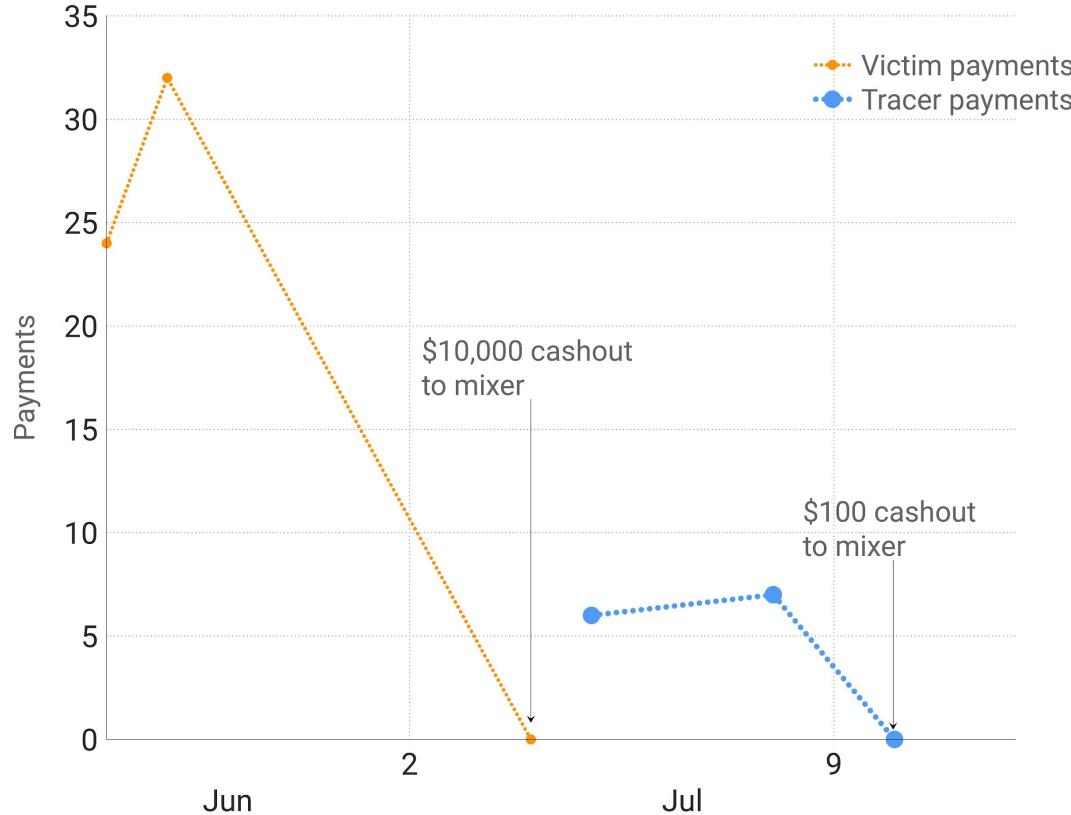
## Forbes

## 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

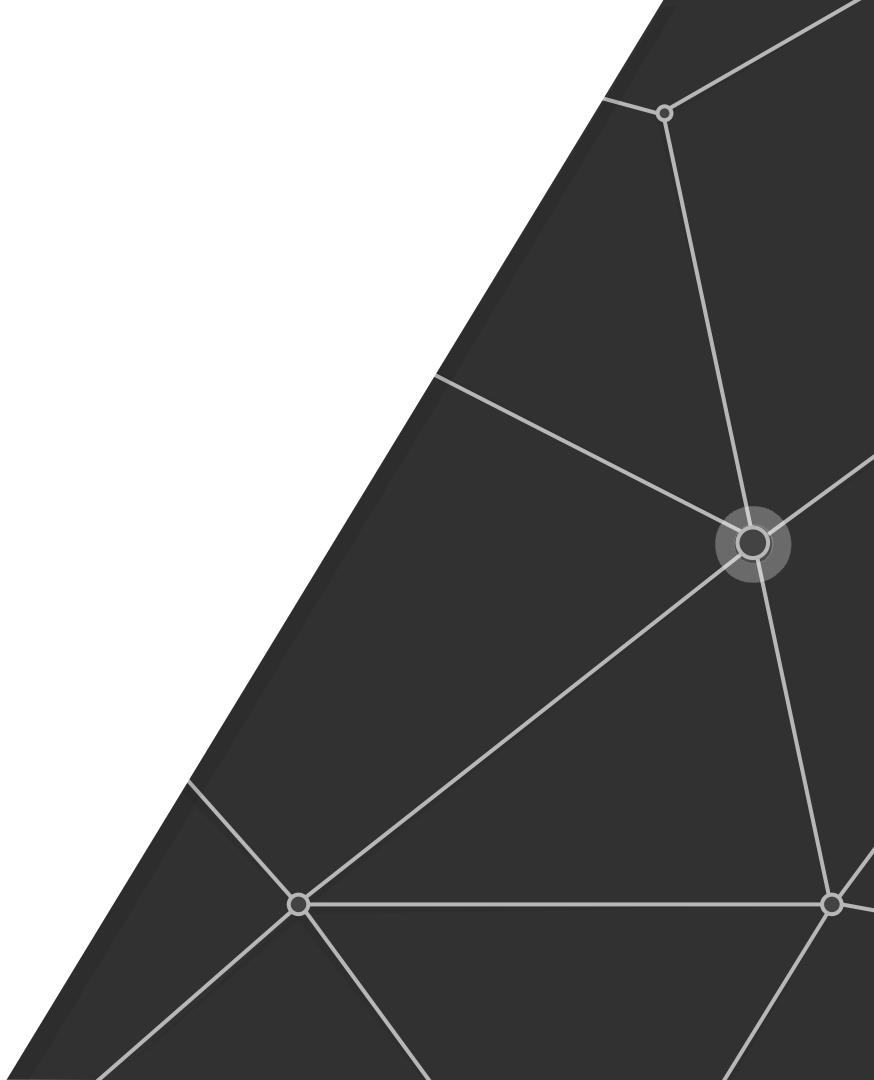
## Rise of the impostors

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



An abstract network graph is positioned on the left side of the slide. It consists of several nodes represented by small white circles and connecting edges shown as thin gray lines. One node in the center has a larger, semi-transparent gray circle centered on it, suggesting it is a hub or a point of focus.

Research at **Google**

# Thank you

[g.co/research/protect](https://g.co/research/protect)