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

Healthcare IT News TOPICS

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

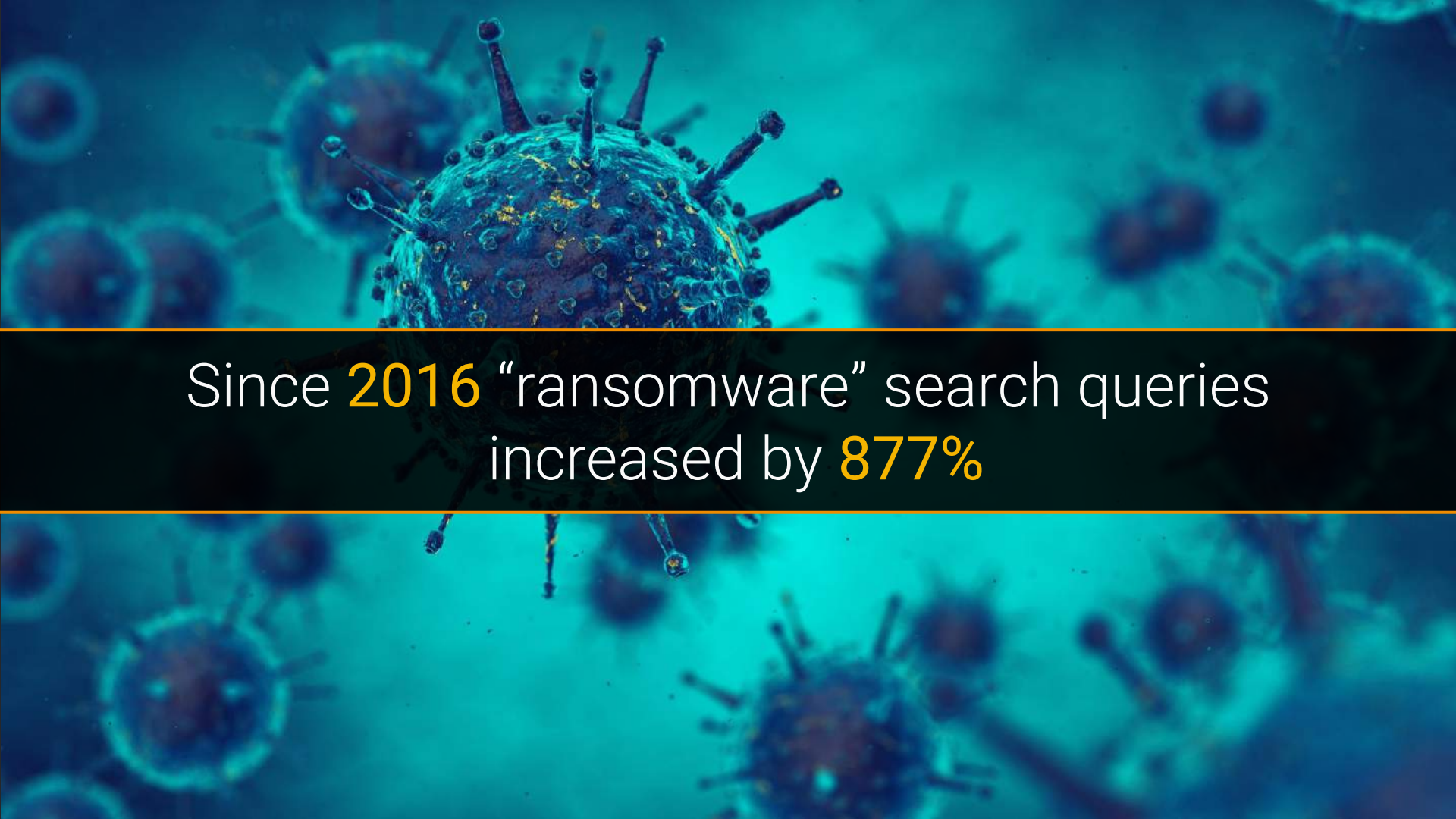
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

ARE YOU FEELING LOCKY? —

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

The Register®
Biting the hand that feeds IT

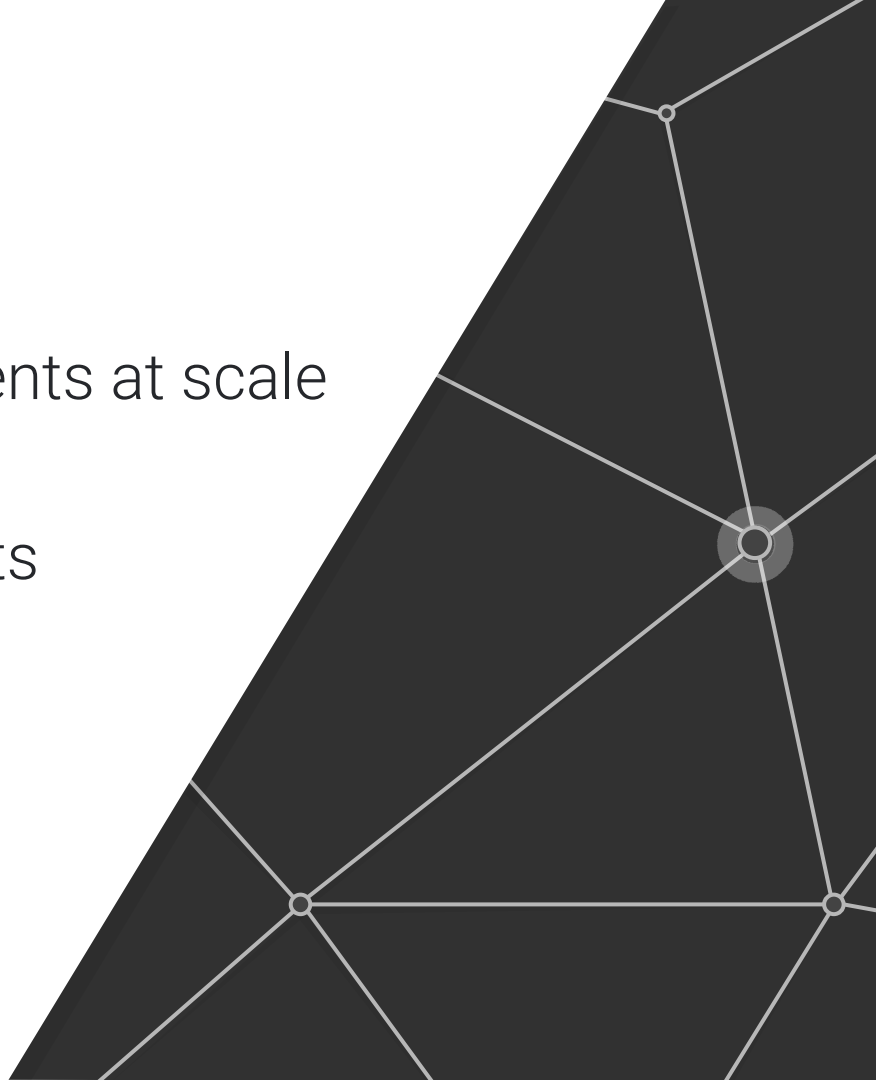
Unbreakable Locky ransomware is on the march again

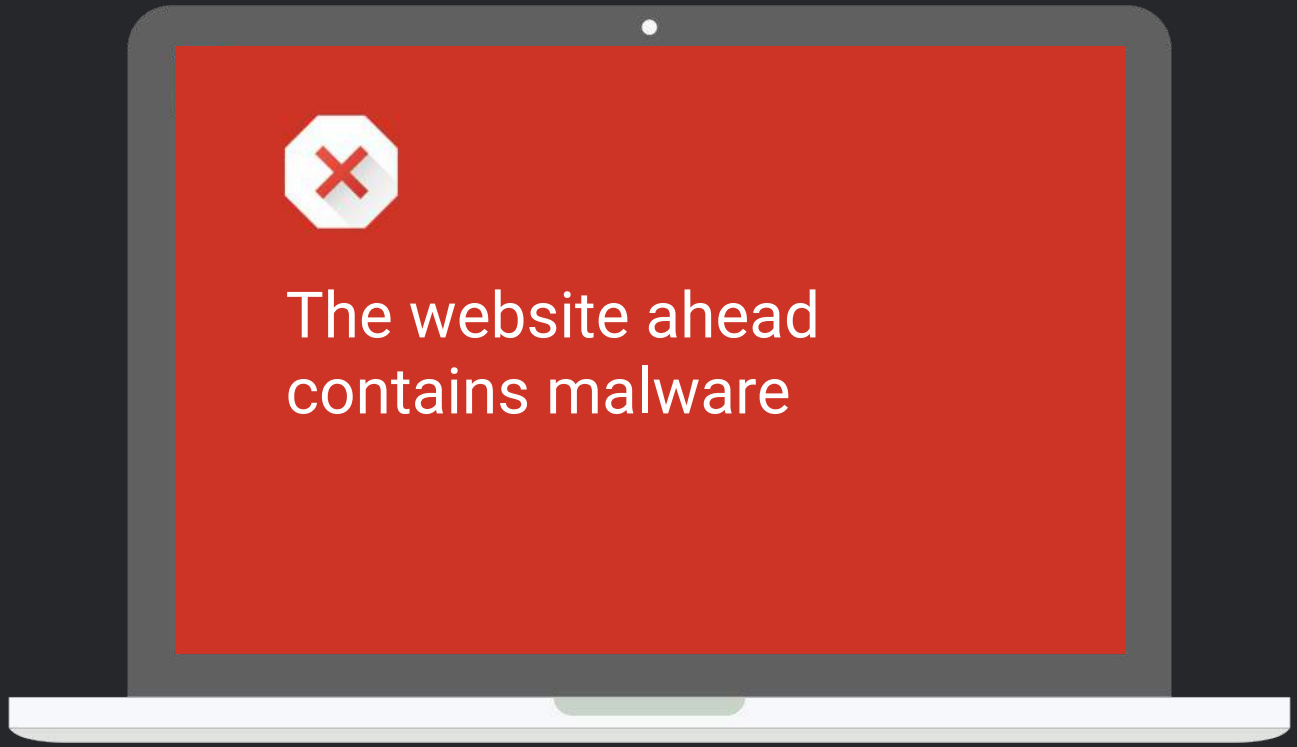

Since 2016 “ransomware” search queries
increased by 877%


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

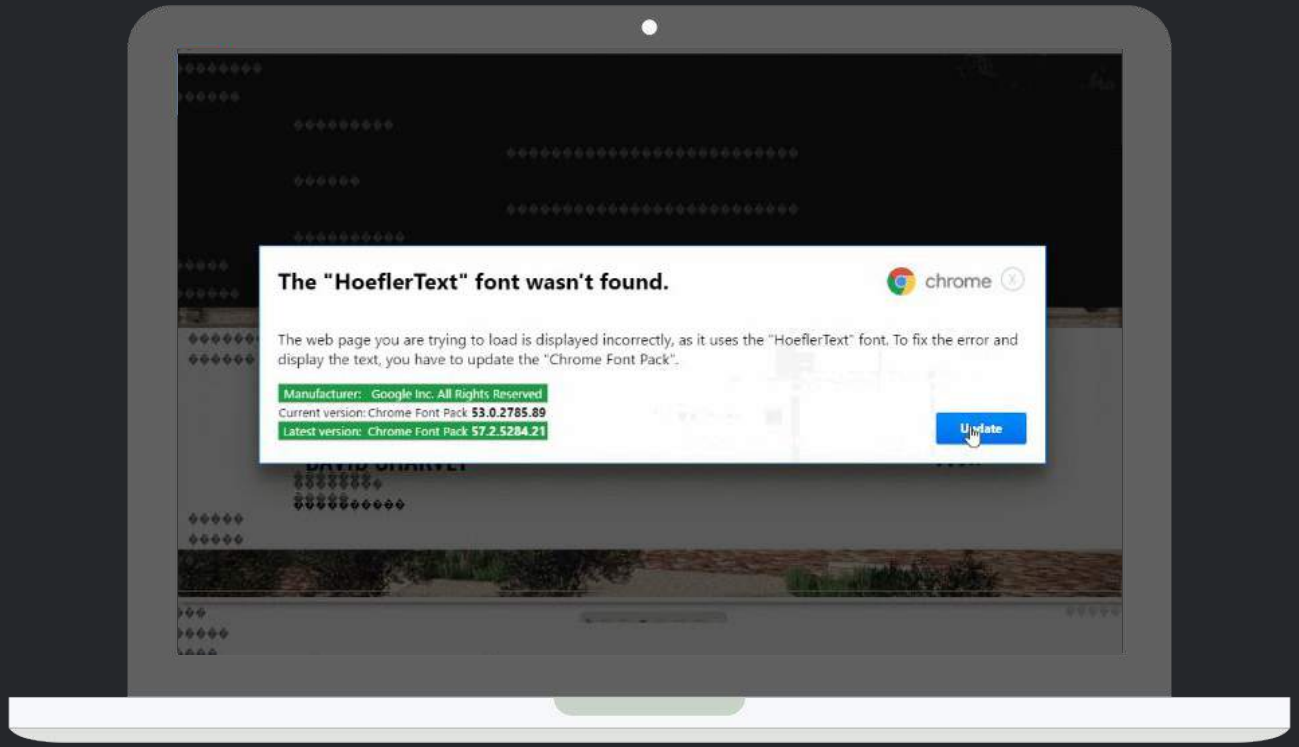
Google

Chainalysis

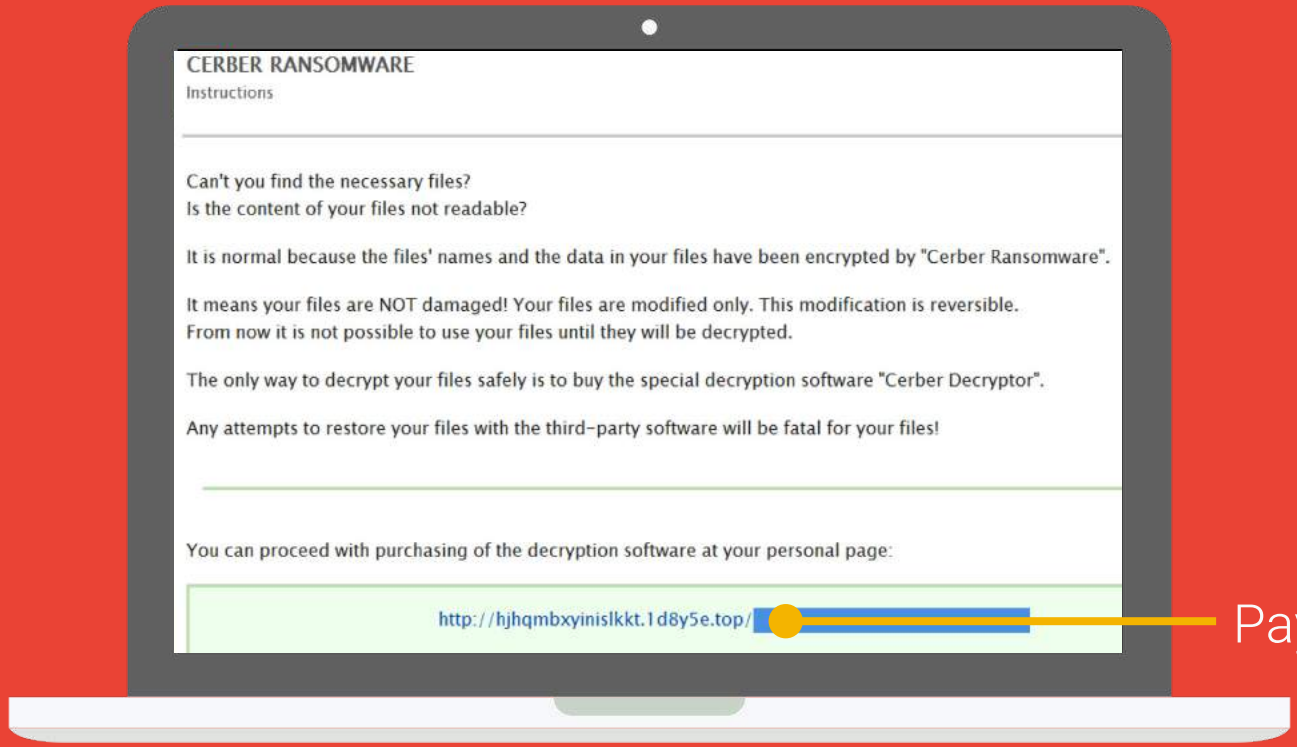
University of California, San Diego

New York University

Life of a ransomware infection

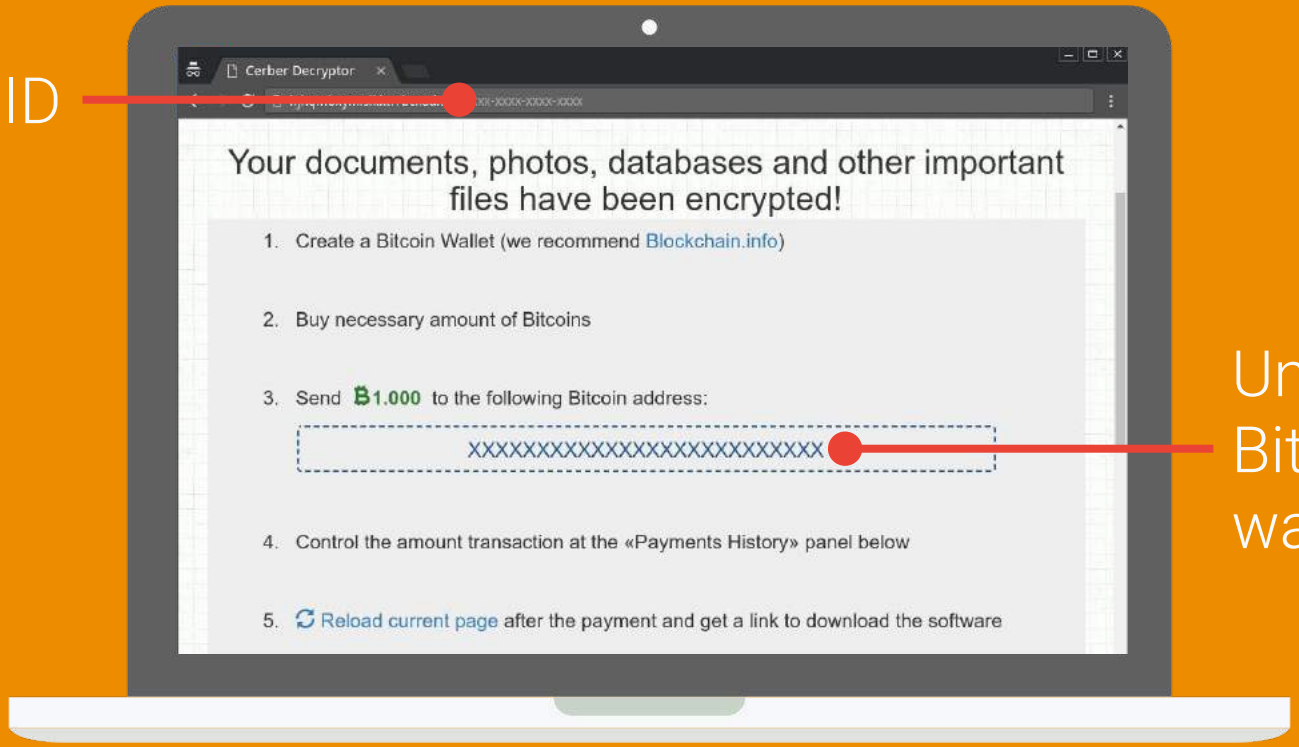


Victim gets infected



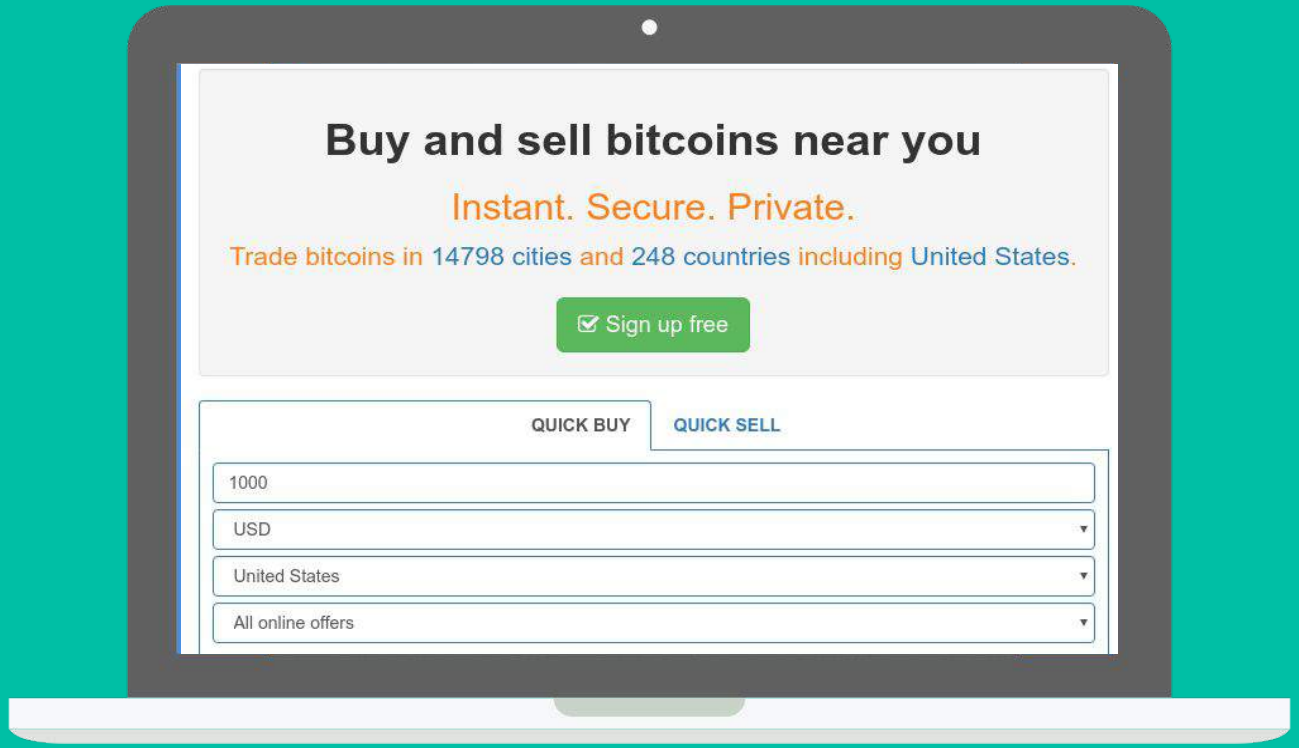
Victim is shown **ransom note**

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

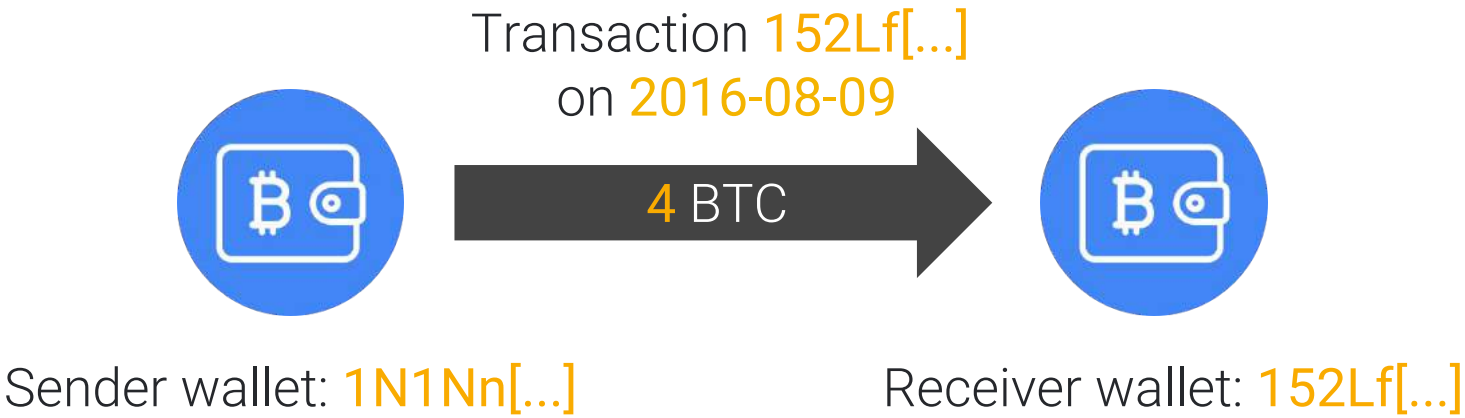
Irrefutable

Transactions can’t be reverted

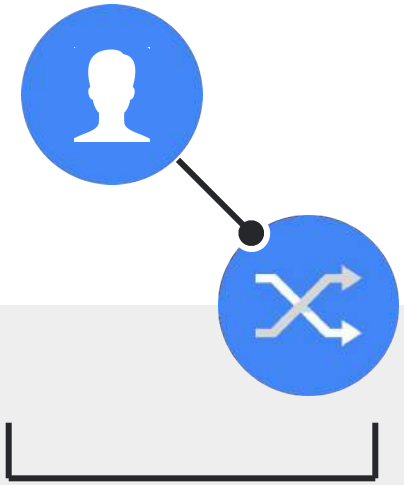
Fungible

Bitcoins are easily converted into cash

Bitcoin transactions are public

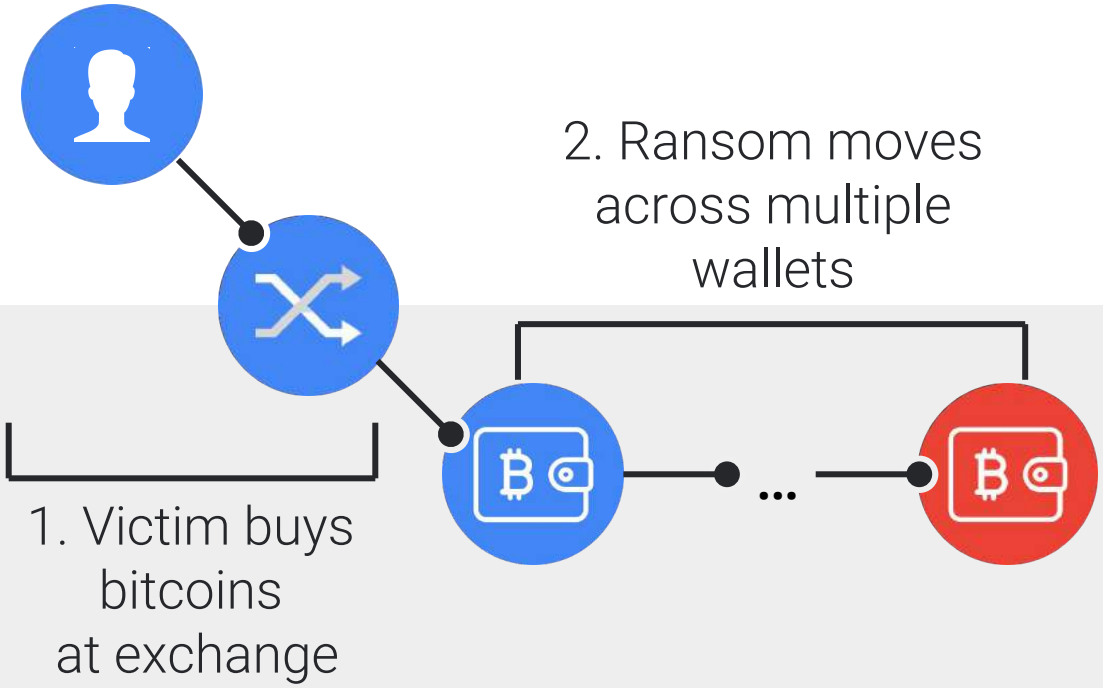


Life of a ransom payment

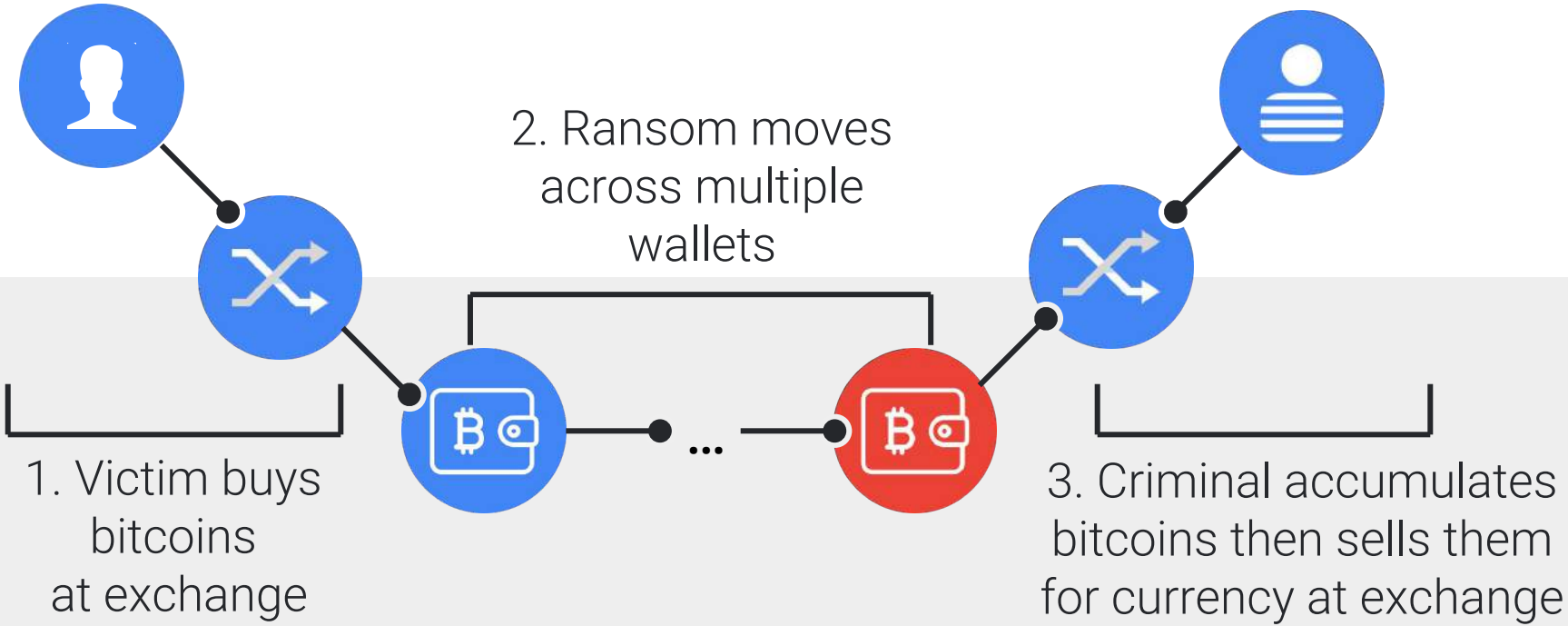


1. Victim buys bitcoins at exchange

Life of a ransom payment

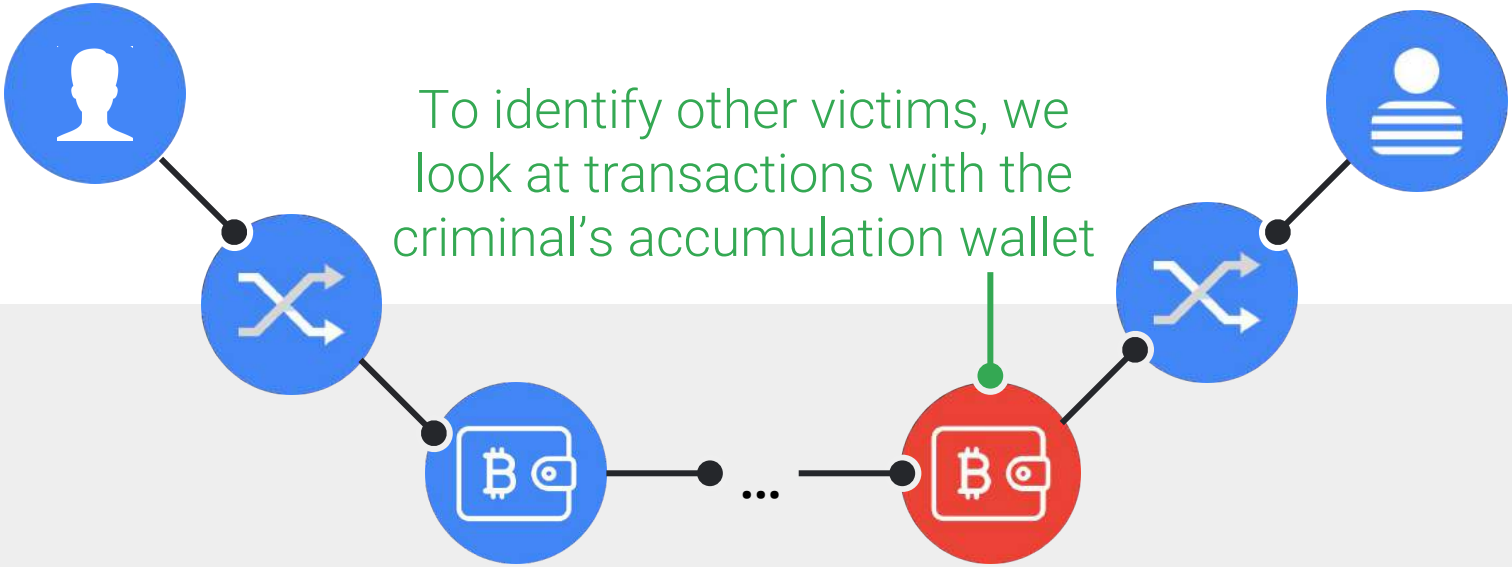


Life of a ransom payment

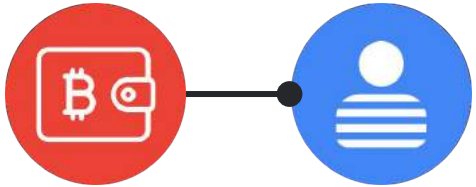


Measuring revenue

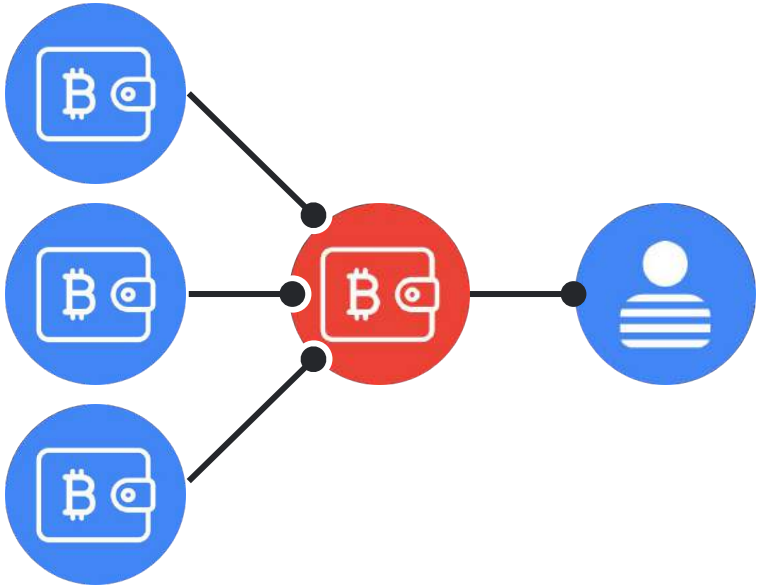
Identifying victims



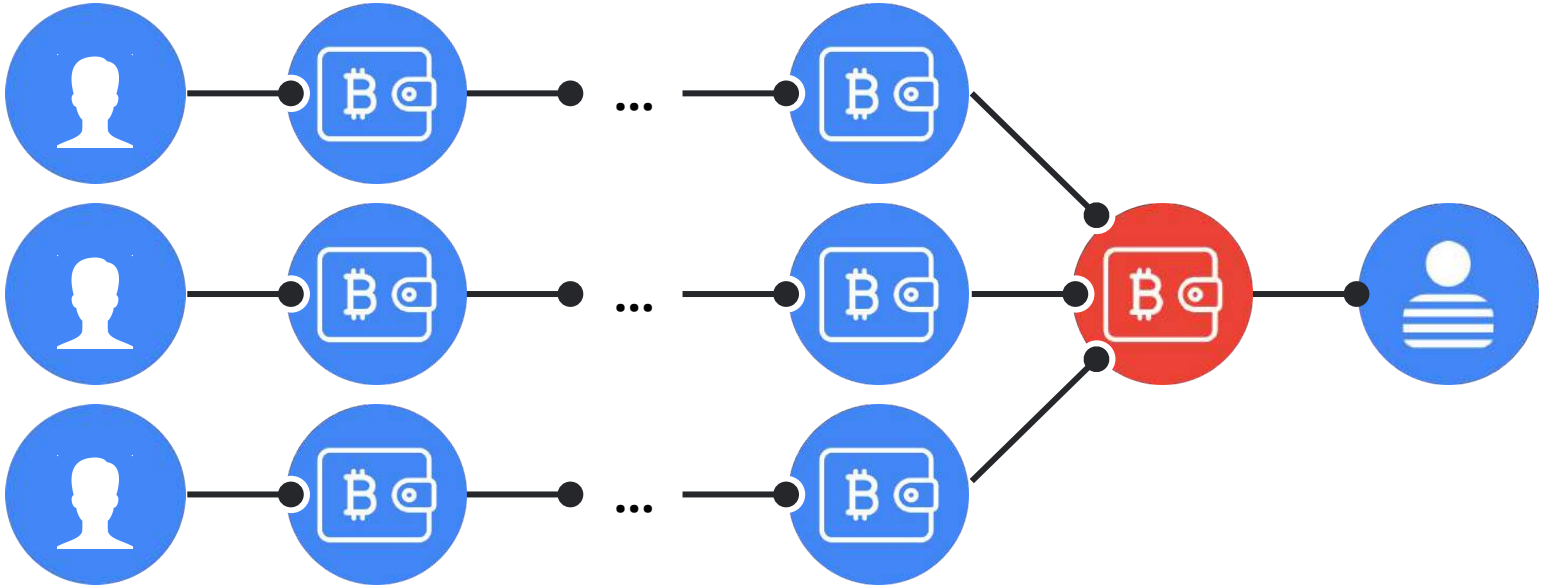
Discovering payment network



Discovering payment network



Discovering payment network

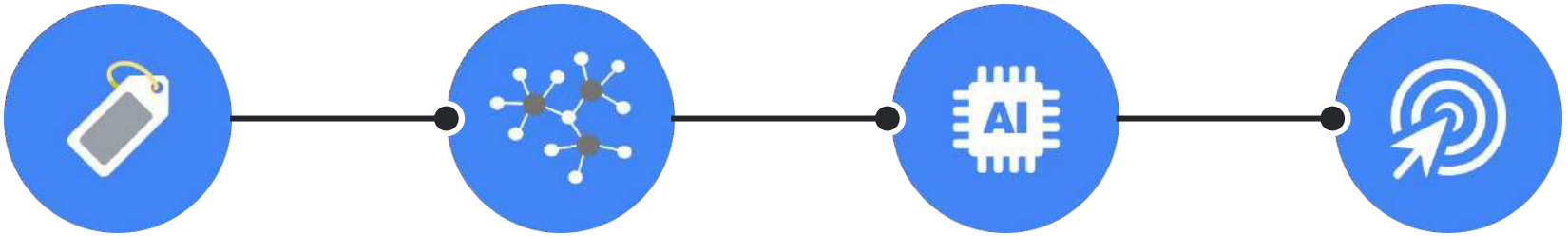


Gathering seed bitcoin transactions

Victim reports

Synthetic “victims”

Automating payment tracing

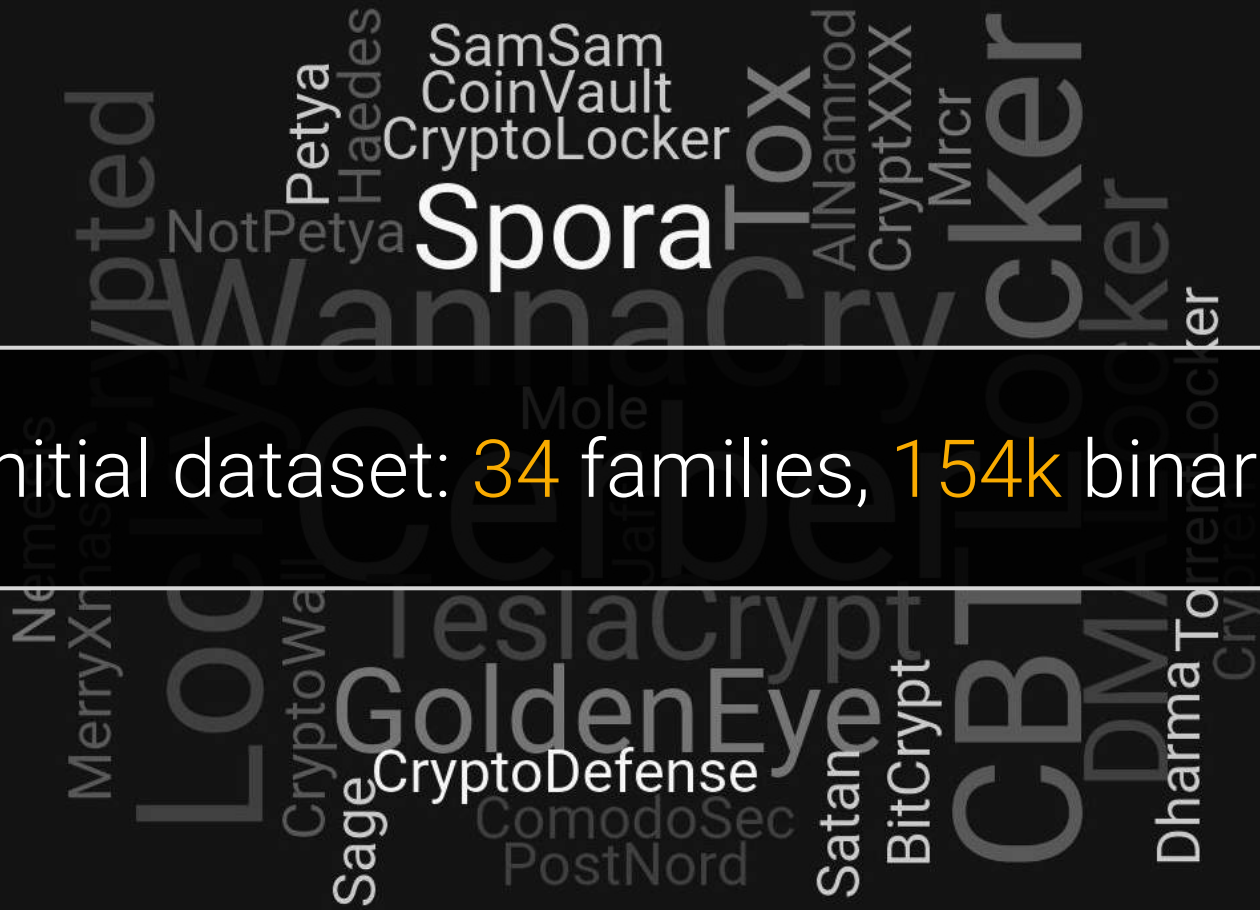


Initial seed ransomware

Dataset expansion & clustering

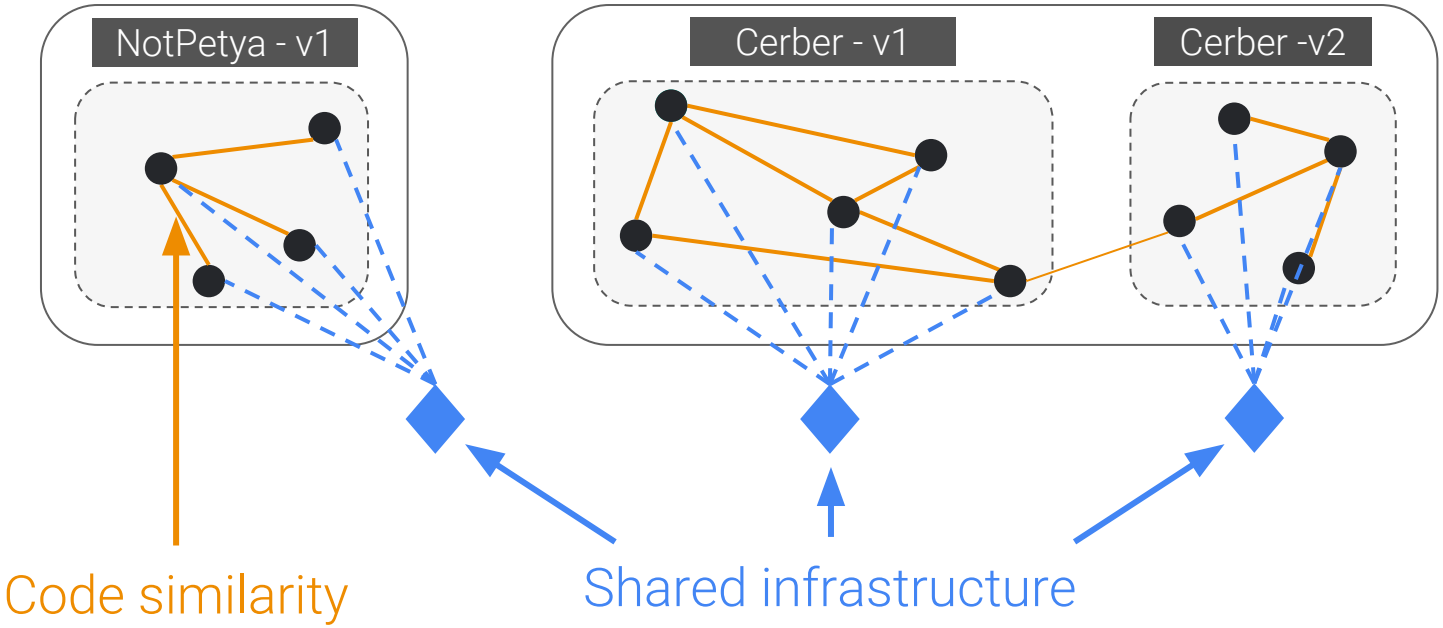
Payment site and wallet extraction

Payment tracing



Initial dataset: 34 families, 154k binaries

Using clustering for dataset expansion

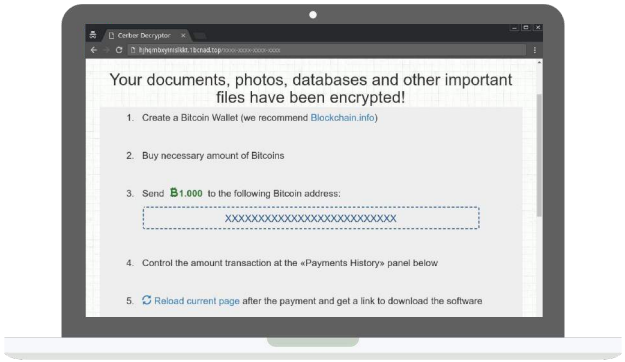


Expanded dataset **301,588 binaries**

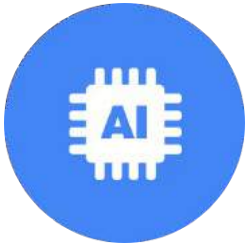
Seed dataset

Additional binaries

Automatically identifying payment sites at scale



+



=

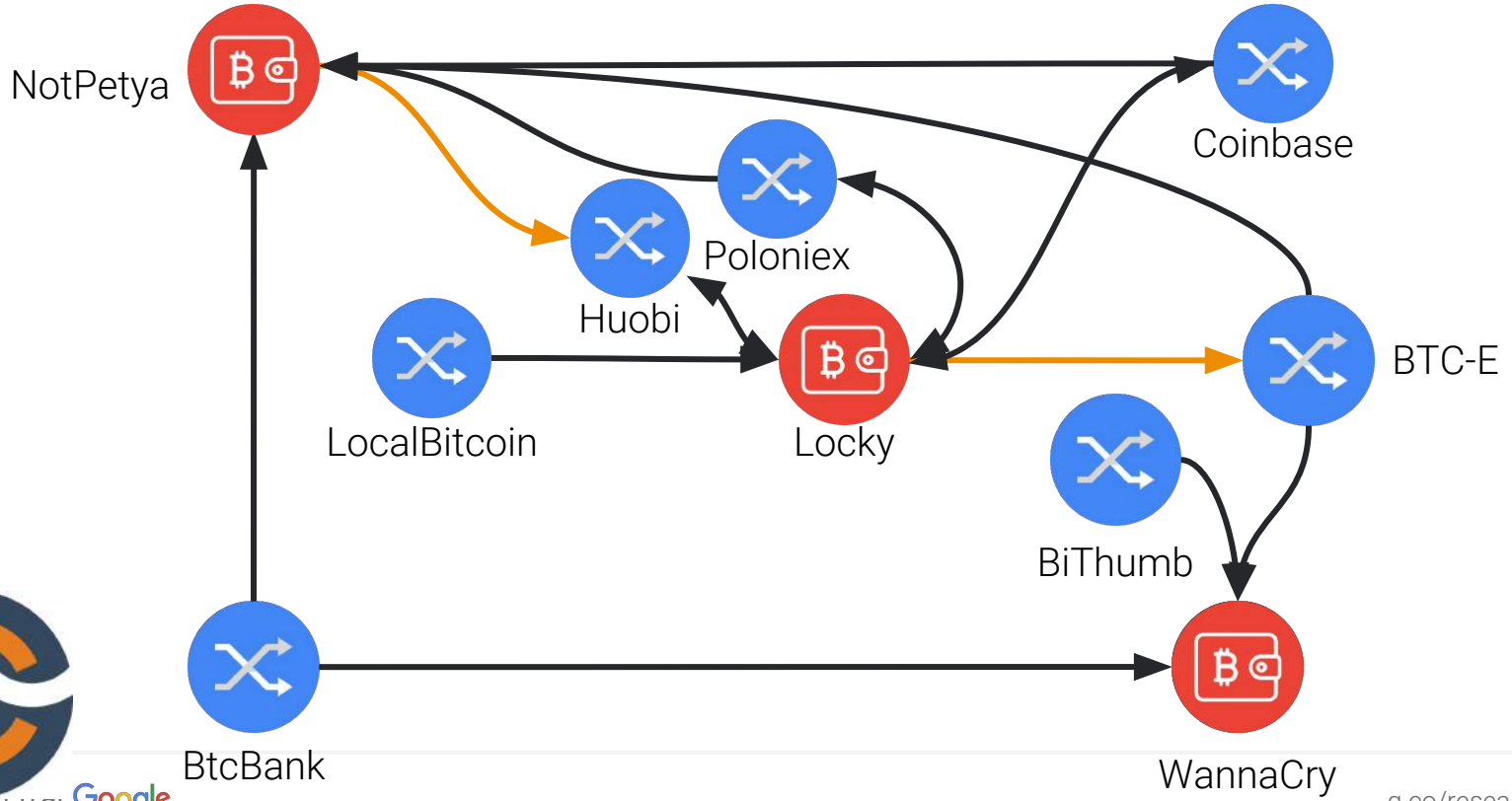
Tor proxy URL
hjhqmbxyinislkkt.1a58vj.top/XXXX

Found in 4 files and 1 screenshot

Bitcoin wallet
1AZvk[...]

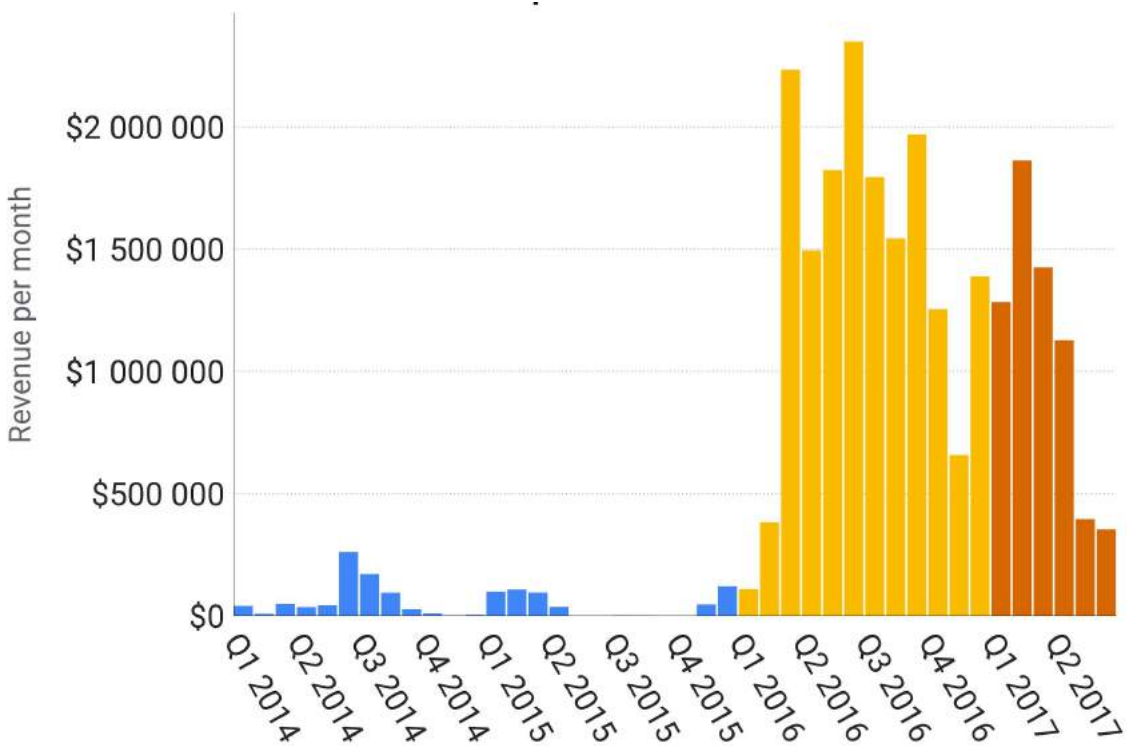
Found in 16 files and 1 screenshot

Tracing payments through the bitcoin chain

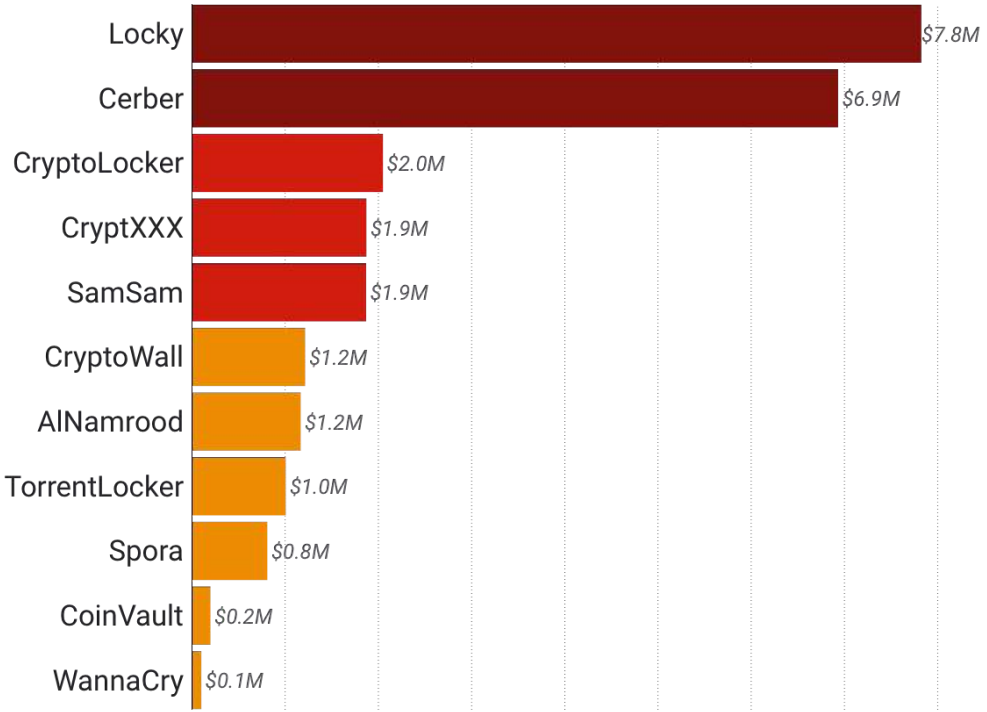


Market insights

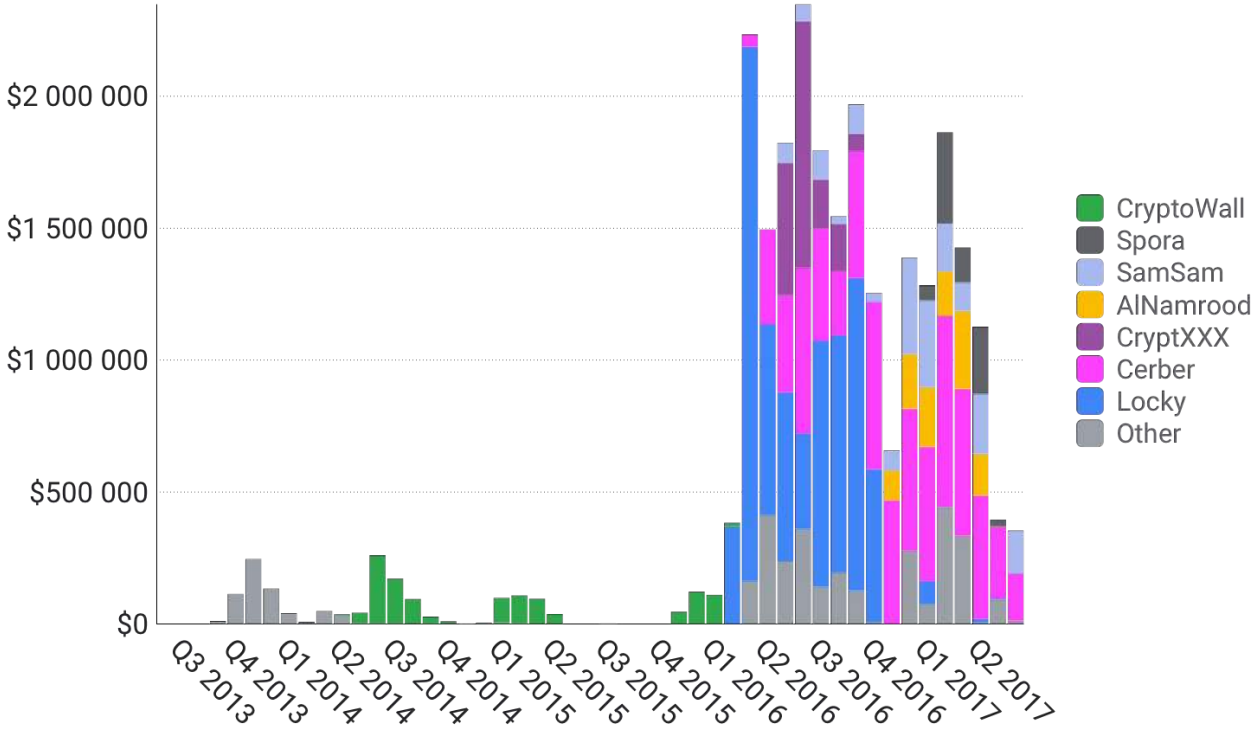
$25,253,505



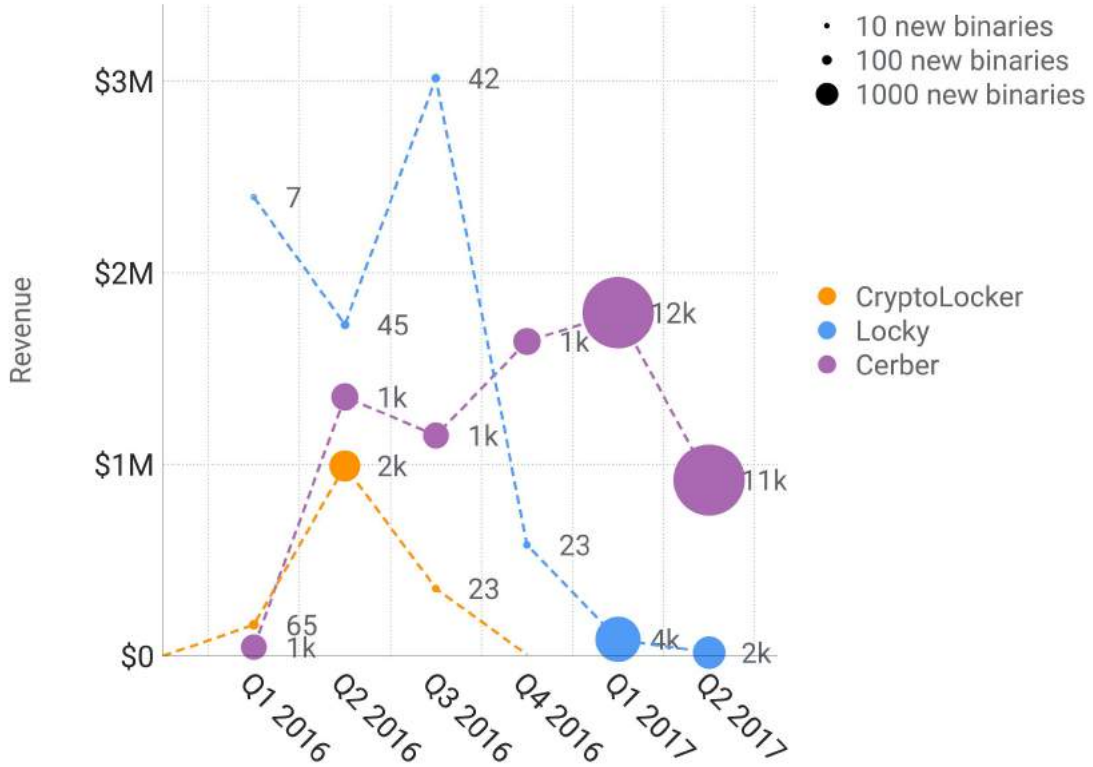
In 2016 ransomware became a multi-million $ business



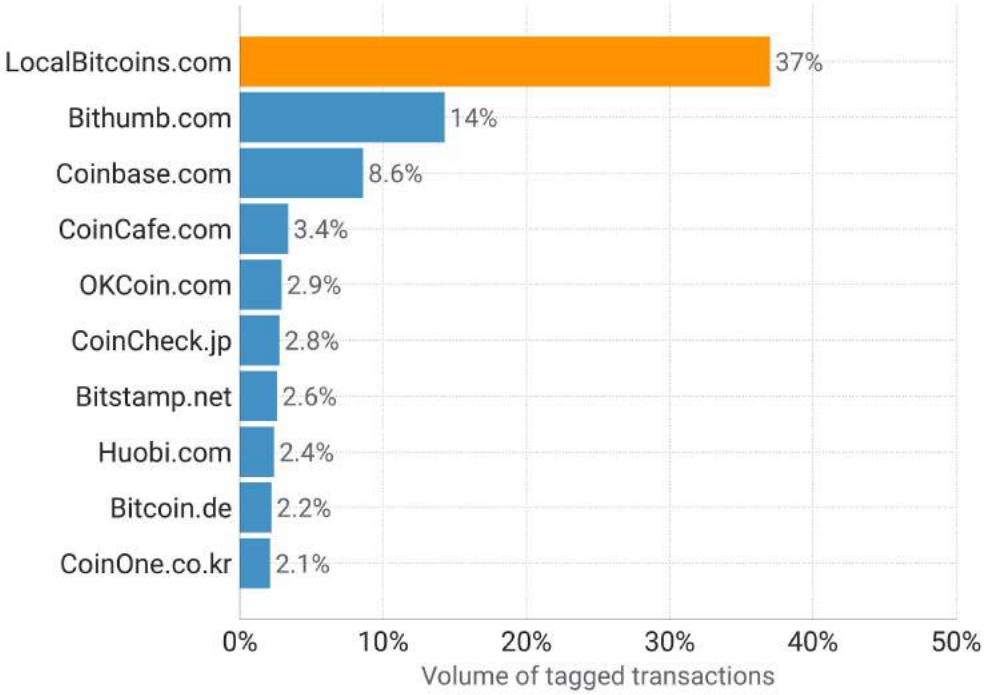
The ecosystem is dominated by a few kingpins



A fast changing market

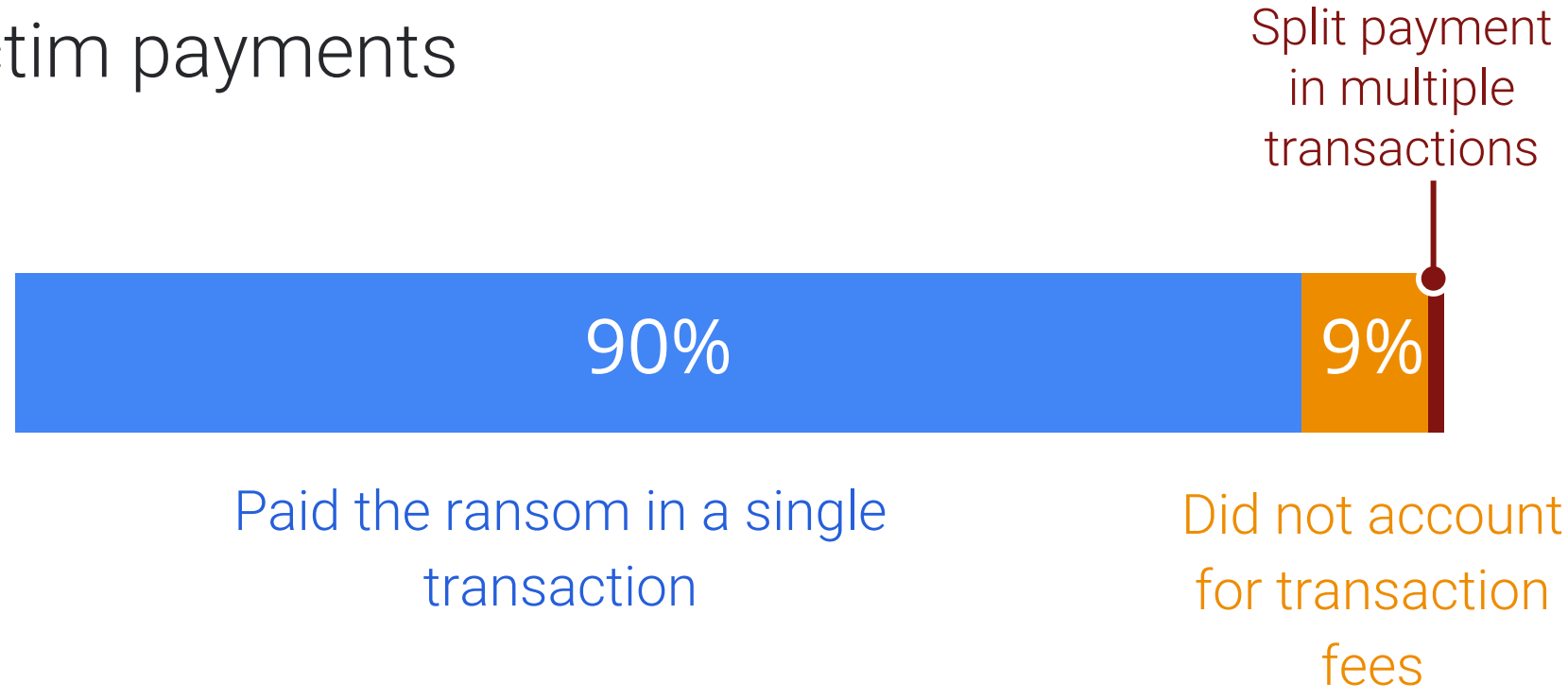


In 2017 ransomware increased binary diversity to evade AVs



Many victims buy Bitcoins through the “Craigslist of Bitcoin”

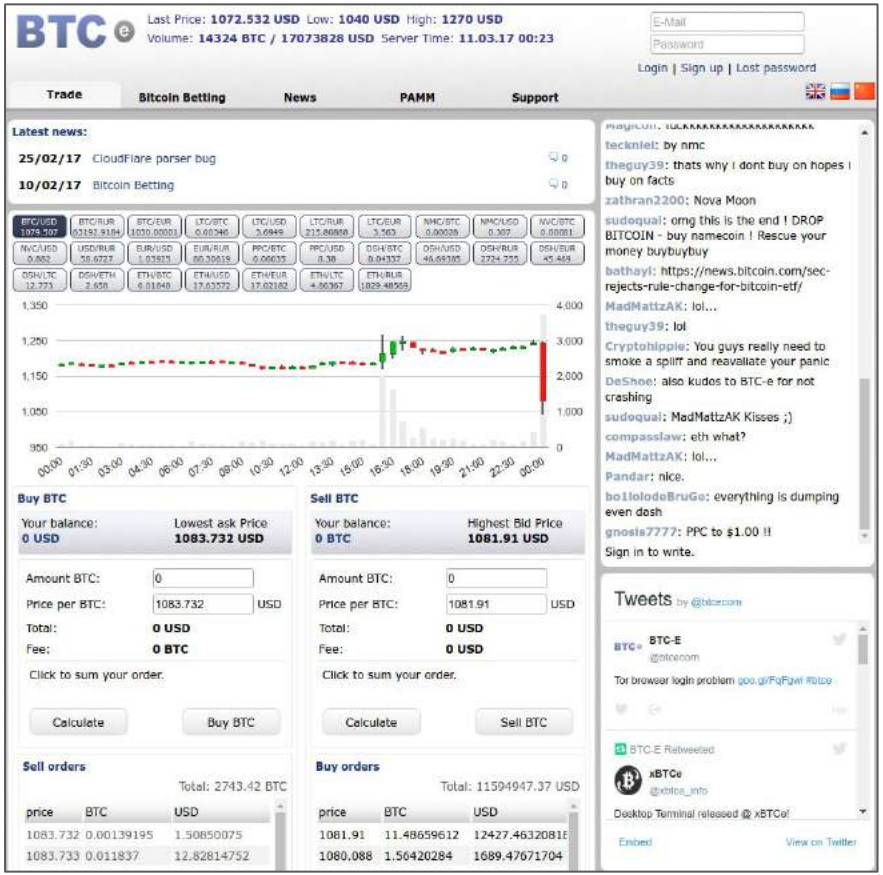
Victim payments



95%

traced ransoms cashed out via BTC-E

Cashout list available on request



Ransomware notable actors

Locky

Bringing ransoms to the masses

International Business Times

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

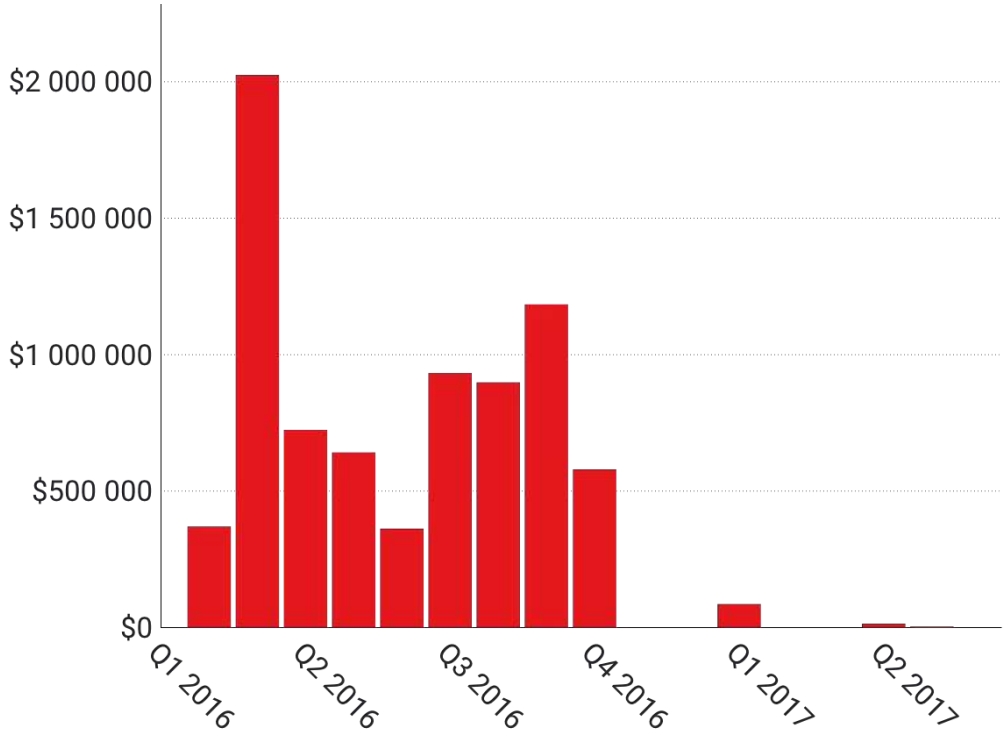
Security experts have warned that 'Locky' is quickly evolving into an effective piece of ransomware (iStock)

SC MEDIA

Locky ransomware is back, this time via Necurs

ZDNet

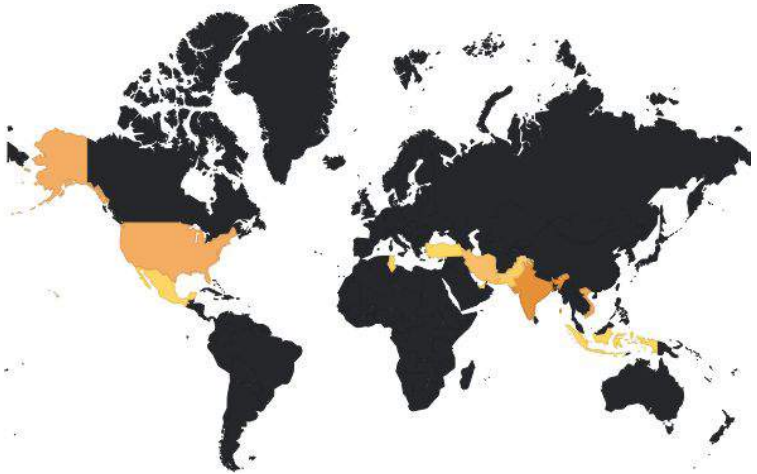
The godfather of ransomware returns: Locky is back and sneakier than ever



The first ransomware to make >$1M per month

Renting-out cybercriminal infrastructure

Dridex



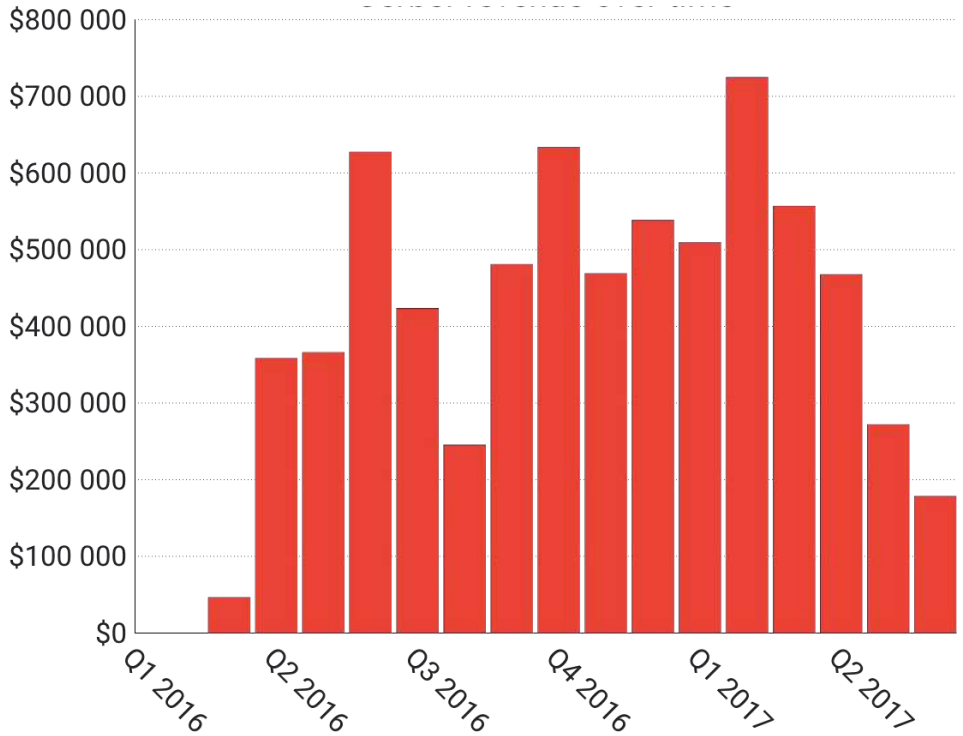
Locky

Dridex, Locky, Cerber are distributed via the Necurs botnet

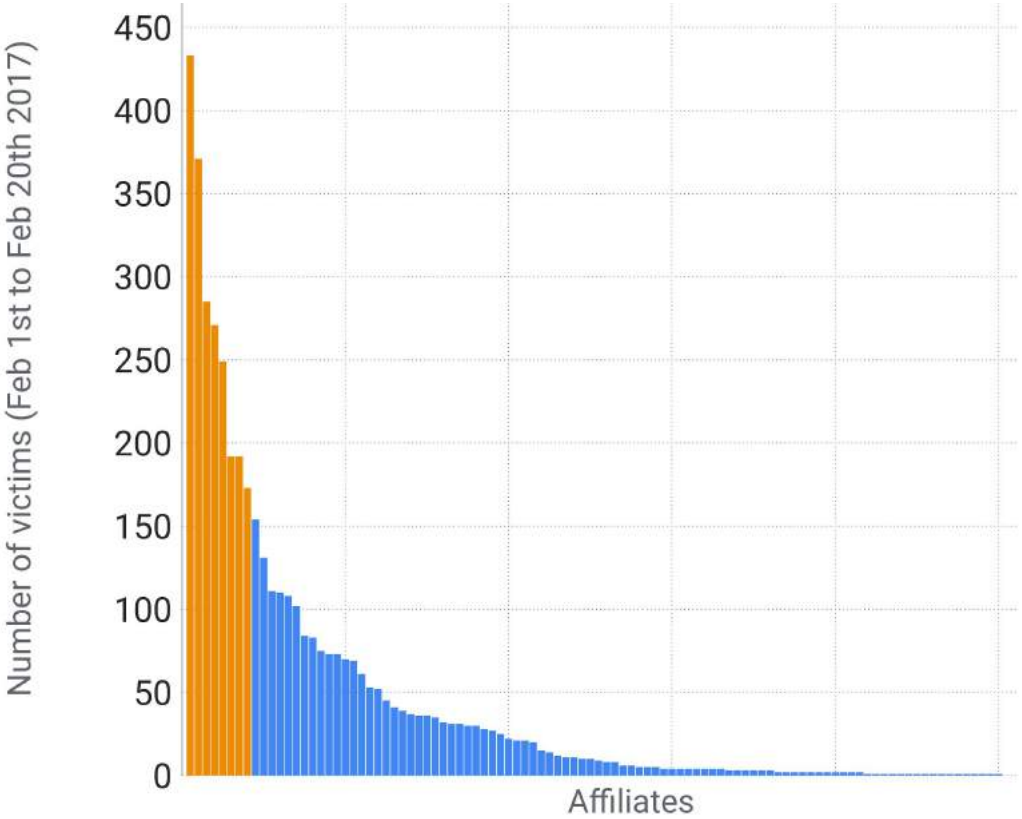
Cerber

Rise of ransomware as service

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

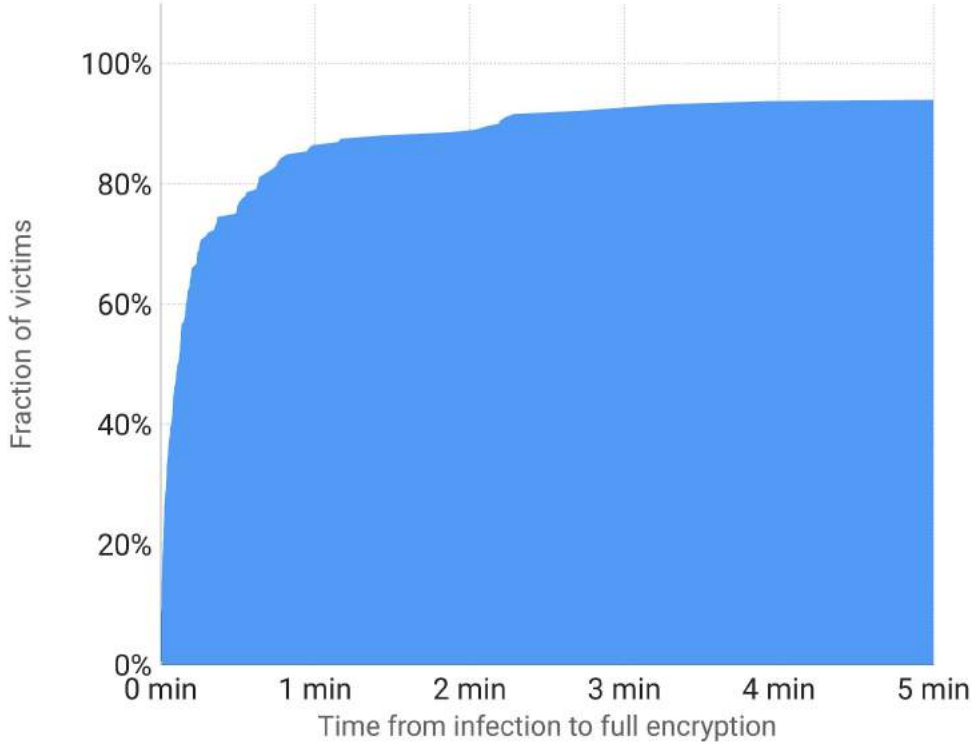
1AzkuxChzMB4[...]

1Azkux.top

Embedding ransom site in the blockchain

Hardcoded wallet transacts with new wallets periodically.

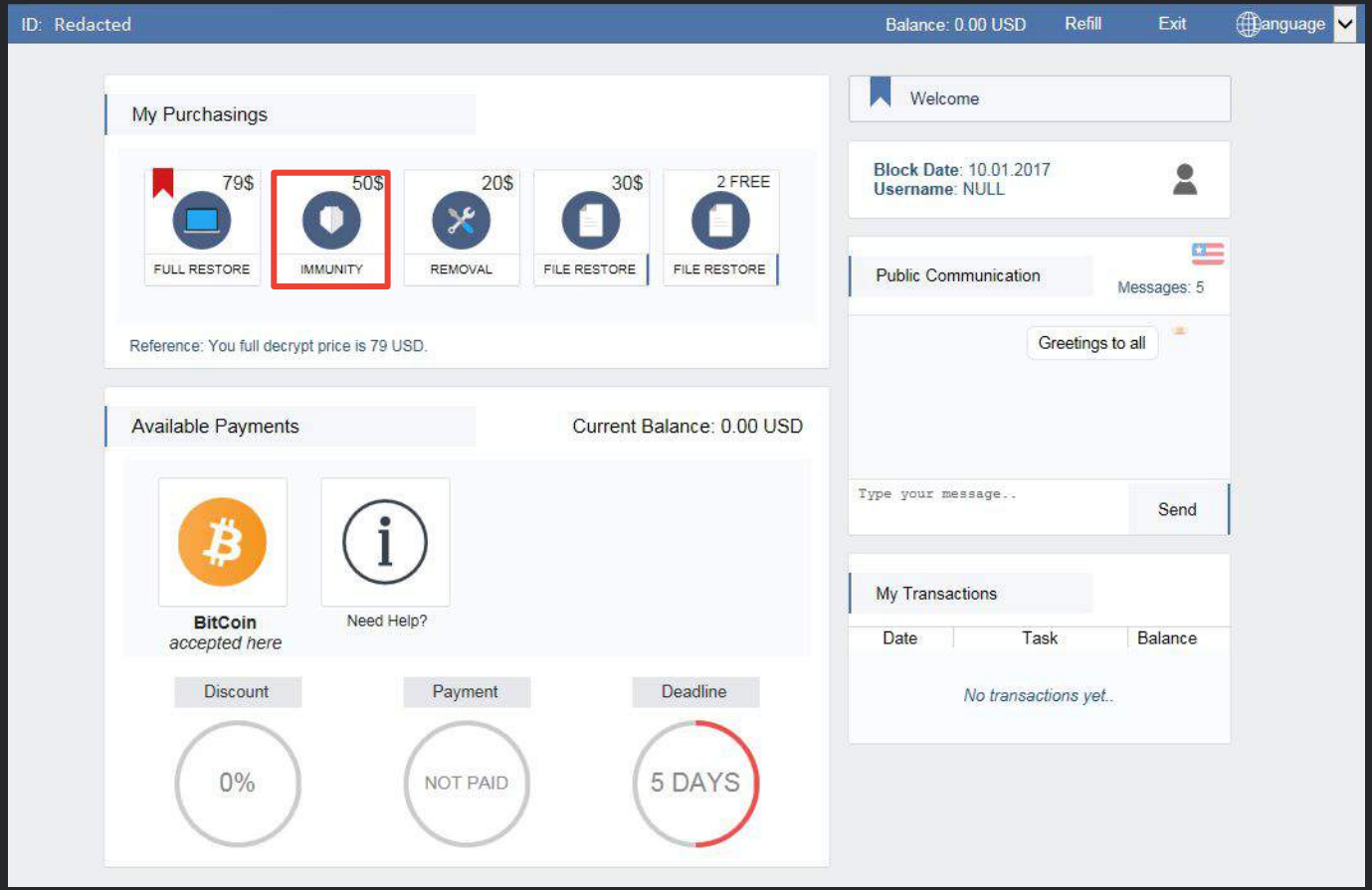
Cerber derives ransom site from these wallets.



From infection to full encryption in under a minute

Spora

Ransomware business model refined


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
0%
Payment
NOT PAID
Deadline
5 DAYS
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
@WanaDecr
@WanaDecr
Ooop
ted.
f you see
hen your
it from yo
r" window,
u deleted
f you nee
tware.
Please fin
any folder
.exe" in
Run and fo
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/18/2017 15:01:24
Time Left
00:00:00:00
Your files will be lost on
5/22/2017 15:01:24
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
Test Mode
Windows 7
Build 7601
3:01 PM
5/15/2017

CNN tech

0:00

Massive cyberattack targeting 99 countries causes sweeping havoc

ZDNet

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.

WIRED

A SCARY NEW RANSOMWARE OUTBREAK USES WANNACRY'S OLD TRICKS

The (low) bottom line

56 BTC

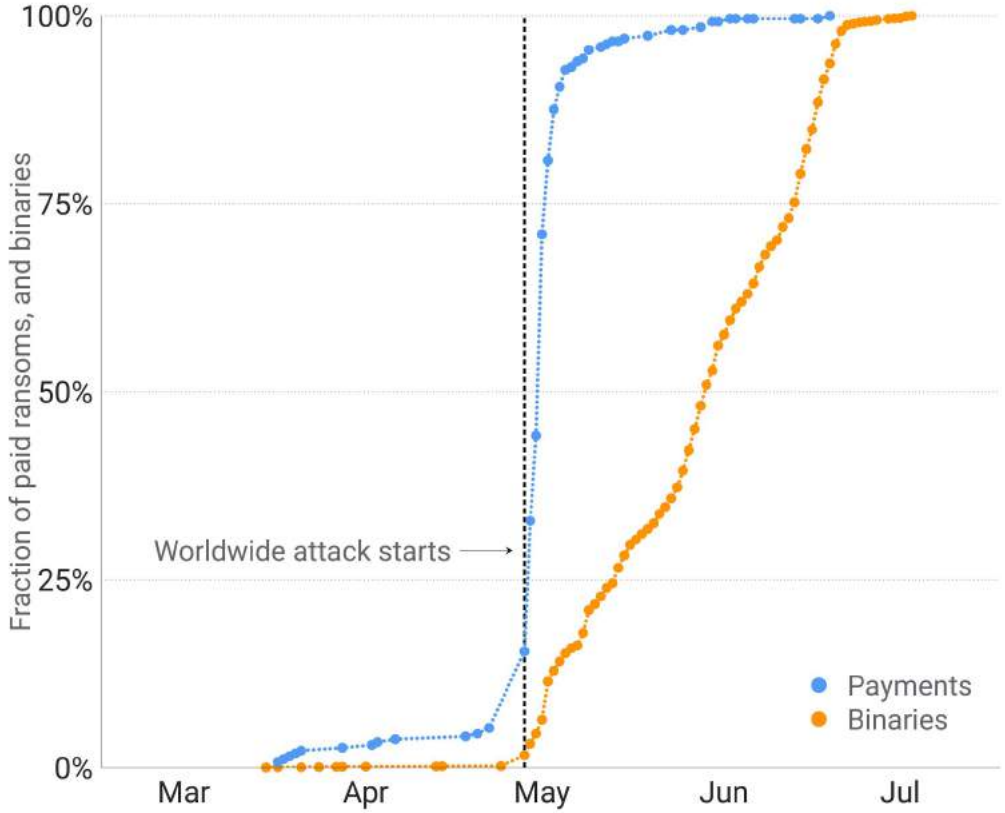
revenue

5

bitcoin wallets

$0

cashed-out

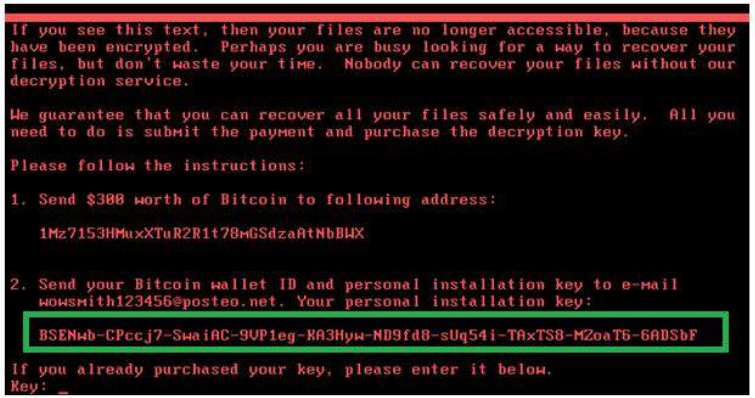


Testing out the malware, then unleashing it at once

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.



Forbes

The NotPetya Ransomware May Actually Be A Devastating Cyberweapon

c|net

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

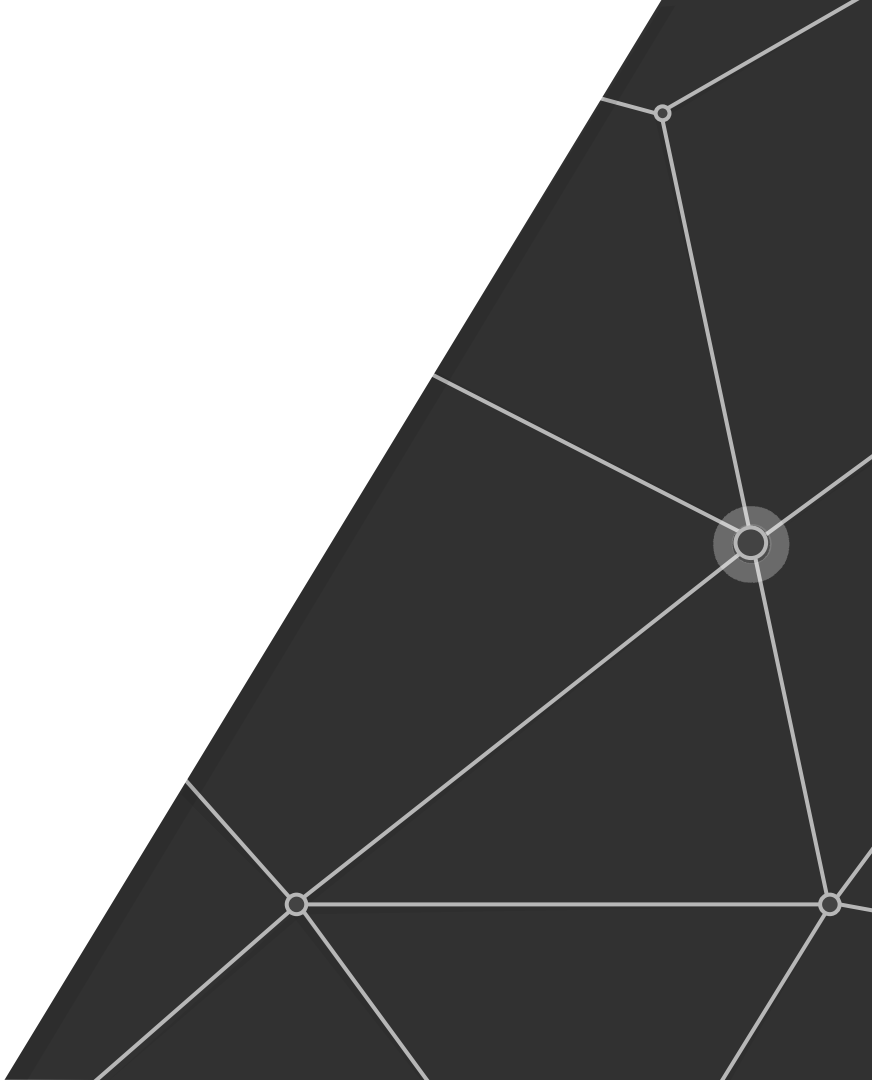
Rise of the impostors

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