Tracking desktop ransomware payments end to end

Elie Bursztein, Kylie McRoberts, Luca Invernizzi
with the help of many people from UCSD, NYU, and Chainalysis
Only 37% of users backup their data.
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

Ransomware Decrypts Your Files For Free If You Infect Your Friends

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
The website ahead contains malware

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 visits payment site via Tor

Victim ID

Unique Bitcoin wallet
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

Transaction 152Lf[...] on 2016-08-09

Sender wallet: 1N1Nn[...]

Receiver wallet: 152Lf[...]
Life of a ransom payment

1. Victim buys bitcoins at exchange
Life of a ransom payment

1. Victim buys bitcoins at exchange

2. Ransom moves across multiple wallets
1. Victim buys bitcoins at exchange
2. Ransom moves across multiple wallets
3. Criminal accumulates bitcoins then sells them for currency at exchange
Measuring revenue
Identifying victims

To identify other victims, we look at transactions with the criminal’s accumulation wallet.
Discovering payment network
Discovering payment network
Discovering payment network
Gathering seed bitcoin transactions

Victim reports

Synthetic “victims”
Automating payment tracing

1. Initial seed ransomware
2. Dataset expansion & clustering
3. Payment site and wallet extraction
4. Payment tracing
Initial dataset: 34 families, 154k binaries
Using clustering for dataset expansion

- NotPetya - v1
- Cerber - v1
- Cerber - v2

Code similarity

Shared infrastructure
Expanded dataset 301,588 binaries

- Seed dataset: 154,227
- Additional binaries: 147,361
Automatically identifying payment sites at scale
Tracing payments through the bitcoin chain

NotPetya

LocalBitcoin

Huobi

Poloniex

Locky

BtcBank

BiThumb

BTC-E

WannaCry

WannaCry

Coinbase

Huobi

BtcBank

BiThumb
Market insights
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

- 90% Paid the ransom in a single transaction
- 9% Did not account for transaction fees

Split payment in multiple transactions
95% traced ransoms cashed out via BTC-E

Cashout list available on request
Ransomware notable actors
Locky

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.

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, 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
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
Welcome

Block Date: 10.01.2017
Username: NULL

Public Communication
Messages: 5
Greetings to all

My Transactions
No transactions yet.

Available Payments
Current Balance: 0.00 USD

BitCoin accepted here
Need Help?

Discount
Payment
Deadline

0%
NOT PAID
5 DAYS
Wannacry
notPetya
Rise of the impostors
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.

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 done enough for us. 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 GMT with 1-2 hours before.

Send $300 worth of bitcoin to this address:
128YD9gMs2N4yMgw519p7A48jreFS4w

Contact Us
Check Payment
Decrypt
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
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

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
Thank you

g.co/research/protect