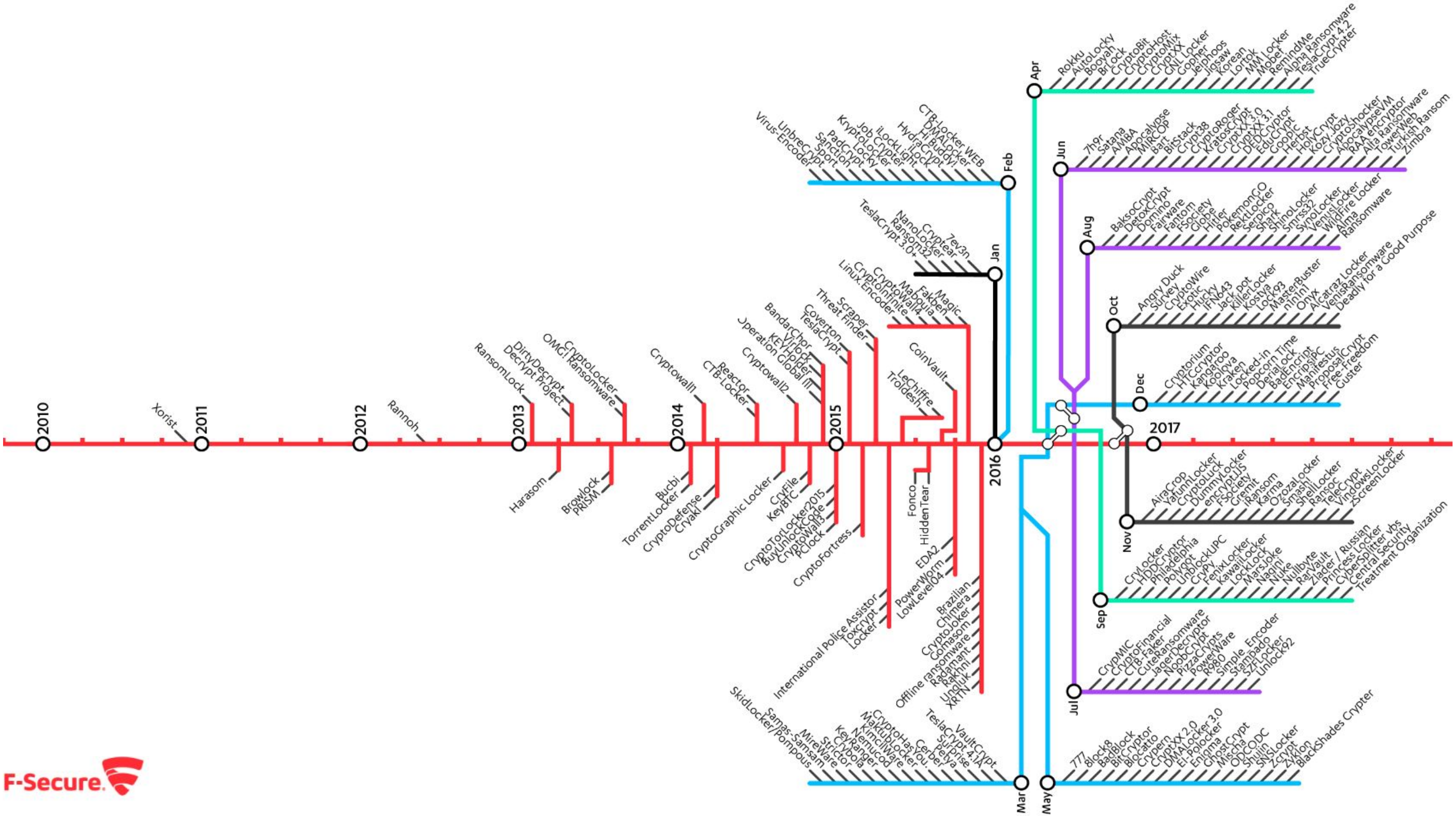
“I was told to buy a software or lose my computer. I ignored it”

A study of ransomware

Camelia Simoiu, Stanford University
Joseph Bonneau, NYU
Christopher Gates, Symantec
Sharad Goel, Stanford University


2010
Xorist
2011
2012
Rannoh
2013
RansomLock
DirtyDecrypt
Decrypt Project
OMG! Ransomware
CryptoLocker
Harasom
Browlock
PRISM
2014
CryptowallI
CTB-Locker
Reactor
Cryptowall2
Operation Global III
KEYHolder
Virlock
BandarChor
Bucbi
TorrentLocker
CryptoDefense
Cryakl
CryptoGraphic Locker
CryFile
KeyBTC
2015
CryptoTorLocker2015
BuyUnlockCode
CryptoWall3
PClock
CryptoFortress
TeslaCrypt
Coverton
Threat Finder
Scraper
Linux.Encoder
CryptoInfinite
CryptoWall4
Mabouia
Fakben
Magic
International Police Assistor
Toxcrypt
Locker
CoinVault
LeChiffre
Troldesh
Fonco
HiddenTear
EDA2
PowerWorm
LowLevel04
Brazilian
Chimera
CryptoJoker
Comasom
Offline ransomware
Radamant
Rakhni
Ungluk
XRTN
2016
Jan
7ev3n
Cryptear
NanoLocker
Ransom32
TeslaCrypt 3.0+
Feb
CTB-Locker WEB
DMALocker
Hi Buddy!
HydraCrypt
iLock
iLockLight
Job Crypter
KryptoLocker
Locky
PadCrypt
Sanction
Sport
UnbreCrypt
Virus-Encoder
Mar
VaultCrypt
TeslaCrypt 4.1A
Surprise
Petya
Cerber
CryptoHasYou.
MaktubLocker
KimcilWare
Nemucod
KeyRanger
Cryboola
Strictor
MireWare
Samas-Samsam
SkidLocker/Pompous
Apr
Rokku
AutoLocky
Booyah
BrLock
CryptoBit
CryptoHost
CryptoMix
CryptXX
GNL Locker
Gopher
Jeiphoos
Jigsaw
Korean
Lortok
MM Locker
Mobef
RemindMe
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
May
777
8lock8
BadBlock
BitCryptor
Blocatto
Crypern
CryptXX 2.0
DMALocker 3.0
El-Polocker
Enigma
GhostCrypt
Mischa
ODCODC
Shujin
SNSLocker
Zcrypt
Zyklon
BlackShades Crypter
Jun
7h9r
Satana
AMBA
Apocalypse
MIRCOP
Bart
BitStack
Crypt38
CryptoRoger
KratosCrypt
CryptXX 3.0
CryptXX 3.1
DEDCryptor
EduCrypt
GoopIc
Herbst
HolyCrypt
Kozy.Jozy
CryptoShocker
ApocalypseVM
RAA encryptor
Alfa Ransomware
TowerWeb
Turkish Ransom
Zimbra
Jul
CrypMIC
CryptoFinancial
CTB-Faker
CuteRansomware
JagerDecryptor
NoobCrypt
PizzaCrypts
PowerWare
R980
Simple_Encoder
Stampado
SZFLocker
Unlock92
Aug
BaksoCrypt
DetoxCrypt
Domino
Fairware
Fantom
FSociety
Globe
Hitler
PokemonGO
RektLocker
Serpico
Shark
ShinoLocker
Smrss32
SynoLocker
VenusLocker
WildFire Locker
Alma
Ransomware
Sep
CryLocker
HDDCryptor
Philadelphia
Polyglot
UnblockUPC
CryPy
FenixLocker
KawaiiLocker
LockLock
MarsJoke
Nagini
Nuke
Nullbyte
RarVault
Zlader / Russian
Princess Locker
CyberSplitter vbs
Central Security
Treatment Organization
Oct
Angry Duck
Survey
CryptoWire
Exotic
Hucky
IFN643
Jack.pot
KillerLocker
Kostya
Lock93
MasterBuster
n1n1n1
Onyx
Alcatraz Locker
VenisRansomware
Deadly for a Good Purpose
Nov
AiraCrop
YafunnLocker
CryptoLuck
DummyLocker
encryptJJS
FSociety
Gremit
iRansom
Karma
OzozaLocker
Smash!
ShellLocker
Ransoc
TeleCrypt
VindowsLocker
zScreenLocker
Dec
Cryptorium
HTCcryptor
Kangaroo
Koolova
Kraken
Locked-in
Popcorn Time
DerialLock
BadEncript
EncripsiPC
Manifestus
ProposalCrypt
Free-Freedom
Guster
2017

*“For the past couple of years consumers have been the most likely victims of ransomware, usually accounting for **two-thirds of all infections**.”*

[An ISTR Special Report: Ransomware and Businesses 2016, Symantec]

Current estimates

Current estimates are based on non-representative data, and often inconsistent:

- [FBI IC3 report, 2017]
  2,700 reports (2016)

- [ISTR Special Report, Symantec, 2017]
  405,000 consumer blocks globally (06/2016 - 06/2017)

- [Huang et al., 2018]
  20,000 potential victims globally, across a 22-month period (2016 - 2017)

Research questions

1. What are the prevalence and characteristics of ransomware attacks in the general US population?

2. What (situational and behavioral) factors affect susceptibility to ransomware ?

Estimating the prevalence of ransomware

Identifying ransomware infections

- Representative sample of 1,180 U.S. adults
  - Weighting adjustment for each respondent
  - Matched to the 2010 American Community Survey (ACS)

Identifying ransomware infections

- Representative sample of 1,180 U.S. adults
  - Weighting adjustment for each respondent
  - Matched to the 2010 American Community Survey (ACS)

- Respondents progressed through (up to) 10 information and question pages
  - Definition of ransomware
  - Screenshots of common strains
  - 5 questions on specific tactics typically seen in attacks
  - Free text description of the attack

Victimization rate

	Victimization rate (06/2016 - 06/2017)
Self-reported	5%
Re-classified (inclusive)	3%
Re-classified (conservative)	2%

2% estimate corresponds to approximately 1.9 million victims in the U.S.

Dealing with the attack

- Almost half of attacks reported include police impersonation (46%)
- Encryption strains (36%) less common than locker strains (74%)
- The median and average ransom reported were $250 and $510, respectively (s.e. $390)
- Few victims paid ransom (4%) or notified authorities (11%)

Payment method

Cryptocurrencies do not seem to be the driving factor for ransomware.

	Proportion
Pre-paid cash voucher	40%
Wire transfer	15%
Cryptocurrency	**13%**
Premium-rate text message	8%
Not displayed	14%
Do not remember	10%

Behavioral changes post-attack

	Proportion
More careful browsing	65%
Purchased AV product	44%
Updated AV product	31%
Started to backup data	26%
Enable automatic updates	24%
Backup data more regularly	22%
Changed OS configurations	20%
Changed OS	10%
Changed default browser	12%

Half of victims reported changing 2 or more security habits following the attack.

Behavioral changes post-attack

	Proportion
More careful browsing	65%
Purchased AV product	44%
Updated AV product	31%
Started to backup data	26%
Enable automatic updates	24%
Backup data more regularly	22%
Changed OS configurations	20%
Changed OS	10%
Changed default browser	12%

Half of victims reported changing 2 or more security habits following the attack.

Susceptibility to ransomware

Predicting ransomware infection (next 12 months)

Model	Lasso	GBT
Demographics + SES	65	63
Demographics + SES + technology + computer skills	64	65
Security habits	66	67
Security habits + Experienced scam	**75**	**74**
All features (saturated model)	**76**	**76**

Average AUC across (stratified) K=5 folds.

Risk heuristic

- Statistically derived self-assessment heuristic to estimate risk of future ransomware infection (within the next 12 months)

Risk heuristic

- Statistically derived self-assessment heuristic to estimate risk of future ransomware infection (within the next 12 months)
    - Consumers -- if made aware they are “at risk”, may be better motivated to improve their security posture and adopt better security habits
    - Perceived susceptibility has been found to be a necessary factor to achieve behavior change in a variety of contexts [Strecher et al., 1997]

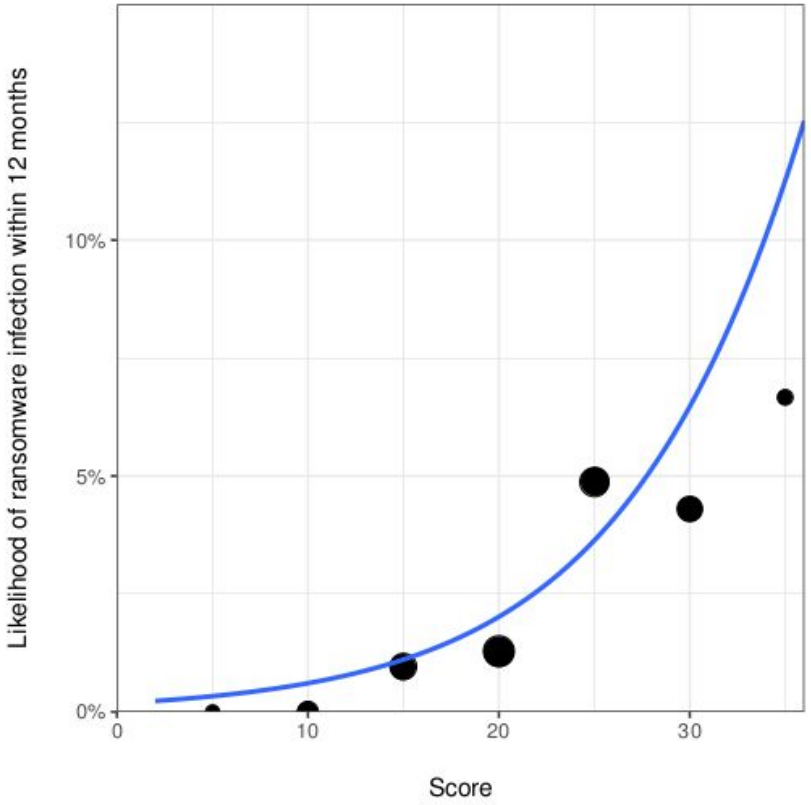
Risk heuristic

Question	Points
How frequently do you **download files from online torrent sites** such as the Pirate Bay or TorrentZ2?	
● I frequently download files from torrent sites	15
● I occasionally download files from torrent sites	10
● I rarely download files from torrent sites	5
● I never download files from torrent sites	0
Do you **backup your personal files** to an external hard drive or cloud-based storage device?	
● I do not have any of my files backed up.	6
● I backup my files once a year	4
● I backup my files every couple of weeks	2
● I backup my files every day.	0
Is your **hard drive encrypted**?	
● Yes, my hard drive is encrypted	0
● No, my hard drive is not encrypted	1

Question	Points
Have you ever downloaded -- or been asked to download-- an application that you suspect was malicious?	10
● Yes, I have.	0
● No, I haven't.	
Do you use **two-factor authentication** for at least one of your online personal accounts (i.e., not for a work-related account)?	
● Yes, I use two-factor authentication.	0
● No, I don't use two-factor authentication.	1
Is your computer **password-protected for login**?	
● Yes, my computer has a password.	0
● No, my computer doesn't have a password.	8

Calibration

Average AUC across K=10 folds is 78%, on par with the saturated model.



Conclusions

- Estimate the rate of ransomware infection across a nationally-representative sample of the US population: 2% - 3%

- Propose a tool for consumers to self-assess their risk of infection that is fast, transparent, and requires limited information

csimiou@stanford.edu
@camiioux

“I was told to buy a software or lose my computer. I ignored it”: A study of ransomware
http://web.stanford.edu/~csimoiu/

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

OK

Sample responses

Description of attack	System Lock	Encryption	Police impersonation	Inclusive	Conservative
"FBI - YOU HAVE BEEN WATCHING PORN OR GAMBLING OR BOTH, YOU MUST PAY $200 TO MONEYGRAM"	•	•	•	Ransomware	Ransomware
"I was working on my computer and a screen popped up stating that my files had been encrypted and to reverse this I had to buy a program. I do not remember the name it showed but it had a black background. I just shut the computer and took it in for repair."		•		Ransomware	Ransomware
"It popped up and stated that I had to pay to gain access back to my computer and I was unable to do anything."	•			Ransomware	False Positive
"A voice said to call a certain number and when we did someone insisted that we pay $300 and they would take care of the problem. We didn't pay. It was a mess for a while and my husband worked on it for a whole day."	•			False Positive	False Positive

Risk perceptions

- Victims believe they are *more* at risk of a future attack and *less* likely to pay a ransom.

	Victims	**Non-victims**
Likelihood of experiencing future attack	47 (sd=34)	30 (sd=25)
Likelihood of paying $300 ransom	2.9 (sd=11)	8.4 (sd=20)

Differences statistically significant using a t test, 95% CI