“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




“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, 22-month period (2016 - 2017)

Research questions

1. What are the prevalence and characteristics of ransomware infections 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)

YouGov
What the world thinks

- Respondents progressed through (up to) 30 information and question pages
  - Definition of ransomware
  - Screenshots of common strains
  - 5 questions on specific tactics typical of ransomware
  - Free text description of the attack
  - Consequences of the attack

Victimization rate

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

3% estimate corresponds to approximately 2.8 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 methods

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

	Proportion
Pre-paid cash voucher	42%
Wire transfer	14%
Cryptocurrency	**12%**
Premium-rate text message	7%
Not displayed	15%
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.

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 a (future) ransomware 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.

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=10 folds.

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=10 folds.

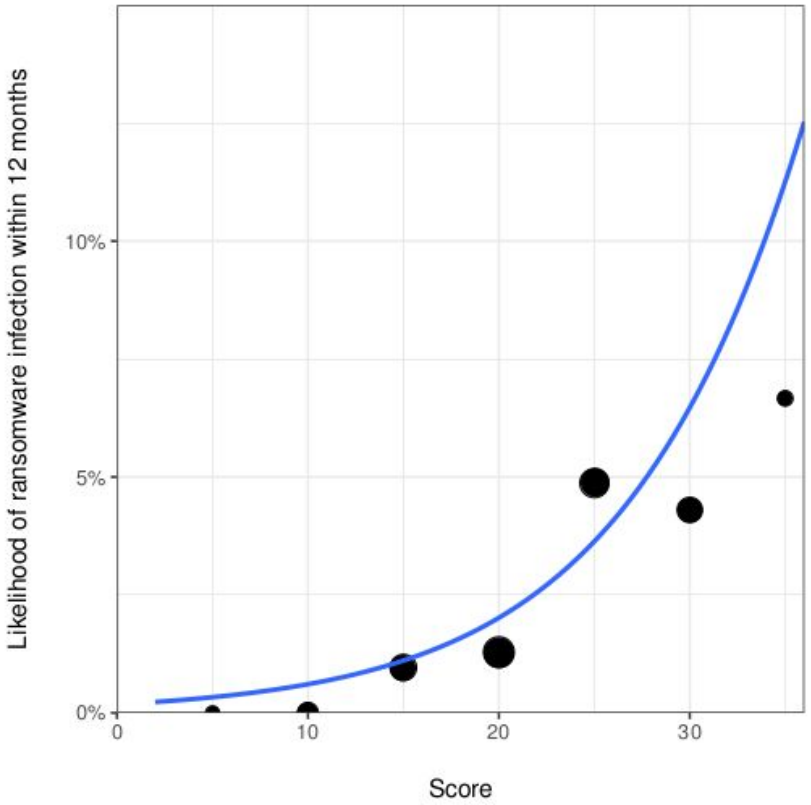
A simpler approach to risk-assessment

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 & future work

- Estimate victimization rate for the U.S.: 3% per year (06/2016 - 06/2017).
- Susceptibility to ransomware infection can be estimated from self-reported security habits and exposure to online scams.
- Present a proof-of-concept approach for consumers to self-assess their risk of infection, that is fast, transparent, and requires limited information.

Questions?

 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/

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