

Introduction to Information Security

14-741/18-631 Fall 2021

Unit 6, Lecture 1:

Security, privacy and behavioral biases

Hanan Hibshi

hhibshi@andrew

Motivation: Security Analysis



- Who/What is the target?
- What are the desired security properties?
- Understand defenders' resources
 - ▼ Economic, technological, behavioral

- Who are the adversaries?
 - ▼ Identify attackers
 - ▼ Probability of attack (risk assessment) and damages
- Estimate attackers' resources
 - ▼ Economic, technological, behavioral

Research Question

How can we better model attackers and defenders?

- ▼ Defenders **have been** assumed knowledgeable, interested in security, and altruistic
 - ▼ But in practice, generally self-interested
 - ▼ Rarely fully informed
 - ▼ Not even really rational: behavioral biases
- ▼ Attackers **have been** assumed omnipotent
 - ▼ But in practice very often financially motivated
 - ▼ Tend to be economically rational
 - ▼ May not lead us to devise effective defenses (see Anderson, 1993)
- ▼ Economics can tell us which intervention strategies most likely to succeed...
 - ▼ ... but for that we need sound economic models of all parties' behavior...

This Lecture's Agenda

■ Outline

- ▼ Motivation
 - ▼ Why security economics?
 - ▼ Why selfishness?
- ▼ Discussion
 - ▼ Limitations of classical game theory
 - ▼ Further challenges in security and privacy

■ Objective

- ▼ Learn techniques to model externalities
- ▼ Learn how economics-inspired techniques can help discover incentive misalignment
- ▼ Get an exposure to behavioral economics

Trivial Observation 1

- Why are security-compromising and privacy-invasive technologies abundant?
 - ▼ Examples: Spyware, Malware, Targeted Advertisement, Phishing...
 - ▼ Answer: Financial incentives
 - ▼ Historical perspective is different

Trivial Observation 2

■ Why and how should users protect themselves?

- ▼ Examples of protective measures: PETs, security software, different behaviors online and offline (i.e., use shredders, use curtains)
- ▼ Motivation: Financial and other incentives (e.g., feeling of safety)

Homo Economicus

■ Assuming a rational, self-interested agent

- ▶ Rational: Individuals are able to estimate the benefits and costs of a particular action (i.e., are able to estimate the net benefit)
- ▶ Self-interested: Agents engage in an activity if the benefit is greater than or equal to the cost (i.e., the net benefit is greater than or equal to zero)

"It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest." (Adam Smith, The Wealth of Nations, 1776)

Network Effects and Externalities

■ Terms often used interchangeably

- ▼ **Effects:** Benefit, or cost, that an agent derives from a good when the number of other agents consuming the same kind of good changes
- ▼ **Externality:** Participants in the market fail to internalize these effects
 - ▼ is the cost or benefit that affects a party who did not choose to incur that cost or benefit

■ Relationship to public goods

- ▼ An externality occurs when a decision causes costs or benefits to third party stakeholders, often, although not necessarily, from the use of a public good
- ▼ E.g., is identifying information and shopping data a public good?

Networking, Security and Economics

■ Problem well-known in economics and game theory

Economics	Networks	Security
Rational players competing in a market	Selfish nodes competing for network resources	Selfish agents whose security impacts others

■ Can use game theory as a tool

- ▶ to determine likely user (nodes) strategies given the context (network topology, network protocols, policies)
- ▶ to design mechanisms (network topology, protocols, policies) which yield desirable strategies

Toward Building a Model

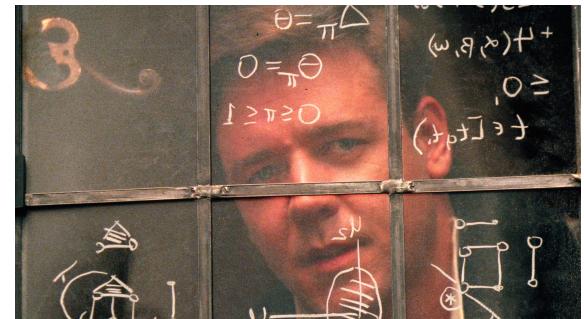
- **Model can be mathematical, or merely describe dependencies or behaviors etc.**
- **Defining models is a process**
 - ▼ Getting ideas
 - ▼ Evaluate usefulness of ideas
 - ▼ Work out examples
 - ▼ Generalize and simplify: Distill essence of phenomenon under investigation
 - ▼ Study literature

Game-Theoretic Model Overview

- **Set of players in a network**
- **Utility function: value each player extracts from the network**
 - ▼ Given by a cost model
- **Strategies: Actions each player can take**
- **Equilibrium concept: situation where all players are content with their utility and don't change their strategy**

Important Equilibria Concepts

- **Social optimum:** set of strategies that maximizes total $U = \sum_{i=1}^N U_i$ network utility
 - ▼ Ideal configuration for the community
 - ▼ What a benevolent government would want
- **Nash equilibrium:** set of strategies in which no individual player can increase their individual utility U_i by changing their protection or insurance settings
 - ▼ Selfish equilibrium
 - ▼ Best response to others' actions



Limitations in a Security Context

- **Asymmetric games: attackers vs. targets**
 - ▼ Different motivations, utility functions...
- **Incomplete information: Are parameters of model known to agents?**
 - ▼ Can attackers infer defense posture?
 - ▼ Can defenders predict likelihood of attack?
- **Information asymmetry: Does one party know more about parameters of interaction?**
 - ▼ Lemons market: Are security products of high or low quality?

Rationality in Practice

- Can researchers formulate a complete model?
- Can consumers act according to model?

Free Giveaway!

Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Home Phone: _____

Work Phone: _____

Single Married

Age: _____ Occupation: _____

Spouses Age: _____ Occupation: _____

Combined Income:

Under \$30,000 Over \$30,000 Over \$50,000

DO YOU: RENT OR OWN YOUR HOME?

VISA MASTERCARD AMERICAN EXPRESS

Would you like info on special events & promotions at Pier 39?

Yes No

E-mail address: _____

Details of Participation and Eligibility Requirements

- Only one Entry per Family.
- Winner allows the use of his or her name, photo, and statements for future promotional use without further compensation.
- Winner must be 18 or over. I.D. required. Winner must provide all necessary federal and state tax reporting information before receiving prizes.
- Drawing held February 23, 2003. Last date to enter drawing is February 16, 2003.
- Winner need not be present to win. Winner will be notified by phone.
- Drawing will be conducted by a Certified Public Accounting Firm at the corporate office of Grand Pacific Resorts, 5900 Pasteur Ct., #200, Carlsbad, CA 92008. To request winner information, correspondence may be forwarded to Grand Pacific Resorts, Promotions Dept. P.O. Box 4068, Carlsbad, CA 92018.
- All local, state, and federal taxes, fees and licenses are the winner's responsibility. Acceptance of the prizes constitutes a release of Facility Management, its agents and employees from all responsibility to the winner.
- Odds are based on number of entries received, approximately 1 in 700,000.
- No purchase or attendance is necessary to be entered into the drawing. Entrants may be invited to attend a sales presentation about the Red Wolf Lodge at Squaw Valley.
- Entries become the property of PNR Marketing Inc.
- The annual "Grand Prize" Giveaway consists of any vehicle with a retail value not to exceed \$25,000 or a three year lease (value to \$25,000) on a luxury car; or any prize (or similar) displayed in a Grand Pacific Resorts Promotion February 25, 2002 - February 23, 2003 (valued up to \$15,000), or the winner may choose cash in the amount of \$15,000.

What Can the Individual Infer?

■ Benefits:

- ▼ Non-monetary benefit (e.g., excitement of participation)
- ▼ Expected monetary benefit:
- ▼ $1/700000 * \$15000 = 2$ cent

■ Costs:

- ▼ Promotions, unsolicited mailing, sales contacts (cannot exclude further use and consequences)
- ▼ Expected monetary cost:
 - ▼ ?

■ What behavioral variables are missing?

Psychological Biases

- We react differently depending on framing of messages
- We make time-inconsistent decisions
- We seek immediate gratification
- We are susceptible to strong biases with ambiguous and unknown information

So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users

Cormac Herley
Microsoft Research

Why Do Users Reject Security Advice?

- **Common perception from tech experts:**
 - ▼ Users are lazy
 - ▼ Users are unmotivated
- **From economic standpoint of view**
 - ▼ Rational decision: Poor cost-benefit
 - ▼ Effects of externalities

Weak Link in Computer Security

■ Users

- ▼ Unpatched machines can be compromised within minutes of connected to the Internet
- ▼ Phishing never gets old
 - ▼ RSA leak, DNC hack, ...

Security Advice

- **Goal: To rid of the weak link in security, we need to educate the users!**
- **Various organizations offer security advice**
 - ▼ US-CERT, large websites, software vendors...
 - ▼ Security firms
 - ▼ Security experts
 - ▼ ...
- **Users are not taking their advice!**

Why?

- **Users are hopelessly lazy**
- **Security tasks must be made more usable and less cumbersome, and better user education**
- **It makes economic sense to reject security advice**
 - ▼ Too much cost, too little gain

What are the Costs and Benefit?

- Direct cost: loss after attack
- Indirect cost: Time and effort spent following security advice
 - ▼ E.g., looking at SSL indicators
- Benefit: ?

Externalities

■ Internet crimes generate negative externalities

- ▼ Criminals' gain
 << (much less than)
 total damage incurred
 (cost incurred on infrastructure by the crime)
- ▼ Spam:
 - ▼ Very low conversion rate vs. huge amount of traffic
 and filtering effort

Cost vs. Benefit

Would like the following to hold, but hard to calculate

$$\sum_{\text{All Users}} \Delta\text{Cost} < \sum_{\text{All Users}} \Delta\text{Benefit}.$$

At least, we would like the following not to hold

$$\sum_{\text{All Users}} \Delta\text{Cost} > \text{Total Direct Losses}$$

For security advice, this can be additional time spent to follow the advice (e.g., examine SSL certificate).

Case Studies

- Password rules
- Look at URLs to avoid phishing
- Certificate errors

Password Rules

■ Lengths/special characters/...

The screenshot shows the PNC Points website interface. At the top, there's a navigation bar with links for PNC.COM, PERSONAL, SMALL BUSINESS, CORPORATE & INSTITUTIONAL, and ABOUT US. Below the navigation is a main menu with WELCOME, REWARDS, and HELP. On the far right of the menu is a prominent orange "Login" button. To the left of the main content area, there's a sidebar with links for Help, FAQs, Retrieve Username, Forgot Password, Contact Us, and Terms and Conditions. The main content area is titled "Change Password" in large orange text. Below the title, there's a detailed description of password requirements: "To change your password, enter your old and new passwords below and then submit. Your password must be 8-15 characters in length containing at least three of the following four character types – (1) capital letter, (2) lower case letter , (3) number, and (4) special character (such as ! \$ % , + - . : = ? { } _ [] ~ @). No spaces are allowed. You cannot use four or more consecutive numbers that match the number of your PNC points card. In addition, the password is case sensitive."

- Don't write it down
- Don't share it with anyone
- Change it often
- Don't re-use passwords across sites.

Password Rules: Benefits/Costs

■ Costs:

- ▼ Indirect: inconveniences
- ▼ Direct: ?

■ Benefits:

- ▼ Against online attacks?
- ▼ Against phishing/keylogging?
- ▼ Composition rules imply hard to brute-force?

Reading URLs to Prevent Phishing

■ Phishing URLs:

- ▶ www.paypa1.com
- ▶ www.bankofthevvest.com

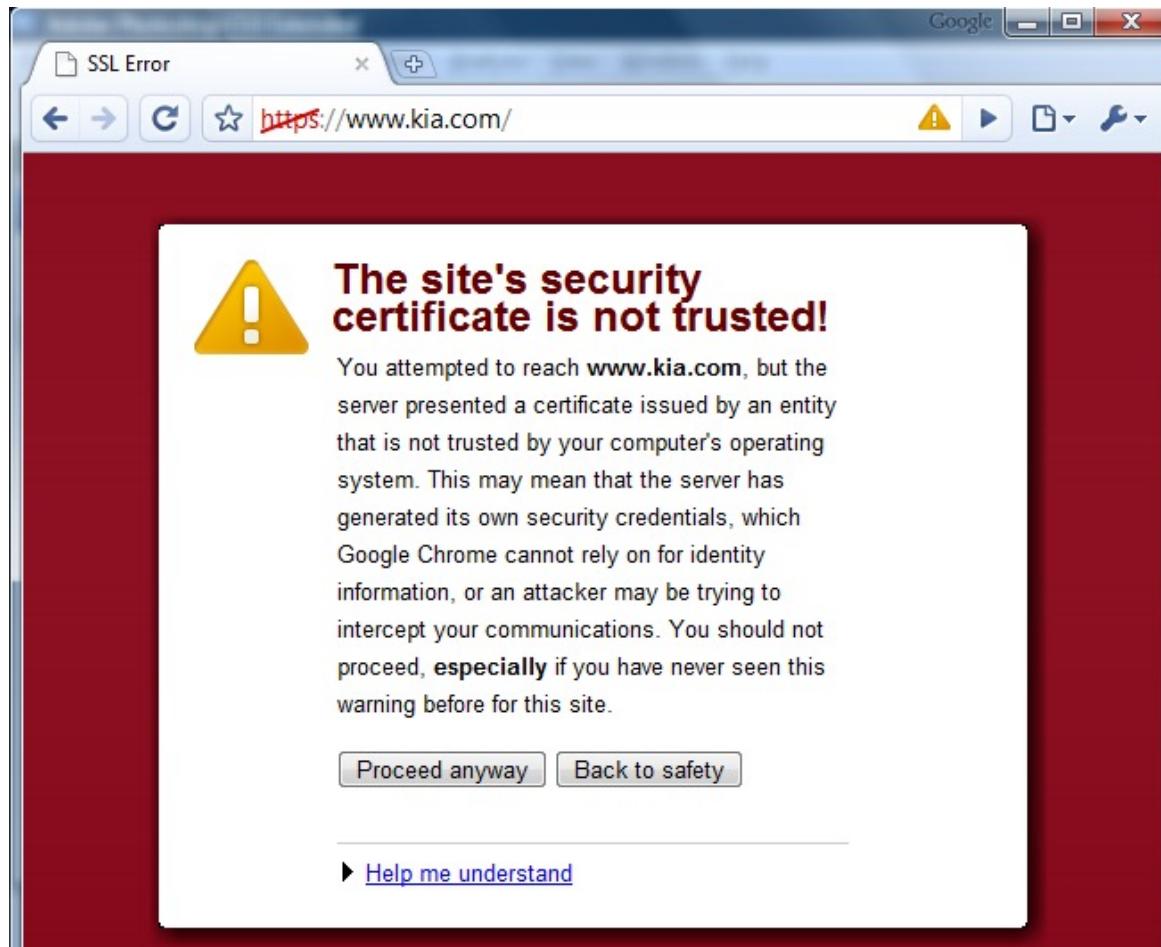
■ Benefits:

- ▶ Avoid some phishing urls
- ▶ Gain: \$loss due to phishing/ user
~ 2.6 minutes per year @ minimum wage

■ Cost:

- ▶ Time spent parsing urls >> 2.6minutes per year

Certificate Errors



Certificate Errors

■ Cost:

- ▼ A lot of confusion
- ▼ Users are trained to ignore such warnings

■ Benefit

- ▼ Could catch MITM attacks
- ▼ Most phishing sites have valid certificates!
- ▼ Certificate error false positive rate: close to 100%

Following Advice May Not be Worth It

- Potential benefit may not be greater than the cost of time spent/inconveniences caused by following security advice
- What to do?
 - ▼ Come-up with better advice
 - ▼ Make it a habit to follow good practices
 - ▼ ...

Take Away Slide

- **Modeling rational choice extremely valuable**
 - ▶ Important conclusions about market processes and behavior of economic agents
 - ▶ Identification of incentive misalignment
- **Careful investigation into characteristics of situation necessary**
 - ▶ E.g., incommensurate resources
- **Models can include aspects of limited rationality**
 - ▶ E.g., near-rational agents
- **Behavioral biases can and should be tested through experimentation**
- **Key concepts:**
 - ▶ Equilibriums
 - ▶ Cost/benefit, externalities
 - ▶ Economics of security

Online Crime

Agenda

- **Overview of online crime**
- **Case studies**
 - ▼ Online sale of drug
 - ▼ How FBI shut down Silk Road
- **Ongoing cyber crime examples**
 - ▼ IRS tax returns
- **Give you an idea of**
 - ▼ Different players involved in online crime
 - ▼ Intervention strategies

Types of Online Crime

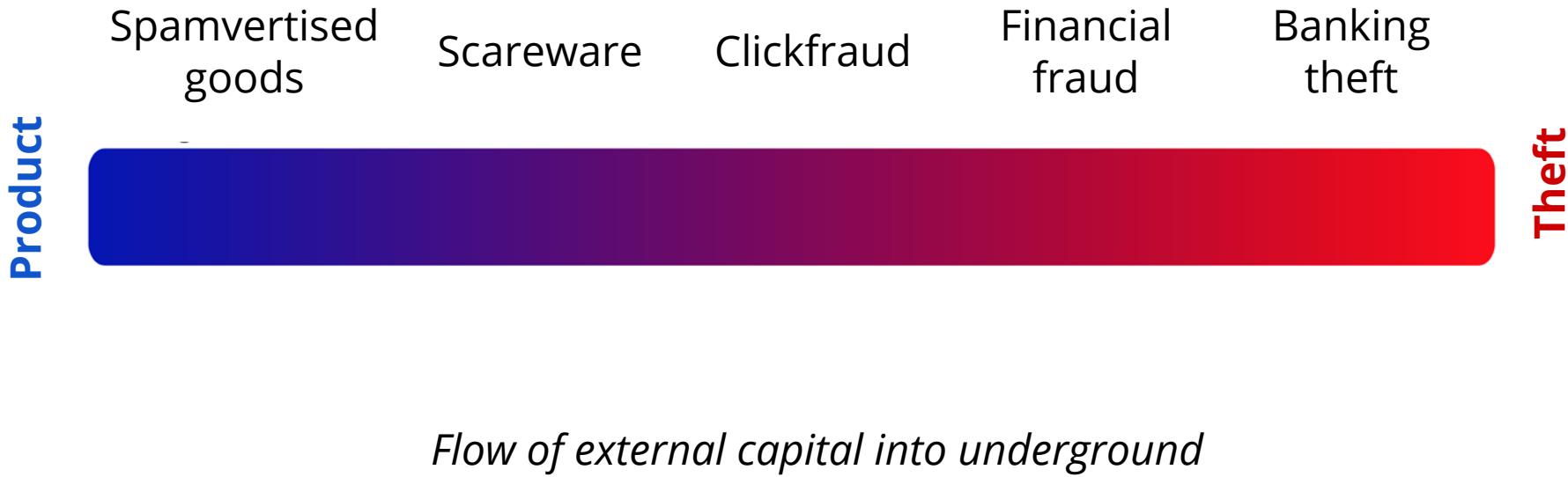
- **Financial Fraud Crimes**
- **Cyberterrorism**
- **Cyberextortion**
- **Cybersex trafficking**
- **Cyberwarfare**
- **Crimes that uses computer as a target**
 - ▼ Malware, DDOS, viruses
- **Crimes that uses computer as a tool**
 - ▼ Fraud, identity theft, Information warfare , Phishing and scam, Threats
- **Obscene or offensive content**
- **Online harassment**
 - ▼ Cyberbullying, Online predator, Cyberstalking, Cyber Racism....
- **Drug trafficking**

Examples: <https://en.wikipedia.org/wiki/Cybercrime>

Online Crime

- **Emergence of underground economy**
 - ▼ Loose federation of specialists selling capabilities, services, and resources explicitly tailored to the abuse ecosystem
- **Streamlines abuse – for a fee**
 - ▼ Commoditization provides access to:
 - ▼ Compromised machinery
 - ▼ Sensitive user data
 - ▼ Human services
 - ▼ Accounts & engagement
 - ▼ Difficult for any single actor to extract all this value

Online Crime – Profit Centers



Online Crime – Support Centers

*Specialized
payloads*

Spambot
Grum, Storm, MegaD

Clickbots
ZeroAccess

Banking trojans
Zeus, SpyEye

*Malware
distribution*

Exploit kits
Nuclear, Blackhole

PPI services
GoldInstall, LoaderAdv

*Traffic
acquisition*

Accounts
Email, social, phishing

SEO, cloaking
Backlinks, websites

*Raw
materials*

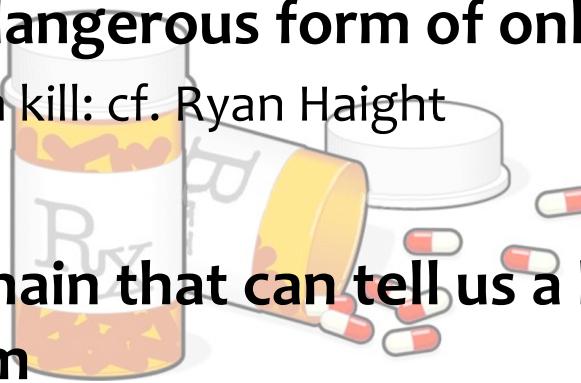
Hosting, networking
Hosts, proxies, domains

Human services
Captcha, SMS, content, mules

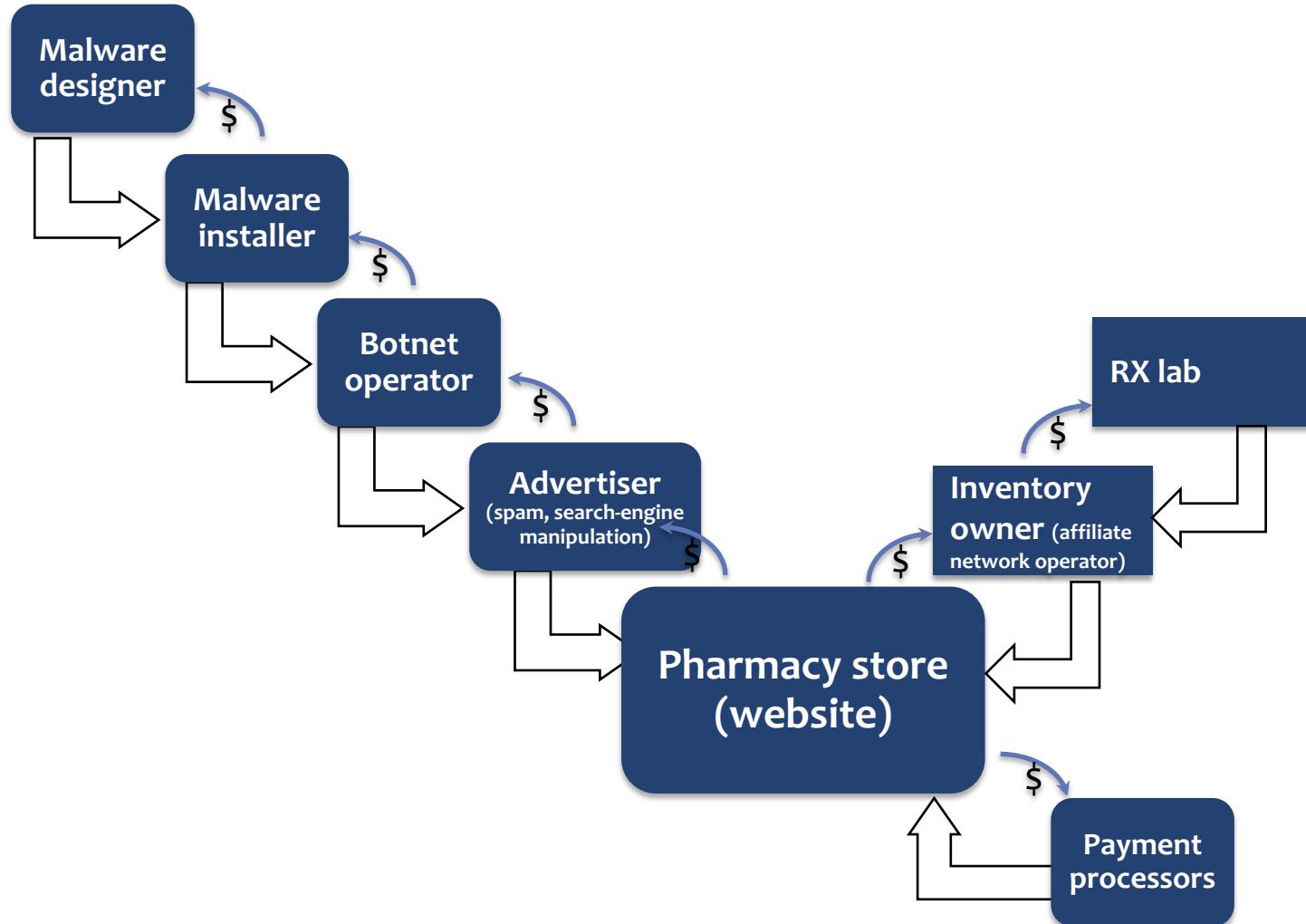
Flow of capital within underground

Case study: Online Sale of Drugs

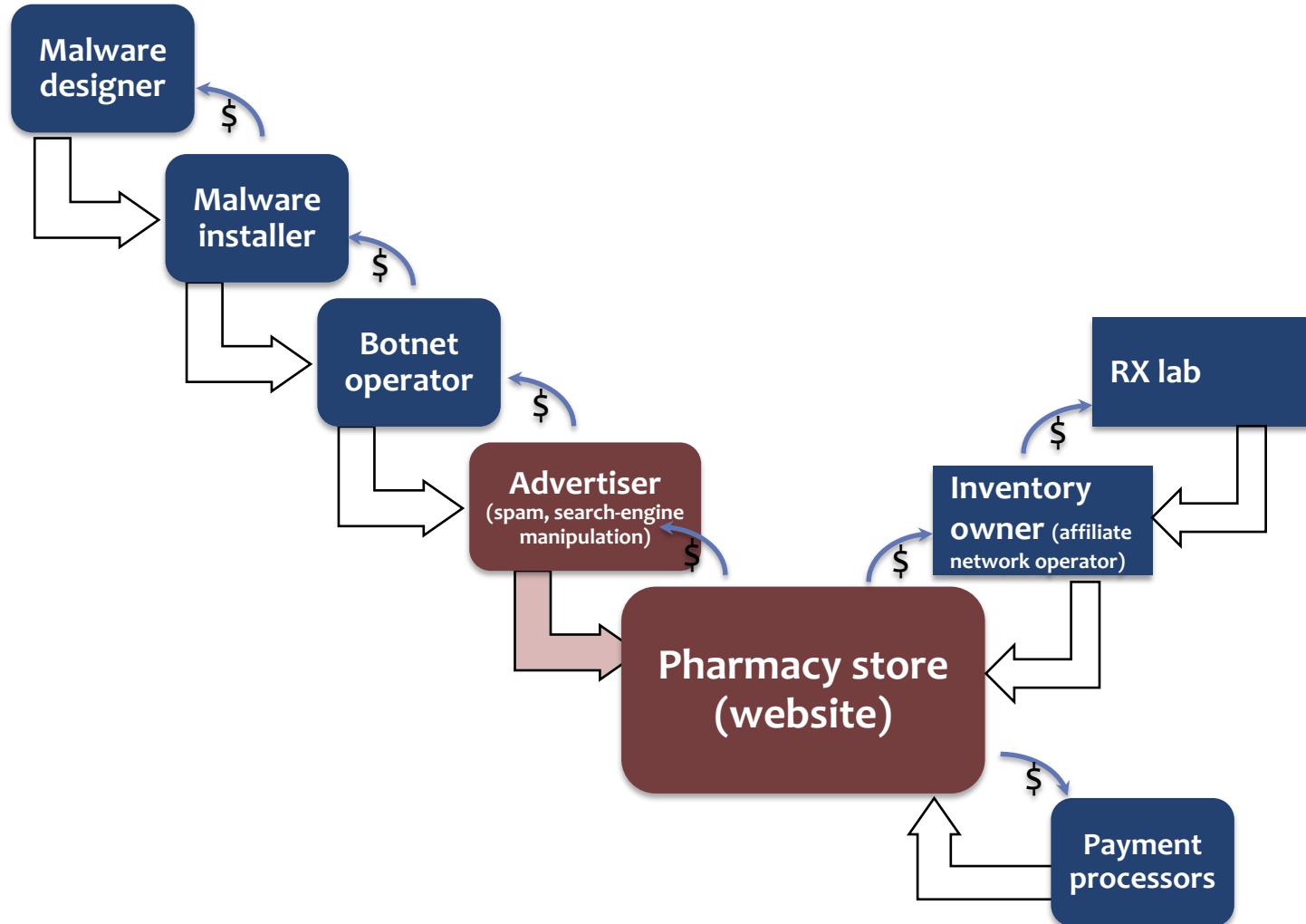
- One of the best known illicit online trades
 - ▼ Who hasn't received email spam for prescription drugs?
- Potentially most dangerous form of online crime
 - ▼ Wrong dosage can kill: cf. Ryan Haight
- Complex supply chain that can tell us a lot about the online criminal ecosystem



Supply Chain: High-Level Overview



Advertising Unlicensed Drugs



Evolution of Advertising of Illicit Products

Email spam has been the primary vector for a long time

Very low conversion rate* (about 1 purchase every 12.5 million emails sent for Rx)

Unsolicited

More recently: social network spam (e.g. Twitter)

Better conversion rate* (Twitter spam: 0.13%)

Posting malicious links via compromised accounts

Exploiting trust relationships

Search engine manipulation

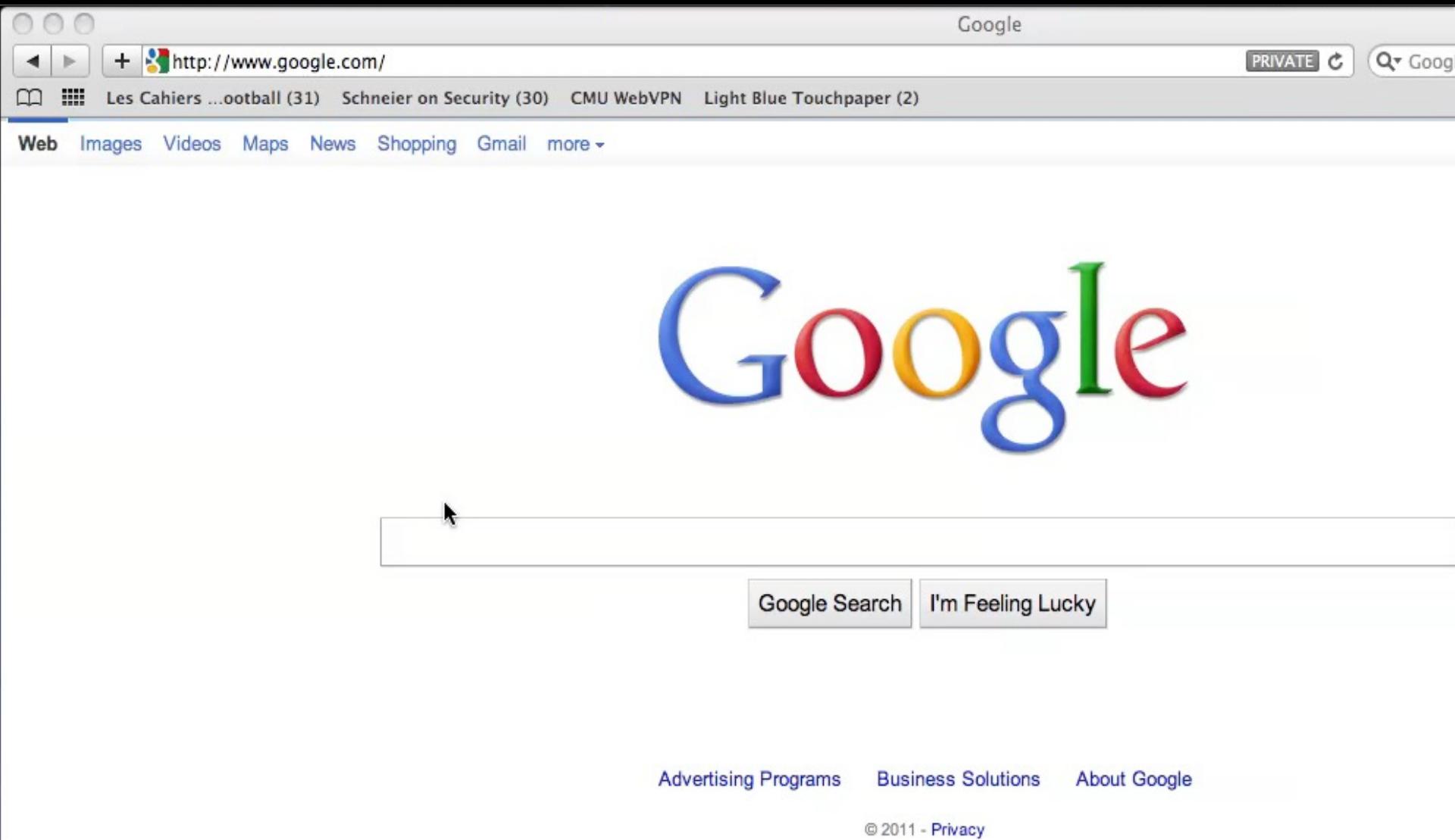
Targeted to users looking for a product

Probably better conversion rates

*Ratio of realized sales over the number of emails/clicks

Original Search-Redirection Attack

[Leontiadis, Moore and Christin, USENIX Security 2011]



Original Search-Redirection Attack

[Leontiadis, Moore and Christin, USENIX Security 2011]

cialis without prescription

About 28,400,000 results (0.11 seconds)

Cialis Without Prescription What And Generic - Online Drug Store ...

Cialis Without Prescription What And Generic. Online Pill Store. Big Discounts. FDA regulations prohibit us from accepting returned medications from a ...

[cgi.media.mi.edu/](http://cigi.media.mi.edu/) - Cached - Similar

Buy Cialis Online Without Prescription

Buy Cialis Without Prescription! Lowest Prices and Satisfaction Guaranteed! Only \$1.99 Per Pill, Bonus 4-12 FREE Pills with all Orders, ...

www.oneboyonegirl.com/ - Cached - Similar

NMSU Library: Research

Research Guides & Help »; Subject & Course Guides »; Subject Specialists »; more ... Services · Renewals »; Request It! » Reserves »; more. ...

lib.nmsu.edu/research.shtml - Cached - Similar

Water-spider orchid | Center for Aquatic and Invasive Plants

Feb 8, 2008 ... Habenaria repens. Native to Florida. Video ID segment (2-3 minutes) You will need Adobe Flash installed to view this video ...

plants.ifas.ufl.edu/node/173 - Cached - Similar

Cialis without prescription - Buy Drugs Online Without Prescription!

Feb 15, 2009 ... Cialis without prescription. Biggest Online Pharmacy Center. No prescription needed. Fast delivery. 24h online support. Special prices!

www.darkroomstudios.com/ - Cached - Similar

Office of the CIO - Gateway

Telephone Services for South Campus Gateway Apartments. OIT is a department of The Ohio State University and the contracted provider for telephone, ...

units.osu.edu/gateway/index.php - Cached - Similar

Buy Drugs Without Prescription. No Prescription Needed Online Pharmacy

buy cialis without prescription, buy viagra no prescription needed, buy levitra without prescription, buy xanax no prescription needed ...

www.peopleprescription.com/ - Cached - Similar

cialis without prescription - Campus Health Services - Home

campushealth.unc.edu/index.php?option=com_content... - Similar

- Only two of the results actually belong to online pharmacies. The rest are unrelated .com or .edu sites that had been compromised to redirect to online pharmacies, or have been populated with spam
- The origin of the click: Referrer field is set to:
`http://www.google.com/search?q=cialis+without+prescription.`

Online Criminal Market-Place

■ A lot of dark market-places

- ▶ Silk Road
- ▶ Agora
- ▶ Utopia
- ▶ TheRealDeal
- ▶ Alpha bay
- ▶ ...

■ Early adopters of technology

- ▶ Tor hidden service
- ▶ Bitcoin

Silk Road—Beginning

■ **Jan 1, 2011**

An unknown individual using the alias 'altoid' begins posting on internet forums shroomery.org and bitcointalk.org, advertising a hidden Tor service like an "anonymous amazon.com."

■ **March 1, 2011**

Messages on Bitcoin Talk: Silk Road has been operational for 3 weeks

■ **April 11, 2011**

Silk Road hits 1000 users

Silk Road—Trails

■ Oct. 11, 2011: Altoid Looks For a Bitcoin IT Pro

Bitcoin Talk user 'altoid' (alleged to be the same altoid who originally announced Silk Road's presence) posts a job ad for an "IT pro in the Bitcoin community" to work in a "venture-backed Bitcoin startup company". Interested parties are asked to write to "**"rossulbricht at gmail dot com."** Allegedly, this post links 'altoid' to Ross Ulbricht, putting him under the authorities' suspicion.

Silk Road—Trails

■ **Feb. 5, 2012: Dread Pirate Roberts**

On Silk Road forums, user "Silk Road" announces "I need an identity separate from the site and the enterprise of which I am now only a part. I need a name. Drum roll please..... my new name is: Dread Pirate Roberts". This becomes the official forum mouthpiece for Silk Road.

■ **Nov. 11, 2011: Dread Pirate Asks Stackoverflow For Tech Tips**

Someone creates an account on programming advice site StackOverflow.com with the name 'Ross Ulbricht' and email address **rossulbricht@gmail.com**.

- ▼ The curl script posted in the above Stack Overflow question is identical to code obtained from one of the Silk Road servers.

Silk Road—the End

- July 23, 2013
The FBI Gets An Image of The Silk Road Server
- July 24, 2013—July 31, 2013
Homeland Security Confronts Ulbricht
- Oct. 1, 2013
Ulbricht is Arrested
- Oct. 2, 2013
Silk Road Seized By Law Enforcement
bitcoin value crashes
vendors arrested

Silk Road—Subpoenas

- A subpoena to Google provided information about the account holder
 - ▼ details of IP addresses used to log into Mr Ulbricht's account (San Francisco, specifically an internet cafe on Laguna Street)
 - ▼ IP address is a VPN server
- VPN server's records were obtained by FBI
 - ▼ VPN server's records indicated a user had accessed it from a San Francisco Internet café near the home of a friend Ulbricht had gone to live with
- The FBI Gets an Image of The Silk Road Server
 - ▼ hosting provider at the request of the FBI via local authorities and the Mutual Legal Assistance Treaty.

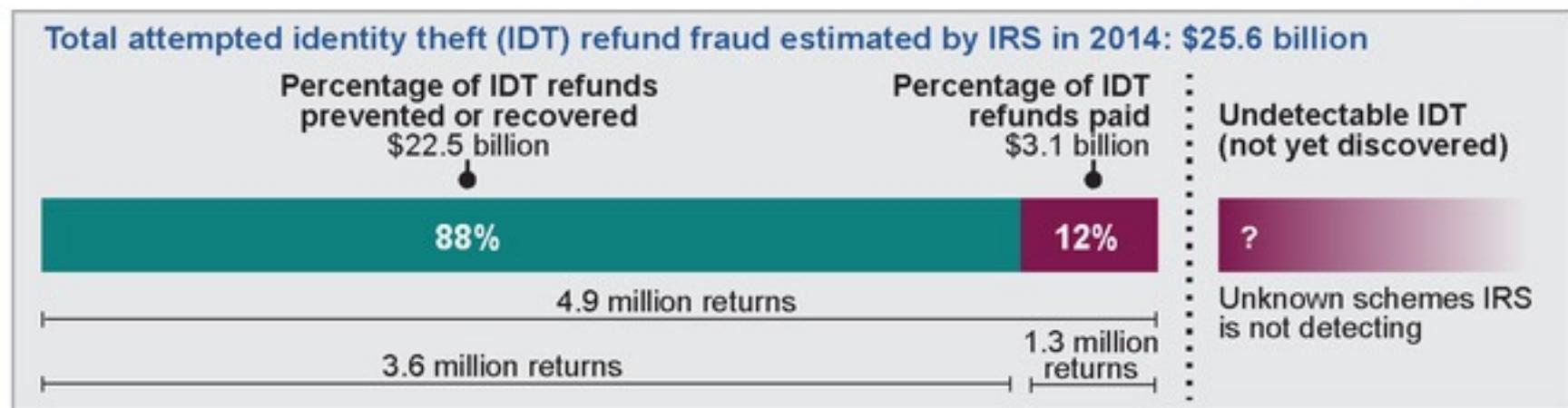
Silk Road—Gaps?

- FBI claimed it was because of a misconfiguration of the site's CAPTCHA, which inadvertently revealed Silk Road's IP address.
 - ▶ Doubts about this claim
 - ▶ Someone claim the attack on Tor around the same time is related

Other Examples: Tax Refund Fraud

■ Race to file tax returns

IRS Estimates of Attempted Identity Theft Refund Fraud, 2014



Source: GAO analysis of IRS data. | GAO-16-578T

Other Examples: Ransomware

■ Possible reuse of intelligence agency tools

The image consists of two side-by-side screenshots. On the left, a screenshot of a medical software interface titled 'medRAD' shows a ransomware overlay. The overlay has a red header 'Oops, your files have been encrypted!' and several sections of text. It includes a padlock icon, a progress bar for payment, and a progress bar for file loss. It also contains a section about Bitcoin payment and a 'Contact Us' button. On the right, a screenshot of a Twitter post from the account @Merck. The tweet reads: 'We confirm our company's computer network was compromised today as part of global hack. Other organizations have also been affected (1 of 2)'. It is timestamped at 10:03 AM - Jun 27, 2017.

medRAD

Oops, your files have been encrypted!

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 enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>. 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'll 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 bitcoins>. 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.

Send \$300 worth of Bitcoin to this address:
B bitcoin
ACCEPTED HERE
12ABM4VW2dhxYgXeQepoHkHSQuy6NgaEb84
Copy

Contact Service

Your files will be lost on 5/15/2017 03:02:31
Time Left: 02:19:34:29

Your files will be lost on 5/15/2017 03:02:31
Time Left: 05:19:34:29

Events

Patient ID: _____
DOB: _____
Weight: _____

Procedure: _____

Accession: _____

Fluids

Fluid A: _____
Fluid B: _____

Events

Start Date: _____
How to Start Date? _____
Contact Us

Patient Worklist

Status

341

Merck
@Merck

We confirm our company's computer network was compromised today as part of global hack. Other organizations have also been affected (1 of 2)

10:03 AM - Jun 27, 2017

to the operations manual or the internet at:
<http://www.radiology.bayer.com>

Other Examples: NFT Frauds

■ NFT: Non-Fungible Token

- ▶ Unique token with a unique digital signature on the blockchain
- ▶ Part of the Ethereum blockchain
 - ▶ Other blockchains can have their NFT versions
- ▶ Not a cryptocurrency, but you can buy an NFT with bitcoin...

■ NFT communities increased in popularity

■ The promise: make money of digital artwork

- ▶ Can be used for images, video music, drawing, etc.
- ▶ Built-in authentication for proof-of-ownership
 - ▶ Monet print vs. The original Monet

■ Online crime increases when there is a financial incentive!

Other Examples: NFT Art Fraud

■ An artist was impersonated

- ▼ Fake artist followed a verification process
- ▼ Listed NFTs of original artist for sale

■ Platforms rely on original artist to find out and report

Chelsea E. Manning 
@xychelsea

non fungible tokens (NFTs) have no inherent value and not even technologically innovative — they require the pre-existing system of violence and control to enforce a belief in the value of what is ultimately a glorified checksum

11:39 AM · Mar 16, 2021

12.6K 209 Copy link to Tweet

Tweet your reply

<https://www.theverge.com/2021/3/20/22334527/nft-scams-artists-opensea-rarible-marble-cards-fraud-art>

Takeaway

- Online crime is increasing in magnitude
 - ▼ Search-redirection for online pharmacies:
 - ▼ top 12 clusters account for 2/3 activity
 - ▼ Few, large, traffic brokers
 - ▼ Large number of participants perhaps induced by these “big shots”
 - ▼ This plays to the advantage of the defender!
 - ▼ Disrupt dependencies of the underground market
- Darknets
 - ▼ Use Tor hidden service
 - ▼ Police manage to collect enough information to shut down many
 - ▼ Now at Silk Road 3.1
- New approaches being created