

Exercise for next week

Think about and jot down answers to the following questions about how to prevent investment fraud.

- 1. Who are the stakeholders in investment fraud?
- 2. What are the most common mechanisms to prevent investment fraud?
- 3. Do they work? Why?
- 4. What are possible mechanisms that can help prevent investment fraud

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS	
Crime Type	Loss
Investment	\$6,570,639,864
Business Email Compromise	\$2,770,151,146
Tech Support	\$1,464,755,976
Personal Data Breach	\$1,453,296,303
Non-Payment/Non-Delivery	\$785,436,888
Confidence/Romance	\$672,009,052
Government Impersonation	\$405,624,084
Data Breach	\$364,855,818
Other	\$280,278,325
Employment	\$264,223,271
Credit Card/Check Fraud	\$199,889,841
Identity Theft	\$174,354,745
Real Estate	\$173,586,820

Who is the Opponent?

INFR11208 (UG4) // NFR11228 (MSc)



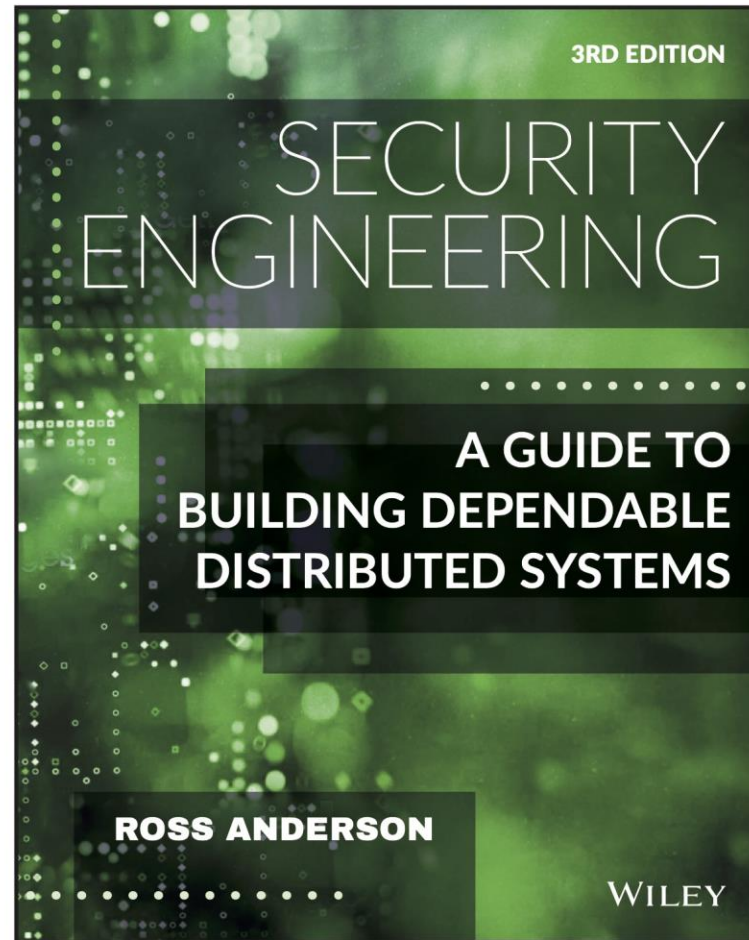
Daniel W. Woods
Email: daniel.woods@ed.ac.uk

Warning: Politics & Security

- Who is targeted is often political
 - Nation states targeting each other (espionage)
 - Nation states targeting civilians (surveillance)
 - Civilians targeting civilians based on all kinds of politics (activism/extremism)
 - Civilians + NGOs targeting nation states (hacktivism)
- Good security engineers understand that threat models often include political actors

That said, I will never intentionally ask you to make a political judgement. I will try not to share my own.

Chapter 2 - Who is the Opponent?



Why threat modelling matters



Why capabilities matter

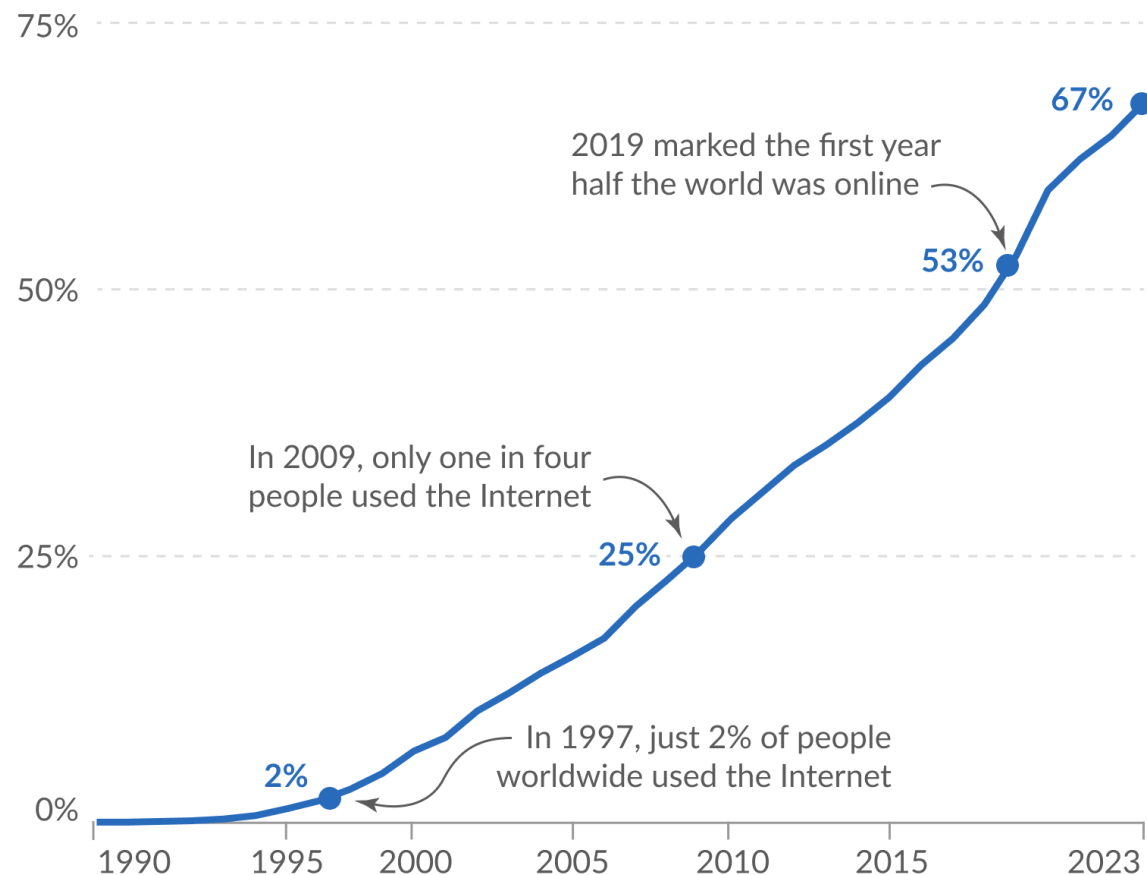


Why digital threat modelling is hard

Most of humanity has been connected to the Internet for only a brief moment in history

Our World
in Data

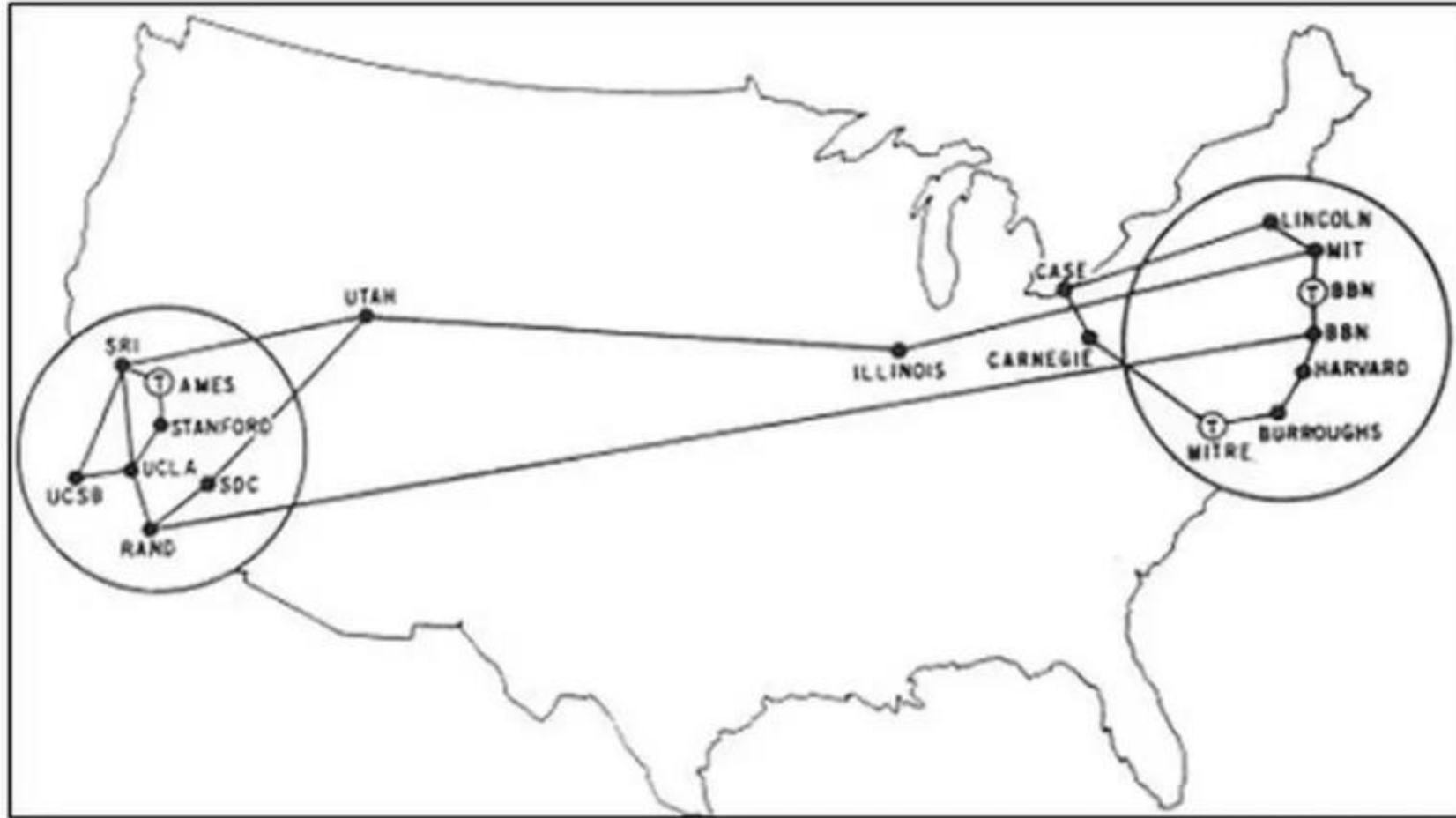
Share of the global population who used the Internet in the last 3 months using a computer, phone or any other technological device.



Data source: International Telecommunication Union (via World Bank)

CC BY

Core infra designed for another threat landscape



By 1971, Arpanet connected the east and west coasts of the US, but did not go beyond

<https://www.bbc.co.uk/news/technology-35579225>

Why pay attention to the opponent?

"Security engineering is about building systems to remain dependable in the face of **malice**, error and mischance."

Defenders face different threat actors, and those threat actors have different capabilities:

- Firewalls don't work against actors with firewall vulnerabilities
- Perimeter controls don't work against a malicious insider
- Intimate partners know the answers to password recovery questions
- Not much works against the intelligence community

This lecture

Who are the opponents? What are their tools/capabilities?

1. Criminals (the crooks)

- Ransomware gangs, botnet operators, fraud gangs, malicious insiders

2. State actors (The spooks)–

- Five eyes; Russia; China; third-tier

3. Lawful operators (The geeks) –

- Employees, security researchers, competitors

4. The swamp

- hate crimes, sex abuse, bullying

Further reading: Security Engineering chapter 2

The crooks

Financially-motivated actors willing to break the law

The boundaries of cyber vs traditional crime

Online highs are old as the net: the first e-commerce was a drugs deal

Mike Power

Ever since the 1970s, drug users have employed chemistry and telecommunications to stay several steps ahead of the law



Through the 70s, 80s and 90s, all manner of drugs – both legal and illegal – were sold online.
Photograph: Ted S Warren/AP

Discuss and come up with an example of each

1. Cyber-Dependent Crime

These are "true" cybercrimes that **can only be committed using computers**. The device is both the tool and the target.

2. Cyber-Enabled Crime

These are traditional crimes that are **increased in scale, speed, or reach** by the use of technology.

3. Cyber-Assisted Crime (or Computer-Supported)

Crimes where the computer is **incidental** to the criminal activity.

Cyber dependent crime vs cyber enabled crime

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss
Investment	\$6,570,639,864
Business Email Compromise	\$2,770,151,146
Tech Support	\$1,464,755,976
Personal Data Breach	\$1,453,296,303
Non-Payment/Non-Delivery	\$785,436,888
Confidence/Romance	\$672,009,052
Government Impersonation	\$405,624,084
Data Breach	\$364,855,818
Other	\$280,278,325
Employment	\$264,223,271
Credit Card/Check Fraud	\$199,889,841
Identity Theft	\$174,354,745
Real Estate	\$173,586,820

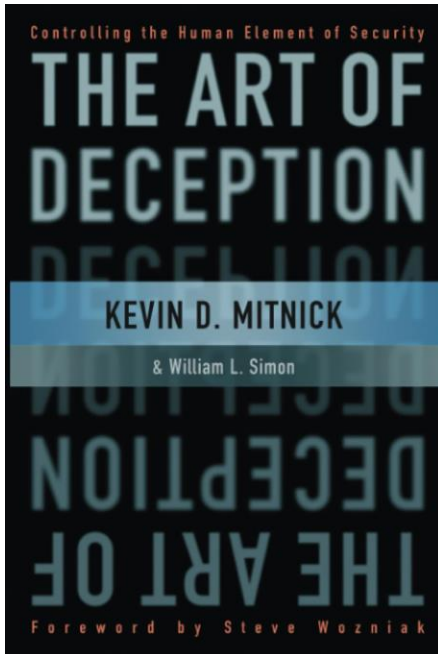
-  **Social engineer individuals**
-  **Social engineer business,**  **sometimes via hack**
-  **Social engineer individuals**
-  **Mostly remote hacking**
-  **Defraud ecommerce buyers (mail order fraud as a comparison)**
-  **Social engineer individuals (digital sweetheart scam)**
-  **Social engineer individuals**
-  **Mostly remote hacking**
-  **Weird but not remote hacking**
-  **Auth failures, but not via remote hacking**
-  **Auth failures at banks,**  **using data from hacking**
-  **Social engineer renters/house buyers**

Revision Challenge: Get a clean version of this list and try to map this on your own by looking up definitions

Cyber-enabled crime capabilities (FRAUD)

Core/necessary capabilities

Other capabilities



Types of money mules



Unknowing individuals

are unaware they are part of a laundering scheme. These could be victims of online romance schemes or fake job offers.



Witting individuals

willfully ignore red flags or turn a blind eye to their money-laundering activity. They usually get paid.



Complicit individuals

are professional money mules who are trained to subvert financial institutions and law enforcement.



- Access to leaked data to establish trust
- Organizational capital, e.g. crime playbooks
- Technical capabilities, e.g. to build/contract fake websites
- People trafficking, e.g. to have real people for romance fraud and/or people to run scams

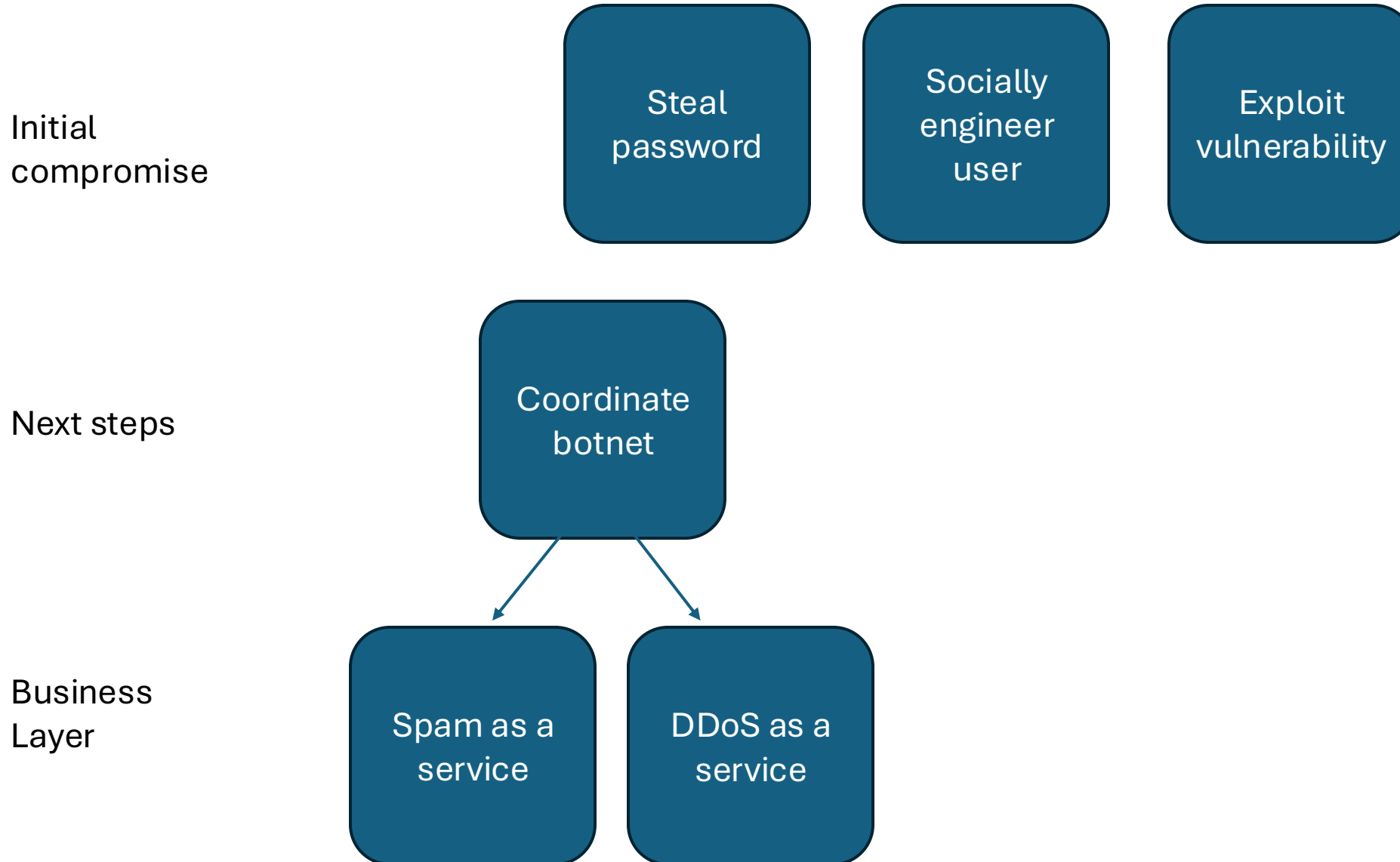
Feds seize \$15 billion in crypto from 'pig butchering' scheme involving forced labor camps

OCT 14, 2025 ✓

By  Kara Scannell

Don't be fooled. Most cyber frauds are run by serious crime organizations.

Cyber Dependent Crimes around ~2003



Cyber-dependent crime: DDoS for hire

September 14, 1996

New York's Panix Service Is Crippled by Hacker Attack

By ROBERT E. CALEM

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

Capabilities

- A network of computers to flood a system with traffic
 - Later DDoS for hire emerged (Booter as a service)
- Some cash out mechanism
 - It's easier to cash out when the adversary pays you than the victim. **Why?**

Who is targeted by DDoS?

- Extortion attempts have largely failed
- Largely a crime of passion linked to "revenge" targeting
 - Cyber crime researchers
 - Countries who "offended" other countries
 - Gamers
- Fascinating quant approach "back scatter analysis"
 - "for direct denial-of-service attacks, programs spoofing their address typically select source addresses at random for each packet sent"
 - "attacks against home machines ... constitute relatively large, severe attacks .. One explanation is that minor denial-of-service attacks are being used to settle personal vendettas."

Source: Moore, David, Colleen Shannon, Douglas J. Brown, Geoffrey M. Voelker, and Stefan Savage. "Inferring internet denial-of-service activity." ACM Transactions on Computer Systems (TOCS) 24, no. 2 (2006): 115-139.

DDoS attack takes down Krebs site

News
Sep 23, 2016 • 4 mins



Attack was so powerful that Akamai threw up its hands



Credit: Thinkstock/Stephen Sauer

World news

This article is more than 18 years old

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

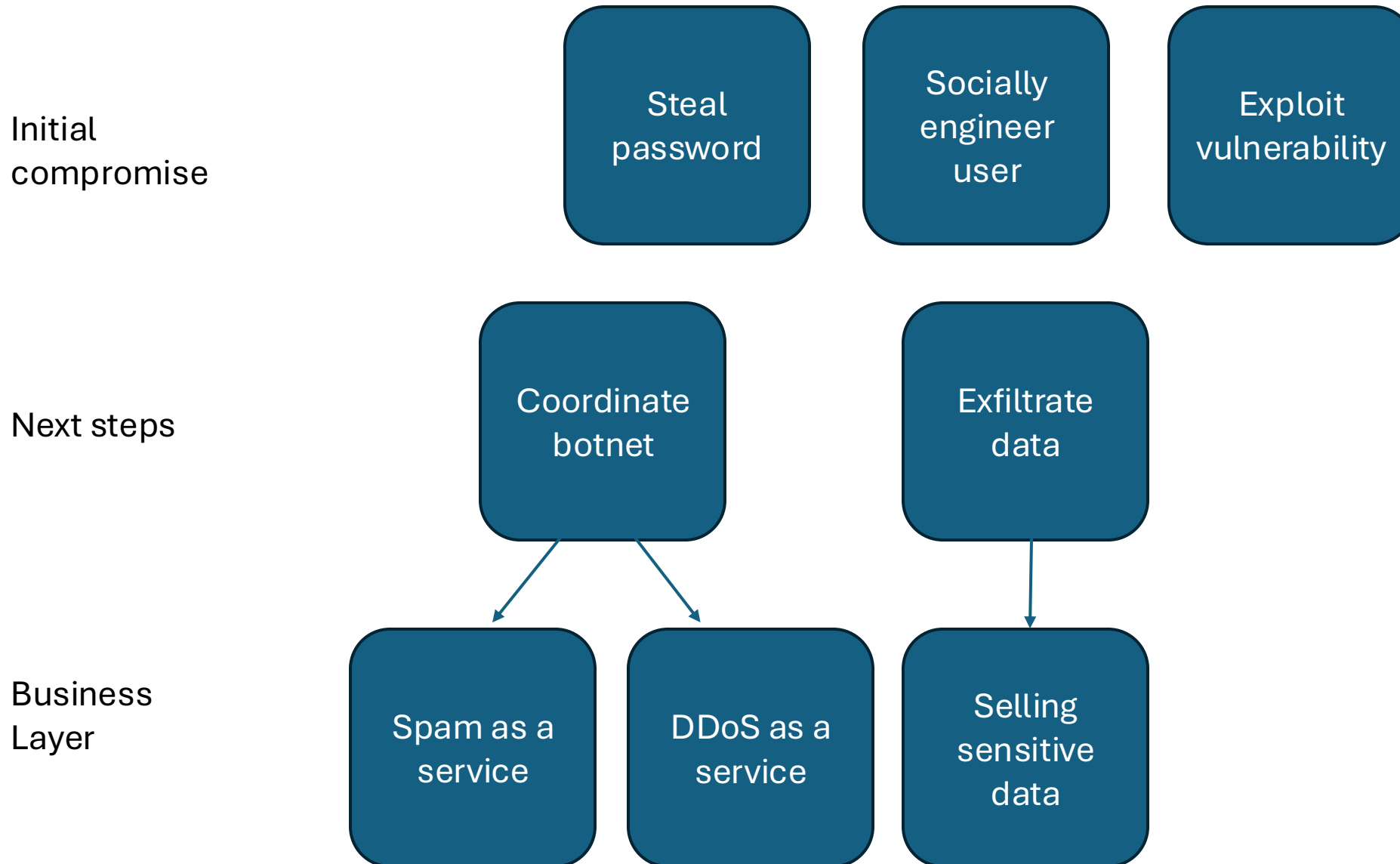


Ian Traynor in Brussels

Thu 17 May 2007 02:32 BST

Share

Cyber Dependent Crimes in ~2005



Cyber-dependent crime: Info stealing + selling

Capabilities

- Access to a network or machine with sensitive data
 - In the 2005—2015, this meant large retail firms for credit card data
 - Increasingly "info stealer" malware focuses on harvesting credentials
- A market to find a buyer, plus a cashout mechanism
 - [DoJ: Forums change everything](#)

Who is targeted?

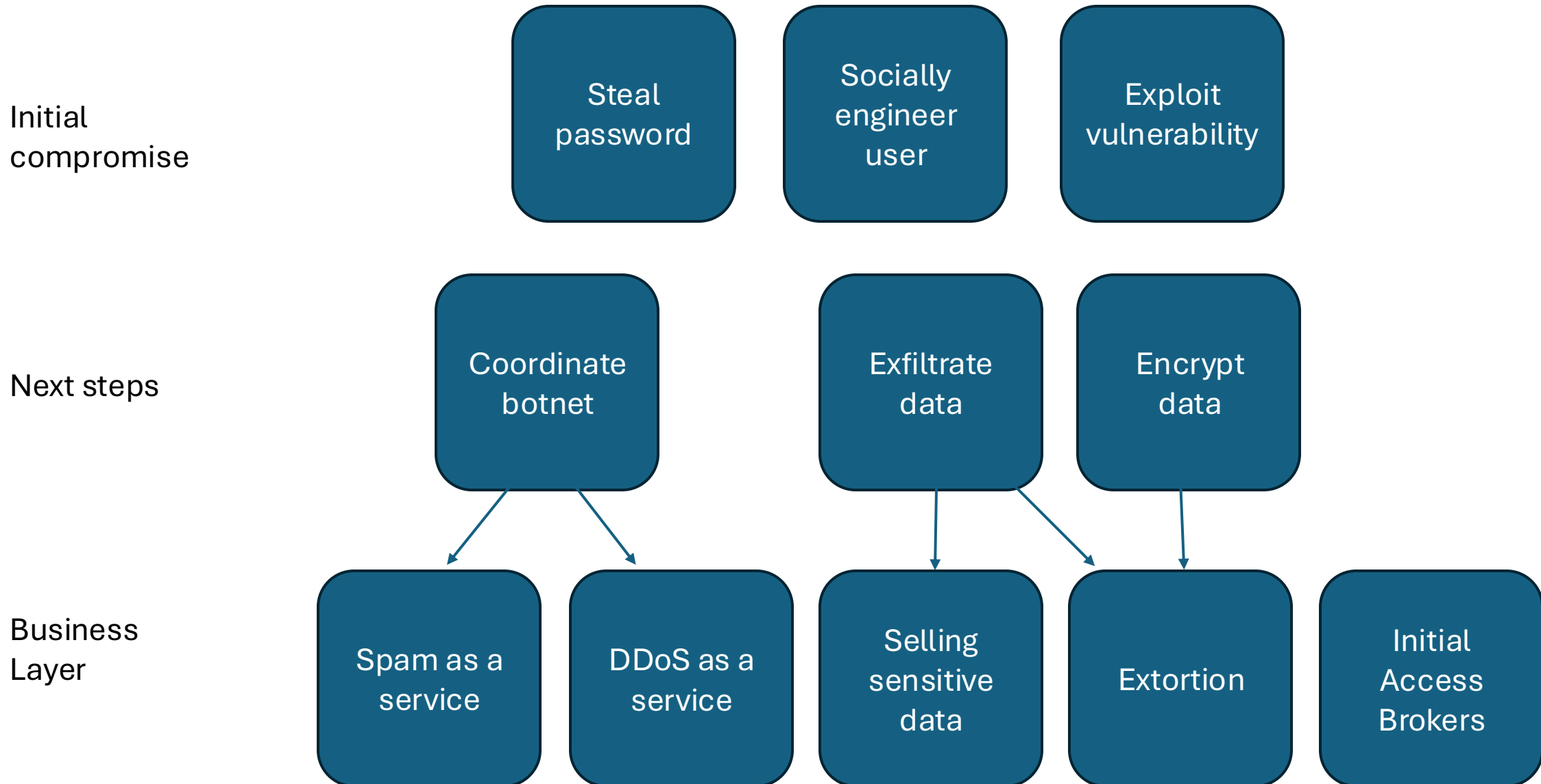
Firms with PII + card data



<http://deepstrike.io/blog/dark-web-data-pricing-2025>

- "Standard U.S. credit card with CVV sells for \$10 to \$40. A card with a verified high credit limit, such as \$5,000, can be priced at \$110 to \$120"
- "A low balance account might sell for \$200 to \$500, but credentials for a high balance account can easily command \$1,000 or more."

Cyber Dependent Crimes since 2015



Cyber-dependent crime: Extortion

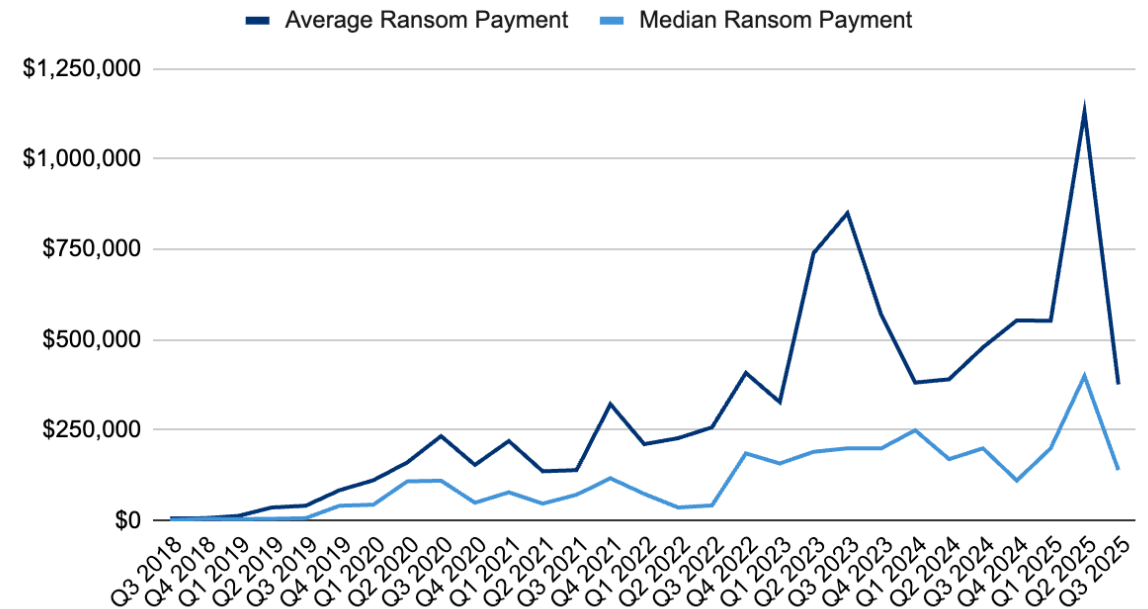
Capabilities

- Access to a network or machine
- Encryption software and/or exfiltration
- Negotiation skills
- Cash out

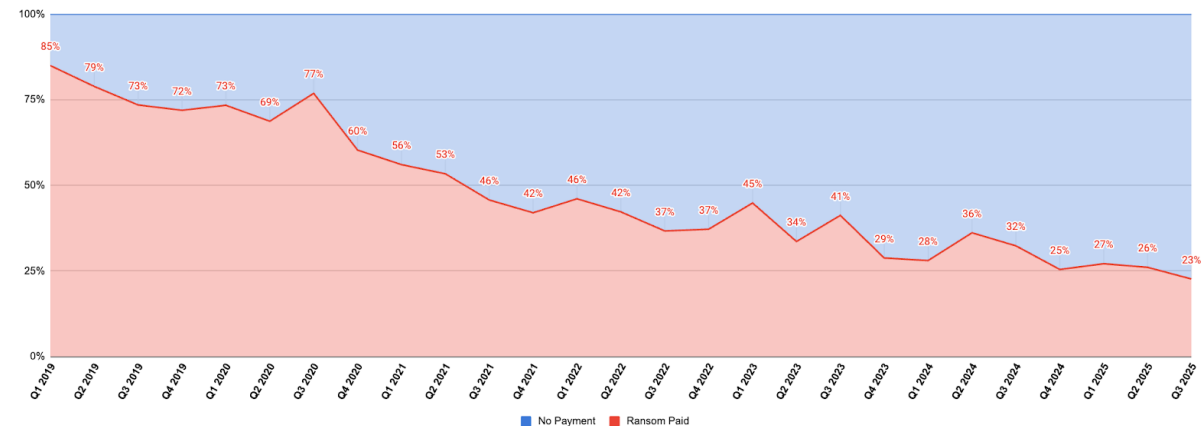
Who is targeted?

More or less everyone!

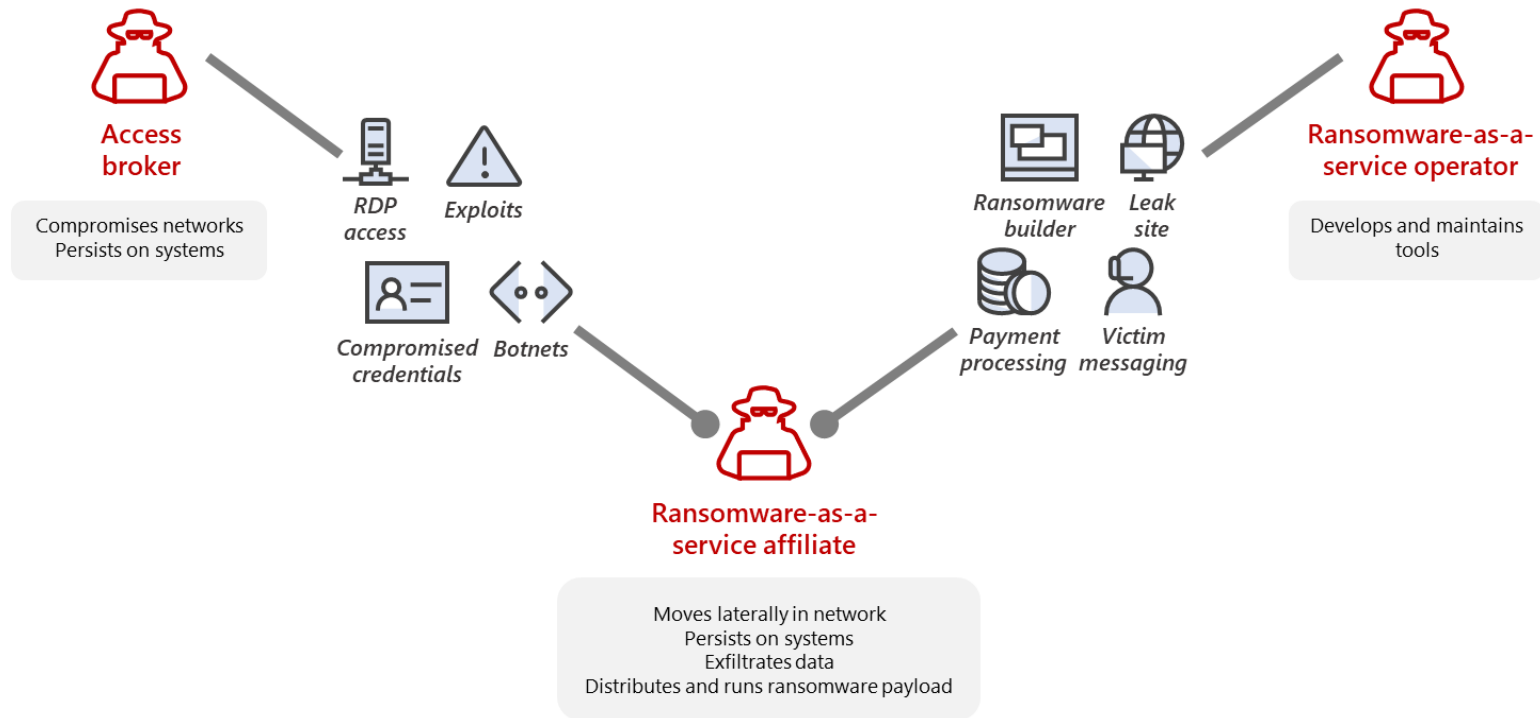
Ransom Payments By Quarter



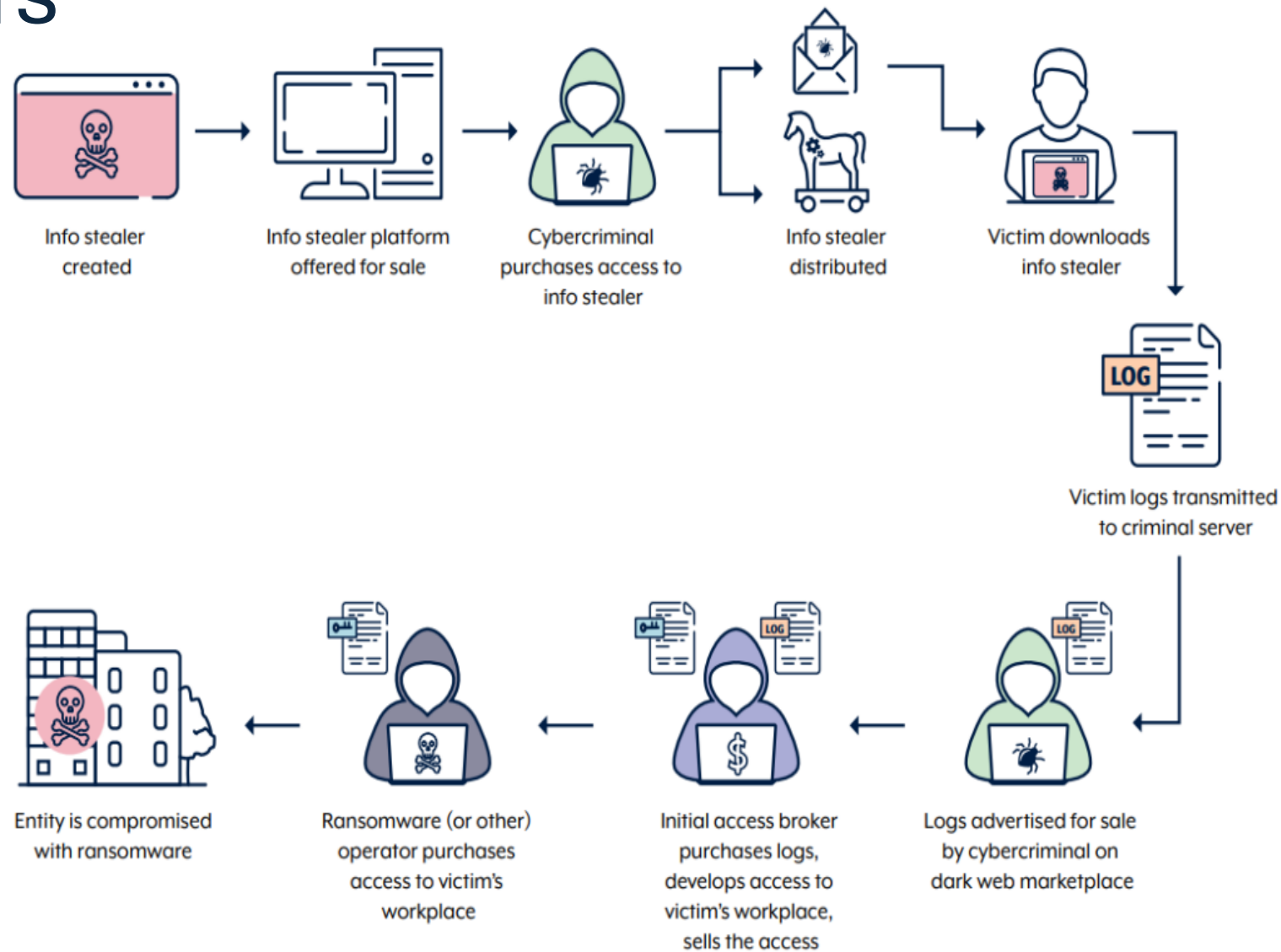
All Ransomware Payment Resolution Rates



Specialization and cyber crime

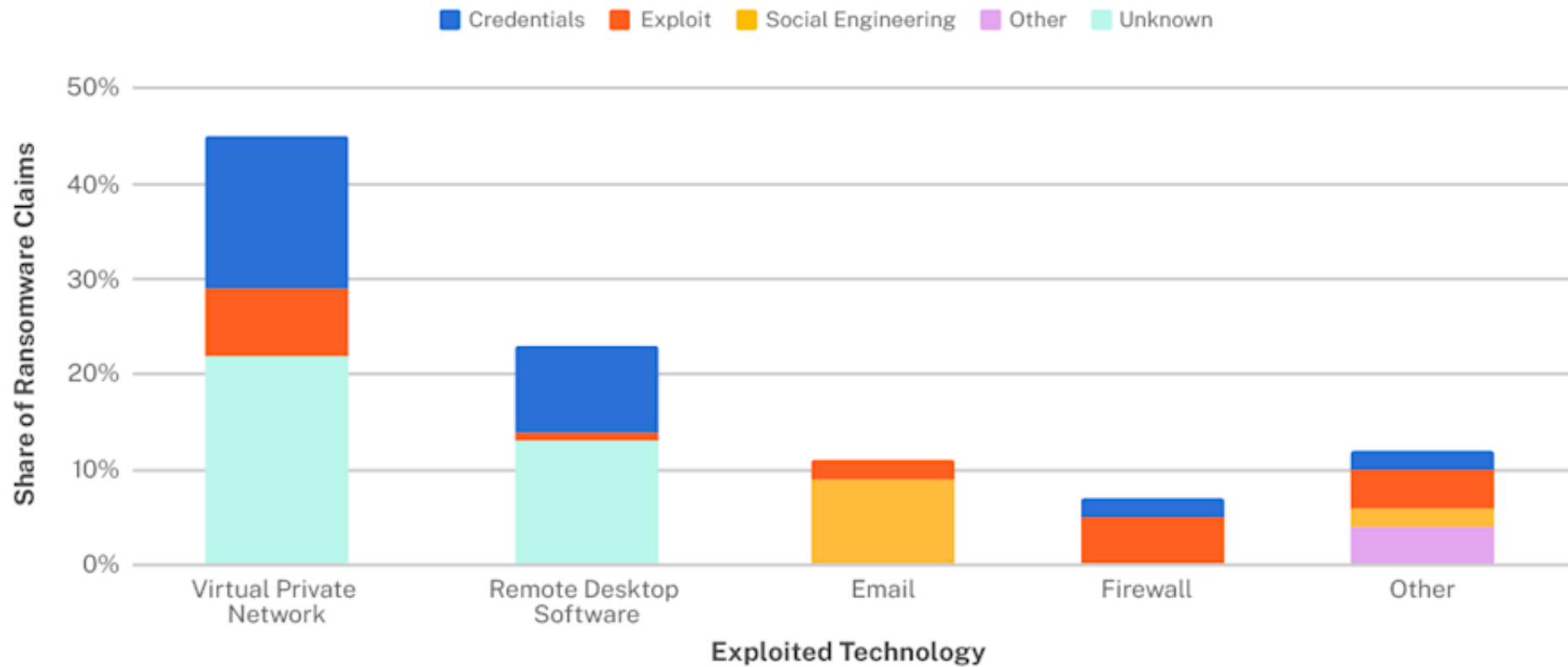


Infostealers

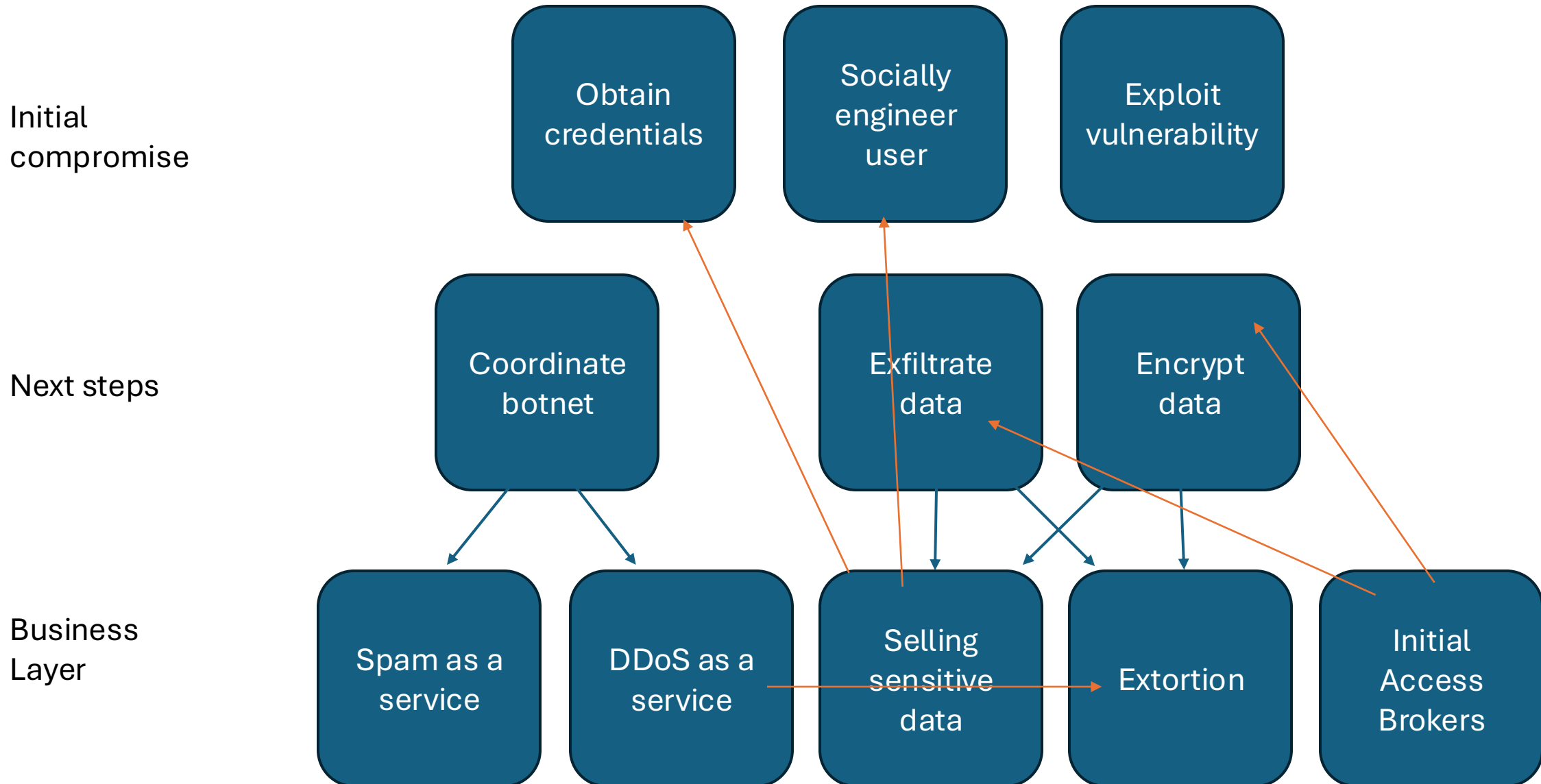


How ransomware gangs get access

Known Initial Access Vectors for Ransomware Claims



Cyber Dependent Crimes



The spooks

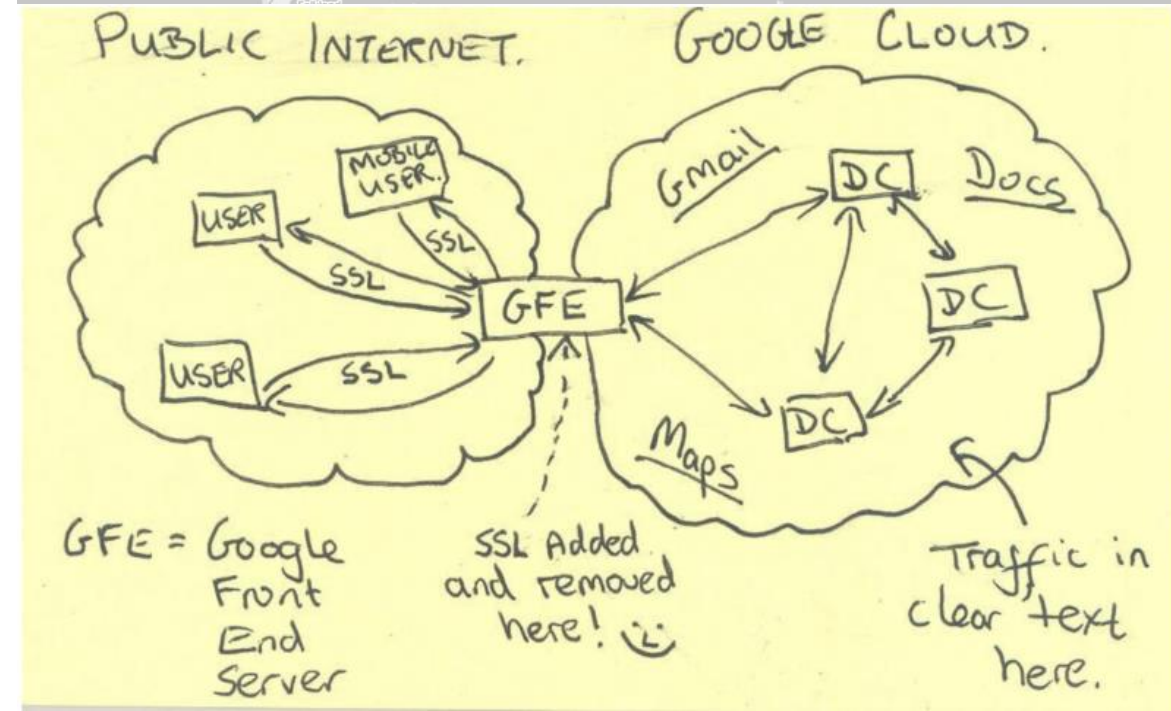
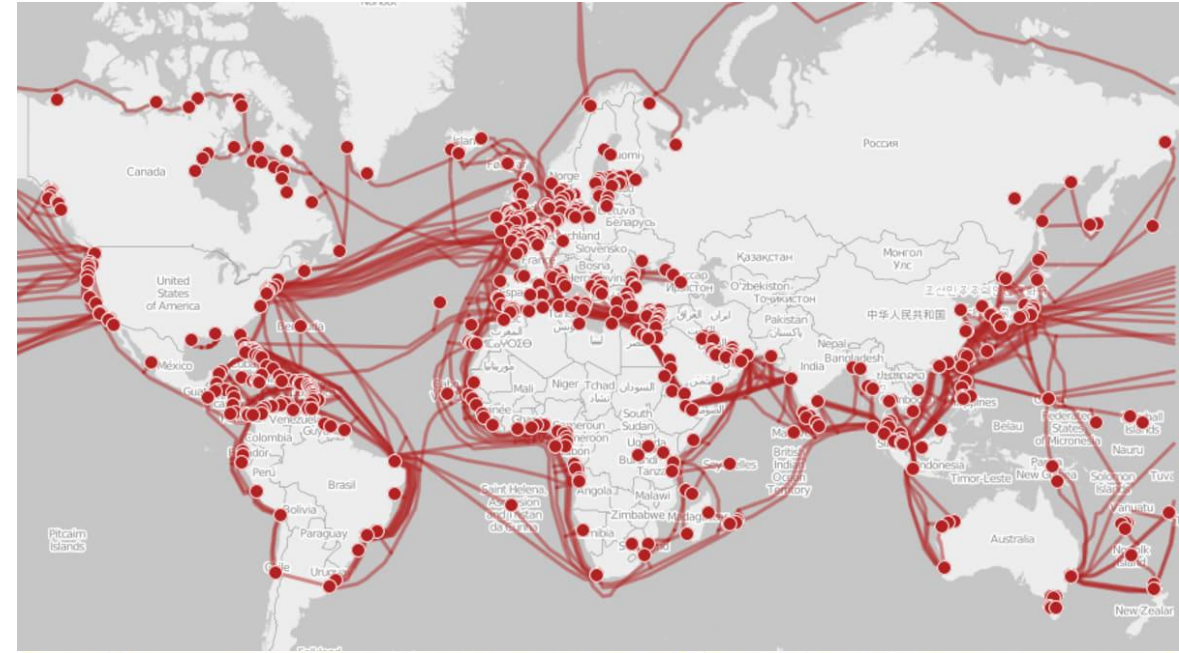
Politically-motivated actors with near endless resources

The Five Eyes

- USA, UK, Canada, Australia and New Zealand share intelligence infra

Capabilities

- PRISM "downstream" access to internet company data
- Combined with "upstream access" via satellites and cables (e.g. Cornwall, Gibraltar etc)
- Computer network exploitation (CNE) hacking, both bulk and targeted
 - 0-day vulns (see Shadow Brokers)



The Five Eyes

Who is targeted?

- Hostile states, terror suspects
- Domestic politics
 - Typically focused on "extremists", but who defines that?
- Even allies targeted
- Own citizens, typically required warrant:
 - probable cause for US persons, typically requested by the FBI
- Less oversight for foreign targets
 - Your citizens are foreign to your allies...

U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR

By Reuters

May 31, 2021 5:09 PM GMT+1 · Updated May 31, 2021

Germany eavesdropped on some Obama calls from Air Force One, book says

Germany's foreign intelligence agency, the BND, intercepted some unencrypted calls around the same time the U.S. was spying on Chancellor Angela Merkel, a new book reveals.

January 5, 2026

GCHQ's mass data interception violated right to privacy, court rules

Human rights judgment follows legal challenge begun in 2013 after Edward Snowden's whistleblowing revelations

Haroon Siddique

Tue 25 May 2021 15.45 BST

China

America's strategic peer competitor

Capabilities

- Hacking went from smart people + simple tools in 2000s to more systematic operations now
- Building own infrastructure over time access via Belt and Road
 - Huawei, ZTE, etc
 - TikTok
- Full-stack competition:
 - chips; 'offshoring' manufacture for US firms; its own tech majors, ...
 - Microsoft uses China-based engineers for U.S. government cloud services

Eleven EU countries took 5G security measures to ban Huawei, ZTE



Explainer: what is Volt Typhoon and why is it the 'defining threat of our generation'?

FBI director has publicly identified the risk posed by a Chinese cyber operation that is believed to have compromised thousands of internet-connected devices

Helen Davidson and agencies

China

Who is targeted?

- Foreign states and political figures
- Domestic politics
 - Typically focused on "extremists", but who defines that?
- Own citizens, including those living abroad
- IP rich companies
- ...

Dalai Lama's Chinese website hacked and infected

🕒 13 August 2013

BRENDAN I. KOERNER

SECURITY OCT 23, 2016 5:00 PM

Inside the Cyberattack That Shocked the US Government

On April 15, 2015, a network engineer noticed a strange signal emanating from the US Office of Personnel Management. That was just the tip of the iceberg.

Chinese hackers took trillions in intellectual property from about 30 multinational companies

By [Nicole Sganga](#)

May 4, 2022 / 12:01 AM EDT / CBS News

China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn

A new report revealed a broad campaign that targeted Muslims in China and their diaspora in other countries, beginning as early as 2013.

Russia, Iran, North Korea ...

- Lacking platform advantage, instead rely on spear-phishing and hacking
- Russia uses cyber weapons in regional conflicts, e.g. Ukraine's grid in 2015
- NotPetya in 2017 estimated to have caused \$10bn of damage
- SolarWinds hack against US gov
- Iran hacks Saudi Aramco in response to Stuxnet
- ...

North Korean programmer charged in Sony hack, WannaCry attack

[Nation](#) Sep 6, 2018 2:16 PM EST

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company

Alex Hern

Thu 7 Jan 2016 13:20 GMT

ANDY GREENBERG

EXCERPT

SECURITY AUG 22, 2018 5:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

Last Revised: April 15, 2021

Alert Code: AA20-352A

Summary

Updated April 15, 2021: The U.S. Government attributes this activity to the Russian Foreign Intelligence Service

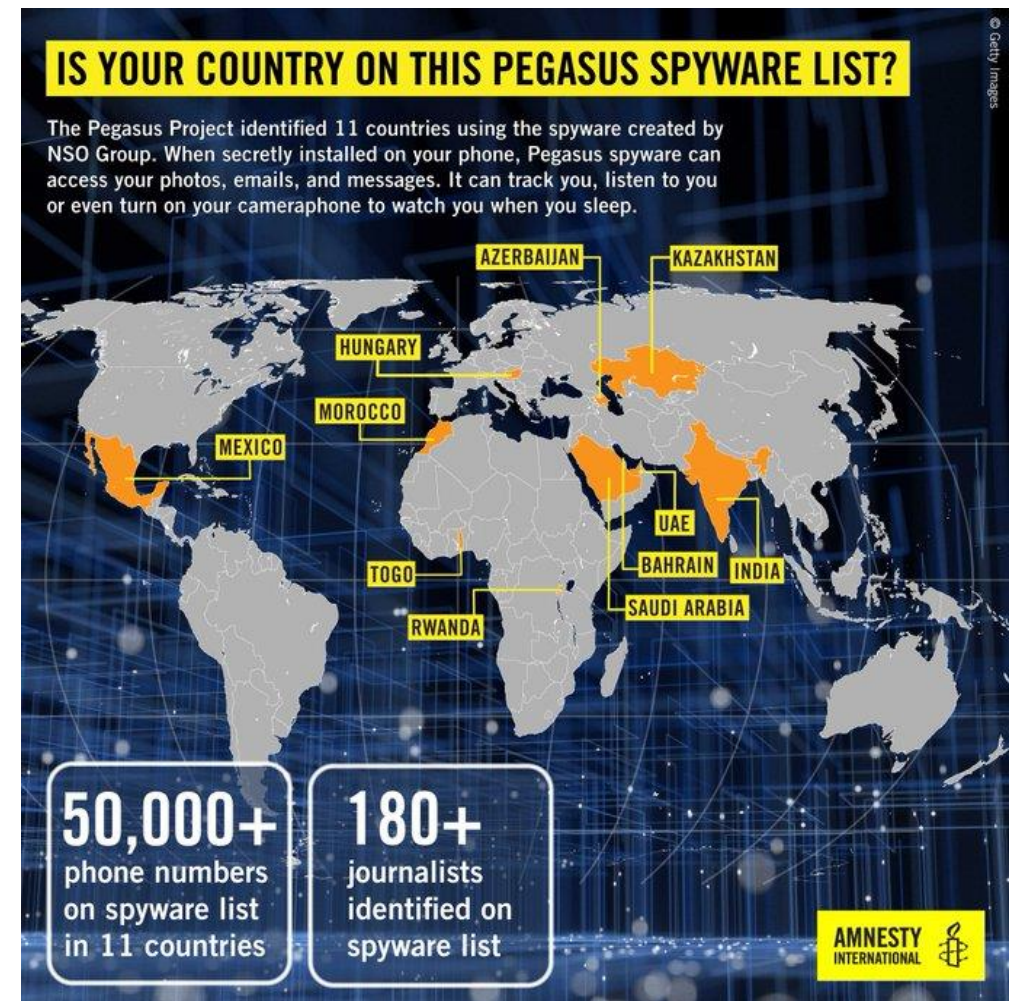
Third tier cyber powers

Capabilities

- No strong internal capabilities, instead buy it from contractors
 - Intelligence-as-a-service
 - Famously, 0-click exploits of phones..
- More constrained than others
 - Can't be too noisy or you burn the exploit
 - May face public backlash (see NSO)

Who do they target

- Political figures, dissidents, journalists



Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'

Exclusive: investigation suggests Washington Post owner was targeted five months before murder of Jamal Khashoggi

- **Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos**

Stephanie Kirchgaessner in Washington

Wed 22 Jan 2020 09.04 GMT

Paranoia as how to mitigate spooks



The geeks

"Good" actors with technical skills and/or elevated access

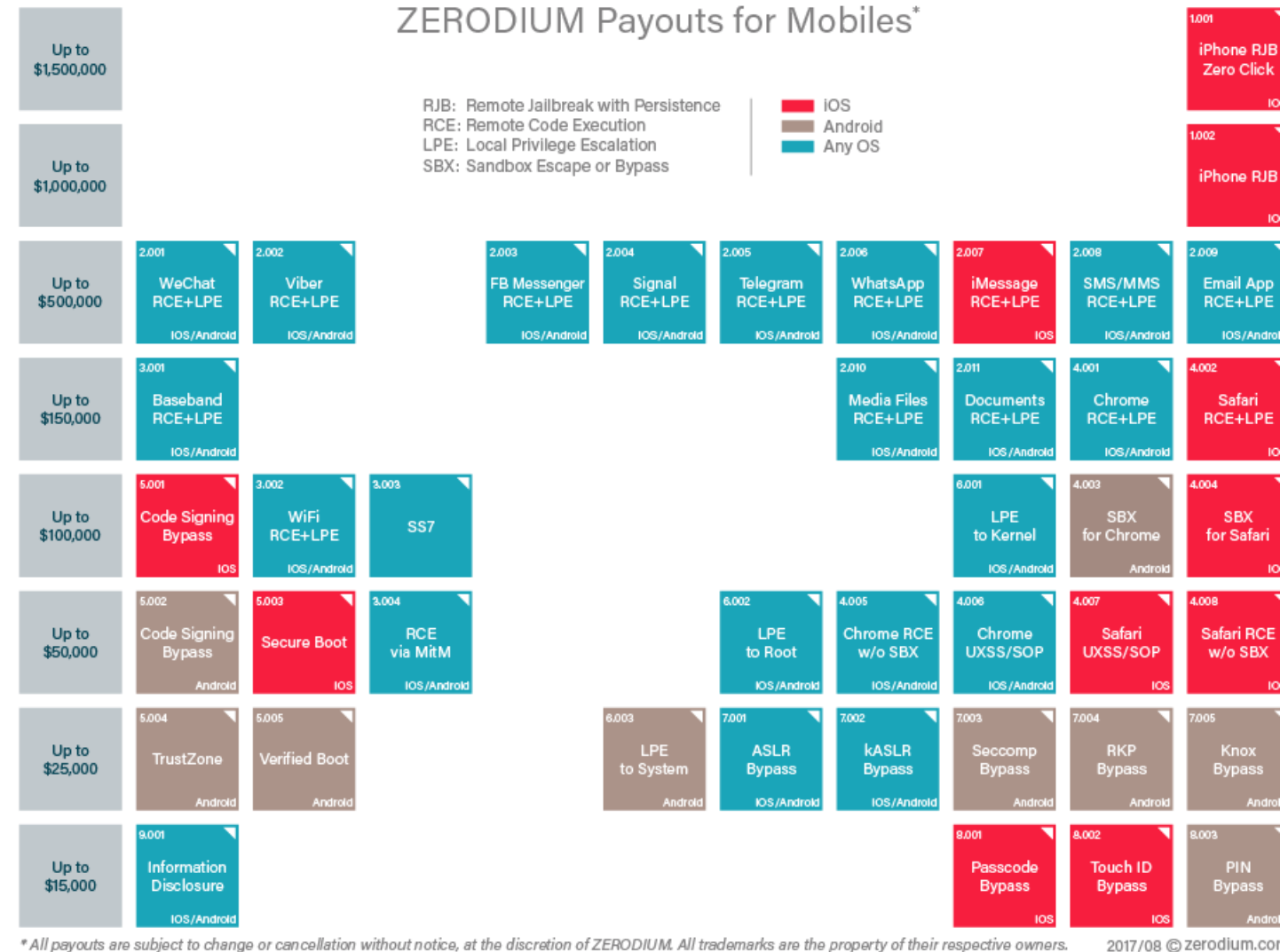
Freelance hackers

Capabilities

- Smart and v talented
 - Some train as spooks, and then get sick of bureaucracy
- Typically specialize in one system

Who do they target

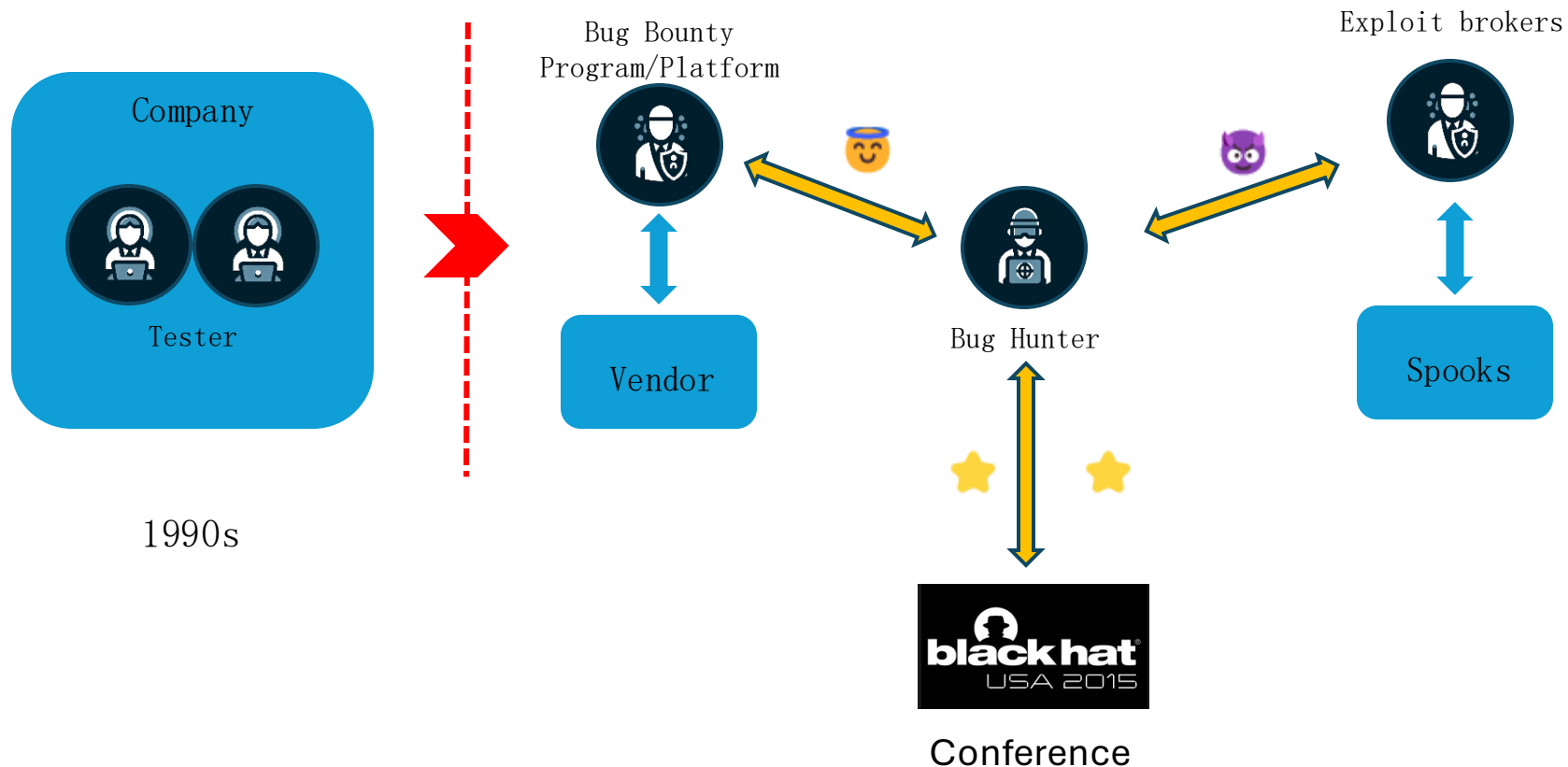
- Depends on disclosure
 - Sell to "responsible" buyers
 - Sell to the vendor
 - Present at conference



* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.

2017/08 © zerodium.com

Freelance hackers



US charges American mercenary hackers over their work in UAE

Three former US intelligence operatives accused of helping UAE spy on enemies

Reuters

Tue 14 Sep 2021 23:57 BST

More money, more problems

JENNIFER GRANICK

SCIENCE AUG 5, 2005 11:00 AM

An Insider's View of 'Ciscogate'

What was it like at the center of the fast-moving legal uproar that pitted a whistle-blowing security researcher against two corporate giants?

At what cost, fame

Source: Dellago, Matthias, Daniel W. Woods, and Andrew C. Simpson. "Characterising 0-day exploit brokers." In The 21st Workshop on the Economics of Information Security. 2022.

Responsible Disclosure

- Google Zero: “**Disclosure deadline of 90 days.** *If an issue remains unpatched after 90 days, technical details are published immediately. If the issue is fixed within 90 days, technical details are published 30 days after the fix.*”

<https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html>

Responsible Disclosure: CERT

- CERT vulnerability reporting chain: JANET CSIRT – UK NCSC – Pittsburgh US NSA – Microsoft's Patch Tuesday.
- 45+/90 day window of disclosure.
- Liability shield/credit for the hacker.
- Only good for OS/networks, not finance.

https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf

<https://vuls.cert.org/confluence/pages/viewpage.action?pageId=4718642>

<https://hackerone.com/disclosure-assistance>

Agents behaving badly

Capabilities

- Inadequate guardrails, or is it theatre?
- Increasingly strong capabilities
 - Draft phishing lures (since 2020)
 - Develop exploits (since 2025)
 - Chain together steps (since 2026)

Who do they target

- Anyone that helps them solve the assigned task

OpenAI agents hijacked German website before Hugging Face hack, report claims



OpenAI is the company behind ChatGPT

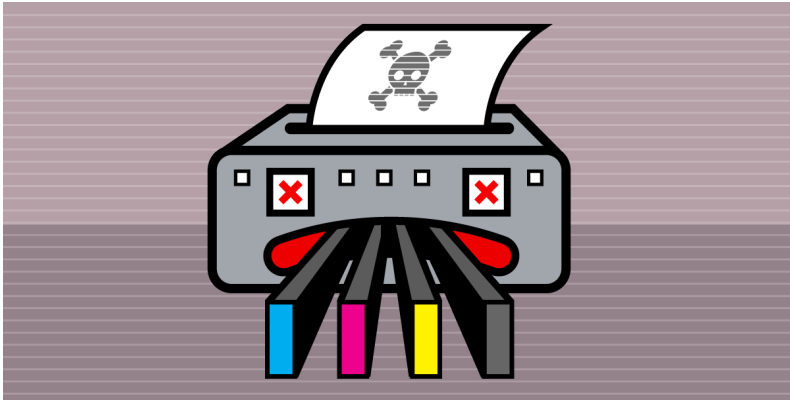
Zoe Kleinman >

Technology & AI editor

4 September 2026 ·  128 Comments

A new report claims a swarm of AI agents, developed by OpenAI, hijacked a German website - months before the firm revealed its AI had hacked tech platform Hugging Face.

Vendor on vendor violence



- Vendors design printers to refuse 3rd party cartridges
- Competitors break the security to enable their cartridges
- Lexmark Int'l, Inc. v. Static Control Components, Inc rules vendors cannot sue under DCMA

==> **Crypto arms race**

Microsoft hits out at Google team over bug report

🕒 12 January 2015

- Google Project zero conducts vulnerability research.... into other companies' products
- Other vendors may do the same

==> **Conflict of interest?**

Uber fires self-driving car engineer amid legal fight with Google

🕒 30 May 2017

- Employees may steal IP to found companies/join competitors

==> **easier to sue here**

Insider threats

Your employees have elevated privileges by design... can you trust them?

56% Of All Cybercrime Prosecutions in the UK Involve Police Officers Misusing Data Access

March 1, 2025 :: 1 min read

And the victims are disproportionately women.

Source: Hutchings, Alice. "Police behaving badly." IEEE Security & Privacy 23, no. 1 (2025): 80-82.

Accountant and two bankers jailed for stealing £390k from customers

Fraud

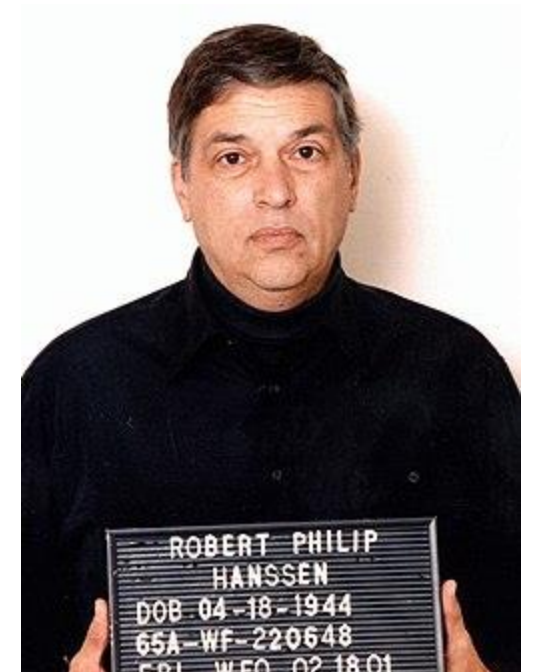
Accountant and two bankers jailed for stealing £390k from customers



Three men have been jailed after defrauding elderly bank customers of more than £390,000 and laundering the cash through multiple fake accounts.

Taminder Viridi aged 33, from Ilford in Essex, and Abubakar Salim, aged 36, from Leyton, who both worked at the same TSB branch in Stoke Newington in 2014, transferred funds out of customer accounts into 65 fraudulent beneficiary accounts they had opened.

Source: <https://www.nationalcrimeagency.gov.uk/news/accountant-and-two-bankers-jailed-for-stealing-390k-from-customers>



FBI agent for 2 decades, sending info to soviets

The swamp

Variously motivated actors with few technical skills

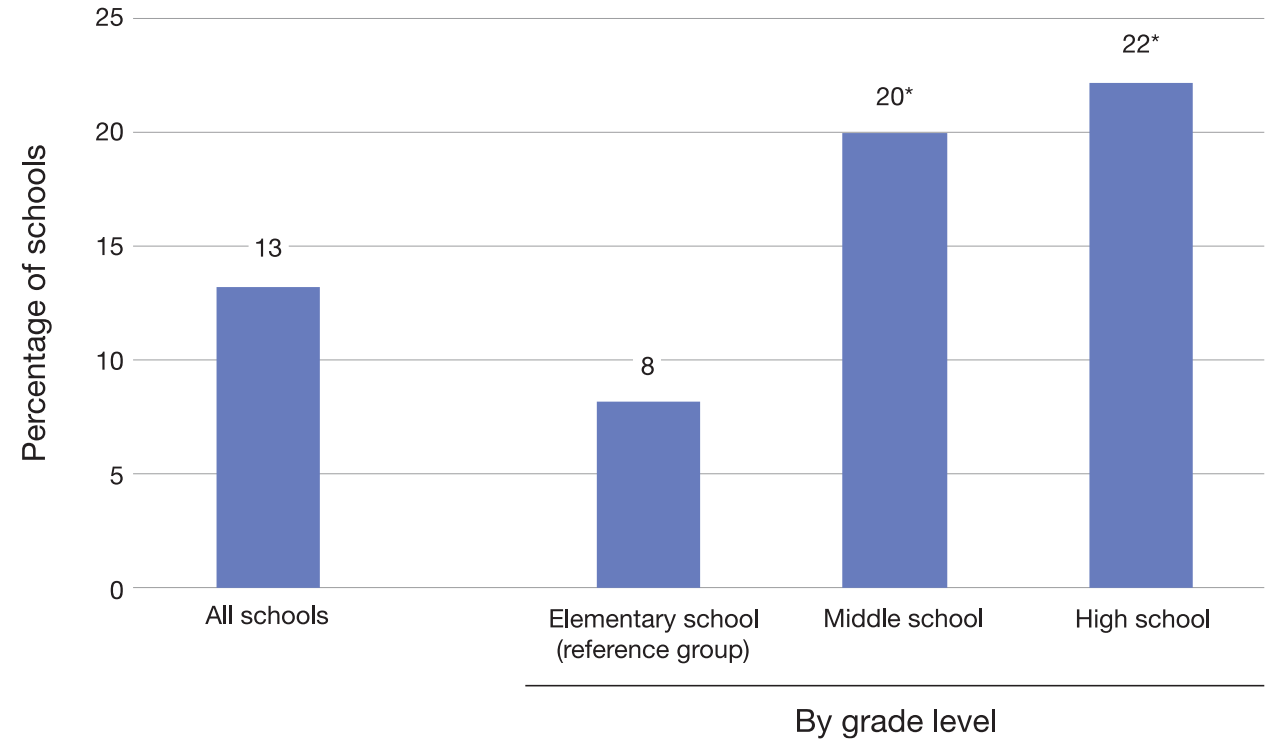
Children

Capabilities

- Access to the victim's social network + personal information
- Increasingly use deepfakes

Who do they target

- Mostly fellow classmates



https://www.rand.org/pubs/research_reports/RRA3930-5.html

Online mobs

Capabilities

- Coordinated groups can manipulate algorithms by mimicking virality
- Weaponizing privacy (doxxing)
- DDoS as a service
- Physical impact too
 - Swatting
 - Mob justice
- Increasingly use deepfakes

Who do they target

- Usually political
 - Broad definition of politics

Feminist Critics of Video Games Facing Threats in 'GamerGate' Campaign

China's internet vigilantes and the 'human flesh search engine'

🕒 28 January 2014

Police shoot man dead after alleged Call of Duty 'swatting' hoax

🕒 30 December 2017

How WhatsApp helped turn an Indian village into a lynch mob

🕒 19 July 2018

Extremists

Capabilities

- Sophisticated media operations with the goal of radicalization
 - High-quality content produced centrally
 - Botnets + decentralized members to amplify
 - "Grooming" targeted at vulnerable groups
- Privacy preserving communications
 - E2E, Tor, bullet proof hosting, "privacy" hardware
- Fund raising/money laundering infrastructure
 - Cryptocurrencies, fake charities

Who do they target

- Typically vulnerable people not integrated in society

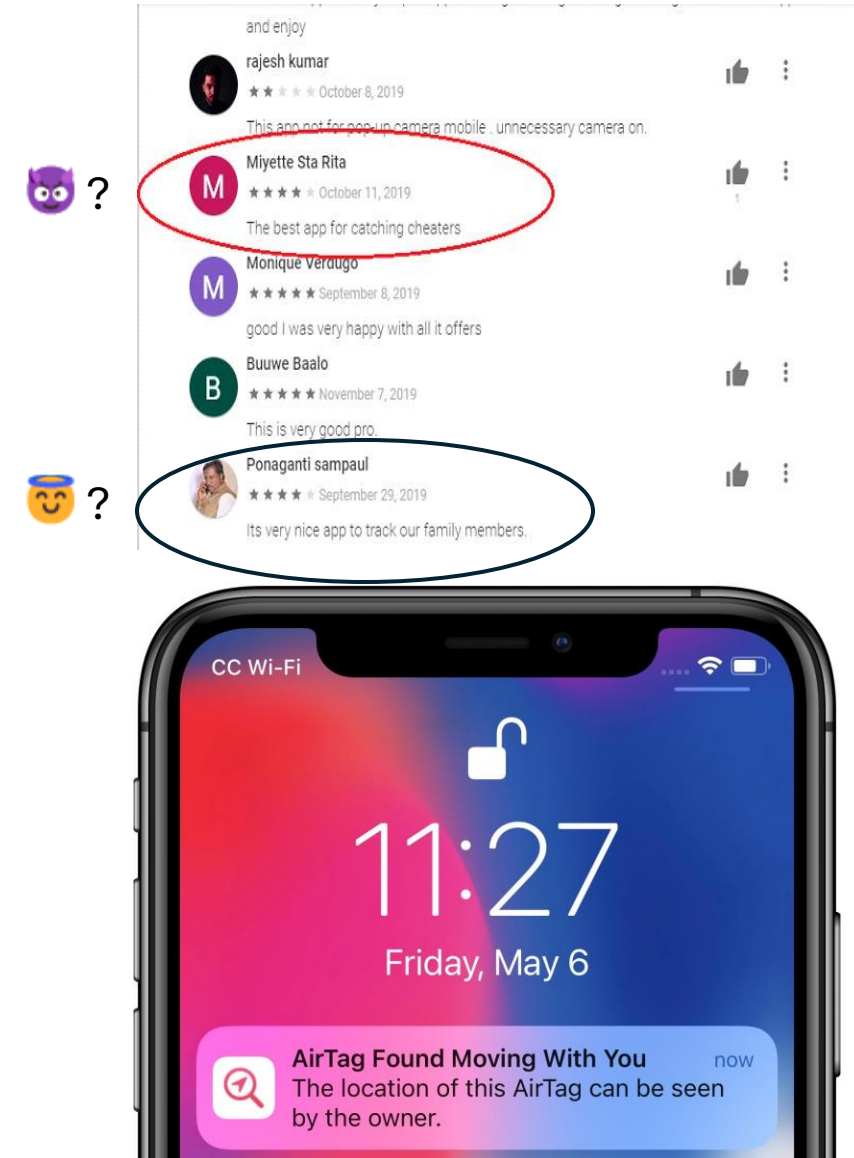
Family members

Capabilities

- Complete knowledge about victims
 - Password recovery questions
 - Coerced into sharing PINs + passwords
- Physical access to devices
- Stalkerware is common
 - Hidden once installed on phone and reports back to another device
 - Why do app stores allow it?
 - Parent tracking child is an ambiguous use case

Who do they target

- Partners and family members



Summary

Depending on the task, a security engineer might have to worry about:

1. Criminals (the crooks)

- Ransomware gangs, botnet operators, fraud gangs, malicious insiders

2. State actors (The spooks)–

- Five eyes; Russia; China; third-tier

3. Lawful operators (The geeks) –

- Employees, security researchers, competitors

4. The swamp

- hate crimes, bullying, family members etc

Further reading: Security Engineering chapter 2