



# ***The Dark Web's Role in Incident Response: Intelligence and Action***

---

# Agenda

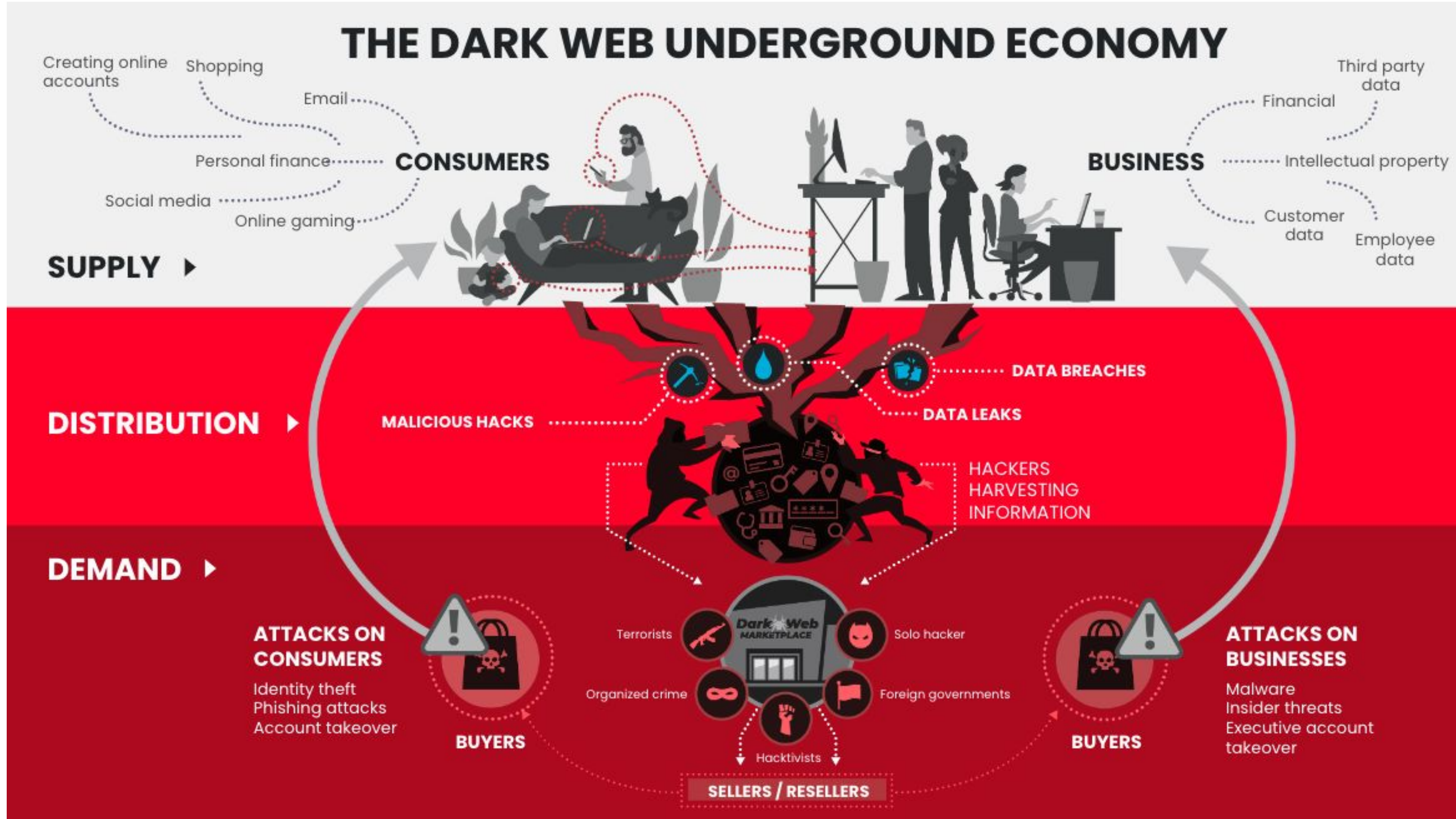
- Meet our panelists
- Dark Web 101
- Discovery
- Investigation
- Examples from the dark web
- Recovery
- Cyber Insurance
- Wrap Up

---

# Meet Our Panelists

- Kelly Garrison, Junior Partner, Pierson Ferdinand
- Jamie Tolles, Vice President, Response, IDX a ZeroFox Company
- Nicholas Cramer, VP, Response Partnerships, IDX a ZeroFox Company (moderator)

# Dark Web 101



---

# Discovery

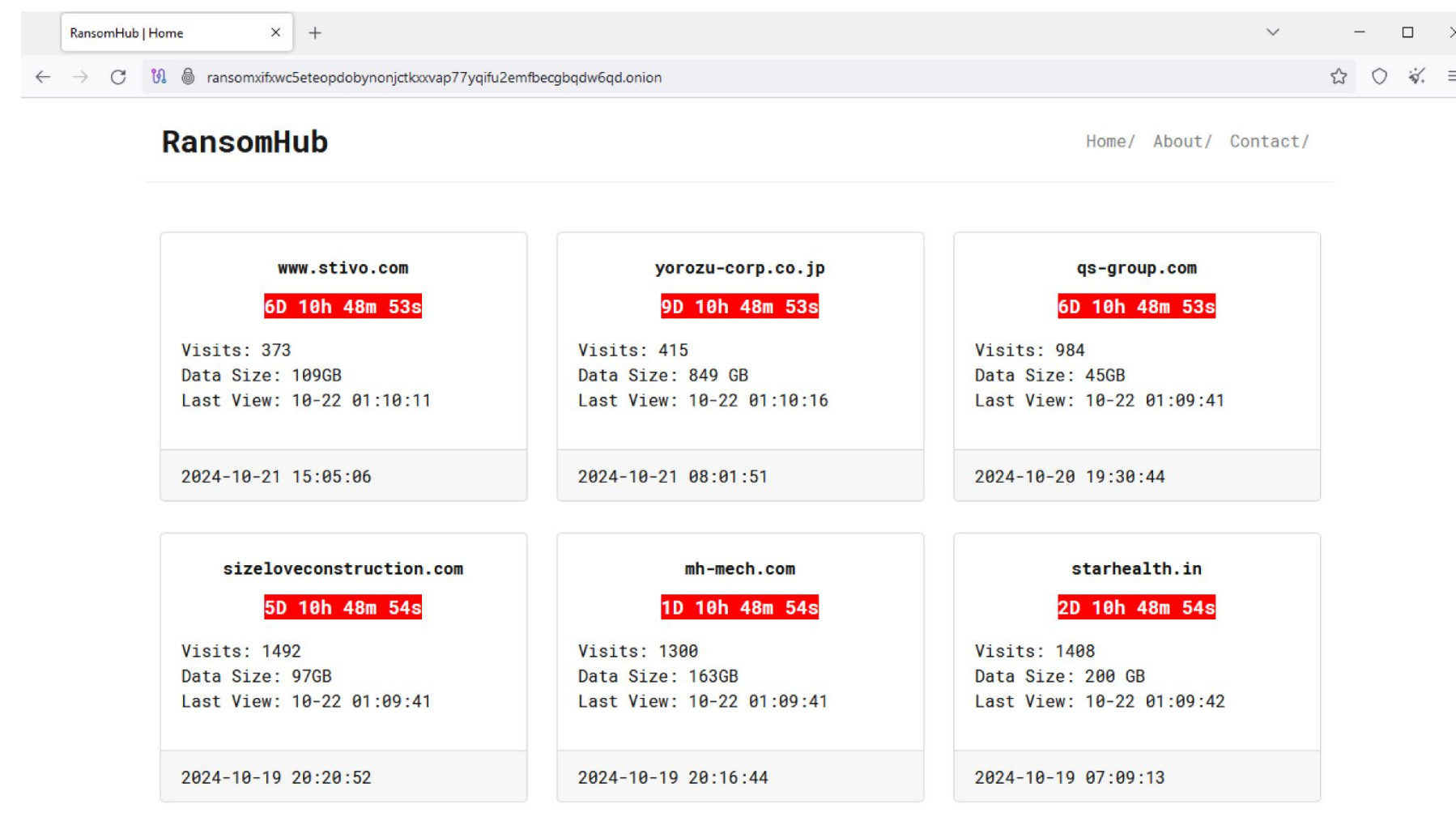
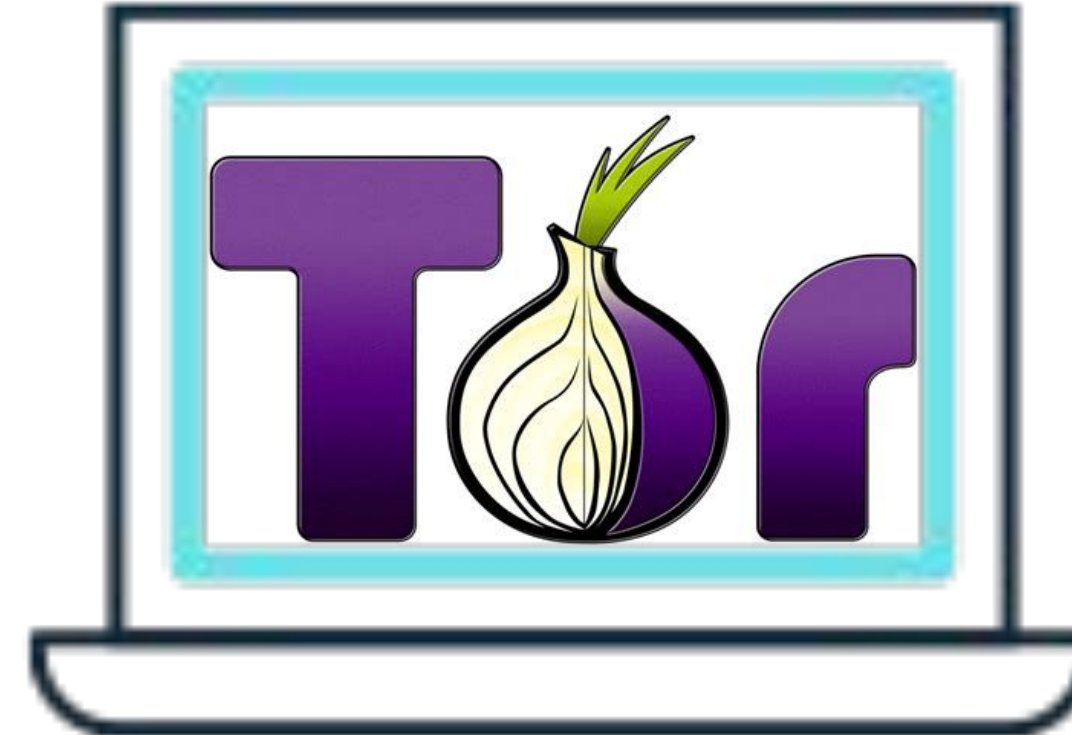
## *Dark web intelligence triggers incident*

- Customer tries to eFile - rejected
- IDX guides customer through resolution process
- Work with IRS Identity Protection Specialized Unit (IPSU)
- Form ([14039](#)) submitted
- Fraud return invalidated / current return processed via mail
- ID.me rarely involved

# Investigation

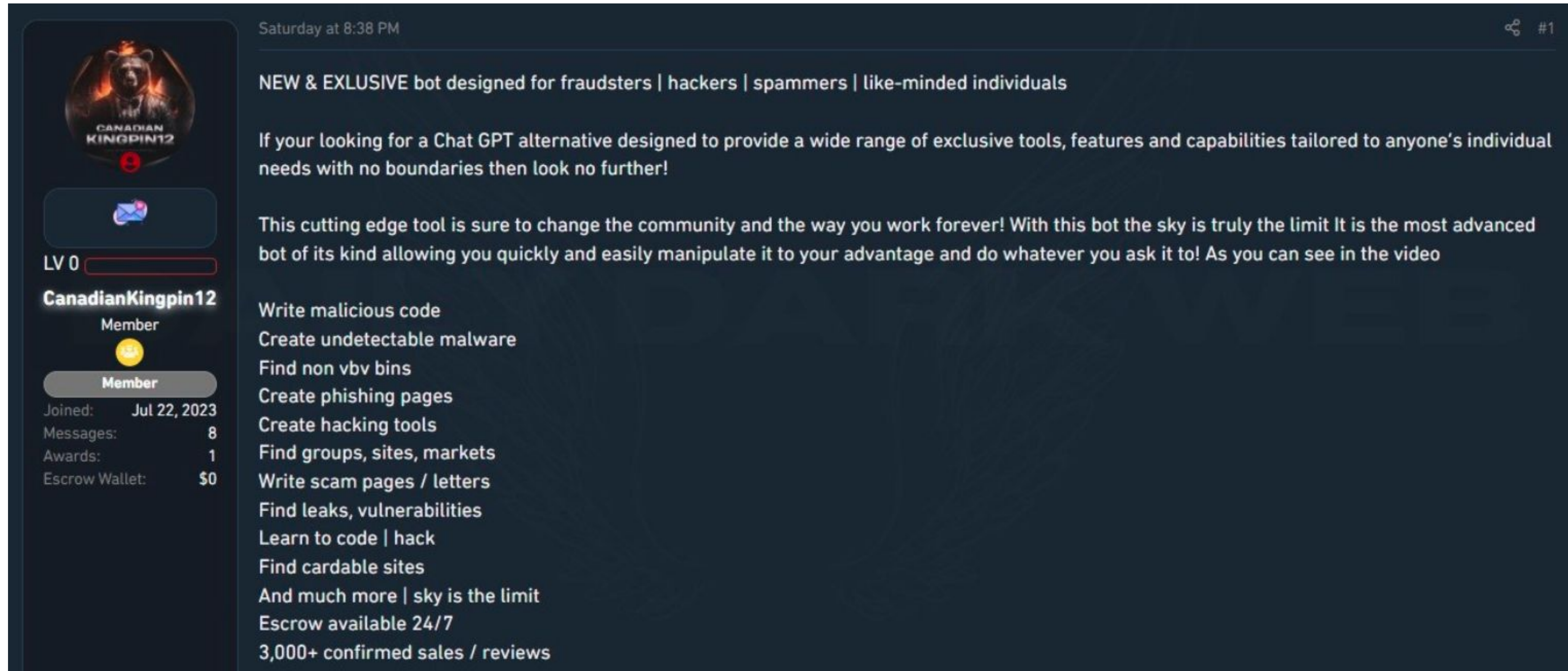
## *The Dark Web's Role In an Investigation*

- What tools are used?
- What are you looking for?
- What is the TA doing?



# Examples from the dark web

## FraudGPT:



Saturday at 8:38 PM #1

**NEW & EXCLUSIVE** bot designed for fraudsters | hackers | spammers | like-minded individuals

If your looking for a Chat GPT alternative designed to provide a wide range of exclusive tools, features and capabilities tailored to anyone's individual needs with no boundaries then look no further!

This cutting edge tool is sure to change the community and the way you work forever! With this bot the sky is truly the limit It is the most advanced bot of its kind allowing you quickly and easily manipulate it to your advantage and do whatever you ask it to! As you can see in the video

**CanadianKingpin12**  
Member  
Member

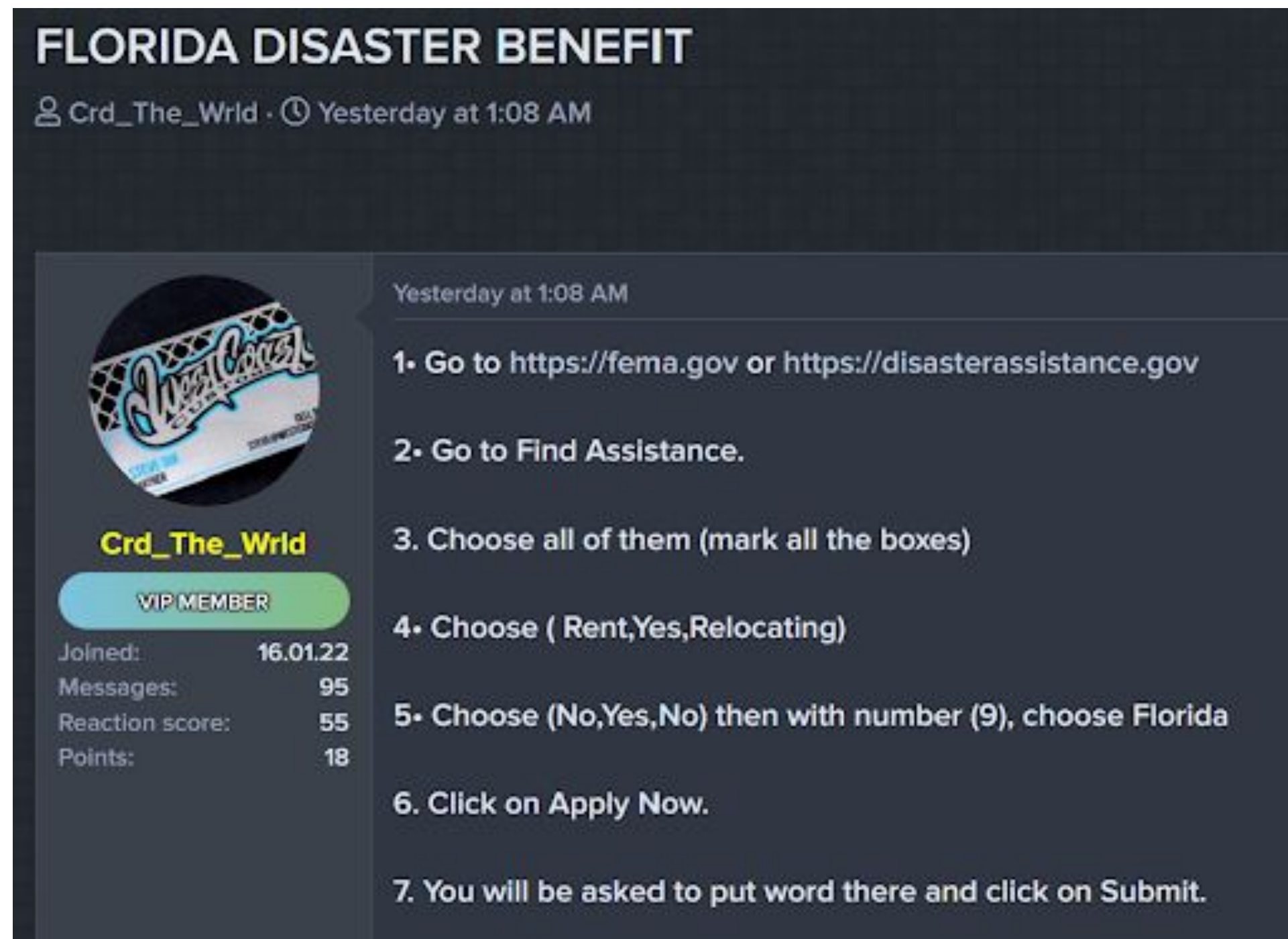
Joined: Jul 22, 2023  
Messages: 8  
Awards: 1  
Escrow Wallet: \$0

- Write malicious code
- Create undetectable malware
- Find non vbv bins
- Create phishing pages
- Create hacking tools
- Find groups, sites, markets
- Write scam pages / letters
- Find leaks, vulnerabilities
- Learn to code | hack
- Find cardable sites
- And much more | sky is the limit
- Escrow available 24/7
- 3,000+ confirmed sales / reviews

Source: <https://2crd.cc/showthread.php?t=146528>

# Examples from the dark web

Industry-related scam:



**FLORIDA DISASTER BENEFIT**  
Crd\_The\_Wrld · Yesterday at 1:08 AM

**Crd\_The\_Wrld**  
VIP MEMBER  
Joined: 16.01.22  
Messages: 95  
Reaction score: 55  
Points: 18

Yesterday at 1:08 AM

1. Go to <https://fema.gov> or <https://disasterassistance.gov>
2. Go to Find Assistance.
3. Choose all of them (mark all the boxes)
4. Choose ( Rent,Yes,Relocating)
5. Choose (No,Yes,No) then with number (9), choose Florida
6. Click on Apply Now.
7. You will be asked to put word there and click on Submit.

Source: <https://www.zerofox.com/blog/the-underground-economist-volume-2-issue-20/>



# Examples from the dark web

## New Ransomware Affiliate:

**Welcome to Cicada3301!**

We are recruiting partners to work in our affiliate program:

- Penetrators.
- Access advertisers.

**General information :**

- Work in the **CIS** countries is strictly prohibited.
- The affiliate program commission is **20%** of the total payout amount.
- To participate in the affiliate program, you must pass a mini-interview.
- A wallet for payments is provided in the chat. For amounts over **1.5 million USD** , two wallets are provided: yours and ours.
- It is strictly forbidden to transfer access to the panel to third parties, except in cases agreed with support.

**LOCKER :**

- The locker is written in **Rust** from scratch. - **ChaCha20 + RSA** is used to encrypt files , which supports full file encryption, as well as encryption of only some of its parts. Modes:

- Full** : full file encryption.
- Fast** : fast file encryption **15** blocks of **1 MB** .
- Auto** : Automatic selection of encryption parameters, optimal for files.

Encryption parameters can be configured individually when assembling the locker.

- The locker operates offline, without requiring an internet connection.
- The locker runs on all versions **of Windows** , starting with **Windows 7** , as well as on **Linux** , **ESXi** and **NAS** .
- File encryption occurs in multithreaded mode.
- The locker supports network mode, which allows parallel scanning of the local network.
- It is possible to encrypt files, folders and partitions at specific points.
- The locker supports impersonation, which allows you to run the program under different credentials.
- Before starting work, the locker terminates the specified processes, stops and deletes the specified services.
- Before encryption, the locker mounts hidden drives.
- Before encryption, the recycle bin is emptied, shadow copies and operating system restore points are deleted.
- A text note with instructions is left in each folder where files were encrypted.
- The locker has a list of exceptions for system file extensions and directories that do not need to be encrypted.
- Stopping **VM ESXi/Hyper-V** .
- The note is stored in encrypted form, the locker can be launched only if there is a key that decrypts the note.
- Delayed start of the locker using a timer, which is optimal for "mining" the network.

**[RaaS] Cicada3301** Reply

Cicada3301 · Jun 29, 2024

Forums > Market \ Market > Partners Program \ RaaS \ Partner Prog...

Jump to new Watch


Jun 29, 2024 New < #1

**Cicada 3301**

**Cicada3301**  
Jun 24, 2024

Messages	4
Reaction score	1
Points	3

**Cicada 3301**



# Examples from the dark web

Initial access brokers:

The screenshot shows a forum thread with three posts from a user named 'citrix'. Each post includes a profile card with a 'NO AVATAR' icon, the name 'citrix', and a 'CD-диск' label. The posts list revenue figures and target locations:

- Post 1 (10.05.2022):** 1. Rev \$2 Billion (finance, USA).... 2. Rev \$354 Million (healthcare, USA).... 3. Rev \$281 Million (sys management, USA) updates toxin: 6119C34F573F133BCD06CEC711CF5B7332B7667757FF4621F679BFD7248B894798F1BA492CEB
- Post 2 (Суббота в 15:42):** 4. Rev \$4 Billion (insurance, USA) 5. Rev \$800 Million (manufacturing, USA) updates toxin: 6119C34F573F133BCD06CEC711CF5B7332B7667757FF4621F679BFD7248B894798F1BA492CEB
- Post 3 (Сегодня в 04:25):** 6. Rev \$2 Billion (health, USA) (user, team workforce) updates toxin: 6119C34F573F133BCD06CEC711CF5B7332B7667757FF4621F679BFD7248B894798F1BA492CEB

Access Broker Sales By Targeted Entity Location, 2024

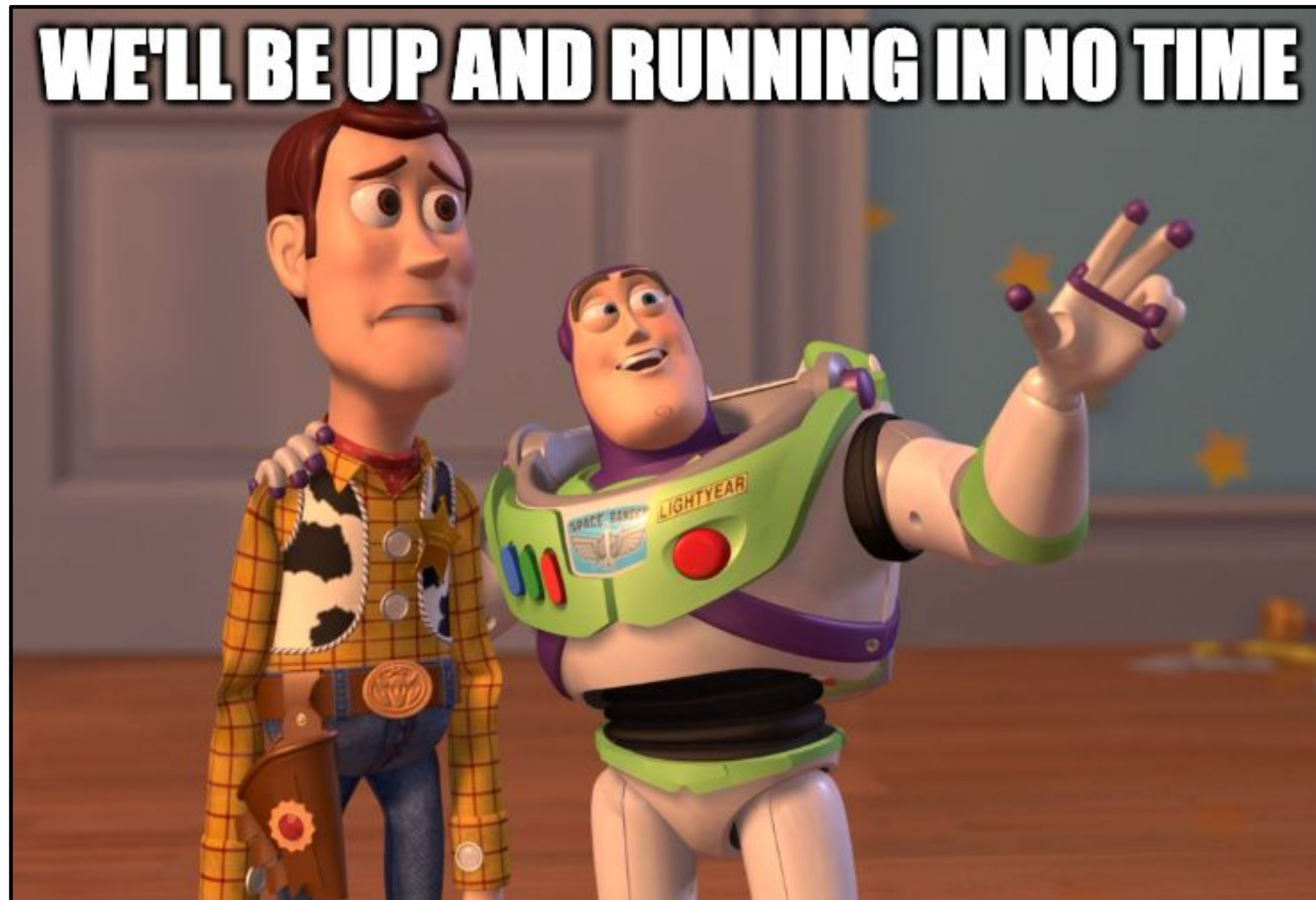
Rank	Country	Count	Average Instant Purchase Price (USD)
1	United States	287	\$4,441
2	United Kingdom	45	\$3,051
3	Brazil	43	\$2,281
4	Germany	30	\$1,655
5	Canada	26	\$3,033
6	Australia	25	\$1,966
7	India	22	\$15,367
8	Spain	17	\$3,715
9	France	17	\$1,600
10	Italy	15	\$1,283
11	Switzerland	11	\$1,312
12	Netherlands	10	\$1,710

Source: Deep Web Forum xss[.]is

# Recovery

## Expectation

## Reality



---

# Cyber insurance

- Risk management tools and resources provided by carriers
- What's covered, what's not covered under your policy
  - Ransom demands
  - Business interruption
  - Attacks on third party vendors, business partners
  - War exclusion
  - Cyber terrorism
- Claims trends
- Costs of a claim

---

# Wrap up