
INFORMATION SYSTEMS SECURITY ASSOCIATION
NORTH ALABAMA CHAPTER

NetSPI

Weaponizing Trust

Social Engineering Tactics for Initial Access Against Hardened Networks

Presented by: Caleb Havens

Principal Security Consultant | Red Team Operations & Social Engineering

July 21, 2026

Background & Credentials

2011-2018

- Captain (O-3)
- Ground Intelligence Officer
- Expeditionary Ground Reconnaissance Officer

2019-2023

- Parsons
- Senior Systems Analyst - Test Directorate
- Cyber Engineering Analyst - Cyber Engineering Directorate

2023-2024

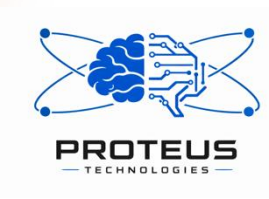
- COLSA
- Red Team Operator - Cyber Division

2024-Present

Principal Security Consultant

- Red Team Operator
- Social Engineer

- Instructor

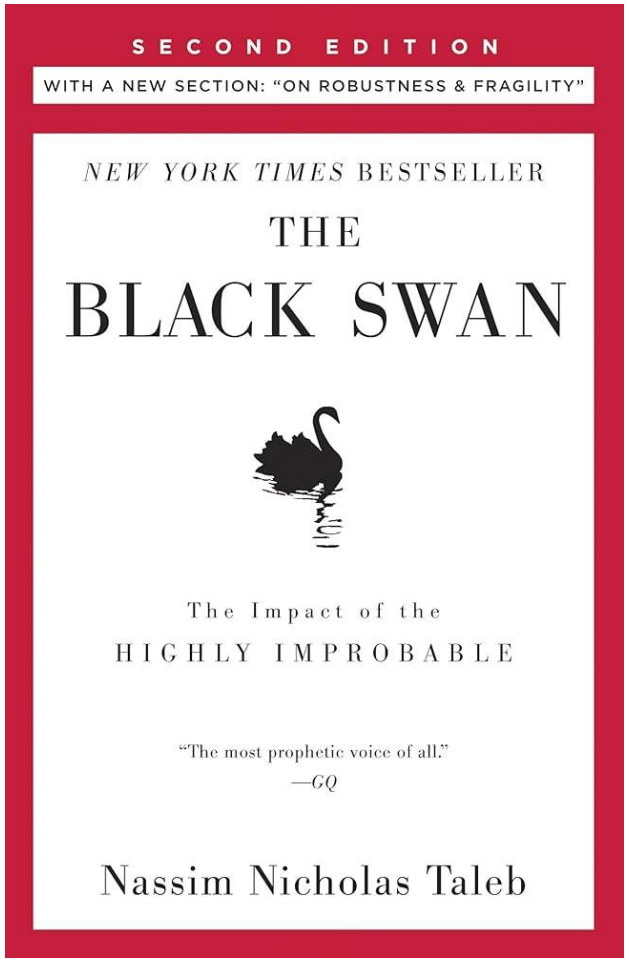


- Founder & CEO

Agenda

- What is Red Teaming?
- Social Engineering for Initial Access
- Three real-world scenarios
- Questions

Agenda

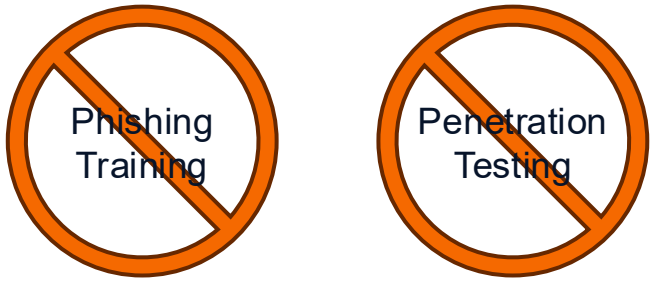


"Systems that haven't experienced stress appear stable, but are actually accumulating risk and becoming more vulnerable to rare, high-impact events."

- Nassim Nicholas Taleb (paraphrased)

What is Red Teaming?

- **An adversarial exercise designed to test whether a business can withstand a real attacker. Not whether a control exists on paper.**



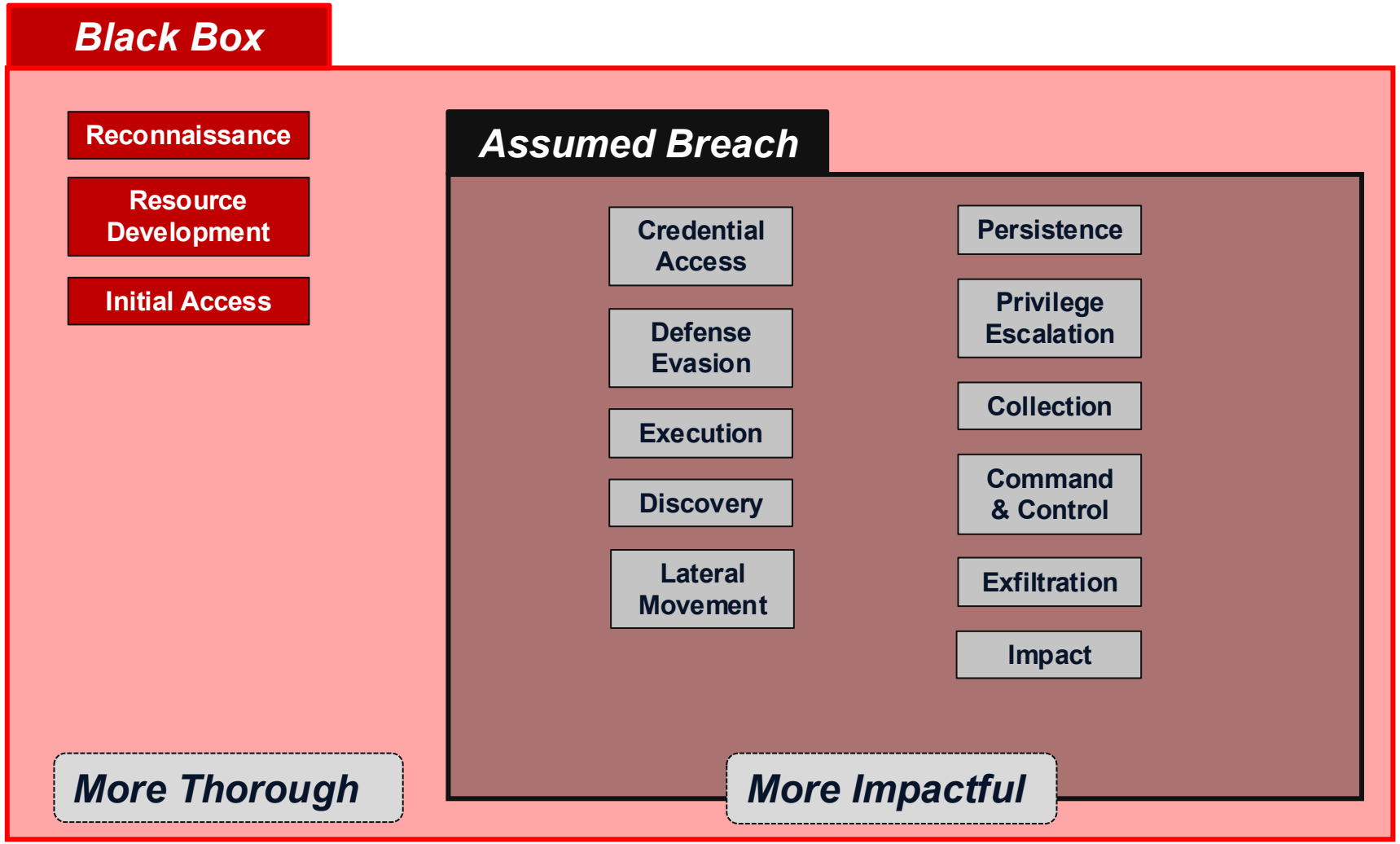
Types of Red Team Operations

Black Box

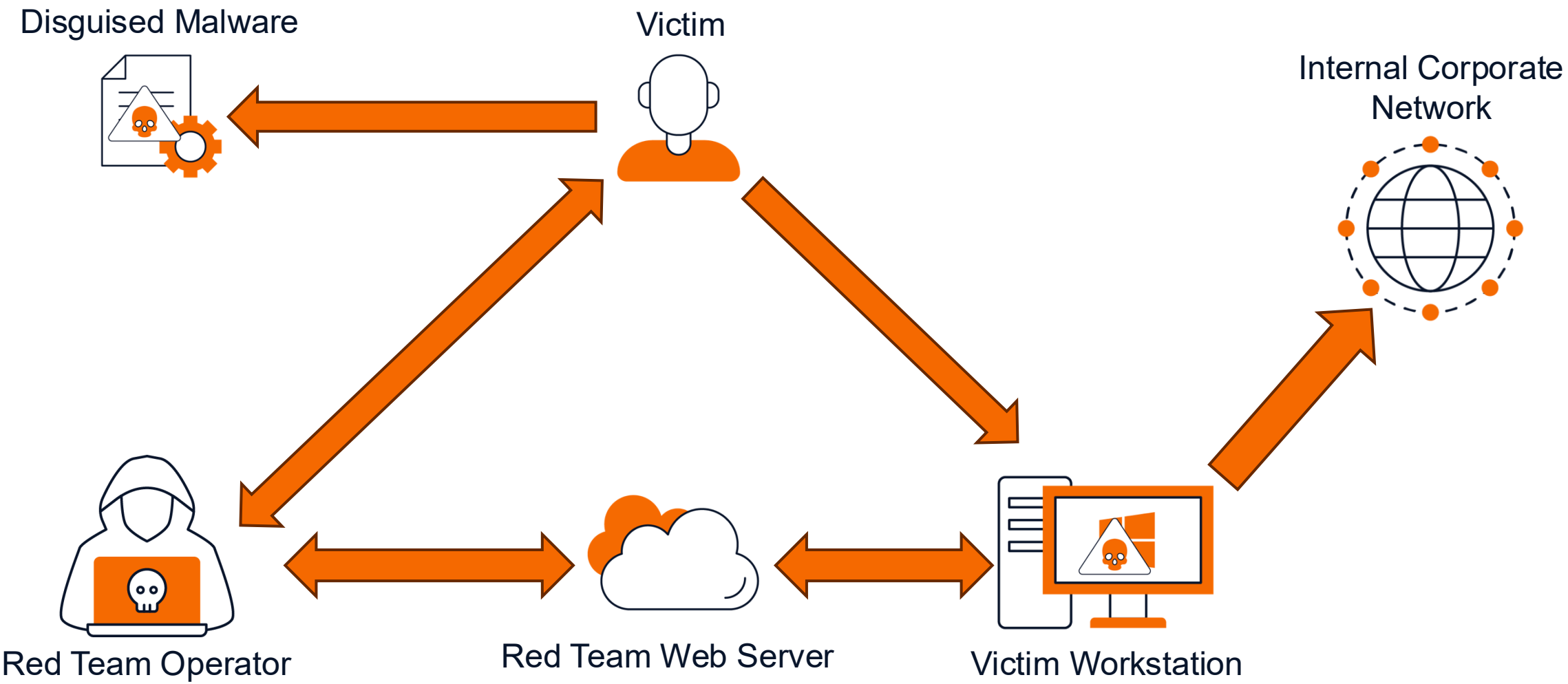
- 6-8 weeks
  - 3-4 weeks external
  - 3-4 weeks internal
    - Assumed Breach Failover (if necessary)

Assumed Breach

- 3-4 weeks
- Assisted clickers (preferable and most realistic)
  - Provisioned laptops
  - Provisioned accounts and remote access
  - NUC in the network (**Don't do this**)



GOAL: Remote Access



Social Engineering: Still King of IA

Verizon's 2024 DBIR: 74% of breaches involved the human element.

CrowdStrike 2024: 71% of attacks are now "hands-on-keyboard" interactive intrusions, and social engineering remains the primary access method for financially-motivated actors

Why?

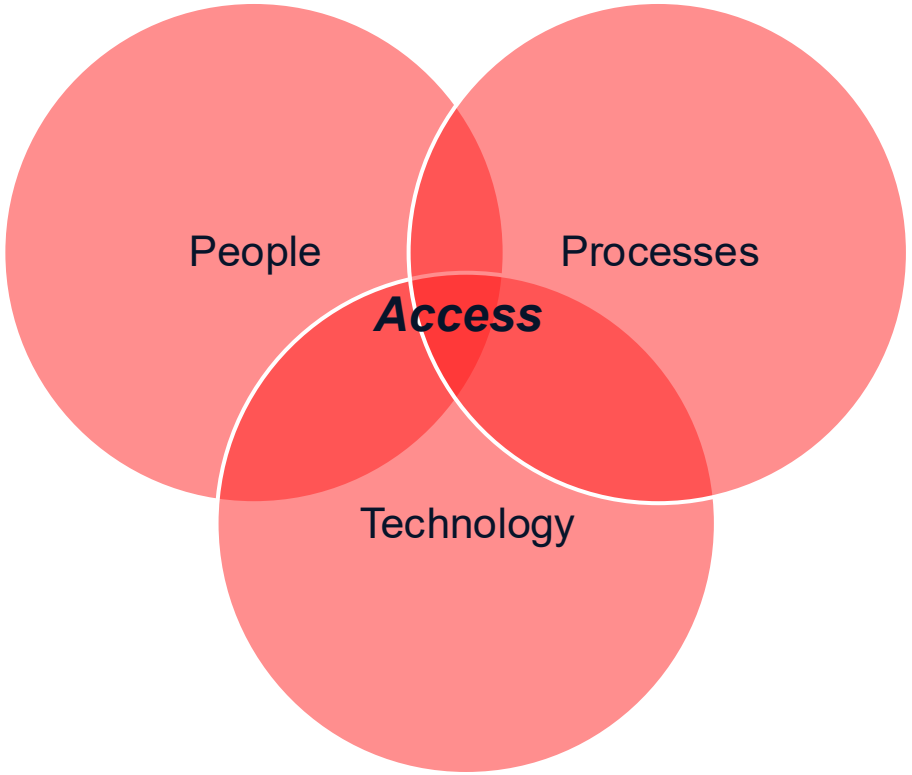
- The attack surface has GROWN
- Social Engineering scales infinitely
- The ROI is Unbeatable
  - Speed, cost, and success rate are all higher than technical exploitation

Examples:

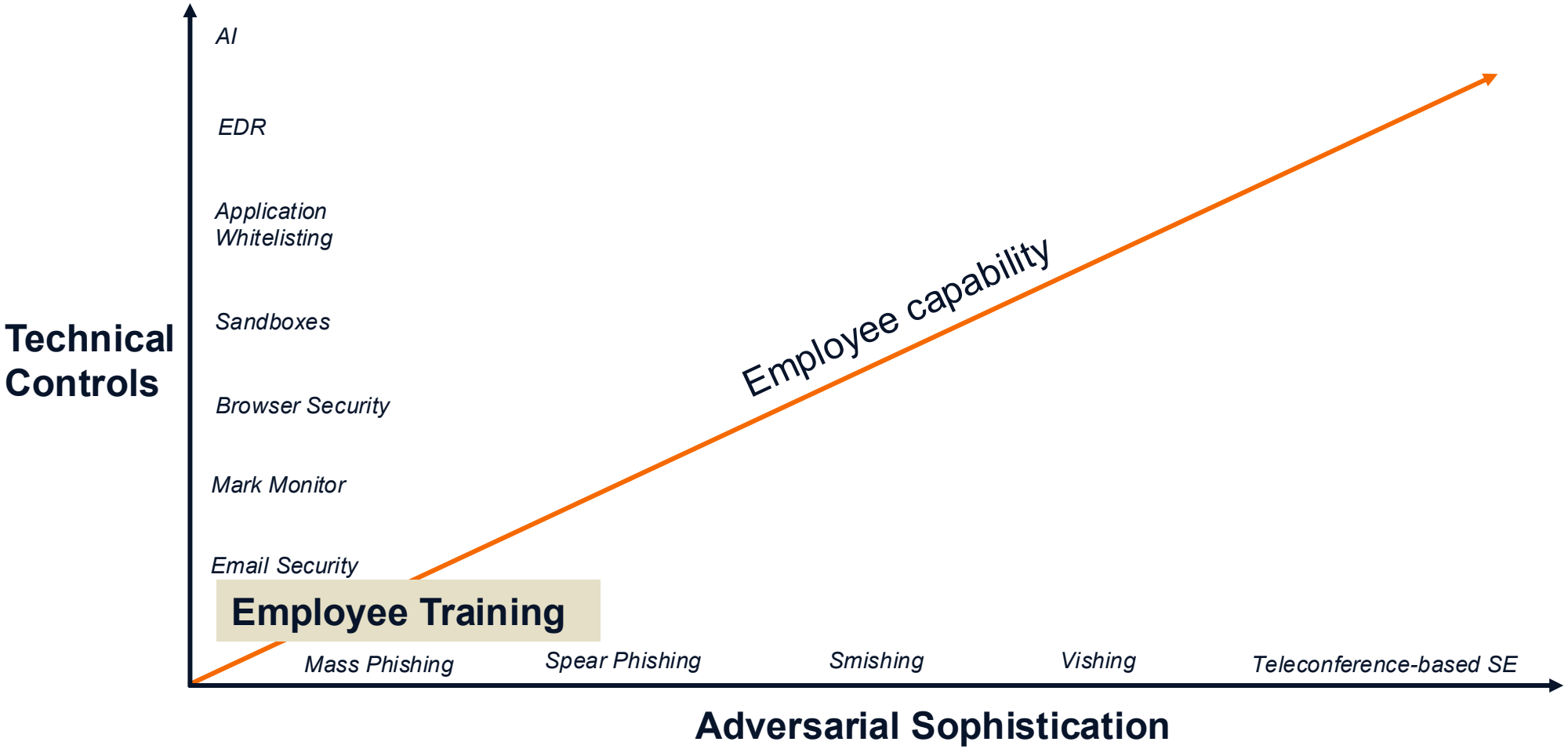
- MGM Resorts Casino Hack (September 2023)
- Okta Support System Breach (2023)
- Twilio (2022)
- Change Healthcare (2024)
- LastPass (2022–2023)

Social Engineering in RTO

- Social Engineering specific assessments
  - Primarily test people
  - Success is measured by metrics (e.g., how many people clicked)
  - Scope is limited---as is the amount of interaction
    - Email
    - Phone
    - Physical
  - Security applications don’t play a factor
- Social Engineering as part of Red Teaming
  - Test people, processes, and technology
  - Success is measured by whether you get in or not
  - Must find a weakness in all three if you’re going to get in



Training Gap



~~Three~~ Scenarios Four

Disclaimer

NetSPI takes the security of our client's data seriously. Company names, employee names, and other information that could be linked back to either of those has been redacted for this presentation.

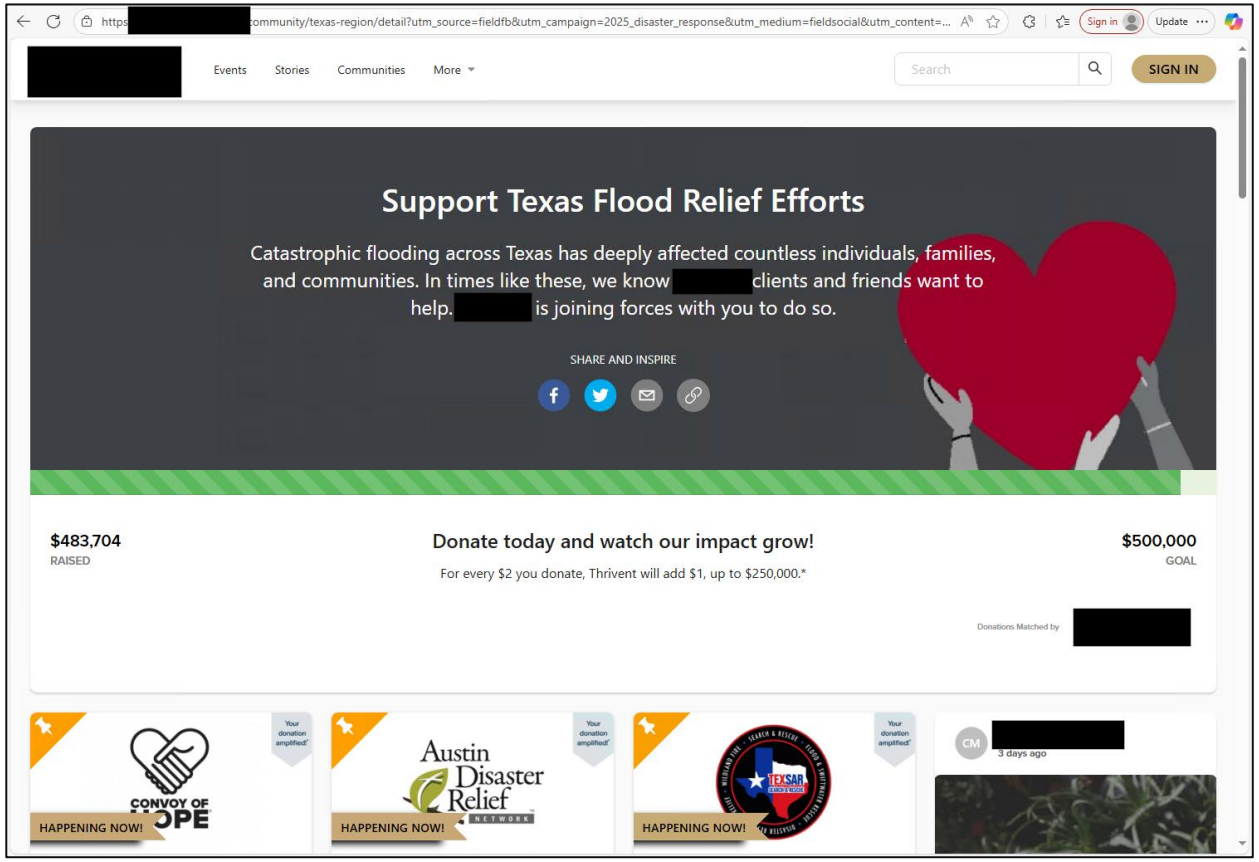
Weaponize the Business Model Against Them

Scenario:

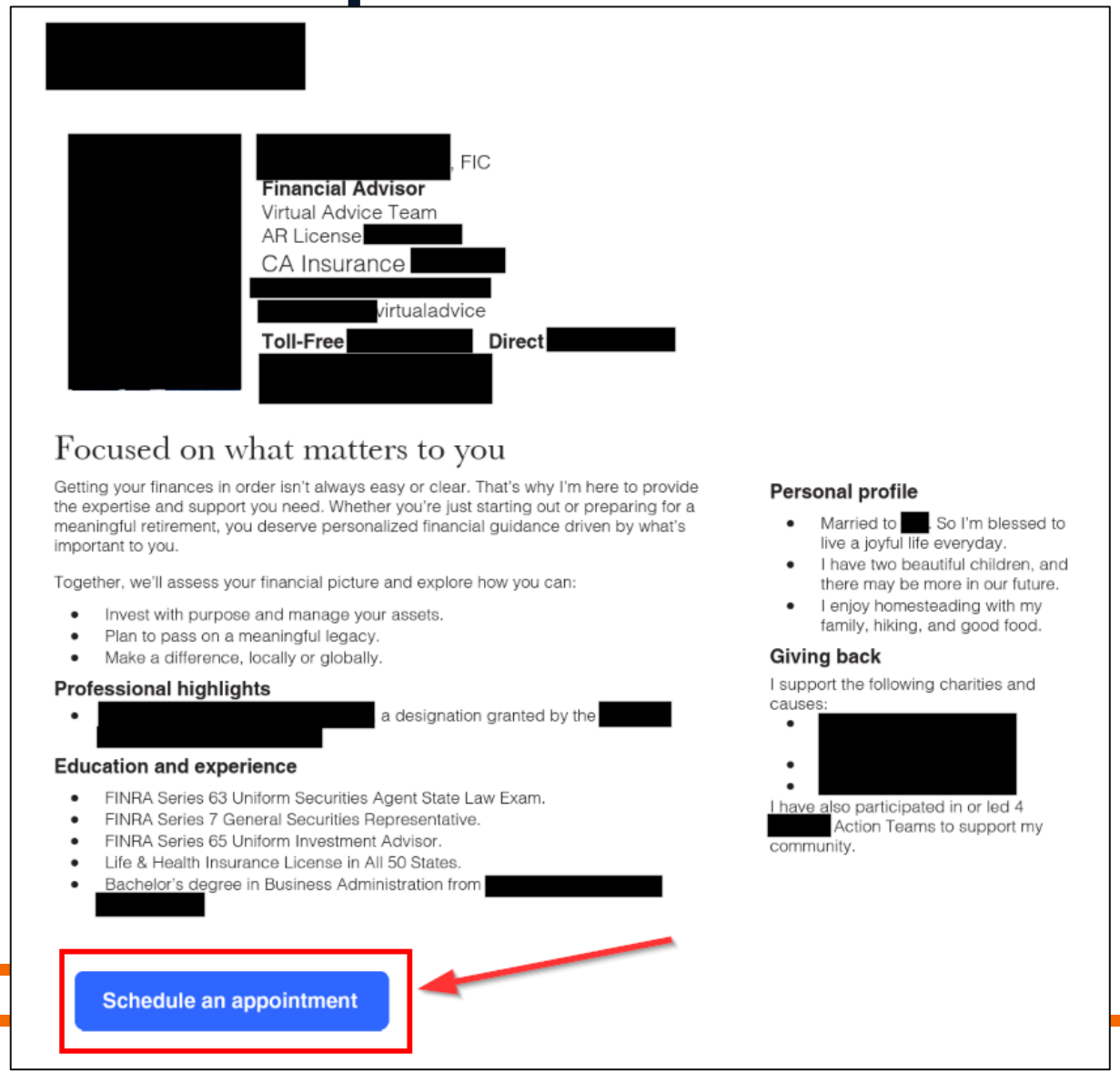
I was conducting a Black Box RTO against a company of Financial Advisors. They had been our client for three years, yet we'd never gotten initial access. They also refused a pivot to an Assumed Breach Failover, so we'd never properly evaluated their internal security posture.

Weaponize the Business Model Against Them

Open Source Intelligence:



Weaponize the Business Model Against Them


[redacted]

[redacted], FIC
Financial Advisor
Virtual Advice Team
AR License [redacted]
CA Insurance [redacted]
[redacted]virtualadvice
Toll-Free [redacted] **Direct** [redacted]
[redacted]

Focused on what matters to you

Getting your finances in order isn't always easy or clear. That's why I'm here to provide the expertise and support you need. Whether you're just starting out or preparing for a meaningful retirement, you deserve personalized financial guidance driven by what's important to you.

Together, we'll assess your financial picture and explore how you can:

- Invest with purpose and manage your assets.
- Plan to pass on a meaningful legacy.
- Make a difference, locally or globally.

Professional highlights

- [redacted] a designation granted by the [redacted]

Education and experience

- FINRA Series 63 Uniform Securities Agent State Law Exam.
- FINRA Series 7 General Securities Representative.
- FINRA Series 65 Uniform Investment Advisor.
- Life & Health Insurance License in All 50 States.
- Bachelor's degree in Business Administration from [redacted]

Personal profile

- Married to [redacted]. So I'm blessed to live a joyful life everyday.
- I have two beautiful children, and there may be more in our future.
- I enjoy homesteading with my family, hiking, and good food.

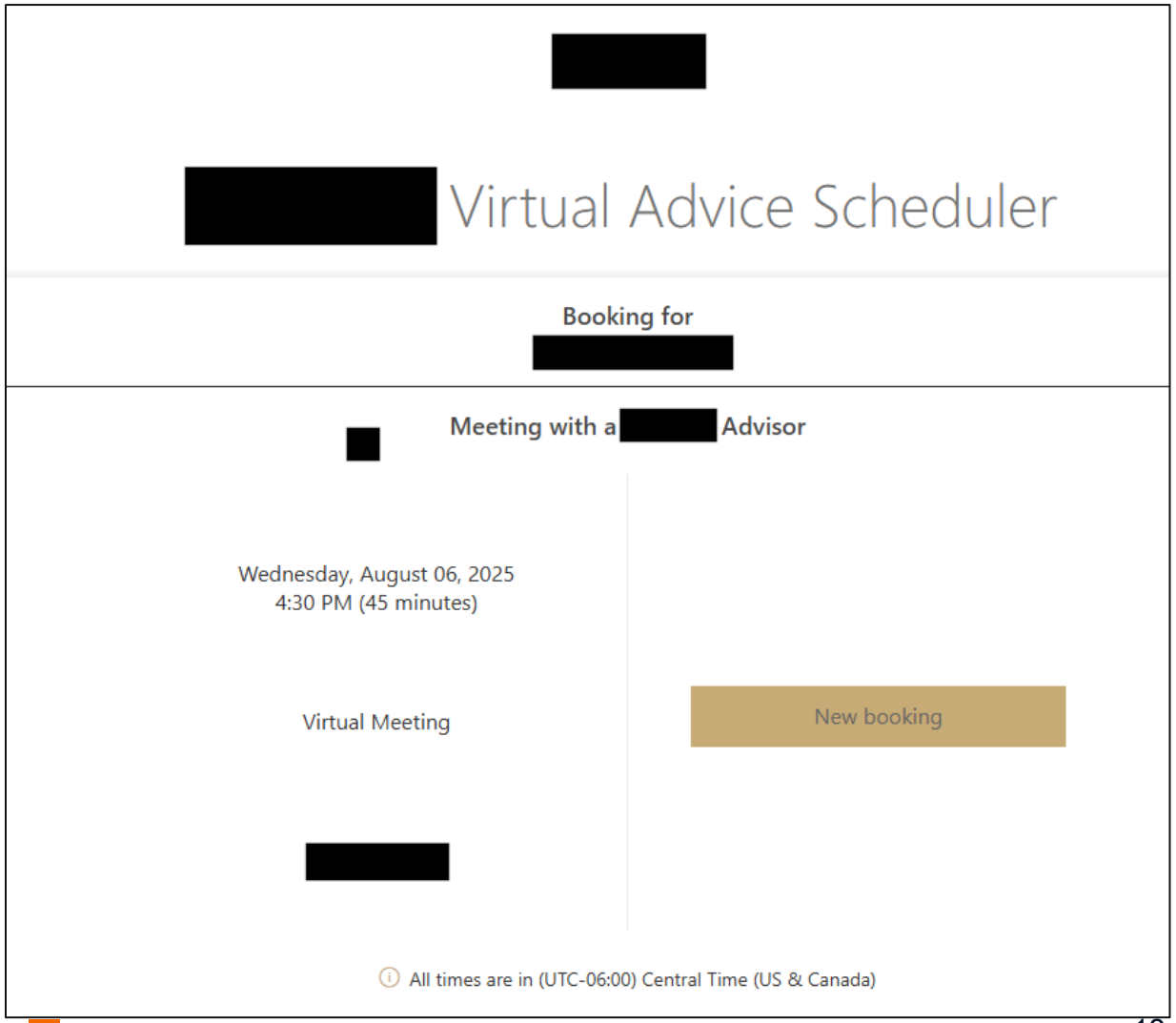
Giving back

I support the following charities and causes:

- [redacted]

I have also participated in or led 4 [redacted] Action Teams to support my community.

Schedule an appointment


[redacted]

[redacted] Virtual Advice Scheduler

Booking for [redacted]

[redacted] Meeting with a [redacted] Advisor

Wednesday, August 06, 2025
4:30 PM (45 minutes)

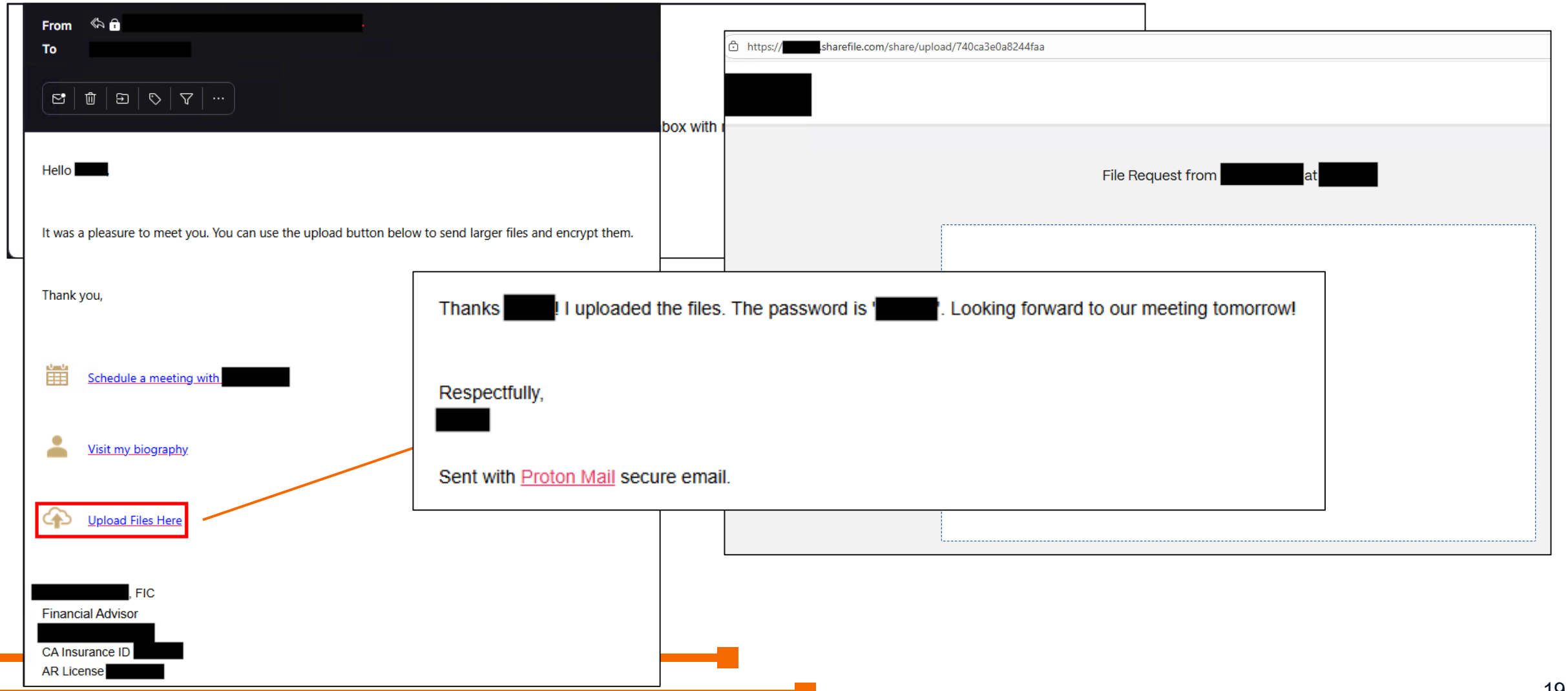
Virtual Meeting

New booking

[redacted]

All times are in (UTC-06:00) Central Time (US & Canada)

Weaponize the Business Model Against Them



Weaponize the Business Model Against Them

In ISO and Password Protected ZIP:

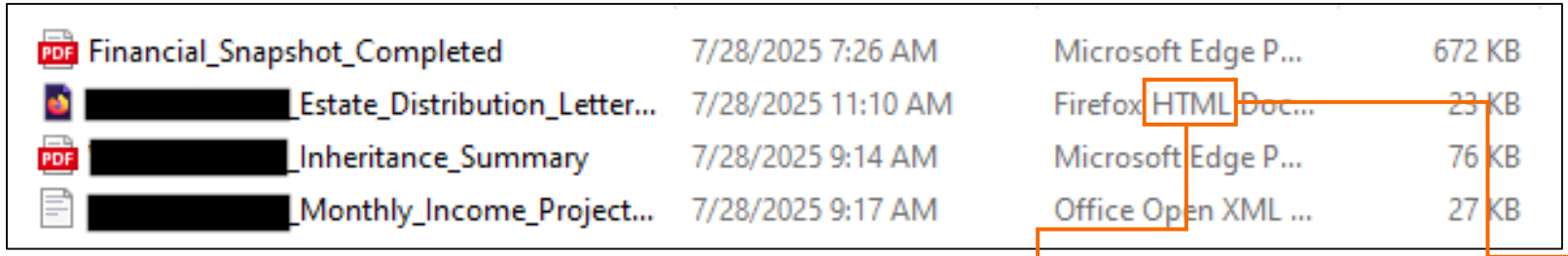
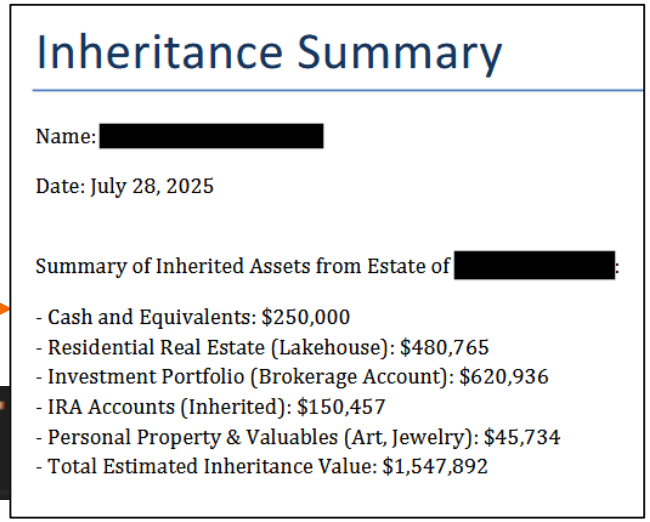


Image pingback in HTML:

```
<img src="https://[redacted].cloudfront.net/[redacted]-files/track.gif?page=landing"
style="display:none;" />
```



Inheritance Summary

Name: [redacted]

Date: July 28, 2025

Summary of Inherited Assets from Estate of [redacted]:

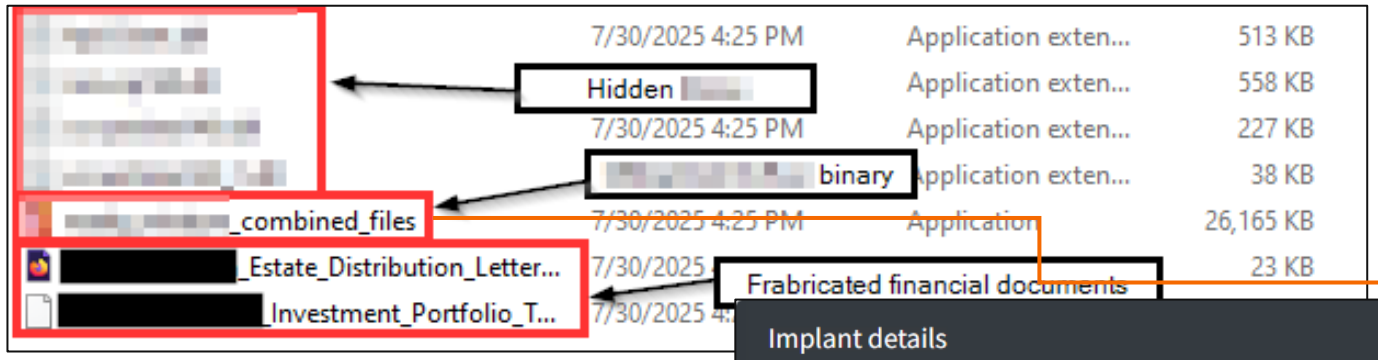
- Cash and Equivalents: $250,000
- Residential Real Estate (Lakehouse): $480,765
- Investment Portfolio (Brokerage Account): $620,936
- IRA Accounts (Inherited): $150,457
- Personal Property & Valuables (Art, Jewelry): $45,734
- Total Estimated Inheritance Value: $1,547,892

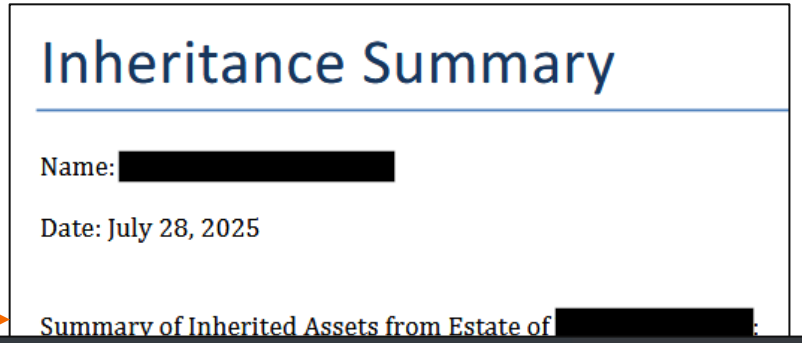
Logs from Image Pingback:

```
[REDACTED]- X-Forwarded-For:[REDACTED] Size:5357 - - [28/Jul/2025:17:59:10
+0000] "GET /[REDACTED]-files/track.gif?page=landing HTTP/1.1" 200 3965 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0"
```

Weaponize the Business Model Against Them

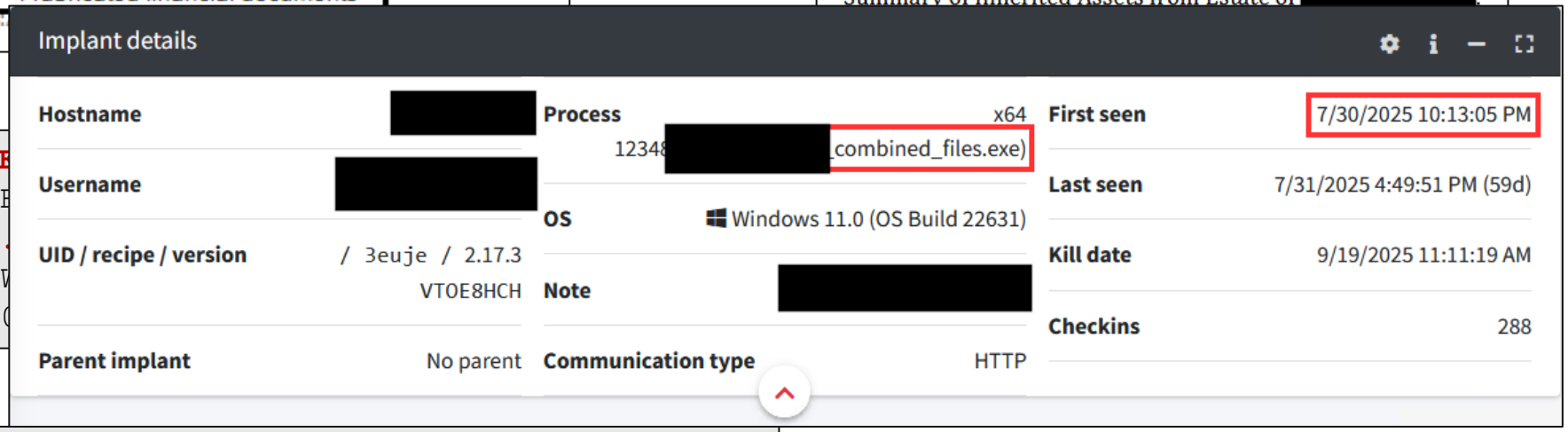
In ISO and Password Protected ZIP:





Decoy Page Accessed:

```
[REDACTED] - X-Forwarded-For:[RE
[30/Jul/2025:22:13:02 +0000] "GE
files/[REDACTED]_Combined_Files.
"Mozilla/5.0 (Windows NT 10.0; W
(KHTML, like Gecko) Chrome/138.0
```



Callback to Apache Redirector:

```
[REDACTED] - X-Forwarded-For:[REDACTED] Size:2816 - -
[30/Jul/2025:22:13:05 +0000] "POST /api/assets/library/elements.json
HTTP/1.1" 200 587 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Edg/138.0.0.0"
```

Weaponize the Business Model Against Them

Risk Exposed:

- Adversaries could quickly access the sensitive financial documents of customers
- Further exposure of sensitive data or ransomware could have been achieved through follow-on actions in the network.

Value to the Client:

- ShareFile application deprecated
- Sanitization of phone numbers and other personal data that could be exploited
- Identity checks for prospective clients

Weaponize Trust… And Typos

Scenario:
I was conducting a Black Box against a major medical lending provider that had won the Cyber Fortress Award several years prior. There were barely any phone numbers posted and a Social Security Number was required to begin the loan process and begin correspondence with a loan processor.

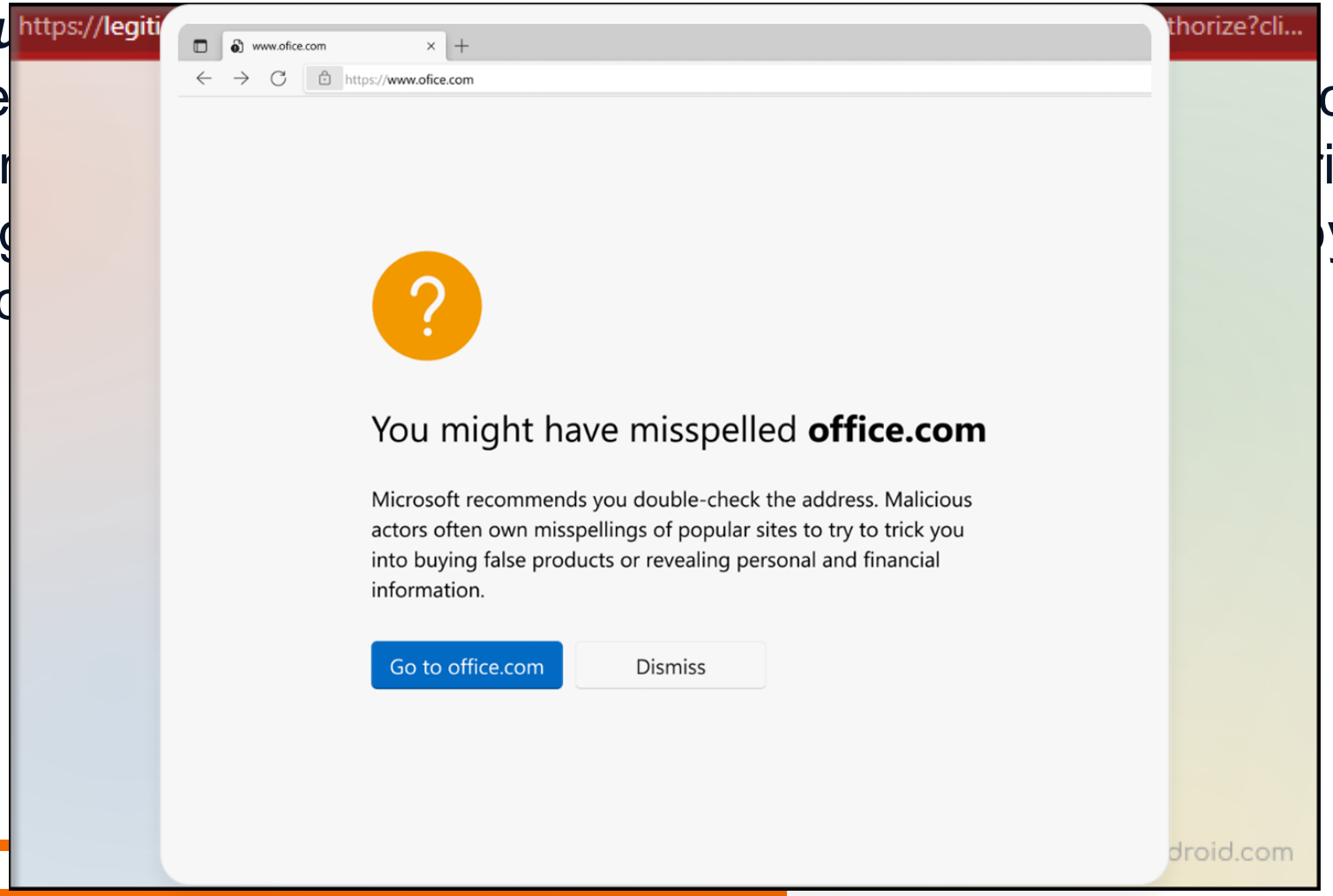
So we used typosquatted domains, but not the way you've seen before.

Weaponize Trust… And Typos

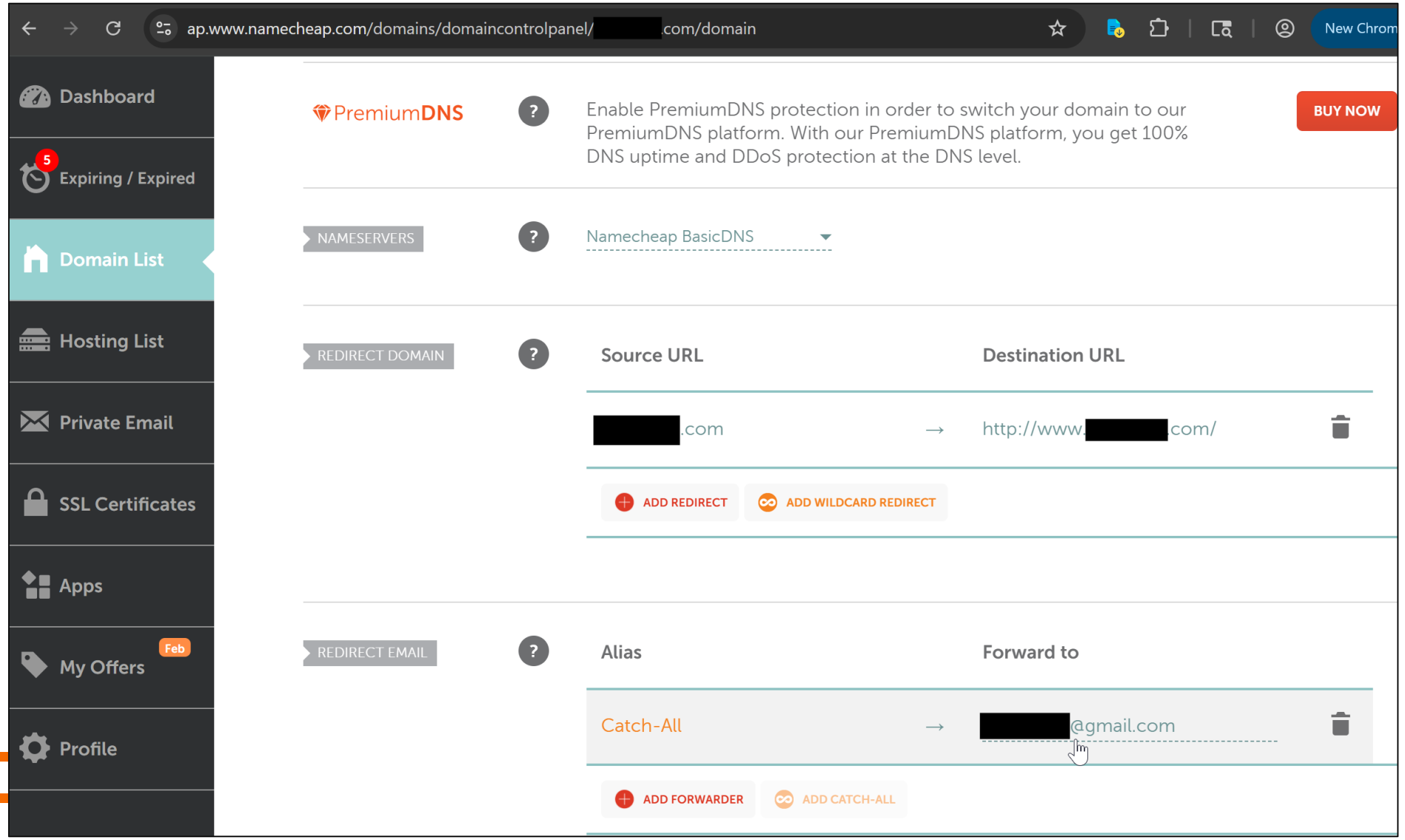
Typosqu

- We've
- Sendi
- Setting
  Monito

com
ity filters
y Mark
registrar



Weaponize Trust… And Typos



john.smith@toyota.com

↓

john.smith@toyta.com

↓

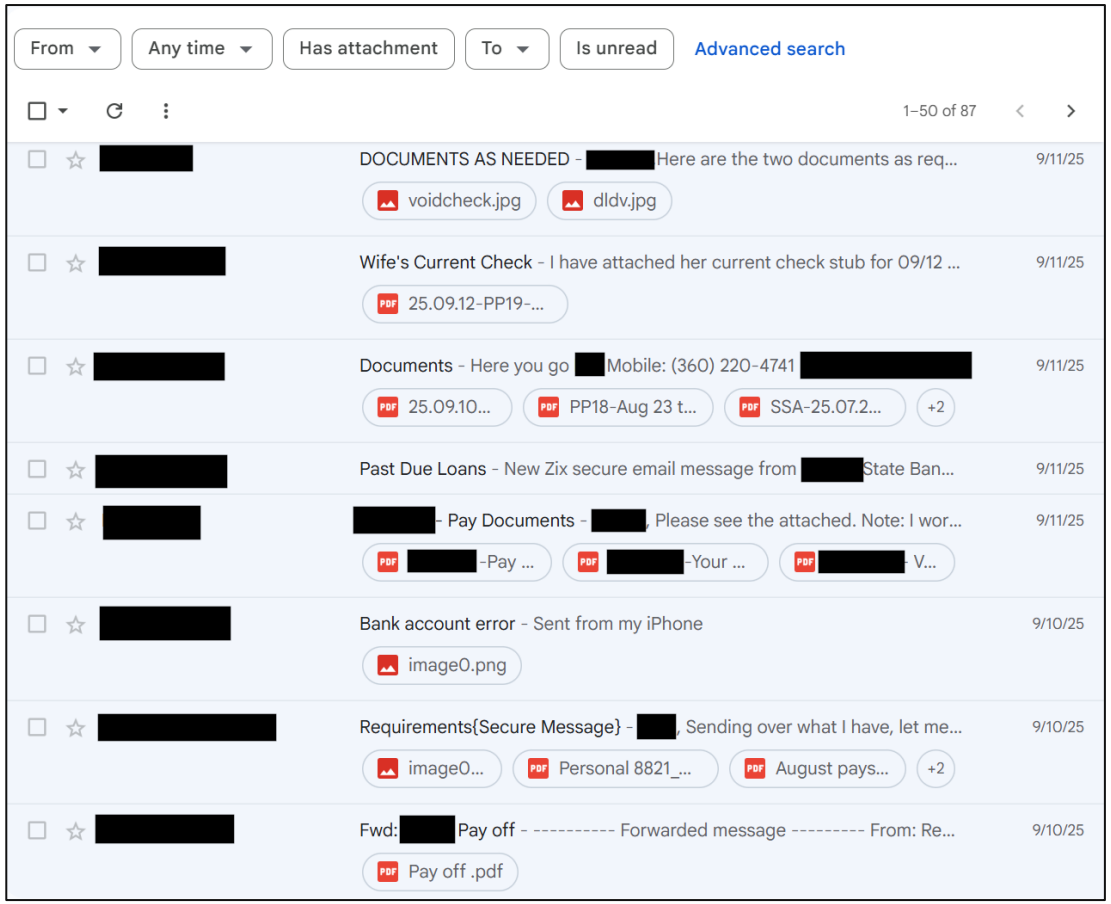
*@toyta.com

↓

attacker@gmail.com

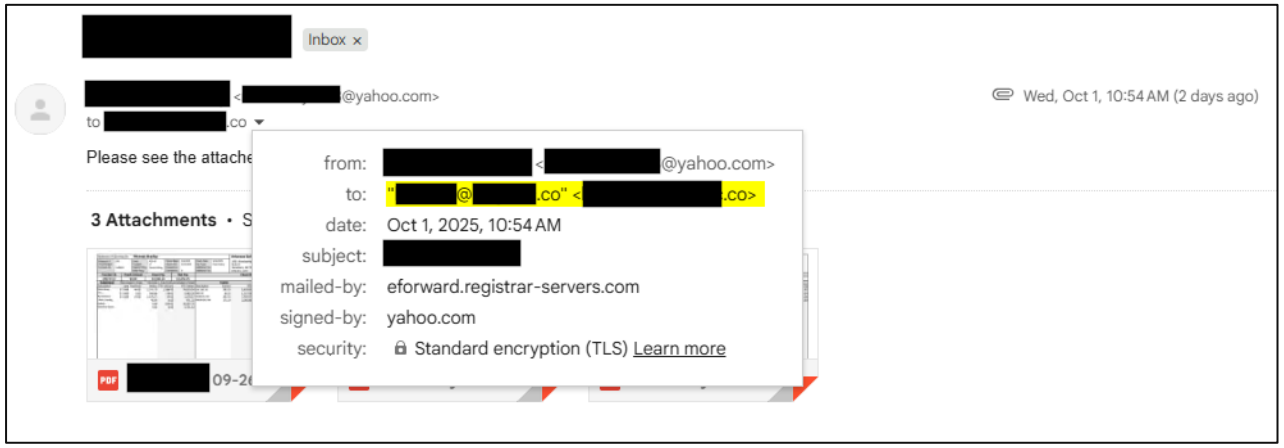
Weaponize Trust… And Typos

Attacker Inbox:

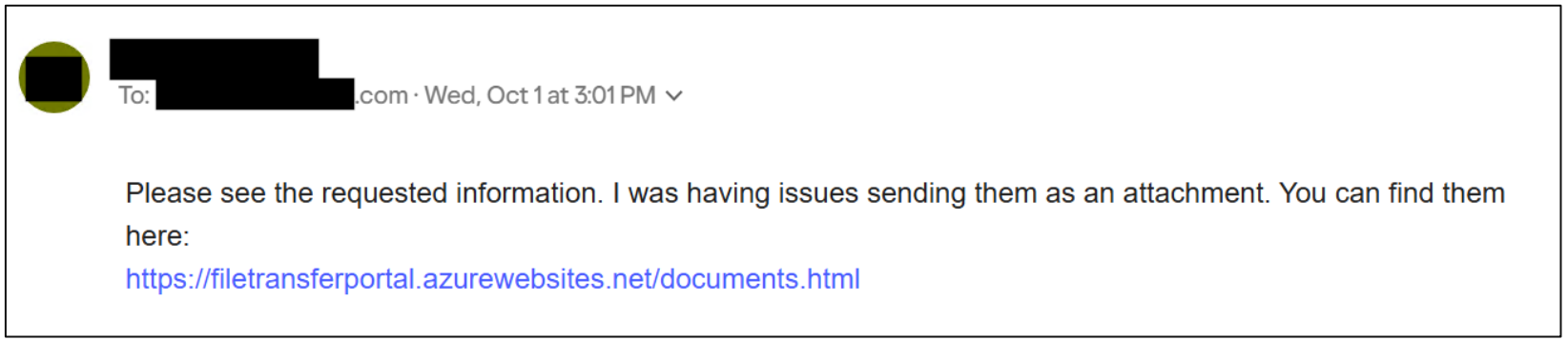


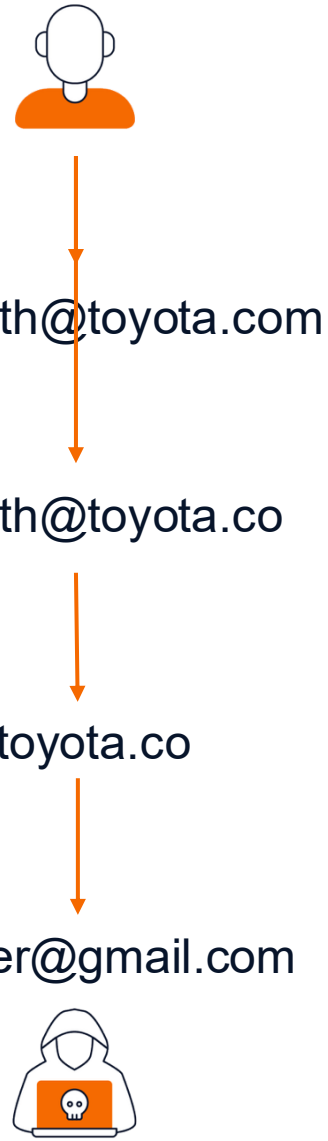
Intercepted Email:

Weaponize Trust… And Typos

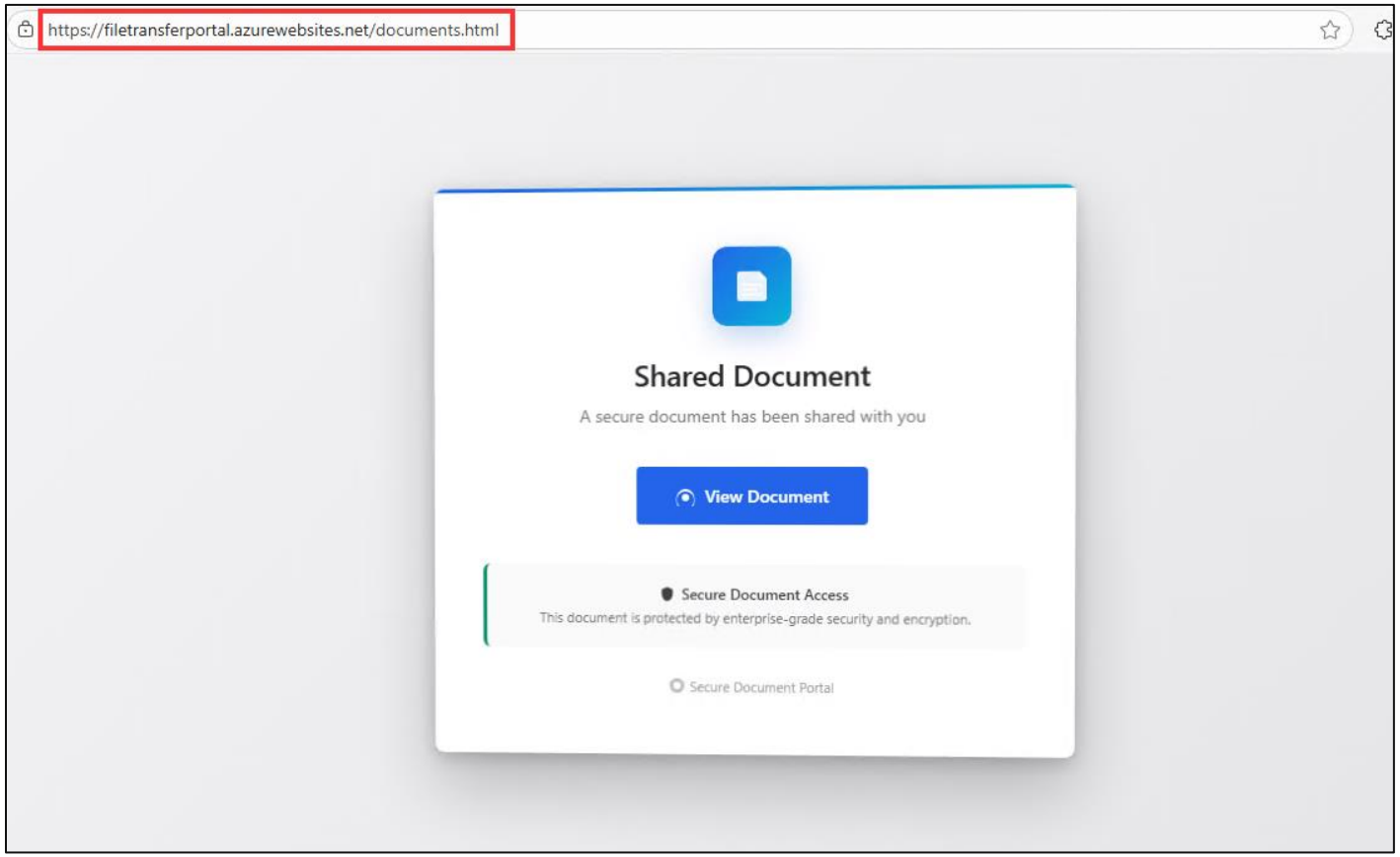


From: first.last@yahoo.com → From: first.last@myyahoo.com



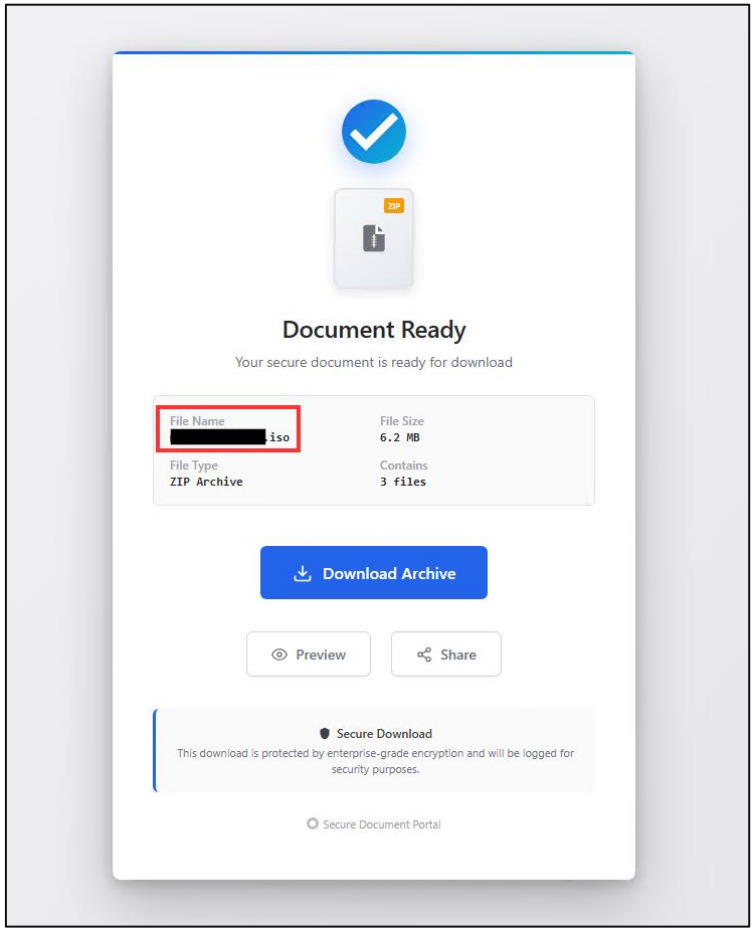


Weaponize Trust… And Typos




```
[REDACTED] - X-Forwarded-For:[REDACTED] Size:5119 - - [01/Oct/2025:20:11:21 +0000] "GET
/transfer/landing/track.gif?page=landing%22 HTTP/1.1" 404 3616
"https://filetransferportal.azurewebsites.net/" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Edg/140.0.0.0"
```

Weaponize Trust… And Typos




```
[REDACTED] - X-Forwarded-For:[REDACTED] Size:5619 - - [01/Oct/2025:20:11:30 +0000] "GET
/filetransfer/track.gif?page=download HTTP/1.1" 404 4063
"https://filetransferportal.azurewebsites.net/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 Edg/140.0.0.0"
```

Weaponize Trust… And Typos

Target process connects to remote file on Apache Web Server:

```
[REDACTED] - X-Forwarded-For:[REDACTED] Size:5036 - - [01/Oct/2025:20:11:51 +0000] "GET /homepage
HTTP/1.1" 200 3963 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; Win64; x64;
Trident/7.0; [REDACTED]"
[REDACTED] - X-Forwarded-For:[REDACTED] Size:1386 - - [01/Oct/2025:20:11:53 +0000] "GET /homepage
HTTP/1.1" 200 649 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; Win64; x64;
Trident/7.0; [REDACTED]"
```

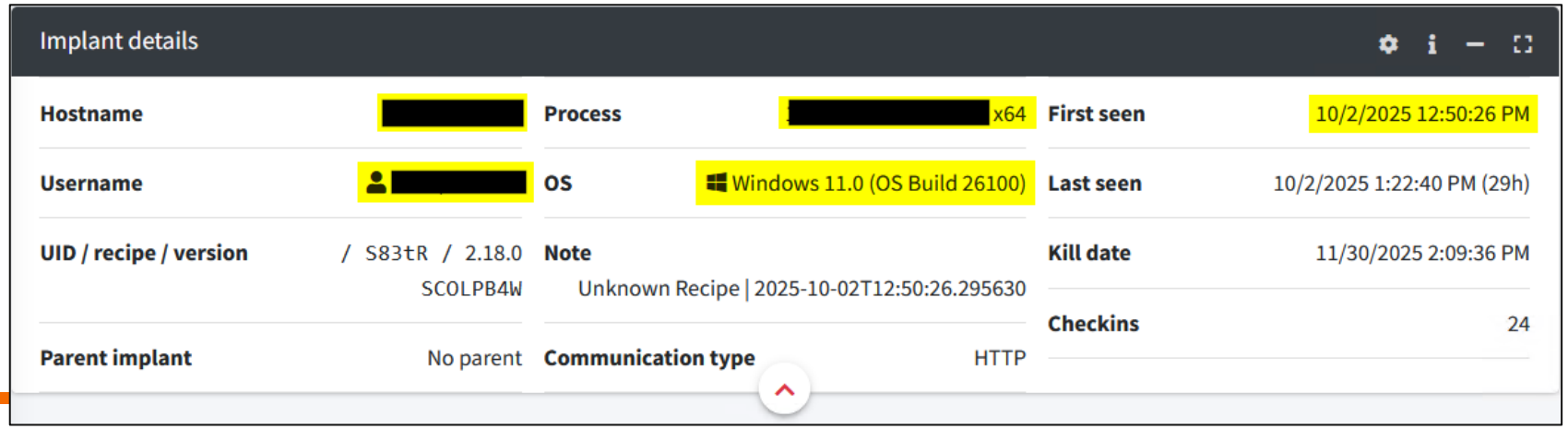
Employee Views Decoy Page:

```
[REDACTED] - X-Forwarded-For: [REDACTED] Size:232598 - - [01/Oct/2025:20:11:54 +0000] "GET
/[REDACTED]/[REDACTED]_Combined-Files.pdf HTTP/1.1" 200 231027 "-" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
```

Weaponize Trust… And Typos

Armed web server to where the process connects to a file containing remotely hosted malicious code. The code is executed by the process:

```
[REDACTED] - X-Forwarded-For: [REDACTED] Size:1322592 - - [02/Oct/2025:12:50:00 +0000] "GET /homepage
HTTP/1.1" 200 1321327 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; Win64; x64; Trident/7.0;
Microsoft [REDACTED])"
[REDACTED] - X-Forwarded-For: [REDACTED] Size:482514 - - [02/Oct/2025:12:50:06 +0000] "GET /homepage
HTTP/1.1" 200 481324 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; Win64; x64; Trident/7.0;
Microsoft [REDACTED])"
[REDACTED] - X-Forwarded-For: [REDACTED] Size:6898 - - [02/Oct/2025:12:50:26 +0000] "POST
/meeting/join/conference/room/audio/settings HTTP/1.1" 200 4322 "-" "Mozilla/5.0 (ZOOM.Win 10.0 x64)"
```



Weaponize the Business Model Against Them

Risk Exposed:

- PII access without any effort
- Access to internal messaging services
- Reputational damage – loss of consumer trust

Value to the Client:

- Employee training point to always check the email
- Implementation of stricter email security rules
- Bought up all potential typo-squatted domains

Weaponize Whales

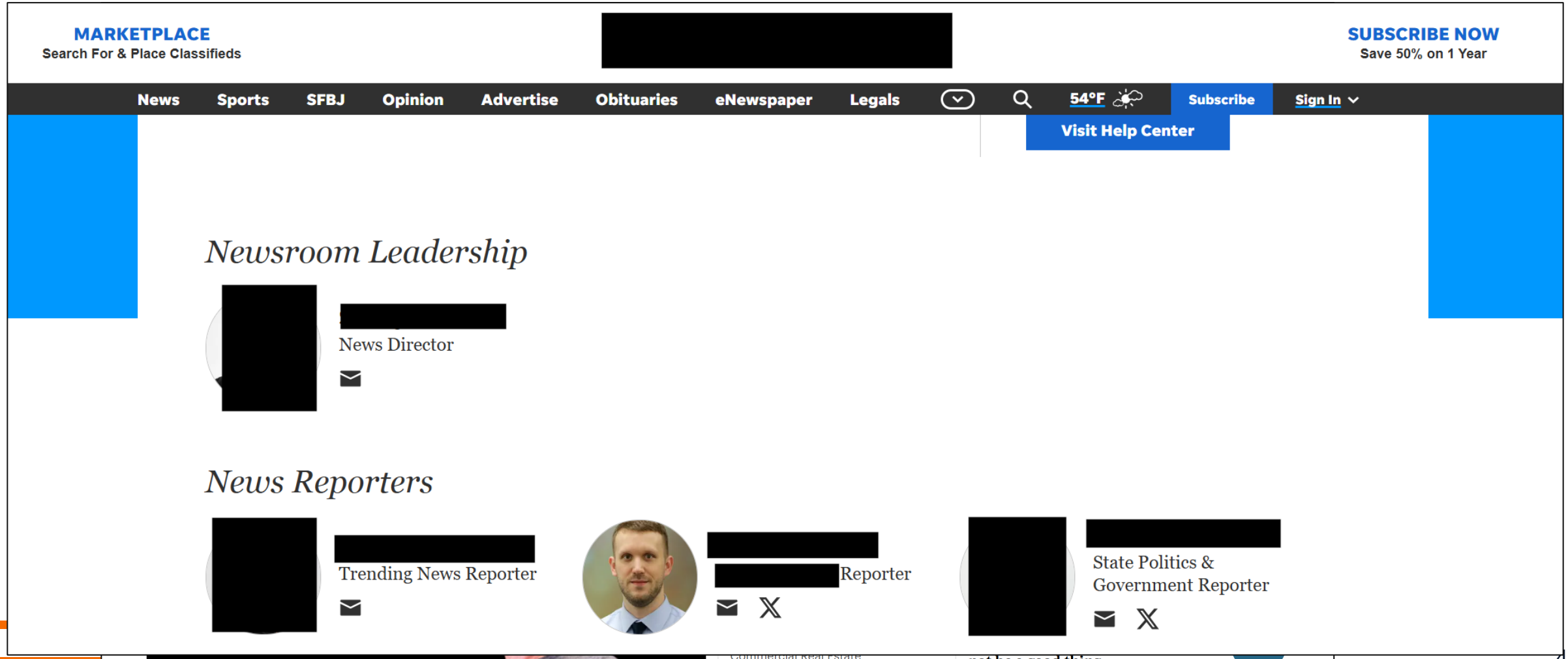
Scenario:

During a Black Box against a major regional telecommunications provider, I identified that the company actively sought out media exposure.

Weaponizing this tendency afforded me access to the C-Suite.

Weaponize Whales

Business Journals



Weaponize Whales

Target: Marketing Manager

Marketing Manager

Hailing from the sweeping skies and rolling prairies of [redacted], [redacted] is no stranger to the world of marketing, event planning and creative leadership. Dipping her toes has never been [redacted]'s life strategy. Unsurprisingly, when she began her career in marketing, it was with a deep dive into entrepreneurship, launching successful photography businesses and expanding her skill set into filmmaking, social media, website development and graphic design.

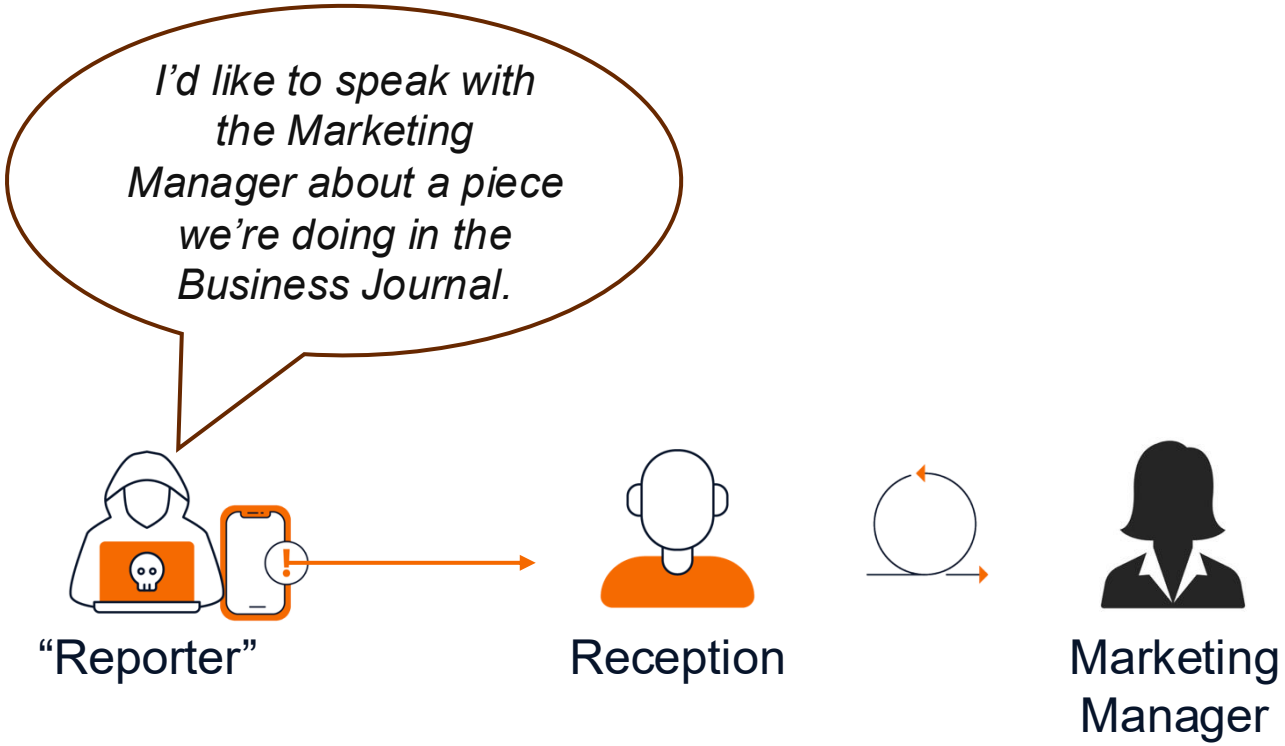
Today, [redacted] manages the marketing team at [redacted], where she blends creativity with strategy to support the company's mission and elevate its business-to-business communications. Her collaborative approach strengthens alignment between marketing and sales, resulting in better experiences for clients, employees and partners alike.

With a strong background in graphic design, photography and event planning, [redacted] oversees major external campaigns and coordinates [redacted]'s large-scale events, including the [redacted] esports series, two annual golf tournaments and the [redacted] Sales Seminar. She also speaks at public events, including her TEDx[redacted] talk on [redacted] which was elevated to the global TED.com platform.

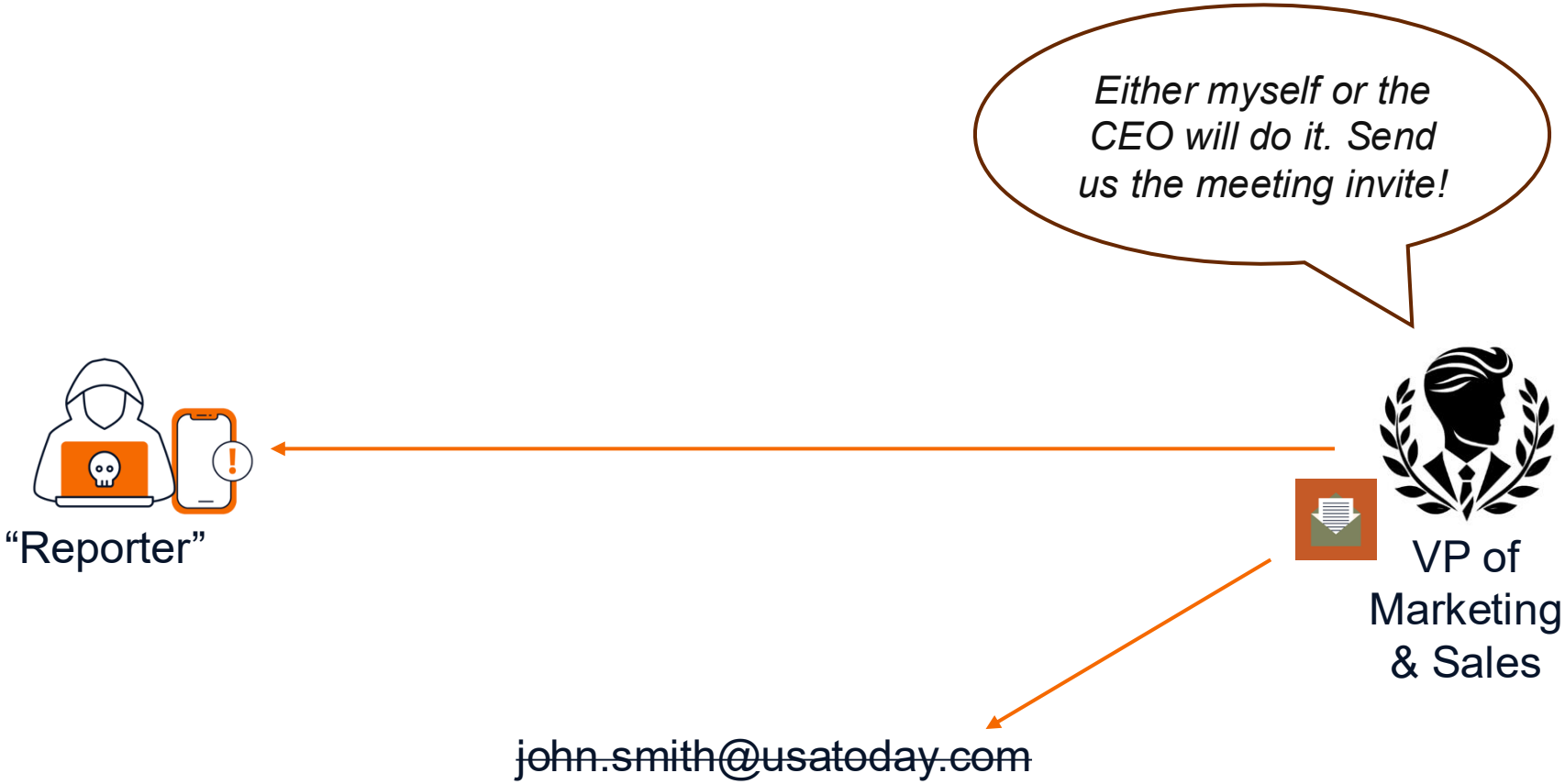
Outside the office, [redacted] loves rock climbing, cycling fast around the [redacted] recreation trails, foraging in the woods and opening virtual treasure chests with her three boisterous sons through their favorite video games. She brings enthusiasm, innovation and a team-first mentality to everything she does.

Futuristic • Strategic • Positivity • Woo • Empathy

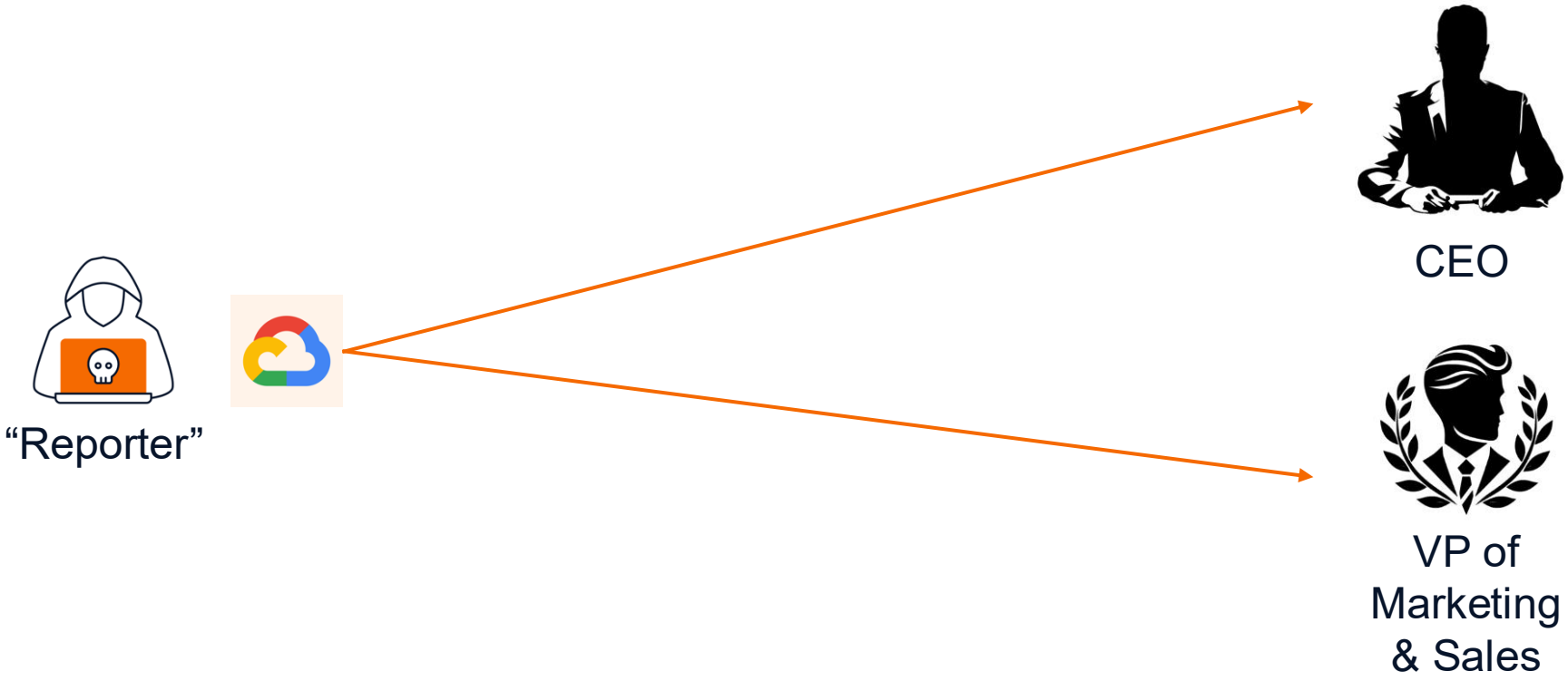
Weaponize Whales



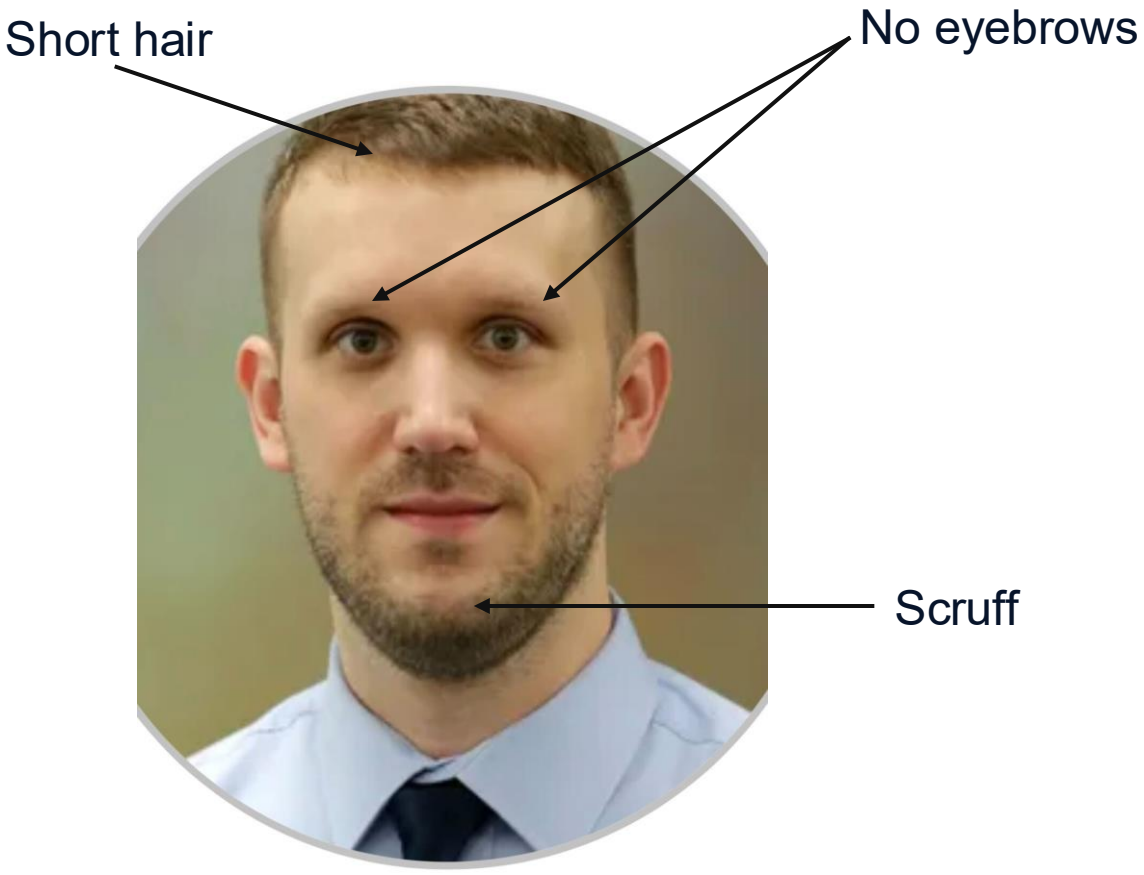
Weaponize Whales



Weaponize Whales



Weaponize Whales

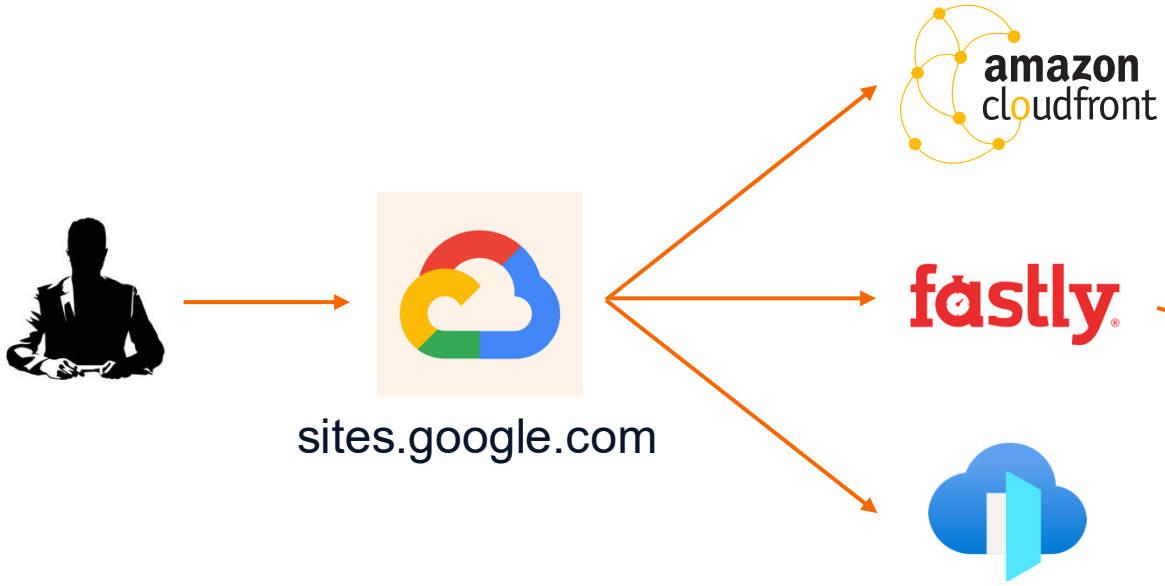


Weaponize Whales

Plan: At the beginning of the meeting, ask, “Did I send you our media consent form?” Then send him to an HTML smuggling page.

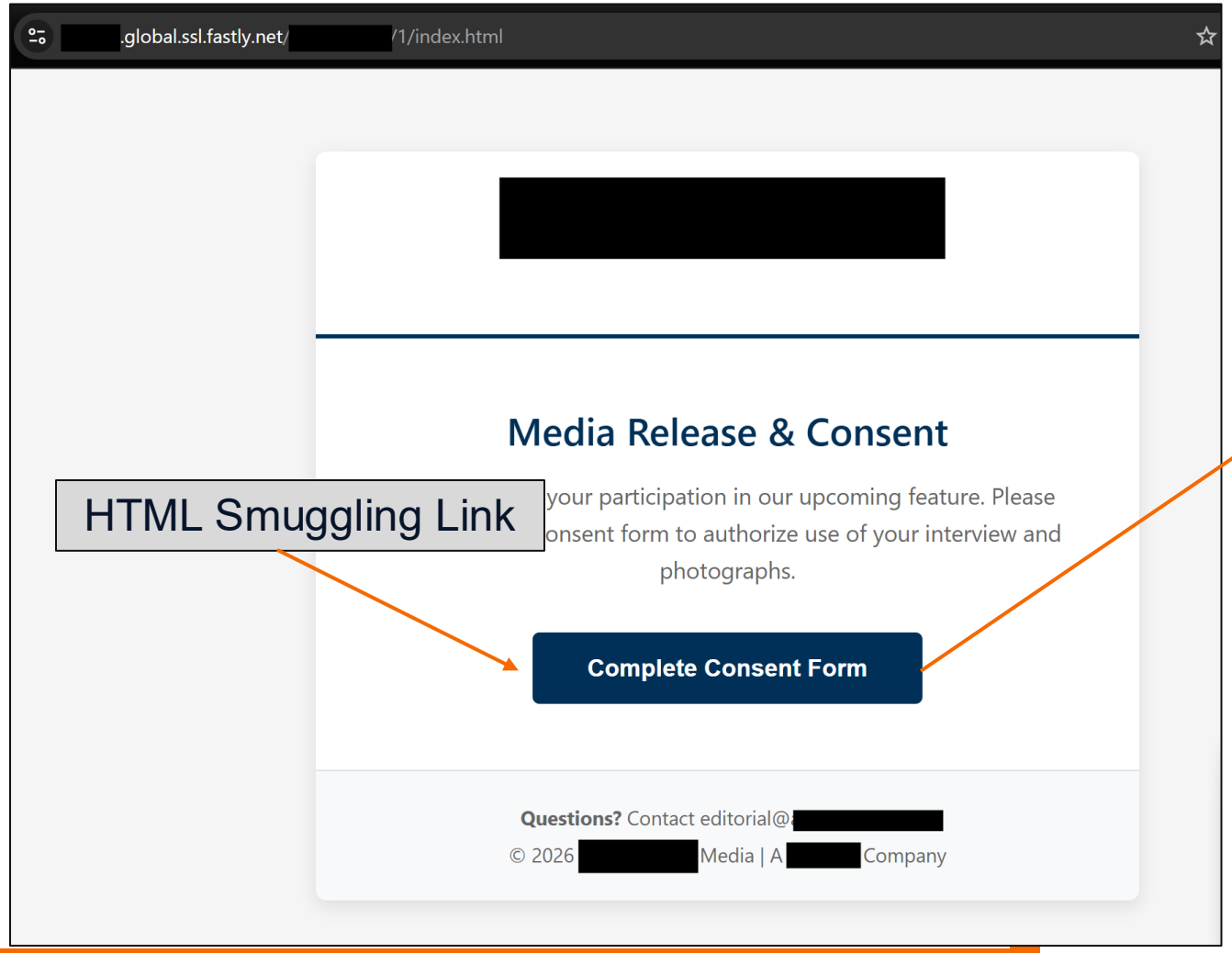
Problem:

- How do I make sure he can get to my CDN?



https://32h89r.global.ssl.fastly.net/[smuggling-page]

Weaponize Whales



HTML Smuggling Link

ZIP Archive

ISO Container

- Signed EXE
- Dependencies (hidden)
- Malicous code (hidden)

Weaponize Whales

Weaponize Whales

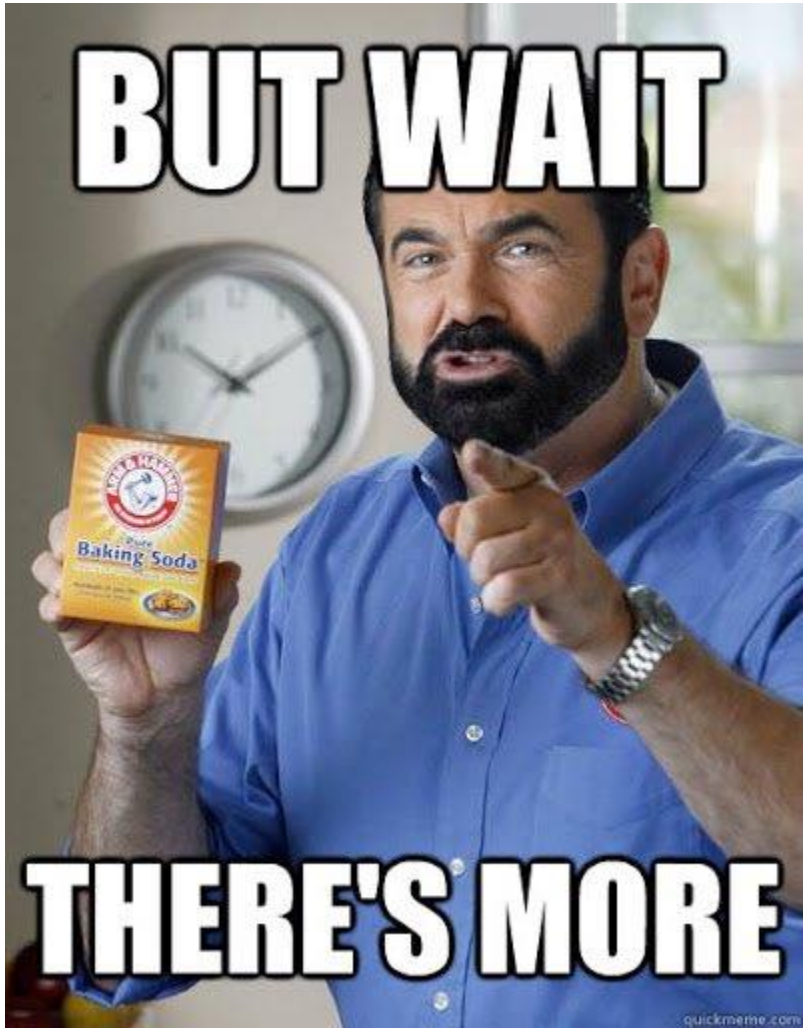
Risk Exposed:

- Reputational damage
- Access to executive data
- Internal SE from this position could prove lucrative

Value to the Client:

- More thorough call screening
- C-Suite security investment buy-in

Weaponize Whales

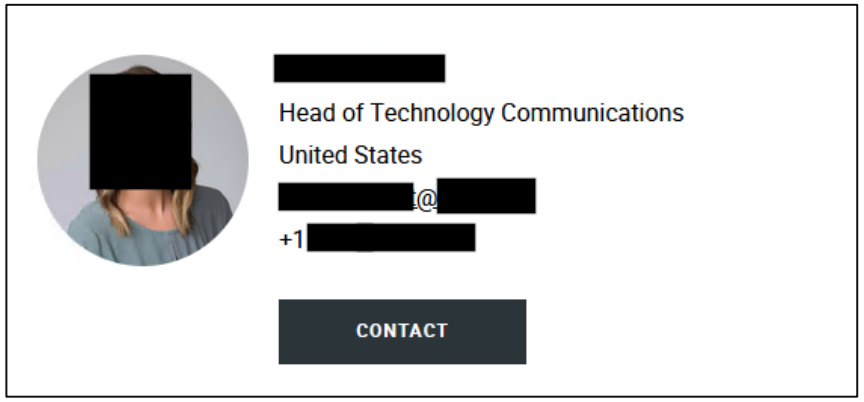


Scenario:

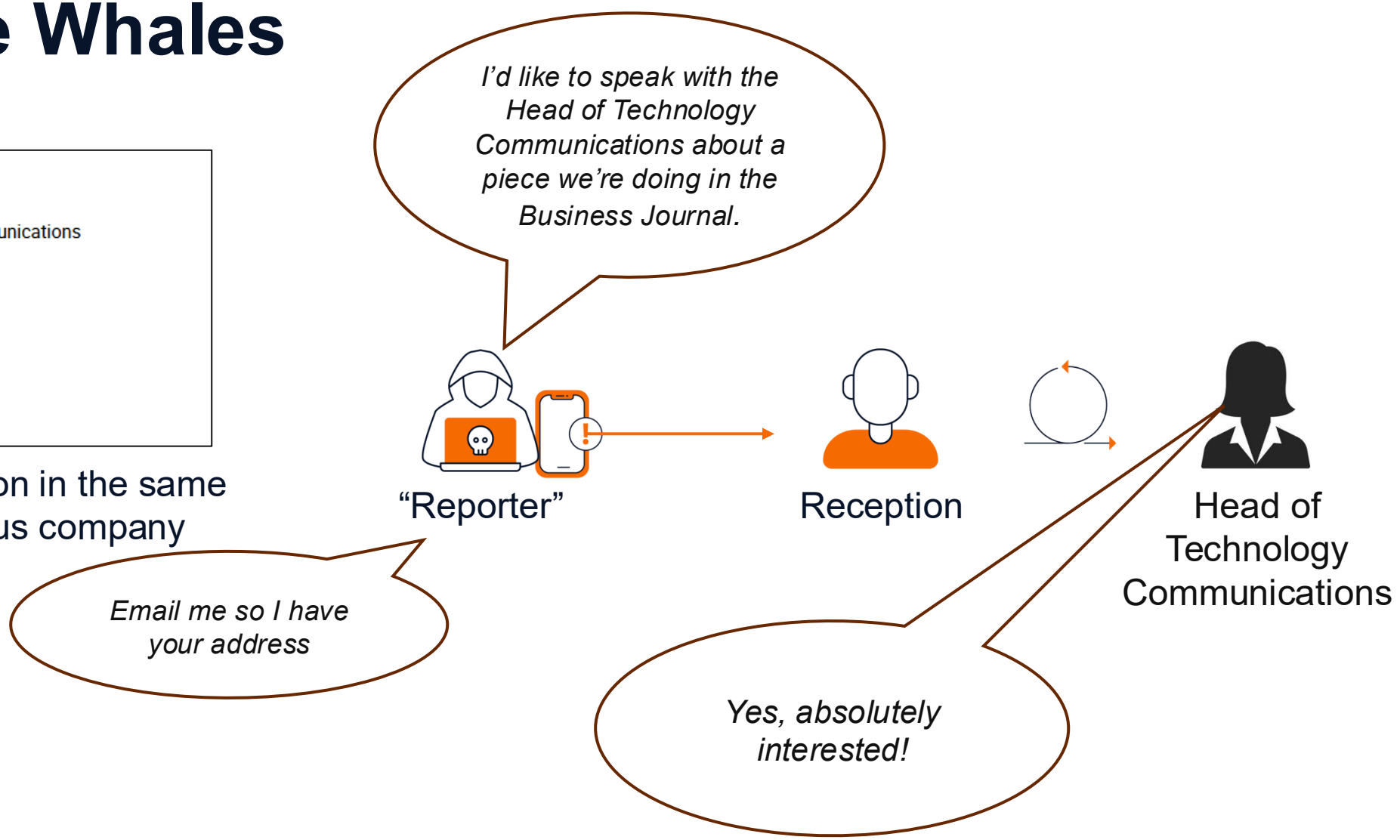
The journalist pretext was weaponized during a recent engagement against a major company that creates automated (AI) systems for agricultural equipment.

Technical and human hurdles had to be overcome to obtain initial access.

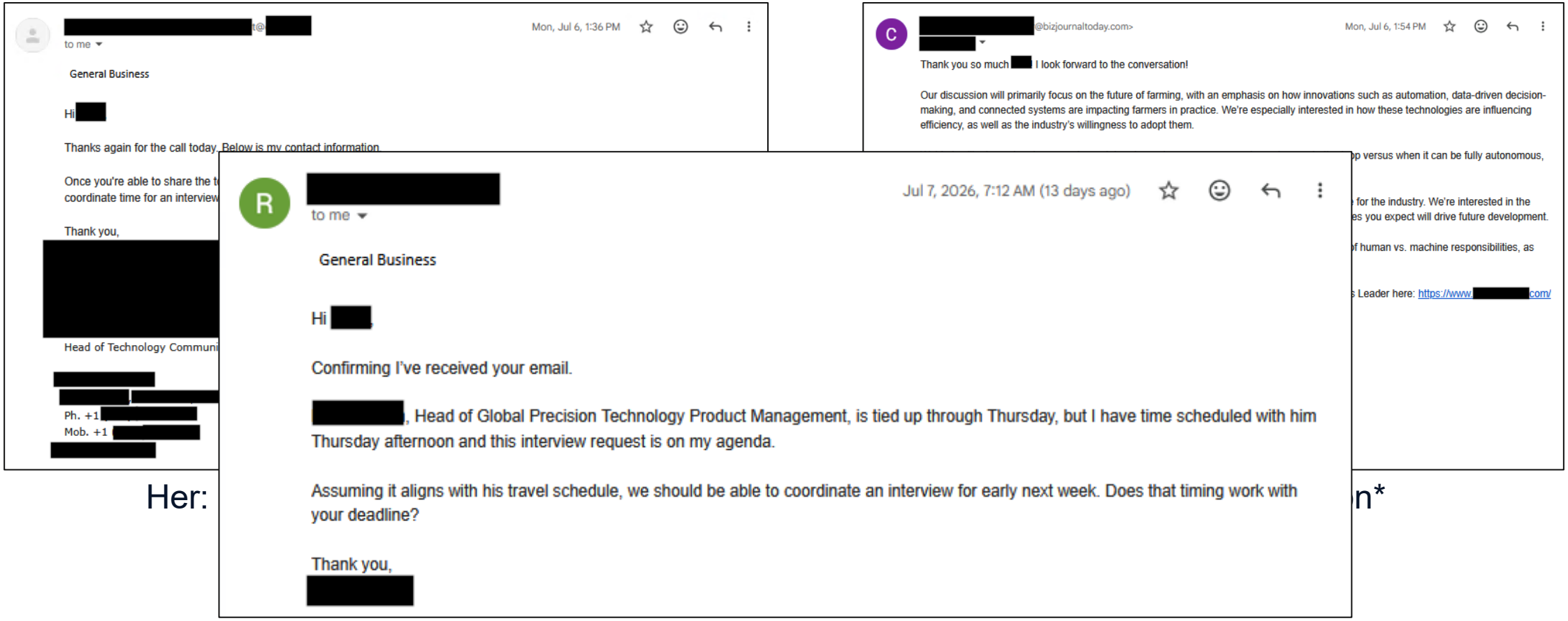
Weaponize Whales



LinkedIn showed her location in the same city and state as the previous company



Weaponize Whales



Mon, Jul 6, 1:36 PM

to me

General Business

Hi [redacted]

Thanks again for the call today. Below is my contact information.

Once you're able to share the t
coordinate time for an interview

Thank you,

[redacted]

Head of Technology Communi

[redacted]

Ph. +1[redacted]

Mob. +1[redacted]

[redacted]

Mon, Jul 6, 1:54 PM

Thank you so much [redacted] I look forward to the conversation!

Our discussion will primarily focus on the future of farming, with an emphasis on how innovations such as automation, data-driven decision-making, and connected systems are impacting farmers in practice. We're especially interested in how these technologies are influencing efficiency, as well as the industry's willingness to adopt them.

...p versus when it can be fully autonomous,

... for the industry. We're interested in the
...es you expect will drive future development.

...f human vs. machine responsibilities, as

... Leader here: https://www.[redacted].com/

Jul 7, 2026, 7:12 AM (13 days ago)

to me

General Business

Hi [redacted]

Confirming I've received your email.

[redacted], Head of Global Precision Technology Product Management, is tied up through Thursday, but I have time scheduled with him Thursday afternoon and this interview request is on my agenda.

Assuming it aligns with his travel schedule, we should be able to coordinate an interview for early next week. Does that timing work with your deadline?

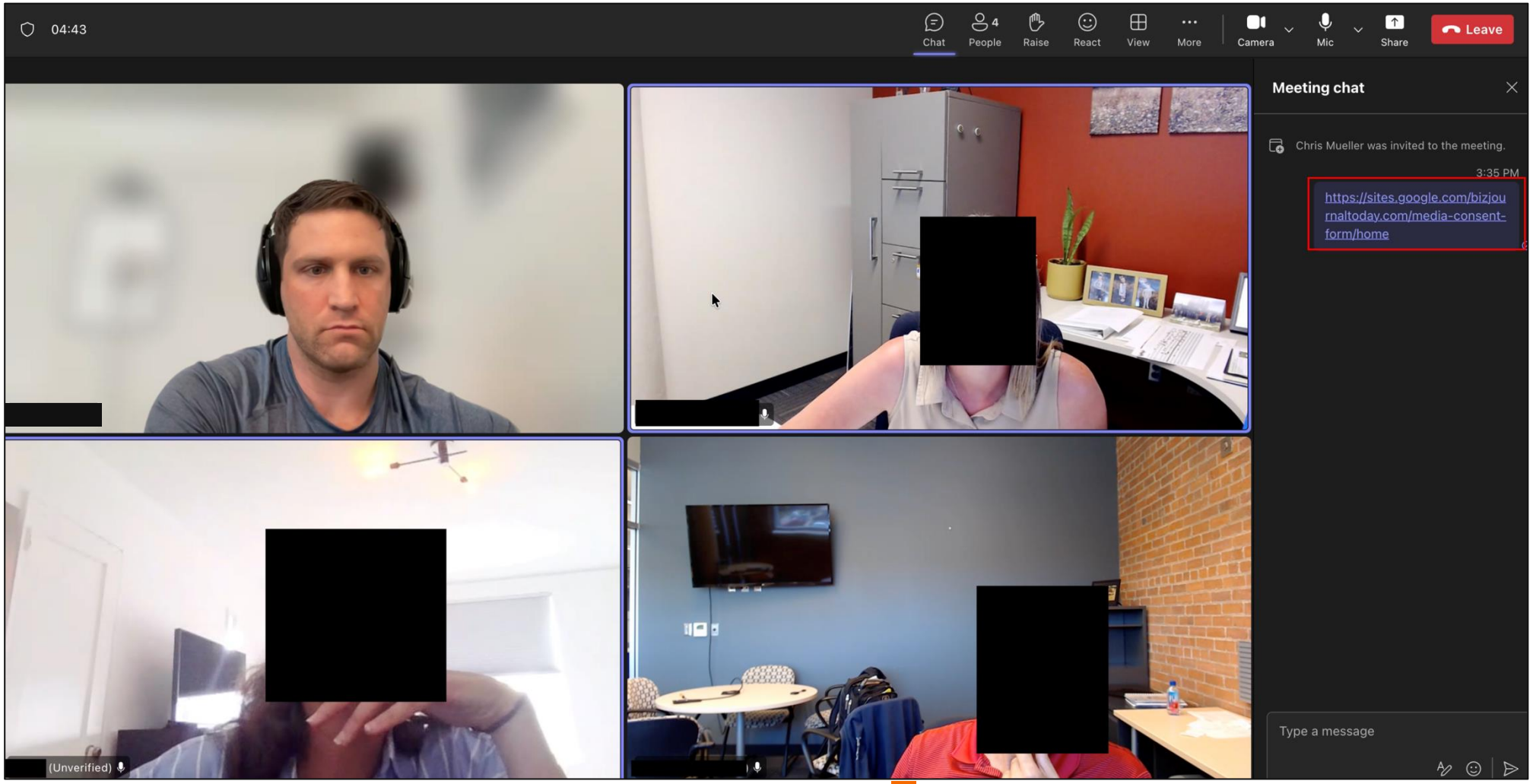
Thank you,

[redacted]

Her: ...n*

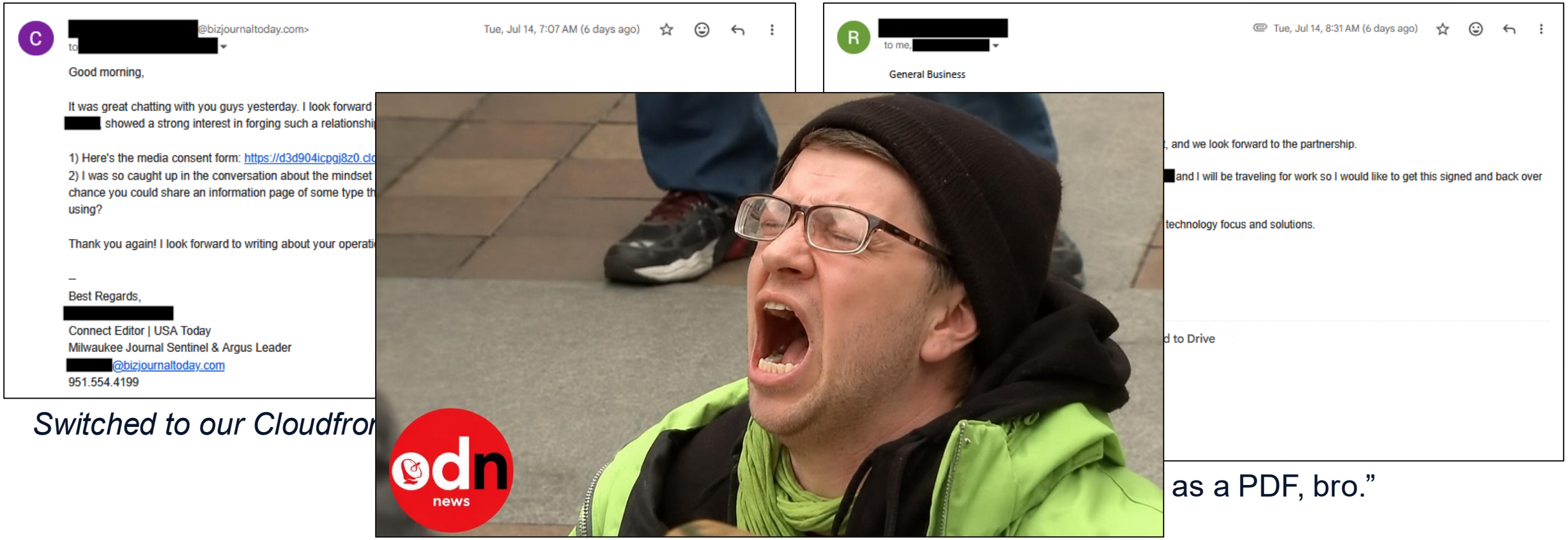
Her: "The Head of Global Precision Technology Product Management will do the interview!"

Weaponize Whales



sites.google.com

Weaponize Whales - *Preserve the Pretext*



Switched to our Cloudfron

as a PDF, bro.”

Weaponize Whales – *Switch Gears*

The Next Frontier for the First Frontier

How artificial intelligence is changing agriculture without replacing the farmer

[redacted]

Agriculture has always been an industry of judgment.

Farmers read the sky, the soil, the equipment, the crop, the calendar and the balance sheet all at once. They make decisions in narrow windows, often under pressure, and often with consequences that last an entire season. A missed planting window, an equipment failure during harvest or an inefficient chemical application can ripple across months of work.

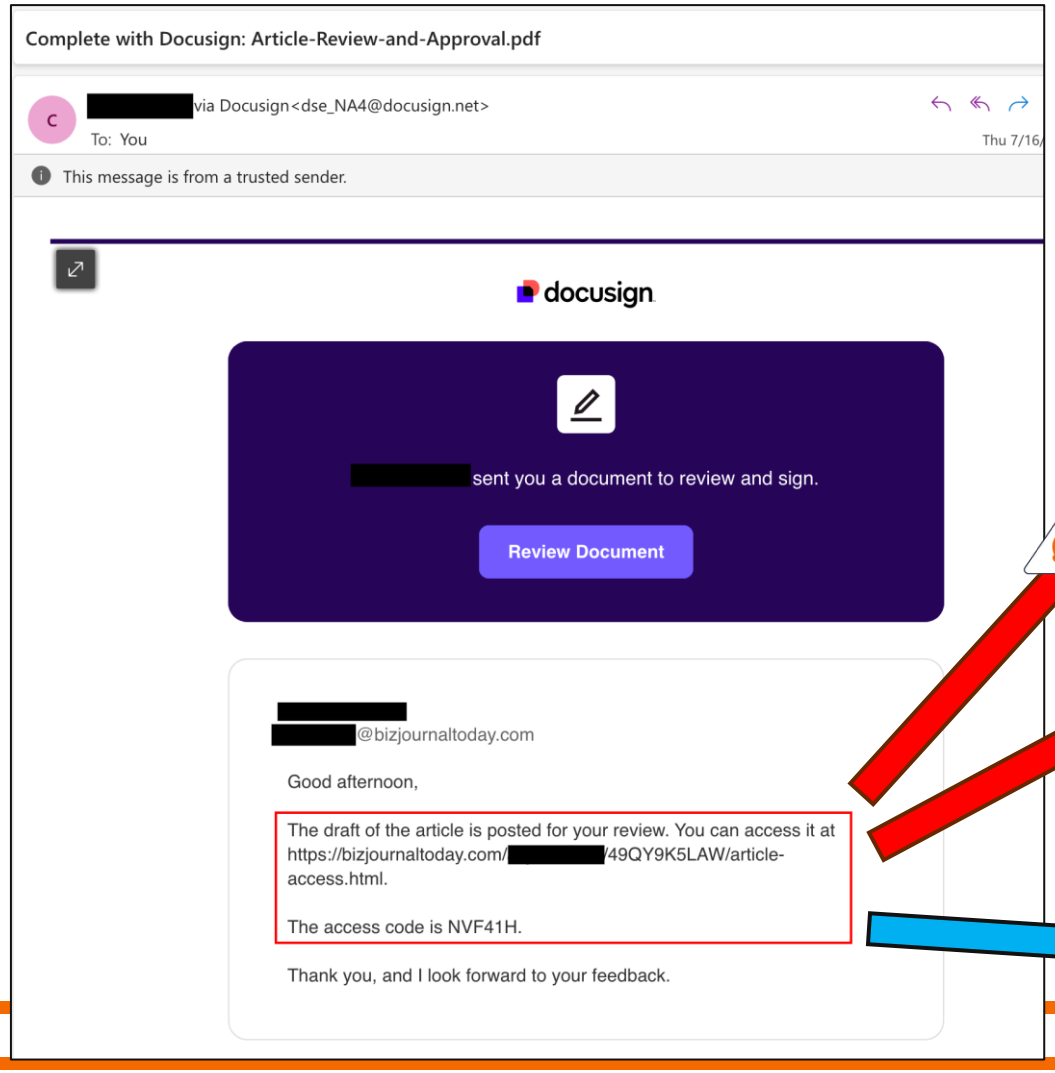
Now, one of the world's oldest industries is being reshaped by one of the world's newest.

Artificial intelligence is coming to agriculture, but not in the way many people imagine. It is not simply a chatbot in the cab or a software platform telling farmers how to run their land. In the most advanced equipment, AI is being embedded directly into tractors, combines, sprayers and other machines designed to operate in real fields, under real conditions, with human operators still at the center.

+

=

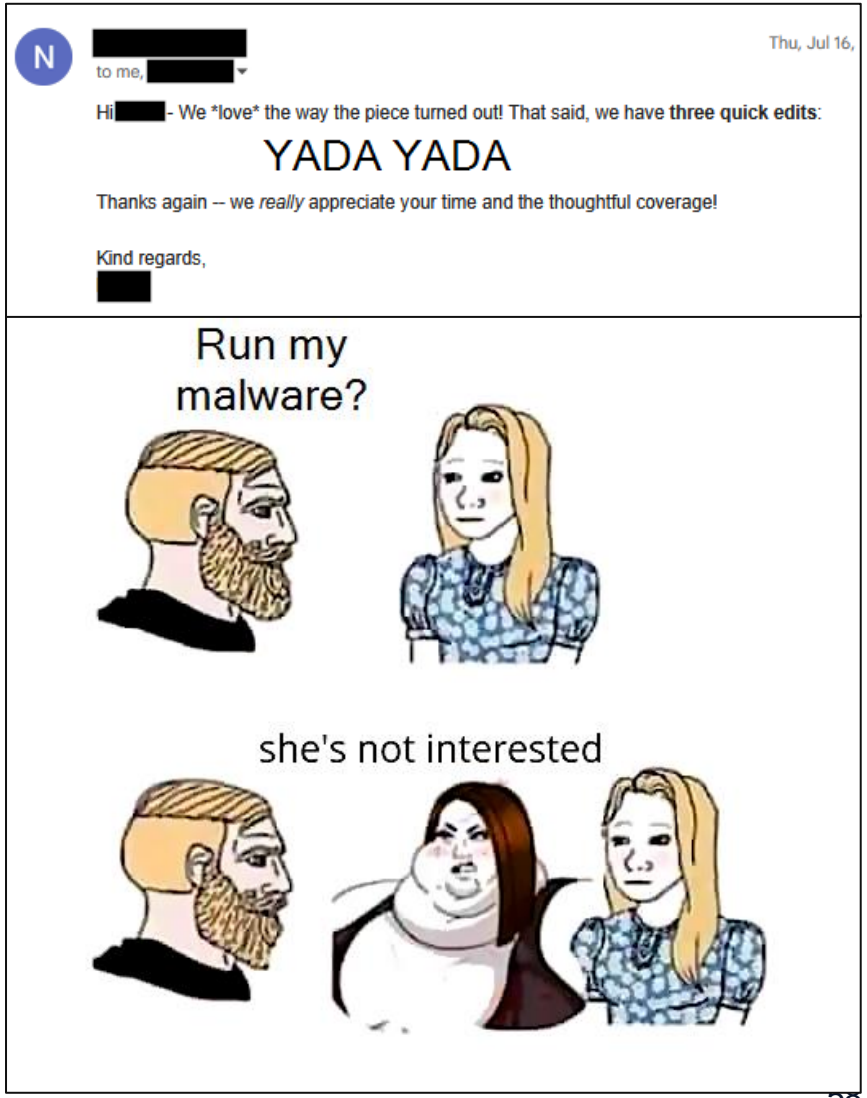
Weaponize Whales – *Switch Gears*



Product Manager

Technology Comms

PR Rep



Weapo

On Mon, Jul 20, 2026 at 11:08 AM [redacted]

Hi [redacted] - Just wanted to follow up on the

Thanks again for the thoughtful reporting
clarify anything.

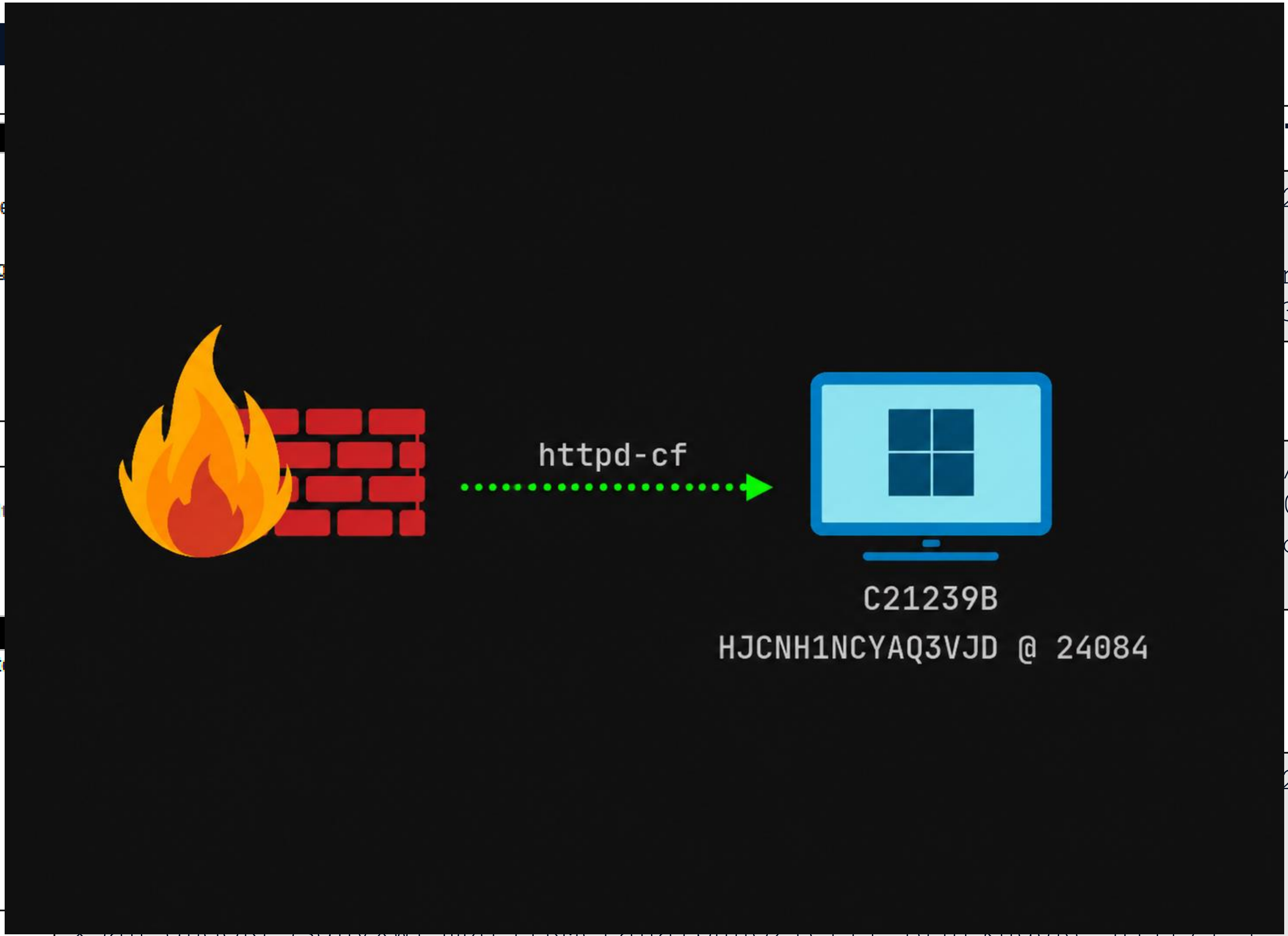
Best,
[redacted]

C [redacted] @bizjournal
to [redacted]

HI [redacted],

I incorporated your edits and sent [redacted]
their signatures before I can submit t

--
Best Regards,
[redacted]
Connect Editor | USA Today
Milwaukee Journal Sentinel & Argus
[redacted] @bizjournaltoday.com
951.554.4199



TML Smuggling Page

```
26:18:21:17 +0000]

n64; x64)
37.36 Edg/150.0.0.0"
```

Decoy Page

```
/2026:18:22:03 +0000]
08 "-" "Mozilla/5.0
cko) Chrome/150.0.0.0
```

Callback URL

```
26:19:09:36 +0000]

200 5632 "-"
"Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; MAM2)"
```

Conclusion

- You, your employees, and leadership need to be aware of this
- Re-evaluate your processes, applications, and training
- More may be at stake than just company data
- ***Stress the system***

Questions?