





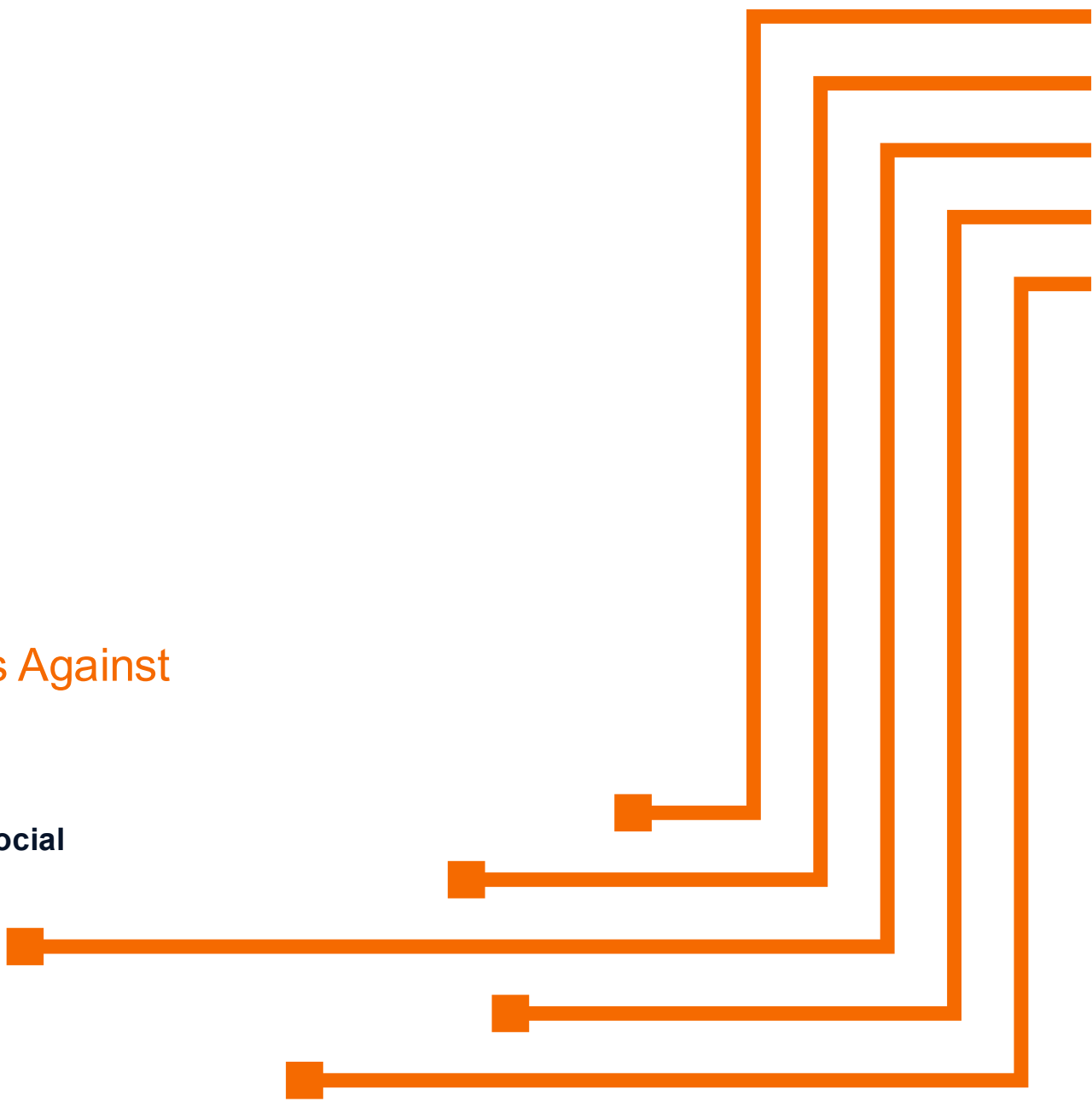
Weaponizing Trust

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



NetSPI™

2024-Present

Principal Security Consultant

- Red Team Operator
- Social Engineer



Fieldra



Offensive Security Certified Professional (OSCP)



Certified Information Systems Security Professional (CISSP)



Certified Red Team Operator (CRTO)



GIAC Cloud Penetration Tester (GCPN)



CompTIA Security+



JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

➤ Instructor



PROTEUS
TECHNOLOGIES

➤ Founder
& CEO

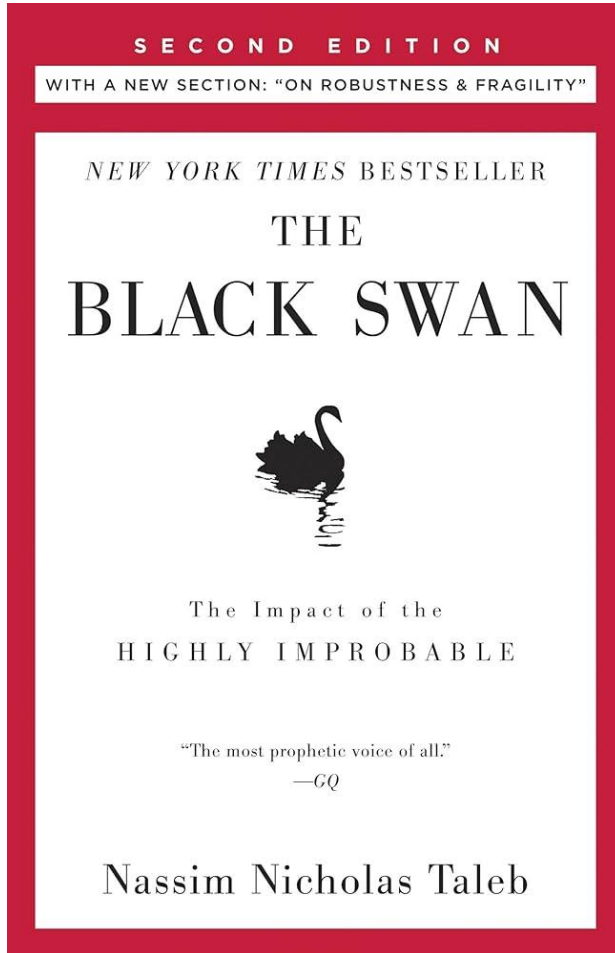


Agenda

- 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.



 Penetration Testing Find & Exploit Vulnerabilities	 Social Engineering Weaponize Human Trust	 Red Teaming Simulate Real Adversaries
OBJECTIVE Identify and exploit technical vulnerabilities in systems and infrastructure	OBJECTIVE Test human defenses by exploiting trust and business processes	OBJECTIVE Achieve specific goals while evading detection
SCOPE Defined and limited. Specific systems or network segments	SCOPE Human attack surface—employees, help desk, executives	SCOPE Entire organization including people, processes, and technology
APPROACH • Loud and visible to defenders • Time-boxed (1-2 weeks) • Technical exploitation focus	APPROACH • Phishing, vishing, smishing • OSINT-driven attacks • Psychological manipulation	APPROACH • Objective-oriented engagements • Stealth and evasion critical • Multi-vector attacks • Phishing, vishing, smishing • OSINT-driven attacks • Psychological manipulation
DELIVERABLE Technical report with findings, risk ratings, and remediation	DELIVERABLE Metrics on user susceptibility awareness training recommendations	DELIVERABLE Technical report showing objectives achieved, vulnerabilities, and detection gaps



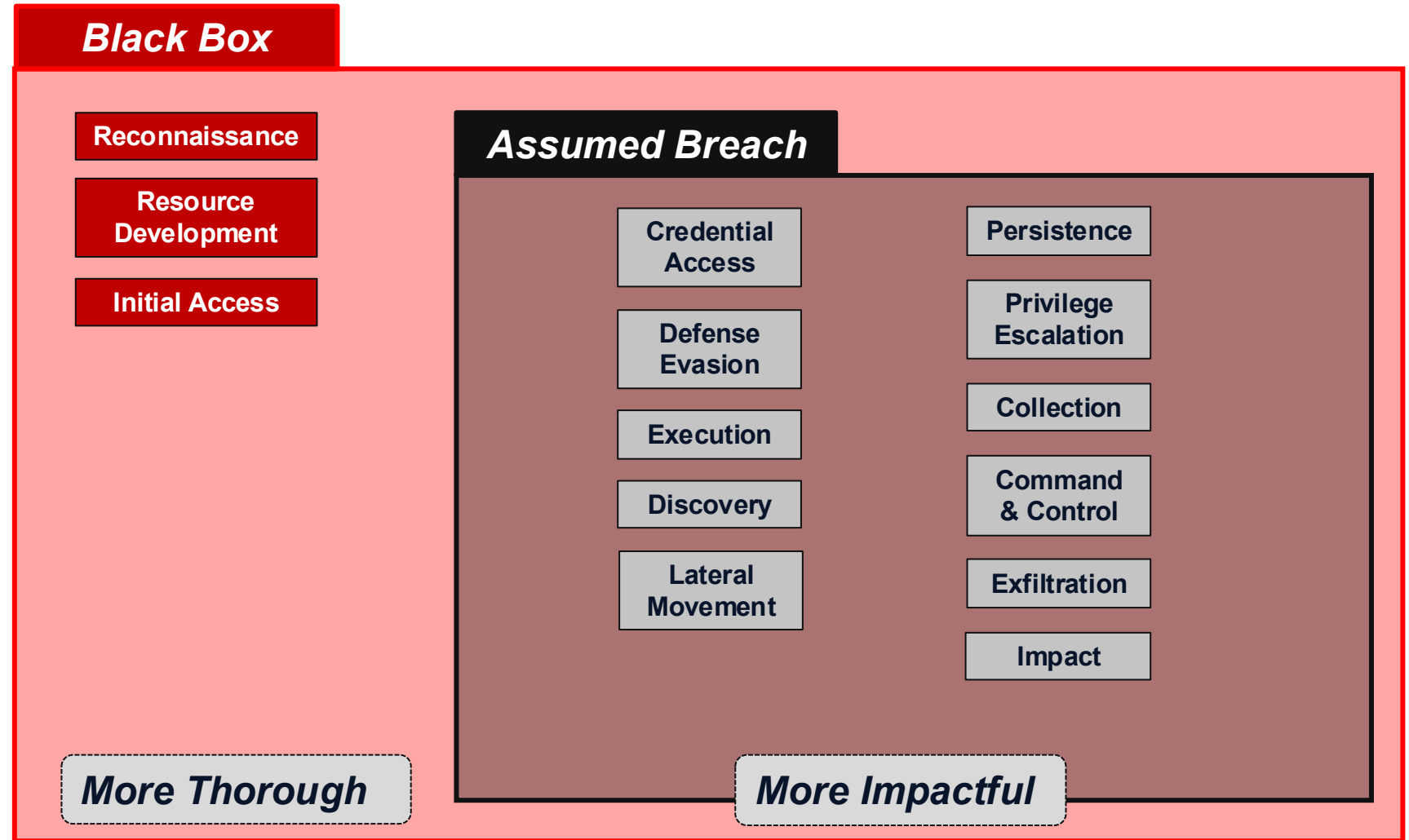
Types of Red Team Operations

Black Box

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

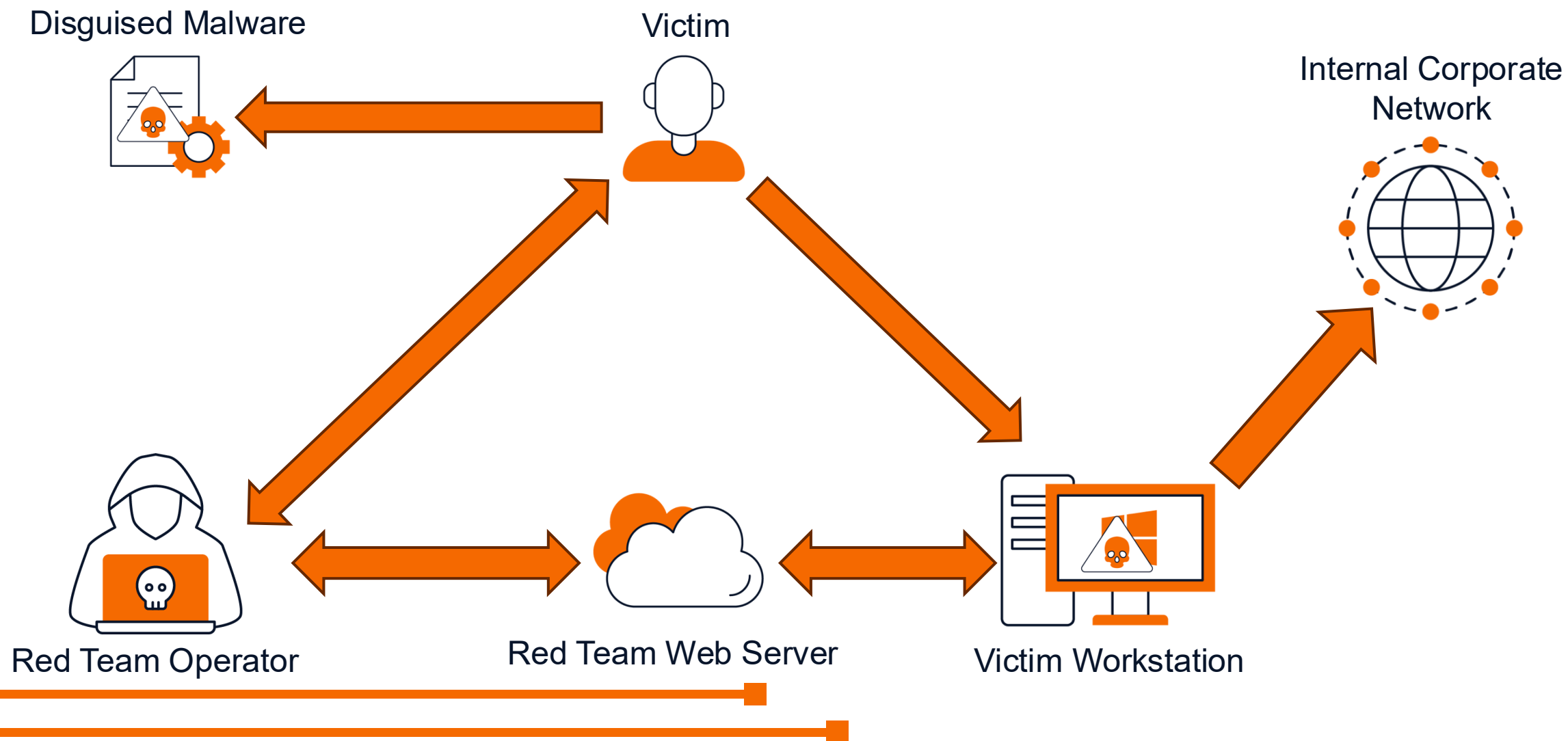
Assumed Breach

- 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

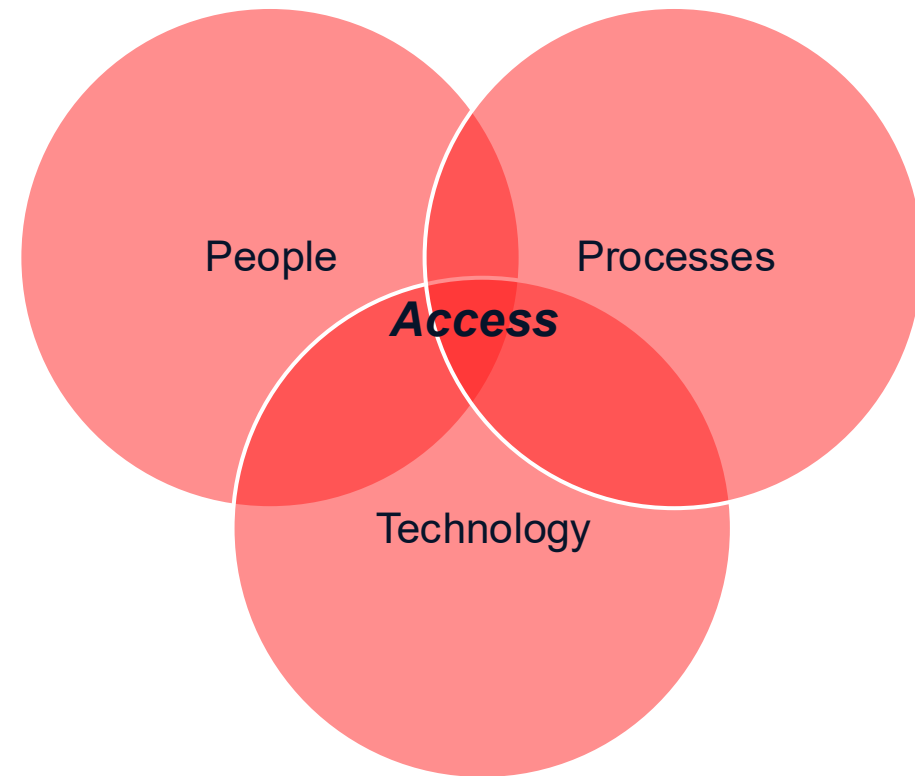
Examples:

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



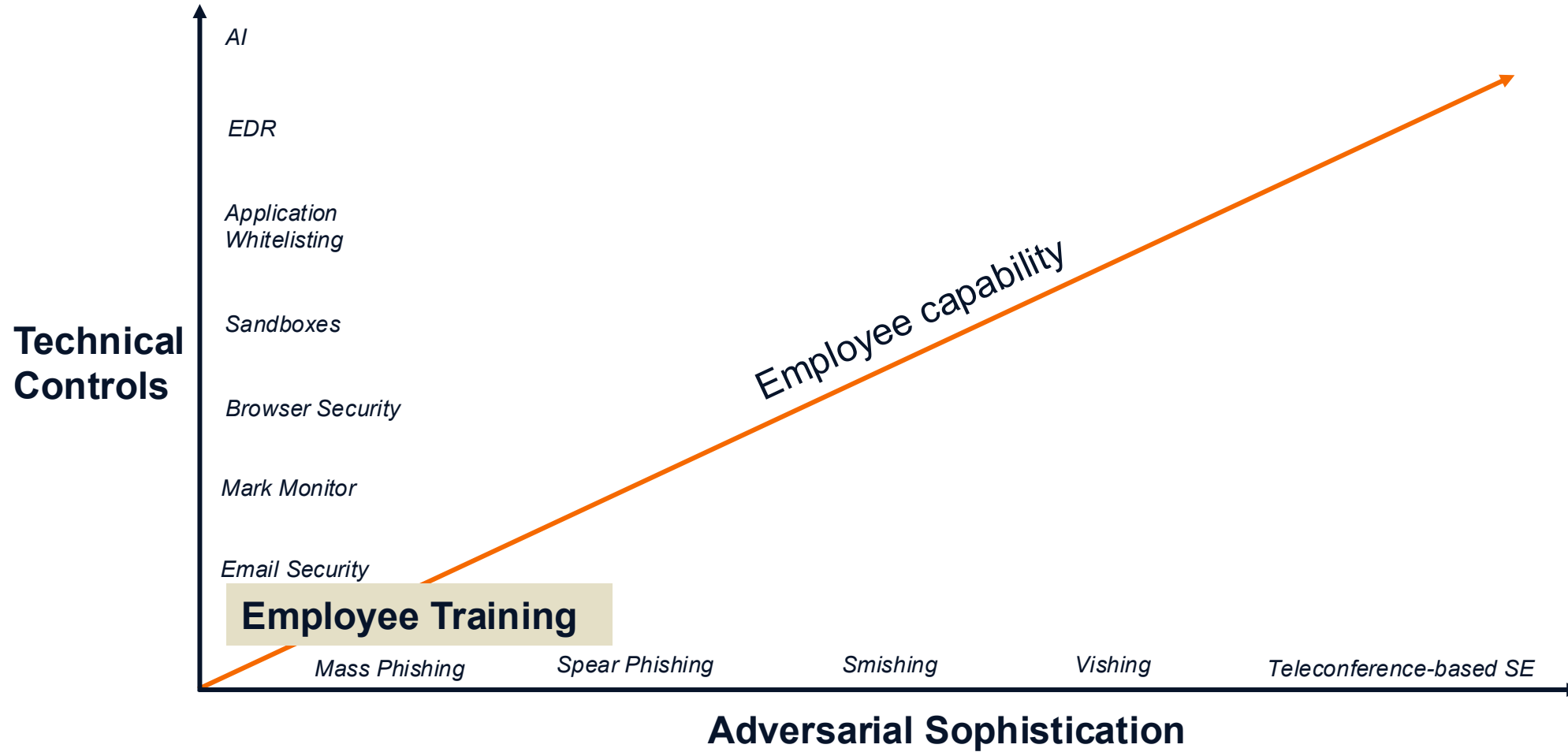
Social Engineering in RTO

- **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:

The screenshot shows a crowdfunding page titled "Support Texas Flood Relief Efforts". The main text reads: "Catastrophic flooding across Texas has deeply affected countless individuals, families, and communities. In times like these, we know [redacted] clients and friends want to help. [redacted] is joining forces with you to do so." Below this is a large red heart graphic. The page shows a progress bar with "\$483,704 RAISED" and a goal of "\$500,000 GOAL". A call to action says "Donate today and watch our impact grow!" with a note: "For every \$2 you donate, Thrivent will add \$1, up to \$250,000.*". At the bottom, there are logos for "CONVOY OF HOPE" and "Austin Disaster Relief".

The screenshot shows a financial advisor's profile page. The header includes the title "Financial Advisor" and "Virtual Advice Team". The profile picture is a woman with long dark hair, smiling, with the text "CALL ME MAYBE" overlaid. The page lists various credentials: "FIC", "AR License", "CA Insurance", "Toll-Free", and "Direct". A section titled "Focused on what matters to you" describes the advisor's mission: "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." Below this is a list of services: "Invest with purpose and manage your assets.", "Plan to pass on a meaningful legacy.", and "Make a difference, locally or globally." A "Professional highlights" section mentions "FIC (Fraternal Insurance Counselor), a designation granted by the Fraternal Field Managers' Association." An "Education and experience" section lists: "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.", and "Bachelor's degree in Business Administration from Mid-America Christian University." A "Personal profile" section includes: "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.", and "I enjoy homesteading with my family, hiking, and good food." A "Giving back" section states: "I support the following charities and causes:" followed by a list of charities (partially redacted) and a note: "I have also participated in or led 4 [redacted] Action Teams to support my community."



Weaponize the Business Model Against Them

FIC

Financial Advisor

Virtual Advice Team

AR License

CA Insurance

virtualadvice

Toll-Free

Direct

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

- a designation granted by the

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

Personal profile

- Married to 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:

-
-
-

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

Schedule an appointment

Virtual Advice Scheduler

Booking for

Meeting with a Advisor

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

Virtual Meeting

New booking

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



Weaponize the Business Model Against Them

From 

To



Hello

It was a pleasure to meet you. You can use the upload button below to send larger files and encrypt them.

Thank you,



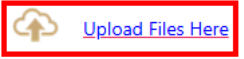
[Schedule a meeting with](#)



[Visit my biography](#)



[Upload Files Here](#)

box with

File Request from at

Thanks! I uploaded the files. The password is . Looking forward to our meeting tomorrow!

Respectfully,

Sent with [Proton Mail](#) secure email.

FIC

Financial Advisor

CA Insurance ID

AR License



Weaponize the Business Model Against Them

In ISO and Password Protected ZIP:

	Financial_Snapshot_Completed	7/28/2025 7:26 AM	Microsoft Edge P...	672 KB
	[REDACTED] Estate_Distribution_Letter...	7/28/2025 11:10 AM	Firefox HTML Doc...	23 KB
	[REDACTED] Inheritance_Summary	7/28/2025 9:14 AM	Microsoft Edge P...	76 KB
	[REDACTED] Monthly_Income_Project...	7/28/2025 9:17 AM	Office Open XML ...	27 KB

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

Image pingback in HTML:

```

```

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:

7/30/2025 4:25 PM	Application exten...	513 KB
7/30/2025 4:25 PM	Application exten...	558 KB
7/30/2025 4:25 PM	Application exten...	227 KB
7/30/2025 4:25 PM	Application exten...	38 KB
7/30/2025 4:25 PM	Application	26,165 KB
7/30/2025 4:25 PM	Fabricated financial documents	23 KB

Inheritance Summary

Name: [REDACTED]

Date: July 28, 2025

Summary of Inherited Assets from Estate of [REDACTED]

Decoy Page Accessed:

```
[REDACTED] - X-Forwarded-For: [REDACTED]  
[30/Jul/2025:22:13:02 +0000] "GET /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"
```

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"
```

Implant details

Hostname	[REDACTED]	Process	12348 [REDACTED] combined_files.exe	First seen	7/30/2025 10:13:05 PM
Username	[REDACTED]	OS	Windows 11.0 (OS Build 22631)	Last seen	7/31/2025 4:49:51 PM (59d)
UID / recipe / version	/ 3euje / 2.17.3	Note	[REDACTED]	Kill date	9/19/2025 11:11:19 AM
Parent implant	No parent	Communication type	HTTP	Checkins	288



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.

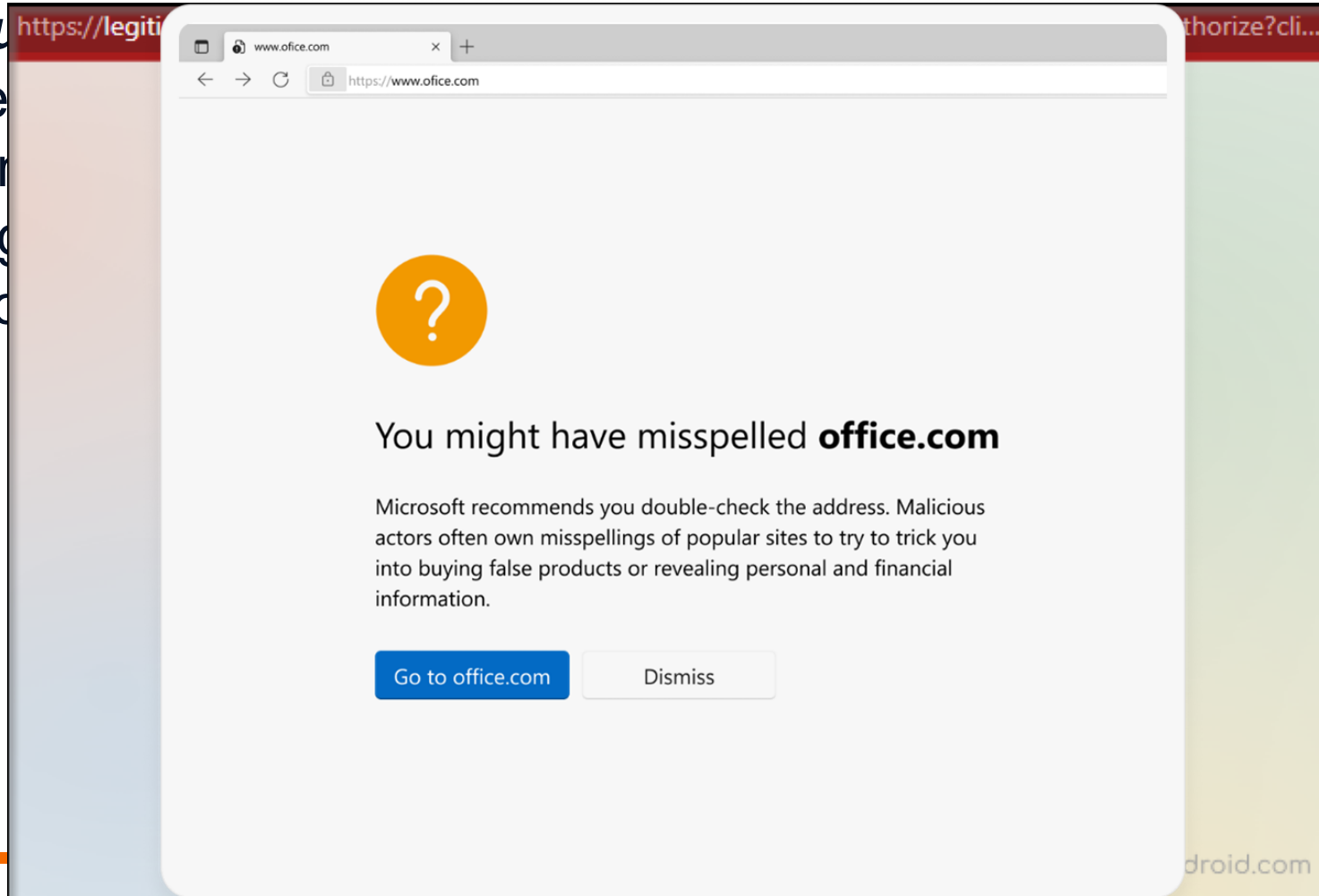
So we used typosquatted domains, but not the way you've seen before.



Weaponize Trust... And Typos

Typosqu

- We've
- Sendin
- Setting
- Monitor



com
ity filters
y Mark
registrar



Weaponize Trust... And Typos

ap.www.namecheap.com/domains/domaincontrolpanel/[REDACTED].com/domain

Dashboard

Expiring / Expired 5

Domain List

Hosting List

Private Email

SSL Certificates

Apps

My Offers Feb

Profile

PremiumDNS ? Enable PremiumDNS protection in order to switch your domain to our PremiumDNS platform. With our PremiumDNS platform, you get 100% DNS uptime and DDoS protection at the DNS level. **BUY NOW**

NAMESERVERS ? Namecheap BasicDNS

REDIRECT DOMAIN ?

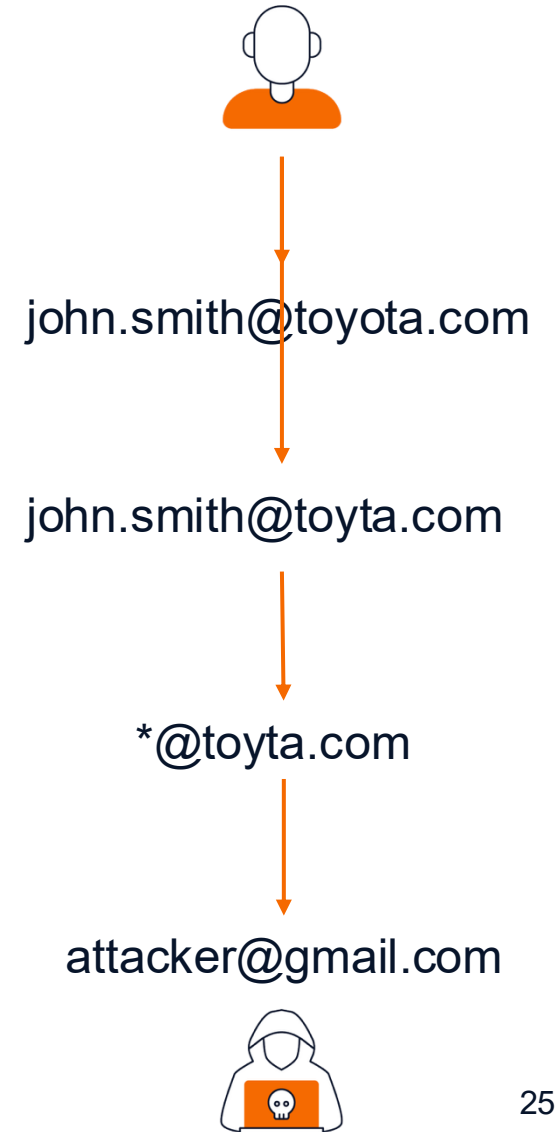
Source URL	Destination URL
[REDACTED].com	→ http://www.[REDACTED].com/

ADD REDIRECT **ADD WILDCARD REDIRECT**

REDIRECT EMAIL ?

Alias	Forward to
Catch-All	→ [REDACTED]@gmail.com

ADD FORWARDER **ADD CATCH-ALL**





Weaponize Trust... And Typos

Attacker Inbox:

From ▾ Any time ▾ Has attachment To ▾ Is unread [Advanced search](#)

1-50 of 87 < >

☐	☆	[Redacted]	DOCUMENTS AS NEEDED - [Redacted] Here are the two documents as req...	9/11/25
☐	☆	[Redacted]	Wife's Current Check - I have attached her current check stub for 09/12 ...	9/11/25
			PDF	
☐	☆	[Redacted]	Documents - Here you go [Redacted] Mobile: (360) 220-4741 [Redacted]	9/11/25
			PDF PDF PDF +2	
☐	☆	[Redacted]	Past Due Loans - New Zix secure email message from [Redacted] State Ban...	9/11/25
☐	☆	[Redacted]	[Redacted] - Pay Documents - [Redacted] Please see the attached. Note: I wor...	9/11/25
			PDF PDF PDF	
☐	☆	[Redacted]	Bank account error - Sent from my iPhone	9/10/25
			image0.png	
☐	☆	[Redacted]	Requirements{Secure Message} - [Redacted] Sending over what I have, let me...	9/10/25
			image0... PDF PDF +2	
☐	☆	[Redacted]	Fwd: [Redacted] Pay off - ----- Forwarded message ----- From: Re...	9/10/25
			PDF Pay off .pdf	

Intercepted Email:

Outgoing Wire - [Redacted] Funding 08 Trust BHG x

funds.management@[Redacted] to [Redacted] Fri, Sep 5, 9:30 AM ☆ ☺

This is a secure message from [Redacted]. It may take up to 3 minutes for this encrypted message to be available.

[Click here](#) by 2026-09-05 09:30 CDT to read your message. After that, open the attachment.

[More Info](#)

Disclaimer: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have received this email in error or simply delete it.

Secured by Proofpoint Encryption, Copyright © 2009-2025 Proofpoint, Inc. All rights reserved.

One attachment • Scanned by Gmail ⓘ

SecureMessageA...

from: funds.management@[Redacted]

to: [Redacted]

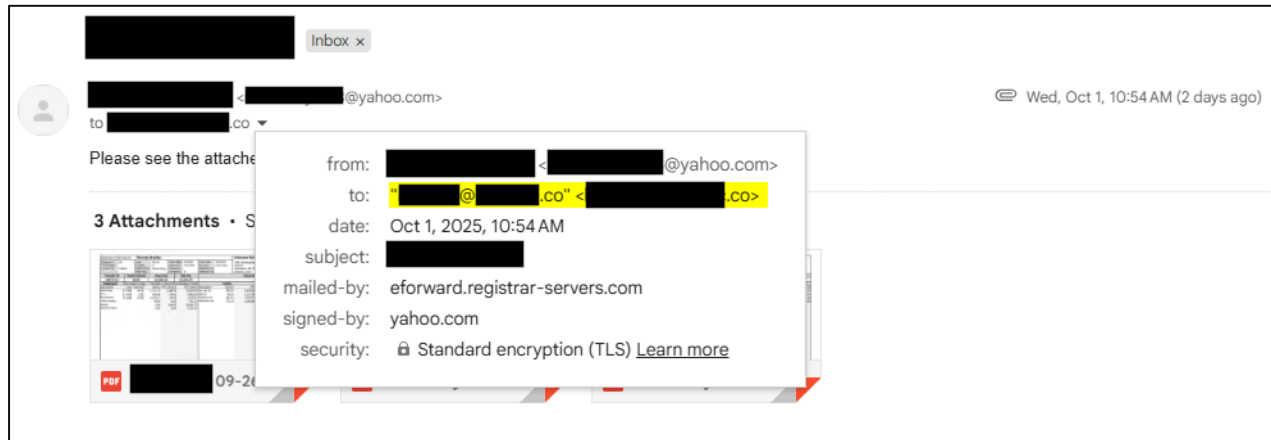
date: Sep 5, 2025, 9:30 AM

subject: Outgoing Wire - [Redacted] Funding 08 Trust

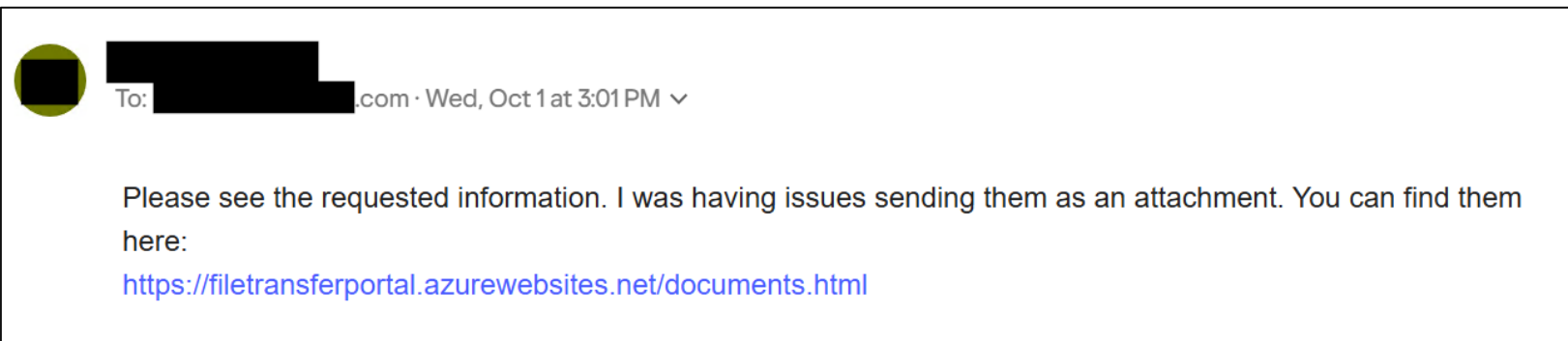
mailed-by: [Redacted]



Weaponize Trust... And Typos



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



john.smith@toyota.com



john.smith@toyota.co



*@toyota.co

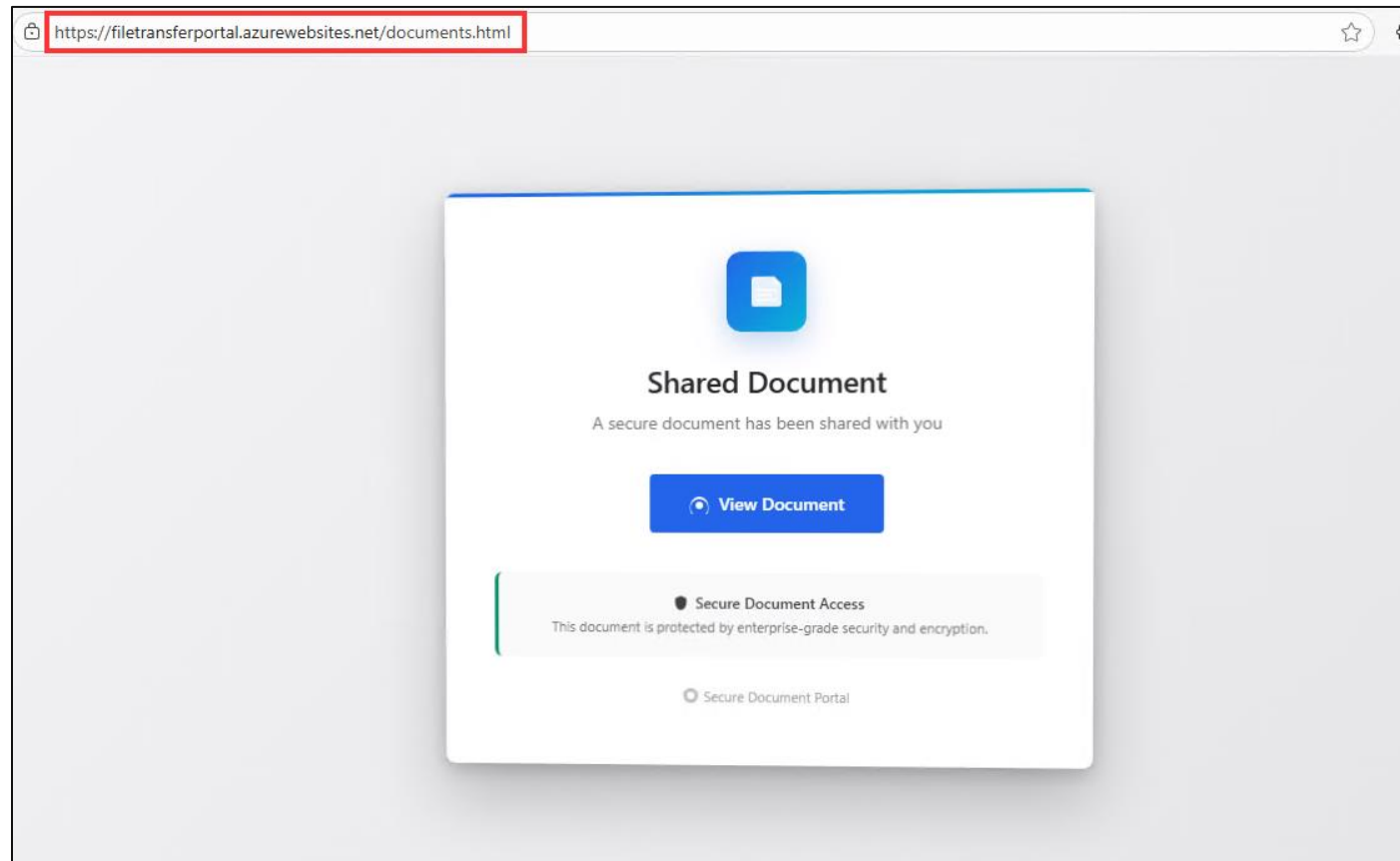


attacker@gmail.com





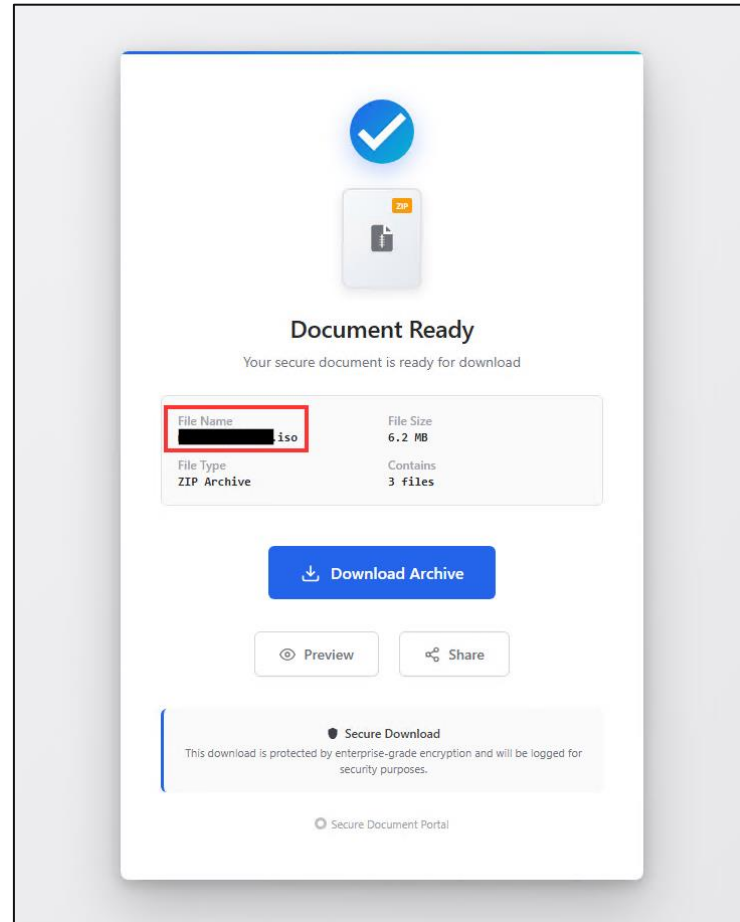
Weaponize Trust... And Typos



```
[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)"
```

Implant details					
Hostname	[REDACTED]	Process	[REDACTED] x64	First seen	10/2/2025 12:50:26 PM
Username	[REDACTED]	OS	Windows 11.0 (OS Build 26100)	Last seen	10/2/2025 1:22:40 PM (29h)
UID / recipe / version	/ S83tR / 2.18.0	Note	Unknown Recipe 2025-10-02T12:50:26.295630	Kill date	11/30/2025 2:09:36 PM
	SCOLPB4W			Checkins	24
Parent implant	No parent	Communication type	HTTP		



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

MARKETPLACE
Search For & Place Classifieds

SUBSCRIBE NOW
Save 50% on 1 Year

NewsSportsSFBJOpinionAdvertiseObituarieseNewspaperLegals

54°F☁️SubscribeSign In

Visit Help Center

Newsroom Leadership



News Director

✉️

News Reporters



Trending News Reporter

✉️



Reporter

✉️ ✕



State Politics & Government Reporter

✉️ ✕

Commercial Real Estate

Lumber Exchange in

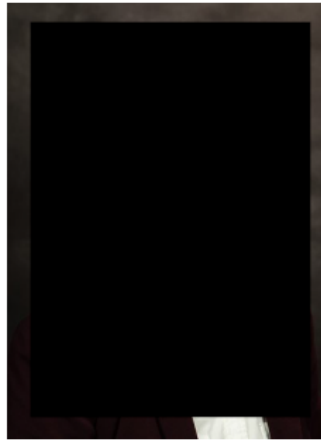
not be a good thing

42



Weaponize Whales

Target: Marketing Manager



Marketing Manager

Hailing from the sweeping skies and rolling prairies of ██████████, ██████████ is no stranger to the world of marketing, event planning and creative leadership. Dipping her toes has never been ██████████'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, ██████████ manages the marketing team at ██████████ 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.

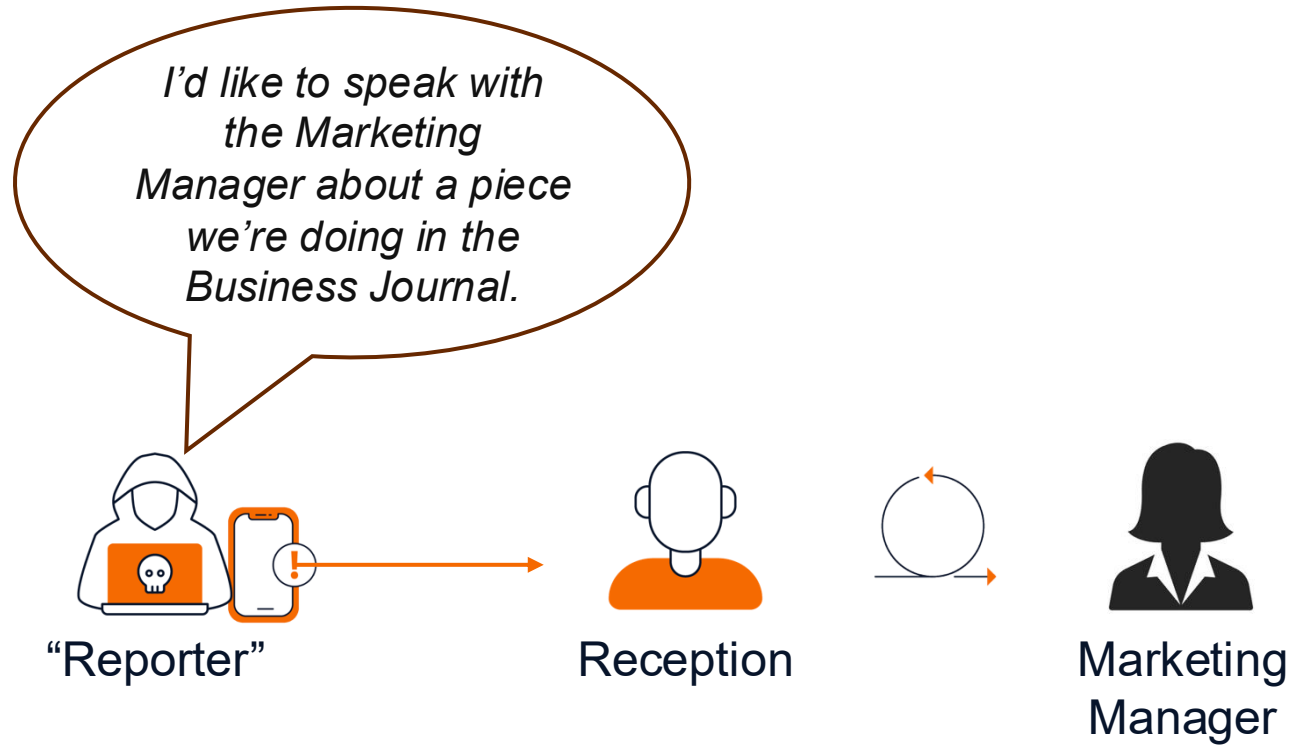
With a strong background in graphic design, photography and event planning, ██████████ oversees major external campaigns and coordinates ██████████'s large-scale events, including the ██████████ esports series, two annual golf tournaments and the ██████████ Sales Seminar. She also speaks at public events,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

Outside the office, ██████████ loves rock climbing, cycling fast around the ██████████ 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

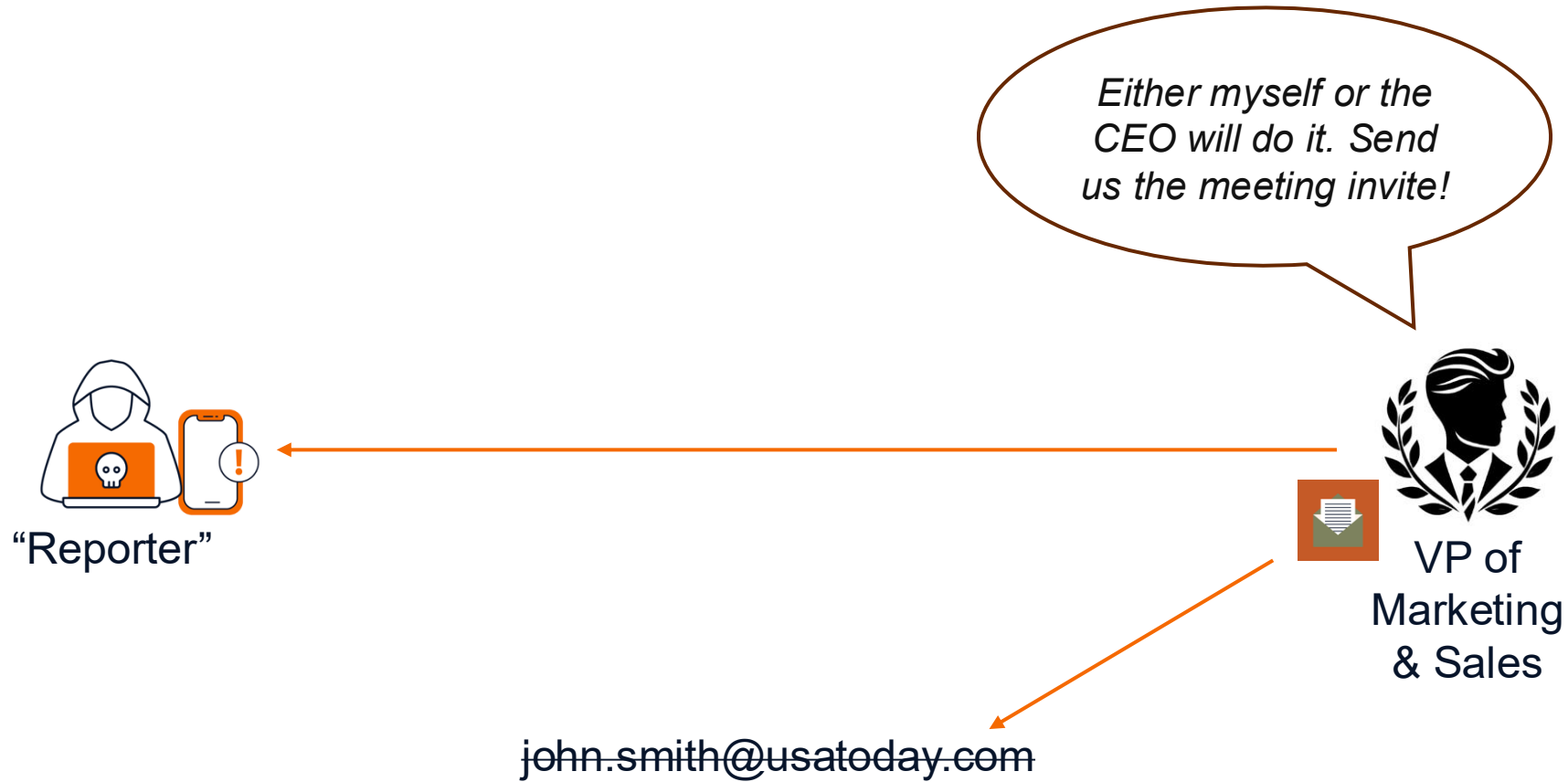


Weaponize Whales



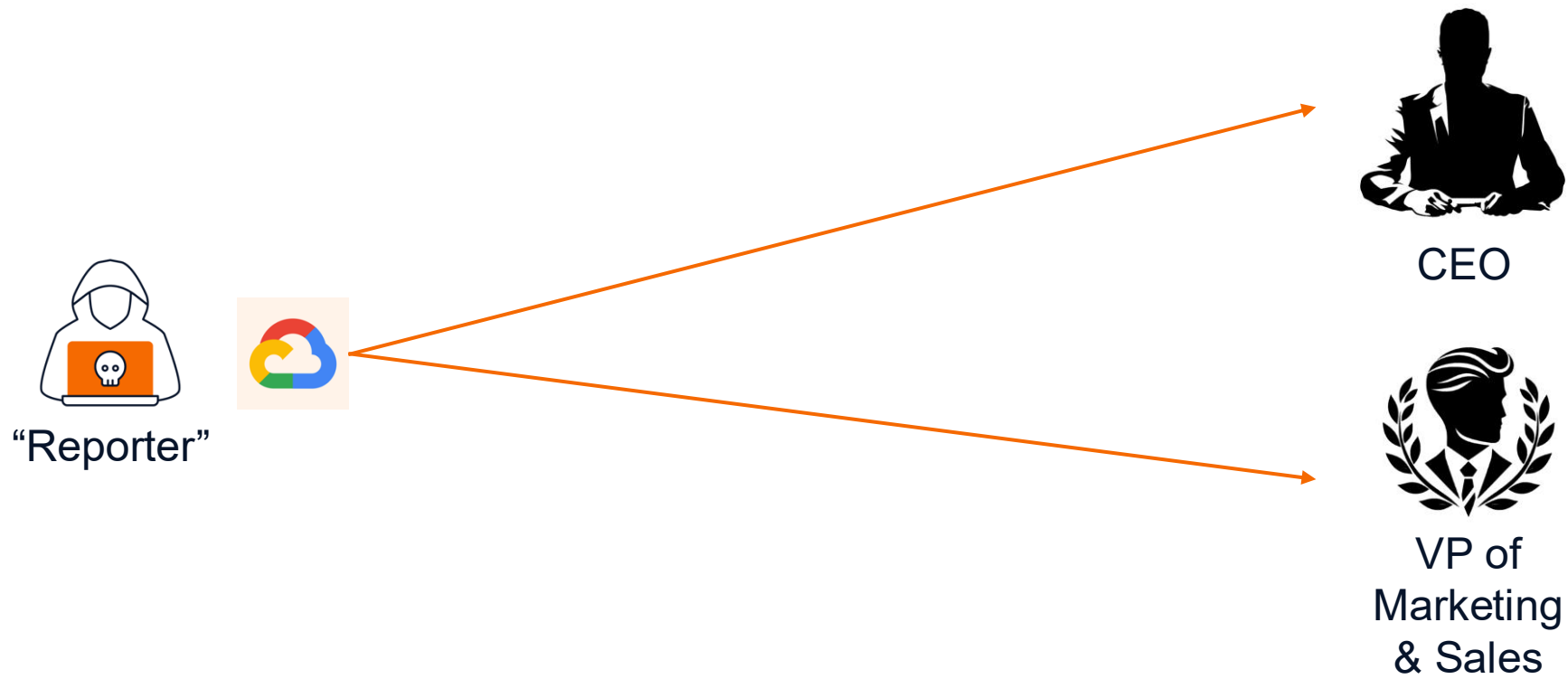


Weaponize Whales





Weaponize Whales

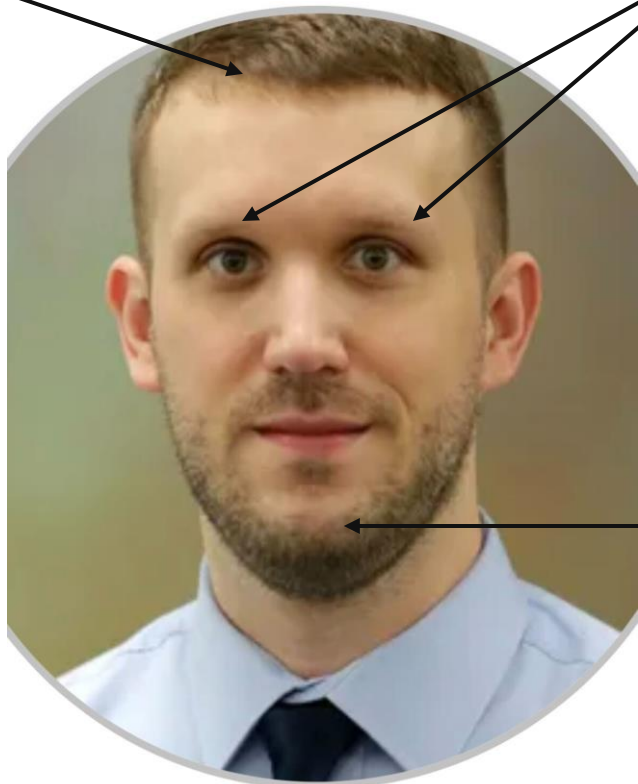




Weaponize Whales

Short hair

No eyebrows



Scruff



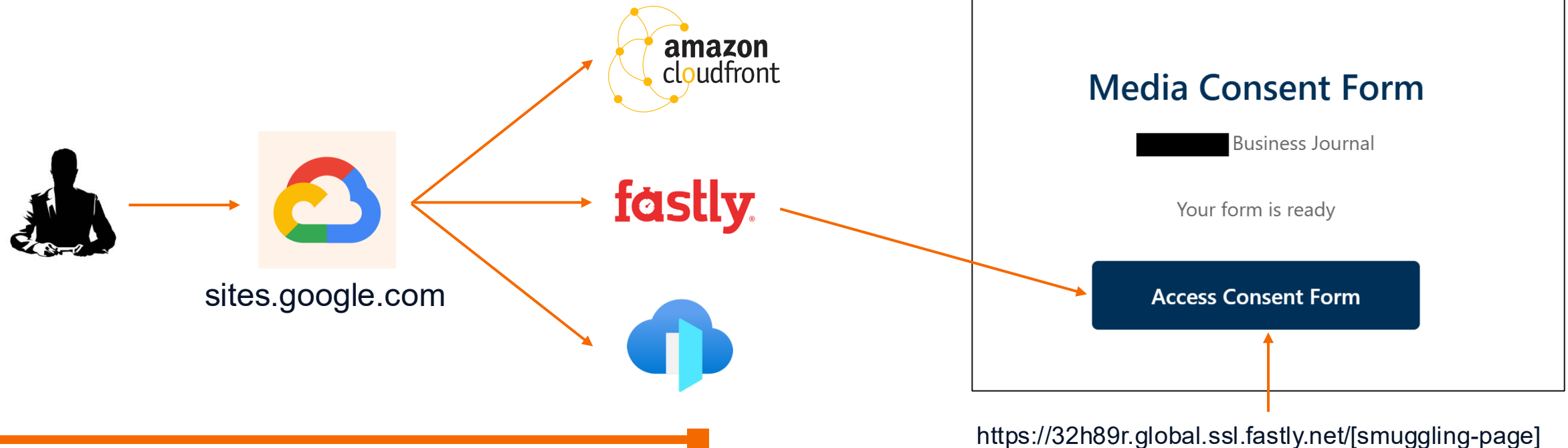


Weaponize Whales

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

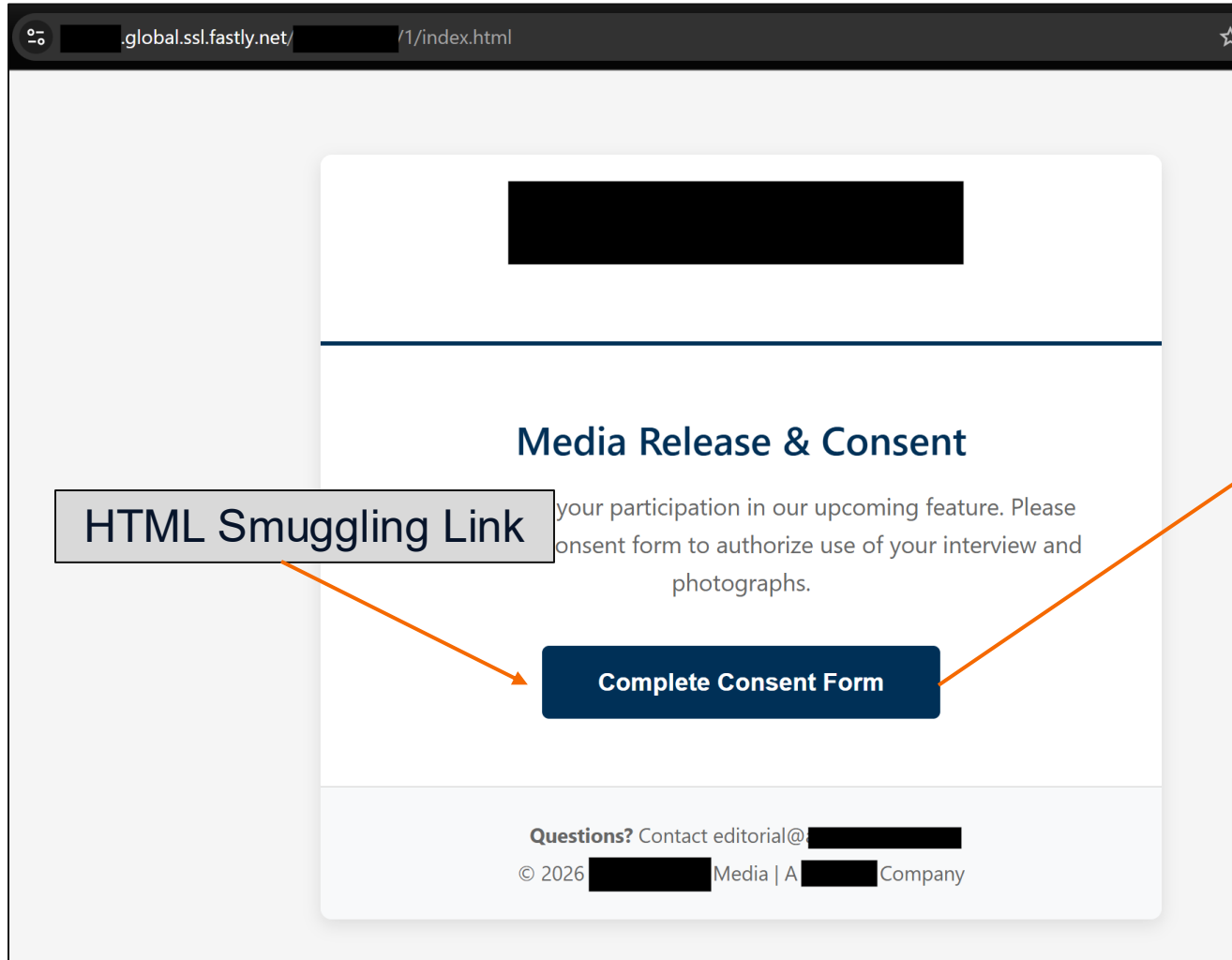
Problem:

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





Weaponize Whales



ZIP Archive

ISO Container

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



Weaponize Whales





Weaponize Whales

Risk Exposed:

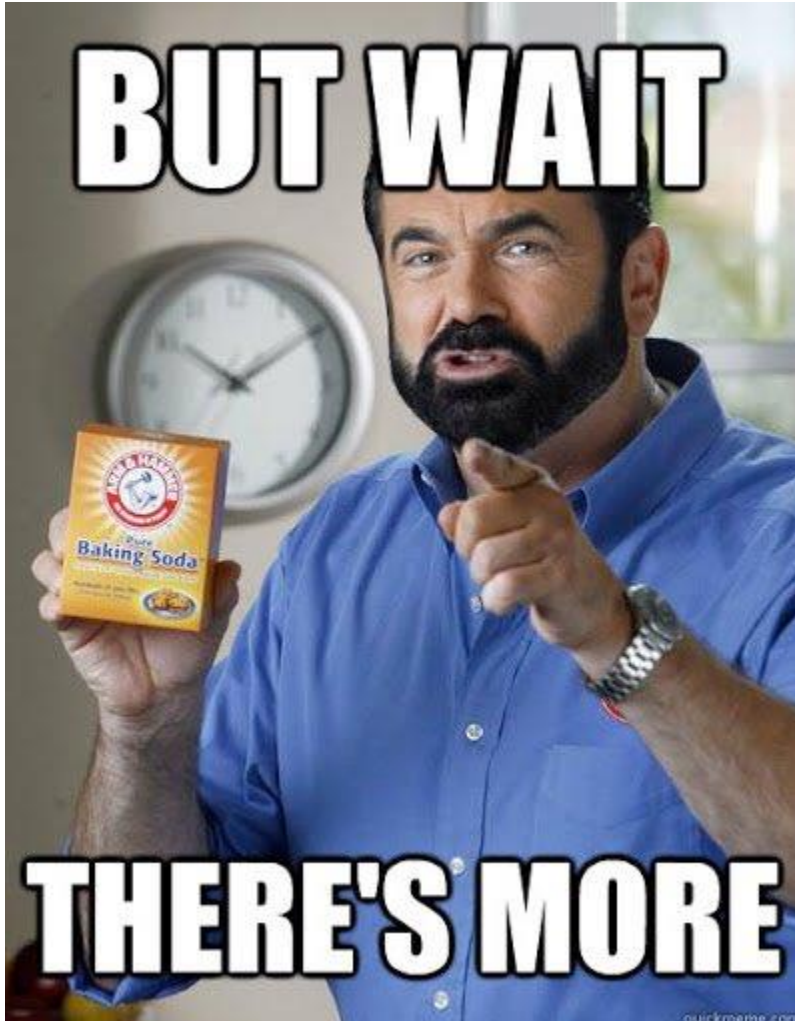
- Reputational damage
- Access to executive data
- Internal SE from this position could prove lucrative

Value to the Client:

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



Weaponize Whales



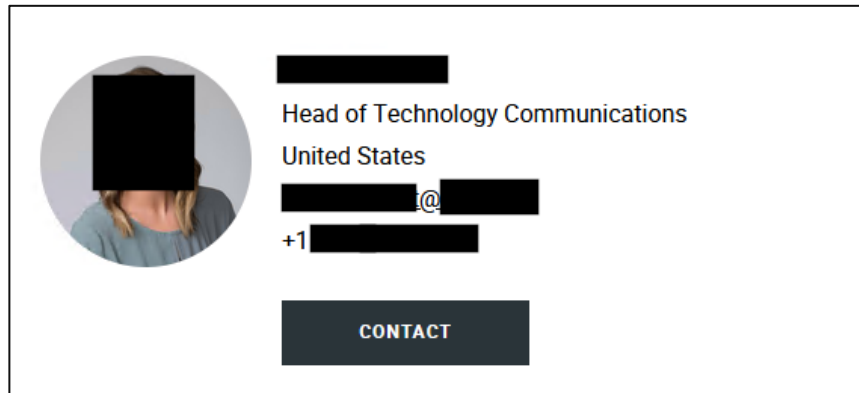
Scenario:

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

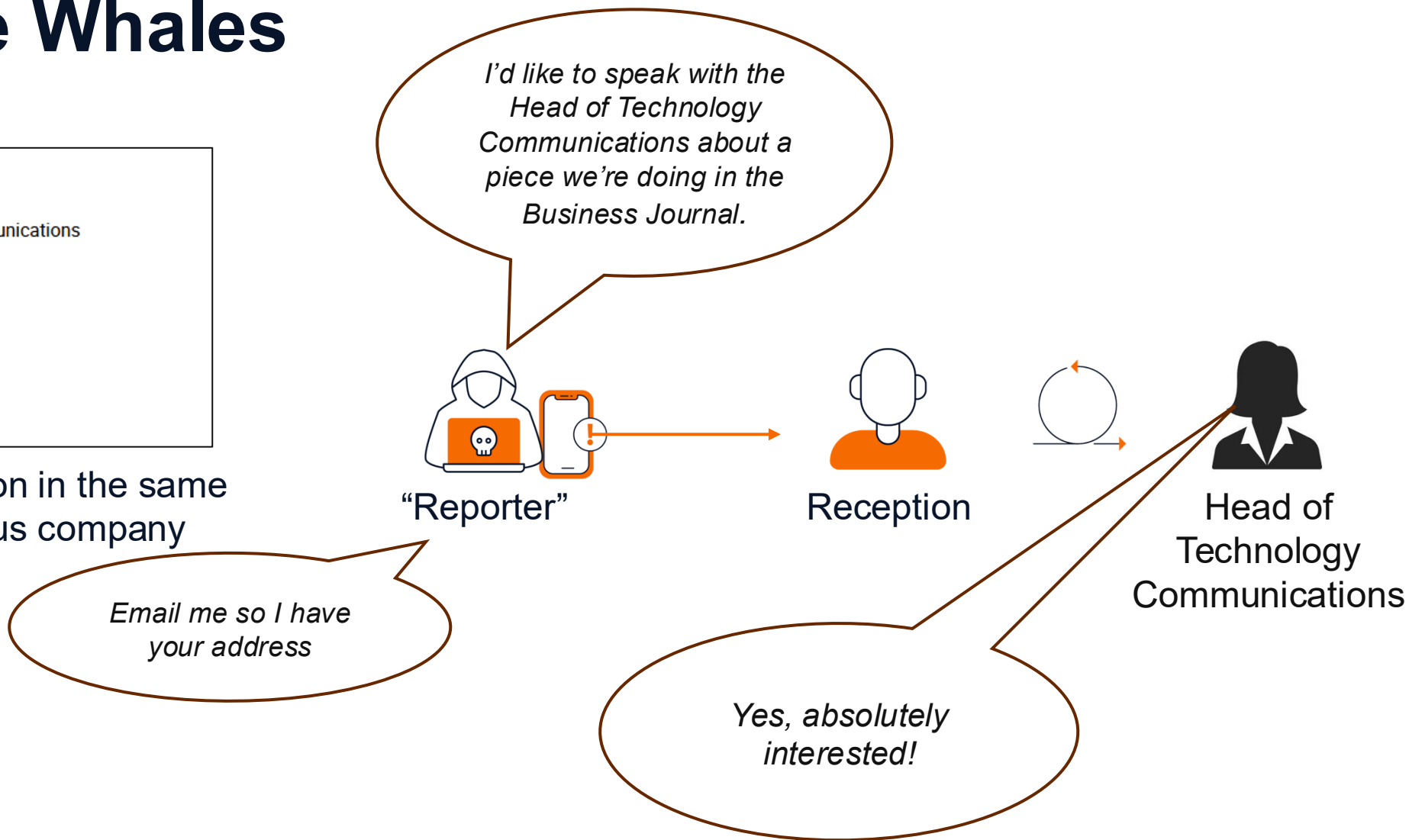
Technical and human hurdles had to be overcome to obtain initial access.



Weaponize Whales



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





Weaponize Whales



██████████@██████████

to me ▾

Mon, Jul 6, 1:36 PM ☆ 😊 ↩ ⋮

General Business

Hi ██████████

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

Once you're able to share the time, please coordinate time for an interview.

Thank you,

██████████

Head of Technology Community

██████████

Ph. +1 ██████████

Mob. +1 ██████████

██████████



██████████

to me ▾

Jul 7, 2026, 7:12 AM (13 days ago) ☆ 😊 ↩ ⋮

General Business

Hi ██████████

Confirming I've received your email.

██████████, 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,

██████████



██████████@bizjournaltoday.com

██████████ ▾

Mon, Jul 6, 1:54 PM ☆ 😊 ↩ ⋮

Thank you so much ██████████ 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.

██████████ versus when it can be fully autonomous,

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

██████████ of human vs. machine responsibilities, as

██████████ Leader here: <https://www.██████████.com/>

██████████

██████████ n*

Her:

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



Weaponize Whales

04:43

Chat People Raise React View More Camera Mic Share Leave

Meeting chat

Chris Mueller was invited to the meeting.

3:35 PM

<https://sites.google.com/bizjournaletoday.com/media-consent-form/home>

Type a message

(Unverified)



sites.google.com



Weaponize Whales - *Preserve the Pretext*

C

@bizjournaltoday.com

to [redacted]

Good morning,

It was great chatting with you guys yesterday. I look forward to [redacted] showed a strong interest in forging such a relationship.

1) Here's the media consent form: <https://d3d904icpgj8z0.cloudfront.net/...>

2) I was so caught up in the conversation about the mindset change you could share an information page of some type that I was using?

Thank you again! I look forward to writing about your operations.

—

Best Regards,

[redacted]

Connect Editor | USA Today
Milwaukee Journal Sentinel & Argus Leader
[redacted] @bizjournaltoday.com
951.554.4199

Tue, Jul 14, 7:07 AM (6 days ago)

☆ 😊 ↩ ⋮

R

to me, [redacted]

General Business

[redacted], and we look forward to the partnership.

[redacted] and I will be traveling for work so I would like to get this signed and back over to you.

[redacted] technology focus and solutions.

[redacted] d to Drive

[redacted] as a PDF, bro.”

Tue, Jul 14, 8:31 AM (6 days ago)

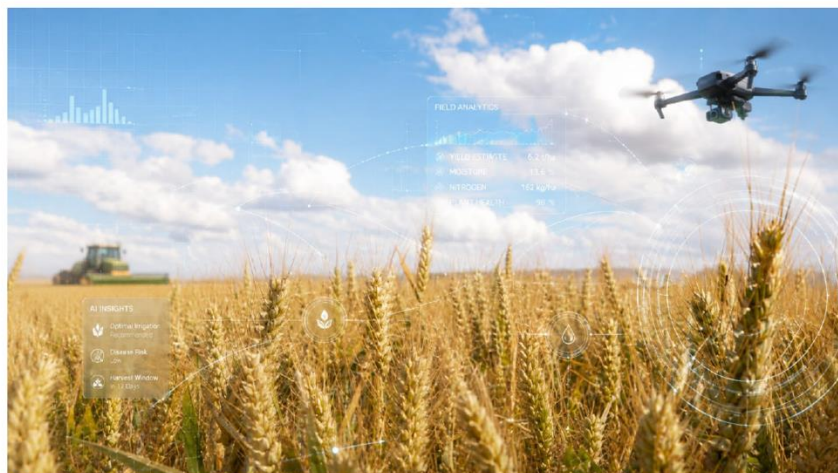
☆ 😊 ↩ ⋮



Switched to our Cloudfront



Weaponize Whales – Switch Gears



The Next Frontier for the First Frontier

How artificial intelligence is changing agriculture without replacing the farmer

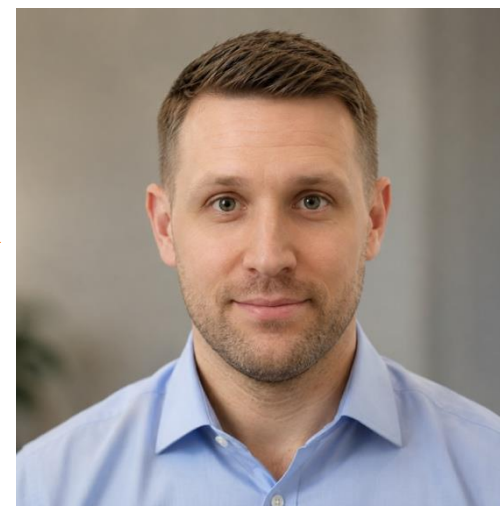


Agriculture has always been an industry of judgment.

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.

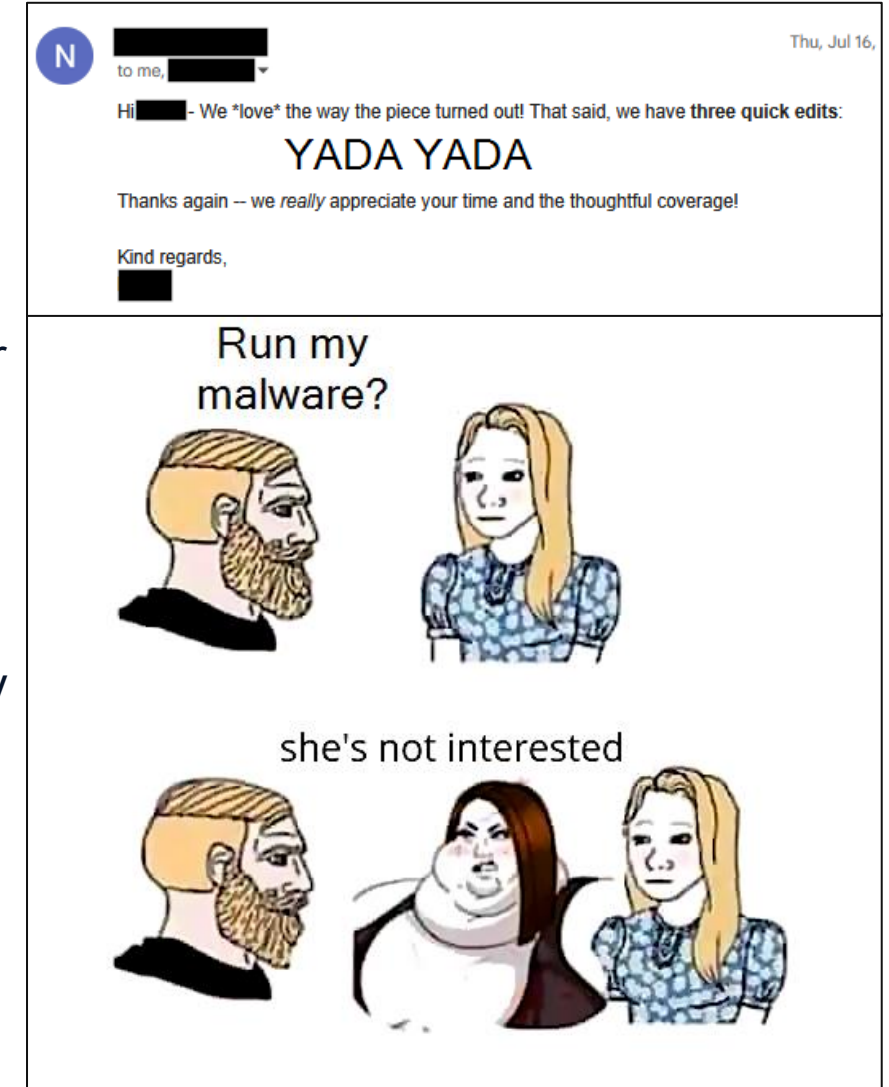
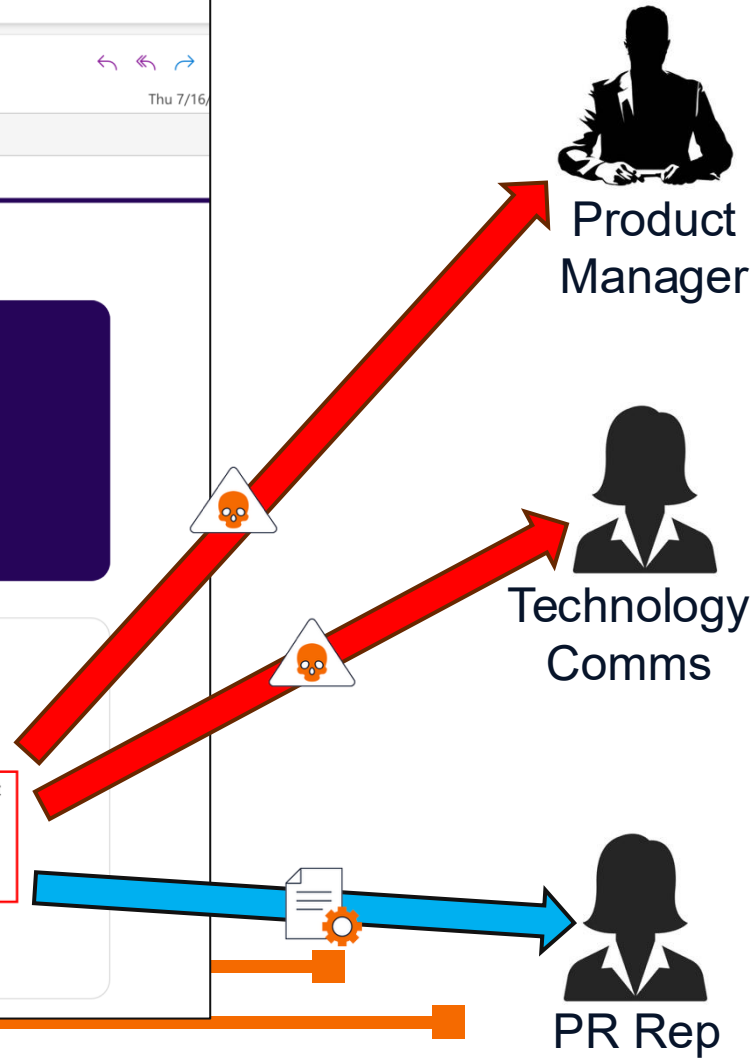
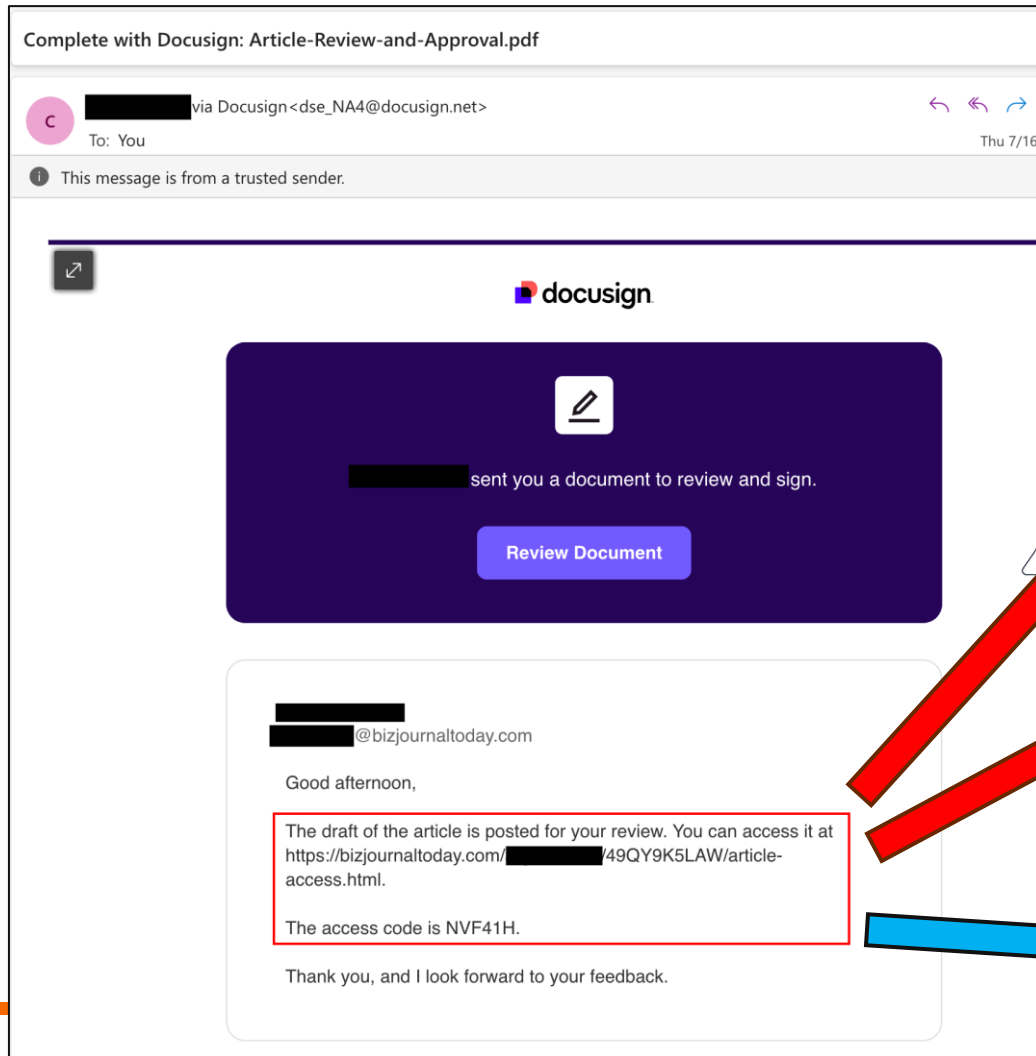
Now, one of the world's oldest industries is being reshaped by one of the world's newest.

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





Weapon

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 and to clarify anything.

Best,
[REDACTED]



[REDACTED] @bizjournal

to [REDACTED]

Hi [REDACTED],

I incorporated your edits and sent [REDACTED]
their signatures before I can submit to

—
Best Regards,
[REDACTED]

Connect Editor | USA Today
Milwaukee Journal Sentinel & Argus
[REDACTED] @bizjournaltoday.com
951.554.4199



httpd-cf



C21239B

HJCNH1NCYAQ3VJD @ 24084

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]

x5uH_dhGRI5SghvXW15hZ1j1K1e1d1p1h0Z1C111-1r1ck1g0r1c111/1.1 200 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?