Tales From the Blue Team

Lessons Learned From Taking Red Teams Too Seriously

Sam Heney

Jane Street

Overview

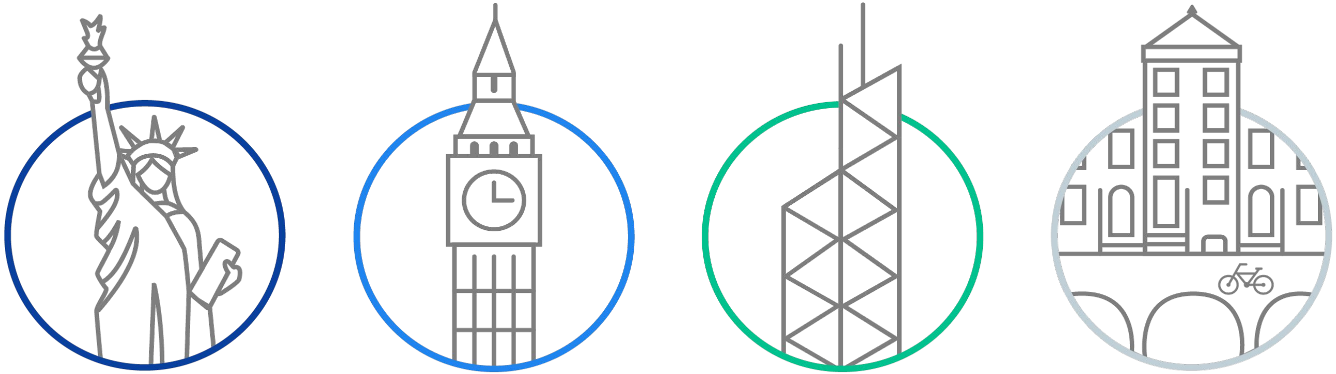
- Background & Context
- Red Team Engagement #1
- Red Team Engagement #2
- Red Team Engagement #3
- Takeaways / Lessons learned

About Me

- Cybersecurity Analyst at Jane Street
- Graduated from Abertay in 2021
- Ex-secretary of Abertay Hackers (2019-20)
- Fan of Linux, CLI, Devops and defensive security!

About Jane Street

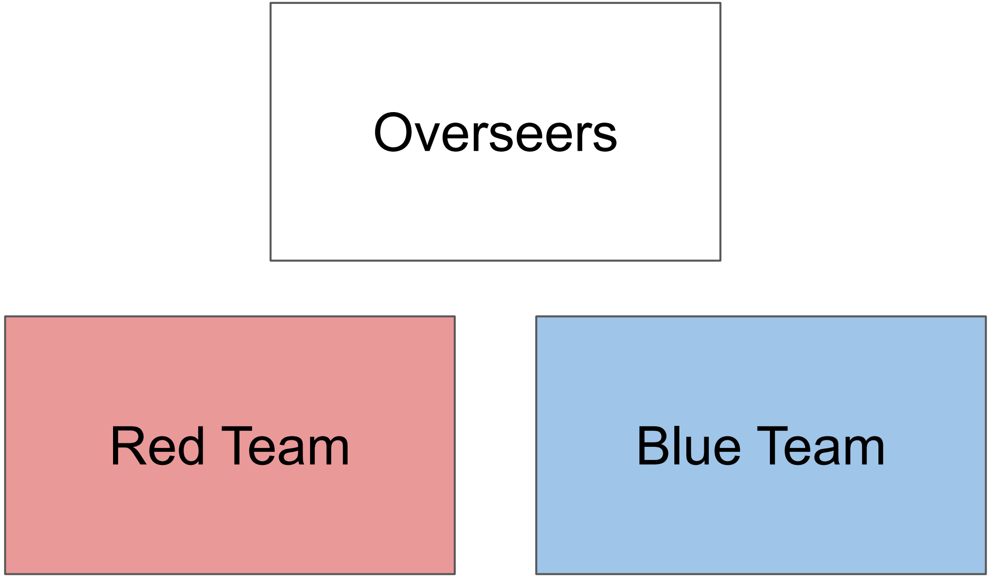
- Global trading / liquidity firm
- ~2000 Employees
- A growing Cybersecurity team
- Not much external facing infrastructure



What Is Red Teaming?

- Adversarial assessment of an organization’s security
- Explicitly goal oriented (exfiltrate x, gain access to y)
- Demonstrates multiple potential attack paths
- Only key stakeholders are aware
- Tests operational security effectiveness

Who are the Players?



Overseers

Red Team

Blue Team

Big Red Team Org

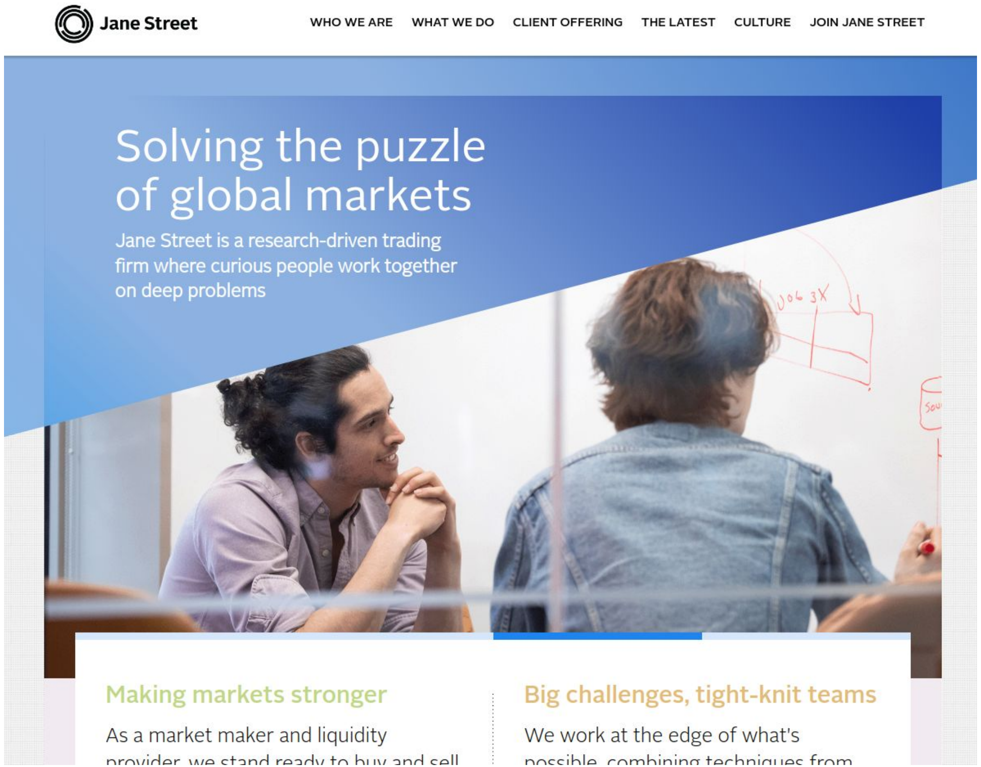
2018

Engagement Structure

- Black box test: they were given no information
- Had a two week window
- No physical testing
- Personal accounts and supply chain attacks out of scope

Footprinting / Initial Enumeration

- Scanned our IP ranges
- Didn't find much
- Decided to focus on phishing / social engineering



Jane Street

WHO WE ARE WHAT WE DO CLIENT OFFERING THE LATEST CULTURE JOIN JANE STREET

Solving the puzzle of global markets

Jane Street is a research-driven trading firm where curious people work together on deep problems

Making markets stronger

As a market maker and liquidity provider, we stand ready to buy and sell

Big challenges, tight-knit teams

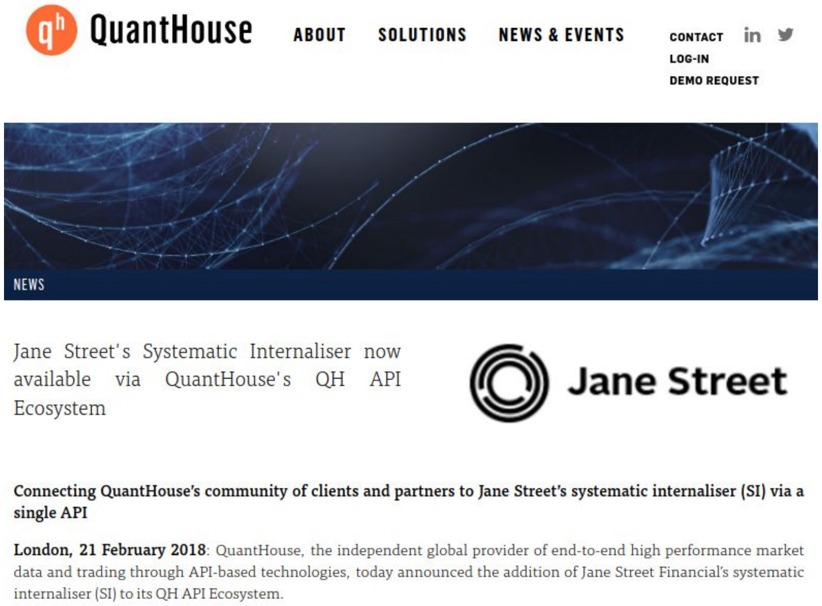
We work at the edge of what's possible, combining techniques from

Attack #1: Risky Resume

- Malicious CV sent to recruiting
- Got a callback from our third party recruitment org...
- Nice find, but out of scope

Attack #2: OSINT Spearphishing

- Found a client using media coverage
- Sent a very targeted email
- User knew the impersonated contact
- They identified it as phishing



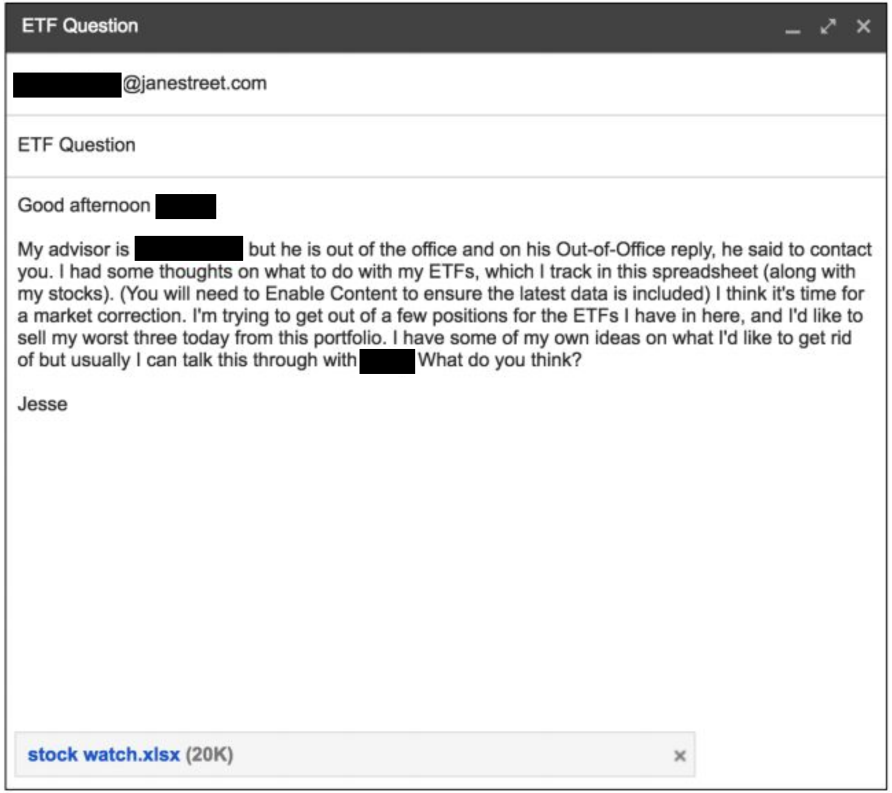
Jane Street's Systematic Internaliser now available via QuantHouse's QH API Ecosystem

Connecting QuantHouse's community of clients and partners to Jane Street's systematic internaliser (SI) via a single API

London, 21 February 2018: QuantHouse, the independent global provider of end-to-end high performance market data and trading through API-based technologies, today announced the addition of Jane Street Financial's systematic internaliser (SI) to its QH API Ecosystem.

Attack #3: Bad Spearphishing

- Very targeted attack (one recipient)
- Context was all wrong!
- Malicious excel file
- User identified it as malicious



ETF Question

[redacted]@janestreet.com

ETF Question

Good afternoon [redacted]

My advisor is [redacted] but he is out of the office and on his Out-of-Office reply, he said to contact you. I had some thoughts on what to do with my ETFs, which I track in this spreadsheet (along with my stocks). (You will need to Enable Content to ensure the latest data is included) I think it's time for a market correction. I'm trying to get out of a few positions for the ETFs I have in here, and I'd like to sell my worst three today from this portfolio. I have some of my own ideas on what I'd like to get rid of but usually I can talk this through with [redacted] What do you think?

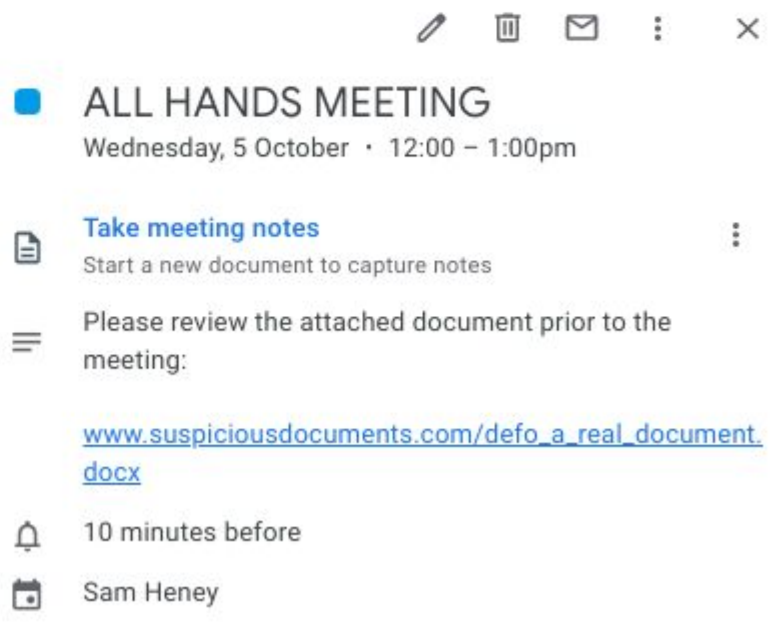
Jesse

stock watch.xlsx (20K)

Jane Street

Attack #4: Calendar Crisis

- Users were added to a meeting event
- Event was updated, sending notification
- Notification came from Google
- Several users clicked the link
- Payload was blocked by our proxy



ALL HANDS MEETING

Wednesday, 5 October · 12:00 – 1:00pm

Take meeting notes

Start a new document to capture notes

Please review the attached document prior to the meeting:

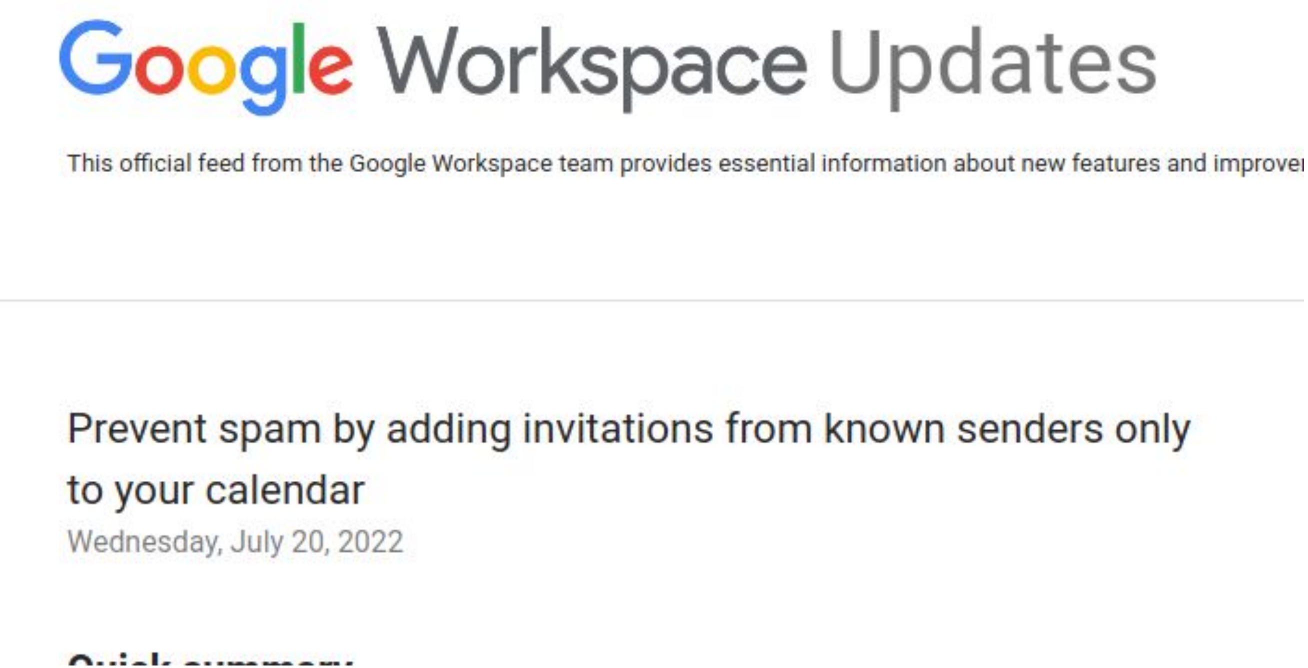
www.suspiciousdocuments.com/defo_a_real_document.docx

10 minutes before

Sam Heney

Attack #4: Calendar Crisis

- Also, we raised this with Google in 2018



Google Workspace Updates

This official feed from the Google Workspace team provides essential information about new features and improve

Prevent spam by adding invitations from known senders only to your calendar

Wednesday, July 20, 2022

Quick summary

Big Red Team Org

Good Stuff

- Used some novel techniques
- Solid OSINT work
- Almost popped a third party

Bad Stuff

- Failed to hack us 😔
- No test of our IR capabilities
- Expensive!

Small Red Team Firm

2020

Engagement Structure

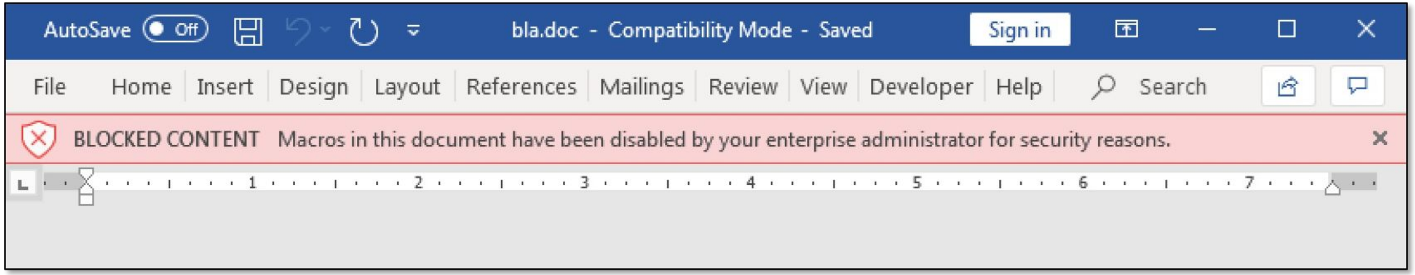
- Very similar to previous rules
- This time the attackers had six weeks rather than just two
- Cost the same! Big Red Team Org were really upselling
- New approach later on in the engagement

Footprinting / Initial Enumeration

- Wider attack surface now (WFH)
- Still didn’t find any promising services
- Found a lot of info about our tech stack and users!
- Again focused on CV upload portal and phishing

Attack #1: Confounding CV

- Blank CV submitted with malicious macros
- HR thought the web viewer was broken, downloaded and opened the doc
- Once opened, the macros didn't run (MOTW)

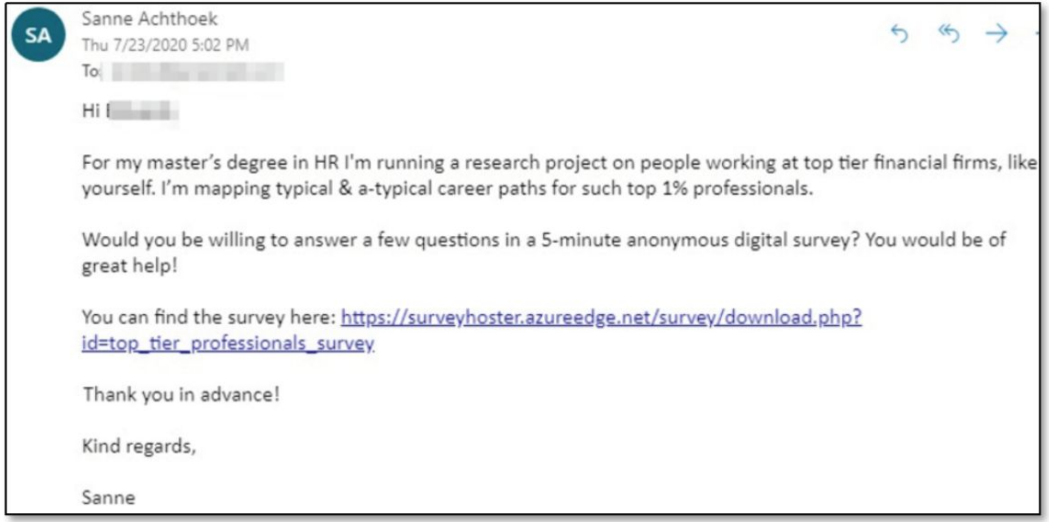


BLOCKED CONTENT Macros in this document have been disabled by your enterprise administrator for security reasons.

- HR got suspicious and called in Cyber
- We thoroughly investigated the file **taking note of any IOCs**

Attack #2: Spearphishing & Smuggling

- Various targeted phishing attempts
- HTML Smuggling link
- Payload would have worked
- No one clicked the link!



Sanne Achthoek
Thu 7/23/2020 5:02 PM
To [redacted]

Hi [redacted]

For my master's degree in HR I'm running a research project on people working at top tier financial firms, like yourself. I'm mapping typical & a-typical career paths for such top 1% professionals.

Would you be willing to answer a few questions in a 5-minute anonymous digital survey? You would be of great help!

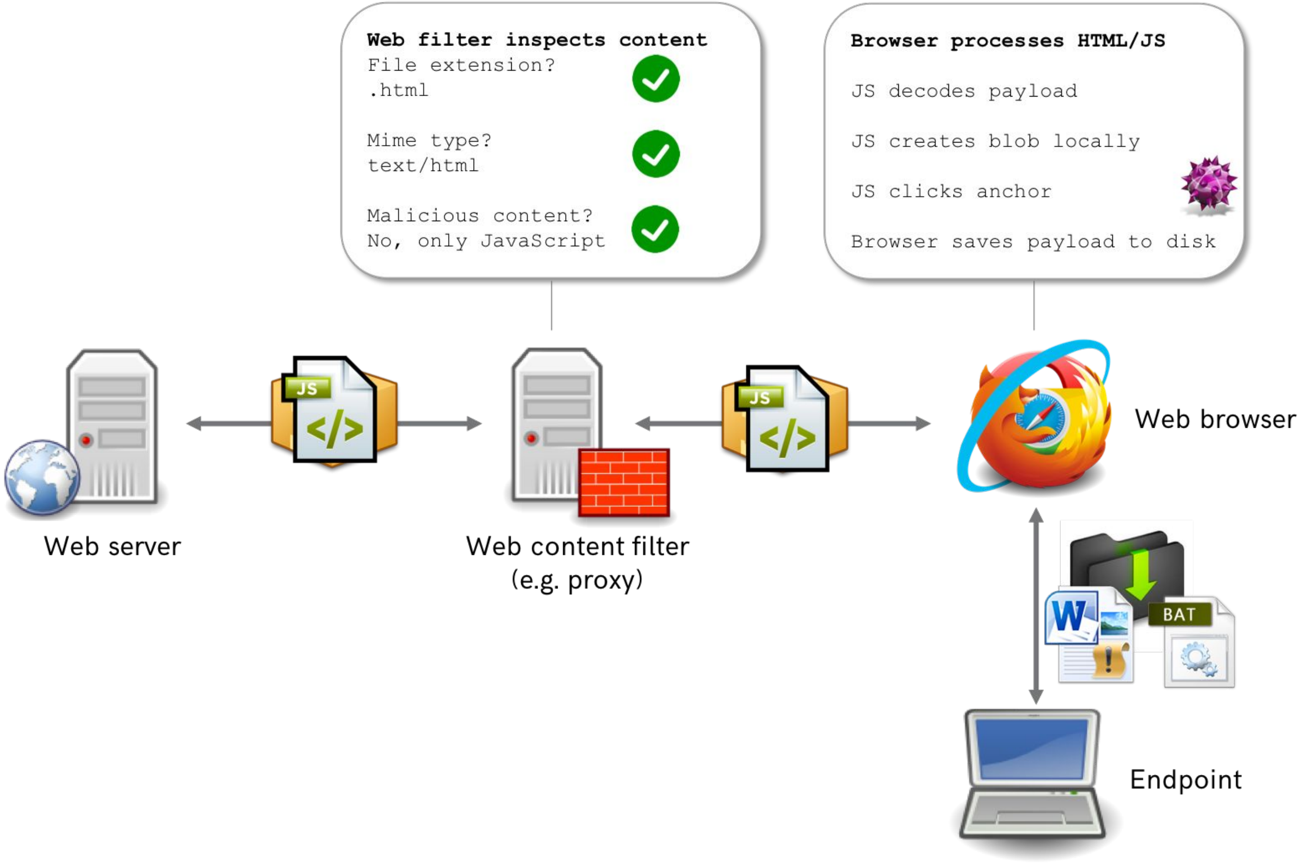
You can find the survey here: https://surveyhoster.azureedge.net/survey/download.php?id=top_tier_professionals_survey

Thank you in advance!

Kind regards,

Sanne

Sidenote: What is HTML smuggling?



Web filter inspects content

File extension?
.html ✓

Mime type?
text/html ✓

Malicious content?
No, only JavaScript ✓

Browser processes HTML/JS

JS decodes payload

JS creates blob locally

JS clicks anchor

Browser saves payload to disk

~~Attack~~ #3: A helping hand

- Sick of not being hacked, overseers let them in
- Employee opened a malicious office doc on behalf of the red team
- Finally, we’re “compromised”!

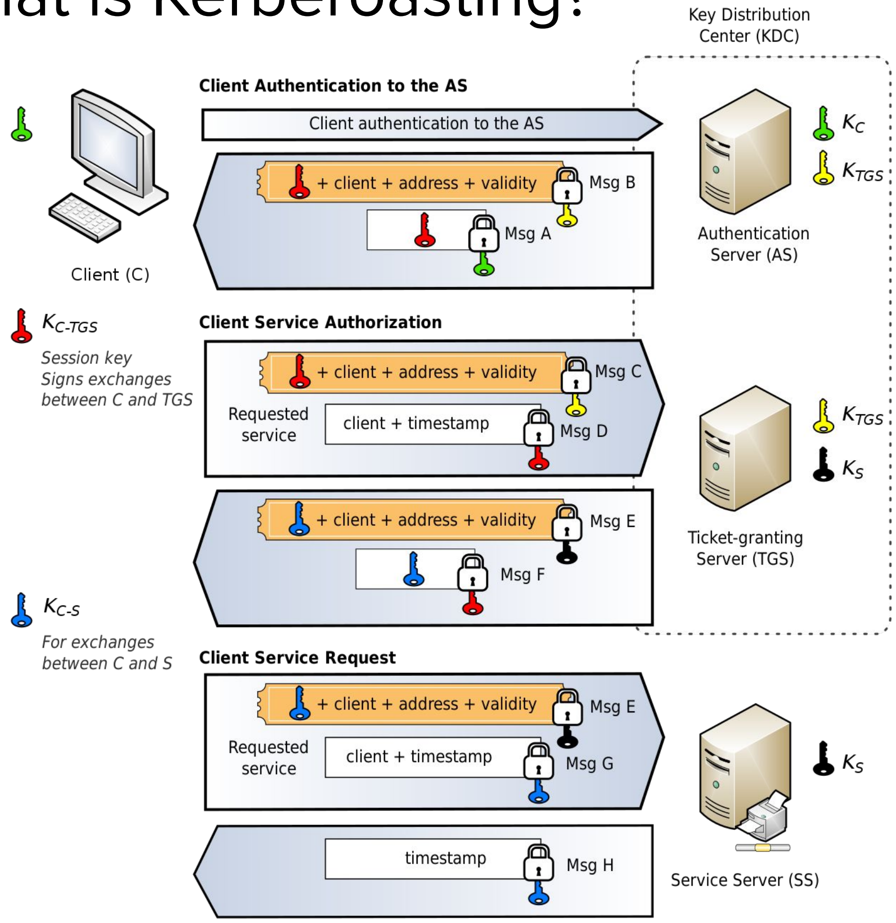
~~Attack~~ #3: A helping hand

- … for approximately 1 hour
- Blue team happened to be looking at the previous IOCs
- Saw a host reaching out to one of the domains
- Immediately cut off the box from the network

Attack #4: Kerberoasted!

- Red team still had about 1 hour on the network
- Managed to kerberoast several accounts
- Cracked two passwords!

Sidenote: What is Kerberoasting?


Key Distribution Center (KDC)
Client Authentication to the AS
Client authentication to the AS
+ client + address + validity
Msg B
Msg A
Client (C)
K_C
K_{TGS}
Authentication Server (AS)
$K_{C\text{-}TGS}$
Session key
Signs exchanges between C and TGS
Client Service Authorization
+ client + address + validity
Msg C
Requested service
client + timestamp
Msg D
K_{TGS}
K_S
+ client + address + validity
Msg E
Msg F
Ticket-granting Server (TGS)
$K_{C\text{-}S}$
For exchanges between C and S
Client Service Request
+ client + address + validity
Msg E
Requested service
client + timestamp
Msg G
K_S
timestamp
Msg H
Service Server (SS)

Attack #4: Kerberoasted!

- Blue team detected that kerberoasting happened
- Overseers couldn’t justify not forcing password resets
- The jig was up! Overseers revealed to blue team what was going on
- The red team were let back in, with the blue team keeping eyes on

Attack #5: Privesc

- Blue team was now ignoring red team alerts (there were a lot!)
- Lateral movement was achieved fairly quickly
- Using a writable $PATH via Bloomberg terminal, local admin was gained
- From there, they eventually found a route to domain admin 🎉

Small Red Team Firm

Good Stuff

- Used some novel techniques
- Validated quality of our password policy/cracking
- Achieved a lot once roaming free
- Validated the need for a SOC

Bad Stuff

- Failed to hack us 😔
- Reused infrastructure, got caught too soon

Big Red Team Org #2

Engagement Structure

- Again, similar to previous
- Lasted for 3 weeks

Footprinting / Initial Enumeration

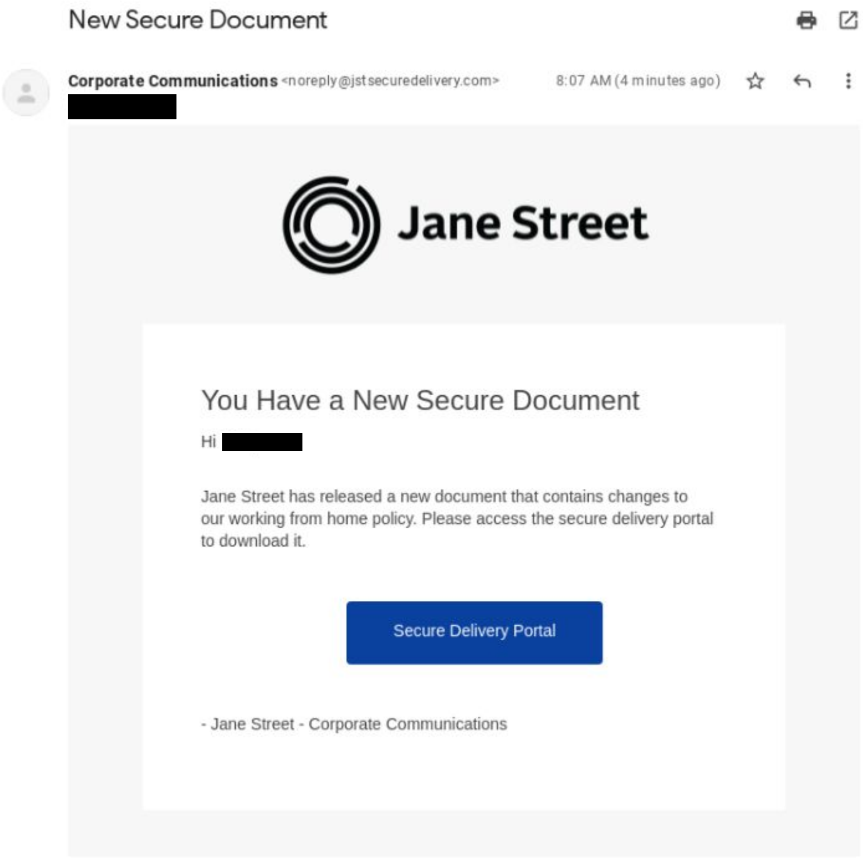
- They found something!
- Internet exposed silent video conferencing tool
- Used to simulate the feeling of sitting together, remotely
- Red team suggested this could be used for social engineering
- We weren’t convinced…

Footprinting / Initial Enumeration

- Nothing other than that
- Focussed on phishing from here

Attack #1: Going phishing

- Multiple waves of phishing emails
- Sent to 80, then 106
- Good template, not perfect
- Great domains



New Secure Document

Corporate Communications <noreply@jstsecuredelivery.com> 8:07 AM (4 minutes ago)

[redacted]

You Have a New Secure Document

Hi [redacted]

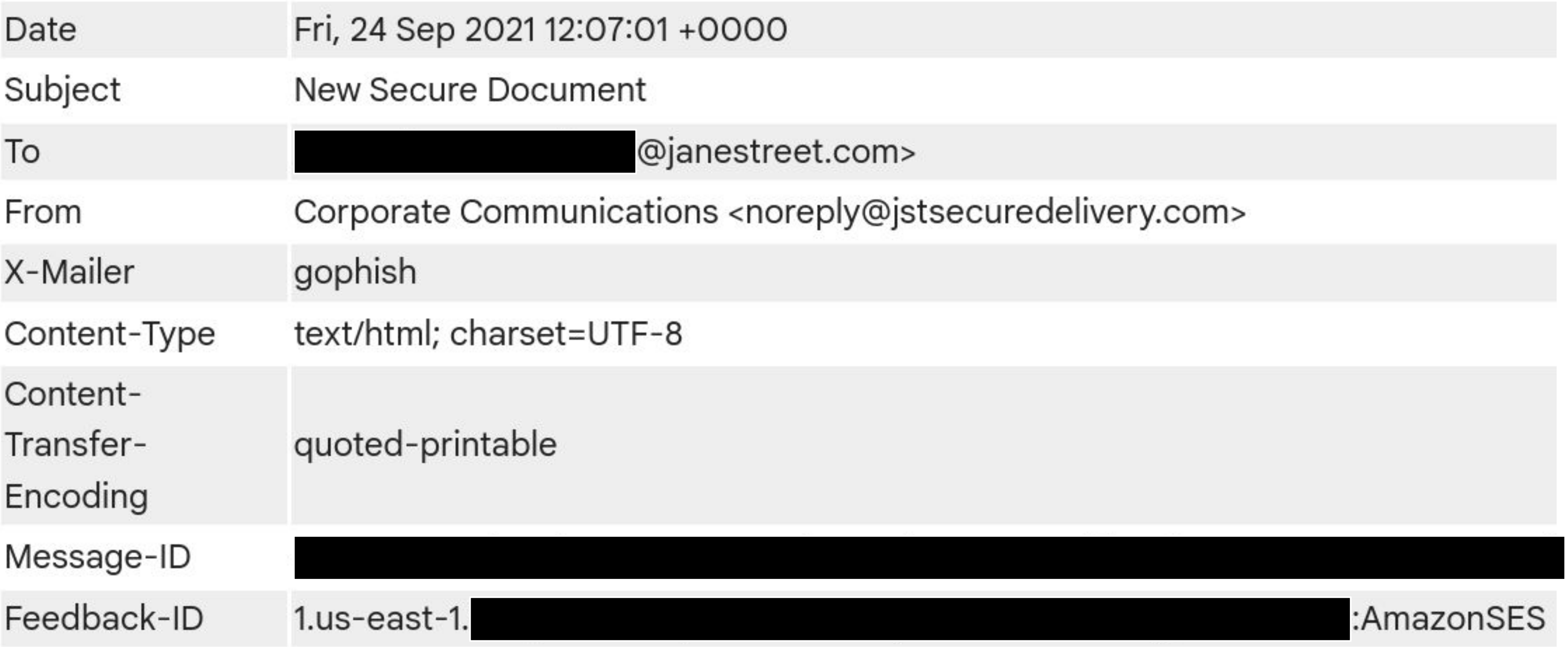
Jane Street has released a new document that contains changes to our working from home policy. Please access the secure delivery portal to download it.

- Jane Street - Corporate Communications

Attack #1: Going phishing

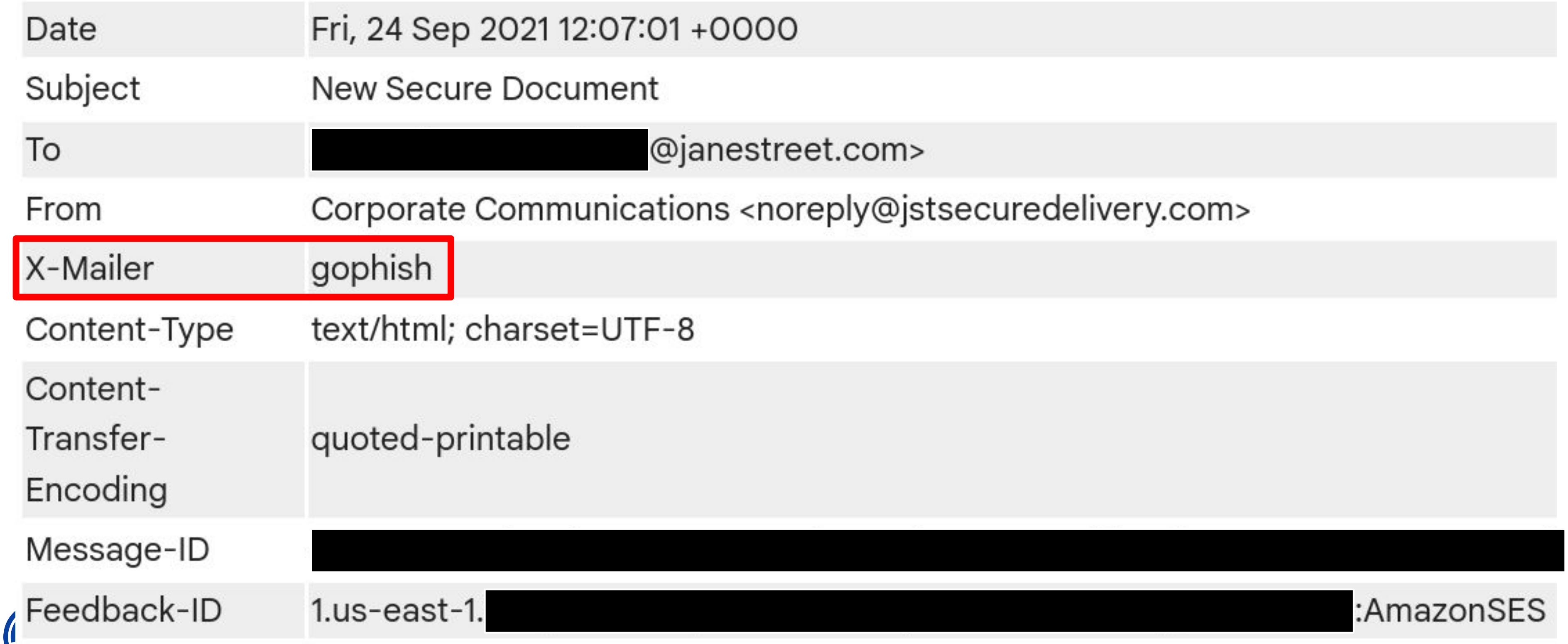
- Employees reported the emails with 10-15 mins
- We hunted the emails
- No luck for the red team

Attack #1: Going phishing



Date	Fri, 24 Sep 2021 12:07:01 +0000
Subject	New Secure Document
To	[redacted]@janestreet.com>
From	Corporate Communications <noreply@jstsecuredelivery.com>
X-Mailer	gophish
Content-Type	text/html; charset=UTF-8
Content-Transfer-Encoding	quoted-printable
Message-ID	[redacted]
Feedback-ID	1.us-east-1.[redacted]:AmazonSES

Attack #1: Going phishing

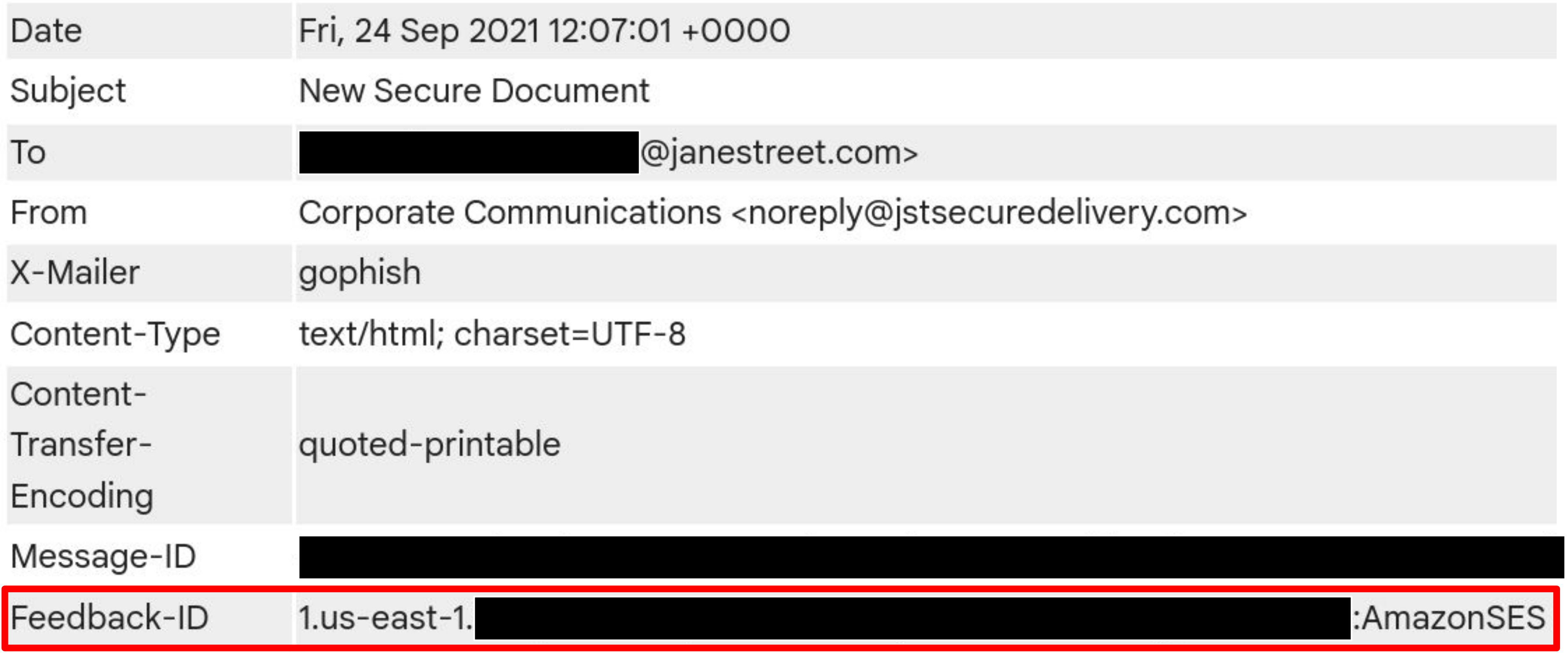


Date	Fri, 24 Sep 2021 12:07:01 +0000
Subject	New Secure Document
To	[redacted]@janestreet.com>
From	Corporate Communications <noreply@jstsecuredelivery.com>
X-Mailer	gophish
Content-Type	text/html; charset=UTF-8
Content-Transfer-Encoding	quoted-printable
Message-ID	[redacted]
Feedback-ID	1.us-east-1.[redacted]:AmazonSES

Attack #1: Going phishing

- Red team used GoPhish and left the X-Mailer header
- Blue team blocked it via our mail server
- They had no idea... 😬

Attack #1: Going phishing



Date	Fri, 24 Sep 2021 12:07:01 +0000
Subject	New Secure Document
To	[redacted]@janestreet.com>
From	Corporate Communications <noreply@jstsecuredelivery.com>
X-Mailer	gophish
Content-Type	text/html; charset=UTF-8
Content-Transfer-Encoding	quoted-printable
Message-ID	[redacted]
Feedback-ID	1.us-east-1.[redacted]:AmazonSES

Attack #1: Going phishing

- Feedback-ID was red team AWS account
- Once again, blue team blocked the header
- Once again, they had no idea

~~Attack~~ #2: We let them in again

- Similar to the previous year, the overseers gave them internal access
- Employee ran a malicious script for the red team
- The game was afoot!

~~Attack~~ #2: We let them in again

- Using `find`, red team found a SUID OCaml binary
- Tried to exfiltrate the binary to look closer
- Blue team caught the data exfil, promptly kicked them out
- At this point, the insiders told the blue team about the engagement

Sidenote: What is an SUID binary?

```
rwxrwxrwx sheney sheney find

rwsrwxrwx sheney sheney find
```

```
$ ./find . -exec /bin/sh -p \; -quit
```

(check out https://gtfobins.github.io/ for more!)

Big Red Team Org #2

Good Stuff

- Decent phishing templates
- Great domains

Bad Stuff

- Failed to hack us 😔
- Sloppy phishing mistakes
- Noisy data exfil

Lessons Learned

Choosing a Red Team is Hard

- Red team legality is tricky
- Good comms are necessary
- Breaking things is disruptive and costly!
- Coordinating attack timings is key
- Knowing what your tools do is important

Jane Street

Coordinating an Engagement is Difficult

- Difficult to know when to tell people
- Difficult to get people to take it seriously
- Difficult to get people to not try way harder than usual
- Important to be able to distinguish between red team and non red team 😬

The Objective is to Learn

- Prioritisation is very important
- Finding things we already know about isn't useful*
- Very difficult to capture everything we might learn
- Reports never include everything we'd like to remember
- Red teams don't often provide detections per attack

*unless to demonstrate that it is, in fact, vulnerable

User Awareness is Key

- A common theme is phishing campaigns failing
- We put a lot of resources into user awareness and training
- Users reporting potential phishing emails is extremely important
- Jane Streeters are a very competent bunch!

The SOC Can Learn a Lot!

- “Huh, that alert *is* useful”
- “That alert should have caught that”
- “We should have an alert for that”
- “I swear we had an alert for that”
- “*That* was the alert that fired?”

We’re Pretty Good 😎

- Perimeter hasn’t been breached by a red team yet
- Once let inside, blue team always caught them quickly
- Quick to implement monitoring for further red team activity
- Red teams are regularly surprised by our capabilities!

But We Need To Stay Humble!

- Several times, we’ve gotten lucky
- Attackers and attacks are always evolving
- Jane Street is continually expanding both headcount and attack surface
- We need strong, capable people, and more of them…

Come Work With Us!

Jane Street

Don’t just find problems, solve them too!

Work with skilled programmers and security experts!

CLI driven workflows!

Come chat with me if you’re interested