RED TEAM OOPS!

on Public

framework for enumerating, spraying,
AD accounts

SharpCollection Public

Nightly builds of common C# offensive tools, fr
master branches built and released in a CI
release pipelines.

☆ 2k 302

If you

- Why talk about Azure
- Story behind the discov
  - https://www.trustedsec.com/2019/04/next
- Cover:
  - What it is
  - Licensing
  - Features
  - Detection
  - Exploit

Windows PowerShell

```
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --spray --passwords C:\Clients\2021\FooBar\
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --exfil --cookie-dump C:\\CookieData.txt --all
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --exfil --aad
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --exfil --tokens C:\\OutputTokens.txt --onedrive --owa
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --exfil --teams --owa --owa-limit 5000
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --debug --exfil --onedrive
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --enum --validate-teams
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --enum --validate-msol --usernames C:\Clients\2021\FooBar\OSINT\Usernames.txt
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --backdoor
    --outpath C:\Clients\2023\FooBar\TFOutput --config myCustomConfig.json --database
    --outpath C:\Clients\2023\FooBar\TFOutput --config .\TeamFiltrationConfig.json --outpath MyCurrentClient --spray
PS C:\Users\User\Desktop> .\TeamFiltration.exe

[♥] TeamFiltration V3.5.2 PUBLIC, created by @Flangvik at @Trusted
[+] Args parsed --config .\TeamFiltrationConfig.json --outpath MyC
[SPRAY] 5/9/2023 5:31:24 PM EST Sleeping between 60-100 minutes for
[SPRAY] 5/9/2023 5:31:26 PM EST 14m since last spray, spraying will
```

Attacking O365 with TeamFiltra

Flangvik
1.78K subscribers

Oddvar Moe
OPEN, MCITP, MVP, MCP, MCSE, MCSA
Red Teamer @TrustedSec
Hacker / Blogger / S
Hobbier - Fiske, 3d
Bor og jobber i Aren
Prosjekter: Lolbas & Ulti

Phishing past Mail Protection Controls using Azure Information Protection (AIP)
Oddvar Moe, Hans Lakhan

User behavior

- Key element is to behave like the user
- or solutions detects user normal behavior
- Monitor machine for 30 days?
- any methods require local admin
- dows Features ♥ to the rescue

fortalte o
erktøy på
tremt moro

et, gjør det unikt, sier Melvin Langvik i

TRUSTEDSEC

KOVERT

What is this talk?

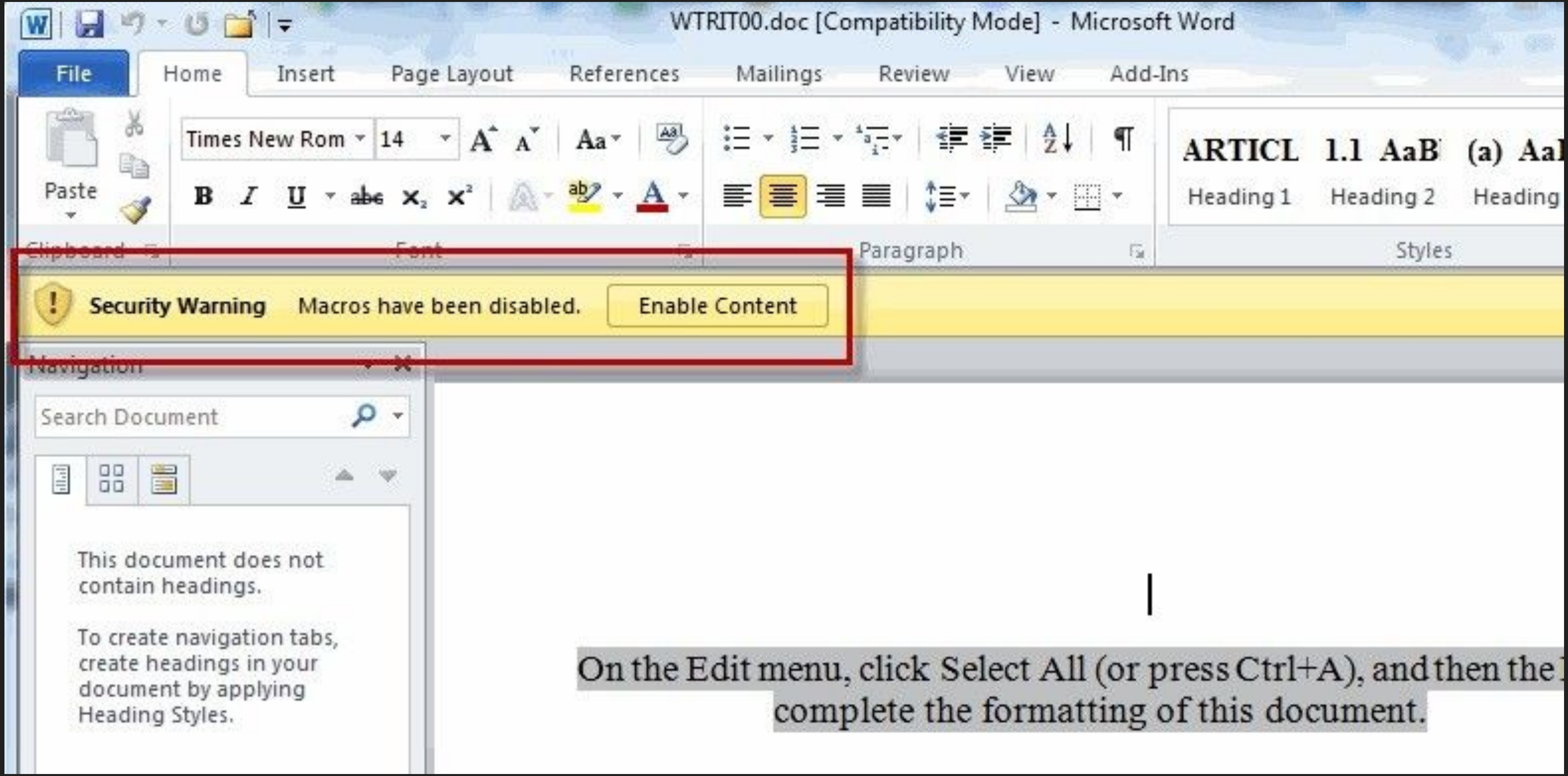
- Coworkers for many years
- Red Team / AAS
- *War Stories*
- What about the failures?
  - **The F*** ups**
  - “lessons” learned
  - TTP found! (sometimes)
- Lean back, it’s storytime!

PHISH PHISH
PHISH PHISH

Must be realistic!

PHISHING
H HD
HISTORY.COM
imgflip.com

Phish #1 - Word document with Macro



Security Warning Macros have been disabled. Enable Content

This document does not contain headings.

To create navigation tabs, create headings in your document by applying Heading Styles.

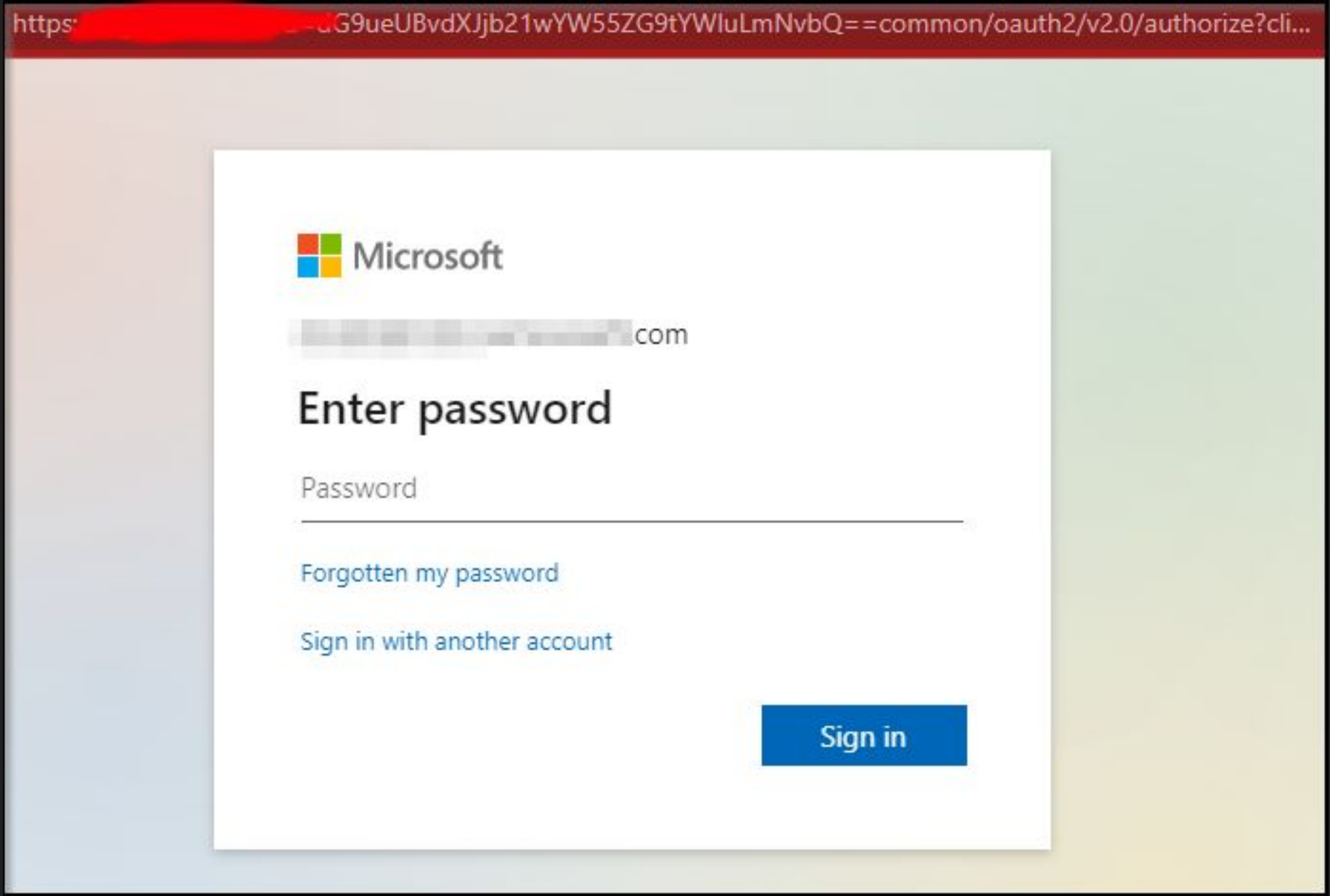
On the Edit menu, click Select All (or press Ctrl+A), and then the

complete the formatting of this document.

Got shell from 2 users

Was Joe and User

Phish #2 - Credentials



https:[redacted]G9ueUBvdXJjb21wYW55ZG9tYWluLmNvbQ==common/oauth2/v2.0/authorize?cli...

Microsoft

[redacted]com

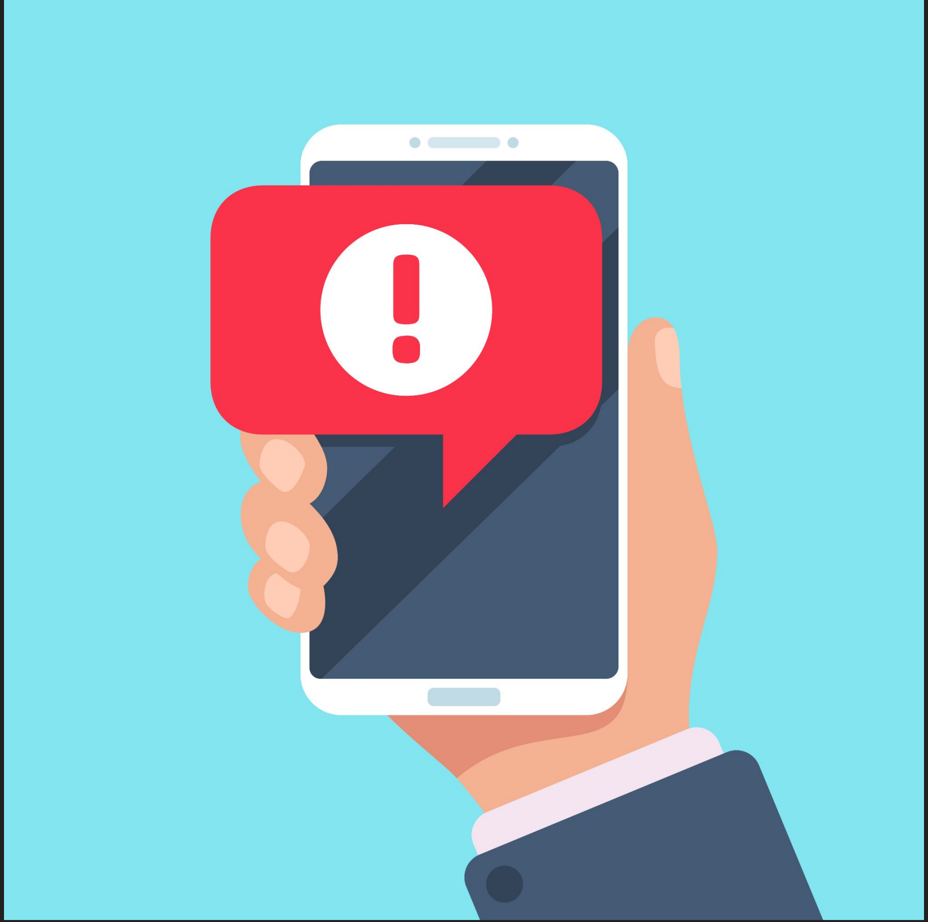
Enter password

Password

Forgotten my password

Sign in with another account

Phish #2 - Credentials



Phish #2 - Credentials

Username:

YourPhish@customer.com

Password: SucksLoser!

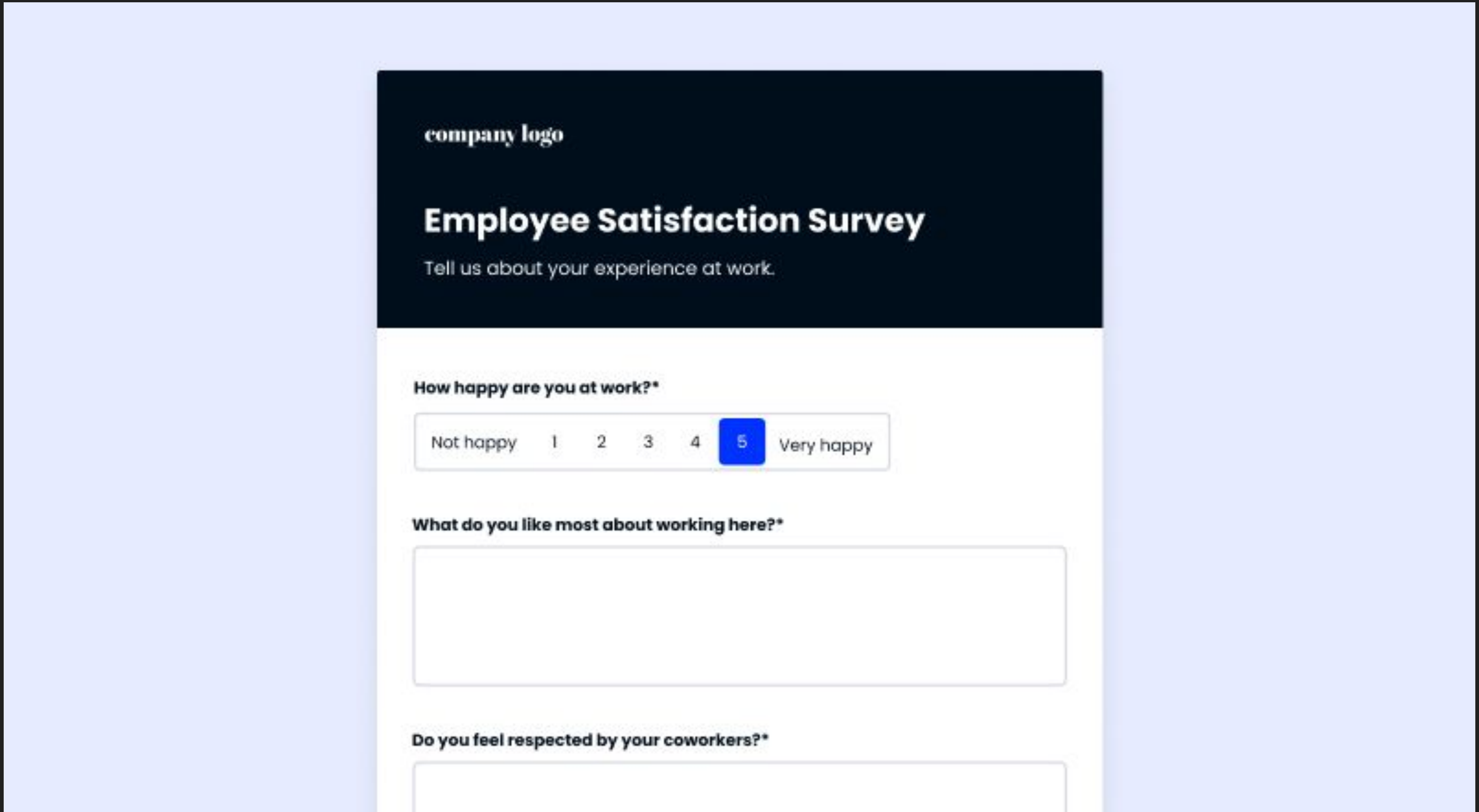
Phish 3 - Don’t want to talk about it…

Phish 4 - Another Failed Phish

My feelings at this moment

Change Career?

Phish # 5 - Survey



company logo

Employee Satisfaction Survey

Tell us about your experience at work.

How happy are you at work?*

Not happy 1 2 3 4 [✓ 5] Very happy

What do you like most about working here?*

Do you feel respected by your coworkers?*

Established persistence

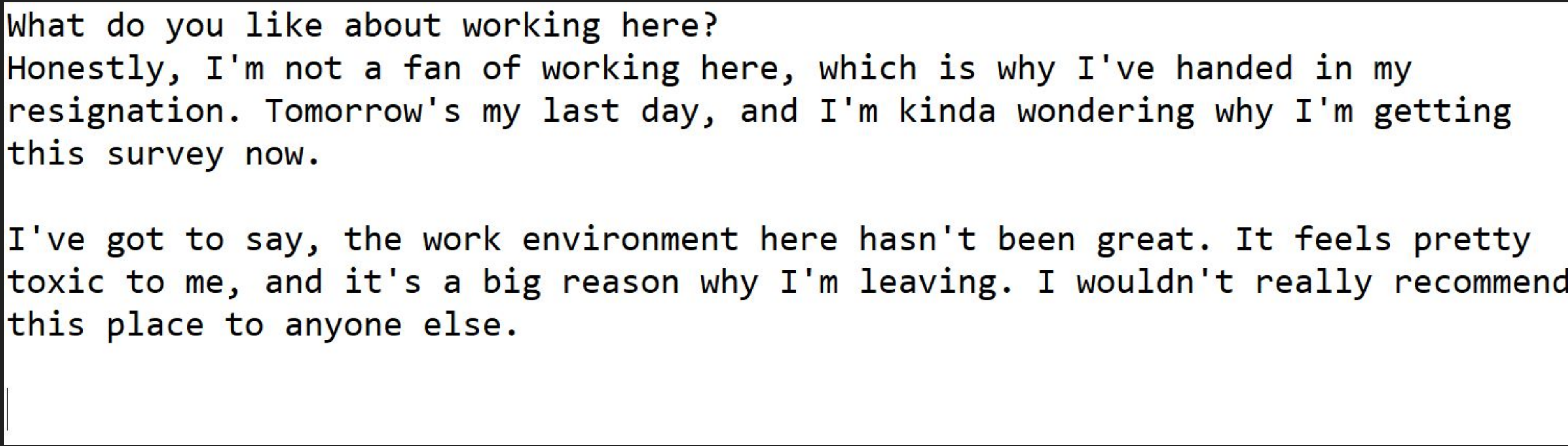
Screenshots

Downloaded files

Explored config of machine

Happy and took an early evening!

Checked the survey answers



What do you like about working here?
Honestly, I'm not a fan of working here, which is why I've handed in my resignation. Tomorrow's my last day, and I'm kinda wondering why I'm getting this survey now.

I've got to say, the work environment here hasn't been great. It feels pretty toxic to me, and it's a big reason why I'm leaving. I wouldn't really recommend this place to anyone else.

Thinking while writing the report on how I failed

T
SPI

AZURE INFORMATION PROTECTION

Encrypts and protects the attachment

Can only be opened by designated target

Bypassed all sandboxes and scanning engines

Blue team had to logon as that user to get the macro out

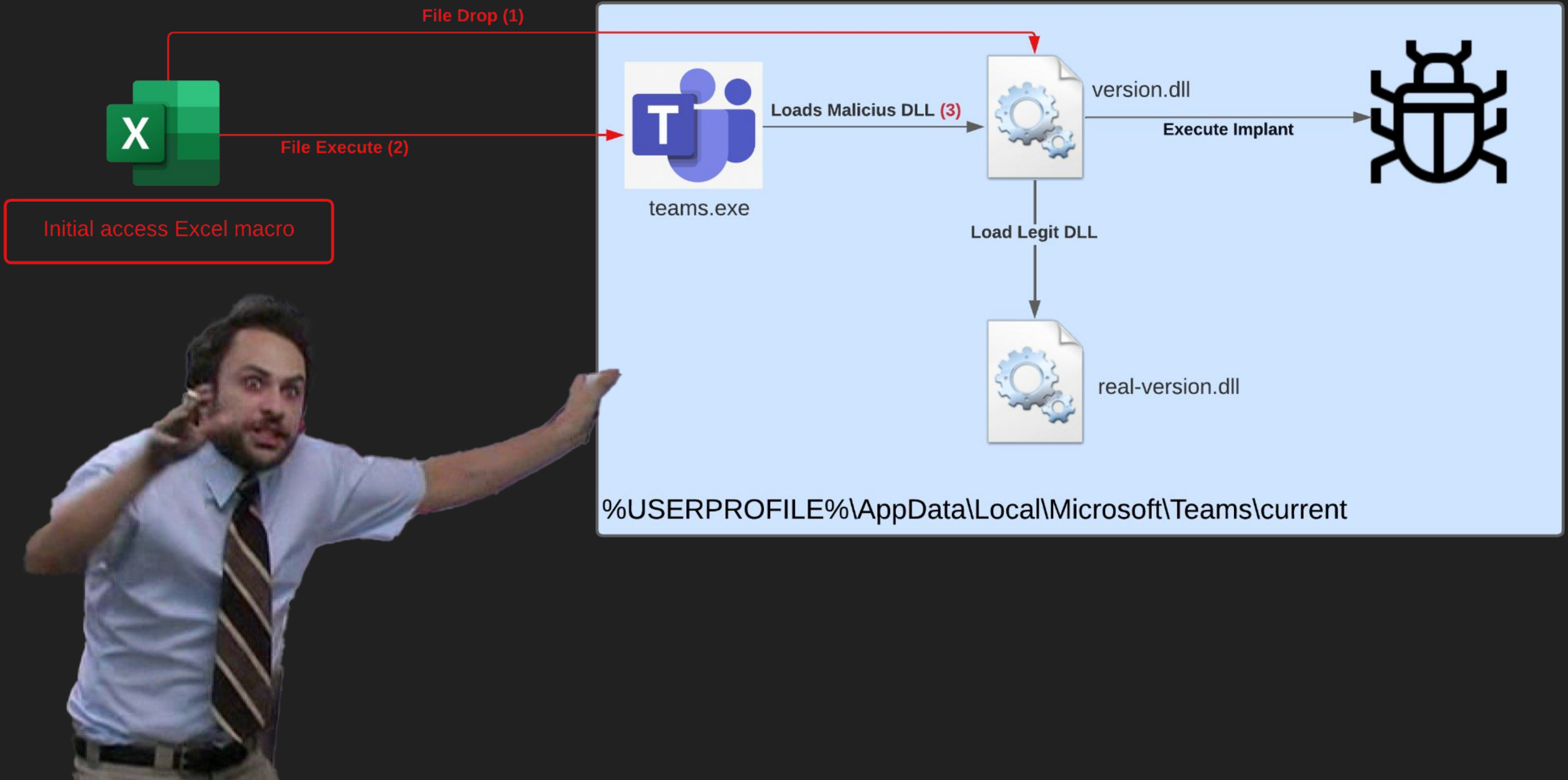
https://www.youtube.com/watch?v=EYUp_MNtJIk (Phishing past Mail Protection Controls using Azure Information Protection)

What did we learn?

- Persistence pays off
- Remember to do in depth osint of people you target (They might be leaving)
- When you meet a lot of resistance and fail over and over and over and over again you get creative!

My very first time

The plan!



File Drop (1)

File Execute (2)

Initial access Excel macro

teams.exe

Loads Malicius DLL (3)

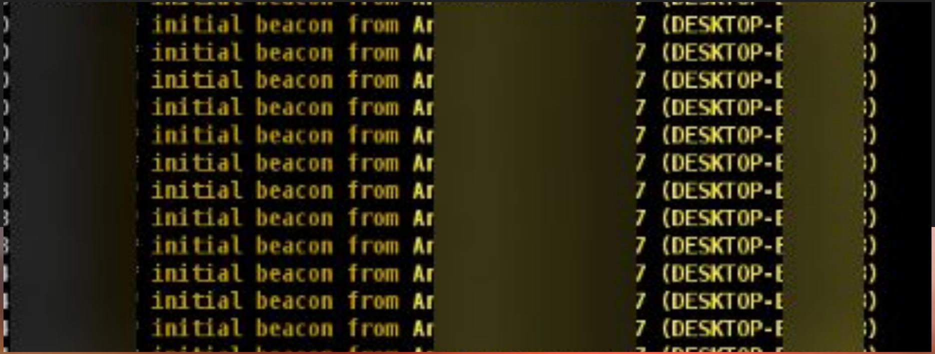
version.dll

Execute Implant

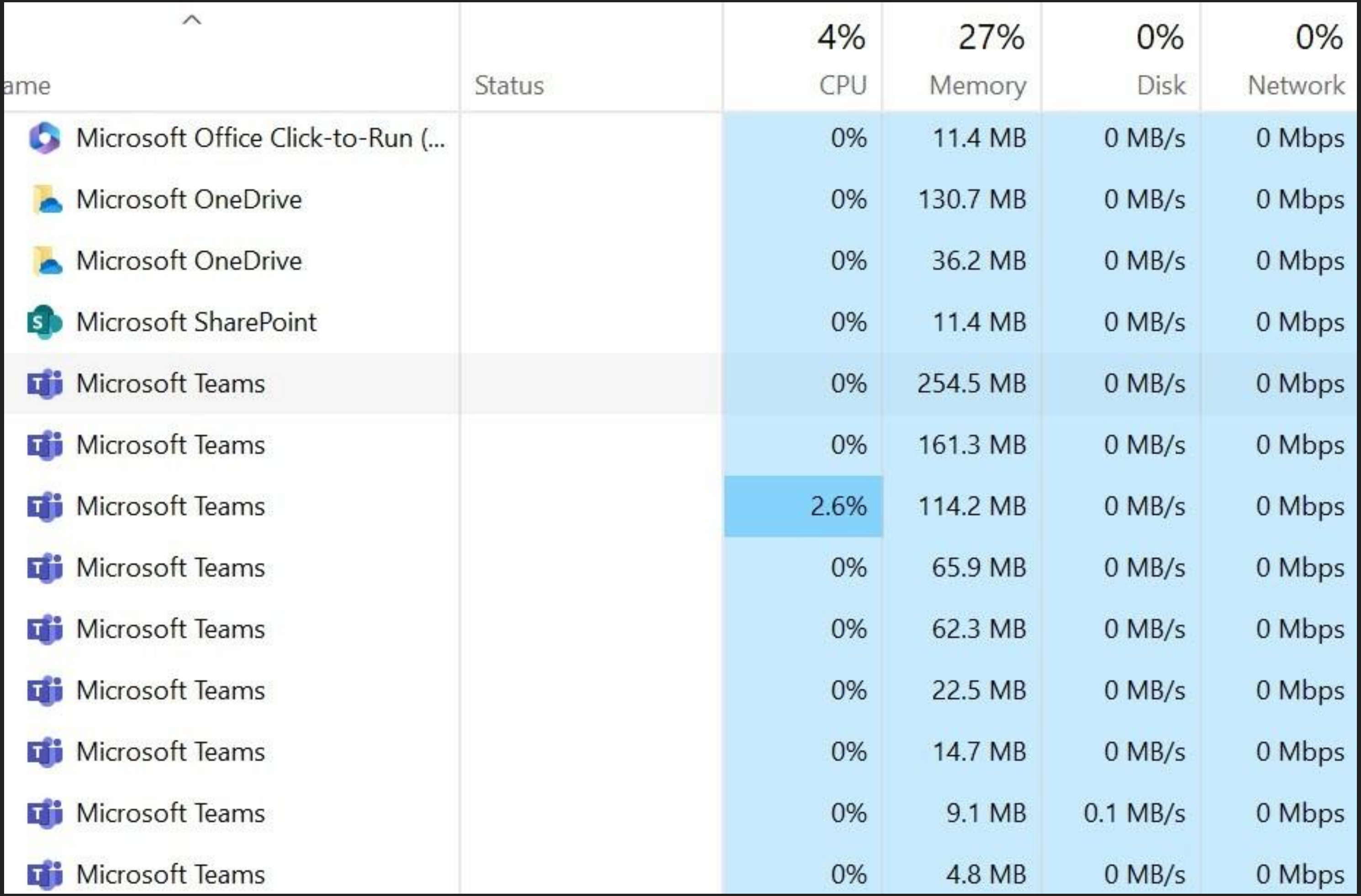
Load Legit DLL

real-version.dll

%USERPROFILE%\AppData\Local\Microsoft\Teams\current

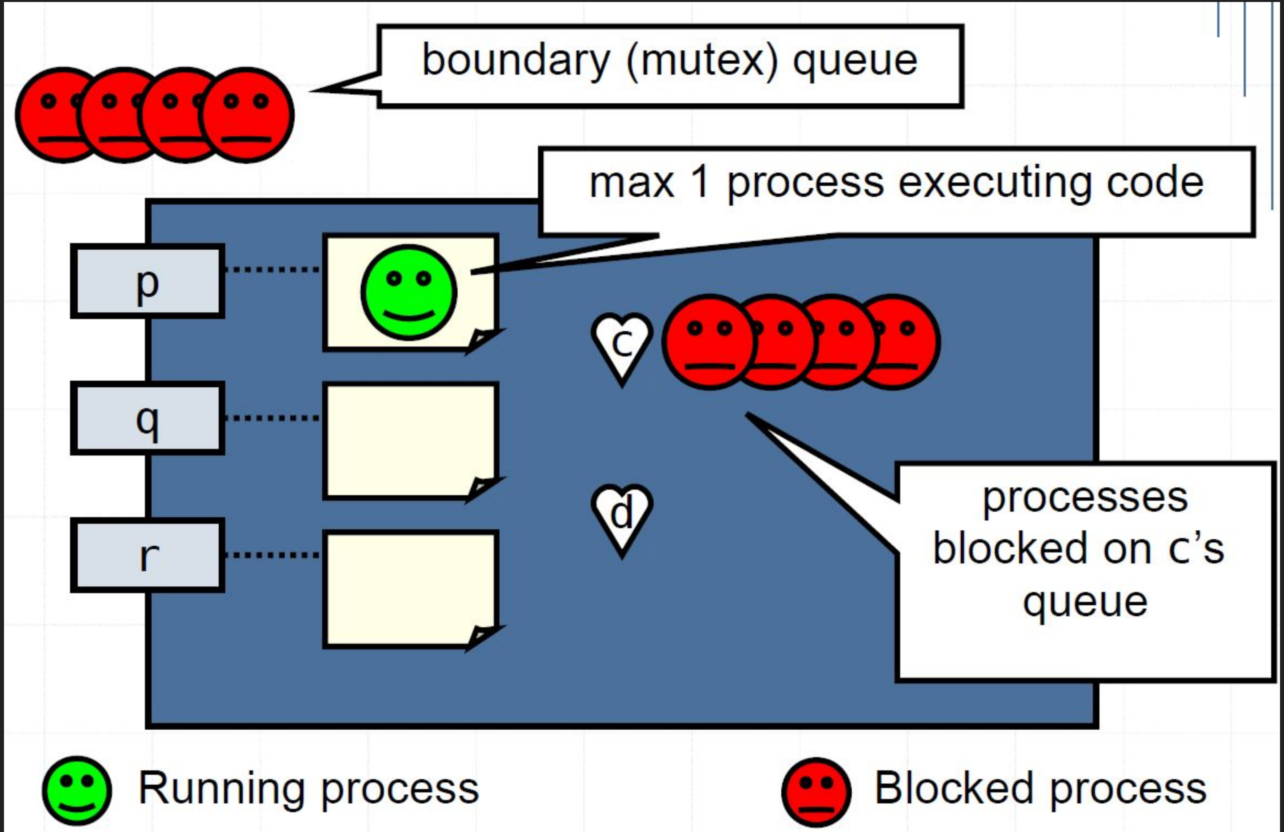


```
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
[redacted] initial beacon from Ar[redacted]7 (DESKTOP-E[redacted])
```



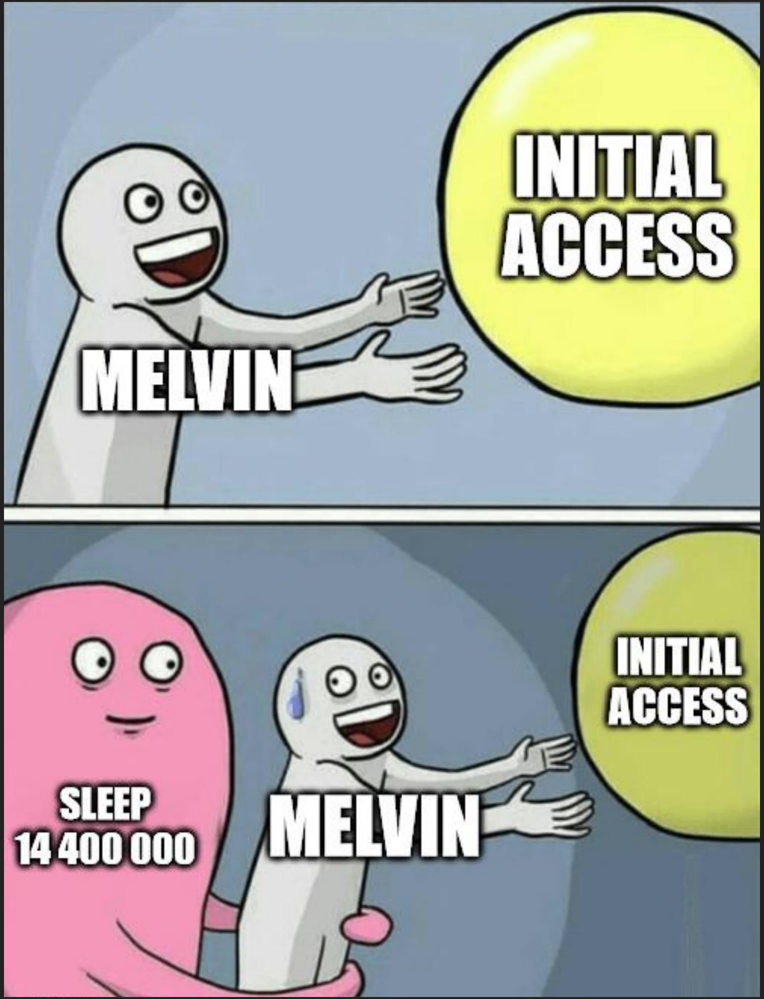
		4%	27%	0%	0%
ame	Status	CPU	Memory	Disk	Network
Microsoft Office Click-to-Run (...		0%	11.4 MB	0 MB/s	0 Mbps
Microsoft OneDrive		0%	130.7 MB	0 MB/s	0 Mbps
Microsoft OneDrive		0%	36.2 MB	0 MB/s	0 Mbps
Microsoft SharePoint		0%	11.4 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	254.5 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	161.3 MB	0 MB/s	0 Mbps
Microsoft Teams		2.6%	114.2 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	65.9 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	62.3 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	22.5 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	14.7 MB	0 MB/s	0 Mbps
Microsoft Teams		0%	9.1 MB	0.1 MB/s	0 Mbps
Microsoft Teams		0%	4.8 MB	0 MB/s	0 Mbps

“Guardrails” - Process mutex

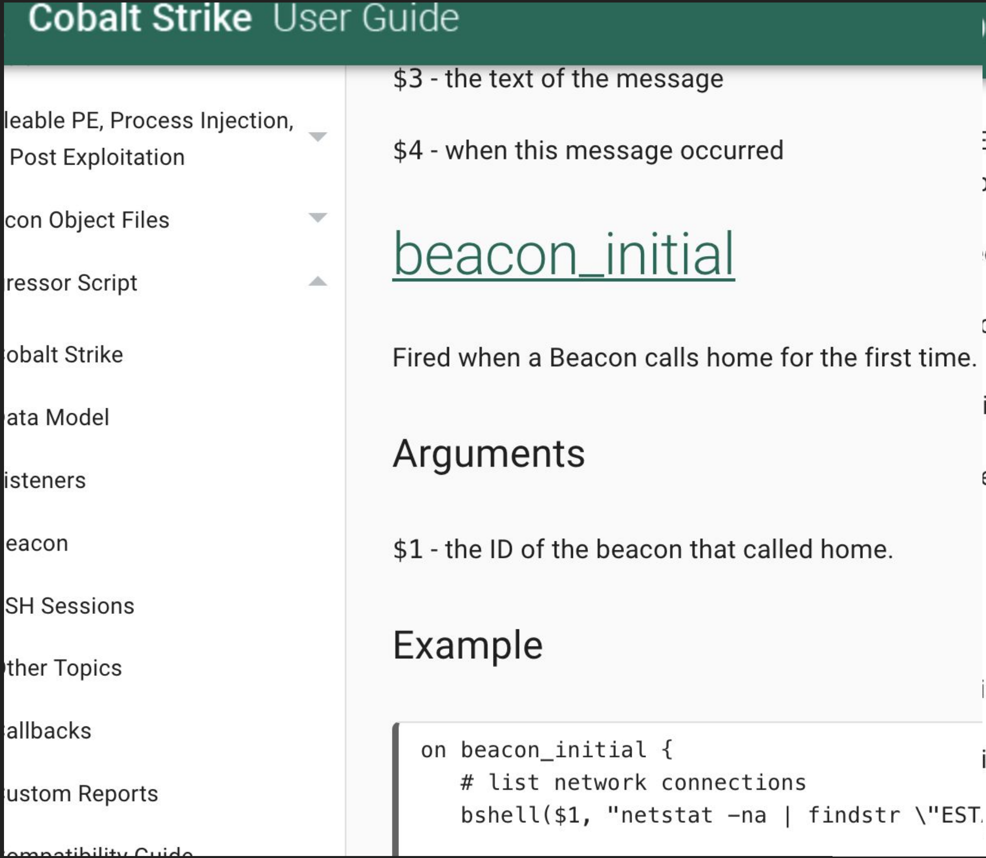


https://www.cse.chalmers.se/edu/year/2015/course/TDA383_LP3/lecture4.html

INITIAL ACCESS
MELVIN


INITIAL ACCESS
MELVIN
INITIAL ACCESS
SLEEP 14 400 000
MELVIN

How can we fix this???



$3 - the text of the message

$4 - when this message occurred

beacon_initial

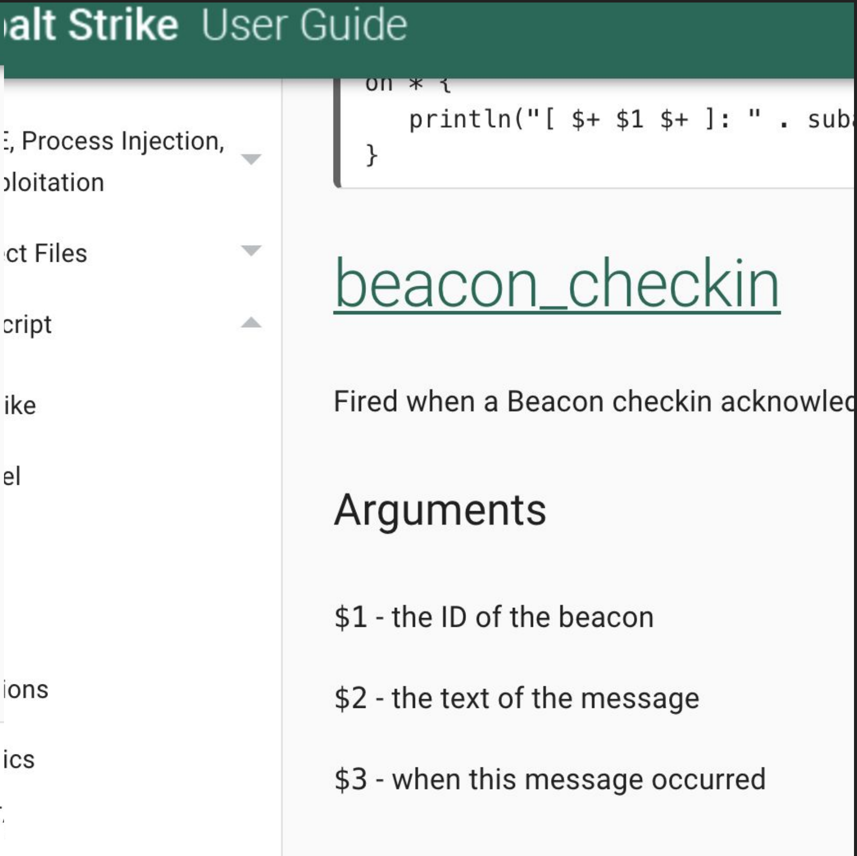
Fired when a Beacon calls home for the first time.

Arguments

$1 - the ID of the beacon that called home.

Example

```
on beacon_initial {
   # list network connections
   bshell($1, "netstat -na | findstr \"EST.
```



```
on * {
   println("[ $+ $1 $+ ]: " . sub
}
```

beacon_checkin

Fired when a Beacon checkin acknowled

Arguments

$1 - the ID of the beacon

$2 - the text of the message

$3 - when this message occurred

What did we learn?

- ALWAYS check your payload configuration before hitting send
- Replicating and “playing out” the initial access scenario in the lab pays off!
- **You can actually get "too much" initial access**

Externally

- Basically nothing
- Barely anything exposed
- No luck on password spraying
- Except “CRITICAL” SSL3 Findings

Phishing - Landed a shell

Used an internal payload and framework for C2

(Details will be released later this year) – Teaser!

Internally - Things are locked down!

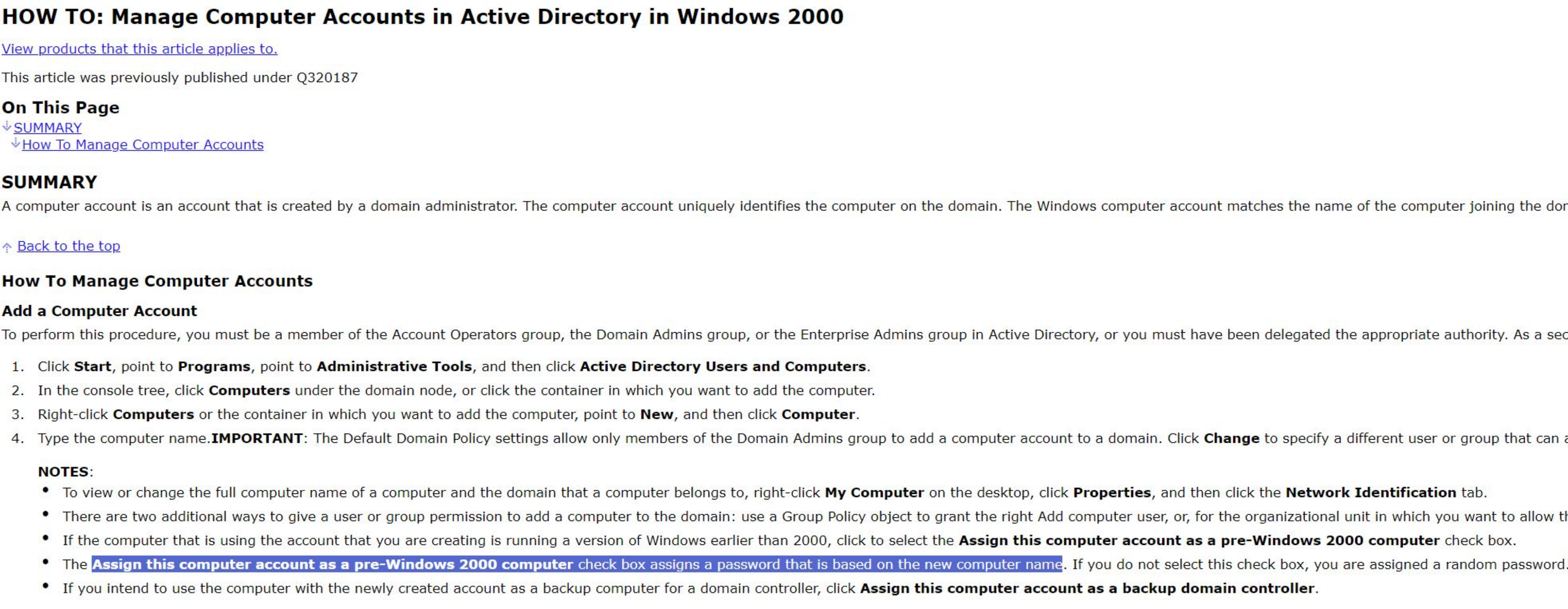
- No weak credentials
- No local escalations
- No SPN to kerberoast
- Nothing on file shares
- No default credentials
- Network stuff? Printers, tomcat - NOPE
- Coercing? Forget it
- Bloodhound paths? Nothing!
- Certs? Well, ESC1 for domain computers
- Stuck at the initial foothold

- This was however an old domain

LOOSER
DO YOU EVEN HACK?
GIVE UP!

-

THE BOYS
I HAVE
AN IDEA



HOW TO: Manage Computer Accounts in Active Directory in Windows 2000

View products that this article applies to.

This article was previously published under Q320187

On This Page

SUMMARY

How To Manage Computer Accounts

SUMMARY

A computer account is an account that is created by a domain administrator. The computer account uniquely identifies the computer on the domain. The Windows computer account matches the name of the computer joining the dor

Back to the top

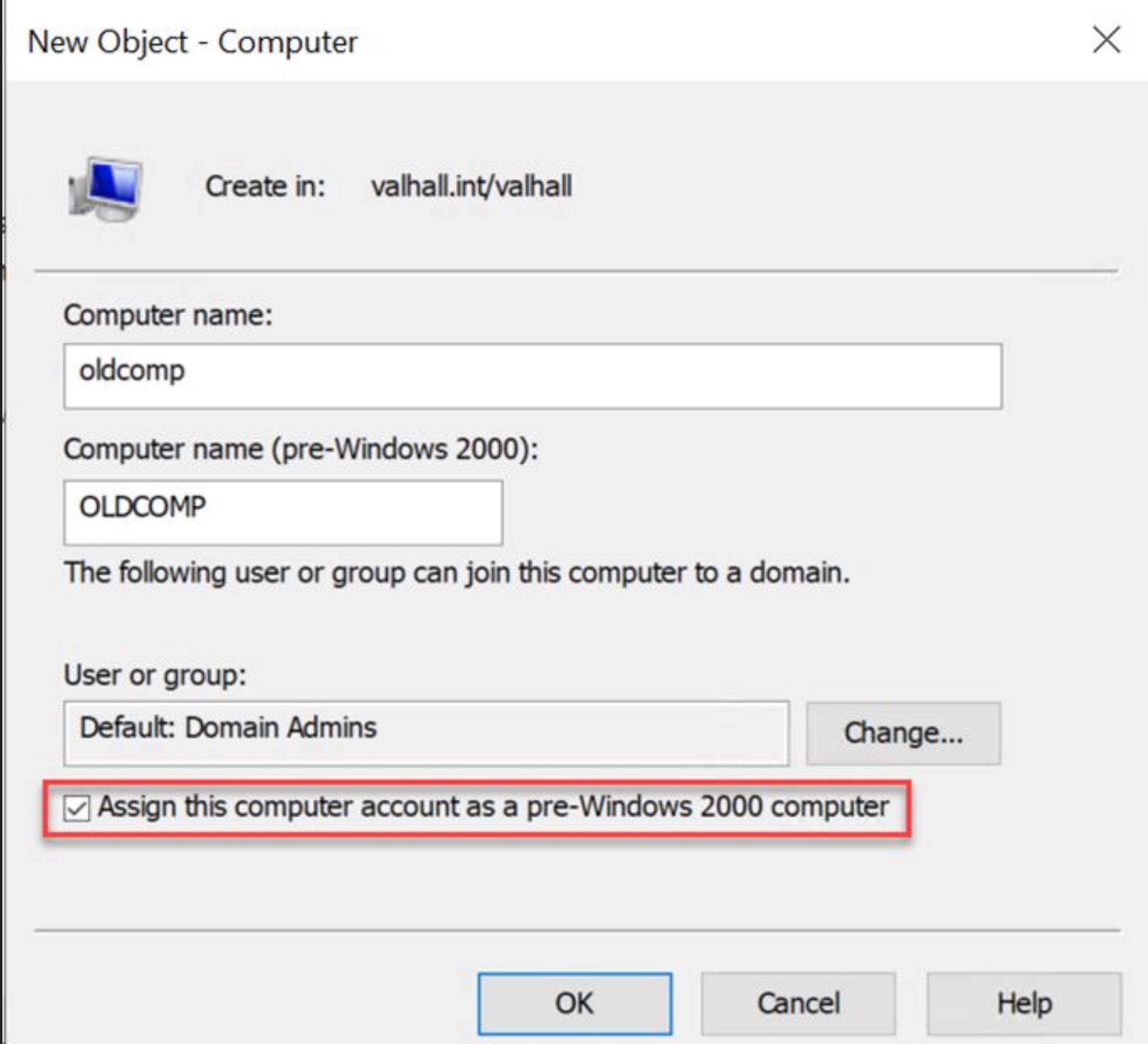
How To Manage Computer Accounts

Add a Computer Account

To perform this procedure, you must be a member of the Account Operators group, the Domain Admins group, or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. As a sec

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, click **Computers** under the domain node, or click the container in which you want to add the computer.
3. Right-click **Computers** or the container in which you want to add the computer, point to **New**, and then click **Computer**.
4. Type the computer name.**IMPORTANT**: The Default Domain Policy settings allow only members of the Domain Admins group to add a computer account to a domain. Click **Change** to specify a different user or group that can a

   NOTES:
   - To view or change the full computer name of a computer and the domain that a computer belongs to, right-click **My Computer** on the desktop, click **Properties**, and then click the **Network Identification** tab.
   - There are two additional ways to give a user or group permission to add a computer to the domain: use a Group Policy object to grant the right Add computer user, or, for the organizational unit in which you want to allow th
   - If the computer that is using the account that you are creating is running a version of Windows earlier than 2000, click to select the **Assign this computer account as a pre-Windows 2000 computer** check box.
   - The **Assign this computer account as a pre-Windows 2000 computer** check box assigns a password that is based on the new computer name. If you do not select this check box, you are assigned a random password.
   - If you intend to use the computer with the newly created account as a backup computer for a domain controller, click **Assign this computer account as a backup domain controller**.



New Object - Computer

Create in: valhall.int/valhall

Computer name:

oldcomp

Computer name (pre-Windows 2000):

OLDCOMP

The following user or group can join this computer to a domain.

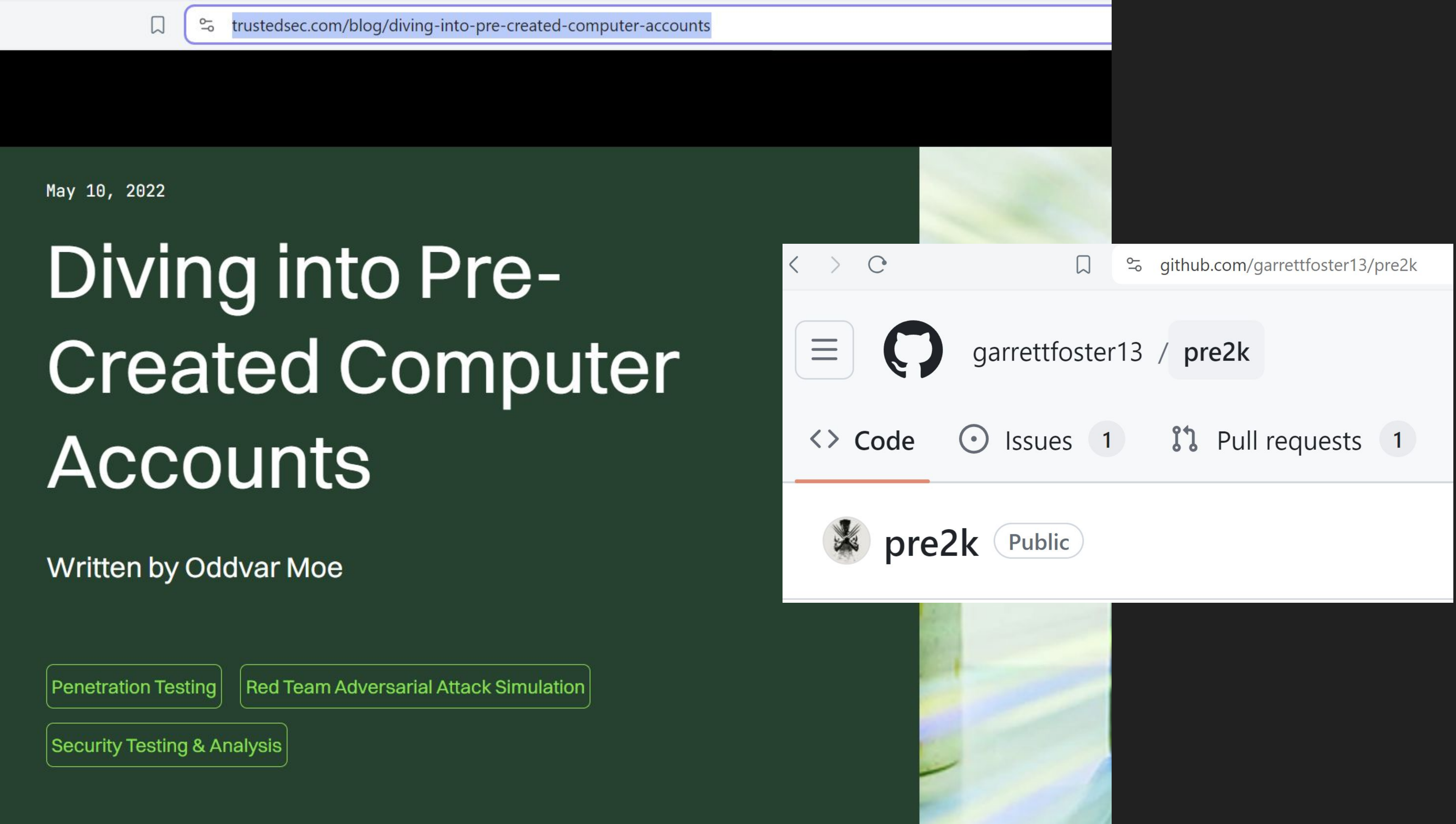
User or group:

Default: Domain Admins

☑ Assign this computer account as a pre-Windows 2000 computer

Searched for old computer accounts

- User account control:
  - PASSWD_NOTREQD
  - WORKSTATION_TRUST_ACCOUNT (4128)
- Found two accounts that actually had the password set to the computer name
- Had to change the password - wrote some custom tooling
- Requested certificate and yeah - full compromise without detection!
- Guess who dreamt of who that following night?



trustedsec.com/blog/diving-into-pre-created-computer-accounts

May 10, 2022

Diving into Pre-Created Computer Accounts

Written by Oddvar Moe

Penetration Testing
Red Team Adversarial Attack Simulation
Security Testing & Analysis

github.com/garrettfoster13/pre2k

garrettfoster13 / pre2k

Code
Issues 1
Pull requests 1

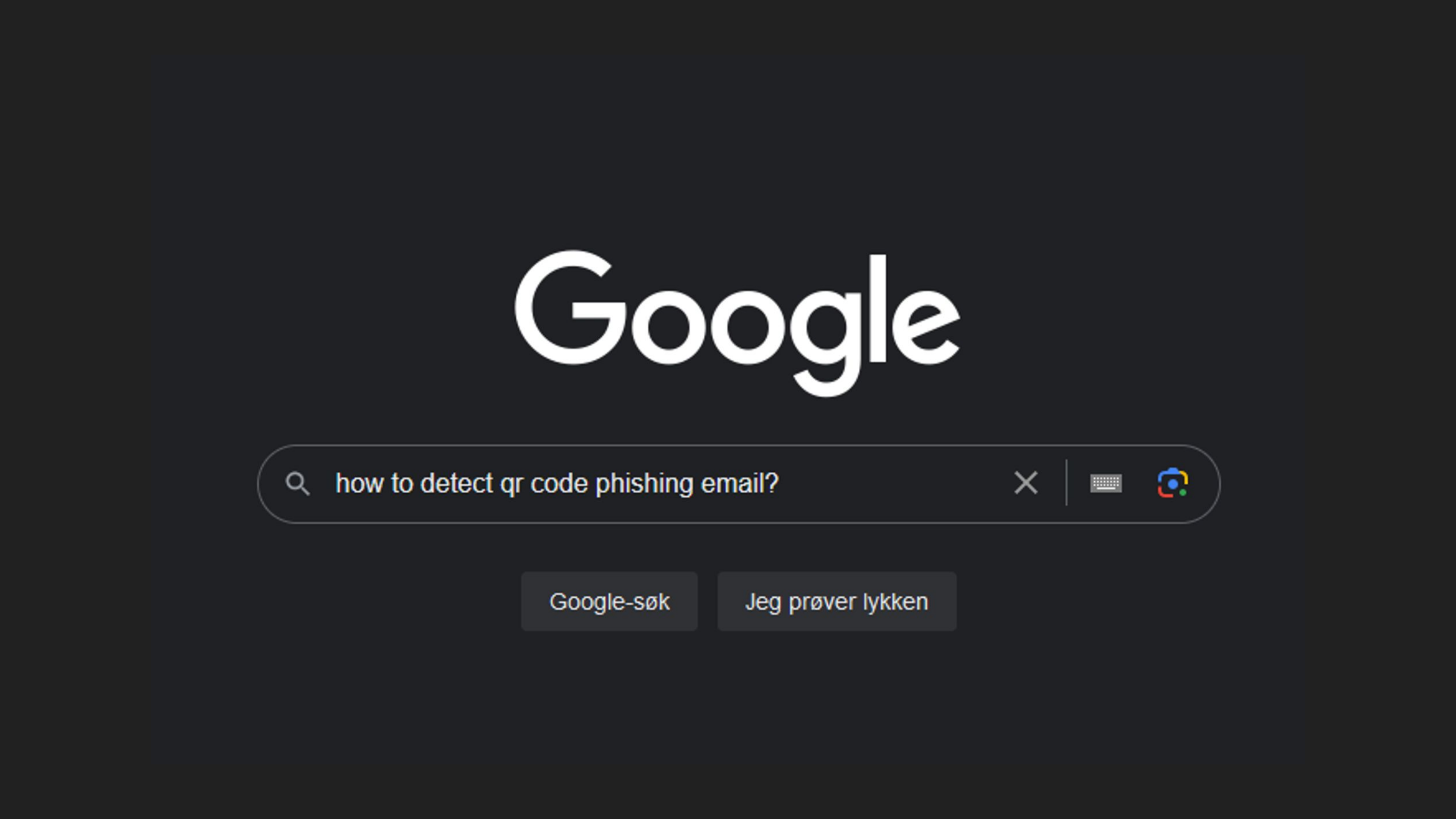
pre2k Public

What did we learn?

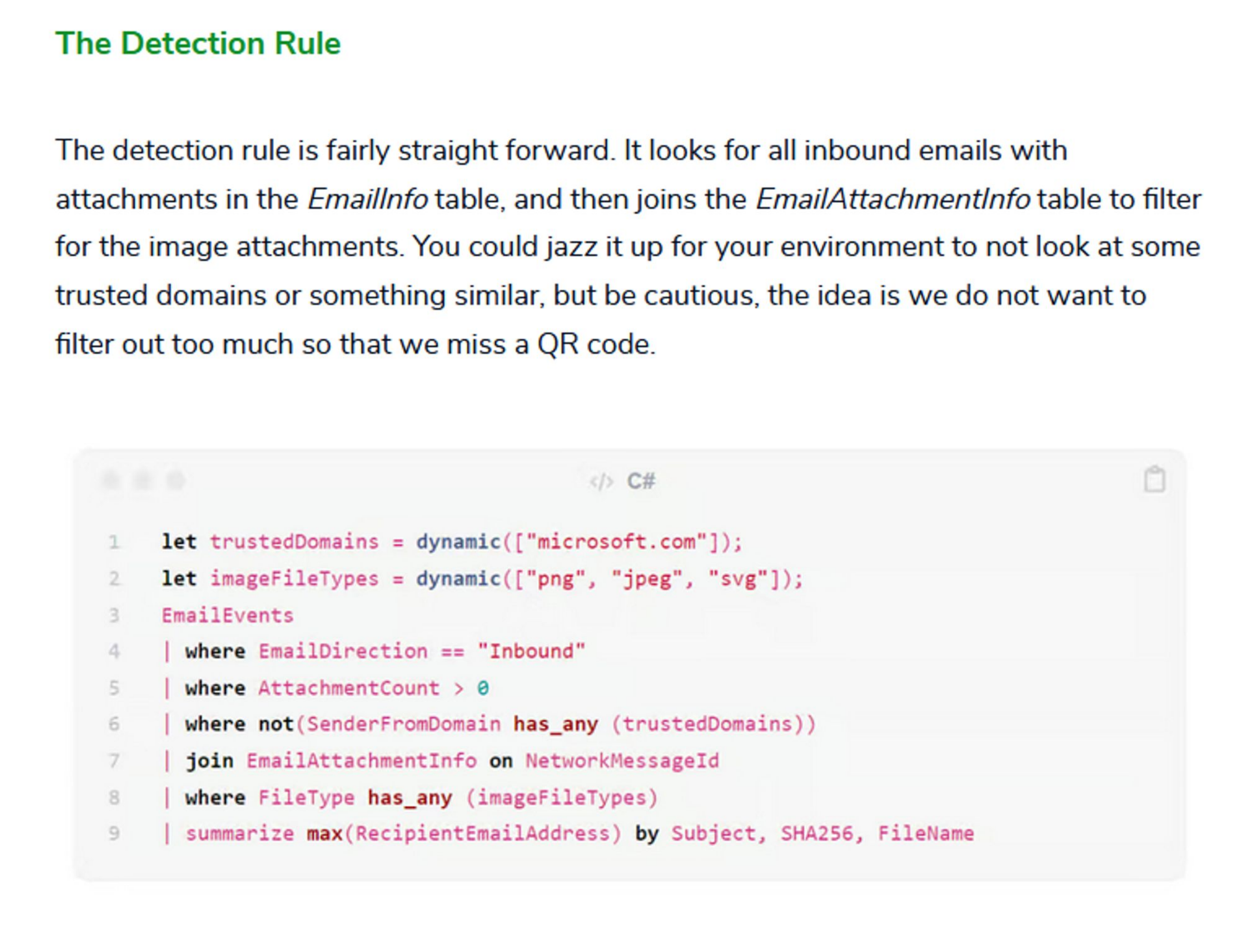
- Never give up! Just try harder until you lose sleep over it!
- Rage fuels creative research ideas
- Legacy knowledge can actually be useful sometimes!

Meeting the client

I got a tingle…



how to detect qr code phishing email?



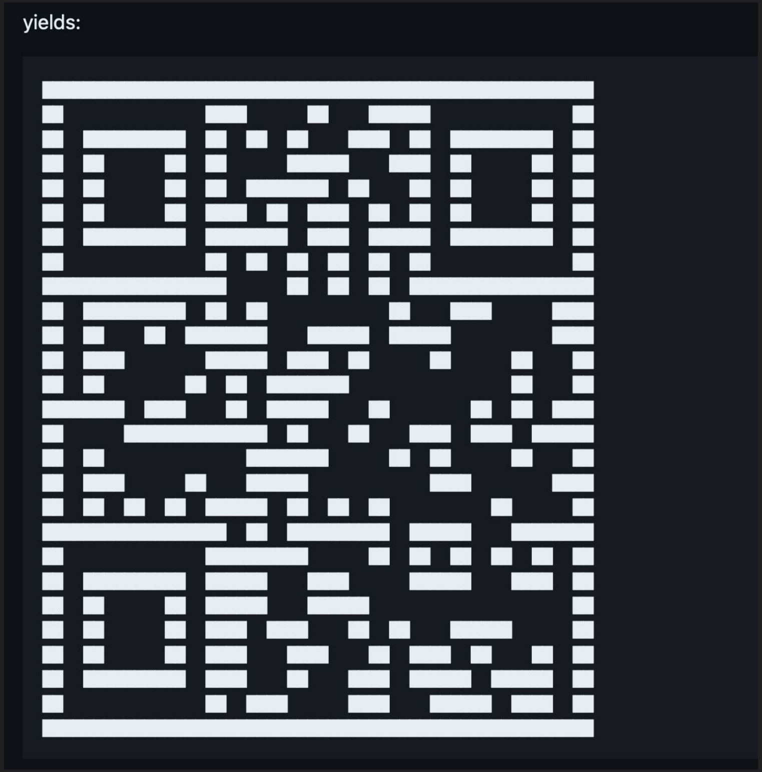
The Detection Rule

The detection rule is fairly straight forward. It looks for all inbound emails with attachments in the *EmailInfo* table, and then joins the *EmailAttachmentInfo* table to filter for the image attachments. You could jazz it up for your environment to not look at some trusted domains or something similar, but be cautious, the idea is we do not want to filter out too much so that we miss a QR code.

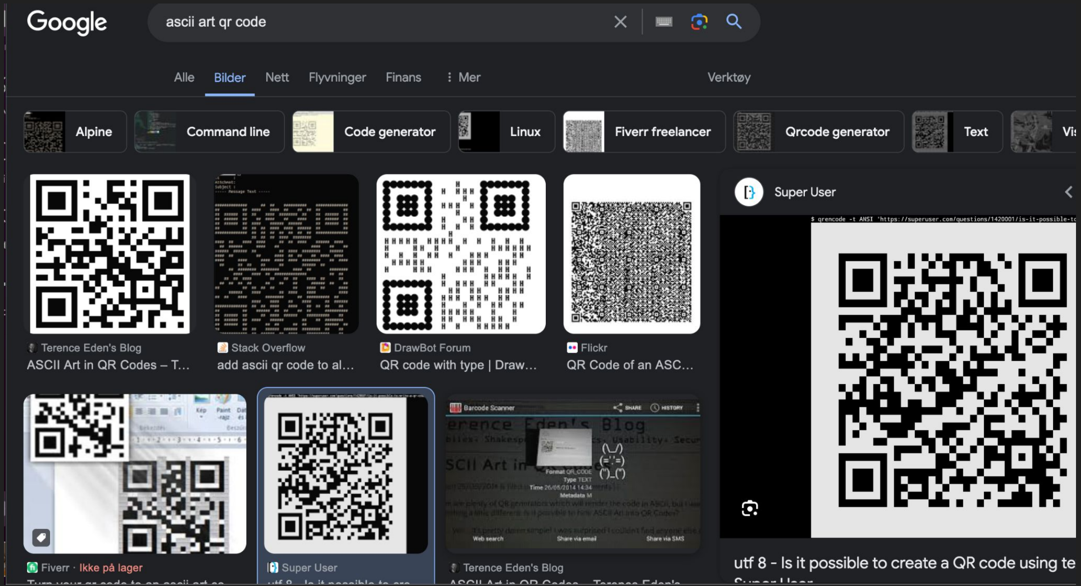
```
let trustedDomains = dynamic(["microsoft.com"]);
let imageFileTypes = dynamic(["png", "jpeg", "svg"]);
EmailEvents
| where EmailDirection == "Inbound"
| where AttachmentCount > 0
| where not(SenderFromDomain has_any (trustedDomains))
| join EmailAttachmentInfo on NetworkMessageId
| where FileType has_any (imageFileTypes)
| summarize max(RecipientEmailAddress) by Subject, SHA256, FileName
```

https://stripeolt.com/knowledge-hub/expert-intel/qr-code-phishing-detection/ - *Liam Jones*

QR Codes without the images?



yields:



Terence Eden's Blog
ASCII Art in QR Codes – T…

Stack Overflow
add ascii qr code to al…

DrawBot Forum
QR code with type | Draw…

Flickr
QR Code of an ASC…

Super User

```
$ qrencode -t ANSI 'https://superuser.com/questions/1420001/is-it-possible-to
```

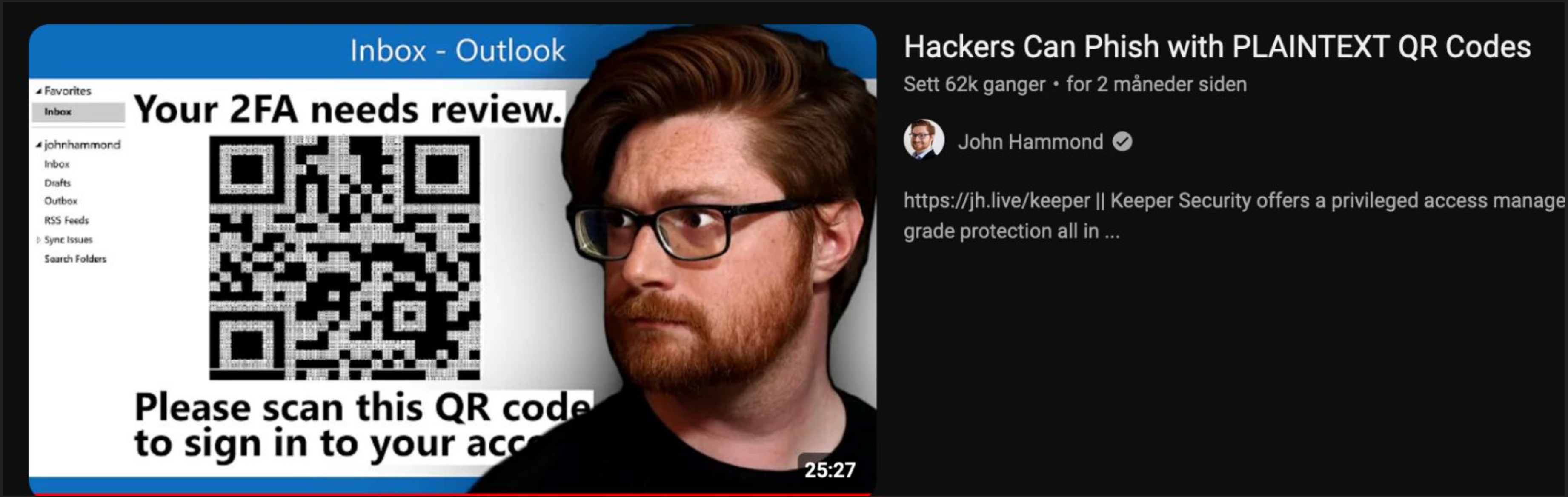
utf 8 - Is it possible to create a QR code using te

Fiverr · Ikke på lager

Super User

Terence Eden's Blog

Old news…



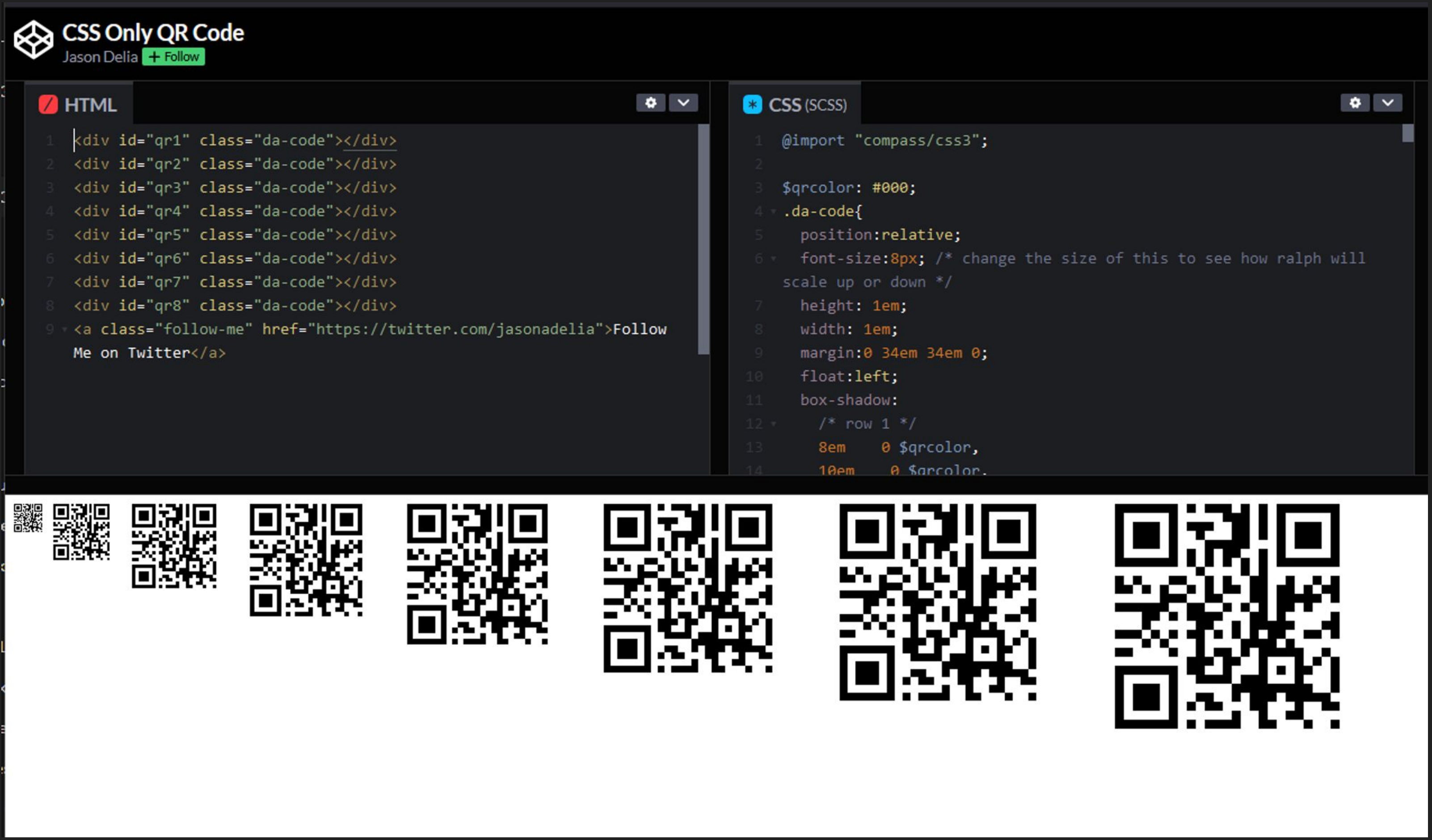
Hackers Can Phish with PLAINTEXT QR Codes

Sett 62k ganger • for 2 måneder siden

John Hammond

https://jh.live/keeper || Keeper Security offers a privileged access manage grade protection all in ...

https://www.youtube.com/watch?v=cG8Uq2VESfM&pp=ygUPSm9obiBIYW1tb25kIFFS

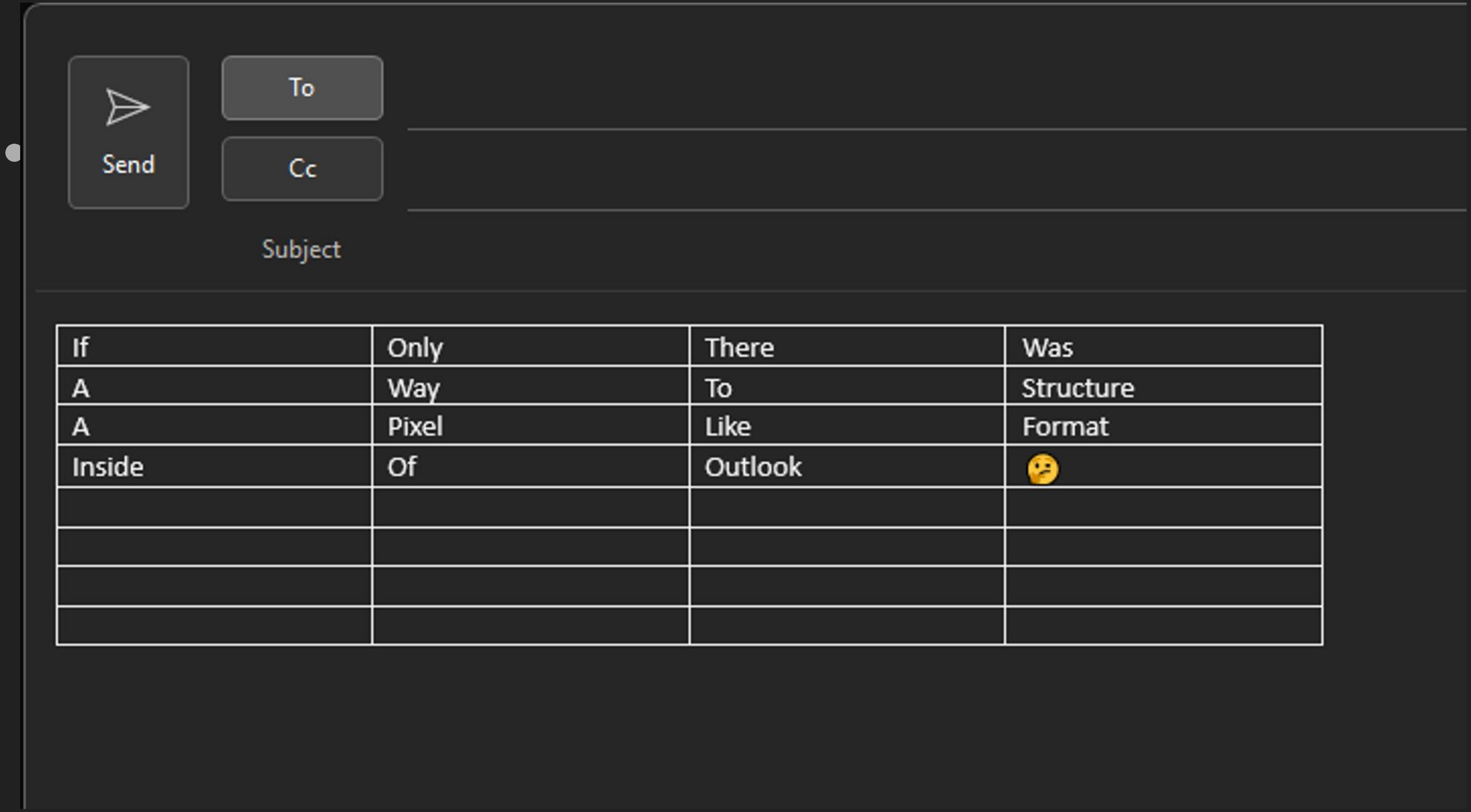


```html
<div id="qr1" class="da-code"></div>
<div id="qr2" class="da-code"></div>
<div id="qr3" class="da-code"></div>
<div id="qr4" class="da-code"></div>
<div id="qr5" class="da-code"></div>
<div id="qr6" class="da-code"></div>
<div id="qr7" class="da-code"></div>
<div id="qr8" class="da-code"></div>
<a class="follow-me" href="https://twitter.com/jasonadelia">Follow Me on Twitter</a>
```

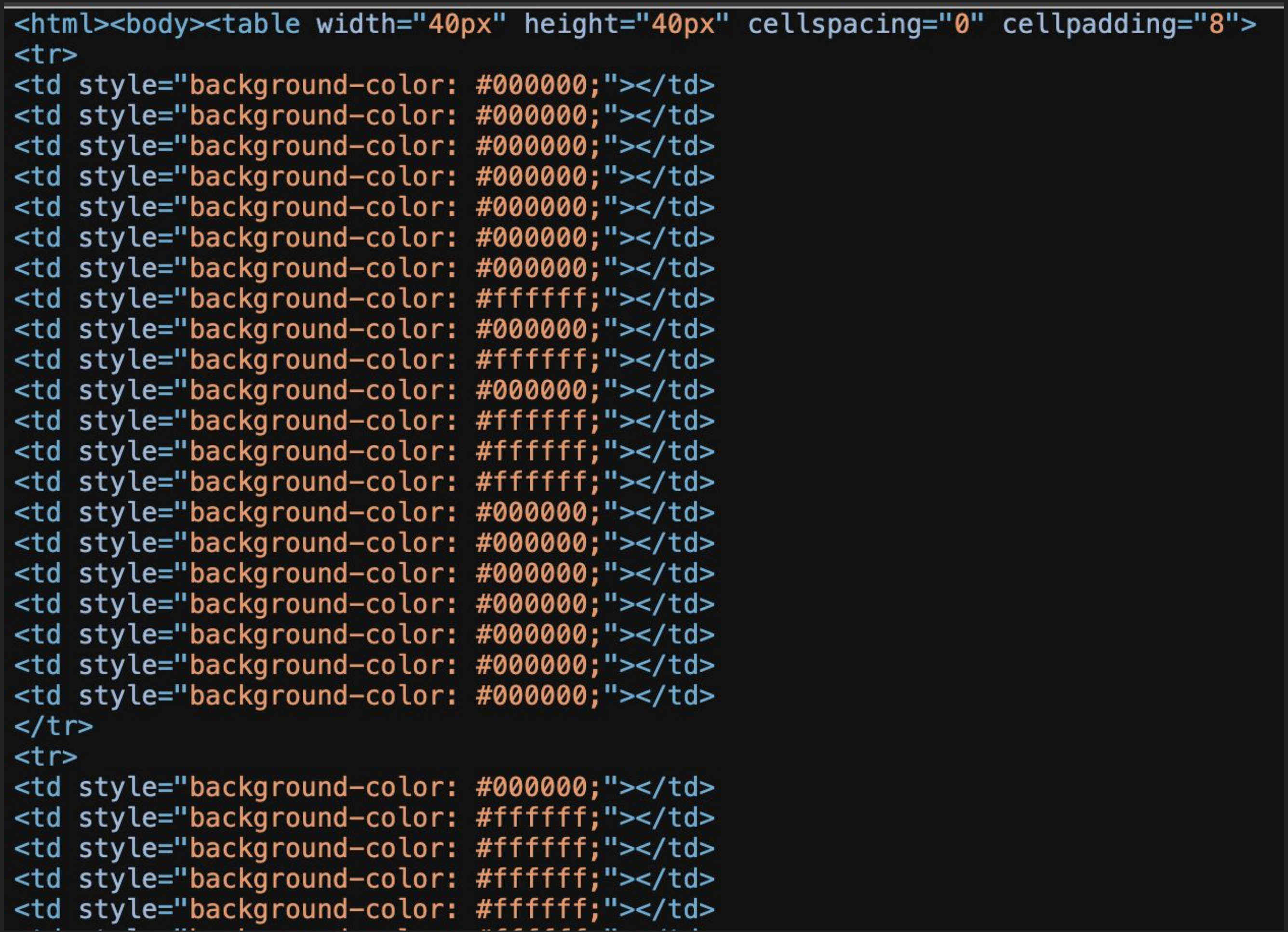
```scss
@import "compass/css3";

$qrcolor: #000;
.da-code{
  position:relative;
  font-size:8px; /* change the size of this to see how ralph will scale up or down */
  height: 1em;
  width: 1em;
  margin:0 34em 34em 0;
  float:left;
  box-shadow:
    /* row 1 */
    8em    0 $qrcolor,
    10em    0 $qrcolor,
```

https://codepen.io/jasonadelia/pen/DwWaNW



If	Only	There	Was
A	Way	To	Structure
A	Pixel	Like	Format
Inside	Of	Outlook	🤔



```html
<html><body><table width="40px" height="40px" cellspacing="0" cellpadding="8">
<tr>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
</tr>
<tr>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
```

Demo time!

What it feels like

What did we learn?

- Basic research on potential detections likely pays off
- KISS
  - Keep it simple, **stupid**
- Project can be found at

Thank you!