
TRACK THE PLANET!
Mapping Identities, Monitoring Presence, and Decoding
Business Alliances in the Azure Ecosystem

about me

- nyxgeek
- hacker at TrustedSec, research my own

- CVE-2020-5774 - Tenable Nessus (lame vuln)
- CVE-2018-8474 - Microsoft Lync 2011 for Mac (cool)
- CVE-2017-8550 - Microsoft Skype for Business 2016 (cool)
- [NO CVE GRANTED] – Microsoft Lync Time-based Enumeration (cool)

- Twitter: @nyxgeek
- Github: https://github.com/nyxgeek

- This talk is about user enumeration, its impacts, and why Microsoft should take it seriously. Everything demonstrated is by design.

- Microsoft has decided that user enumeration does not qualify as a vulnerability.

user enumeration: what it is and why it matters

an overview of user enumeration, its various forms, and its impacts

What is User Enumeration?

- Enables an attacker to identify VALID accounts, and INVALID accounts based on server response

Examples:

- Verbose login response - "Your username is invalid"

- Time-based login response
  - INVALID Username response time: 10s
  - VALID Username login response time: 1s

- Web server response differs (403 vs 404 HTTP Status Code)

  [404] http://fakedomain.com/application/users/tom
  [403] http://fakedomain.com/application/users/john

```
Started enumerating onedrive at 2019-03-05 16:32:43.570917
[-] [404] not found acmecomputercompany.com - fakeuser
[-] [404] not found acmecomputercompany.com - fake.user
[-] [404] not found acmecomputercompany.com - westb
[+] [403] VALID ONEDRIVE FOR acmecomputercompany.com - westa
[-] [404] not found acmecomputercompany.com - westc
[+] [403] VALID ONEDRIVE FOR acmecomputercompany.com - lightmand
[-] [404] not found acmecomputercompany.com - admin
[-] [404] not found acmecomputercompany.com - crabapplee
[+] [403] VALID ONEDRIVE FOR acmecomputercompany.com - johns
[-] [404] not found acmecomputercompany.com - venturej
[-] [404] not found acmecomputercompany.com - stevens
[-] [404] not found acmecomputercompany.com - stevenf
```

User Enumeration is a Security Flaw

- ENABLES:
  - Password sprays
  - Phishing
  - Targeted RCE or similar (every so often)
- Unnecessary "feature"
- Allows identification and targeting of users directly
  - Often includes full names (john.smith or john.j.smith formats)
  - Durable lists – names change infrequently in a lifetime
- Can't hit what you can't see (or at least it's harder)

User Enum and Password Sprays

- User enumeration reduces time per spray – HUGE
  - reduce attempts from 4,200,000 -> 2,000 or less
- User enumeration reduces noise generated – avoid Smart Lockout

- http://weakpasswords.net
  - 100~ common passwords based on last 90 days, updated daily

- Most large organizations will have at least one weak password in AD
- Assume at least one weak password exists, hunt for the associated username

[username] + [password] = [valid login]

[?] + [known within 100] = [valid login]

Why Azure Enumeration Matters

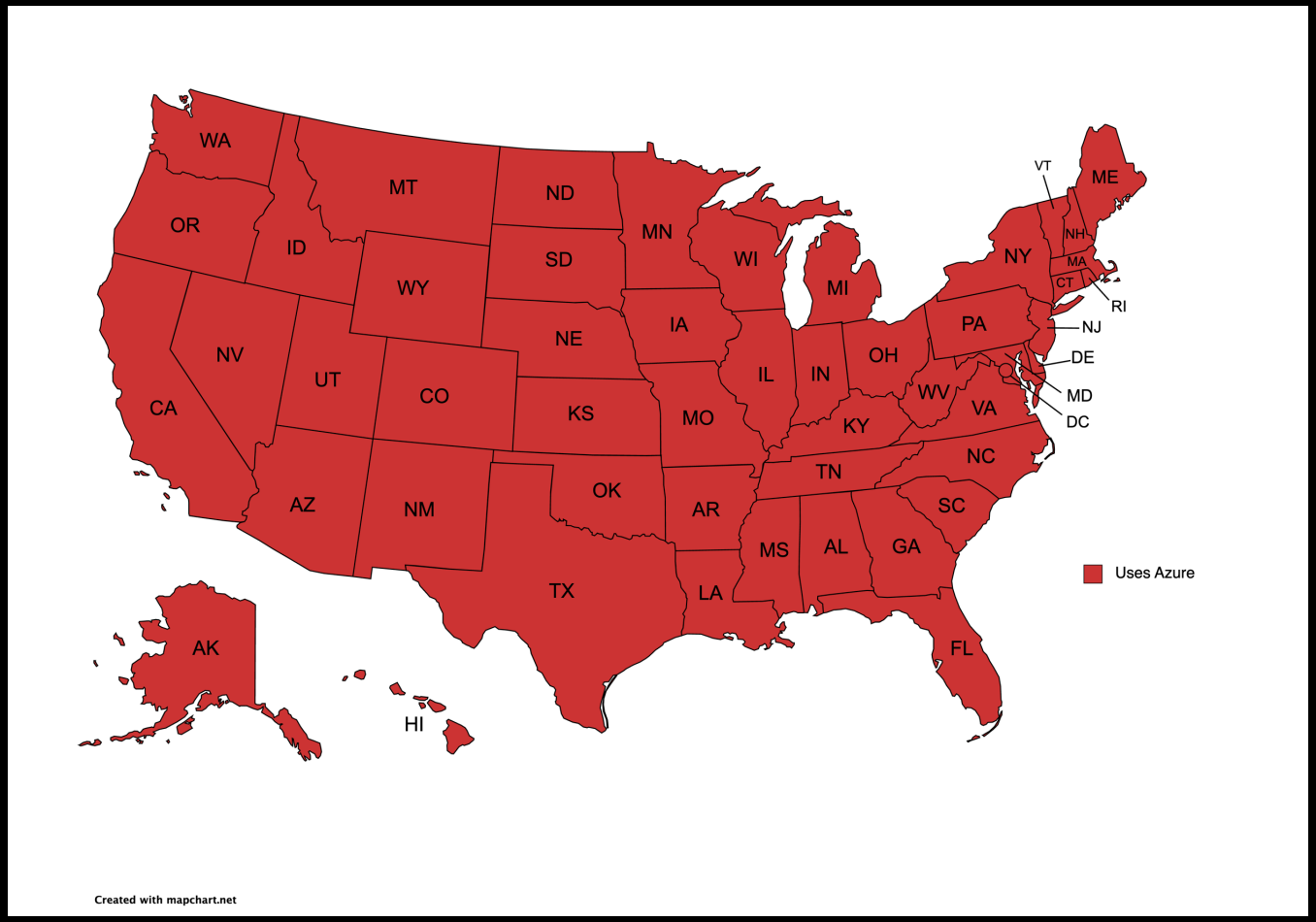
- Fortune 500 Adoption Rate
  - 496 / 500 had Azure tenants (99.2%)
  - 482 / 500 had SharePoint enabled (96.4%)
  - 445 / 500 had usernames identified (89%)

Total Employees - Fortune 500
32.5m~

- Fortune 1000 Adoption Rate
  - 997 / 1000 had Azure tenants (99.7%)
  - 966 / 1000 had SharePoint enabled (96.6%)
  - 806 / 1000 had usernames identified (80.6%)

Total Employees - Fortune 1000
35.5m~

Azure Adoption in State Governments



Azure and OneDrive Adoption in FedGov



Who might not want to be enumerated?

- Any of those agencies in the previous slide?
- Single Issue Groups
- Law Enforcement
- K-12
- Political Organizations

OWASP, MITRE, and User Enumeration

- Both OWASP and MITRE Consider User Enumeration to be a weakness



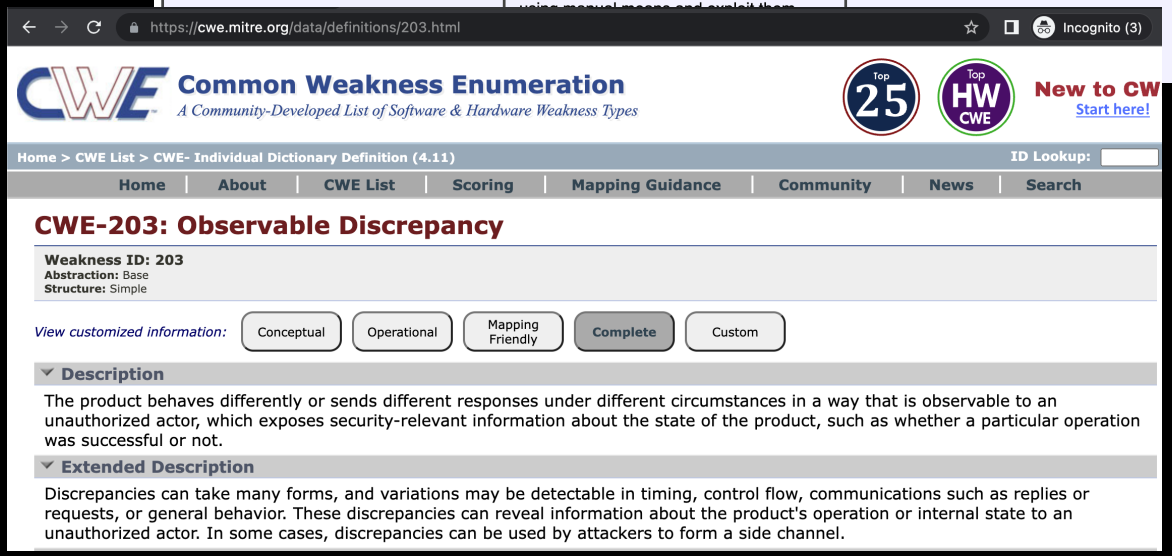
OWASP Top Ten 2017

A2:2017-Broken Authentication

Languages: [en] de

← A1:2017-Injection | OWASP Top Ten 2017 PDF version | A3:2017-Sensitive Data Exposure →

Threat Agents / Attack Vectors		Security Weakness		Impacts	
App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 2	Technical: 3	Business ?
Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Session management attacks are well understood, particularly in relation to unexpired session tokens.		The prevalence of broken authentication is widespread due to the design and implementation of most identity and access controls. Session management is the bedrock of authentication and access controls, and is present in all stateful applications. Attackers can detect broken authentication		Attackers have to gain access to only a few accounts, or just one admin account to compromise the system. Depending on the domain of the application, this may allow money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.	



https://cwe.mitre.org/data/definitions/203.html

Incognito (3)

Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Top 25 | Top HW CWE | New to CW Start here!

Home > CWE List > CWE- Individual Dictionary Definition (4.11) ID Lookup:

Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

CWE-203: Observable Discrepancy

Weakness ID: 203
Abstraction: Base
Structure: Simple

View customized information: Conceptual | Operational | Mapping Friendly | Complete | Custom

Description

The product behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

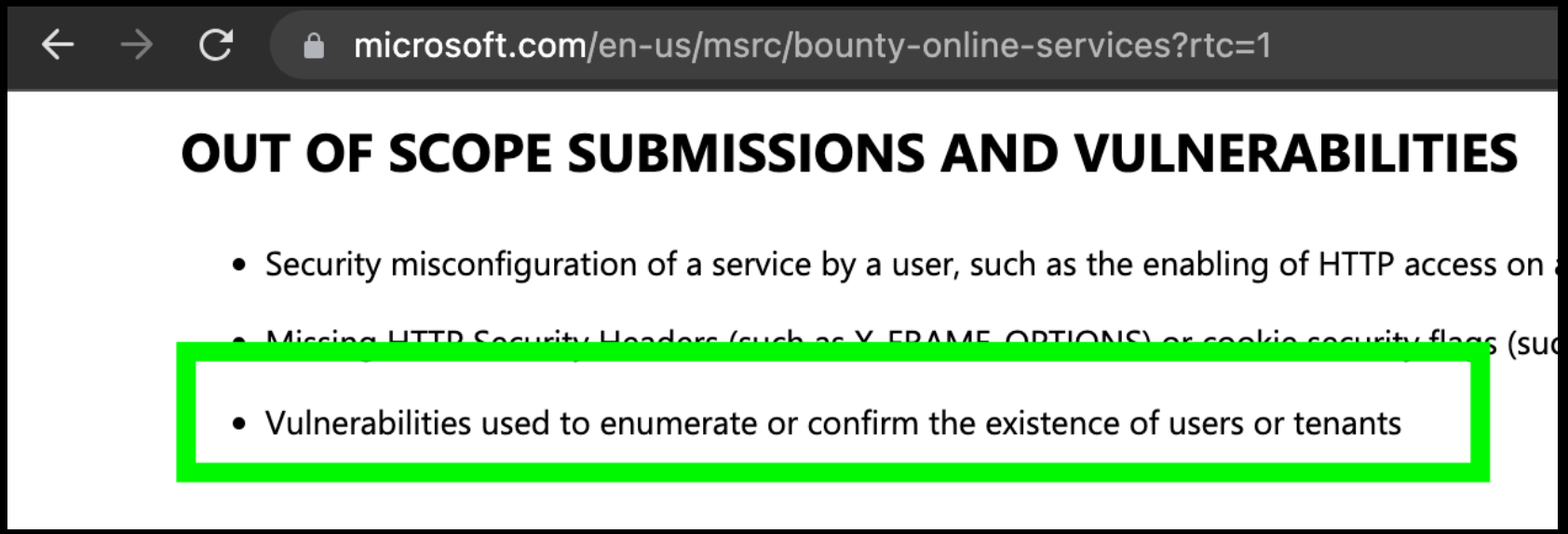
Extended Description

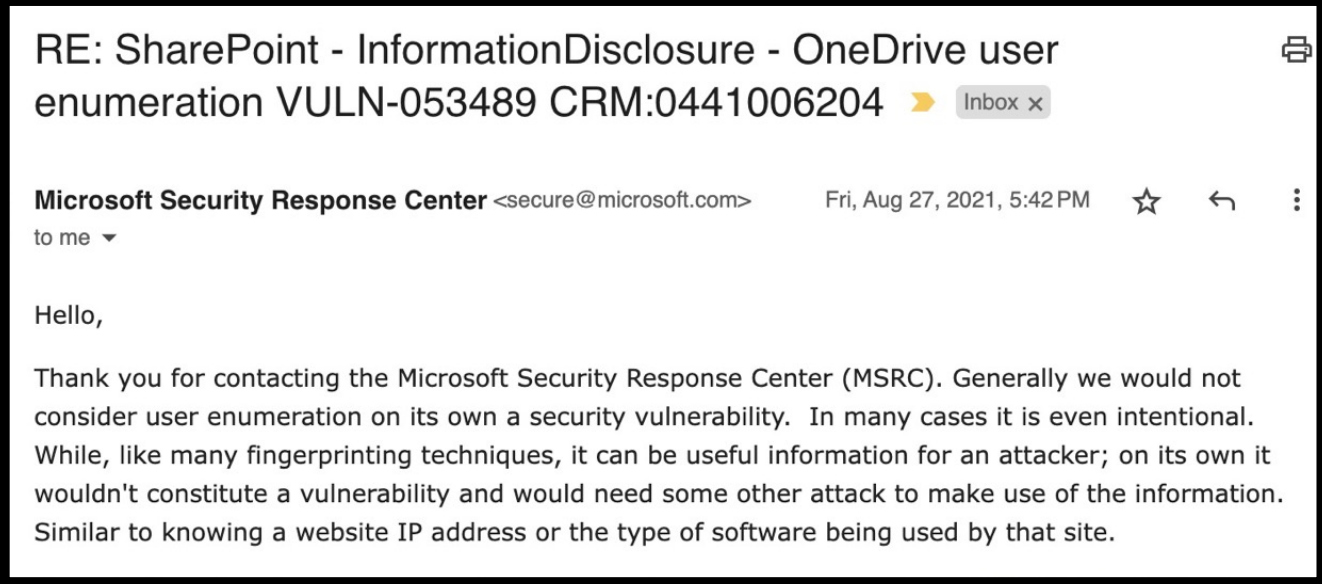
Discrepancies can take many forms, and variations may be detectable in timing, control flow, communications such as replies or requests, or general behavior. These discrepancies can reveal information about the product's operation or internal state to an unauthorized actor. In some cases, discrepancies can be used by attackers to form a side channel.

A Brief History of User Enumeration in Microsoft Products

- 2014 Exchange time-based enumeration - foofus.net
- 2016 Lync time-based enumeration - nyxgeek
- 2016 Skype for Business PowerSkype - kfosaaen
- 2017 O365 ActiveSync Enum - office365userenum
- 2019 OneDrive Enum - nyxgeek
- 2019 Azure AD SSO - DrAzureAD
- 2020 Graph User Enum - MSOLSpray
- 2021 TeamFiltration - flangvik

Microsoft's Stance on User Enumeration





RE: SharePoint - InformationDisclosure - OneDrive user enumeration VULN-053489 CRM:0441006204

Inbox ×

Microsoft Security Response Center <secure@microsoft.com> Fri, Aug 27, 2021, 5:42 PM

to me

Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). Generally we would not consider user enumeration on its own a security vulnerability. In many cases it is even intentional. While, like many fingerprinting techniques, it can be useful information for an attacker; on its own it wouldn't constitute a vulnerability and would need some other attack to make use of the information. Similar to knowing a website IP address or the type of software being used by that site.

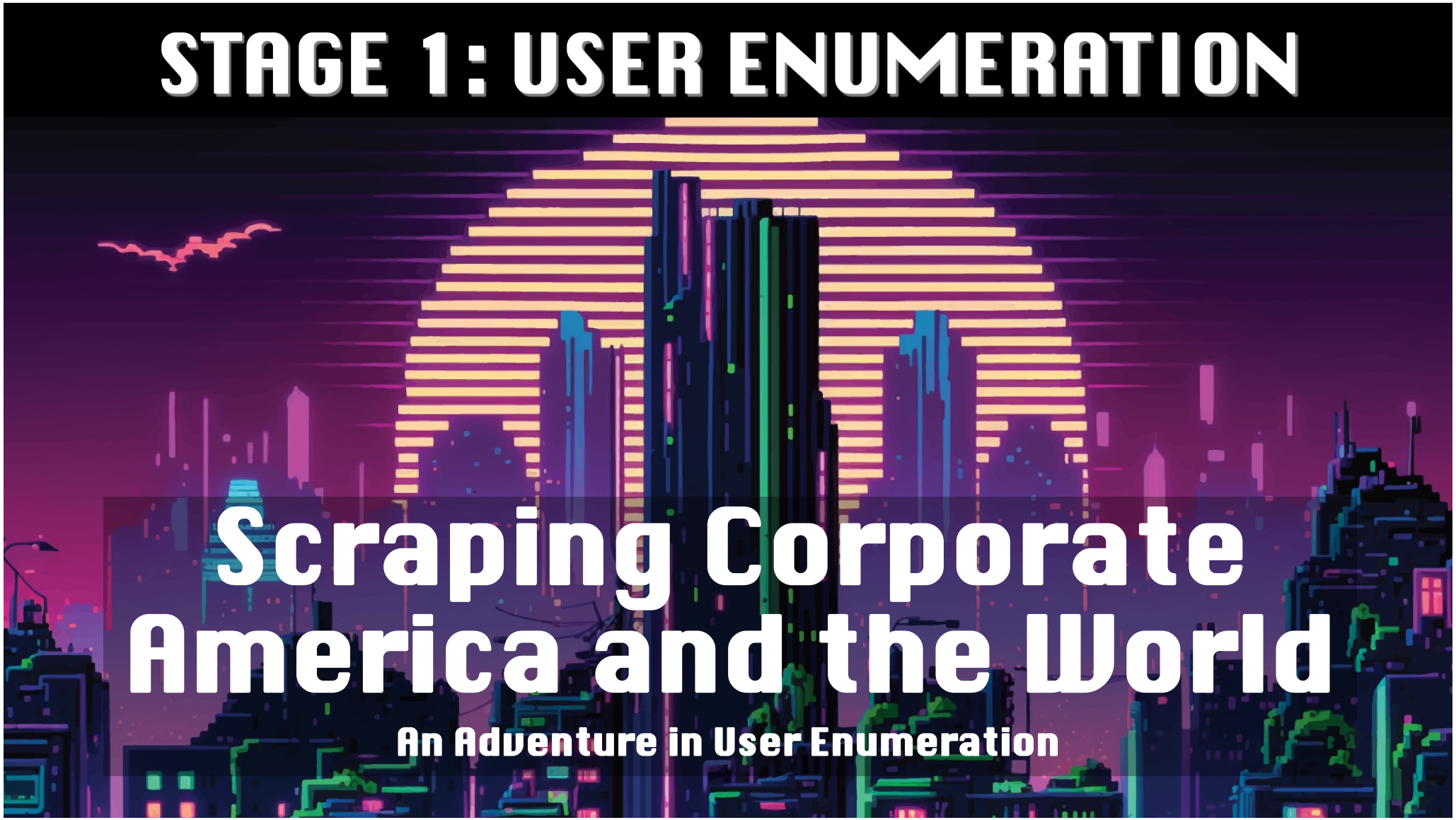
… we would not consider user enumeration on its own a security vulnerability. In many cases it is even intentional. …

… on its own it wouldn't constitute a vulnerability and would need some other attack to make use of the information.

Similar to knowing a website IP address …


IT'S NOT A BUG
IT'S A FEATURE

STAGE 1: USER ENUMERATION



Scraping Corporate America and the World

An Adventure in User Enumeration

A project is born

- Realization – OneDrive user enumeration is a simple HTTP request to Microsoft servers
- No authentication attempts
- This is web scraping

- 404 = Invalid Username
- 403/401 = Valid Username

```
root@TRON1:~# curl --head https://microsoft-my.sharepoint.com/personal/john_microsoft_com/_
HTTP/2 404
cache-control: private
content-length: 18
content-type: text/plain; charset=utf-8
```

Azure Enumeration Methods

- Microsoft Graph Authentication
  - Logon-based (error code from logon attempt)
  - Most accurate
  - Shows up in logs
- Seamless SSO/O365 Logon Page
  - Checks "IfExistsResult:0" or in "IfExistsResult:1" HTTP response
  - False positives by 100,000~ attempts
- Teams Presence
  - Silent enumeration (HTTP POST request), IF External Access is enabled (default)
  - No logs
  - Better coverage than OneDrive
- OneDrive
  - Silent enumeration (HTTP HEAD request), no login attempt
  - No logs
  - Requires user to have logged in once to Office product in order to enumerate

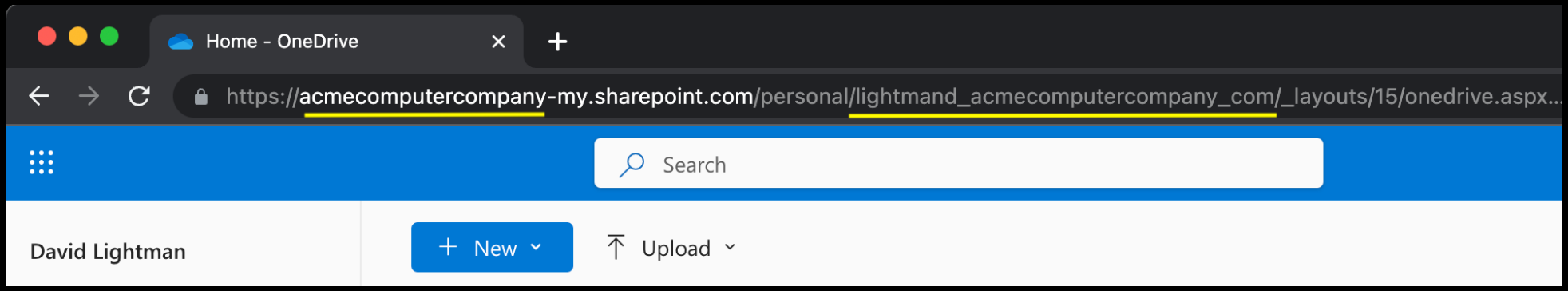
Why OneDrive?

- No rate limits
- No false positives
- Stupid simple (HTTP HEAD or GET request)
- No account or license required to test (no Terms of Service)
- No logon attempt

- Downsides
  - Not all Azure tenants use OneDrive
  - Sometimes significantly less coverage than logon-based enumeration
  - Azure Recycling Bin
  - No differentiation between "john.smith" and "john_smith" formats

OneDrive Enum Requirements

- Domain Name
  - Easy
- Tenant Name
  - Not always predictable
  - Tenants can sometimes mirror domain, but often not



AADInternals to the Rescue!

- Discovered AADInternals tenant lookup by way of TREVORspray

- https://github.com/Gerenios/AADInternals
- https://github.com/blacklanternsecurity/TREVORspray

```
[INFO] Retrieving tenant domains at https://autodiscover-s.outlook.com/autodiscover/autodiscover.svc
[SUCC] Found tenant names: "microsoft, MicrosoftAPC, msfts2, microsoftcan, microsoftprd, microsoft, msf
[SUCC] Found 282 domains under tenant!
[SUCC]
[
    "azmosa.io",
    "educatorcommunity.microsoft.com",
    "africa.corp.microsoft.com",
    "eventscommunication.microsoft.com",
    "m12.vc",
    "winfarmmail.ntdev.corp.microsoft.com",
    "codenauts.de",
    "incentgames.com",
    "start.gg",
```

OneDrive Enumeration in Action



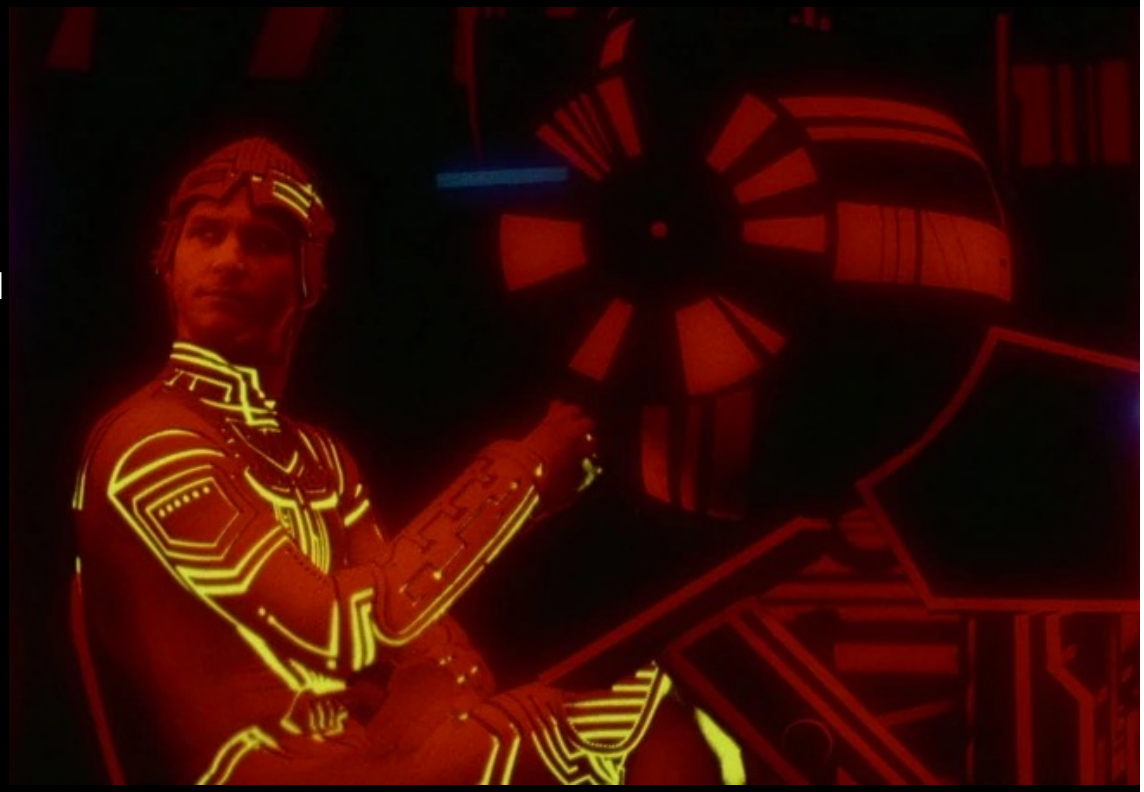
Infrastructure Overview

Client (CLU)

Cloud **L**ookup **U**tility

- Performs actual scraping, sends back to mysql db named TRON
- TRON has a /home/wordlists user
- Sync this home folder from TRON to the client
- Base image for client is replicated via a snapshot in VPS

TRON		CLU
/home/wordlists/DOMAINS	→	/root/DOMAINS
/home/wordlists/USERNAMES	→	/root/USERNAMES



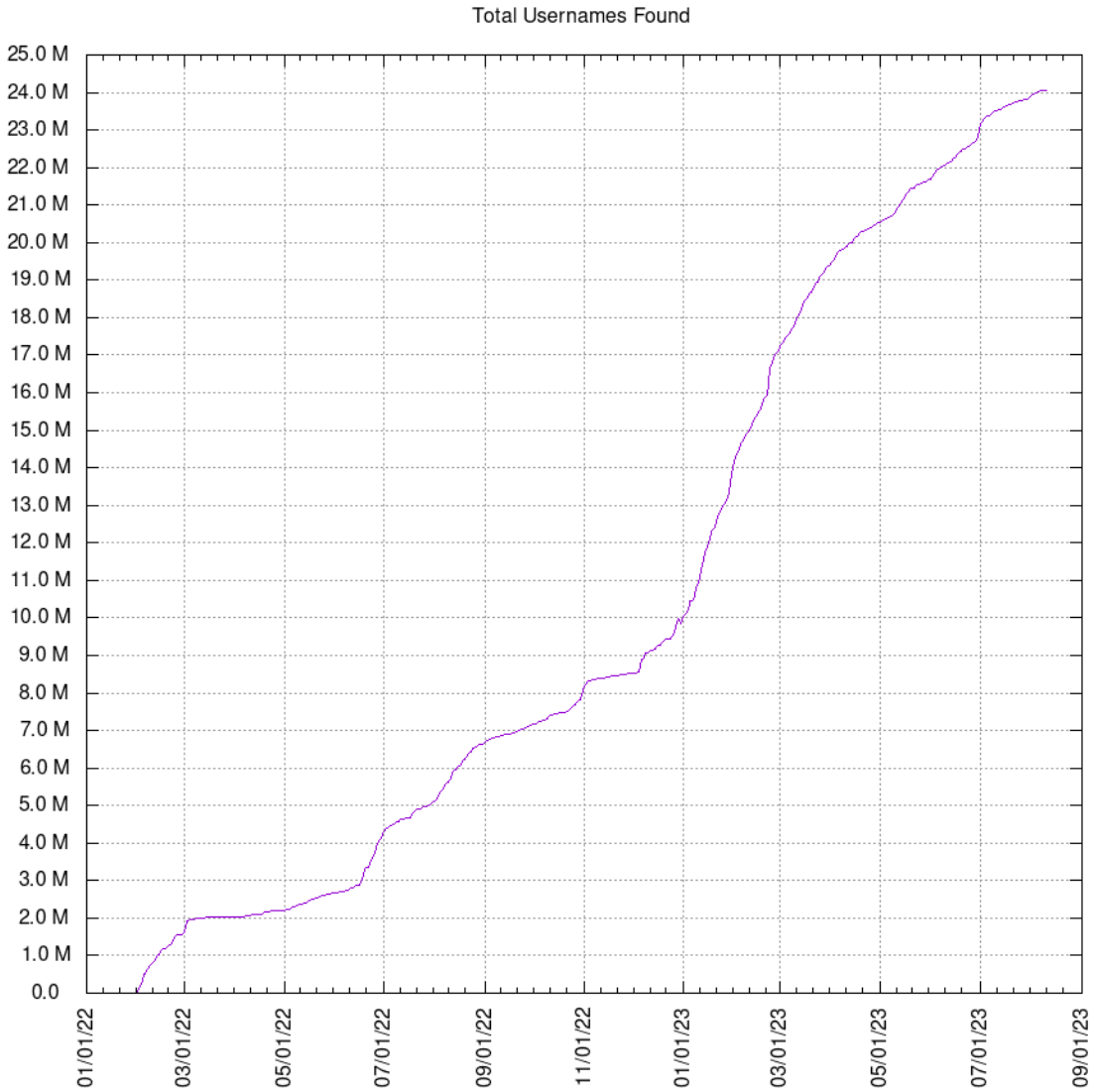
THE ORIGINAL CLU CREW



THE CLU CORP (40 HOSTS - STANDARD)



24 Million Usernames



20 million – for comparison

- NYC – 9 million people
- New York State – 20 million people

- Florida – 21 million people

- Australia – 25 million people

- Fortune 500 – 32 million people



user enumeration: analysis

analysis of the data from our azure census/survey

Overall Username Stats

- Total usernames: 24,041,389
  - Non-numeric: 21,501,038
- Unique usernames: 10,305,703
  - Non-numeric: 8,323,471
- Timeframe of Enumeration: 556 days
- Average Rate of Enumeration: 43,329 / day

Identifying Username Formats

- Run an exploratory 'survey' list against domain
- List contains equal number of top usernames in each format – no overlap
    - 175 john.smith
    - 175 johnsmith
    - 175 jsmith
    - 175 j.smith
    - 175 smith.john
    - 175 smithjohn
    - 175 smithj
    - 175 smith.j
    - 175 johns
    - 175 john.s
    - 175 jjsmith
    - 175 firstname
    - 175 lastname

```
root@TRON1:~/survey_tool# ./run_survey.sh microsoft
104:jsmith
92:johnsmith
65:smithjohn
54:firstname
35:smithj
29:jjsmith
27:john.smith
17:lastnames
1:smith.john
1:john.s
1:j.smith
0:smith.j.txt
0:sjohn
0:s.john
0:johns
0:john.j.smith
0:jjs
```

Survey Results: Format Popularity

- Fortune 1000 Companies
- Tried every tenant/domain combination
- 17 username formats
- 175 of each username format run against each
- Not a perfect survey
  - john.j.smith has more variations than jsmith
  - therefore, likely under-represented

userlist_format	sumfound
john.smith	6885
jsmith	3884
sjohn	820
johnsmith	747
john.j.smith	669
firstname	591
johns	544
smithj	539
jjsmith	460
lastnames	426
j.smith	301
jjs	256
smith.john	234
john.s	164
smithjohn	161
s.john	39
smith.j.txt	10

17 rows in set (1.15 sec)

Username popularity – multi-format

- When an organization runs out of "space" for users
- Go up – append digits:
  - jsmith1, jsmith2, etc
- Add a format:
  - jsmith -> jjsmith
  - john.smith -> john.j.smith
- Truncate:
  - smithjohn -> smithjoh, smithjo

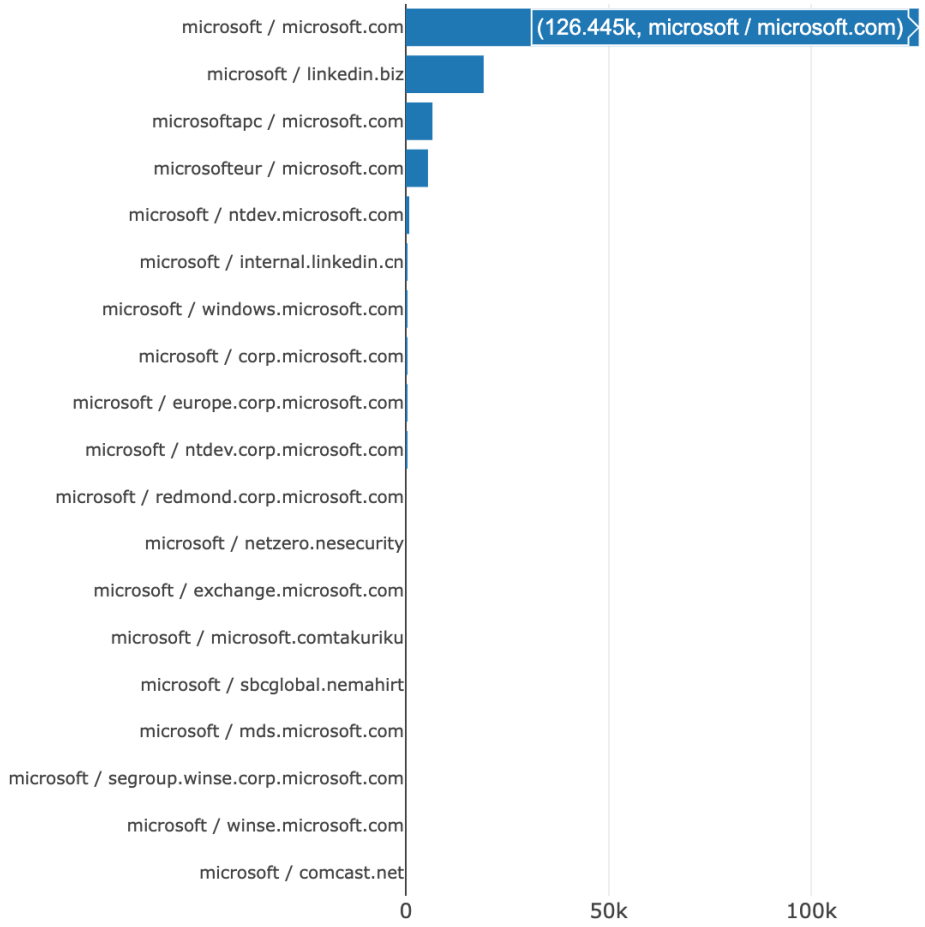
Combinations of Username Formats

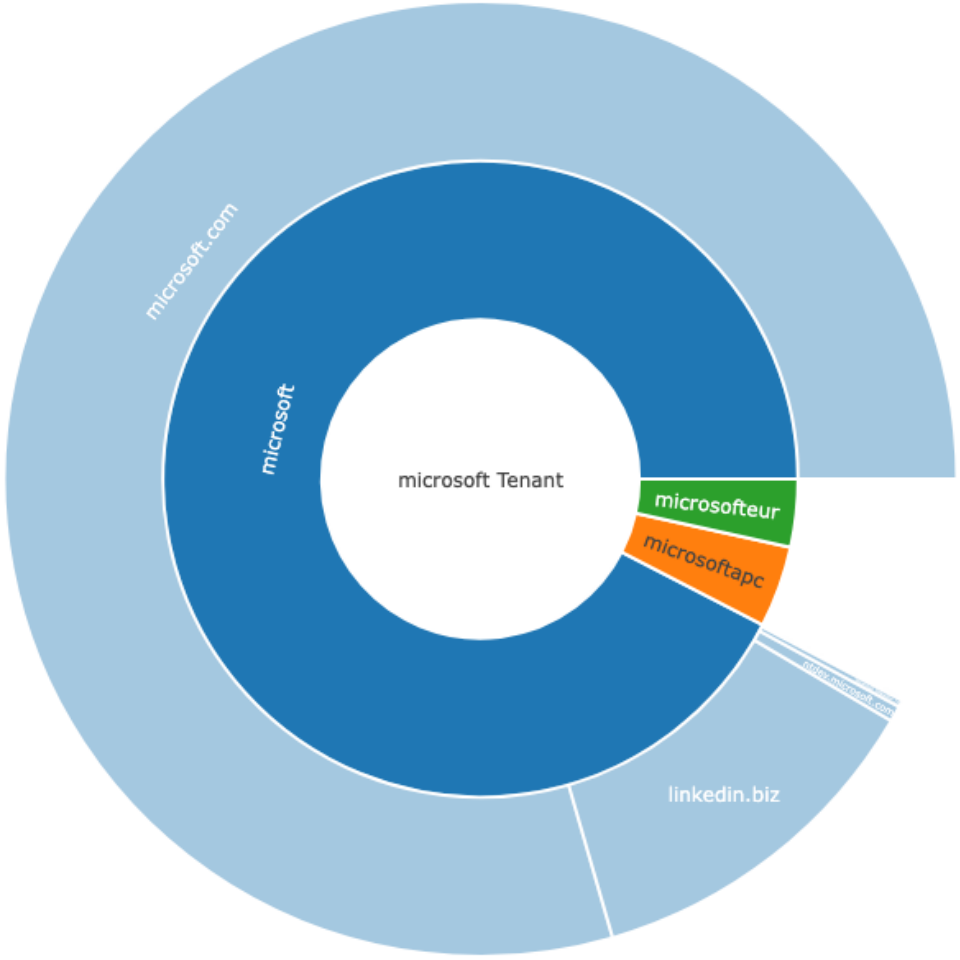
```
22039 jsmith
10414 john.smith
  968 jsmith,john.smith
  540 john.smith,jsmith
  469 firstname
  233 jsmith,sjohn
  113 jsmith,jjsmith
   98 john.smith,john.j.smith
   84 johns
   83 jsmith,sjohn,jjsmith
   70 jsmith,firstname
   70 john.smith,smith.john
   68 jsmith,jjsmith,sjohn
   66 john.smith,j.smith
   63 john.smith,firstname
   52 jjs
   48 johns,firstname
   46 sjohn
   45 johnsmith
   43 firstname,lastnames
   36 lastnames
   36 jsmith,sjohn,firstname
   30 firstname,johns
   28 lastnames,firstname
   28 john.smith,john.s
   28 j.smith
   27 smithj
   27 sjohn,jsmith
   26 jsmith,sjohn,jjsmith,firstname
   22 numeric
   22 firstname,john.smith
   21 john.smith,jjs
   20 john.j.smith
   19 jsmith,sjohn,lastnames
   18 jsmith,jjsmith,sjohn,firstname
   18 jjsmith
   18 firstname,jsmith
   17 smithj,johns
   17 john.smith,johns
   16 jsmith,lastnames
```

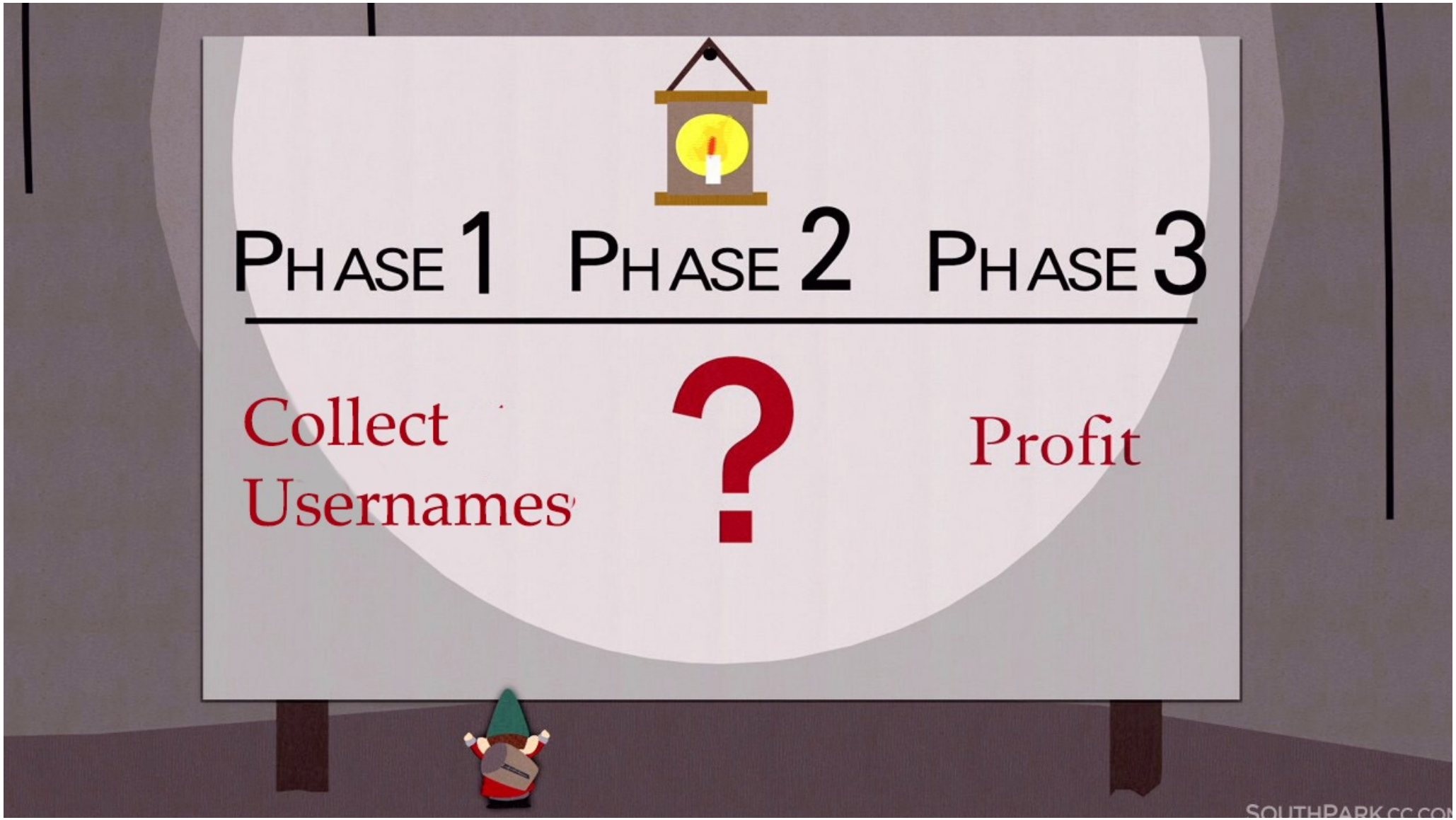
Fortune 1000 Primary Tenant – Top User Counts

	Name	Primary Tenant	Domains	Tenants	Users Enumerated	Estimated Employee Count	Percent Found
2	Lowe's	lowes	2	1	474094	270000	175.59%
3	Cognizant Technology Solutions	cognizantonline	1	4	407345	330600	123.21%
4	Johnson & Johnson	jnj	6	1	345078	141700	243.53%
5	Microsoft	microsoft	19	3	158884	221000	71.89%
6	Tesla	teslamotorsinc	2	1	141889	99290	142.90%
7	Meta Platforms	fb	4	1	137867	71970	191.56%
8	CVS Health	aetnao365	29	1	120947	258000	46.88%
9	FedEx	myfedex	3	1	116725	484000	24.12%
10	AT&T	att	1	1	113738	202600	56.14%
11	Wells Fargo	wellsfargo	7	1	105228	247848	42.46%
12	UnitedHealth Group	uhgazure	27	1	101735	350000	29.07%
13	IBM	ibm	82	1	95739	297800	32.15%
14	UPS	upsazure	1	1	92524	400945	23.08%
15	Delta Air Lines	deltaairlines	5	1	91217	83000	109.90%
16	CBRE Group	cbre	22	1	89823	105000	85.55%
17	U.S. Bancorp	usbank	3	1	86884	68796	126.29%
18	Ford Motor	azureford	1	1	85183	183000	46.55%
19	PepsiCo	pepsico	2	1	82299	309000	26.63%
20	Target	targetonline	1	1	74463	450000	16.55%
21	Dell Technologies	dell	6	1	63711	133000	47.90%
22	Charter Communications	chartercom	2	1	61415	93700	65.54%
23	State Street	statestreet	8	1	56273	38784	145.09%
25	Morgan Stanley	morganstanley	1	7	54983	74814	73.49%
26	Walt Disney	twdc	12	1	53079	171000	31.04%
27	Abbott Laboratories	abbott	2	1	51621	113000	45.68%
28	Humana	inspirewellness	7	1	51424	95500	53.85%
29	Southwest Airlines	wnco	1	1	50833	55093	92.27%
30	Honeywell International	honeywellprod	13	1	49407	99000	49.91%
31	Jones Financial (Edward Jones)	ejprod	1	1	47376	50000	94.75%

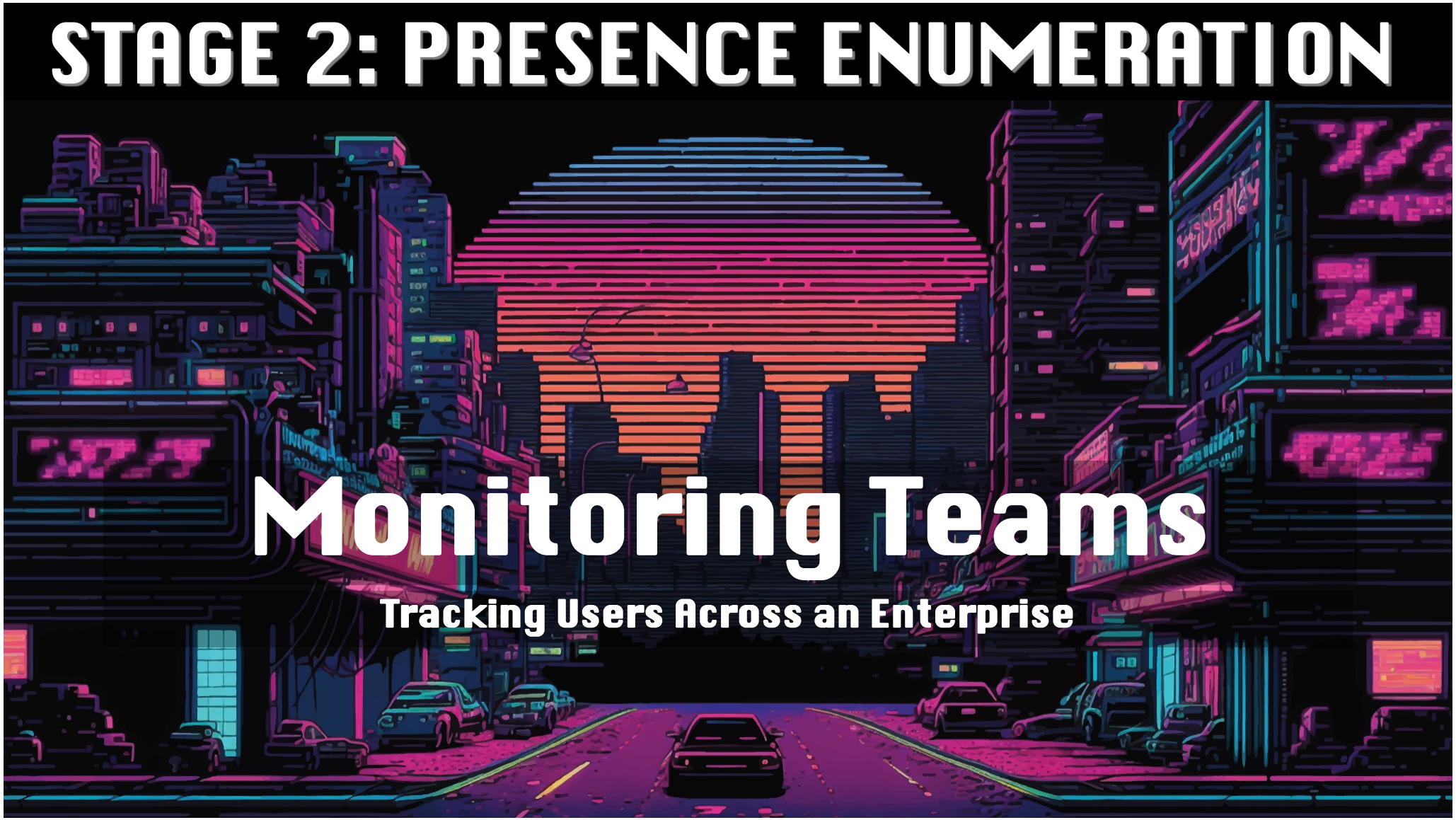
Exploring Tenant and Domain Relationships






PHASE 1 PHASE 2 PHASE 3
Collect Usernames
?
Profit
SOUTHPARK.CC.COM

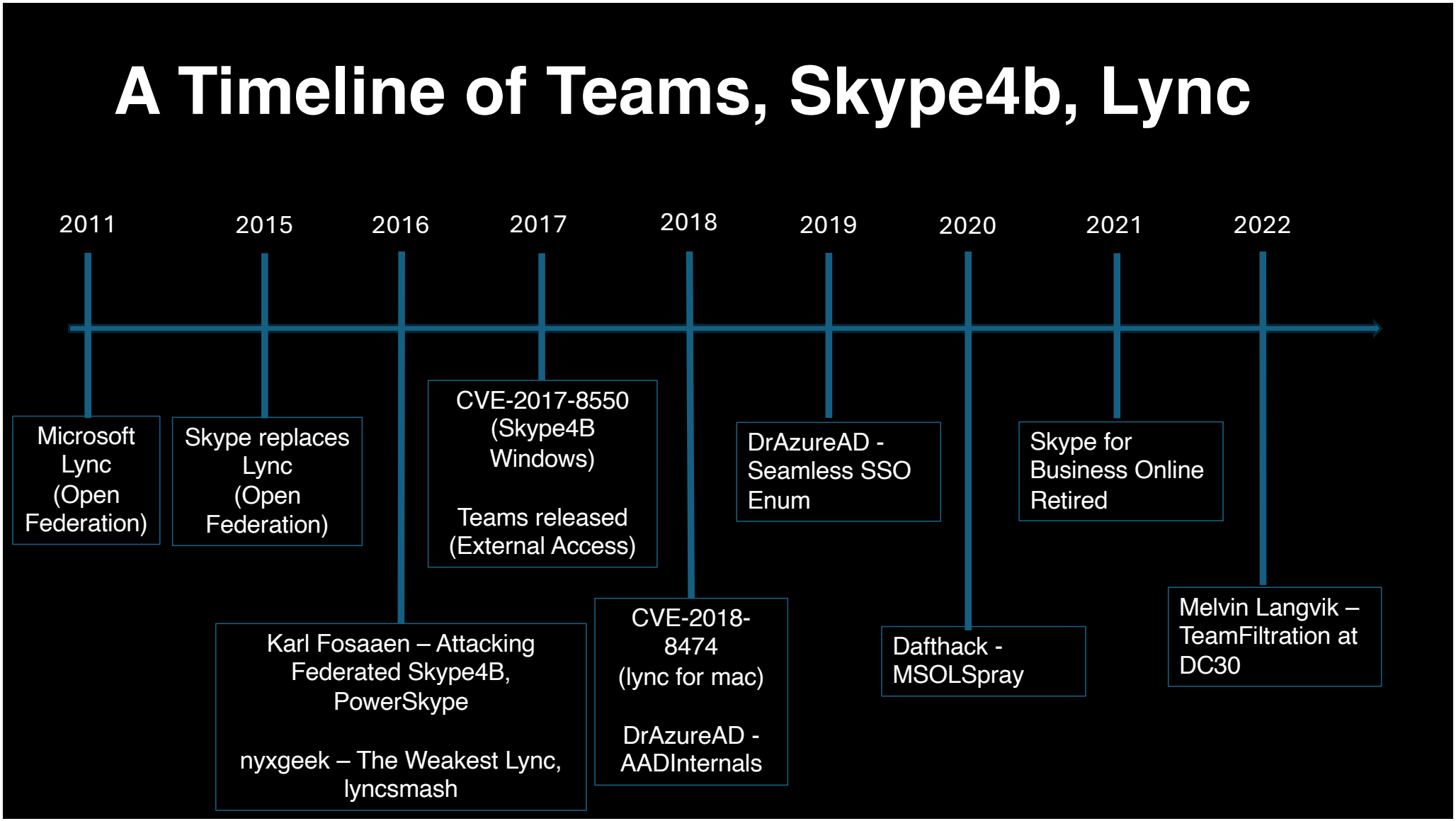
STAGE 2: PRESENCE ENUMERATION



Monitoring Teams

Tracking Users Across an Enterprise

A Timeline of Teams, Skype4b, Lync



TLP: RED - DO NOT SHARE, NOT FOR RELEASE

Skype for Creepers

These companies have Microsoft Federation enabled, allowing the world to see their users' full name, online status, title, and more. All information below, with exception of the 'Company' field, has been retrieved via Skype for Business using PowerShell and the Lync 2013 SDK.

To learn more about this project, click here. For instructions on disabling open federation, click here.

Status	Title	Full Name	Company
Offline		[redacted]	20th Century Fox
Offline	Chief Executive Officer		Accuweather
Offline	Responsable		Air France
Offline	Office of the Chairman		Air Procucts and Chemicals Inc
Offline	President and CEO		AMD
Away	Chairman, President and CEO		AmerisourceBergen
Away	Chairman of the Board, President & CEO		Amgen Inc
Offline	VP, FINANCE & SOLUTIONS		Anheuser-Busch
Offline	EVP & Chief Financial Officer		Aramark Corp
Offline			ArcelorMittal
Offline	Chief Executive, AstraZeneca		AstraZeneca
Offline			ASUS
Offline	CEO		Avon
Offline			Barcelo
Offline			Barneys
Away	EVP & Chief Technology Officer		Bentley
Offline	CEO		Best Buy
Offline	Chairman		BiC Pens
Offline	CEO & President		Big Lots
Offline	Chairman, CEO & President		BlackBoard
Offline	Chairman, CEO		Bloomingdales
Offline	Chief Executive Officer		British Telecom (BT)
Offline	PDG		Capgemini

Skype for Creepers 2017

Offline	President & Chief Executive Officer	[redacted]	Novo Nordisk A/S
Away	GM-GM-General Manager EMT member		NXP Semiconductors
Offline			NYC Dept of Education
Offline	President & Chief Operating Officer		Papa John's Pizza
Away	Chief Executive Officer		Polycom
Away	Chief Executive Officer		Puma
Offline	Chief Executive Officer		QualComm
Offline	Evp Store Operations		RiteAid
Offline	Dr.		Roche Holding AG
Offline	President and CEO		Sandvik
Offline			SAP SE
Offline			Scania AB
Away	CFO		Sears
Offline	Chairman and Chief Executive Officer		SLB
Offline	DIRECTEUR GENERAL DU GROUPE		Sodexo
Busy	PRESIDENT & CEO		Sprint
Offline	CEO		Staples
Away	EVP CFO		Statoil ASA
Offline	President & CEO		Sutter Health
Offline	Senior Vice President and Chief Information Officer		ThermoFisher Scientific
Offline			Trump Organization
Offline			Trump Organization
Offline			Tupperware
Away	Executive Director		UNICEF
Offline	Chief Executive Officer		Unilever
Away			Unisys Corp
Offline	President & CEO		United Airlines
Offline	Chairman, President & CEO		VF Corporation
Offline	EVP & Chief Financial Officer		Viacom
Offline	President Volvo Group and CEO		Volvo
Offline			Warner Bros
Offline	GVP & Chief Info Officer		Whole Foods

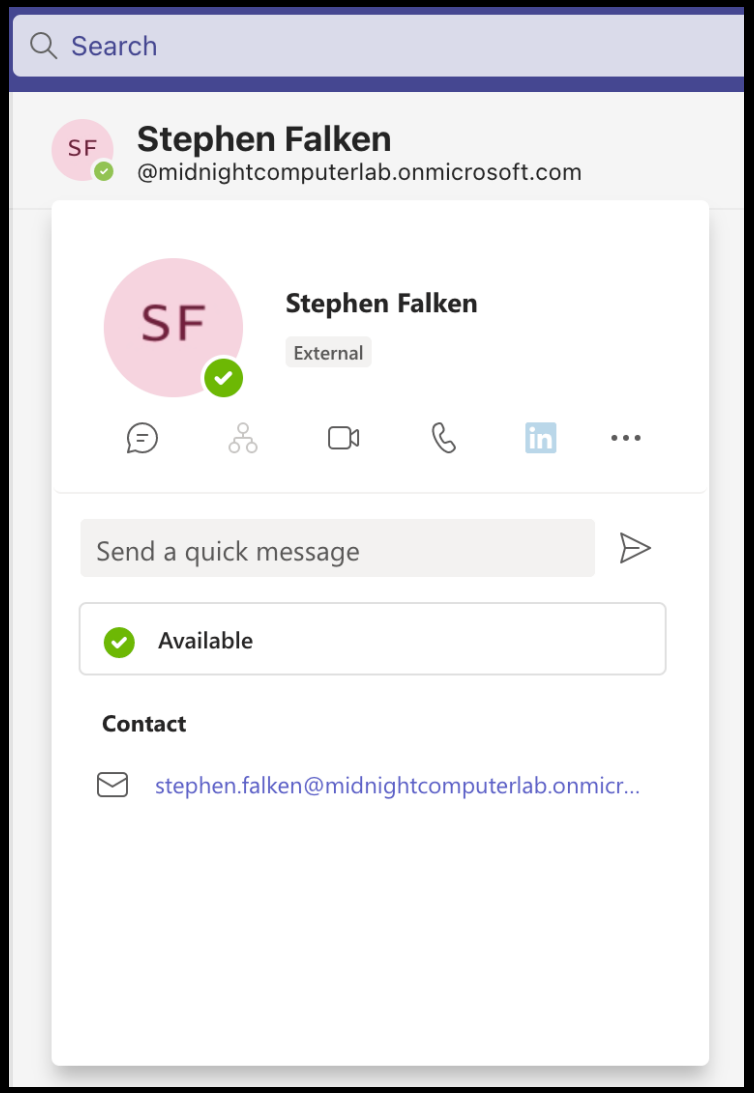
Total Users Online: 22 of 125 - Last query completed at 12/18/2017 05:05:39 UTC

Available: 0 Busy: 1 Away: 21 Other: 0 Offline: 84

External Access in Teams

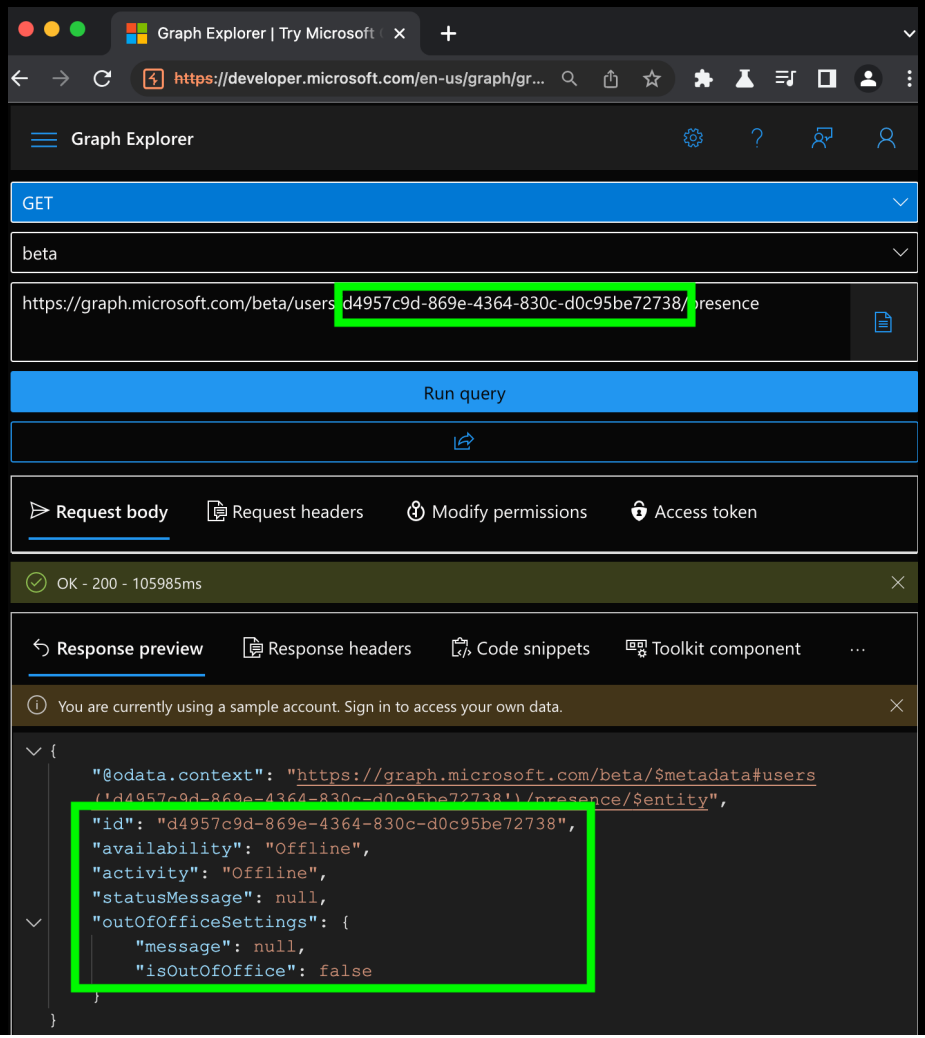
- Default setting for External Access allows any Teams user to communicate, see presence

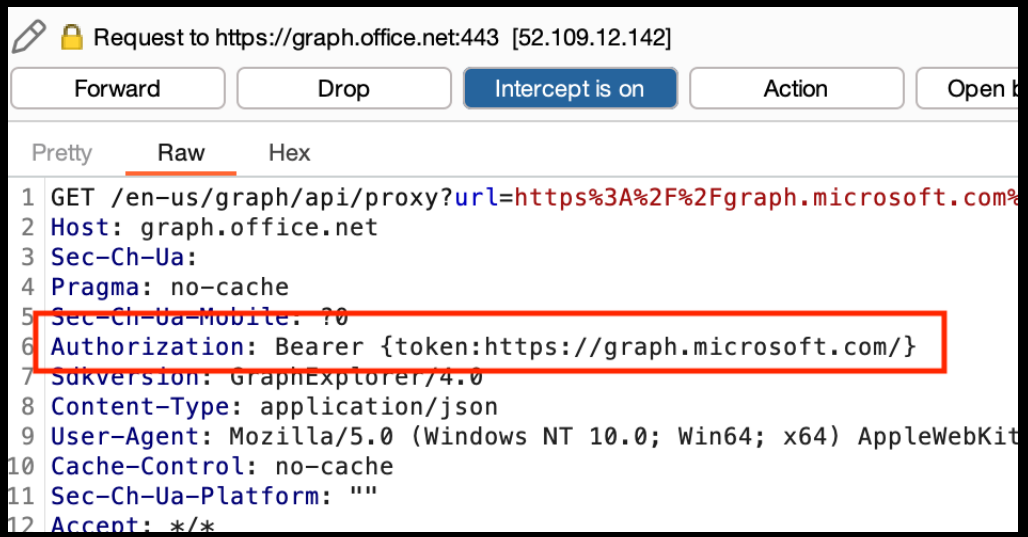
- Previously known as Open Federation with Lync and Skype for Business



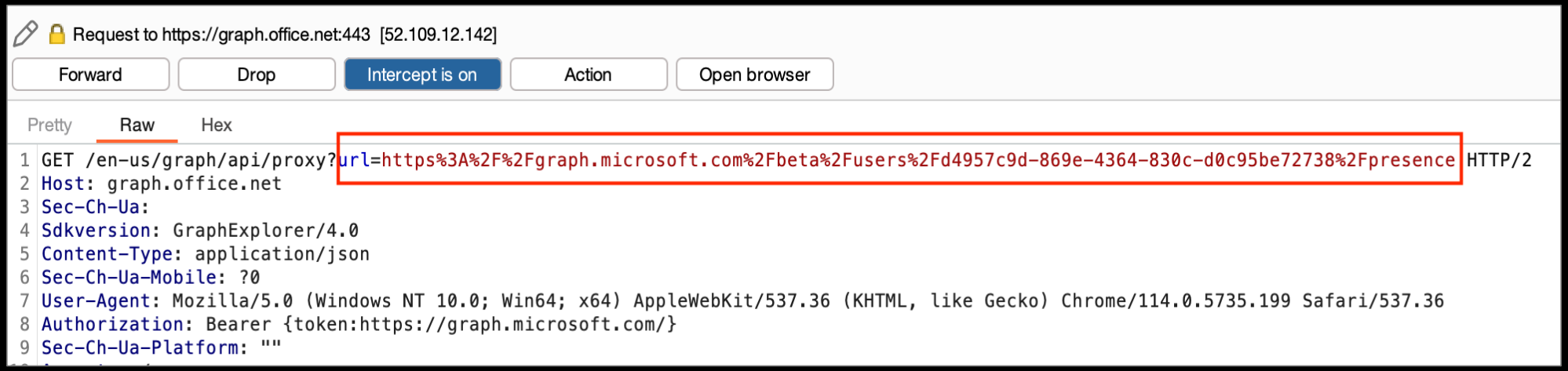

IT'S NOT A BUG
IT'S A FEATURE!
imgflip.com

Presence Lookup via Graph Explorer



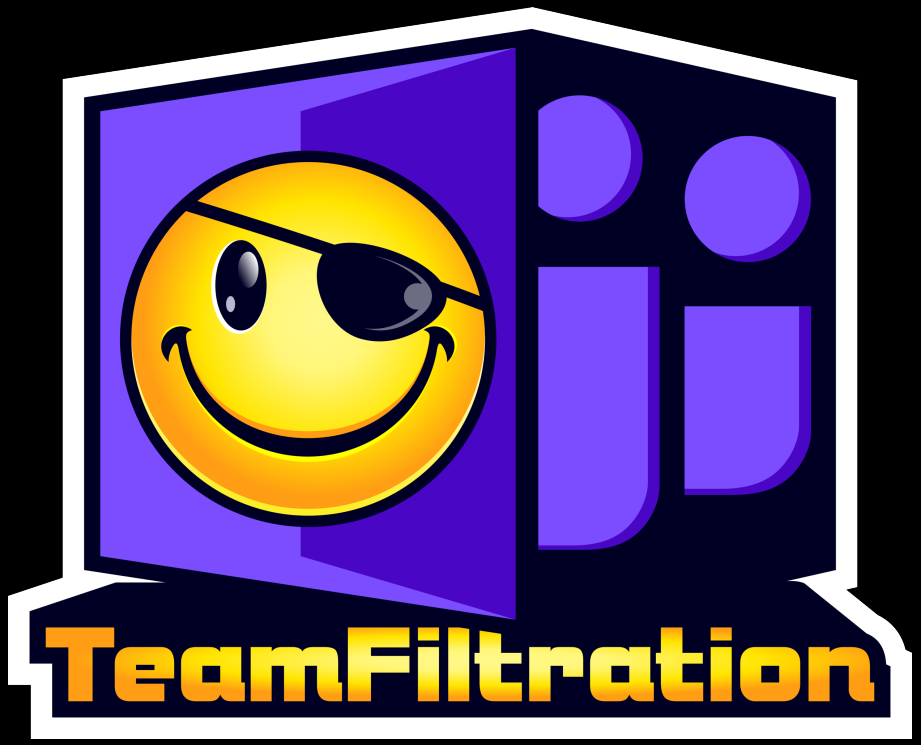


Presence Lookup via Graph Explorer



TeamFiltration

- Released at DefCon 30 by @flangvik
- Enumerate Users via Teams External Access
- Stores Teams GUID, name, ooo in local DB
- Additional spraying,exfil features as well.



https://github.com/Flangvik/TeamFiltration

teamstracker

- PoC utilizing the unauthenticated Graph proxy method
- Requires GUIDs
  - Read from file
  - Import directly from TeamFiltration database
- Checks Status
- Grabs OOO messages, if any

- https://github.com/nyxgeek/teamstracker

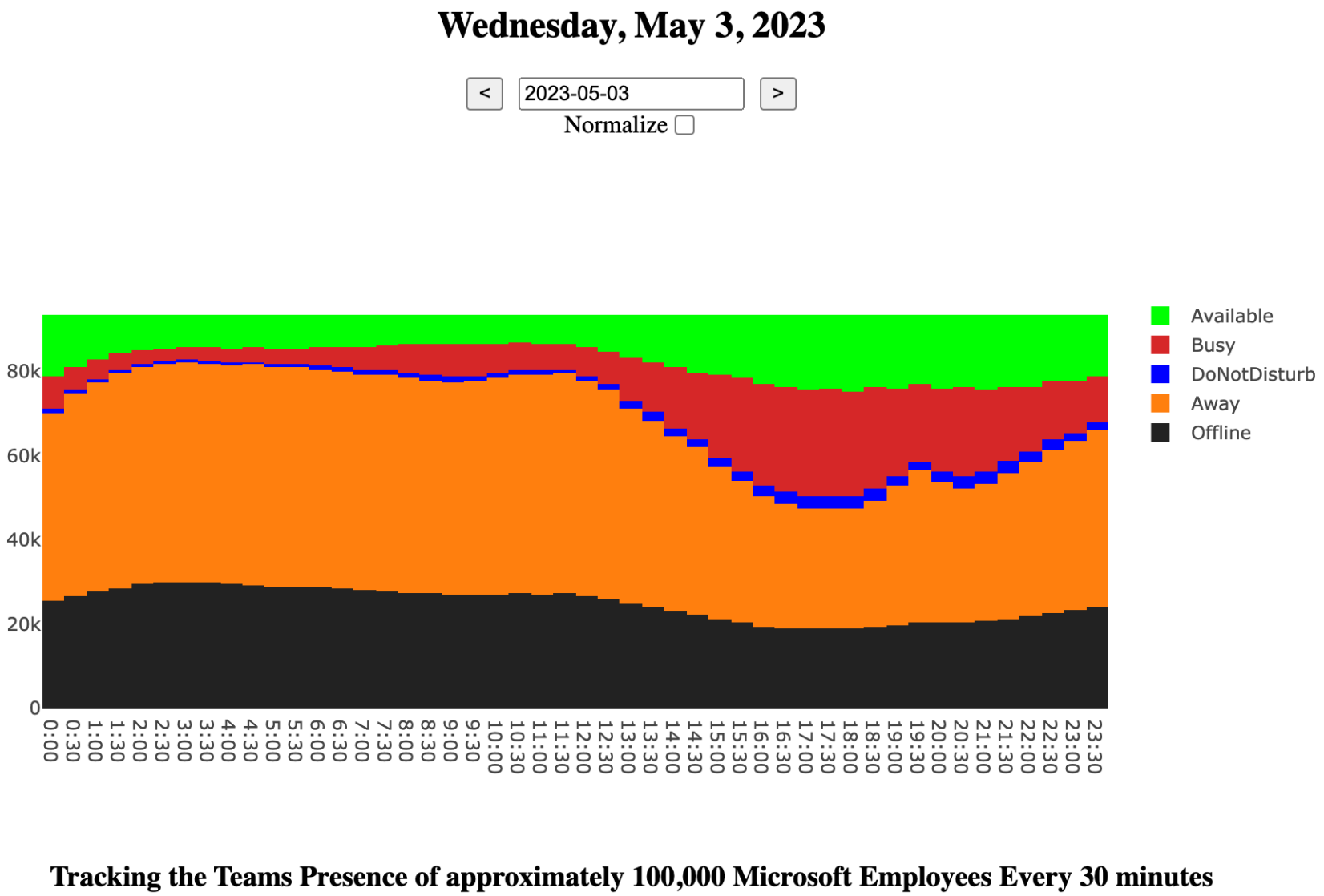


TRACKING A COMPANY

- Who better to demonstrate with, than Microsoft?
- 140,000~ usernames enumerated via OneDrive
- Approximately 100,000 were current users, with Teams licenses

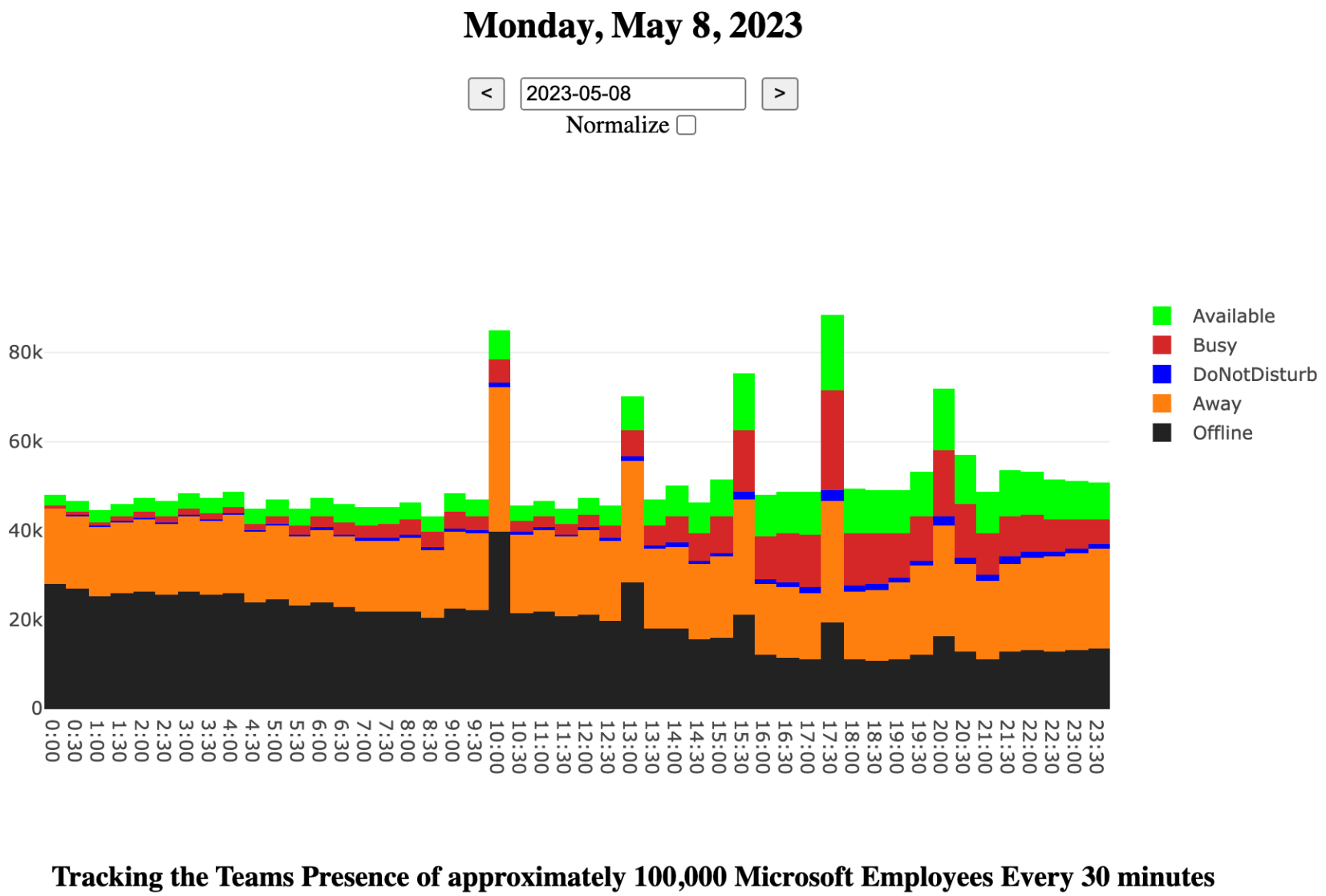
- Monitoring began April 28, 2023

Initial Scans



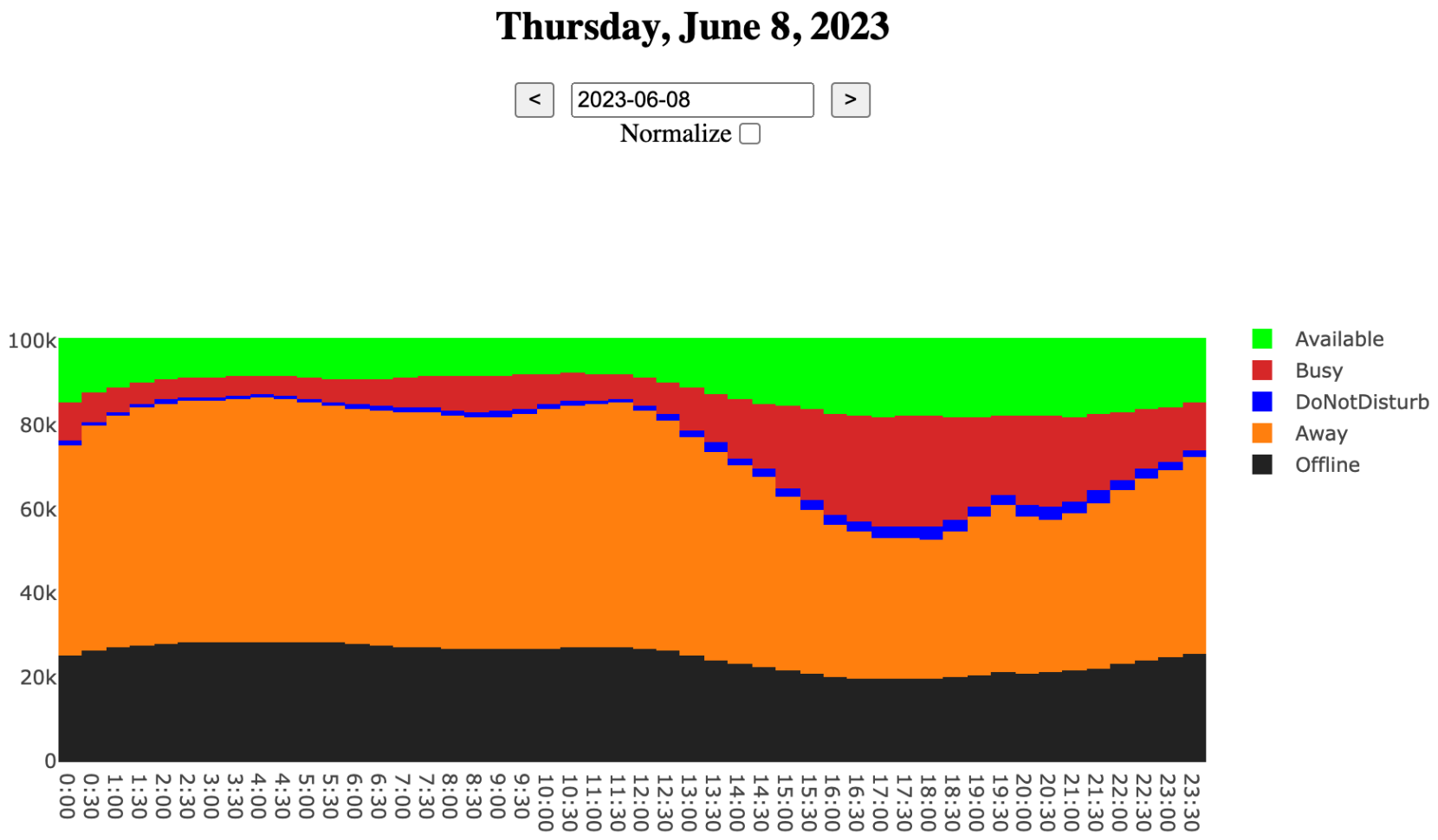
Tracking the Teams Presence of approximately 100,000 Microsoft Employees Every 30 minutes

One week later…



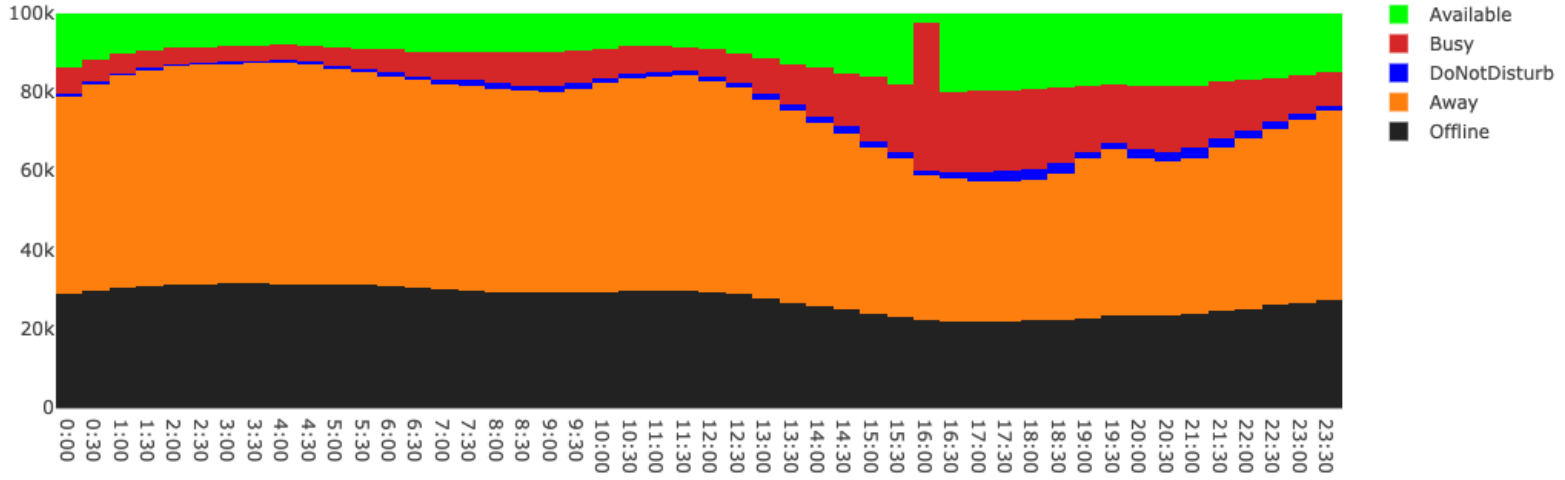
Tracking the Teams Presence of approximately 100,000 Microsoft Employees Every 30 minutes

One Month Later

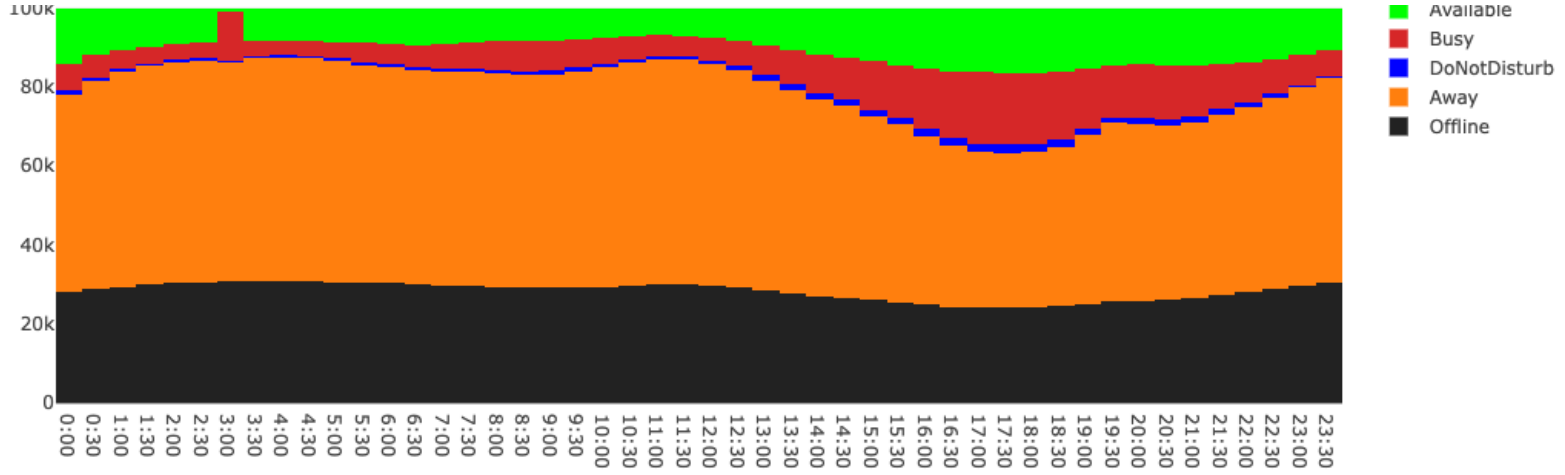


Tracking the Teams Presence of approximately 100,000 Microsoft Employees Every 30 minutes

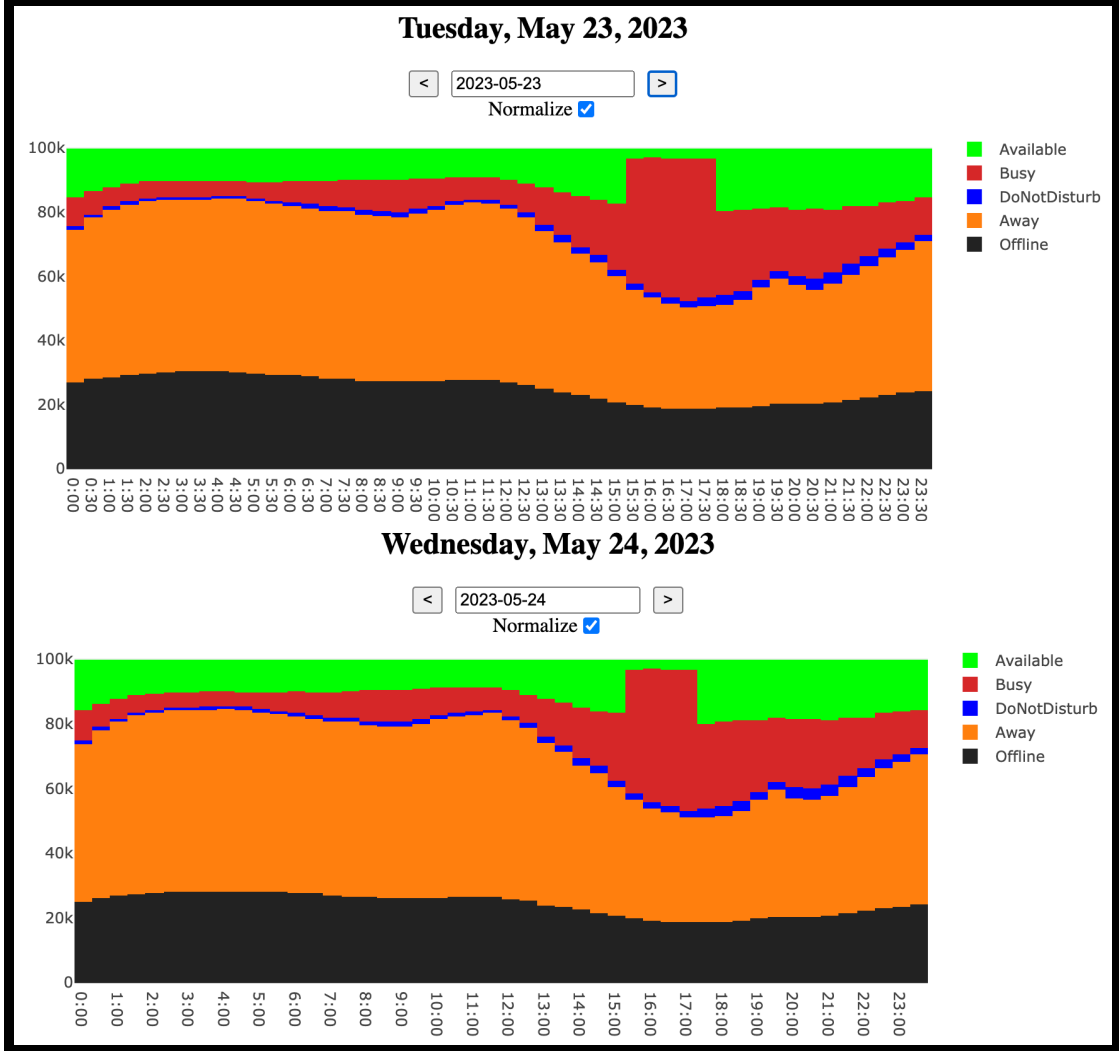
July 6


100k
80k
60k
40k
20k
0
0:00 0:30 1:00 1:30 2:00 2:30 3:00 3:30 4:00 4:30 5:00 5:30 6:00 6:30 7:00 7:30 8:00 8:30 9:00 9:30 10:00 10:30 11:00 11:30 12:00 12:30 13:00 13:30 14:00 14:30 15:00 15:30 16:00 16:30 17:00 17:30 18:00 18:30 19:00 19:30 20:00 20:30 21:00 21:30 22:00 22:30 23:00 23:30
Available
Busy
DoNotDisturb
Away
Offline

July 7


100k
80k
60k
40k
20k
0
0:00 0:30 1:00 1:30 2:00 2:30 3:00 3:30 4:00 4:30 5:00 5:30 6:00 6:30 7:00 7:30 8:00 8:30 9:00 9:30 10:00 10:30 11:00 11:30 12:00 12:30 13:00 13:30 14:00 14:30 15:00 15:30 16:00 16:30 17:00 17:30 18:00 18:30 19:00 19:30 20:00 20:30 21:00 21:30 22:00 22:30 23:00 23:30
Available
Busy
DoNotDisturb
Away
Offline

Microsoft Build Event



Microsoft Developer ✅
@msdev

📣 Calling all devs!

Connect with product experts, industry disruptors, and cutting-edge partners to share ideas to build the future.

🌎 Digitally: May 23–24
🌆 In person in Seattle, WA: May 23–25

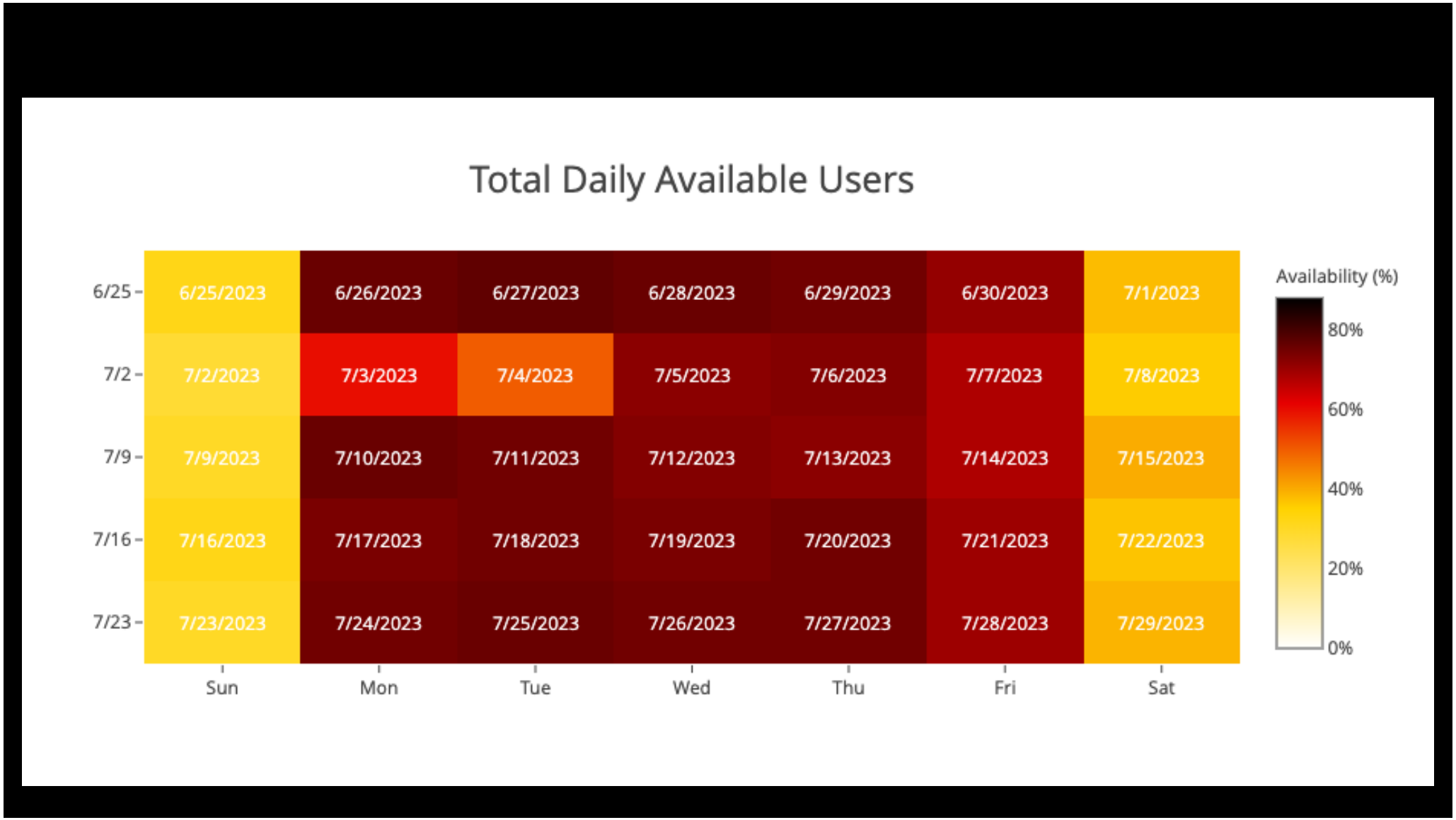
Register now for #MSBuild—made by and for developers:
msft.it/60105ljg6



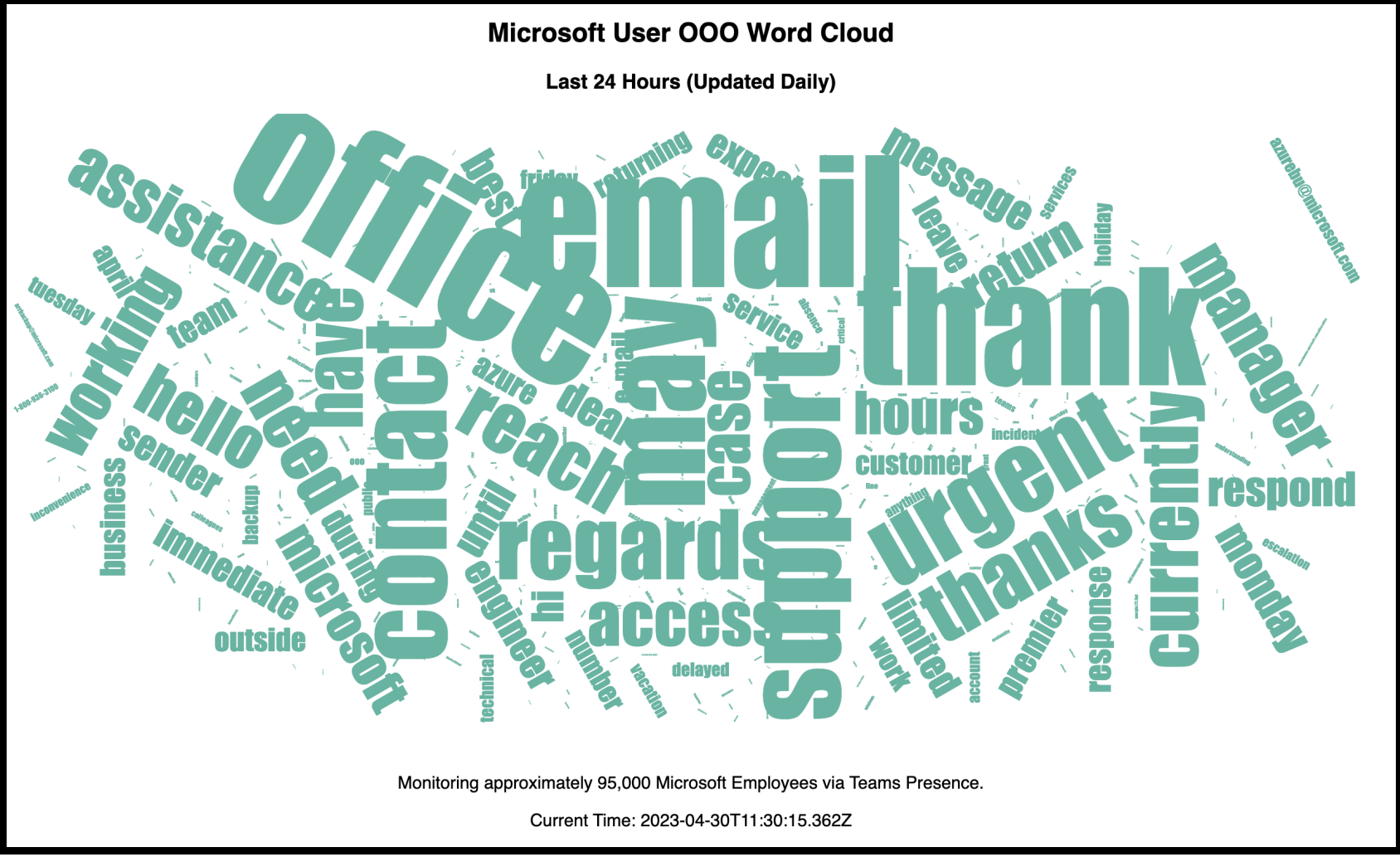
1:00 PM · Mar 14, 2023 · **211.2K** Views

"... we would not consider user enumeration on its own a security vulnerability. In many cases it is even intentional."

- MSRC


Total Daily Available Users
6/25
7/2
7/9
7/16
7/23
6/25/2023
6/26/2023
6/27/2023
6/28/2023
6/29/2023
6/30/2023
7/1/2023
7/2/2023
7/3/2023
7/4/2023
7/5/2023
7/6/2023
7/7/2023
7/8/2023
7/9/2023
7/10/2023
7/11/2023
7/12/2023
7/13/2023
7/14/2023
7/15/2023
7/16/2023
7/17/2023
7/18/2023
7/19/2023
7/20/2023
7/21/2023
7/22/2023
7/23/2023
7/24/2023
7/25/2023
7/26/2023
7/27/2023
7/28/2023
7/29/2023
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Availability (%)
80%
60%
40%
20%
0%

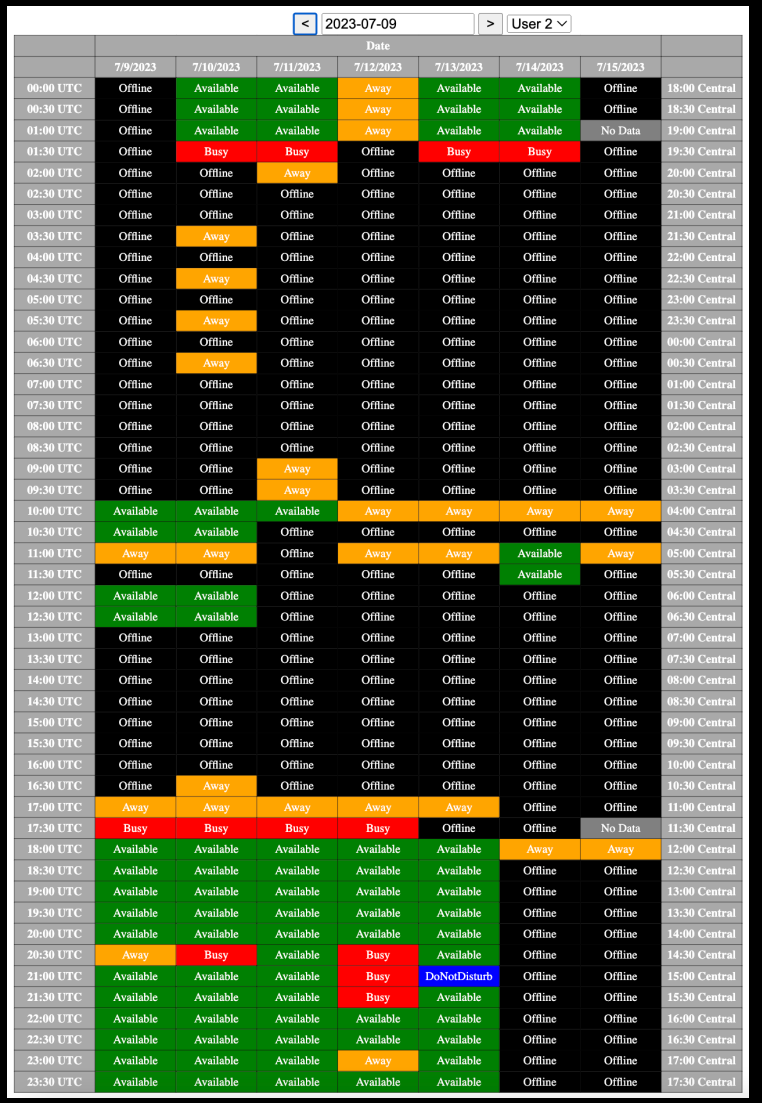
Out of Office Messages



Tracking the MS Security Folks

Step 1: Collect usernames of security/SOC employees from LinkedIn
Step 2: Put their names into john.smith@microsoft.com format
Step 3: TRACK!

- Is security online now?
- Did security come online during my attack?
- When is security usually AFK?

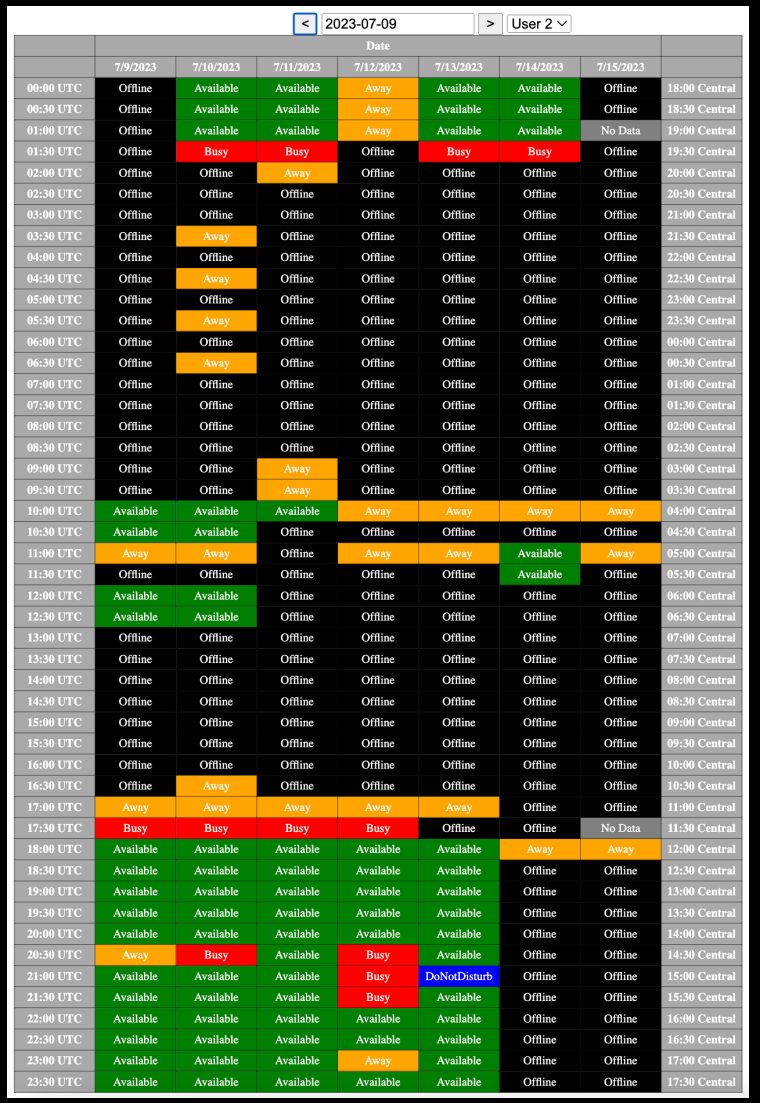


< 2023-07-09 > User 2

	Date							
	7/9/2023	7/10/2023	7/11/2023	7/12/2023	7/13/2023	7/14/2023	7/15/2023	
00:00 UTC	Offline	Available	Available	Away	Available	Available	Offline	18:00 Central
00:30 UTC	Offline	Available	Available	Away	Available	Available	Offline	18:30 Central
01:00 UTC	Offline	Available	Available	Away	Available	Available	No Data	19:00 Central
01:30 UTC	Offline	Busy	Busy	Offline	Busy	Busy	Offline	19:30 Central
02:00 UTC	Offline	Offline	Away	Offline	Offline	Offline	Offline	20:00 Central
02:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	20:30 Central
03:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	21:00 Central
03:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	21:30 Central
04:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	22:00 Central
04:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	22:30 Central
05:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	23:00 Central
05:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	23:30 Central
06:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	00:00 Central
06:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	00:30 Central
07:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	01:00 Central
07:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	01:30 Central
08:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	02:00 Central
08:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	02:30 Central
09:00 UTC	Offline	Offline	Away	Offline	Offline	Offline	Offline	03:00 Central
09:30 UTC	Offline	Offline	Away	Offline	Offline	Offline	Offline	03:30 Central
10:00 UTC	Available	Available	Available	Away	Away	Away	Away	04:00 Central
10:30 UTC	Available	Available	Offline	Offline	Offline	Offline	Offline	04:30 Central
11:00 UTC	Away	Away	Offline	Away	Away	Available	Away	05:00 Central
11:30 UTC	Offline	Offline	Offline	Offline	Offline	Available	Offline	05:30 Central
12:00 UTC	Available	Available	Offline	Offline	Offline	Offline	Offline	06:00 Central
12:30 UTC	Available	Available	Offline	Offline	Offline	Offline	Offline	06:30 Central
13:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	07:00 Central
13:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	07:30 Central
14:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	08:00 Central
14:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	08:30 Central
15:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	09:00 Central
15:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	09:30 Central
16:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	10:00 Central
16:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	10:30 Central
17:00 UTC	Away	Away	Away	Away	Away	Offline	Offline	11:00 Central
17:30 UTC	Busy	Busy	Busy	Busy	Offline	Offline	No Data	11:30 Central
18:00 UTC	Available	Available	Available	Available	Available	Away	Away	12:00 Central
18:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	12:30 Central
19:00 UTC	Available	Available	Available	Available	Available	Offline	Offline	13:00 Central
19:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	13:30 Central
20:00 UTC	Available	Available	Available	Available	Available	Offline	Offline	14:00 Central
20:30 UTC	Away	Busy	Available	Busy	Available	Offline	Offline	14:30 Central
21:00 UTC	Available	Available	Available	Busy	DoNotDisturb	Offline	Offline	15:00 Central
21:30 UTC	Available	Available	Available	Busy	Available	Offline	Offline	15:30 Central
22:00 UTC	Available	Available	Available	Available	Available	Offline	Offline	16:00 Central
22:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	16:30 Central
23:00 UTC	Available	Available	Available	Away	Available	Offline	Offline	17:00 Central
23:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	17:30 Central

Identifying Details via Presence

- What are their normal working hours?
- What times are they always offline?
- Did they work on the 4th of July, or other country-specific holidays?
- Did they work on religious holidays?



< 2023-07-09 > User 2

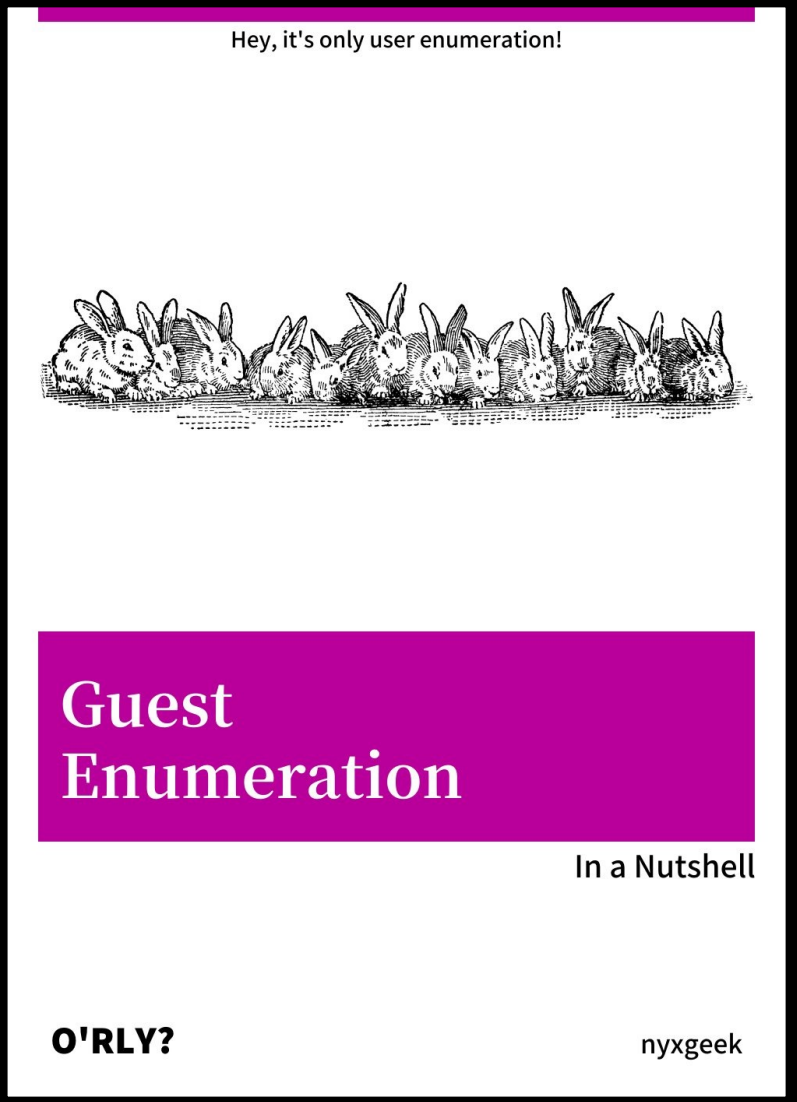
	Date							
	7/9/2023	7/10/2023	7/11/2023	7/12/2023	7/13/2023	7/14/2023	7/15/2023	
00:00 UTC	Offline	Available	Available	Away	Available	Available	Offline	18:00 Central
00:30 UTC	Offline	Available	Available	Away	Available	Available	Offline	18:30 Central
01:00 UTC	Offline	Available	Available	Away	Available	Available	No Data	19:00 Central
01:30 UTC	Offline	Busy	Busy	Offline	Busy	Busy	Offline	19:30 Central
02:00 UTC	Offline	Offline	Away	Offline	Offline	Offline	Offline	20:00 Central
02:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	20:30 Central
03:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	21:00 Central
03:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	21:30 Central
04:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	22:00 Central
04:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	22:30 Central
05:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	23:00 Central
05:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	23:30 Central
06:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	00:00 Central
06:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	00:30 Central
07:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	01:00 Central
07:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	01:30 Central
08:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	02:00 Central
08:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	02:30 Central
09:00 UTC	Offline	Offline	Away	Offline	Offline	Offline	Offline	03:00 Central
09:30 UTC	Offline	Offline	Away	Offline	Offline	Offline	Offline	03:30 Central
10:00 UTC	Available	Available	Available	Away	Away	Away	Away	04:00 Central
10:30 UTC	Available	Available	Offline	Offline	Offline	Offline	Offline	04:30 Central
11:00 UTC	Away	Away	Offline	Away	Away	Available	Away	05:00 Central
11:30 UTC	Offline	Offline	Offline	Offline	Offline	Available	Offline	05:30 Central
12:00 UTC	Available	Available	Offline	Offline	Offline	Offline	Offline	06:00 Central
12:30 UTC	Available	Available	Offline	Offline	Offline	Offline	Offline	06:30 Central
13:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	07:00 Central
13:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	07:30 Central
14:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	08:00 Central
14:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	08:30 Central
15:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	09:00 Central
15:30 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	09:30 Central
16:00 UTC	Offline	Offline	Offline	Offline	Offline	Offline	Offline	10:00 Central
16:30 UTC	Offline	Away	Offline	Offline	Offline	Offline	Offline	10:30 Central
17:00 UTC	Away	Away	Away	Away	Away	Offline	Offline	11:00 Central
17:30 UTC	Busy	Busy	Busy	Busy	Offline	Offline	No Data	11:30 Central
18:00 UTC	Available	Available	Available	Available	Available	Away	Away	12:00 Central
18:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	12:30 Central
19:00 UTC	Available	Available	Available	Available	Available	Offline	Offline	13:00 Central
19:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	13:30 Central
20:00 UTC	Available	Available	Available	Available	Available	Offline	Offline	14:00 Central
20:30 UTC	Away	Busy	Available	Busy	Available	Offline	Offline	14:30 Central
21:00 UTC	Available	Available	Available	Busy	DoNotDisturb	Offline	Offline	15:00 Central
21:30 UTC	Available	Available	Available	Busy	Available	Offline	Offline	15:30 Central
22:00 UTC	Available	Available	Available	Available	Available	Offline	Offline	16:00 Central
22:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	16:30 Central
23:00 UTC	Available	Available	Available	Away	Available	Offline	Offline	17:00 Central
23:30 UTC	Available	Available	Available	Available	Available	Offline	Offline	17:30 Central

Stage 3: Guest User Enumeration



Overview

- It is possible to enumerate guest users in Azure tenants
- Consider your guest membership to be public information



Guest Users in Azure

- Allows Business-to-Business collaboration
- Guests use their own email address (UPN) to access Azure resources in an external tenant
    1. **John at Acme Computers** needs help with some old C code.
    2. **Acme Compute**rs invites **David Lightman** from the **Midnight Computer Lab** Consultancy Group.
    3. **David Lightman** can now access the **Acme Computer Azure cloud** with his **dlightman@midnightcomputerlab.com** work email.
    4. Permissions are restricted to whatever is assigned, if any. By default, can read user and group membership.
- Anybody can invite Guests by default (even other guests!)
    - Does not necessarily mean a partnership or vendor relationship

Guest Account Translation

User Principal Name: dlightman@midnightcomputerlab.com



Display name	David Lightman
First name	David
Last name	Lightman
User principal name	dlightman_midnightcomputerlab.com#EXT#@acmecomputercompany.onmicrosoft.com
Object ID	82354523-5479-4216-85d0-0c169cd98096
Identities	acmecomputercompany.onmicrosoft.com
User type	Guest

Guest User Principal Name (UPN) Translation:

- UPN has "@" replaced with "_"
- UPN has "#EXT#@<tenant>.onmicrosoft.com" appended


IT'S NOT A BUG
IT'S A FEATURE
imgflip.com

Silent Guest Enumeration

- @DrAzureAD revealed Guest Enum via Seamless SSO in October 2019.
  - This method will return false positives after approximately 100,000 attempts
- Guest Enumeration has been published for nearly 4 years

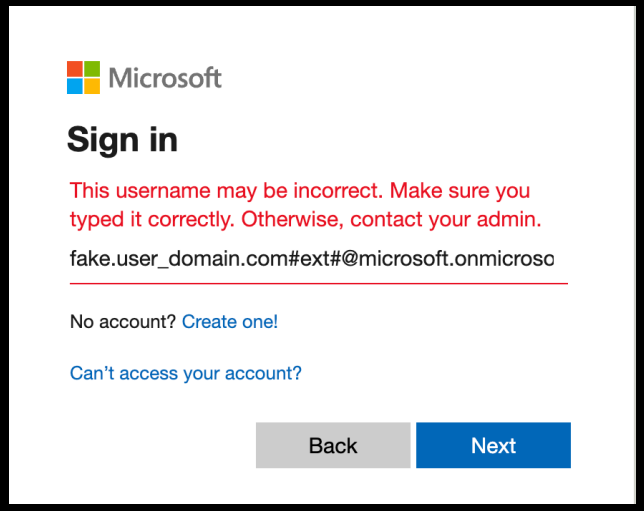
So, what is the big deal? Using the **GetCredentialType** API, one can find valid user accounts of the tenant and focus password-spray attack on those. Not so surprisingly, as Oliver Morton mentioned in his **blog**, Microsoft does not regard the enumeration to be an issue because the potential attacker still needs to pass the authentication to get in. However, my enumeration method has one advantage compared to Morton's method: **It can be used to enumerate external users!**

External users are users to whom are given some access to tenant. For instance, if a file is shared from OneDrive to someone outside your organization, an external user is added to Azure AD. The external users have a special format: **<email_address>#EXT#@<tenant>.onmicrosoft.com** where **email_address** is the external user's email address where the '@' is replaced with '_'

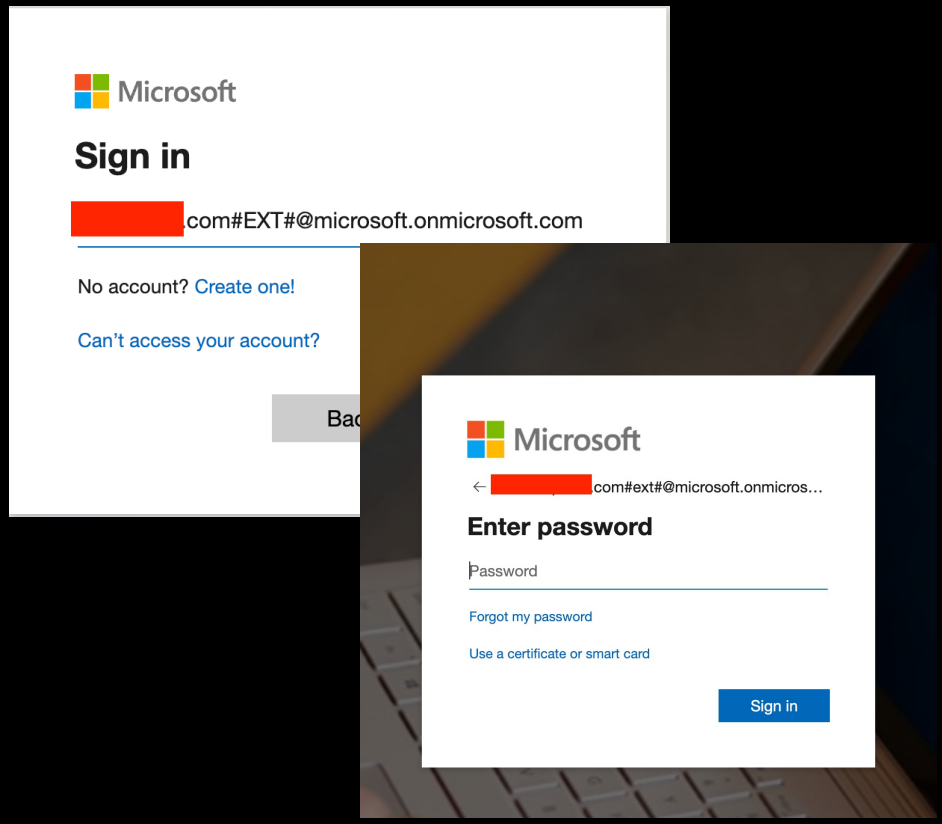
https://aadinternals.com/post/desktopsso/

Nestori's Silent Enum

Invalid



Valid



guestlist

https://github.com/nyxgeek/guestlist

- Will be released shortly after this talk
- Includes Nestori's Silent Method AND a NEW Graph Auth Method
- Email address does NOT have to be UPN – can be an alias, any email address

Active Enumeration

- Graph-based user enumeration (standard)
  - Authenticates against Microsoft Graph
- **YOU CANNOT LOG IN THIS WAY** – EVEN WITH VALID PASSWORD
- IF YOU IDENTIFY A VALID GUEST, THIS WILL SHOW UP IN AUDIT LOGS AS FAILED LOGIN
- No indicator if password is valid/invalid with Guest Accounts

If only we had a huge list of usernames…

- Email sources:
  - Could buy business email lists online ($$$)
  - OneDrive Enum
  - Public dump files

- Guest Enumeration was the end-goal of my 1.5 year user enumeration via OneDrive

- Now, with 23 million business emails on hand, we can begin mapping!

Identifying Public Partnerships

big4accountingfirms.com/ernst-and-young-clients/

EY Clients 2022

A listing of Ernst and Young's largest clients is inc
provide some background about the client and if t
current auditor. We also provide the amount of fe
some of the clients.

1. Hewlett Packard
2. Verizon
3. State Street
4. AT&T
5. Coca Cola

siliconangle.com/2023/06/29/vmware-partners-samsung-amd-risc-v-accelerate-confidential-compu

siliconANGLE [the voice of enterprise and emerging tech]

CLOUD AI SECURITY INFRA BLOCKCHAIN POLICY BIG DATA APPS EMERGING TECH

blogs.cisco.com/datacenter/cisco-partners-with-amd-to-set-a-world-record

April 11, 2022 Leave



Data Center

Cisco Partners with AMD to set a World Record!

John McAbel

siliconrepublic.com/machines/intel-arm-chip-design-partnership

siliconrepublic TECHNOLOGY SCIENCE CARE

MACHINES

Intel partners with Arm to create next-gen chip designs

by Leigh Mc Gowran

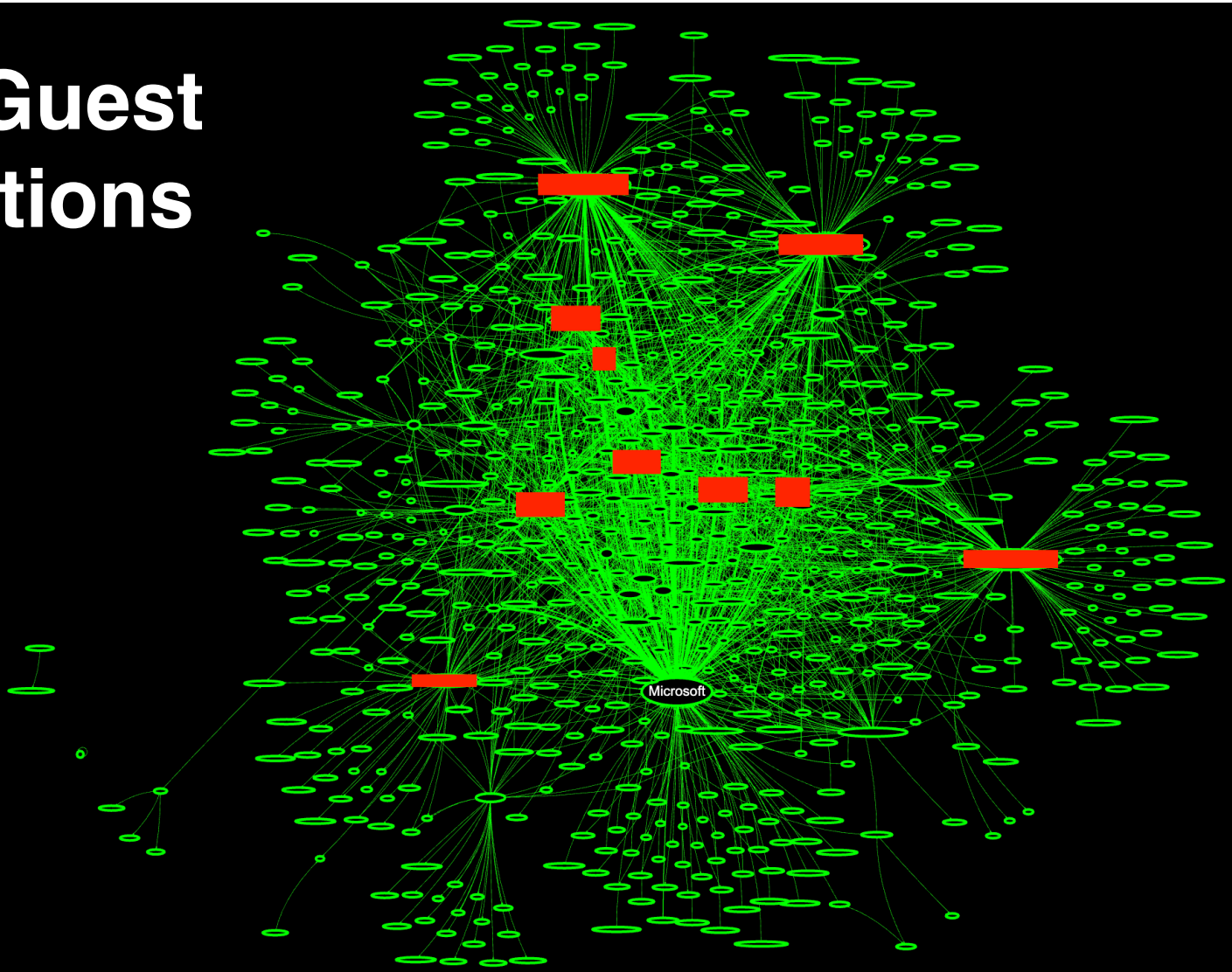
13 APR 2023 SAVE ARTICLE



VMware partners with Samsung, AMD and RISC-V to accelerate confidential computing

BY MIKE WHEATLEY

30,000 Guest Connections



Discovered Guest Accounts Involving:

- Microsoft
- Tesla
- VMware
- Facebook
- Fedex
- Adobe
- Pepsi
- Pfizer
- Berkshire Hathaway
- Halliburton
- HP
- Sanofi
- Cisco
- BakerHughes
- Thermofisher

- And many more.

- 790 unique domain -> tenant relationships identified

- 168 unique source domains
- 214 unique host tenants

- 30,000 individual guest relationships

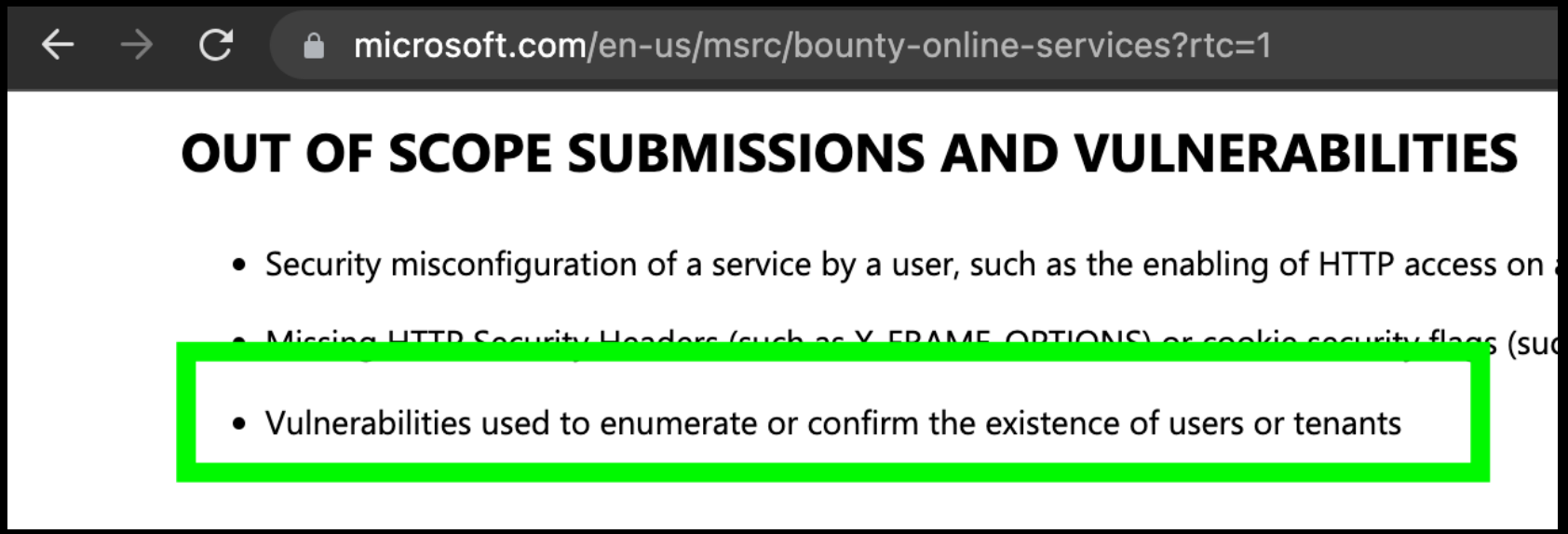
"… we would not consider user enumeration on its own a security vulnerability."

--MSRC

Microsoft Relationships: It's a Feature!

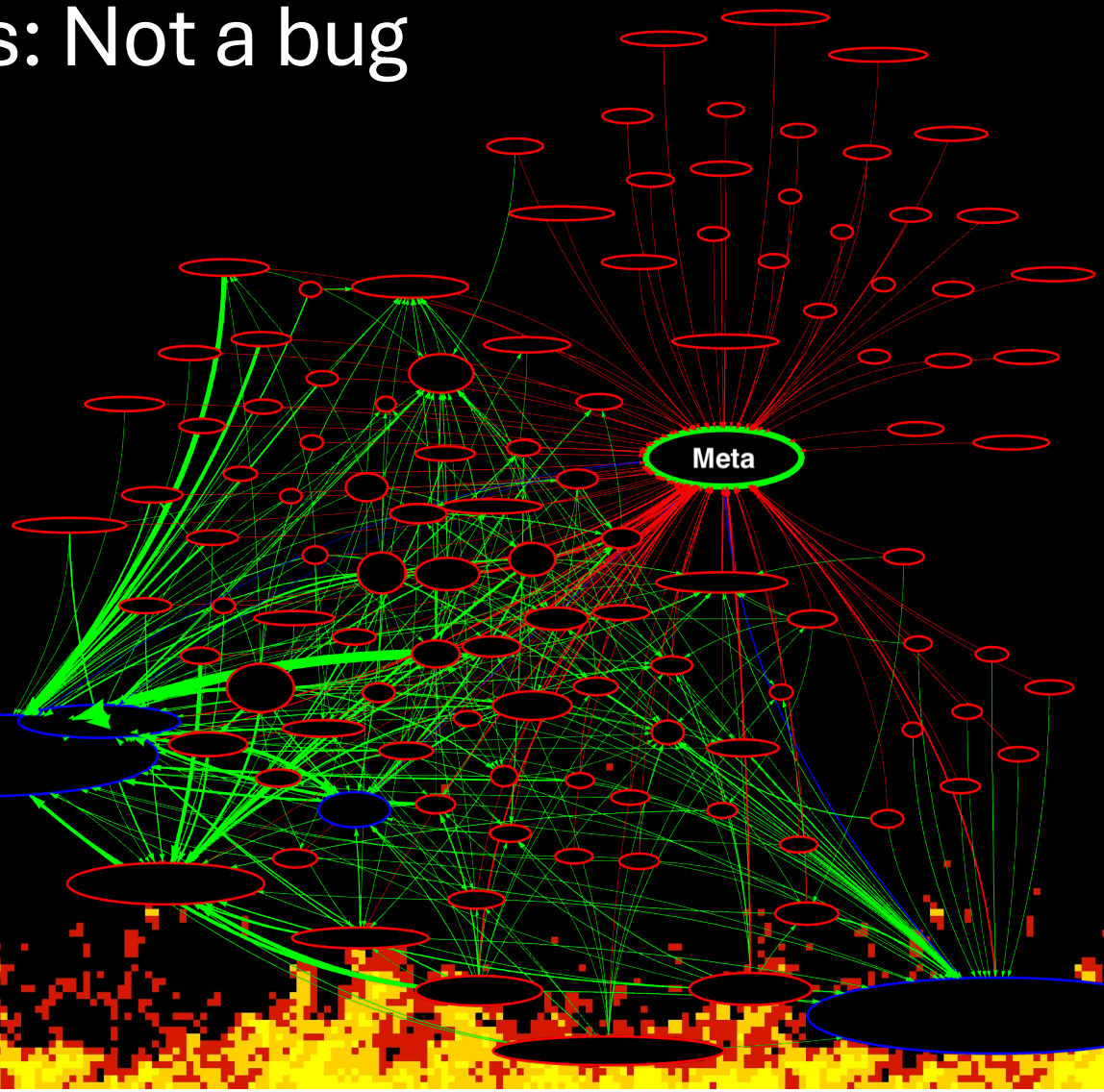


Microsoft's Stance on User Enumeration



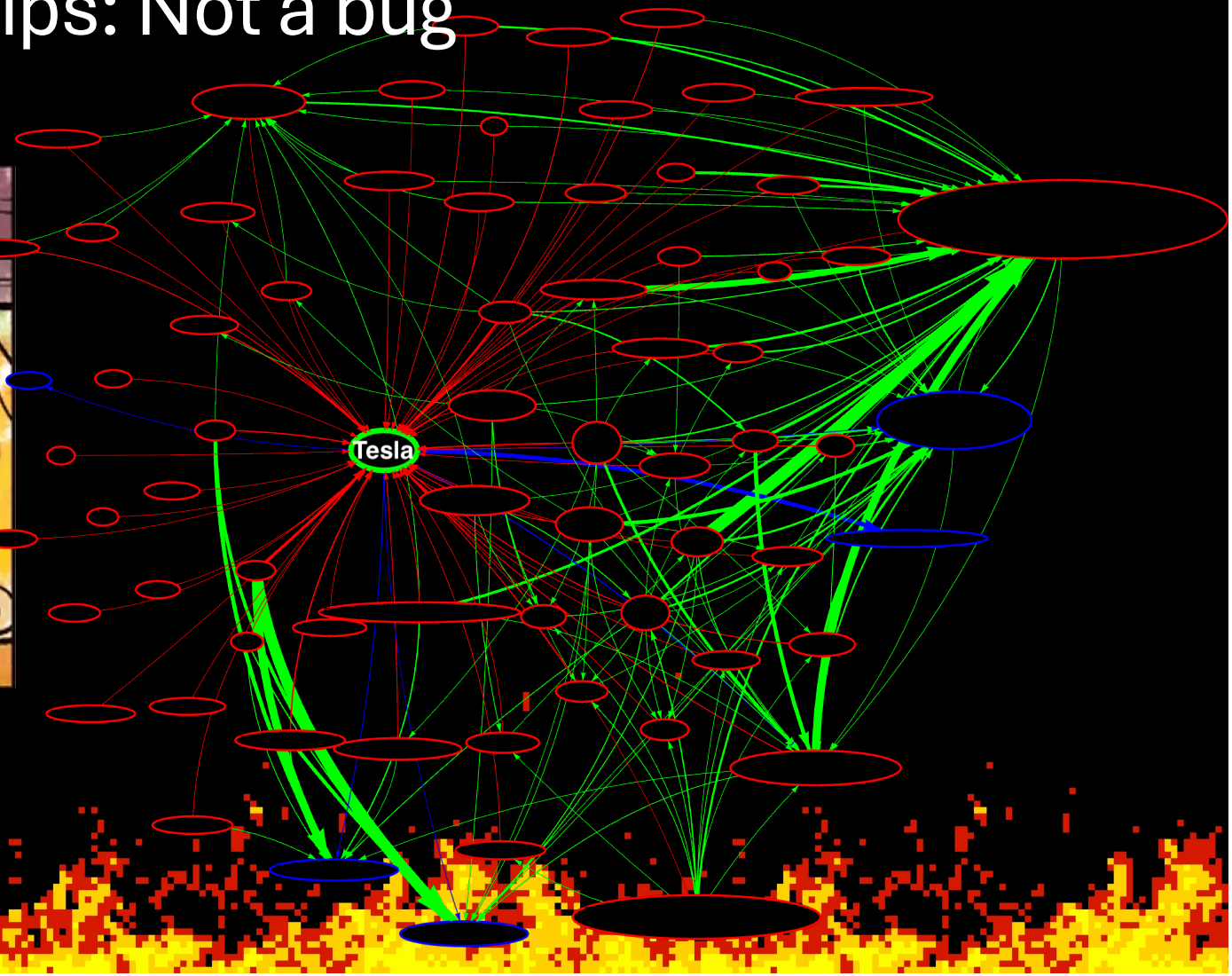
Meta Relationships: Not a bug



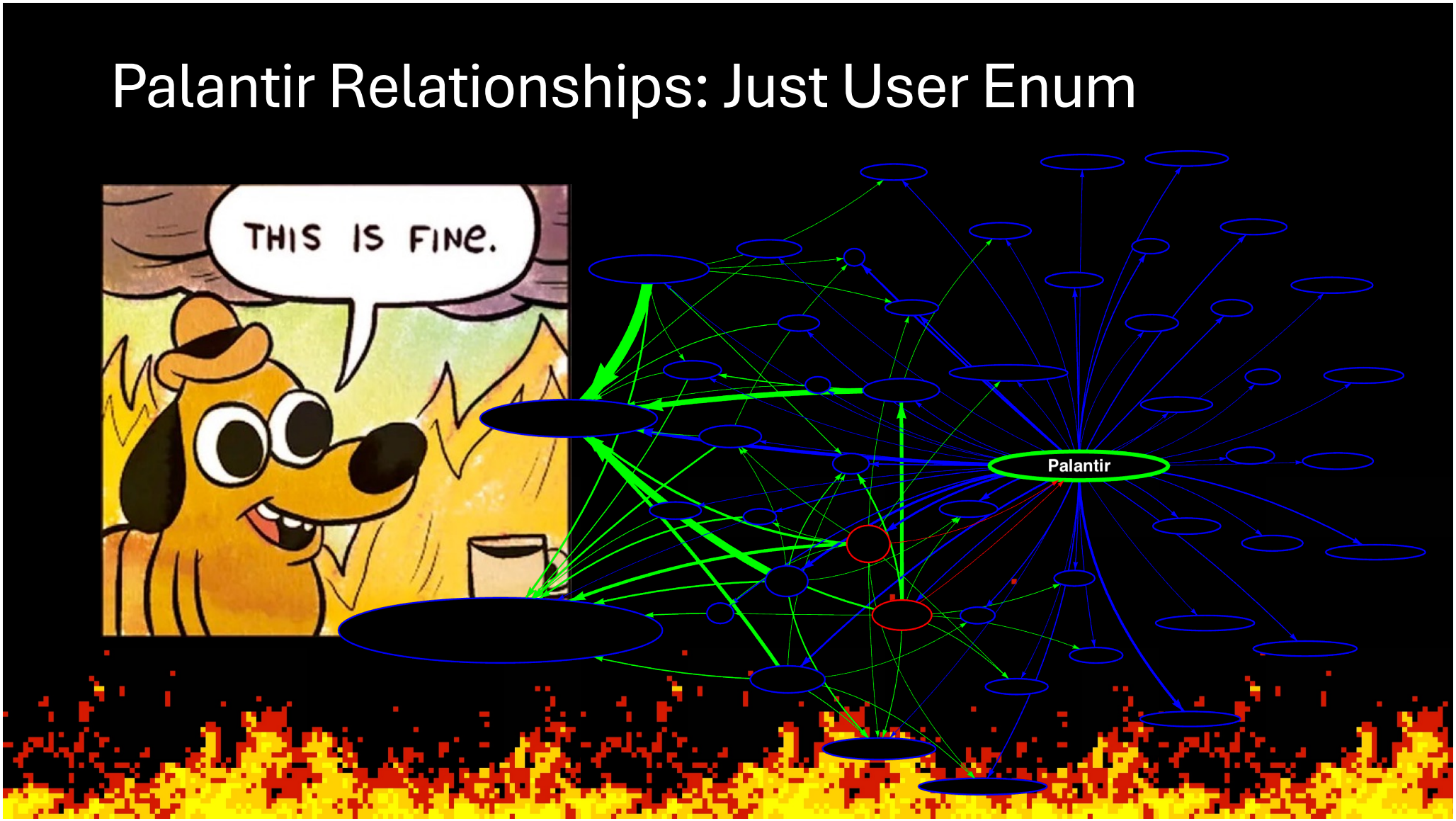


Tesla Relationships: Not a bug



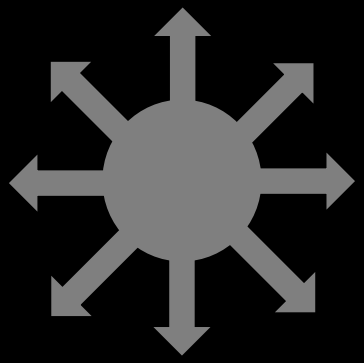


Palantir Relationships: Just User Enum



Most Widespread Companies

- List of DISTINCT host tenants per domain
- This is a list of what companies (domains) have access to the most other organizations
- Lots of consulting firms



source_domain	found
ey.com	55
cdw.com	47
kpmg.com	38
palantir.com	37
pwc.com	36
microsoft.com	33
deloitte.com	33

Digging Deeper

- Usernames are often names
- Names can be linked to identities
- Guest accounts often remain for long periods



Stephen Falken
Senior Unix Engineer
2018-Present

Acme Computers



nyxgeek
nerfherder, 2016-2020

Midnight Computer Lab



John Doe
Shipping Manager, 2020-Present

Generic Supply Co

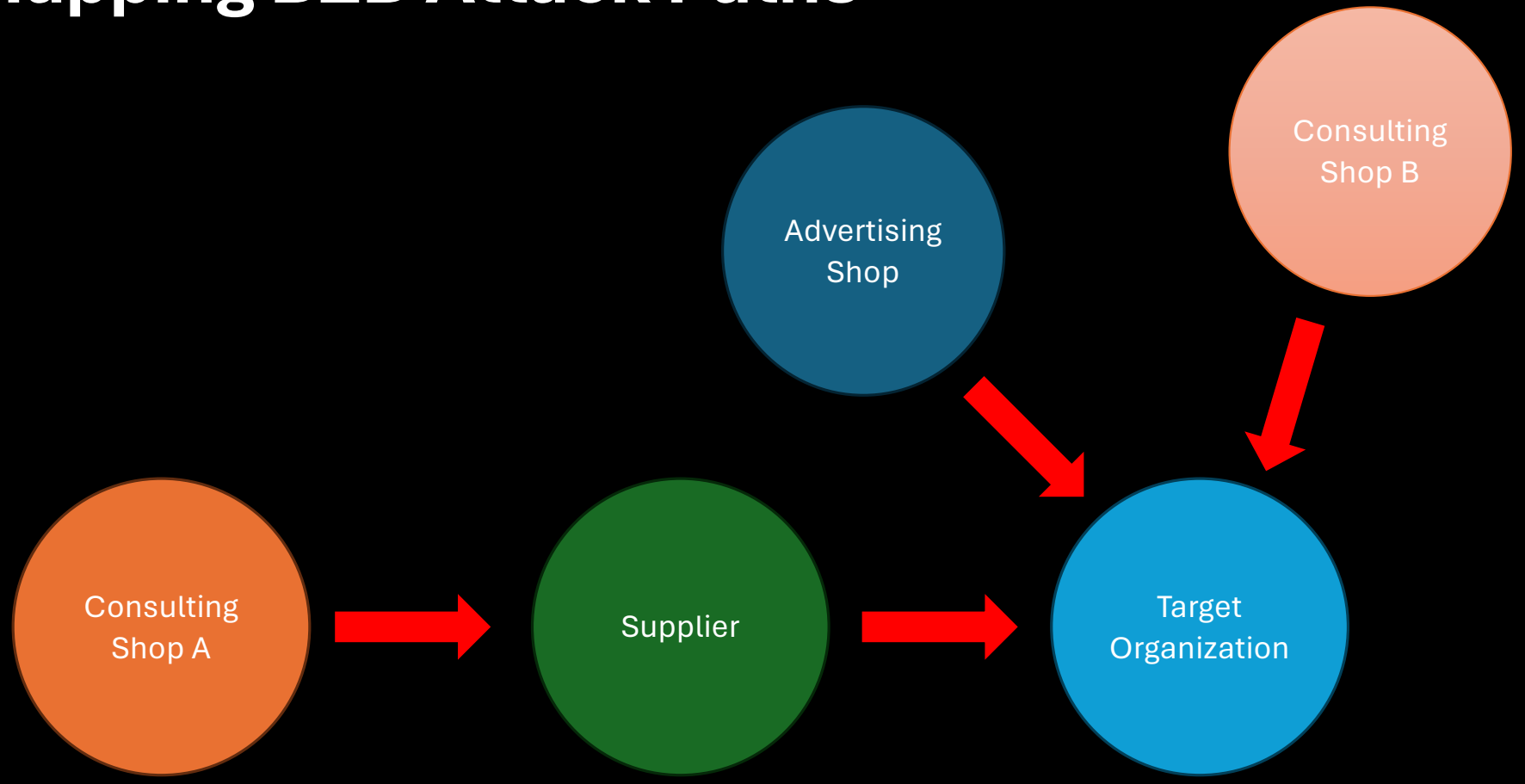


David LIghtman
Security Consultant, 2021-2023

Consultants-R-Us

Target Org

Mapping B2B Attack Paths



User Enumeration and US

- US Adversary's dream
  - A list of target companies in
    - US Federal Gov
    - State Gov
    - Corporate America
  - All suffer from various user enumeration flaws in Azure
- Do we want people to be able to create lists of users in:
  - critical infrastructure companies
  - supply chain companies
  - federal agencies
  - federal government
- People don't change their names often – long term investment

Review:

- We demonstrated that it is possible to enumerate over 24 MILLION Azure users from across many organizations
- We have demonstrated monitoring of 100,000 employees every 30 minutes every day
- We have demonstrated mapping of guest relationships between organizations.

But, it's just user enumeration.

REMEMBER

- This affects everyone* – everyone is in azure
- I am just the messenger, Microsoft made it this way

A request:

- If you have large accounts with Microsoft, please speak with your Microsoft Representative and recommend that they take user enumeration seriously.

shoutoutz and greetz

- @DrAzureAD
- @techr0mancer
- @karlfosaaen
- @rootsecdev
- @flangvik

- The entire crew at TrustedSec
- My horde of bots working around the clock

More Information

https://github.com/nyxgeek/onedrive_user_enum

https://github.com/nyxgeek/teamstracker

https://github.com/nyxgeek/guestlist

@nyxgeek on twitter