

REDACTED VERSION –  
Microsoft asked to  
redact some of this  
publicly-available  
information, that they  
have said repeatedly IS  
NOT A VULNERABILITY.

# 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%)

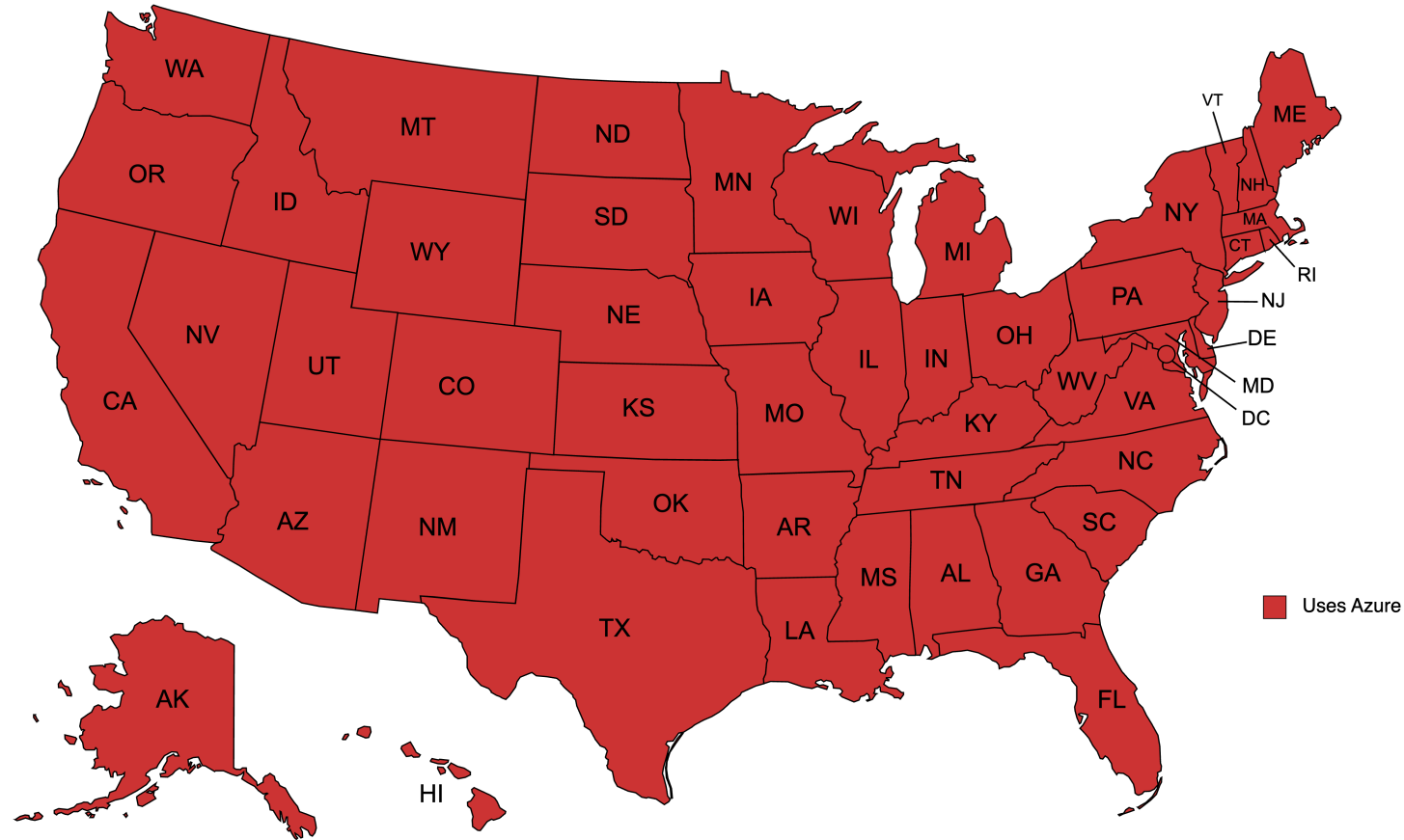
Total Employees - Fortune 500  
32.5m~

- 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

## A2:2017-Broken Authentication

[← 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 using manual means and exploit them.		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.	

The screenshot shows the MITRE Common Weakness Enumeration (CWE) website. The browser address bar displays <https://cwe.mitre.org/data/definitions/203.html>. The page header includes the CWE logo, the text "Common Weakness Enumeration - A Community-Developed List of Software & Hardware Weakness Types", and two circular icons: "Top 25" and "Top HW CWE". A "New to CWE Start here!" link is also present. The breadcrumb trail reads "Home > CWE List > CWE- Individual Dictionary Definition (4.11)". The navigation menu contains "Home", "About", "CWE List", "Scoring", "Mapping Guidance", "Community", "News", and "Search". The main heading is "CWE-203: Observable Discrepancy". Below this, the "Weakness ID: 203" is listed, along with "Abstraction: Base" and "Structure: Simple". A "View customized information:" section offers buttons for "Conceptual", "Operational", "Mapping Friendly", "Complete" (which is selected), and "Custom". The "Description" section states: "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." The "Extended Description" section states: "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

← → ↻ [microsoft.com/en-us/msrc/bounty-online-services?rtc=1](https://microsoft.com/en-us/msrc/bounty-online-services?rtc=1)

## OUT OF SCOPE SUBMISSIONS AND VULNERABILITIES

- Security misconfiguration of a service by a user, such as the enabling of HTTP access on a service
- Missing HTTP Security Headers (such as X-FRAME-OPTIONS) or cookie security flags (such as HttpOnly, Secure, and SameSite)
- Vulnerabilities used to enumerate or confirm the existence of users or tenants

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

Microsoft Security Response Center <secure@microsoft.com>  
to me ▾

Fri, Aug 27, 2021, 5:42 PM



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

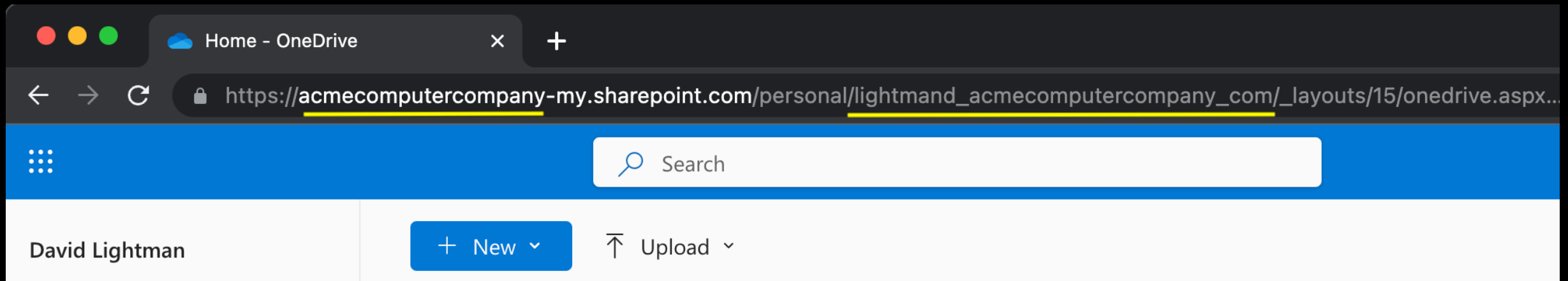
# Why OneDrive?

- 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",
  "exchange.microsoft.com"
```

# OneDrive Enumeration in Action

```
# ./onedrive_enum.py -T150 -d microsoft.com -U USERNAMES/statistically-likely
*****
onedrive
enum
OneDrive Enumerator
2023 @nyxgeek - TrustedSec
version 2.00
https://github.com/nyxgeek/onedrive_user_enum
*****

Tenants Identified:
-----
microsofteur
microsoftapc
msfts2
microsoftprd
microsoftcan
microsoft

OneDrive hosts found:
-----
microsofteur-my.sharepoint.com
microsoftapc-my.sharepoint.com
microsoftprd-my.sharepoint.com
microsoft-my.sharepoint.com

+++++

Running with user list 1 of 3 : USERNAMES/statistically-likely/smithj.txt

Beginning enumeration of https://microsoft-my.sharepoint.com/personal/USER_microsoft_com/
-----
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - sin [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - kum [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - tho [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - jon [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - her [REDACTED] ndezj@microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - ngu [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - tho [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - sin [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - sha [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - gor [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - tho [REDACTED] microsoft.com
[-] [403] VALID USERNAME FOR microsoft,microsoft.com - kel [REDACTED] microsoft.com
1109 / 43378 tested, 205 valid, 0 errors
```

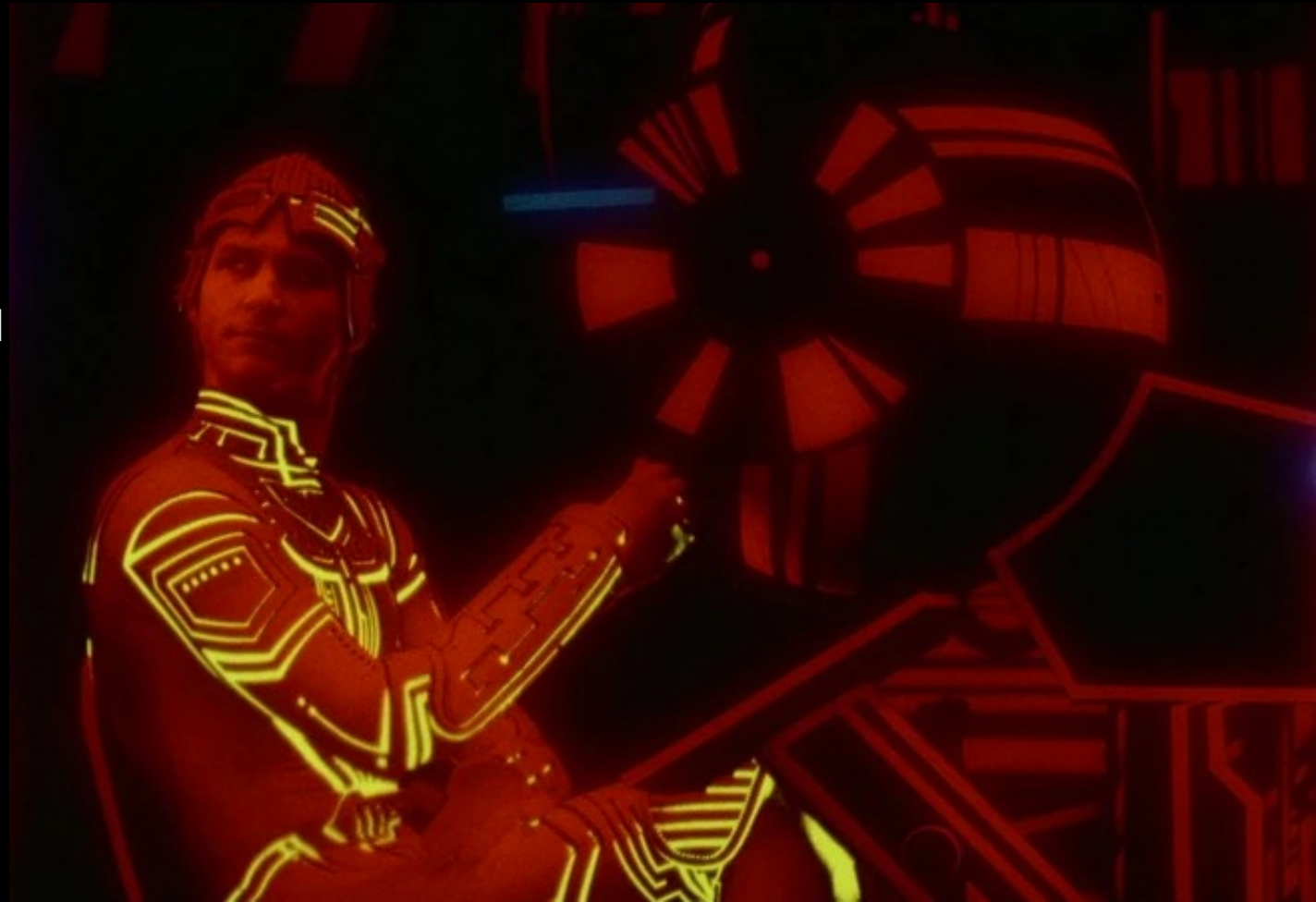
# Infrastructure Overview

## Client (CLU)

### Cloud Lookup Utility

- 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



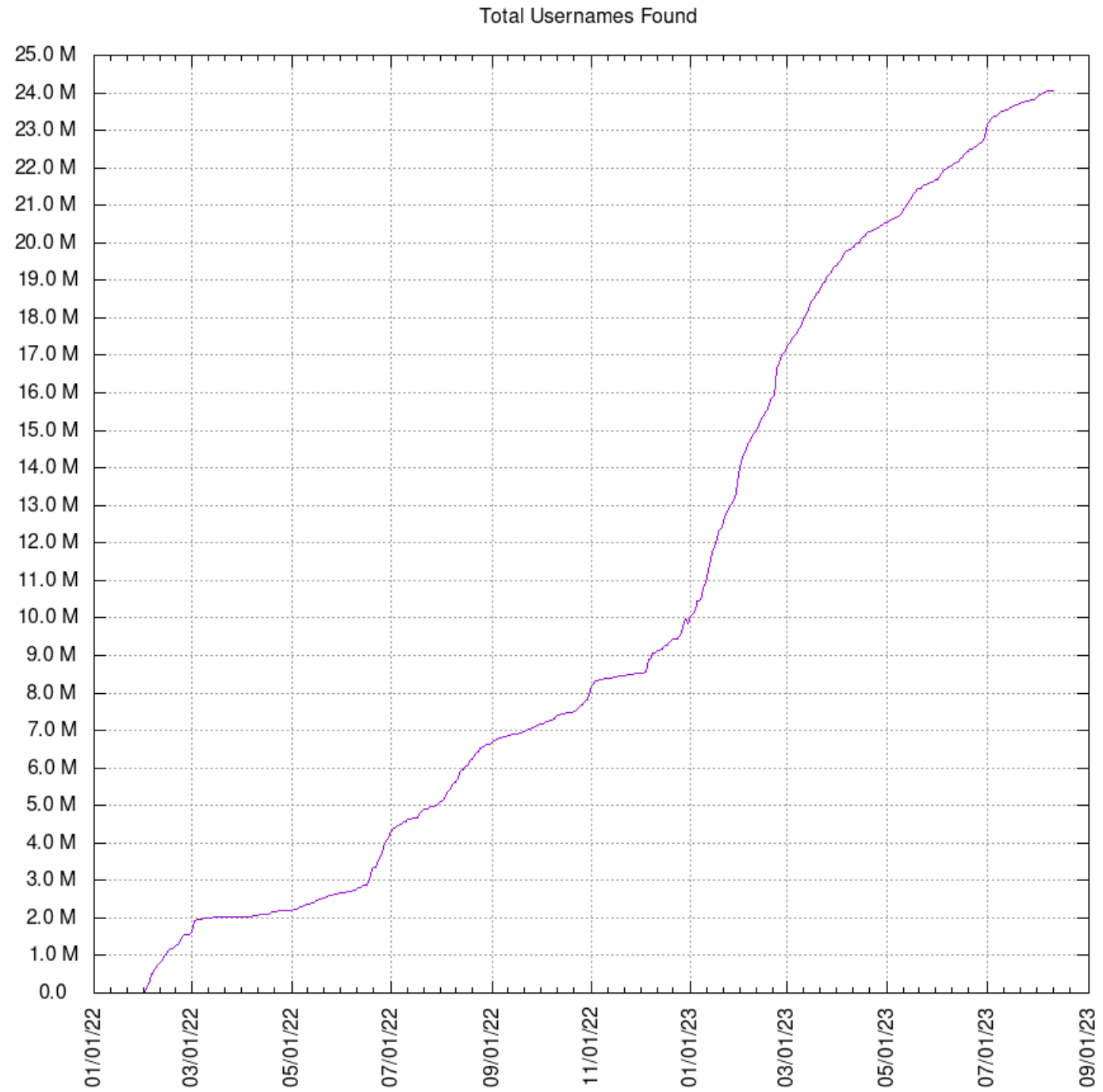
# THE ORIGINAL CLU CREW



# 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:jjjs
```

# 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

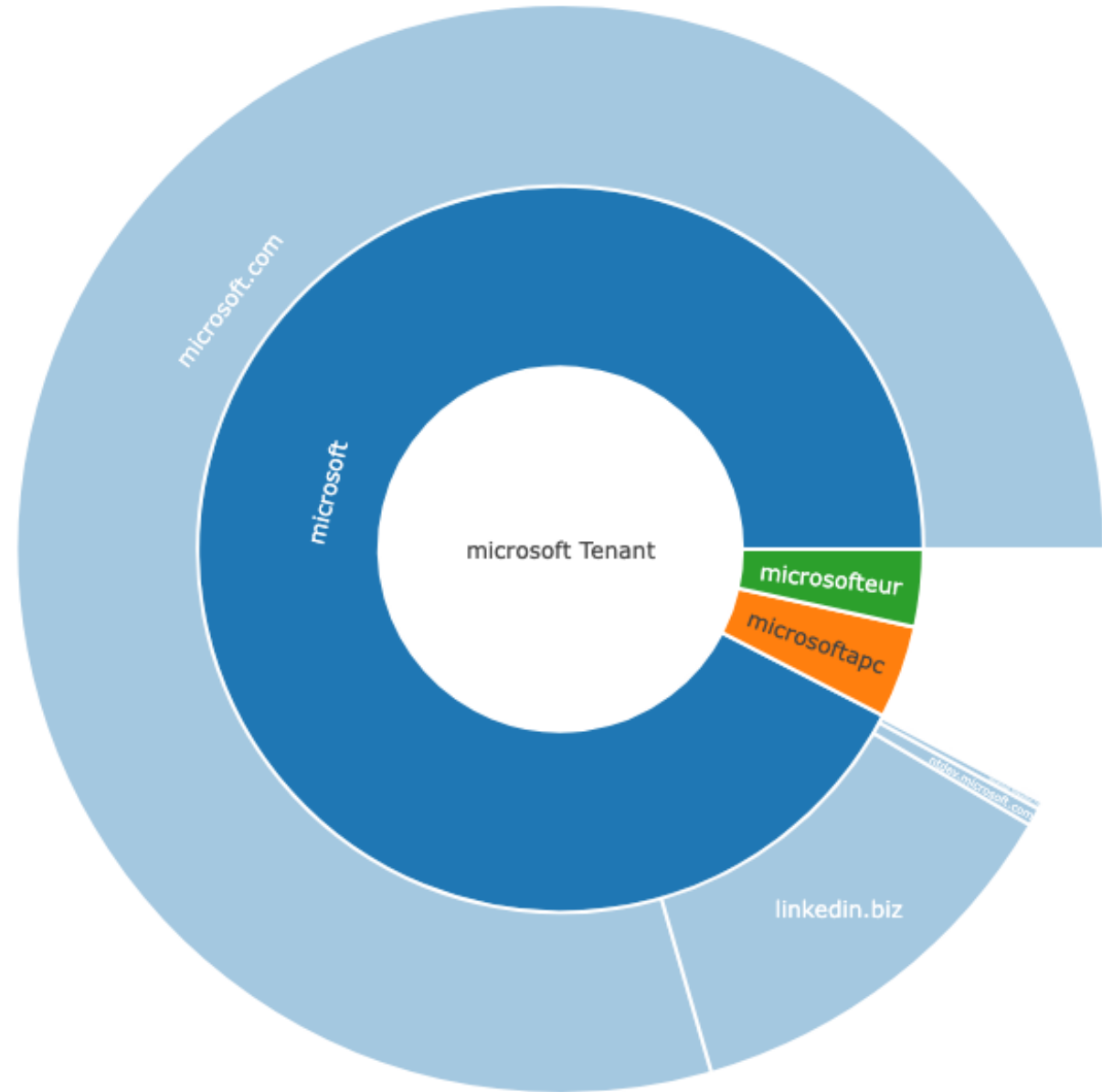
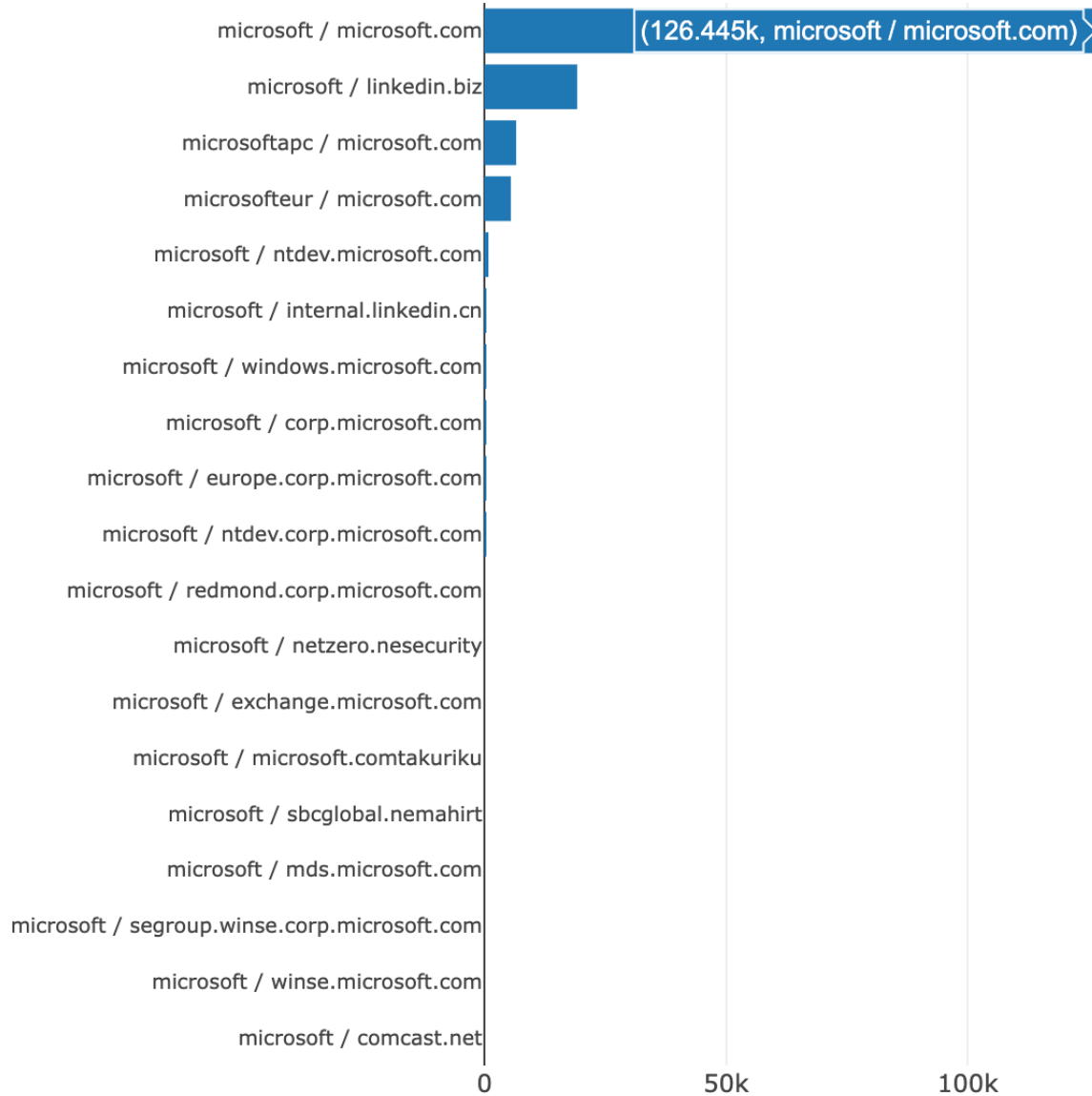
# Combinations of Username Formats

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

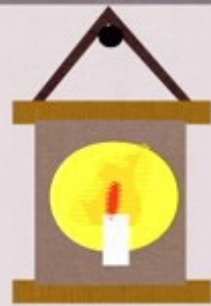
# Fortune 1000 Primary Tenant – Top User Counts

1	Name	Primary Tenant	Domains	Tenants	Users Enumerated	Estimated Employee Count	Percent Found
2			2	1	474094	270000	175.59%
3			1	4	407345	330600	123.21%
4			6	1	345078	141700	243.53%
5			19	3	158884	221000	71.89%
6			2	1	141889	99290	142.90%
7			4	1	137867	71970	191.56%
8			29	1	120947	258000	46.88%
9			3	1	116725	484000	24.12%
10	Redacting	Redacting	1	1	113738	202600	56.14%
11	at	at	7	1	105228	247848	42.46%
12	Microsoft's	Microsoft's	27	1	101735	350000	29.07%
13	Request	Request	82	1	95739	297800	32.15%
14			1	1	92524	400945	23.08%
15			5	1	91217	83000	109.90%
16			22	1	89823	105000	85.55%
17			3	1	86884	68796	126.29%
18	This is	This is	1	1	85183	183000	46.55%
19	publicly	publicly	2	1	82299	309000	26.63%
20	available	available	1	1	74463	450000	16.55%
21	information	information	6	1	63711	133000	47.90%
22			2	1	61415	93700	65.54%
23			8	1	56273	38784	145.09%
25			1	7	54983	74814	73.49%
26			12	1	53079	171000	31.04%
27			2	1	51621	113000	45.68%
28			7	1	51424	95500	53.85%
29			1	1	50833	55093	92.27%
30			13	1	49407	99000	49.91%
31			1	1	47376	50000	94.75%

# Exploring Tenant and Domain Relationships







PHASE 1

PHASE 2

PHASE 3

---

Collect  
Usernames



Profit



# STAGE 2: PRESENCE ENUMERATION

## Monitoring Teams

Tracking Users Across an Enterprise





# A Timeline of Teams, Skype4b, Lync

2011

2015

2016

2017

2018

2019

2020

2021

2022

Microsoft  
Lync  
(Open  
Federation)

Skype replaces  
Lync  
(Open  
Federation)

Karl Fosaaen – Attacking  
Federated Skype4B,  
PowerSkype  
  
nyxgeek – The Weakest Lync,  
lynasmash

CVE-2017-8550  
(Skype4B  
Windows)  
  
Teams released  
(External Access)

CVE-2018-  
8474  
(lync for mac)  
  
DrAzureAD -  
AADInternals

DrAzureAD -  
Seamless SSO  
Enum

Dafthack -  
MSOLSpray

Skype for  
Business Online  
Retired

Melvin Langvik –  
TeamFiltration at  
DC30

# 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			
Offline	Chief Executive Officer		
Offline	Responsible		
Offline	Office of the Chairman		
Offline	President and CEO		
Away	Chairman, President and CEO		
Away	Chairman of the Board, President & CEO		
Offline	VP, FINANCE & SOLUTIONS		
Offline	EVP & Chief Financial Officer		
Offline			
Offline	Chief Executive, AstraZeneca		
Offline			
Offline	CEO		
Offline			
Offline			
Away	EVP & Chief Technology Officer		
Offline	CEO		
Offline	Chairman		
Offline	CEO & President		
Offline	Chairman, CEO & President		
Offline	Chairman, CEO		
Offline	Chief Executive Officer		
Offline	PDG		

Redacting at Microsoft's Request

This is publicly available information

# Skype for Creepers 2017

Offline	President & Chief Executive Officer
Away	GM-GM-General Manager EMT member
Offline	
Offline	President & Chief Operating Officer
Away	Chief Executive Officer
Away	Chief Executive Officer
Offline	Chief Executive Officer
Offline	Evp Store Operations
Offline	Dr.
Offline	President and CEO
Offline	
Offline	
Away	CFO
Offline	Chairman and Chief Executive Officer
Offline	DIRECTEUR GENERAL DU GROUPE
Busy	PRESIDENT & CEO
Offline	CEO
Away	EVP CFO
Offline	President & CEO
Offline	Senior Vice President and Chief Information Officer
Offline	
Offline	
Offline	
Away	Executive Director
Offline	Chief Executive Officer
Away	
Offline	President & CEO
Offline	Chairman, President & CEO
Offline	EVP & Chief Financial Officer
Offline	President Volvo Group and CEO
Offline	
Offline	GVP & Chief Info Officer

Redacting at Microsoft's Request

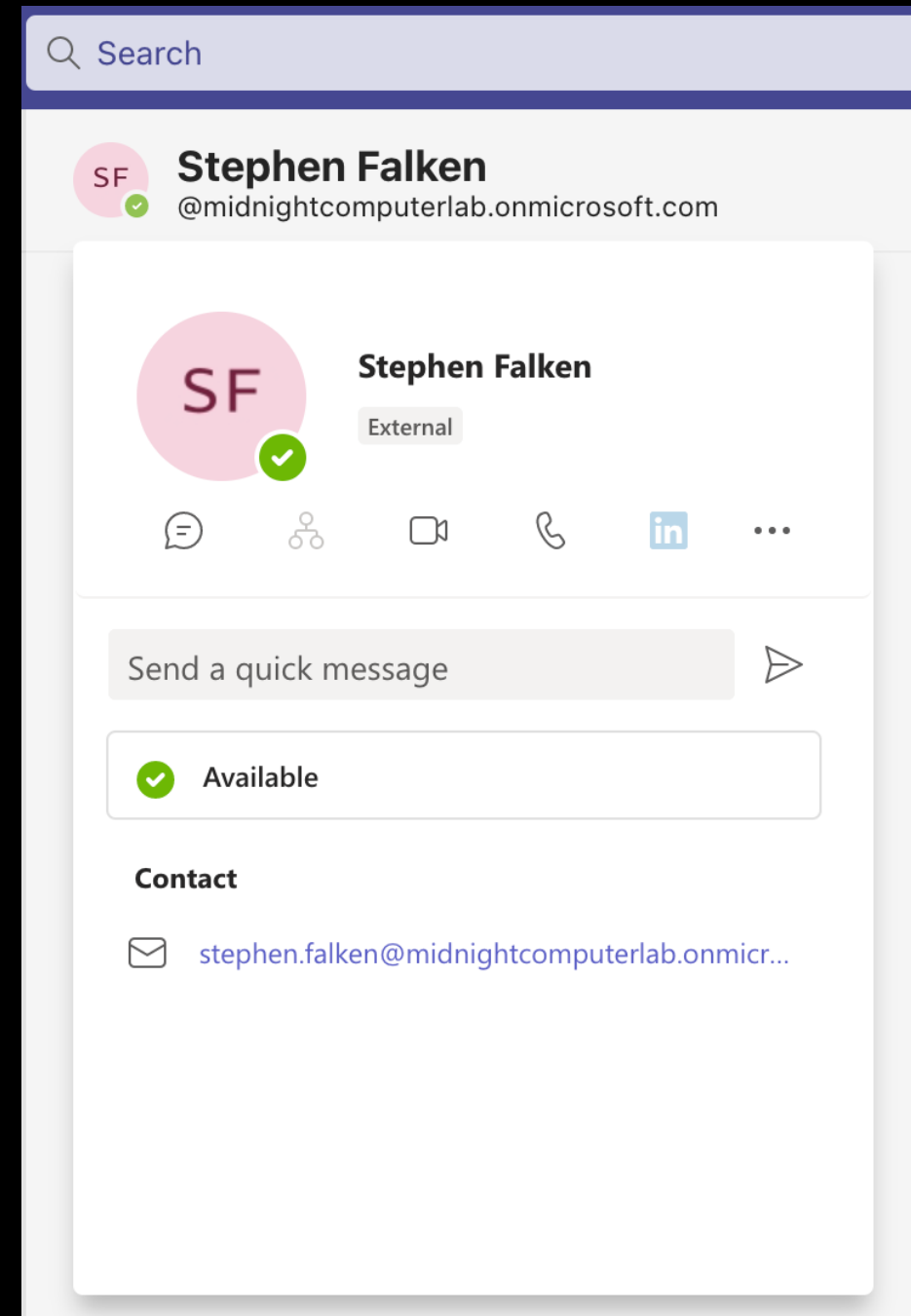
This is publicly available information

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!**

# Presence Lookup via Graph Explorer

The screenshot shows the Microsoft Graph Explorer interface. The URL bar contains the endpoint: `https://graph.microsoft.com/beta/users/d4957c9d-869e-4364-830c-d0c95be72738/presence`. The user ID `d4957c9d-869e-4364-830c-d0c95be72738` is highlighted in green. The response status is `OK - 200 - 105985ms`. The response preview shows the following JSON data:

```
{  "@odata.context": "https://graph.microsoft.com/beta/$metadata#users('d4957c9d-869e-4364-830c-d0c95be72738')/presence/$entity",  "id": "d4957c9d-869e-4364-830c-d0c95be72738",  "availability": "Offline",  "activity": "Offline",  "statusMessage": null,  "outOfOfficeSettings": {    "message": null,    "isOutOfOffice": false  }}
```

The screenshot shows a network request intercept tool displaying the raw HTTP request. The request is to `https://graph.office.net:443`. The raw request body is as follows:

```
1 GET /en-us/graph/api/proxy?url=https%3A%2F%2Fgraph.microsoft.com%
2 Host: graph.office.net
3 Sec-Ch-Ua:
4 Pragma: no-cache
5 Sec-Ch-Ua-Mobile: ?0
6 Authorization: Bearer {token:https://graph.microsoft.com/}
7 sdkversion: GraphExplorer/4.0
8 Content-Type: application/json
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
10 Cache-Control: no-cache
11 Sec-Ch-Ua-Platform: ""
12 Accept: */*
```



# Presence Lookup via Graph Explorer

Request to https://graph.office.net:443 [52.109.12.142]

Forward Drop Intercept is on Action Open browser

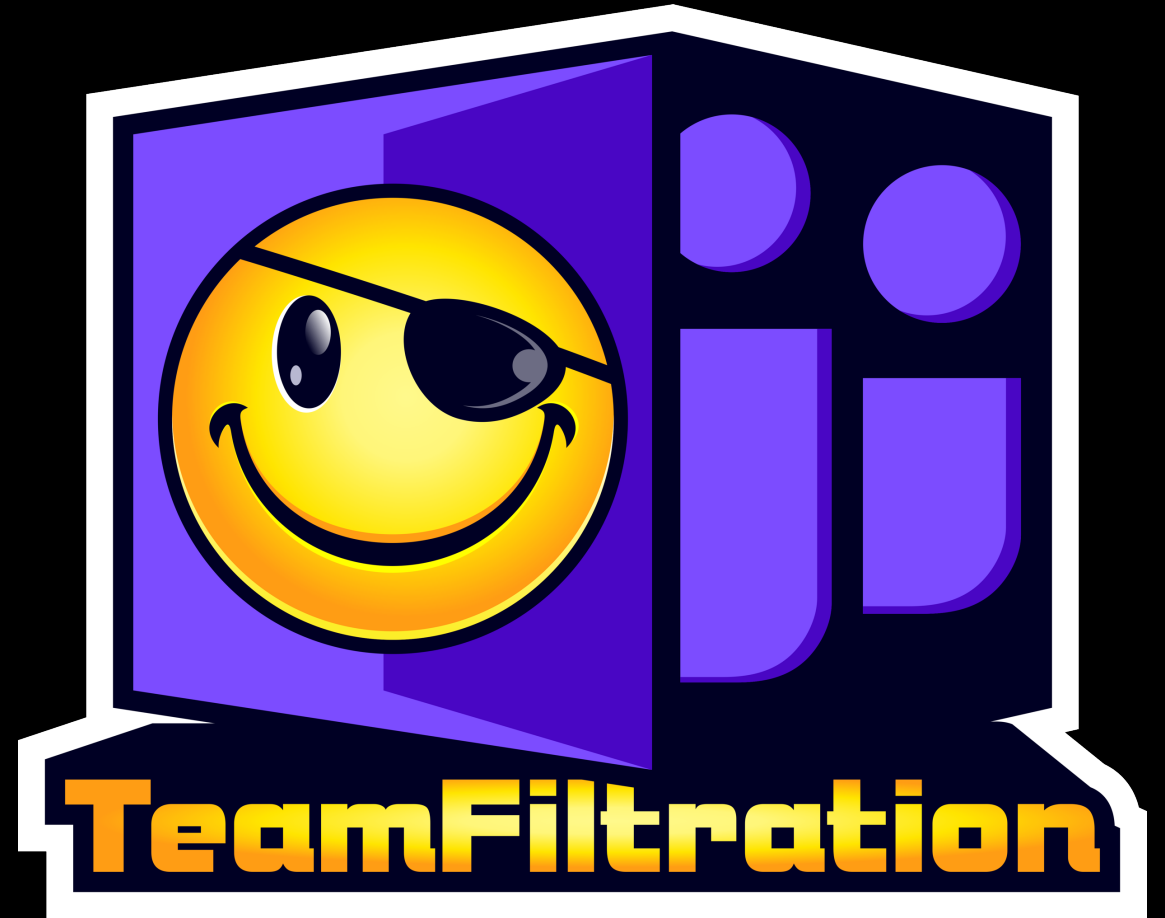
Pretty Raw Hex

```
1 GET /en-us/graph/api/proxy?url=https%3A%2F%2Fgraph.microsoft.com%2Fbeta%2Fusers%2Fd4957c9d-869e-4364-830c-d0c95be72738%2Fpresence HTTP/2
2 Host: graph.office.net
3 Sec-Ch-Ua:
4 Sdkversion: GraphExplorer/4.0
5 Content-Type: application/json
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36
8 Authorization: Bearer {token:https://graph.microsoft.com/}
9 Sec-Ch-Ua-Platform: ""
```



# 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>

```
( '997b8758add6', 'Offline', 'Offline', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '9ab48fa60ea3', 'Available', 'Available', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '28d4376a409f', 'Available', 'Available', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '4bbff197a5c1', 'Offline', 'Offline', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '4cb1ba5c2bc5', 'Away', 'Away', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( 'aa139c386b95', 'Away', 'Away', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( 'b9cc67cd99d9', 'Offline', 'Offline', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '3bded935c6c6', 'Away', 'Away', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '41834ca52377', 'Away', 'Away', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
( '24ca17b3ae66', 'Away', 'Away', 0, 0, 'None', '1682761884', '2023-04-29', 39, 19)
```

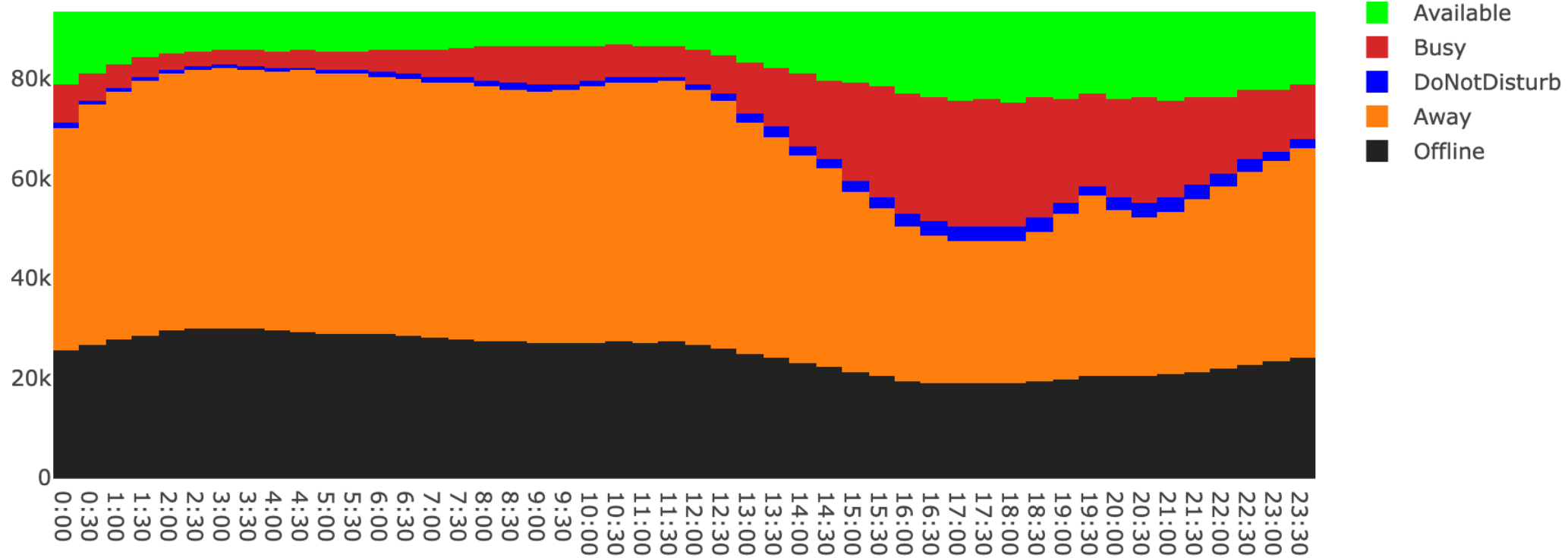
# TRACKING A COMPANY

- 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

Wednesday, May 3, 2023

< 2023-05-03 >  
Normalize

Initial  
Scans

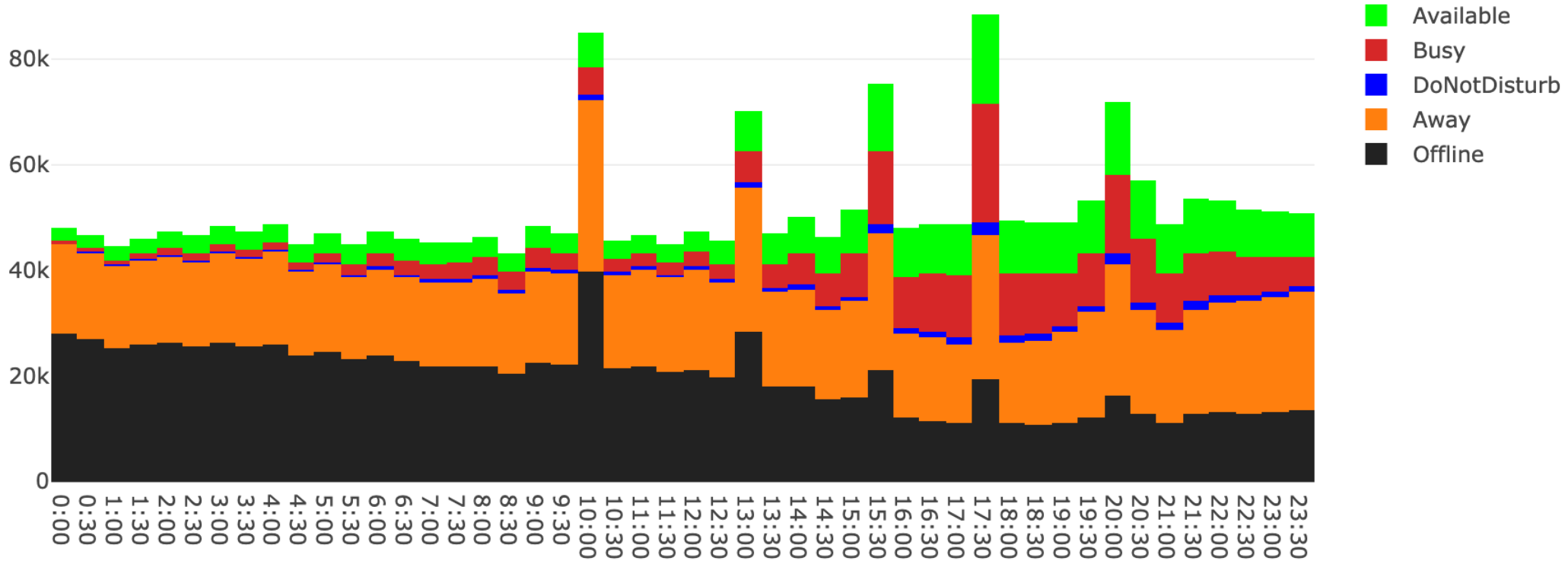


Tracking the Teams Presence of approximately 100,000 Microsoft Employees Every 30 minutes

One week later...

Monday, May 8, 2023

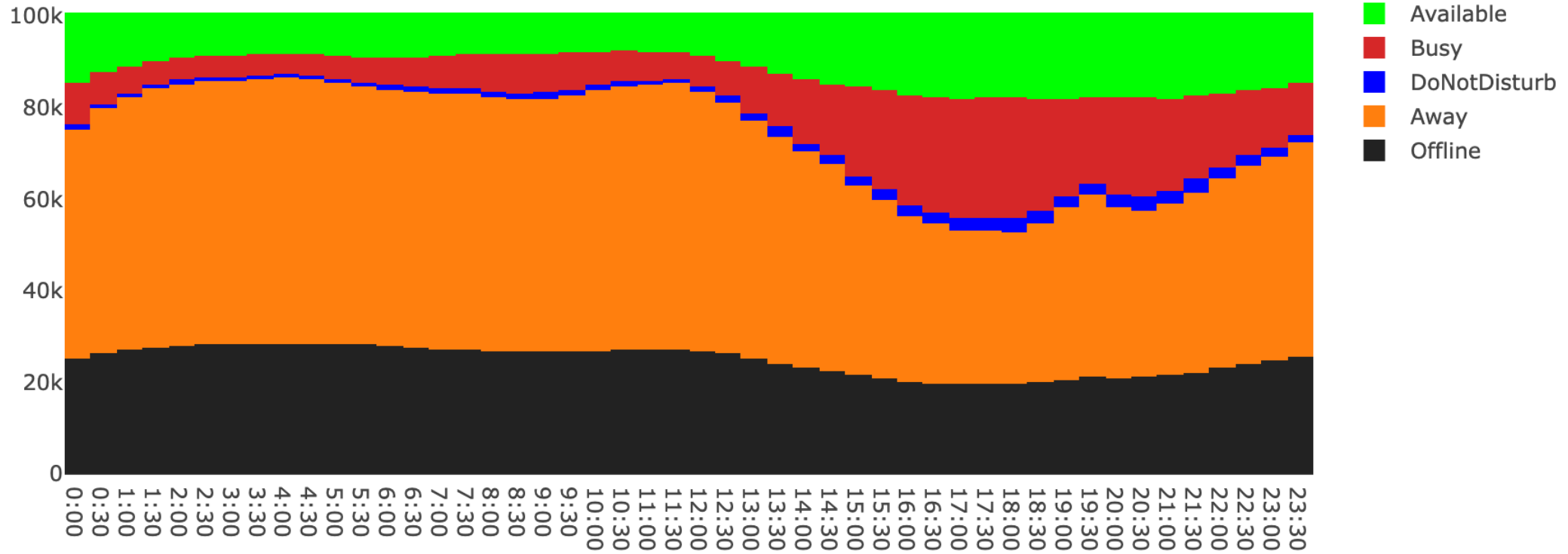
< 2023-05-08 >  
Normalize



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

**Thursday, June 8, 2023**

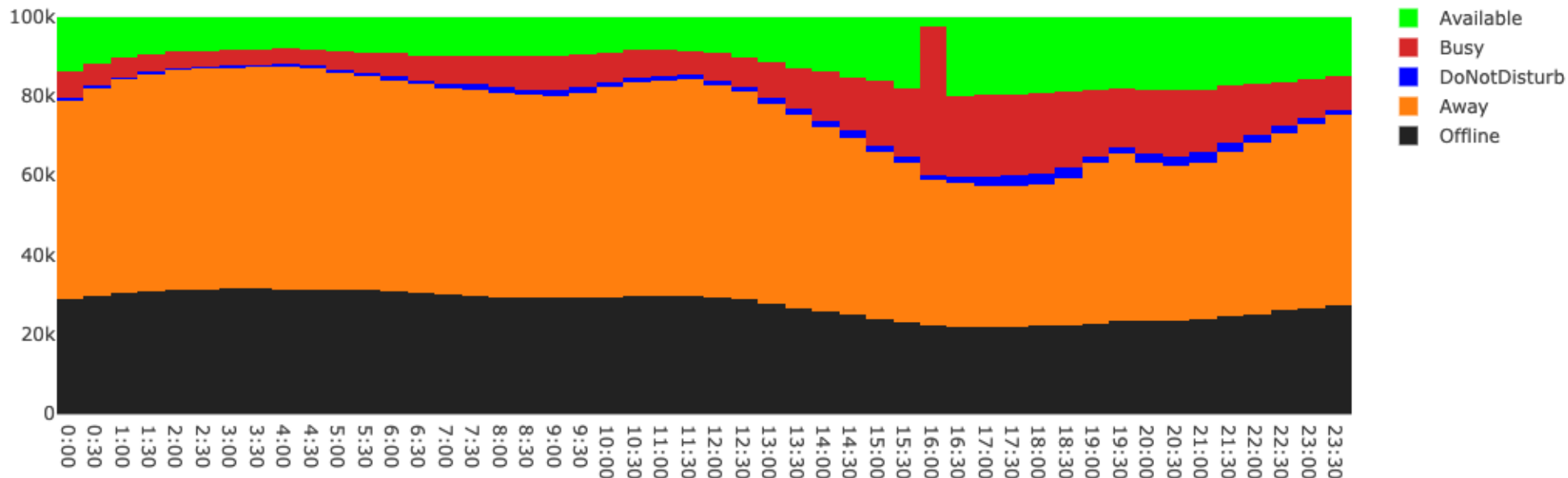
< 2023-06-08 >  
Normalize



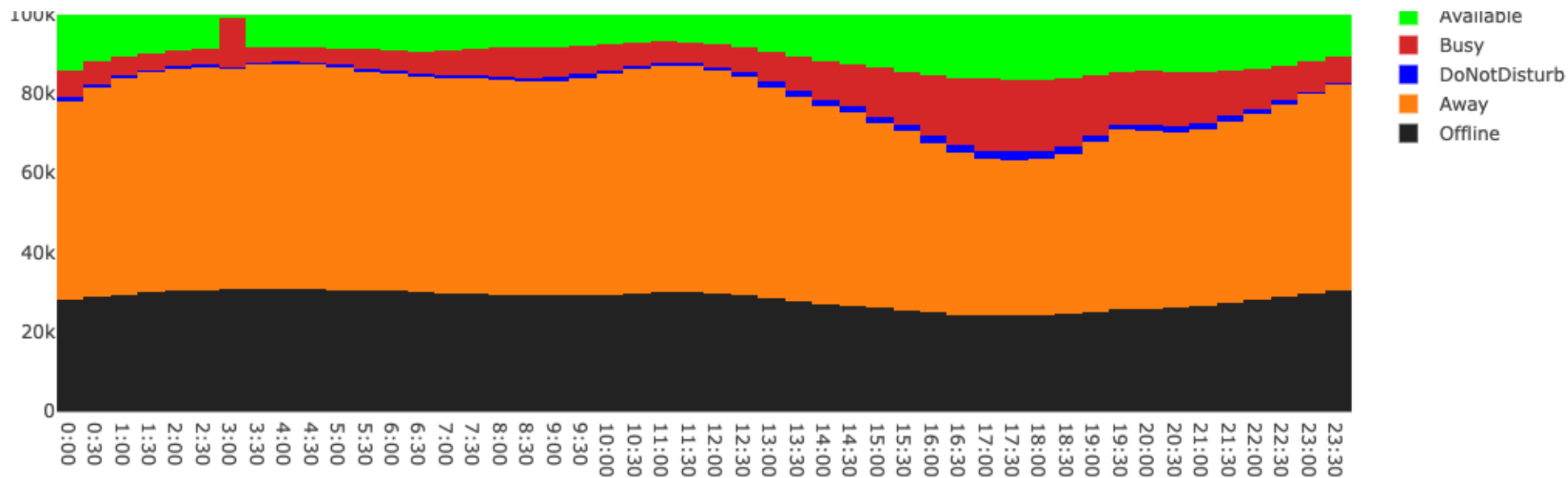
One  
Month  
Later

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

July 6



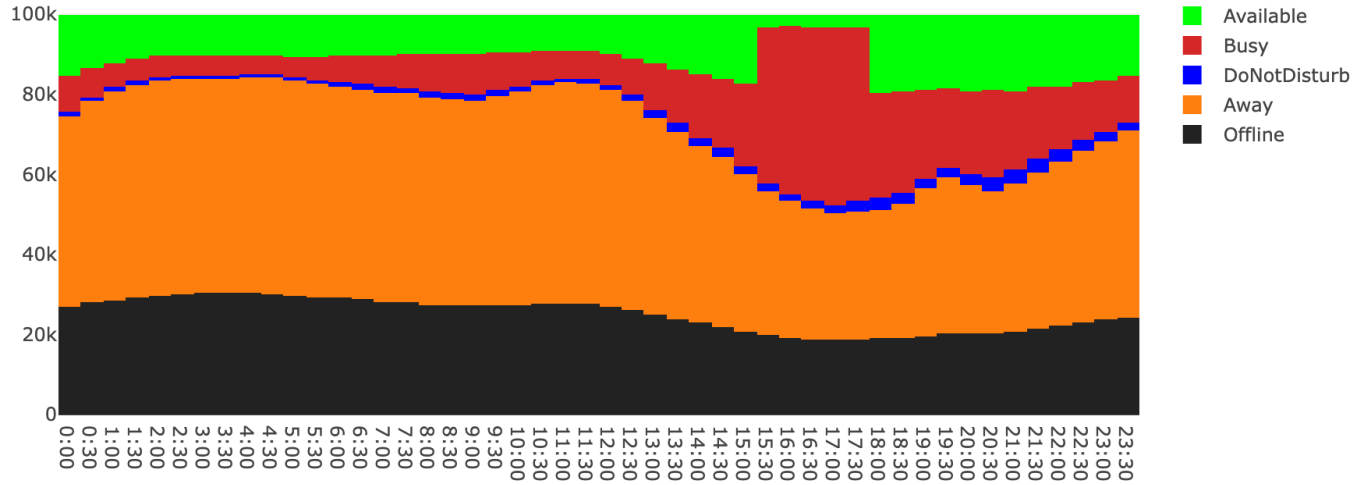
July 7



# Microsoft Build Event

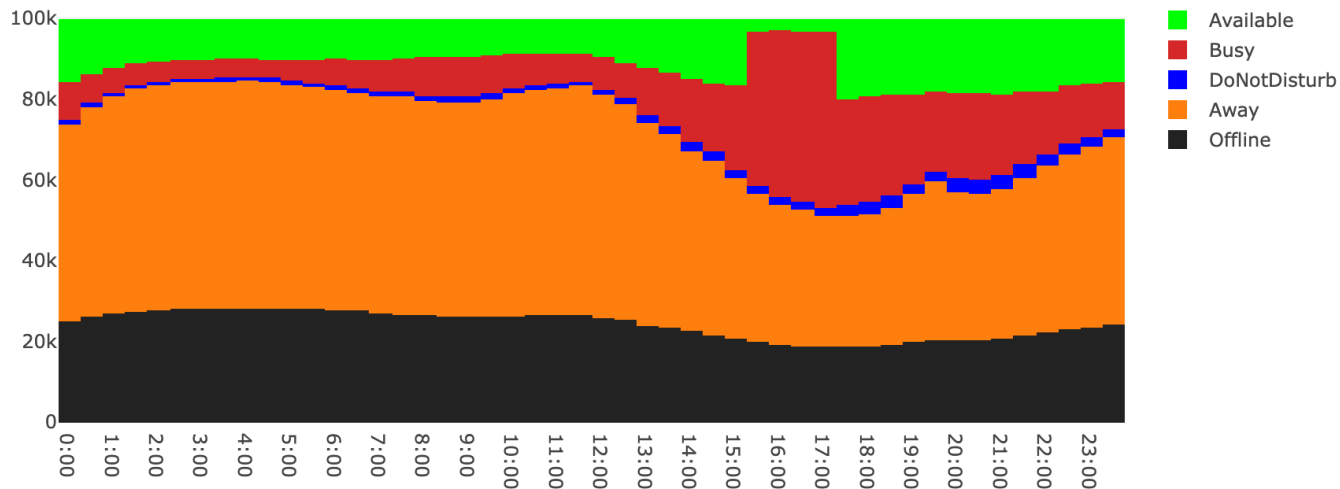
Tuesday, May 23, 2023

< 2023-05-23 >  
Normalize




Wednesday, May 24, 2023


< 2023-05-24 >  
Normalize




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](https://msft.it/60105ljg6)



Microsoft

OPENING KEYNOTE  
Satya Nadella

Registration now open

Microsoft Build

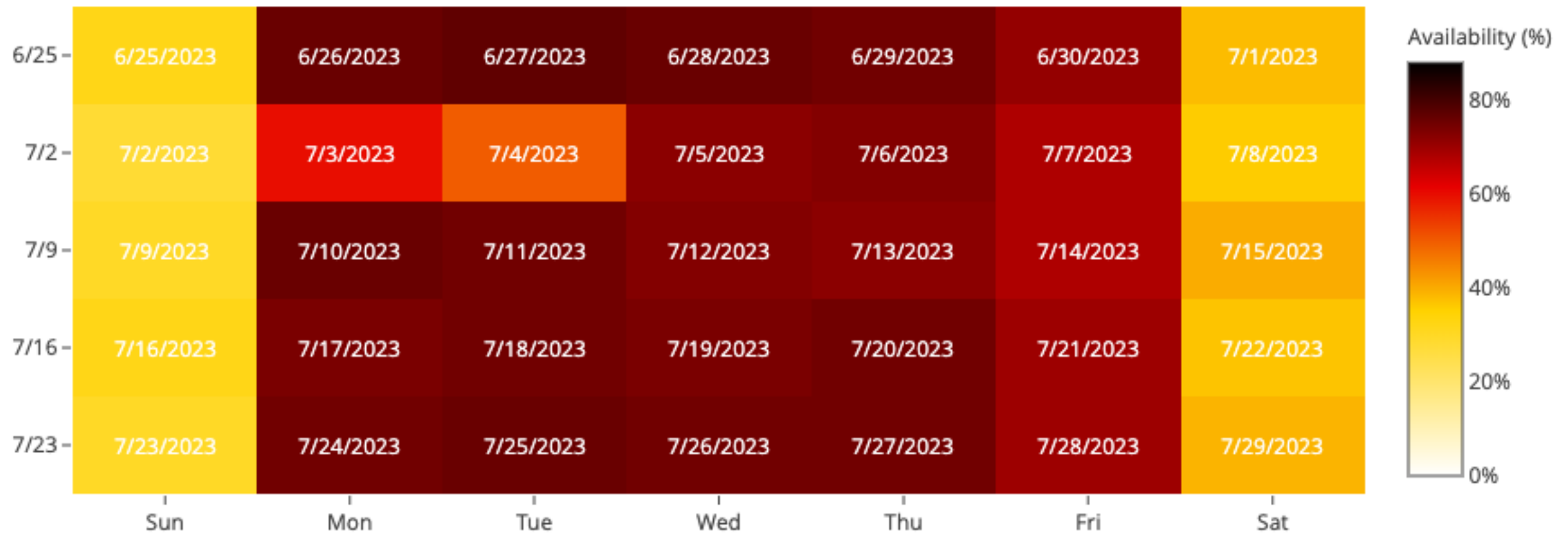
1:00 PM · Mar 14, 2023 · 211.2K Views



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

**- MSRC**

## Total Daily Available Users





# 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?

		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 4<sup>th</sup> 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



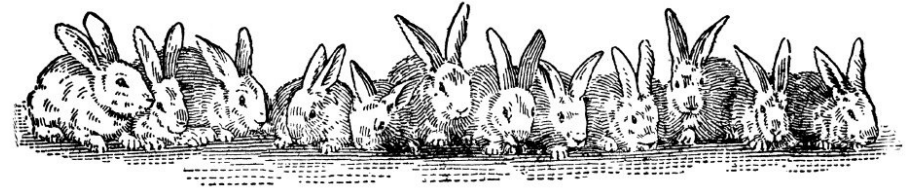
CATS : ALL YOUR GUEST ARE BELONG  
TO US.



# Overview

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

Hey, it's only user enumeration!



## Guest Enumeration

In a Nutshell


# 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 Computers** 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	<a href="#">acmecomputercompany.onmicrosoft.com</a>
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**

# 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

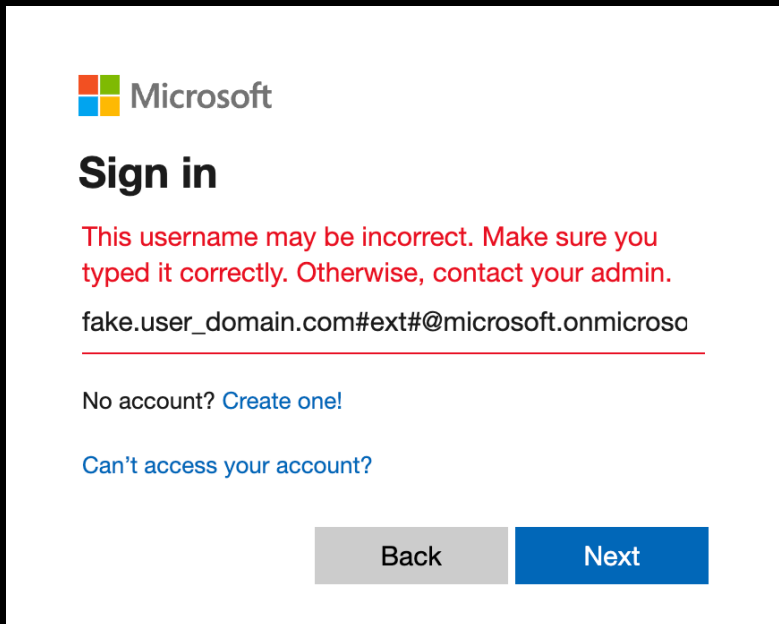
So, what is the big deal? Using the **GetCredentialType** API, one can find valid user accounts of the tenant and focus password-spray attack on those. Not so surprisingly, as Oliver Morton mentioned in his [blog](#), Microsoft does not regard the enumeration to be an issue because the potential attacker 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 '\_'

# Nestori's Silent Enum

Valid

Invalid



Microsoft

## Sign in

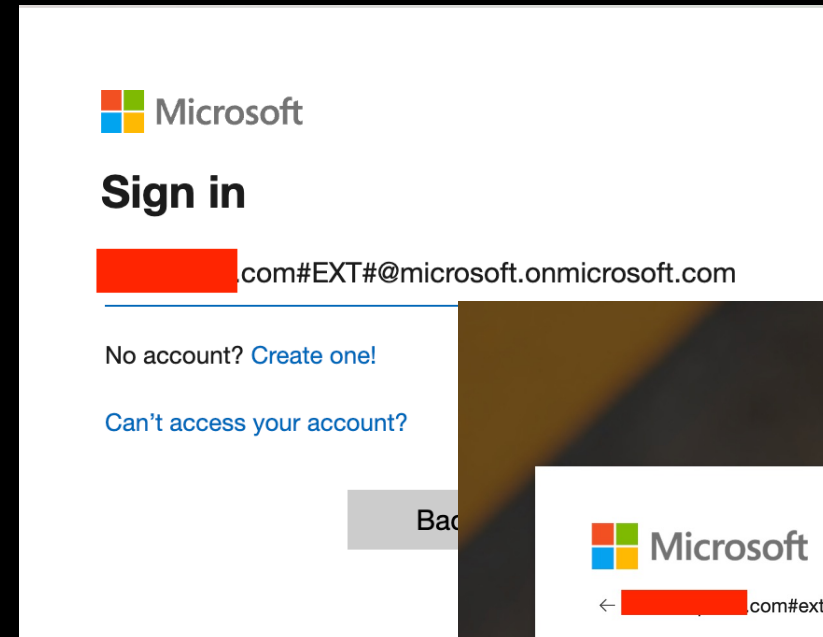
This username may be incorrect. Make sure you typed it correctly. Otherwise, contact your admin.

fake.user\_domain.com#ext#@microsoft.onmicroso

No account? [Create one!](#)

[Can't access your account?](#)

[Back](#) [Next](#)



Microsoft

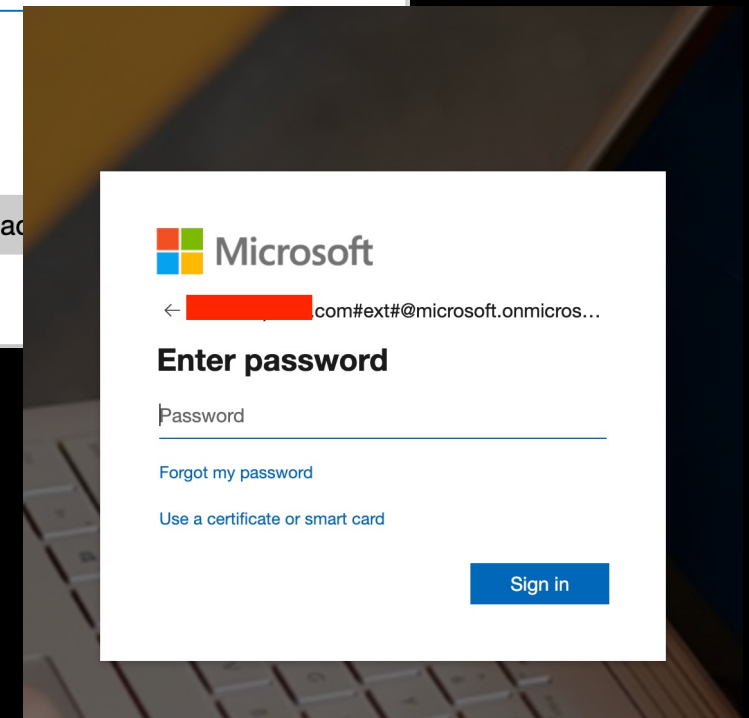
## Sign in

[redacted]com#EXT#@microsoft.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Back](#)



Microsoft

[← \[redacted\]com#ext#@microsoft.onmicros...](#)

## Enter password

Password

[Forgot my password](#)

[Use a certificate or smart card](#)

[Sign in](#)

# 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!

← → ↻ big4accountingfirms.com/ernst-and-young-clients/

## EY Clients 2022

A listing of Ernst and Young's largest clients is included. We provide some background about the client and if they are a current auditor. We also provide the amount of fees received from some of the clients.

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

# Identifying Public Partnerships

← → ↻ 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



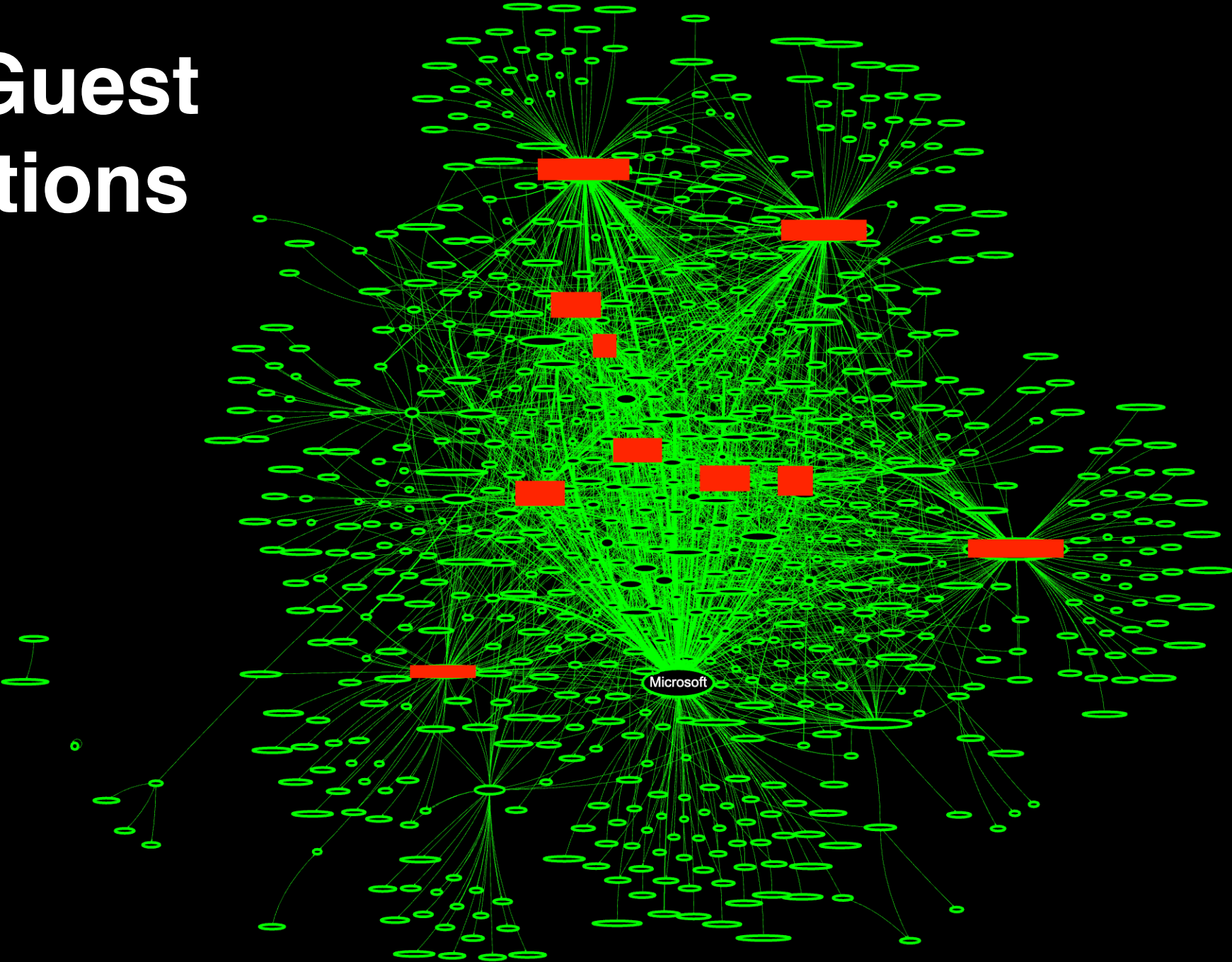
**SECURITY**

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

 BY MIKE WHEATLEY



# 30,000 Guest Connections



# Discovered Guest Accounts Involving:

Redacting  
at  
Microsoft's  
Request

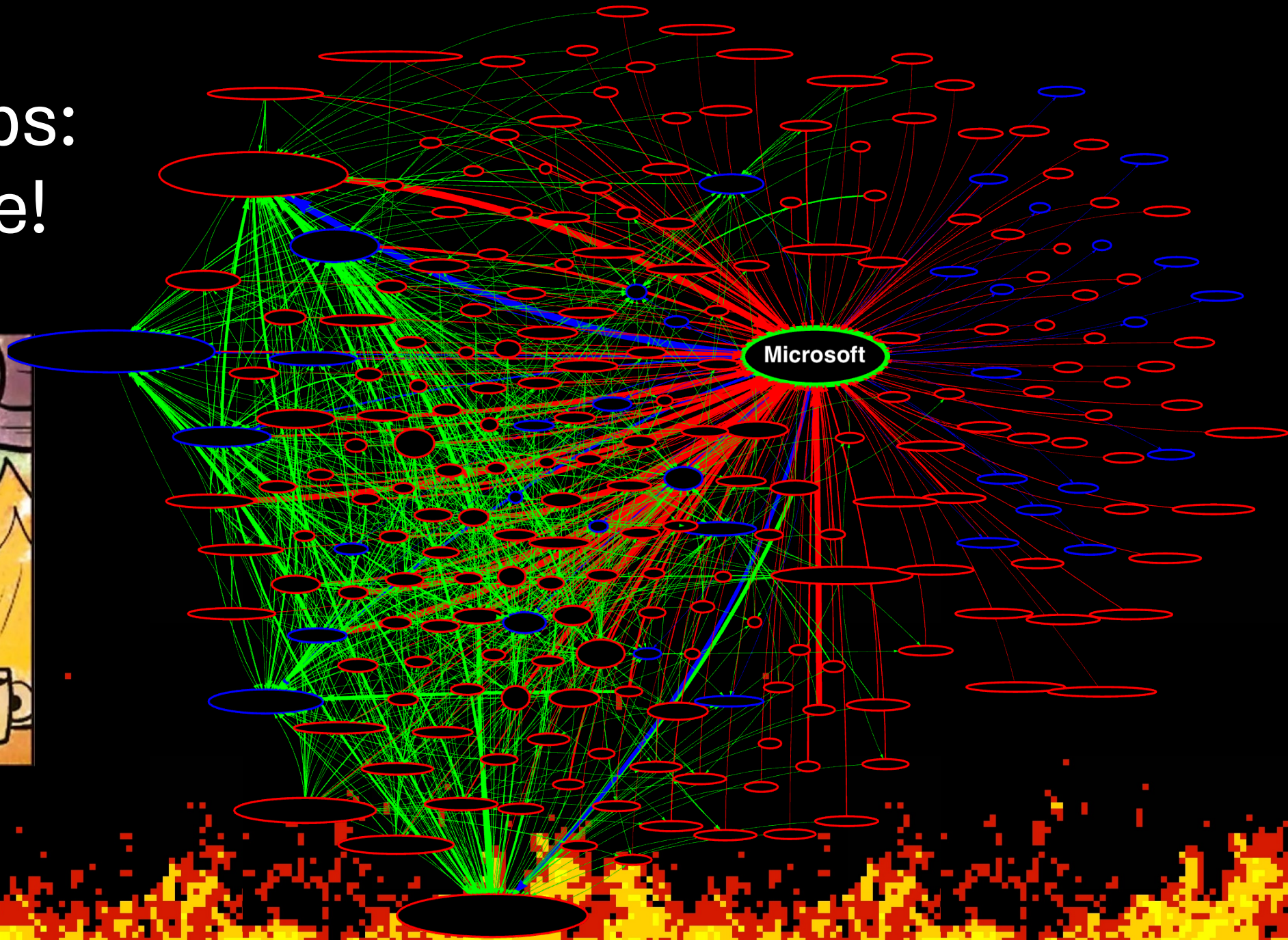
This is publicly  
available  
information

- 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

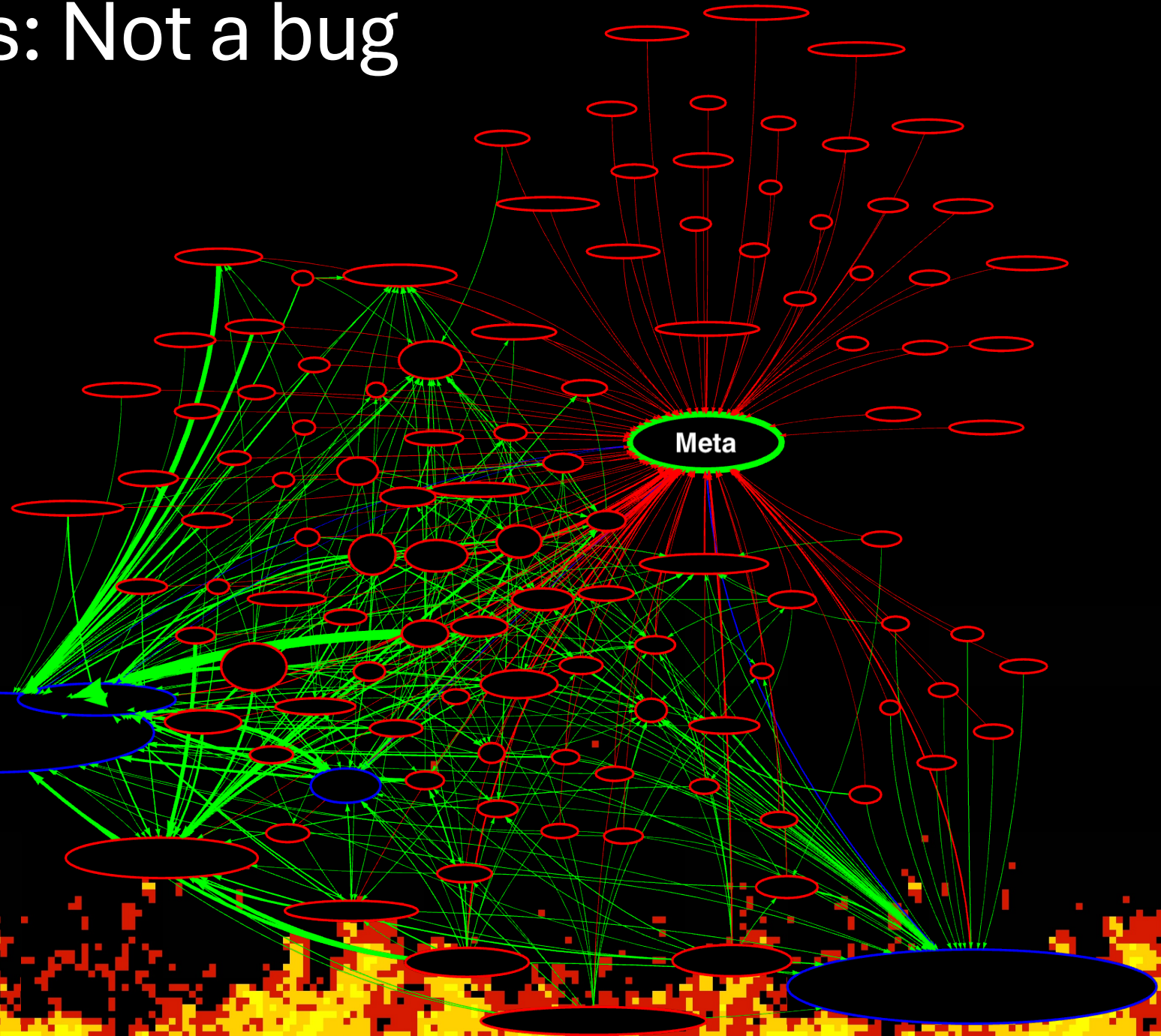
← → ↻ [microsoft.com/en-us/msrc/bounty-online-services?rtc=1](https://microsoft.com/en-us/msrc/bounty-online-services?rtc=1)

## OUT OF SCOPE SUBMISSIONS AND VULNERABILITIES

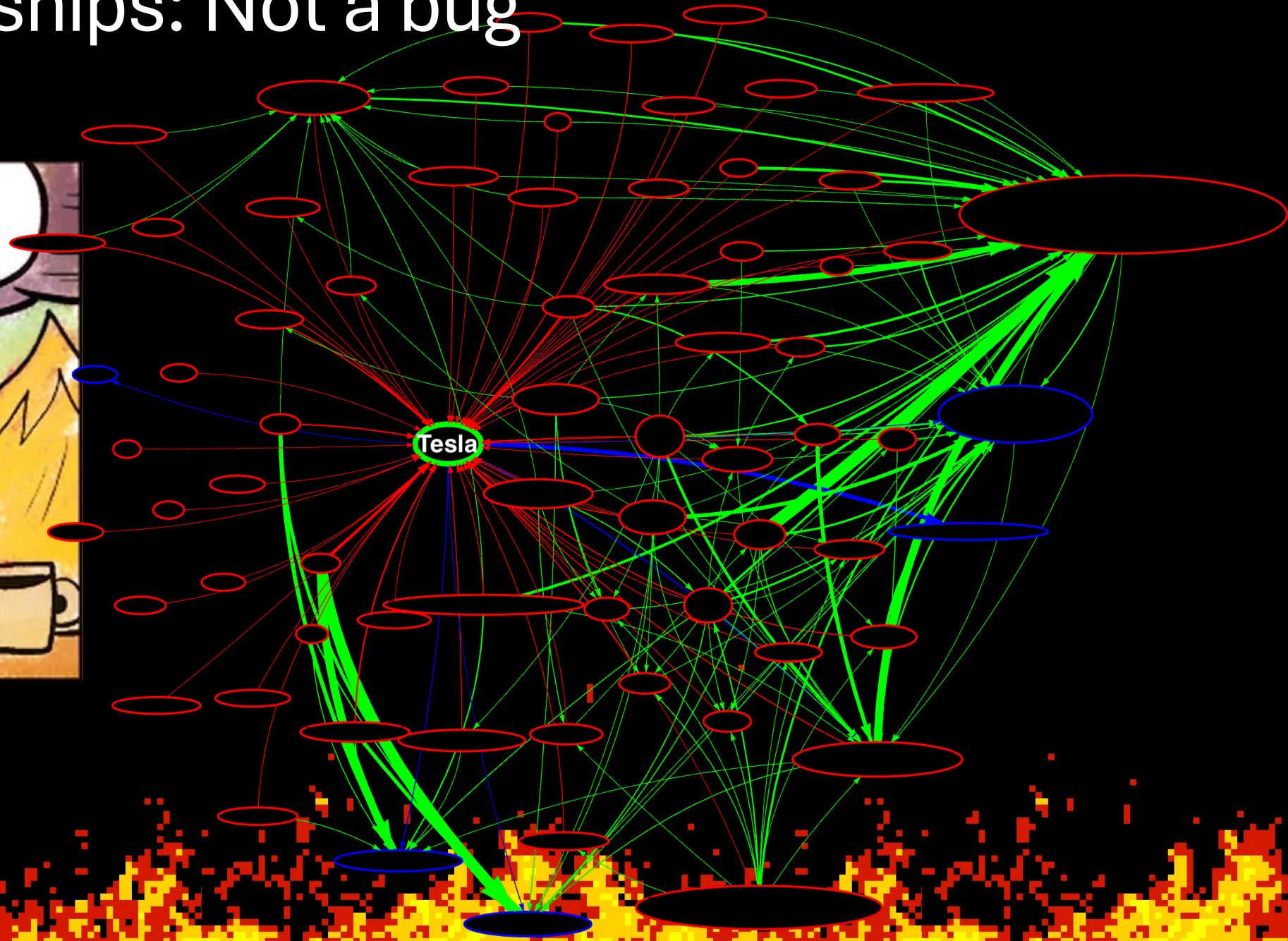
- Security misconfiguration of a service by a user, such as the enabling of HTTP access on a service
- Missing HTTP Security Headers (such as X-FRAME-OPTIONS) or cookie security flags (such as Secure, HttpOnly, SameSite)
- Vulnerabilities used to enumerate or confirm the existence of users or tenants



# Meta Relationships: Not a bug

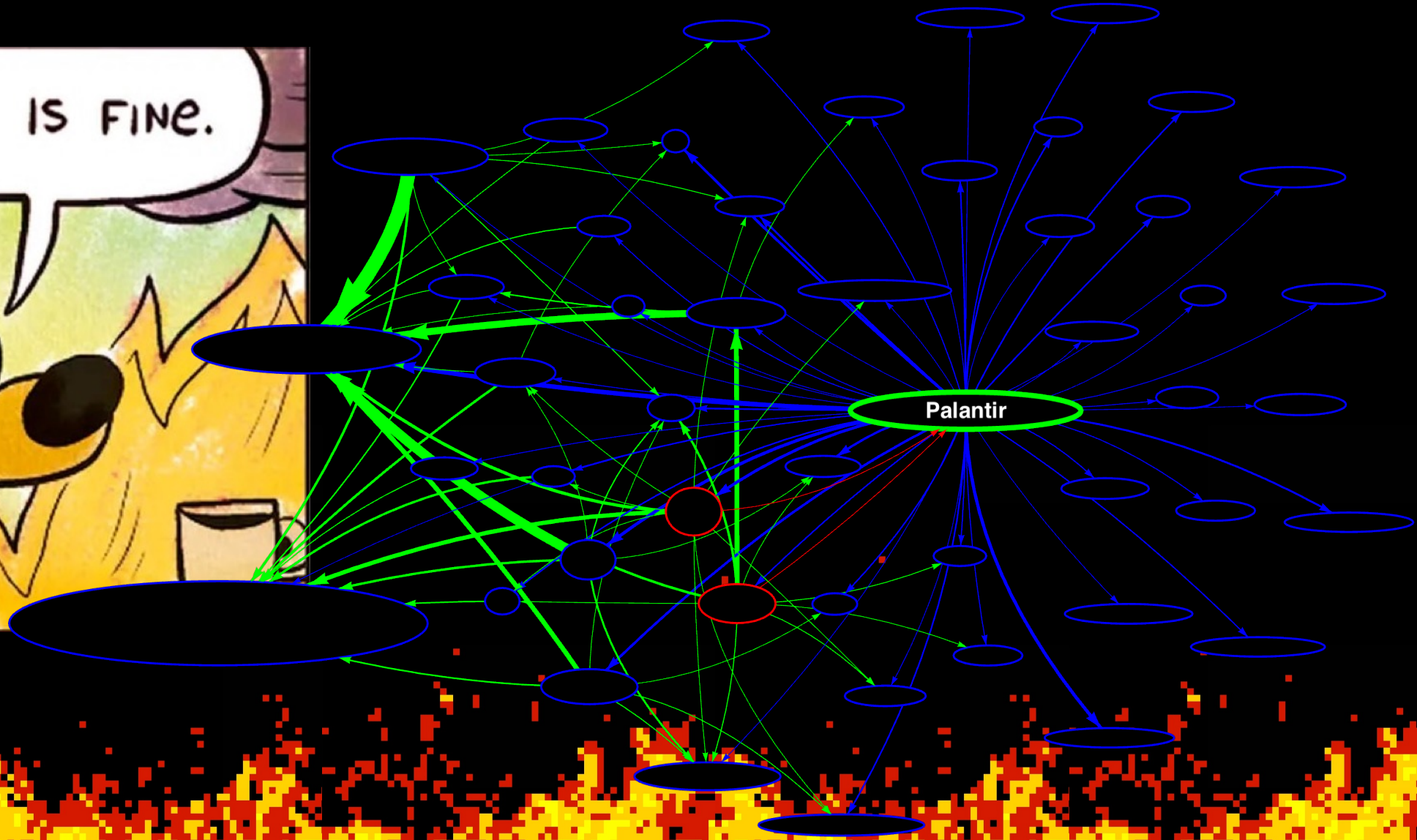


# Tesla Relationships: Not a bug





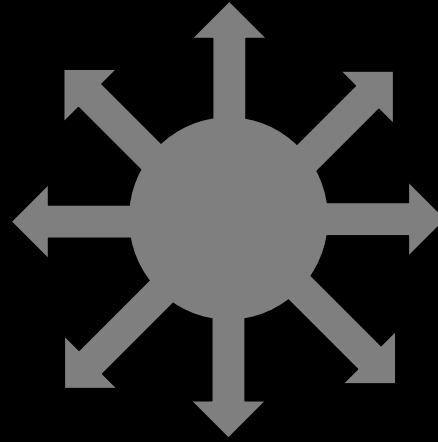
# Palantir Relationships: Just User Enum





# 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

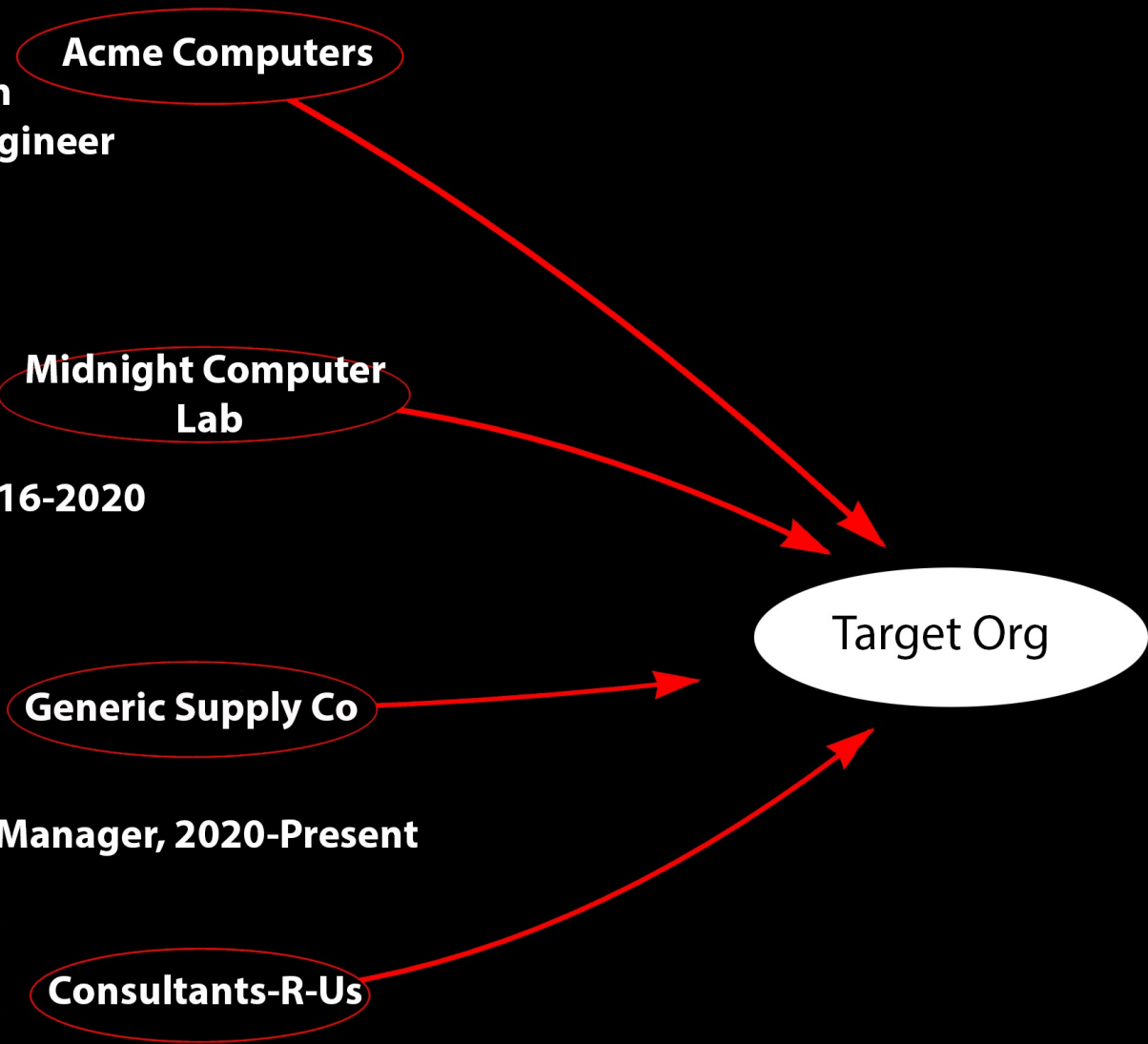
**Generic Supply Co**



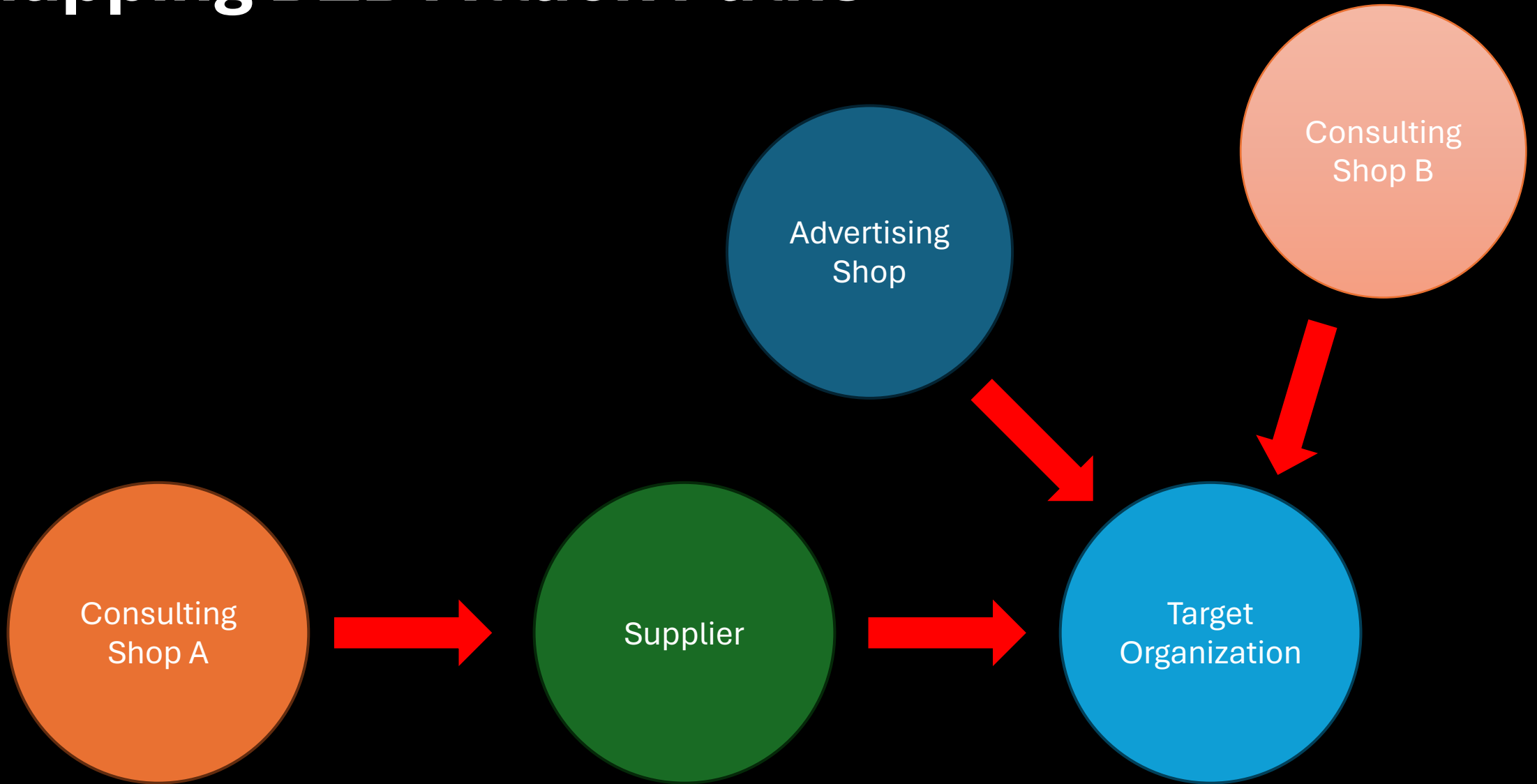
**David Lightman**  
Security Consultant, 2021-2023

**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

- Special thanks to the EFF!



# More Information

[https://github.com/nyxgeek/onedrive\\_user\\_enum](https://github.com/nyxgeek/onedrive_user_enum)

<https://github.com/nyxgeek/teamstracker>

<https://github.com/nyxgeek/guestlist>

@nyxgeek on twitter



# More Information

## External Access:

<https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings>

## Leaving an Organization as a Guest:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/leave-the-organization>