



What We Assume

A Presentation About Identity, Zero Days, and Raccoons

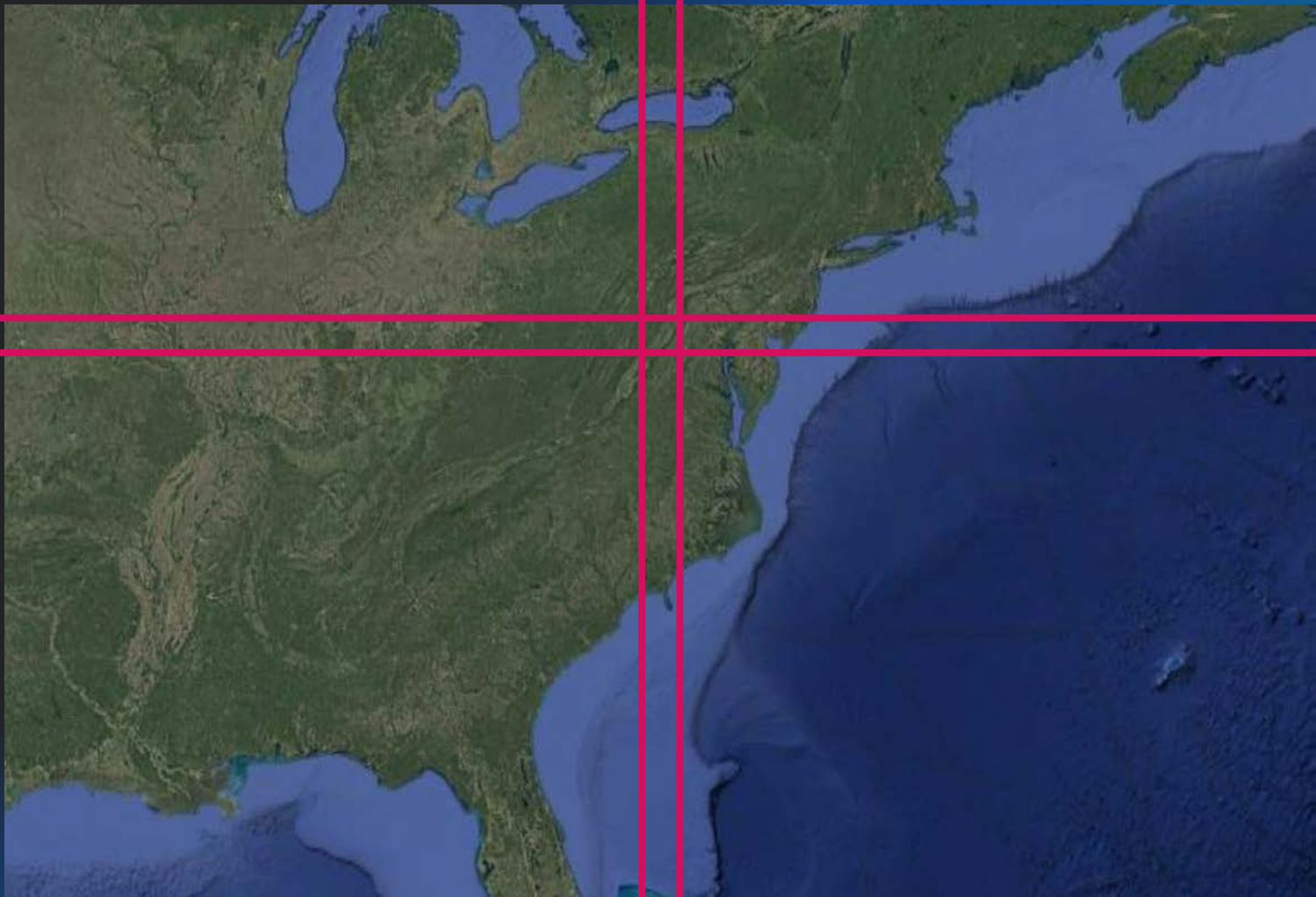


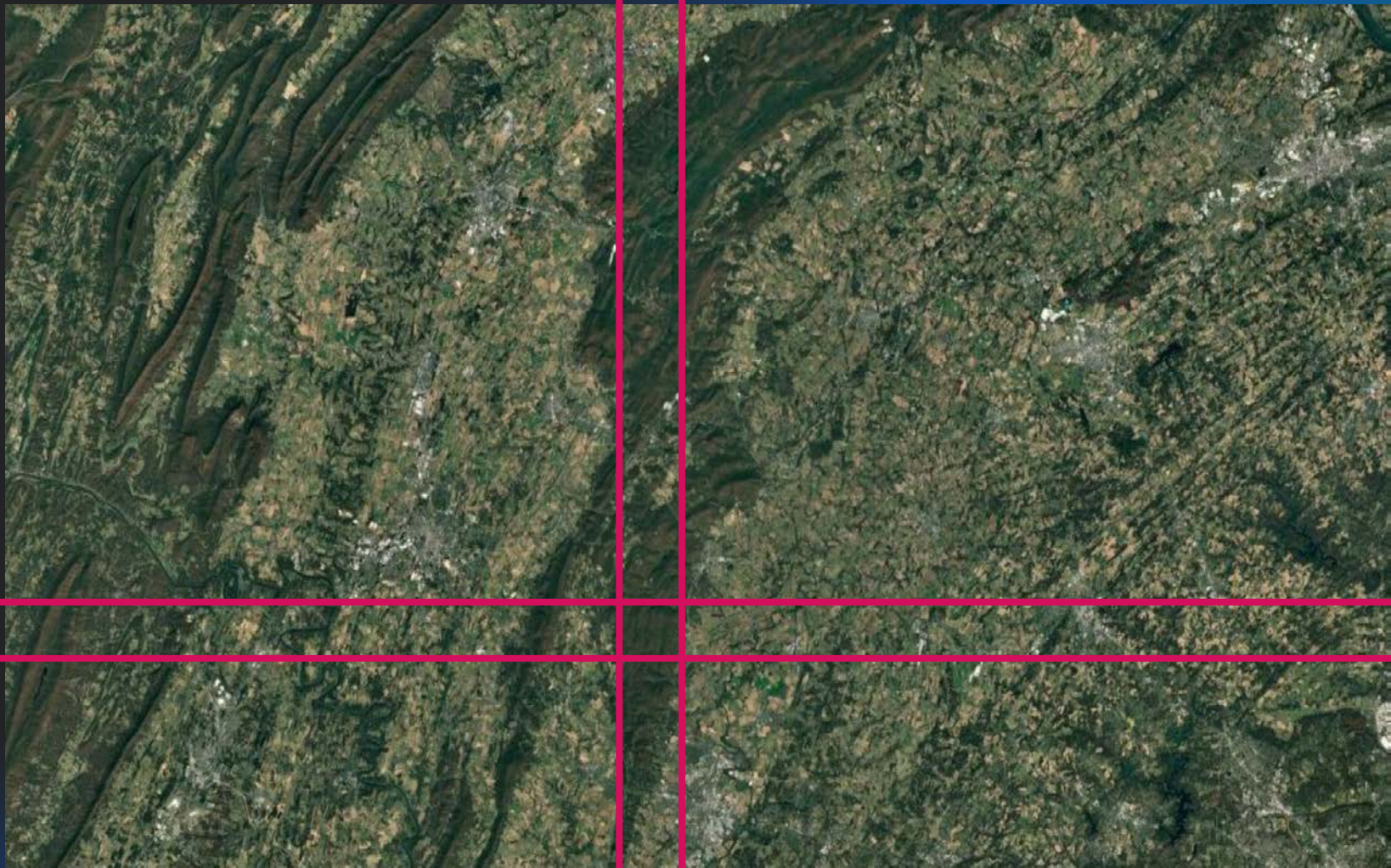
Matthew Kiely

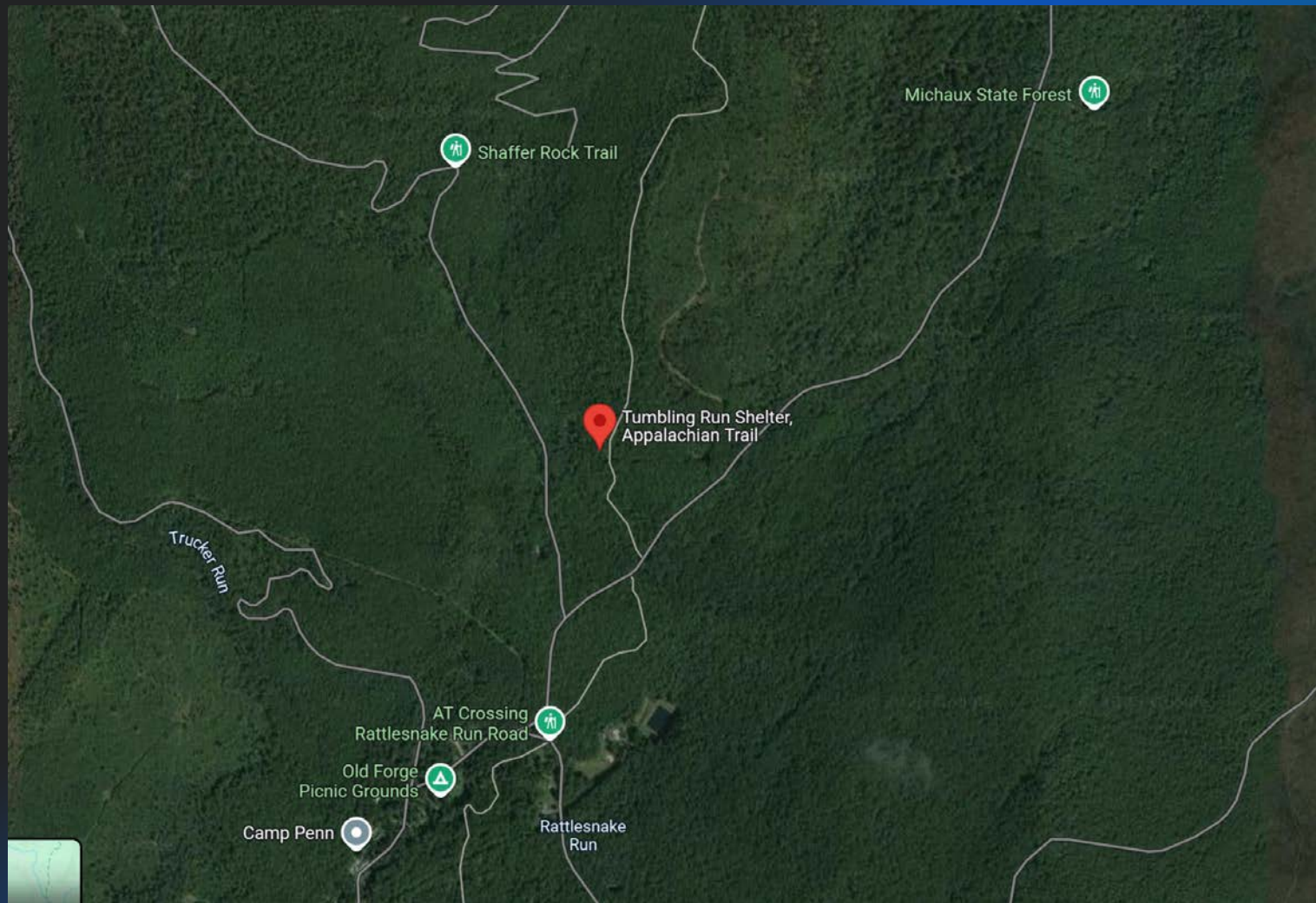
Principal Security Researcher
Huntress

- Lead researcher for Huntress Identity Threat Detection & Response
- Red teamer, malware reverse engineer
- 12+ years in system/network administration, offensive security research, and malware reverse engineering
- Formerly: MIT Lincoln Laboratory, SimSpace, USMC

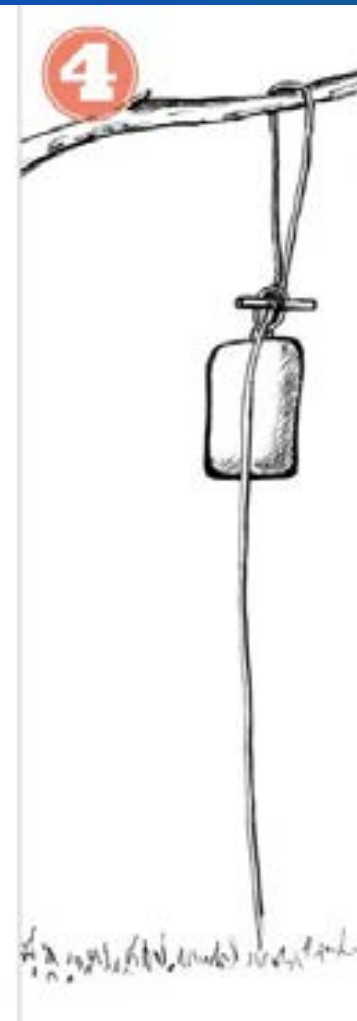
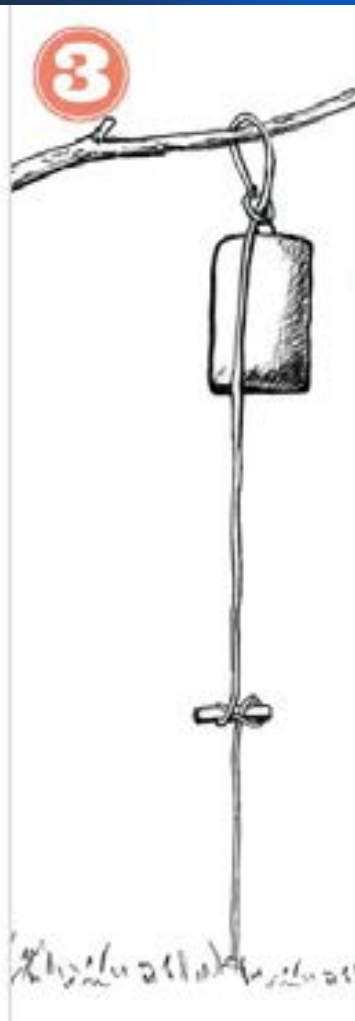
The worst breach I ever experienced...











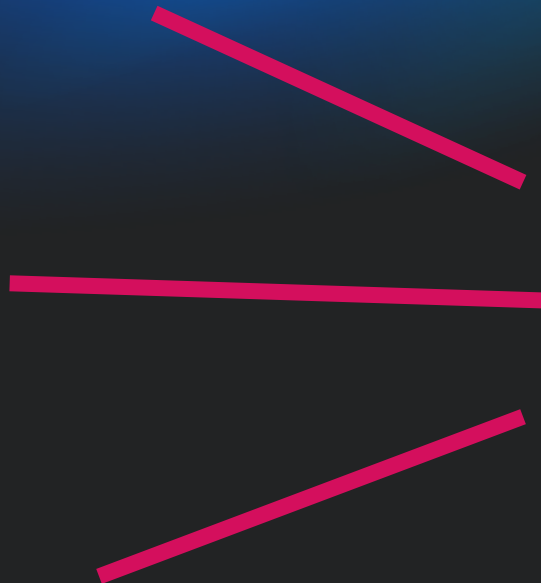




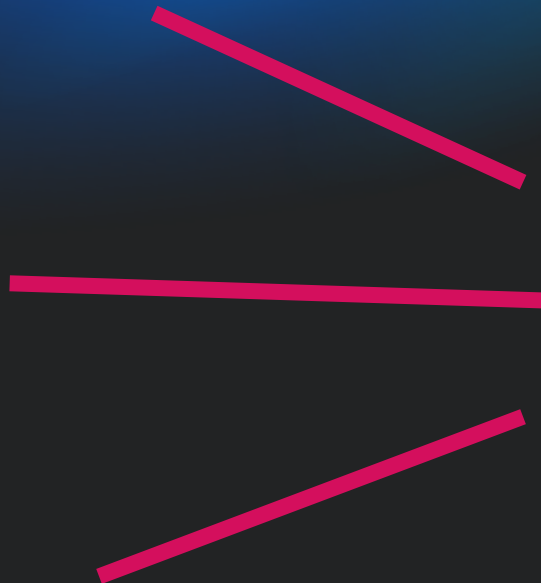




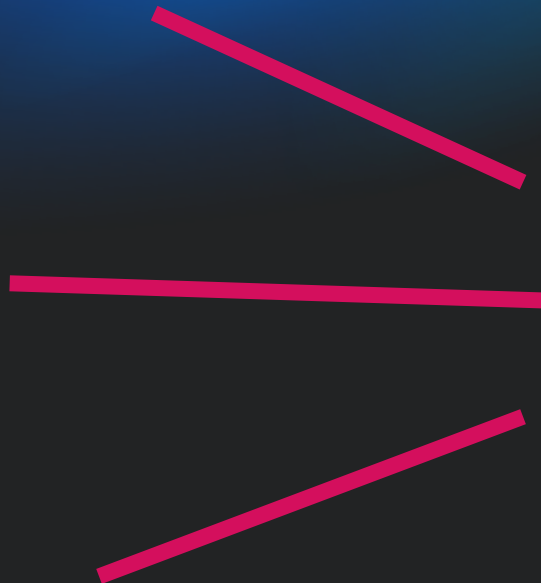
April 22, approx. 11:45pm



April 22, approx. 11:45pm



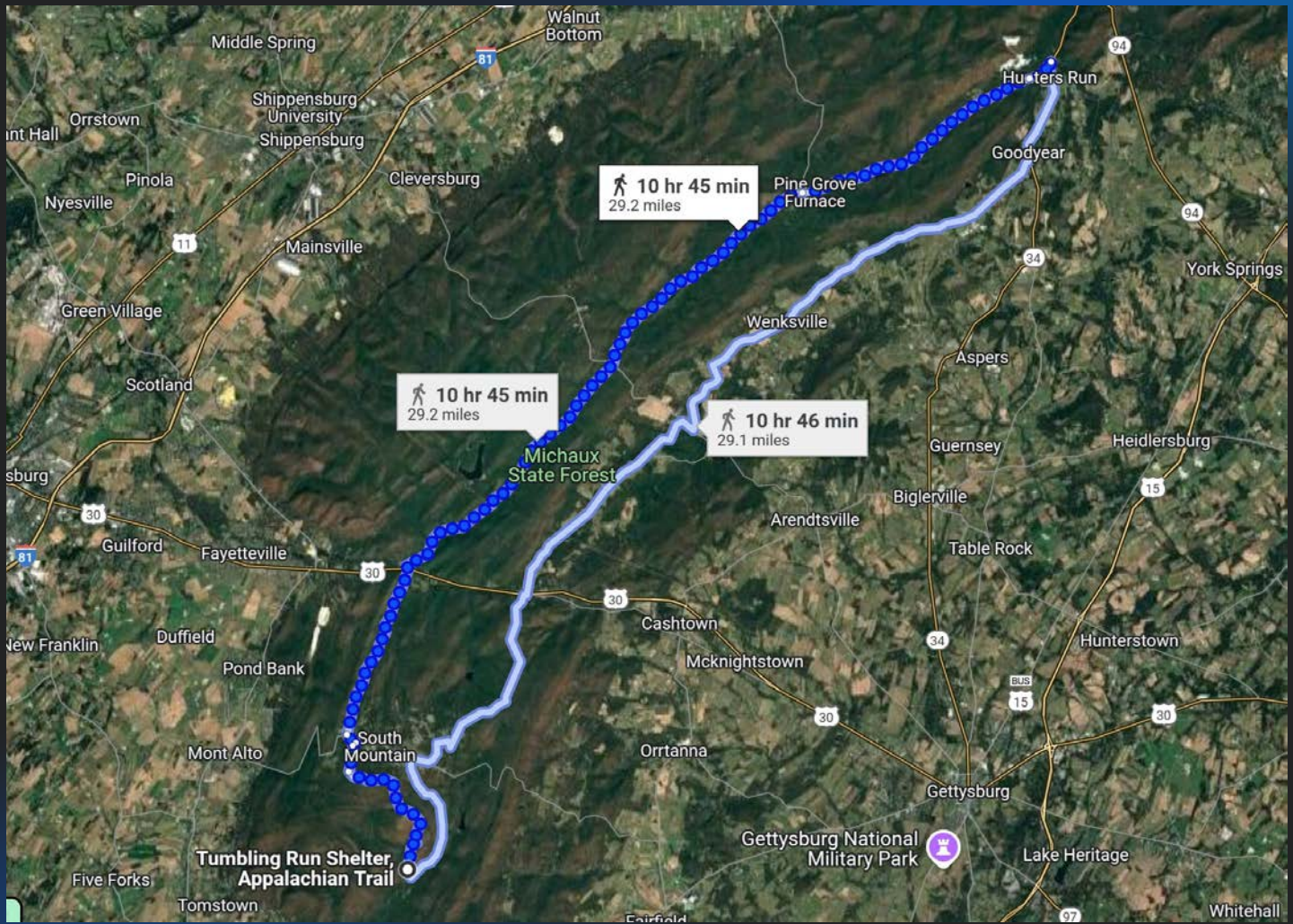
April 22, approx. 11:45pm



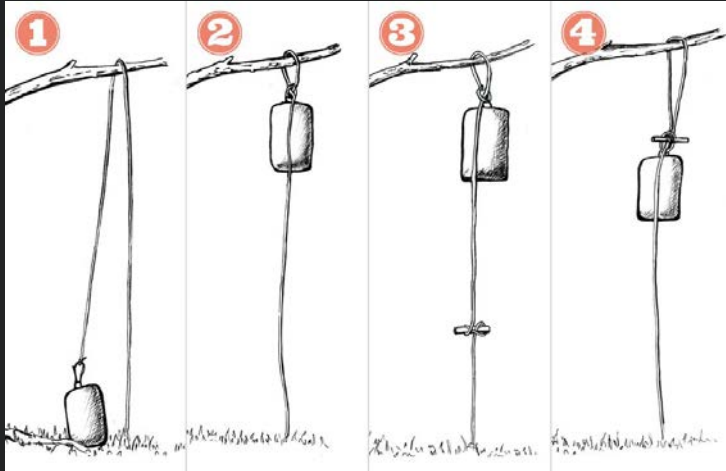
April 22, approx. 11:45pm

The next morning...





... what does this have to do with cybersecurity, Matt?





Even throughout hundreds of miles of backcountry hiking, when my life was boiled down to food, water, shelter, and walking in a straight line, I could not escape **threat modeling**, **risk mitigation**, and (most importantly) my **assumptions**.

assumptions.

Zero Worry ^ Day

Assumption

I should be concerned about zero days

You should be concerned about zero days...

... but not even *close* to as concerned as you probably are.

February 23, 2024

SlashAndGrab: ScreenConnect Post-Exploitation in the Wild (CVE-2024-1709 & CVE-2024-1708)

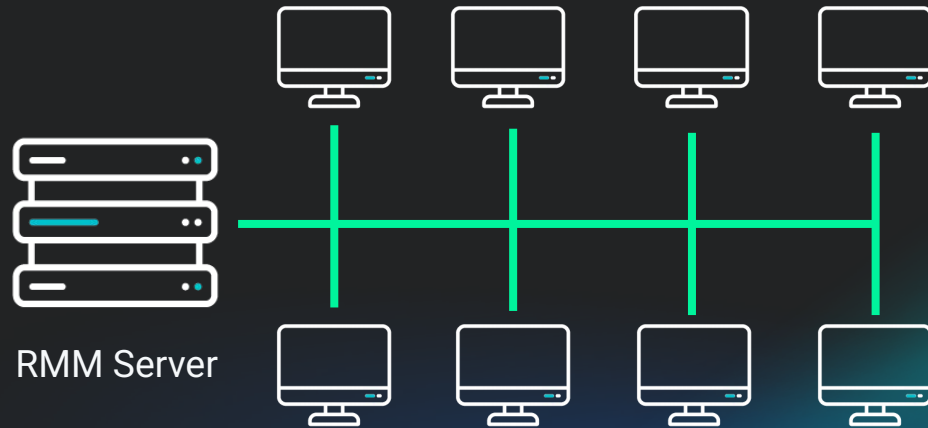
By Team Huntress

Share



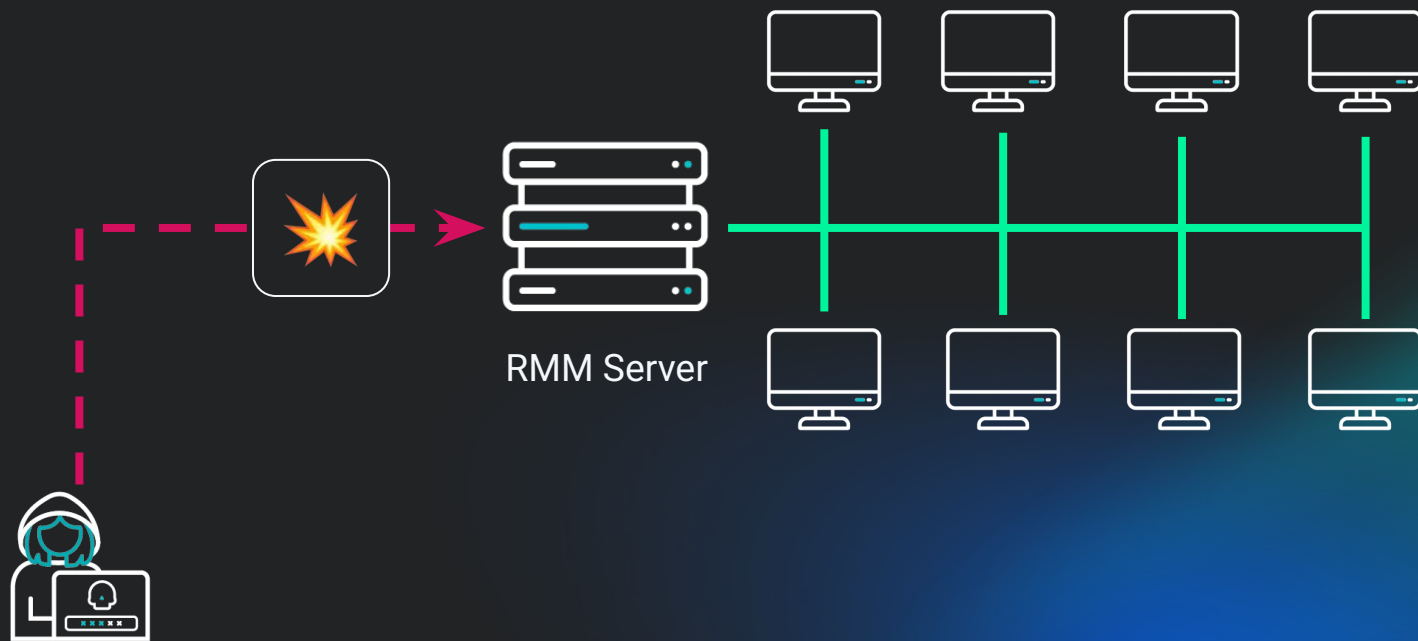
Table of Contents:

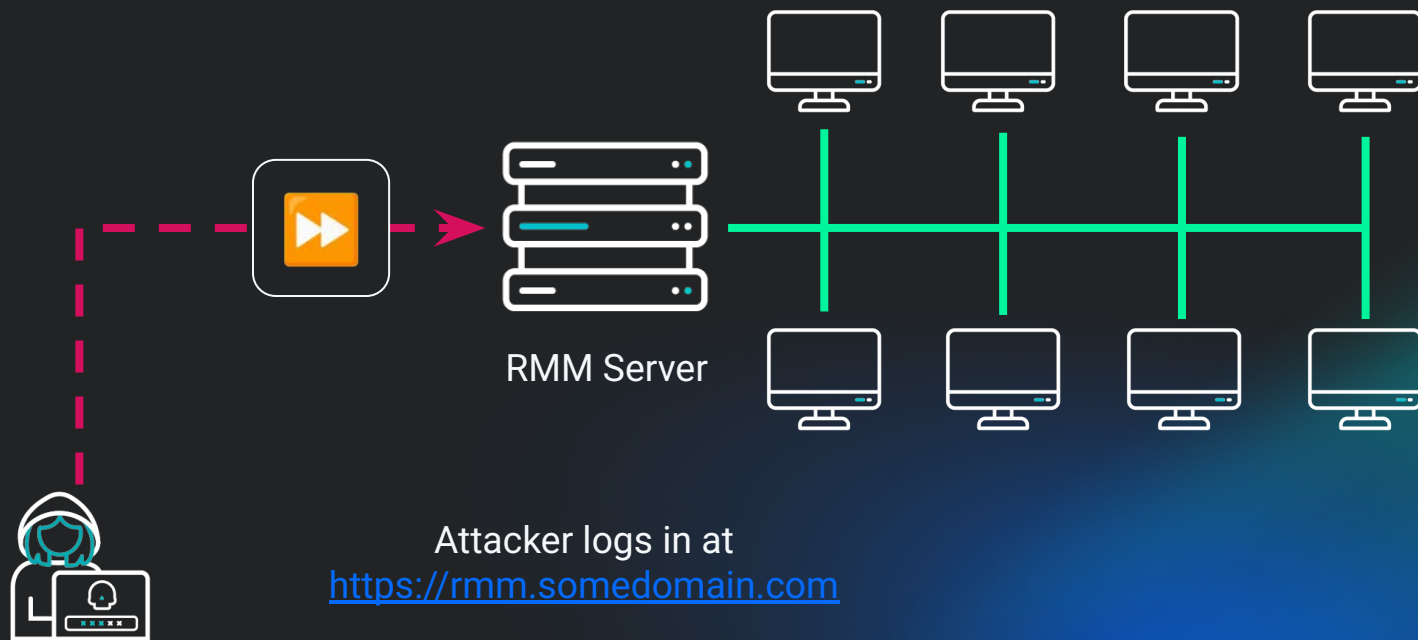
- [Adversaries Deploying Ransomware](#)
- [Adversaries Enumerating](#)
- [Adversary Cryptocurrency Miners](#)
- [Adversaries Installing Additional Remote Access](#)
- [Downloading Tools and Payloads](#)
- [Adversaries Dropping Cobalt Strike](#)
- [Adversaries Persisting](#)
- [Wrapping Up](#)

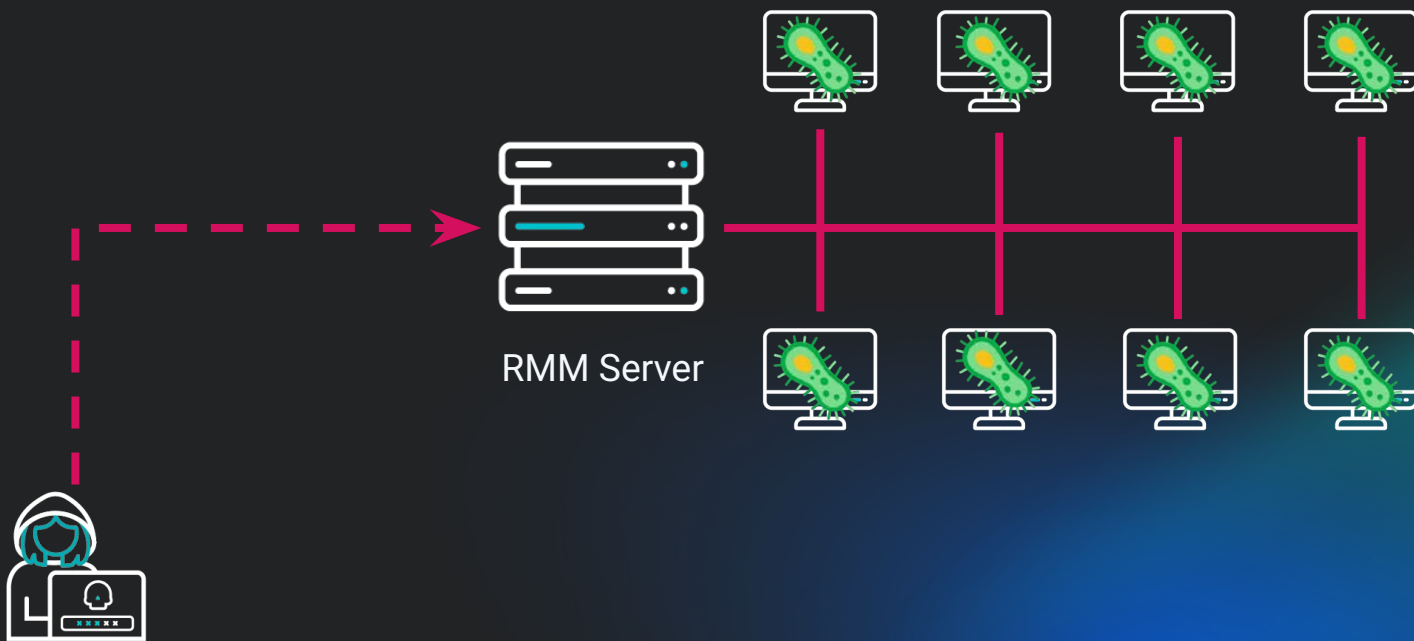


RMM Server





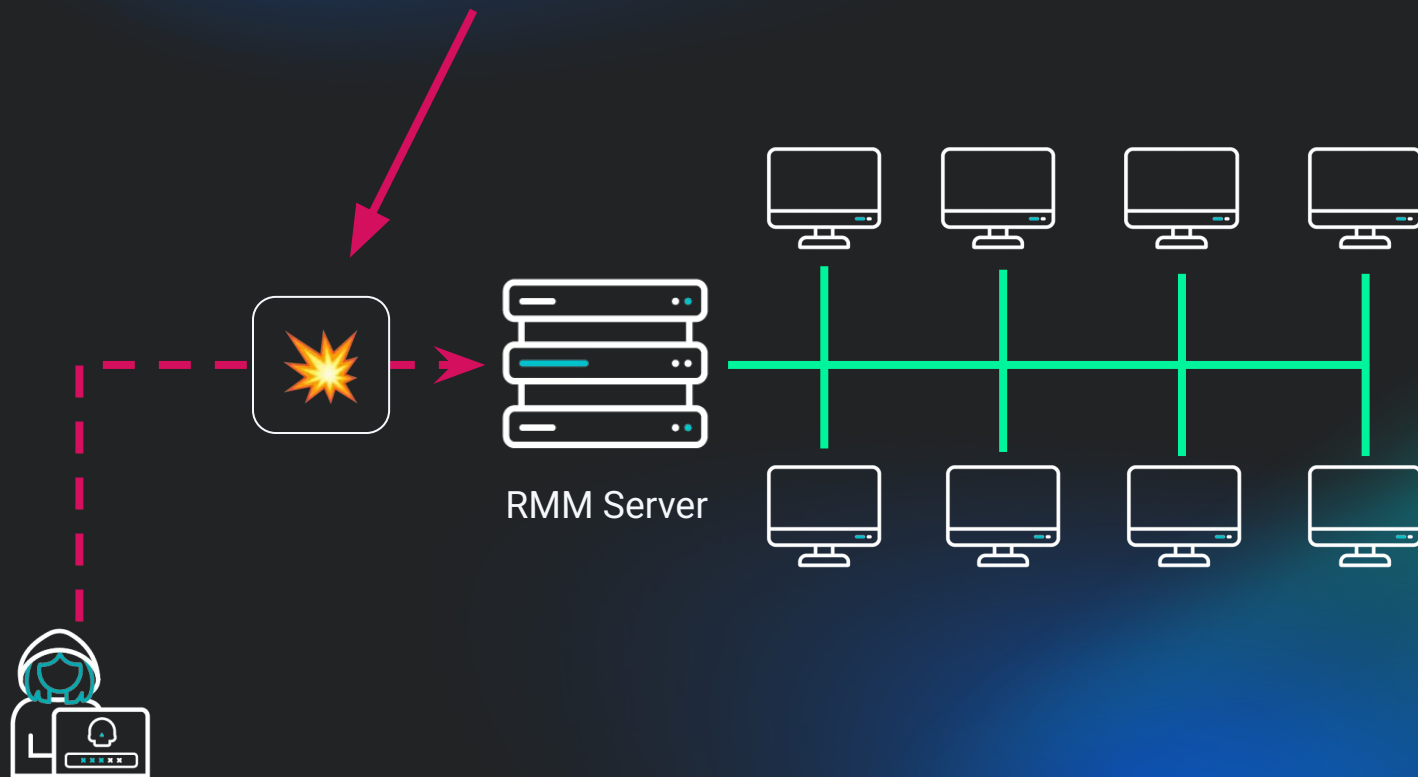


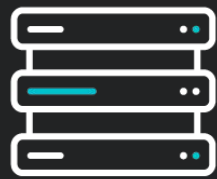


This incredibly interesting ScreenConnect exploit has enamored many of us at Huntress for the last few days, but it's a shame our adversaries didn't commit to pairing this new exploit with *new* tradecraft.

It's worth driving this point home: **most of the post-compromise activities we have documented in this article aren't novel, original, or outstanding.** Most threat actors simply don't know what to do beyond the same usual, procedural tradecraft; **cybercriminals are rarely sophisticated**, and the infosec community can beat them together.

You may have no control over stopping this part...





RMM Server



But *everything* they do once they get in the door is usually predictable

[Home](#) > [Blog](#) > [CrushFTP CVE-2025-31161 Auth Bypass and Post-Exploitation](#)

Published: April 4, 2025


CrushFTP CVE-2025-31161 Auth Bypass and Post-Exploitation

By:  Team Huntress

UPDATED 04/08/2025 @ 3pm ET

TL;DR: CVE-2025-31161 is a critical severity vulnerability allowing attackers to control how user authentication is handled by CrushFTP managed file transfer (MFT) software. We strongly recommend patching immediately to avoid affected versions 10.0.0 through 10.8.3 and 11.0.0.

```
...ction from: <ATTACKER-IP-ADDRESS>:<EPHEMERAL-PORT>  
[S>] WROTE: "HTTP/1.1 200 OK"
```

 **RAPID RESPONSE**

Critical Vulnerability: CrushFTP CVE-2025-31161

**See Huntress in
action**

Our platform combines a suite of

Initial access is just that – *initial access*.

Zero days could get them in the door, but they usually fall into predictable patterns after that point.

Mitigate zero days, but focus on post-compromise detection.

Identity Attack Origins

Assumption

Geofencing my identity logins should prevent identity attacks

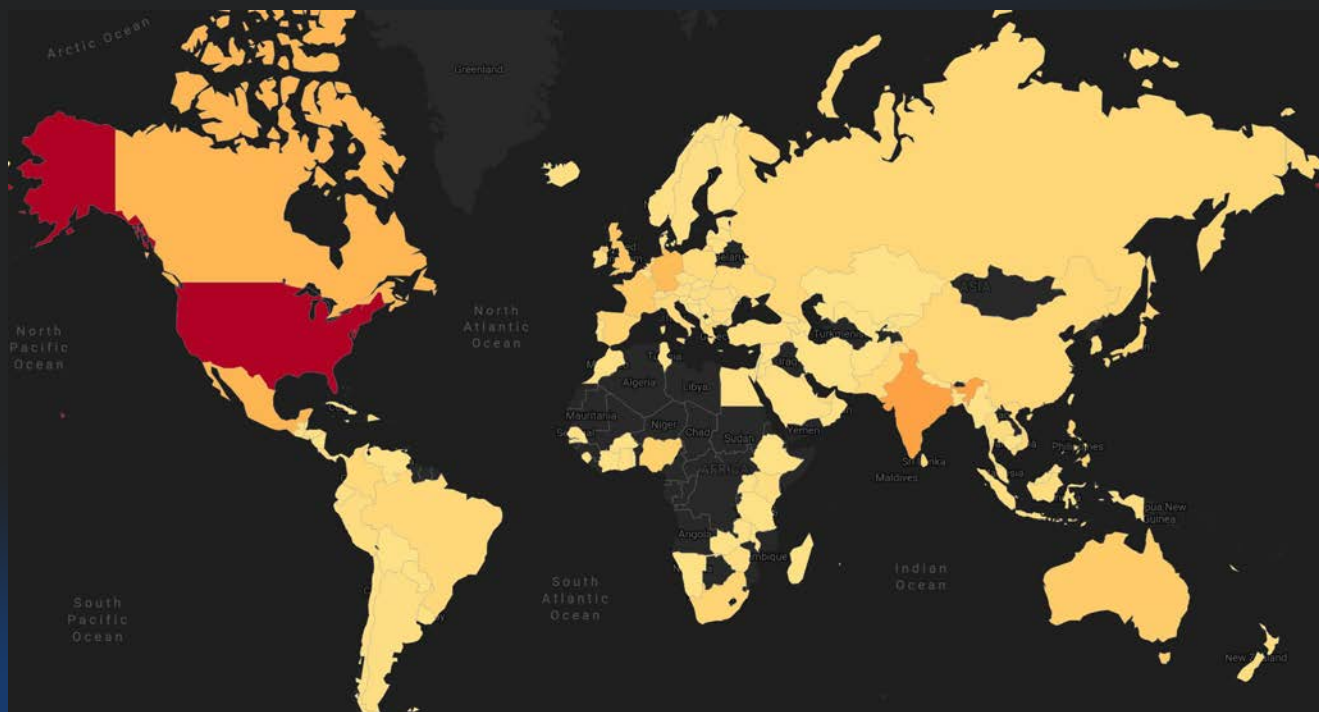


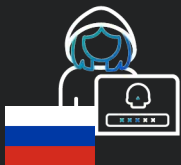
Identity Attack Origins

Created At



Last 2 quarters including this quarter (10/2024 – 03/2025)

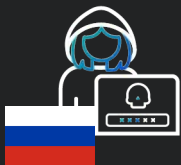




Credential Attack

SomeCorp Azure Tenant





Credential Attack



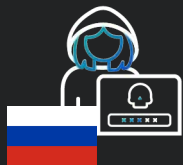
Conditional Access
Policies

SomeCorp Azure Tenant



*Geo-fencing CAP blocks a login from
Russia. So the day is saved! ... right?*

Proxies, VPNs, and datacenter infrastructure make the implied geography of an IP address meaningless



Credential Attack



SomeCorp Azure Tenant




Identity Attack Origins

*More than **2:1 ratio** of proxy/VPN/datacenter incidents to geographically relevant incidents*

Total Reported Geo-relevant Signals [Data on Geo]

8,355

↑ 56 Mar 26 vs Mar 25, 2025



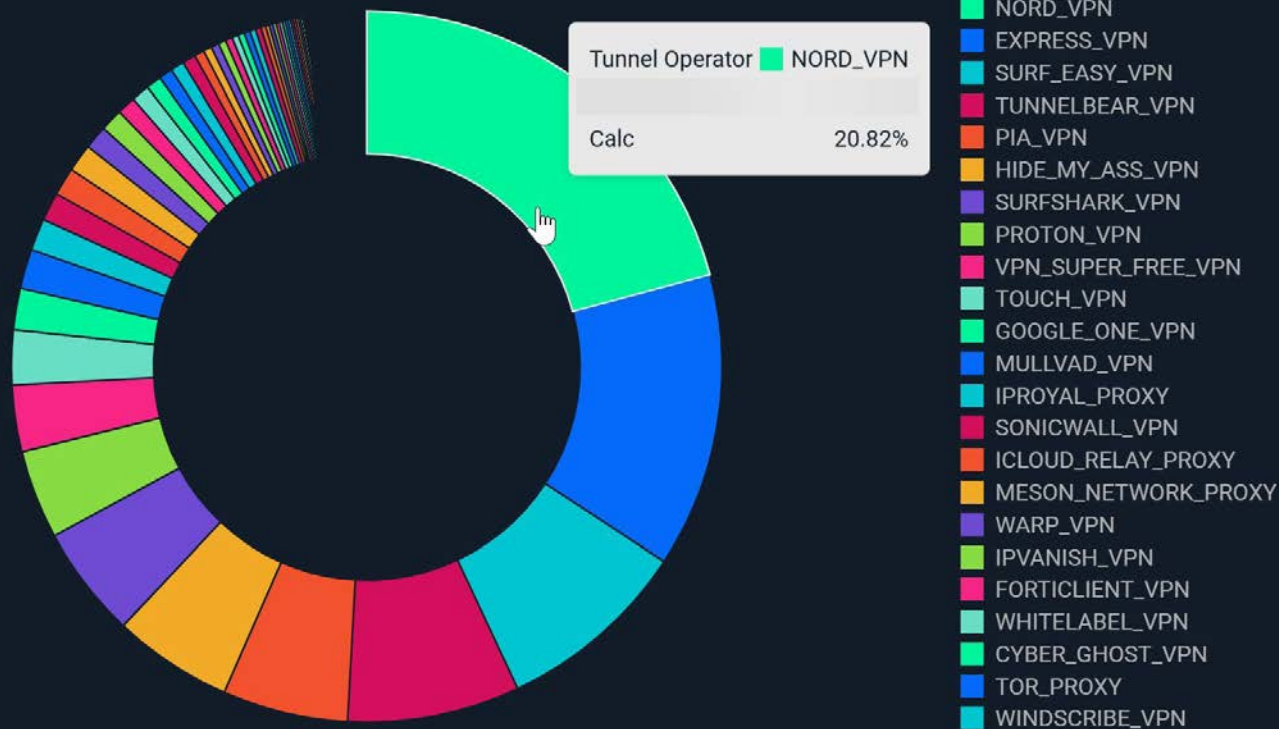
Total Reported Tunnel-relevant Signals [Data on Tunnels]

17,936

↑ 68 Mar 26 vs Mar 25, 2025



Top Tunnel Operators [All Tunnel Relevant Confirmed IRs]



Any assumptions about where identity attacks come from is incomplete if it only accounts for geographical location.

Geofencing (alone) is not enough.

We have to treat each kind of VPN, proxy, and datacenter IP as its own “location.”

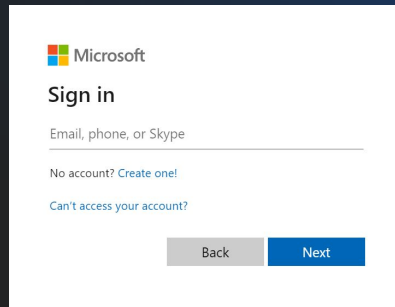
MFA Saves the Day

Assumption

Enforcing MFA on my users will prevent attacks.

ANY MFA > no MFA

No MFA is perfect!



[https://some.evilmalware.site\[.\]com](https://some.evilmalware.site[.]com)



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



From: Microsoft IT
Subj: URGENT!!! Account Action Required

Something weird is going on with your Microsoft online account. Please log in [here](#) to receive further instructions



Sign in

Email, phone, or Skype

No account? [Create one!](#)

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

Back

Next







Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

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



[https://some.evilmalware.site\[.\]com](https://some.evilmalware.site[.]com)

Username ✓
Password ✓



Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

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

Username ✓
Password ✓



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)





Microsoft

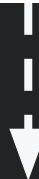
Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

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



MFA?



[https://some.evilmalware.site\[.\]com](https://some.evilmalware.site[.]com)





Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

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



MFA?

[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

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



MFA Code 

[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



Microsoft

Sign in


Email, phone, or Skype

No account? [Create one!](#)

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

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



MFA Code 



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)





Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

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




Looks good! Here's
your session token:



```
0.AVEA8G610F4ouEapV9XtGtBX01tEZUfGMrBJg-Ydk3ZSdsrQAF4.  
AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qWgxJE9CjF56ILVSFOP  
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6zOzNkpVUUFsmpzQJx7CjdfD1ne55sqz4  
1vvRs5uM-AFM4J34xNB11Dp9sXMQJj6hV-Get8Wba1Hefod1MKgNcdVxyAr_OdEon4vczAd8m_K_zRh_lG-B-rE2Ex69FI
```

[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



Session token 

```
0.AVEA8G6iOF4ouEapV9Xt6tBX01tEZUFGMrBJg-Ydk3ZSdsrQAF4.  
AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qW6xJE9Cjf5GILVSFOP  
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6z0zNkpvUUFsmpzQJx7CjdFD1ne55zq4  
1vvRs5uM-AFM4J4xNB11Dp9sXMQJj6hV-Get8WbalHefod1MKgNcdVxyAr_OdEon4vczAdBm_K_zRh_1G-B-rE2Ex69FI
```



Sign in

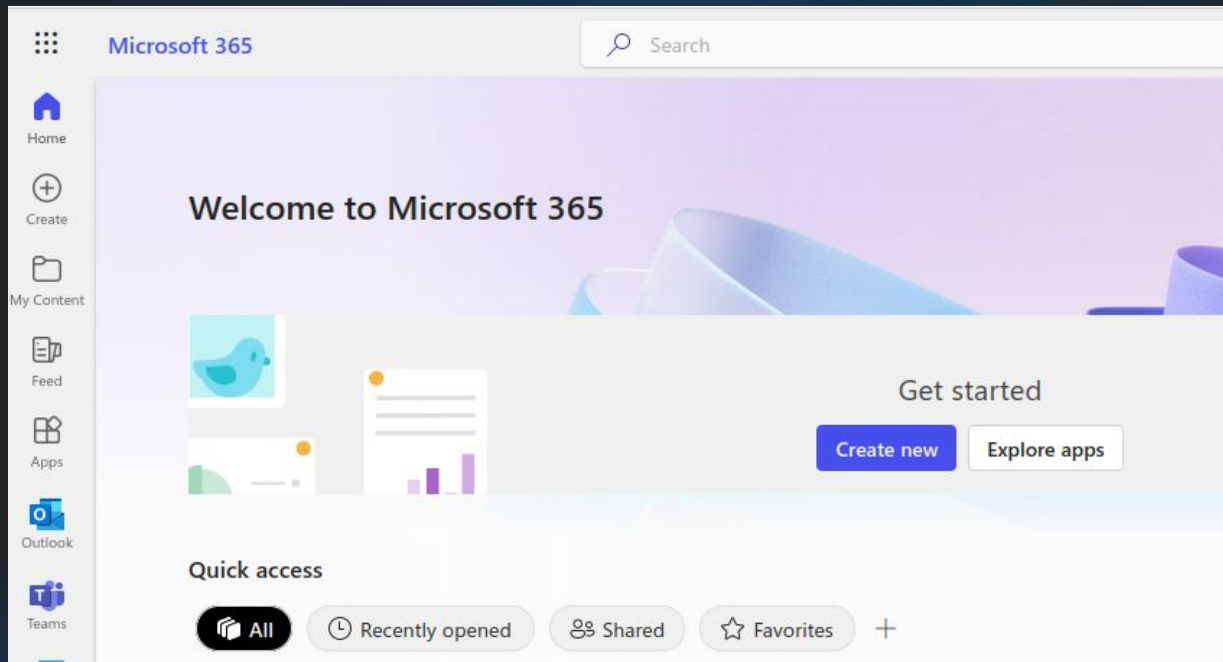
Email, phone, or Skype

No account? [Create one!](#)

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

Back

Next



Phishing the Phishing Resistant

Phishing for Primary Refresh Tokens in Microsoft Entra

Dirk-jan Mollema

**Any MFA is better than no MFA. But MFA alone can't
always save the day.**

MFA raises the technical barrier to entry.

The Scariest Assumption I've Heard

Assumption

My business is too small and I have nothing of value, so hackers won't go after me.

\$250 - \$984,855

*Range of financial damage resulting
from BEC attacks, Verizon DBIR, 2021*

\$250

There is no business too small to be a target.
Hackers will steal a single dollar if that's all they could get.

Takeaways

Talk to your CISOs & Engineers about your assumptions

- **Perimeter Zero Days:**
 - “How do we fare in an assumed breach scenario?”
- **Identity Attacks:**
 - “What assumptions are we making about geofencing our identity logins?”
- **MFA:**
 - “Is MFA applied across all identities? What type of MFA do we use?”
- **Too Small to be attacked:**
 - “What assumptions do we make about the kind of threat actor that would attack our business?”



Matthew Kiely

matt.kiely@huntresslabs.com

Thank you! Q/A

Connect with me on
LinkedIn!

