Evading Entra ID Protection

Red Team Tradecraft Against Modern Identity Defenses

(Part of Altered Security Month of Azure Red Teaming 2026)

About me

- Twitter - @nikhil_mitt
- Founder of Altered Security - alteredsecurity.com
- GitHub - github.com/samratashok
- Creator of Nishang, Deploy-Deception, RACE toolkit and more
- Interested in Active Directory, Offensive PowerShell and Azure Red Team.
- Previous Talks and/or Trainings
  - DEF CON, BlackHat, BruCON and more.

Altered Security

- Trained more than 50000 security professionals from more than 130 countries!
- Our Red Team Labs Platform enables labs to be:
  - Affordable
  - Easy to Access
  - Stable and provide great user experience
  - Fun to Solve
  - Big enough to feel enterprise-like

Red team labs	alteredsecurity.com/online-labs
Instructor-led bootcamps	alteredsecurity.com/bootcamps
GitHub	github.com/AlteredSecurity
Lab Platform	enterprisesecurity.io
Free Labs and Challenges	redlabs.enterprisesecurity.io

What is Month of Azure Red Teaming (MoART)

- Compared to the traditional/on-prem Red Teaming, Azure Red Teaming is not as well understood and discussed.
  - Lack of awareness
  - Lack of good and cost-effective learning resources
- Month of Azure Red Teaming is our way to bring awareness around Azure attacks.
- Red Labs (https://redlabs.enterprisesecurity.io) tries to solve the 'learning resources' issue.

Webinar Ground Rules

- You can ask questions on redlabs channel (#redlabs) on our Discord server (https://discord.com/invite/vcEwaRMwJe). We won't be able to monitor Zoom Chat.
- The lab will be made available to all users on the RedLabs platform for practice tomorrow (1st May 2026), so there is no follow along.
- To ensure a smooth experience, participants are not allowed to use their microphone.
- Please maintain professional conduct and a respectful atmosphere throughout the webinar.

Agenda

- Discussion on Entra ID Protection and some OpSec aware techniques to avoid detection.
- Focus on "can't fix" evasion of Entra ID Protection.
- Love for ~~Microslop~~ Microsoft.

Microsoft Entra ID Protection

- "Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks."
- Use of a compromised identity in an "abnormal" or "suspicious" way may result in a risk detection.
- Entra ID P2 required :P

- Not to be confused with Microsoft Defender for Identity (MDI).

https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

Microsoft Entra ID Protection - Detections

- Can detect Risky agents (Preview), Risky users and Risky workload identities.
- Real-time and Offline detections.

- My personal favorite detection type is - Nonpremium vs premium.
- "We detected something risky, but the details aren't available without a Microsoft Entra ID P2 license."

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

Microsoft Entra ID Protection - Detections

- Some of the most interesting Sign-in risks are:
  - Activity from anonymous IP address
  - Unfamiliar sign-in properties
  - Anonymous IP address
  - Atypical travel
  - Impossible travel
  - Suspicious MFA authentication approval
- There are risks for Users, Workload identities and Agents too.

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#sign-in-risk-detections-mapped-to-riskeventtype

Microsoft Entra ID Protection - Detections Types and Levels

- Can detect Risky agents (Preview), Risky users and Risky workload identities.
- Three risk levels:
  - High: High confidence
  - Medium: May need further investigation
  - Low: Needs further investigation
- Real-time (5-10 minutes) and Offline detections (up to 48 hours).

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

Microsoft Entra ID Protection - Integration

- Entra ID Protection risks can be consumed by Conditional Access Policies (CAP) to decide on access.
- CAPs can consume User risk or Sign-in Risk as Conditions.
- You can protect user and agents using this. But for a workload identity more licensing is required.

Detection Demo

- Login to Red Labs Platform -> Evading Entra ID Protection - User Identity -> Start Lab -> Sign-in using the provided username and password.
- Above "should" generate a detection in some time. Most probably "Unfamiliar sign-in properties".
- The target tenant also uses a Risk based Conditional Access policy so the sign-in will be blocked.

- Also try the "Evading Entra ID Protection - Workload Identity" lab.

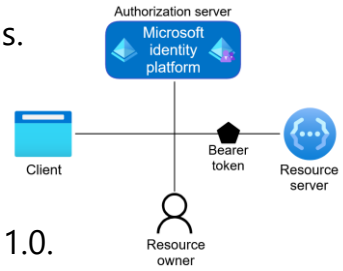
What is considered as an attack in Entra ID Protection?

- "An attack is an event where we detect a bad actor attempting to **sign-in** to your environment."
- Sign-in means (non-exhaustive list):
  - Interactive login using username password, TOTP, passwordless, Refresh tokens, PRT reuse, session refresh etc.
  - Use of client secret/application password or certificates by workload identities.
  - Federated sign-ins.
  - Any other token issuance event.

Microsoft Entra ID Protection - Evasion

- Authorization only events are NOT sign-ins.
- That is, Access Token = Profit.

- This is a standard implementation of OAuth 2.0 and OpenID Connect(OIDC) 1.0.



How to get an access token?

- **Hybrid environments and Assume Breach scenario** - Compromised identity in a "trusted" environment used to request access tokens.
- **Phishing Attacks** - Illicit Consent Grant, Attacker-in-The-Middle, Device Code Phishing.
- **Cached or Live Tokens** - MS Office Applications and others.
- **Web applications and Service Principals with Managed Identities** - Request tokens from Azure IMDS.

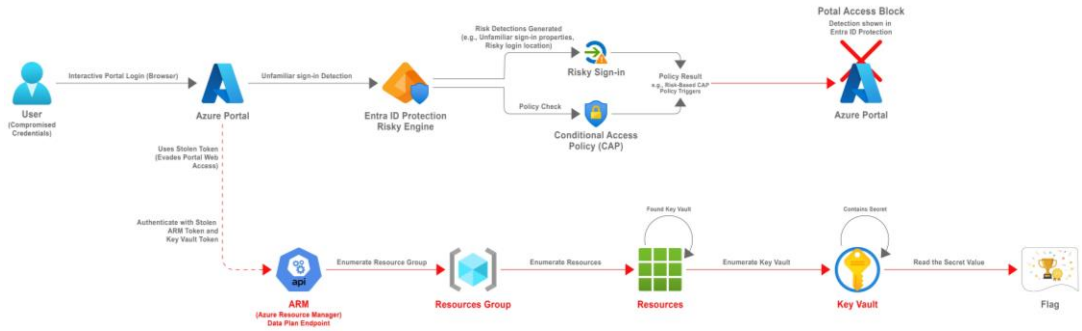
Red Labs Platform - Victim View

- Introducing **Victim View** in the Red Labs Platform!
- This takes out the requirement to setup an attacker's infrastructure to play with techniques that need user interaction.
- It is a live simulation, you get the exact same tokens that you see in the victim view.
- Enables you to focus on understanding the techniques after a user is phished.

Evasion Demo - User Identity

- For the "Evading Entra ID Protection - User Identity" lab, we have a live simulation in the Victim View running for Device Code Phishing.
- You get the access token that is requested on the victim's machine.
- Using the access token would not be detected or blocked.

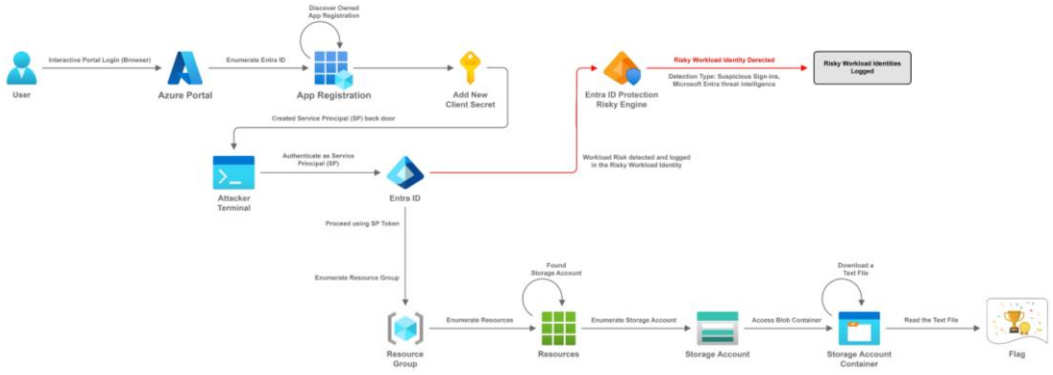
Evasion Demo - User Identity



Evasion Demo - Workload Identity

- For the "Evading Entra ID Protection - Workload Identity" lab, you can click on "Fetch Access Token" to simulate abuse of Azure Instance Metadata Service (IMDS).
- Once again, using the access token would not be detected or blocked.

Evasion Demo - Workload Identity



Conclusion and Limitations

- Don't be reckless. This is true for all the "Microsoft Defender for <insert shiny new service>"
- Target workload identities.
- Access tokens = profit!

- Security controls like Continuous Access Evaluation (CAE) may still stop you.

Thank you

- Please provide feedback.
- Follow me @nikhil_mitt
- Recording, slides and labs for this webinar are available on the Red Labs Platform: https://redlabs.enterprisesecurity.io/
- Complete both the 'User Identity' and 'Workload Identity' Labs to claim a badge.

- Discord (#redlabs channel for this webinar) - https://discord.com/invite/vcEwaRMwJe
- Red Team labs: https://www.alteredsecurity.com/online-labs
- Bootcamps: https://www.alteredsecurity.com/bootcamps