# Evading MDI

## Red Team Tradecraft for AD Attacks

(Part of Altered Security Hacker Summer 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 Hacker Summer

- Altered Security's month-long Red Teaming event.
  - Research blogs and webinars on Red Teaming for on-prem, Azure and AI.
  - Call for papers.
  - Discounts and giveaways.

# Webinar Ground Rules

- You can ask questions on general channel (#general) on our Discord server (https://discord.com/invite/vcEwaRMwJe). We won't be able to monitor Zoom Chat.
- 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

- We will discuss OPSEC considerations for a Red Team Operation.
- Focus on evasion of "Identity Attacks" for on-prem AD detected by Microsoft Defender for Identity (MDI).

# Microsoft Defender for Identity (MDI)

- "Defender for Identity is designed to detect threats that specifically target identities.."
- MDI looks for anomalous and suspicious activities based on identity behaviour.
- It collects data using sensors. Sensors can be installed on DCs, AD FS, AD CS and Entra Connect servers.



https://learn.microsoft.com/en-us/defender-for-identity/what-is

# MDI - Detections

- Detections are aligned to stages of an identity based attack:

| Attack stage | Defender for Identity detections |
|---|---|
| Reconnaissance | Identifies suspicious discovery activity, such as attempts to enumerate user names, group membership, IP addresses, and resources. |
| Compromised credentials | Detects attempts to compromise credentials using techniques such as brute force, repeated failed authentications, and suspicious changes to user group membership. |
| Lateral movement | Detects attempts to move laterally and expand control of sensitive identities and across different environments. |
| AD Domain dominance | Highlights behavior associated with full domain compromise, such as remote code execution on domain controllers, DCShadow, malicious domain controller replication, and Golden Ticket activity. |



https://learn.microsoft.com/en-us/defender-for-identity/what-is#detect-identity-based-threats

# MDI - Alerts

- MDI alerts are divided into the following categories:
  - MDI Classic alerts
  - MDI Defender alerts
- Both the categories are based on MDI sensors but differ whether alert was generated by MDI or Microsoft defender (based on MDI sensors).
- Regardless of category, our focus will be on On-Prem AD.
- "The differences are part of an ongoing transition to a unified alerting experience across Microsoft Defender products."



https://learn.microsoft.com/en-us/defender-for-identity/alerts-overview

# MDI - Alerts - Classic Format

- Reconnaissance and discovery
- Persistence and privilege escalation
- Credential access
- Lateral movement
- Other alerts



https://learn.microsoft.com/en-us/defender-for-identity/alerts-mdi-classic

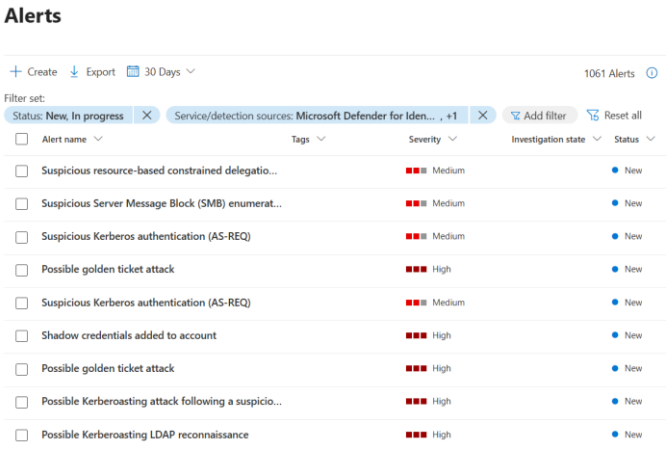
# MDI - Alerts - Defender Format

- Command and Control alerts
- Credential Access alerts
- Defense Evasion alerts
- Discovery alerts
- Execution alerts
- Impact alerts
- Initial Access alerts
- Lateral Movement alerts
- Persistence alerts
- Privilege Escalation alerts



https://learn.microsoft.com/en-us/defender-for-identity/alerts-xdr

# Detection Demo - From our labs



# Detection Statistics - From our labs

- Altered Security has a unique visibility in how attackers operate.
- We observe more than 3000 attacker machines executing thousand of attacks everyday.
- Our users generated more than 7000 alerts by MDI in past 6 months.
- Note that, in all our on-prem red teaming courses, we discuss MDI evasion, the alerts are deliberately generated as we want to discuss identity OPSEC :P

# Detection Statistics - From our labs

Top 10 MDI alerts in past 6 months:

| No. | Alert Name | Count |
|---|---|---|
| 1.<br>2.<br>3. | Suspected Kerberos SPN exposure<br>Possible Kerberoasting LDAP reconnaissance<br>Possible Kerberoasting attack following a suspicious LDAP query | 1257 |
| 4. | Possible golden ticket attack | 944 |
| 5.<br>6. | Suspicious Kerberos authentication (AS-REQ)<br>Suspected overpass-the-hash attack (Kerberos) | 870 |
| 7. | Security principal reconnaissance (LDAP) | 781 |
| 8. | Suspicious Server Message Block (SMB) enumeration from untrusted host | 756 |
| 9. | Suspected DCSync attack (replication of directory services) | 595 |
| 10. | Suspicious LDAP query | 291 |

# MDI - Evasion - Mindset

- There are detections other than EDR. EDR evasion is not the only OPSEC.
- Avoid communication with DCs. Don't chase Domain Admin privileges - No DA before lunch.
- Don't be reckless.
- For me, tools that silently detect activities are scarier.

# MDI - Evasion - Tradecraft

- Understand how your activities and tools interact with DCs.
- Don't downgrade encryption - No RC4.
- Avoid using SAMR and be careful with LDAP for enumeration - Use ADWS
- Make sure forged tickets are compliant to the Kerberos Policy of the target AD.
- Do not forge tickets for any Domain Admin.

# MDI - Evasion - Enumeration

- Detections:
  - Security principal reconnaissance (LDAP)
  - Suspicious Server Message Block (SMB) enumeration from untrusted host
  - Suspicious LDAP query
- Triggered by - SharpHound and other automated enumeration
- Evaded by -
  - Manual enumeration using ADModule (uses ADWS)
  - SOAPHound is mostly fine (uses ADWS)

# MDI - Evasion - Kerberoasting

- Three detections:
  - Suspected Kerberos SPN exposure
  - Possible Kerberoasting LDAP reconnaissance
  - Possible Kerberoasting attack following a suspicious LDAP query
- Triggered by - Requesting multiple Service Tickets in quick succession.
- Evaded by - Enumeration using ADModule or PowerView and request one ST/TGS at a time.

# MDI - Evasion - PTH/AskTGT

- Detections:
  - Suspicious Kerberos authentication (AS-REQ)
  - Suspected overpass-the-hash attack (Kerberos)
- Triggered by - Over-PTH or Authentication from a new machine.
- Evaded by - No blanket evasion. This is difficult to avoid.

# MDI - Evasion - Golden Ticket

- Detection: Possible golden ticket attack
- Triggered by - Using a forged TGT with no prior ST/TGS request.
- Evaded by - As of July 2026, use of Diamond ticket is not detected.

# MDI - Evasion - DCSync

- Detection: Suspected DCSync attack (replication of directory services)
- Triggered by - Replication requests by non-DC principals.
- Evaded by - Silver ticket/TGT/credentials of DC or inject sIDHistory of Domain Controllers or Enterprise Domain Controllers.

# MDI - Evasion - MDIChoker

- Based on the fantastic EDRChoker research by "Zero Salarium".
- Set a very small outbound bandwidth for MDI sensor service (microsoft.tri.sensor.exe) = No alerts!
- No health issues are reported by the sensor.
- Administrator privileges required on the machine (DC or others) with sensor. May still be useful in Domain Dominance scenarios.

# MDI - Evasion - No Alerts

- Diamond Ticket
- Silver Ticket (even when the target service is on DC)
- Persistence techniques for GPO related attacks, Security descriptors abuses on remote access services and more.

# Conclusion and Limitations

- Don't be reckless. This is true for all the "Microsoft Defender for <insert shiny new service>"
- No more "Domain Admin before lunch".

- _Most_ of the testing was performed in a lab environment.

# Thank you

- Please provide feedback.
- Follow me @nikhil_mitt

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