Analysis of Bypassing Detection by Microsoft Advanced Threat Analytics

Edgar Bohte and Nick Offerman

Research Project 2 #72

Introduction - Advanced Threat Analytics (ATA)

- Microsoft Active Directory (AD)
- On-premise Post-Infiltration detection tool
- Advanced Persistent Threats
- User and Entity Behaviour
  - Anomaly or behavioural analysis
- Advanced monitoring
- Windows, macOS or *nix Operating Systems (OS)

Research Context

- Not extensively researched
- Subject an AD test environment to a wide variety of attacks
- Latest version 1.9.2
- Determine attack triggers
- Bypass detection
- Anomaly-based attacks

Relevant research

- Mittal (2017) [1]
  - ATA v1.7 + 1.8
  - Attacking the Domain Controller (DC) with Lightweight Gateway increases detection
- Thompson (2017) [2]
  - ATA v1.8
  - Different protocols decreases detection

Research questions

How can Microsoft Advanced Threat Analytics using anomaly mode be bypassed?

- Which kind of attacks trigger suspicious activity alerts?
- Does the privilege level of the account influence the detection?
- Which particular event in the attack generates the suspicious activity alert?

Methods

1. AD environment running ATA
2. Compose a list of categories to index attacks
3. Subject attacks to test environment
4. Examine ATA detections to determine trigger steps
5. Alternative ways to bypass detection

Test Environment

Setup

- ATA Center
  - analyses traffic
- Lightweight Gateway
  - sends DC1 traffic only
- Client Machines
  - Initial starting point

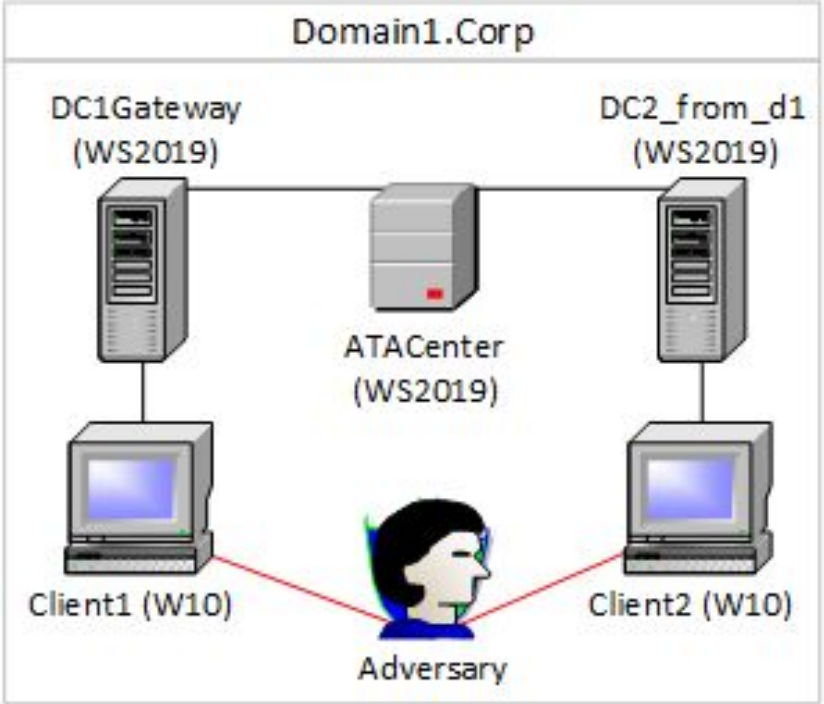

Figure 1: Test Environment

Attack Categories

- Discovery
  - network and endpoint knowledge
- Credential Access
  - steal credentials
- Lateral Movement
  - exploit remote endpoint
- Privilege Escalation
  - elevated permissions
- Persistence
  - prevent losing access.

Attacking the Test Environment

- Privileged levels Accounts:
  - Domain Administrator
  - Domain User + Local Administrator
  - Domain User
  - Local Administrator
- ~ 85 Attacks
  - Main findings only

- Attack Outcome in Text:
  - Success
  - Fail
  - Access Denied
- Alert Classification in Color:
  - High
  - Medium
  - Low
  - None

Domain Admin
Success

Table 1: Result Example

Discovery

Invoke-UserHunter

- Domain admin accounts
- Enumerating repeated sessions

Domain Admin	Domain User + Local Admin	Domain User	Local Admin
Success	Success	Success	Access Denied

Table 2: Detection of ATA for the Invoke-UserHunter command

Discovery - detection and bypass

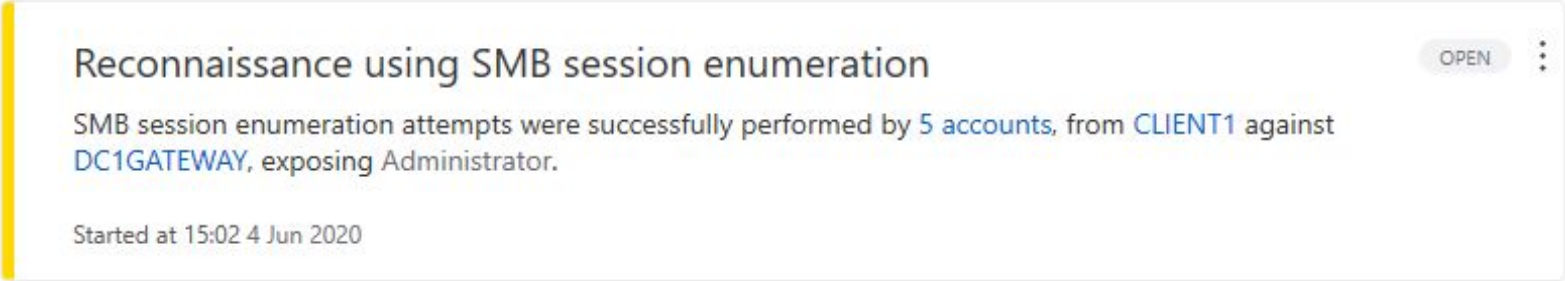

Figure 2: Invoke-UserHunter (medium alert)

SMB is used to enumerate too many domain users

- Create Domain Userlist (Get-NetUser)
- Include ComputerFile
  - exclude DC with Lightweight Gateway
  - target local machine or DC2 without Lightweight gateway

Credential Access

- DCSync
- Simulate the behaviour of DC in order retrieve password via domain replication

Targeted user	**Domain Admin**	**Domain User + Local Admin**	**Domain User**	**Local Admin**
KRBTGT	Success	Fail	Fail	Fail
Domain Admin	Success	Fail	Fail	Fail
Domain User	Success	Fail	Fail	Fail

Table 4: Detection of ATA for the DCSync attack

Credential Access - detection and bypass

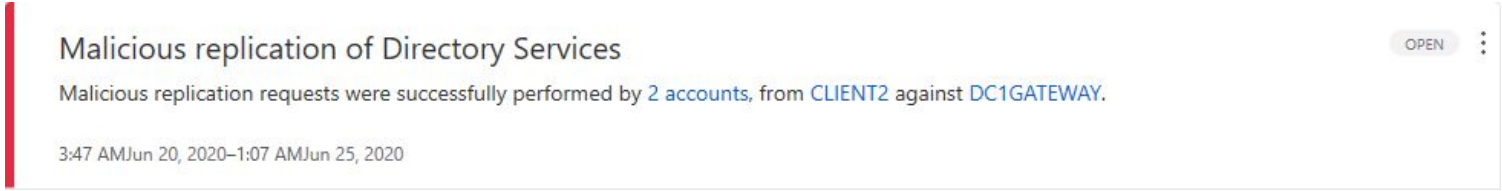

Figure 3: DCsync High severity Alert

- Detected because a workstation tries to act as a DC
- Bypass by creating a shadow copy of directory using vssadmin.exe. Then get the ntds.dit file. Crack the ntds.dit file and obtain the hashes.

Privilege Escalation

- Seven Attacks
- Nothing got detected
  - Partly because most attacks are local

Lateral Movement

- Pass The Hash using Cobalt Strike
- Move from one machine or user to another machine or user
- NTLM hash user is needed
- Only accessing the DC1gateway as administrator was detected

Lateral Movement - detection and bypass

Suspicious service creation

OPEN

Administrator created 2 services in order to execute potentially malicious commands on DC1GATEWAY.

4:57 AM–4:58 AMJun 22, 2020

Figure 4: ATA alert creating reverse shell

- Detected because cobalt strike return shell
- Currently working on finding a bypass

Persistence

- Golden ticket
- Complete access to the domain
- KRBTGT NTLM hash, group id, security identifier current user

Domain Admin	Domain User + Local Admin	Domain User	Local Admin
Success	Success	Fail	Success

Table 5: ATA alerts for the golden ticket attack for all tested privileges levels

Persistence - detection and bypass

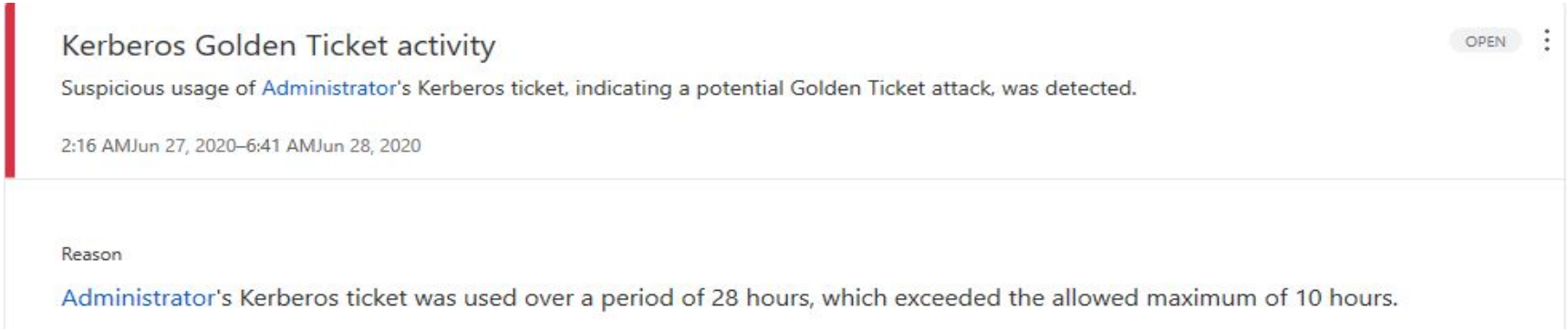

Figure 5: ATA golden ticket alert

- If the golden ticket is used too long in use. Depends on the security policy of the AD
- Create a new ticket before this time

Overview performed attacks

Category	Total performed	Total detected
Discovery	54	17 (32%)
Credential access	10	3 (30%)
Privilege escalation	7	0 (0%)
Lateral movement	7	2 (29%)
Persistence	9	4 (45%)
Total	87	26 (30%)

Table 6: Overview of all performed attacks

Overview detections bypassed

Category	Total performed	Total detected	Total detected after variants
Discovery	54	17 (32%)	4 (7%)
Credential access	10	3 (30%)	0 (0%)
Privilege escalation	7	0 (0%)	0 (0%)
Lateral movement	7	2 (29%)	2 (29%)
Persistence	9	4 (45%)	2 (22%)
Total	87	26 (30%)	8 (9%)

Table 7: Overview attacks after attack variants

Discussion

- Many attacks performed after each other could influence detections
  - E.g. user10 enumerated all users 2 times in 10 minutes

- ATA alert seen against all possible ATA alerts
  - 5 out 11 not seen from anomaly based
  - 2 behavioral alerts seen, which need one week learning period

Conclusion

How can Microsoft Advanced Threat Analytics using anomaly mode be bypassed?

- For Privilege escalation no attacks were detected or categories some attacks. The most attacks were detected for discovery
- Privilege level did not influence the detection, but only the outcome of the attack
- Most alerts were generated because of the use of the protocol or that the lightweight gateway was included in the attack
- Most attack were not detected by ATA and even more alerts were bypassed

Future work

- Behavioural analysis
- Larger test environment
- Azure ATP

Thanks for your attention

Sources

- [1]: https://www.blackhat.com/docs/us-17/thursday/us-17-Mittal-Evading-MicrosoftATA-for-ActiveDirectory-Domination.pdf
- [2]:https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf