

ATT&CKING ACTIVE  
DIRECTORY:  
AUTOMATED AD  
ADVERSARY  
SIMULATION

**EU MITRE  
ATT&CK®  
Community**

EU MITRE ATT&CK® Community Workshops

June 2, 2021

Mauricio Velazco  
@mvelazco



#WHOAMI

- ✕ Threat Research @ Splunk
- ✕ [@mvelazco](https://twitter.com/mvelazco)
- ✕ Bsides, Derbycon, Defcon, BlackHat
- ✕ [github.com/mvelazco](https://github.com/mvelazco)

# ADVERSARY SIMULATION

Goal: Identify gaps in visibility & detection capabilities

- ✗ Collaborative exercise / knowledge transfer
- ✗ Allows blue to identify and understand TTPs
- ✗ Allows red to identify evasion paths



DETECTION ENGINEERS NEED THE CAPABILITY TO  
GENERATE ATTACK TELEMETRY

# SIMULATION SCENARIOS

Simulating the same TTP under different scenarios will test detection resilience

## ✗ Example: Kerberoasting

Simulation 1: Invoke-Kerberoast -Domain domain.com

Simulation 2: GetUserSPNs.py -dc-ip X.X.X.X domain.com/user

VS

Simulation 3: PowerView / SharpView recon to identify target  
Rubeus.exe kerberoast /user:secureservice



# PURPLESHARP

- ✗ Executes adversary techniques within Windows AD environments following the MITRE ATT&CK Framework (47 supported).



- ✗ Goal:  
Generate telemetry to build, test & enhance detection controls

<https://github.com/mvelazc0/PurpleSharp>

# DISCOVERY – TA0007

- ✗ After initial access, adversaries perform reconnaissance against AD for situational awareness

## Sodinokibi (aka REvil) Ransomware

*March 29, 2021*

```
cmd.exe /c chcp >&2
WMIC.exe WMIC /Node:localhost /Namespace:\
ipconfig.exe ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net.exe net group "Domain Admins" /domain
```

## Conti Ransomware

*May 12, 2021*

```
ipconfig /all
systeminfo
whoami /groups
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
new group "Domain Admins" /domain
```

The DFIR Report → <https://thedfirreport.com/>

# Active Directory Discovery Simulation

## AD Discovery Scenario #1 – Cmdline

- T1033 – User Discovery
- T1018 – Remote System Discovery
- T1482 – Domain Trust Discovery
- T1087.001 – Local Account Discovery
- T1069.001 – Domain Group Discovery

## AD Discovery Scenario #2 – PowerShell

- T1087.001 – Local Account Discovery
- T1087.002 – Domain Account Discovery
- T1069.002 – Domain Group Discovery
- T1018 – Remote System Discovery

## AD Discovery Scenario #3 – LDAP

- T1087.002 – Domain Account Discovery
- T1069.002 – Domain Group Discovery





# DETECTION TAKEAWAYS

- ✗ 4688 + Command line, Sysmon or your favorite EDR
  - Identify most common enumeration techniques
  - Should deploy the capability to decode base64 encoded commands
- ✗ PowerShell visibility
  - Script Block Logging – Event Id 4104
  - Module Logging
  - Transcription Logging
- ✗ Network visibility
  - Zeek or favorite comercial NTA vendor

# PASSWORD SPRAYING

- ✗ Iterate through a list of users with a commonly used password ( Summer2021 )
- ✗ Used to obtain initial access / situational awareness / privilege escalation
- ✗ <https://attack.mitre.org/techniques/T1110/003>

## APT 29

SVR Cyber Operations Tactics, T

### Password Spraying

In one 2018 compromise of a large network, SV conducted the password spraying activity in a password spraying used a large number of IP a The Onion Router (TOR) addresses.

<https://us-cert.cisa.gov/ncas/alerts/aa21-116a>

# AD Password Spraying Simulation

## Scenario #1

An adversary has obtained physical access to the target network and performs a password spray attack against one host using the SMB protocol.

## Scenario #2

A domain joined device has been compromised and is being controlled by a trojan. With this access, an adversary executes a Password Spraying attack using the Kerberos protocol.

## Scenario #3

A domain joined device has been compromised and is being controlled by a trojan. With this access, an adversary executes a Password Spraying attack using the NTLM protocol.





## DETECTION TAKEAWAYS

- ✗ For full visibility, we need to log both Domain Controller and Domain Member endpoints
- ✗ Events Seen
  - 4771 – Kerberos Authentication Service
  - 4776 – Credential Validation
  - 4625 – Logon
  - 4648 – Logon

# ENTERPRISE SECURITY CONTENT UPDATE v3.21

- ✗ Active Directory Password Spraying Analytic Story
- ✗ 8 detections for different password spraying scenarios
- ✗ You don't need be a Splunk user to leverage the logic
- ✗ TODO: Sigma rules

- Multiple Disabled Users Failing To Authenticate From Host Using Kerberos
- Multiple Invalid Users Failing To Authenticate From Host Using Kerberos
- Multiple Invalid Users Failing To Authenticate From Host Using NTLM
- Multiple Users Attempting To Authenticate Using Explicit Credentials
- Multiple Users Failing To Authenticate From Host Using Kerberos
- Multiple Users Failing To Authenticate From Host Using NTLM
- Multiple Users Failing To Authenticate From Process
- Multiple Users Remotely Failing To Authenticate From Host

[https://github.com/splunk/security\\_content](https://github.com/splunk/security_content)  
<https://splunkbase.splunk.com/app/3449/>  
<https://docs.splunk.com/Documentation/ESSOC/3.21.0/stories/>

# THE ACTIVE DIRECTORY PURPLE TEAM PLAYBOOK ( BETA )

- ✗ Library of ready-to-use playbooks designed to be used with PurpleSharp

<https://github.com/mvelazco/PurpleAD/>

- ✗ Allows blue teams to run internal Purple Team exercises against Active Directory in an easy way at 0 cost !

THANKS!

<https://twitter.com/mvelazco>

<https://github.com/mvelazco/PurpleAD/>

<https://github.com/mvelazco/Purplesharp/>

ATT&CKING ACTIVE  
DIRECTORY:  
AUTOMATED AD  
ADVERSARY  
SIMULATION

**EU MITRE  
ATT&CK®  
Community**

EU MITRE ATT&CK® Community Workshops

June 2, 2021

Mauricio Velazco

@mvelazco