# ATT&CKING ACTIVE DIRECTORY: AUTOMATED AD ADVERSARY SIMULATION

# EU MITRE ATT&CK® Community EU MITRE ATT&CK® Community Workshops

I June 2, 2021 I Mauricio Velazco I @mvelazco



- X Threat Research @ Splunk
- **X** <u>@mvelazco</u>
- 🗶 Bsides, Derbycon, Defcon, BlackHat
- x github.com/mvelazc0

# ADVERSARY SIMULATION

Goal: Identify gaps in visibility & detection capabilities

- Collaborative exercise / knowledge transfer
- X Allows blue to identify and understand TTPs
- X 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).



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

https://github.com/mvelazc0/PurpleSharp

# DISCOVERY - TAOOO7

\* 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 -> <a href="https://thedfirreport.com/">https://thedfirreport.com/</a>

# Active Directory Discovery Simulation

AD Discovery Scenario #1 - Cmdline

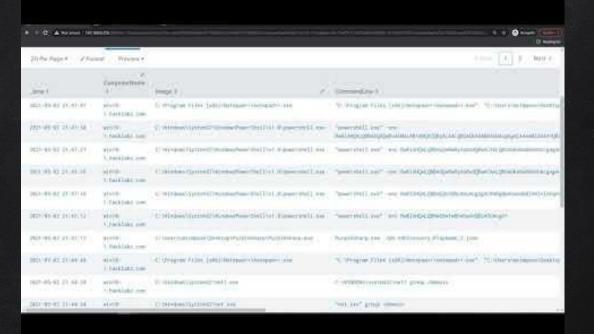
T1033 - User Discovery
T1018 - Remote System Discovery
T1482 - Domain Trust Discovery
T1087.001 - Local Account Discovery
T1069.001 - Domain Group Discovery

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



# HTTPS://YOUTU.BE/8JRSITZB1UE

### DETECTION TAKEAWAYS

- X 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
- X Network visibility
  Zeek or favorite comercial NTA vendor

# PASSWORD SPRAYING

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

#### **APT 29**

SVR Cyber Operations Tactics,

### **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 #2

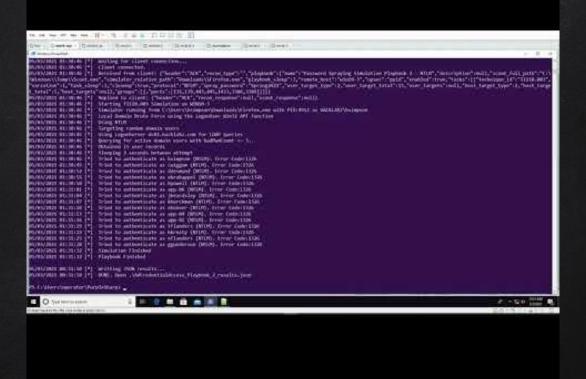
A domain joined device has been compromised and is being controlled by a trojan. With this access, an adversary executes a Password Spraying attack using the Kerberos protocol.

#### Scenario #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 #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.



# HTTPS://YOUTU.BE/HGDUxKQx-\_E

## DETECTION TAKEAWAYS

For full visibility, we need to log both Domain Controller and Domain Member endpoints

**X** Events Seen

4771 – Kerberos Authentication Service

4776 - Credential Validation

4625 - Logon

4648 - Logon

## ENTERPRISE SECURITY CONTENT UPDATE V3.21

- X Active Directory Password Spraying Analytic Story
- X 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

les <a href="https://github.com/splunk/security\_content">https://github.com/splunk/security\_content</a>
<a href="https://splunkbase.splunk.com/app/3449/">https://splunkbase.splunk.com/app/3449/</a>
<a href="https://docs.splunk.com/Documentation/ESSOC/3.21.0/stories/">https://docs.splunk.com/Documentation/ESSOC/3.21.0/stories/</a>

# THE ACTIVE DIRECTORY PURPLE TEAM PLAYBOOK (BETA)

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

https://github.com/mvelazc0/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/mvelazc0/PurpleAD/

https://github.com/mvelazc0/Purplesharp/

ATT&CKING ACTIVE DIRECTORY: AUTOMATED AD ADVERSARY SIMULATION

# EU MITRE ATT&CK® Community EU MITRE ATT&CK® Community Workshops

I June 2, 2021 I Mauricio Velazco I @mvelazco