

CLOUD IDENTITY SUMMIT '22

Identity Security Track

Azure AD Security Testing with AADInternals Dr. Nestori Syynimaa (Secureworks®)

Community Event by





CLOUD IDENTITY SUMMIT '22

Thanks to our sponsors!



business. people. technology.

glueckkanja gab

yubico



Azure AD Security Testing with AADInternals

@DrAzureAD

https://linkedin.com/in/nestori

About the speaker



Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks CTU
- Creator of AADInternals toolkit
- MVP (Identity & Access, Mobile Device Management), MVR

Contact details

- <u>nsyynimaa@secureworks.com</u>
- Twitter: <u>@DrAzureAD</u>
- <u>https://linkedin.com/in/nestori</u>
- <u>https://o365blog.com</u>

MITRE ATT&CK Defender MITRE ATT&CK Defender MITRE ATT&CK Defender ATT&CK® ATT&CK® **ATT&CK®** SECURITY OPERATIONS **CYBER THREAT** ADVERSARY EMULATION CENTER ASSESSMENT INTELLIGENCE METHODOLOGY CERTIFICATION CERTIFICATION CERTIFICATION Microsoft Microsoft Microsoft 365 CERTIFIED IDENTITY AND ACCESS AZURE SOLUTIONS SECURITY ARCHITECT ADMINISTRATOR ADMINISTRATOR EXPERT ASSOCIATE ASSOCIATE $\star\star$



Contents

- Introduction to Adversary Emulation
- Introduction to AADInternals
- Adversary Emulation using AADInternals

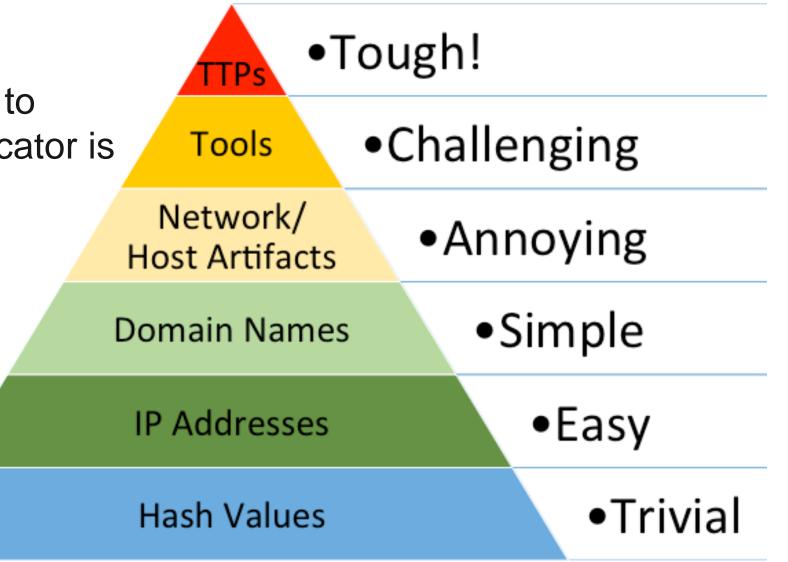
Introduction to Adversary Emulation

Adversary Emulation

- MITRE: "Adversary Emulation is an intelligence driven discipline that entails researching, modeling, and executing cyber adversary tactics, techniques, and procedures (TTPs) to assess and improve cybersecurity"
- Adversary emulation != penetration testing

Pyramid of Pain

 The "cost of change" to adversaries if an indicator is blocked



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Adversary Emulation sources



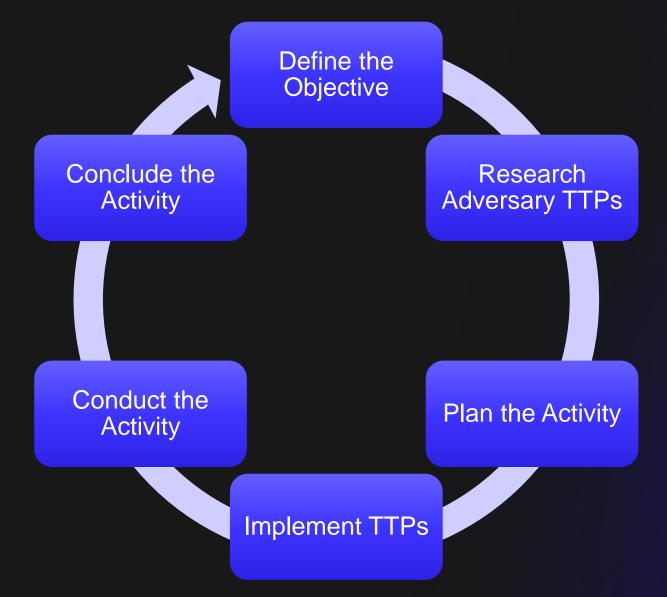
The Center for Threat-Informed Defense

An R&D organization focused on advancing the state of the art and the state of the practice in threat-informed defense.

Attps://ctid.mitre-engenuity.org/

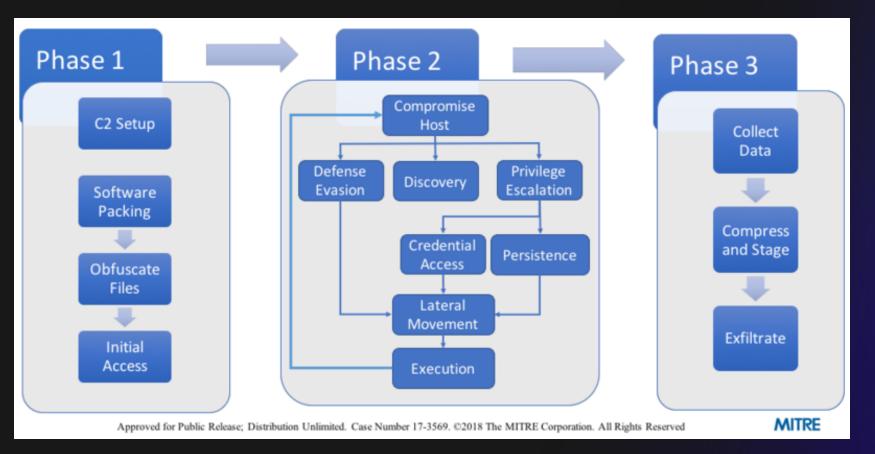
• <u>https://github.com/center-for-threat-informed-defense</u>

Adversary Emulation Framework



Adversary Emulation Plan

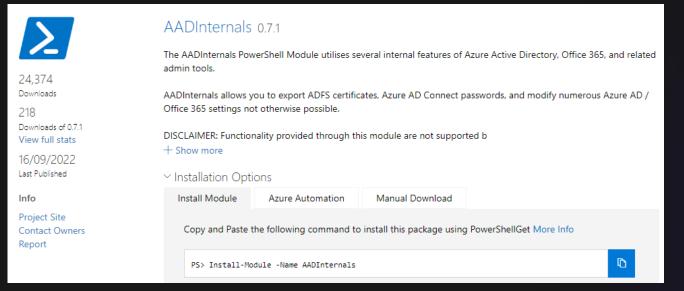
- Content depends on the adversary's TTPs
- Example of APT 3 Emulation Plan:



Introduction to AADInternals

AADInternals 1/2

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
 - https://github.com/gerenios/aadinternals
 - https://o365blog.com/aadinternals/
 - https://www.powershellgallery.com/packages/AADInternals





@DrAzureAD



AADInternals 2/2

• MITRE ATT&CK

https://attack.mitre.org/software/S0677/

| Groups That Use This Software | | |
|-------------------------------|-------|------------|
| ID | Name | References |
| G0016 | APT29 | [5] |



Two (technical) categories of functionality

"Local"

- Do stuff in/against local computer (or other onprem computer)
- Most functionality in PowerShell
- Some functionality required custom/external .dlls
- "Cloud"
 - Do stuff by communicating against cloud services
 - All functionality in PowerShell
 - Most functionality requires authentication

Logical categories of functionality

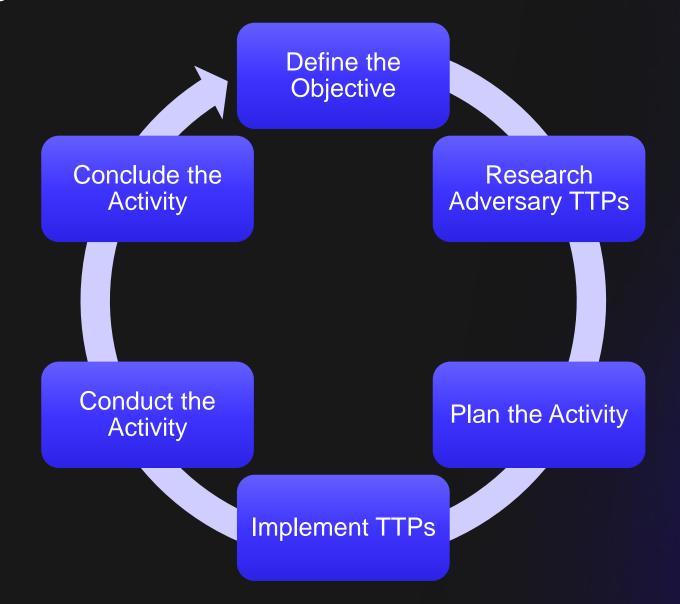
- Tenant information and manipulation
- Rollout policy functions
- Utilities
- User manipulation
- User MFA manipulation
- User manipulation with AD sync API
- Exchange Online
- SharePoint Online
- OneDrive for business
- Teams
- Client & SARA
- Azure
- Hybrid Health
- Kill chain
- DRS (DSInternals)
- MS Partner
- OneNote
- Certificate Based Authentication

- Hacking:
 - Identity Federation
 - PTA
 - Directory Synchronization
 - ADFS
 - SSSO
 - AD
 - Azure AD Join, MDM & PRT

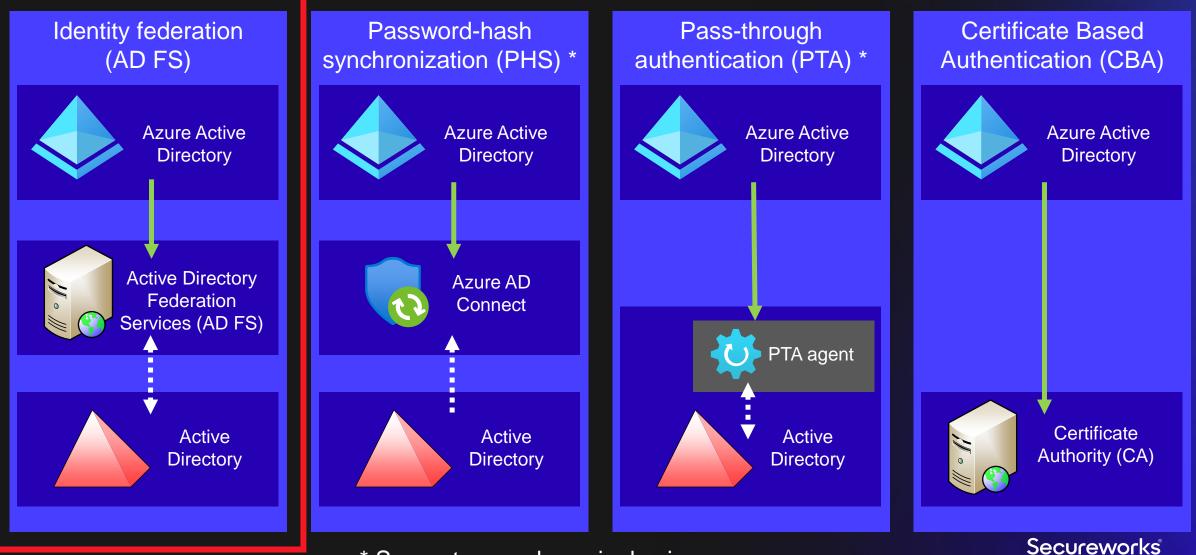


Adversary emulation using AADInternals

Adversary Emulation



Hybrid Authentication Options



* Supports seamless single sign-on

@DrAzureAD **Adversary Emulation** APT29 is known to attack identity federation. Is our AD FS environment Define the secured? Objective Conclude the Research Adversary TTPs Activity Conduct the Plan the Activity Activity Implement TTPs Secureworks

Selected TTPs

Tactics:Defense EvasionCredential AccessLateral Movement

Techniques:

T1550 Use Alternate Authentication Material T1552.004 Unsecured Credentials: Private Keys T1606.002 Forge Web Credentials: SAML Tokens

Procedures:

Forge SAML tokens Export AD FS signing certificates

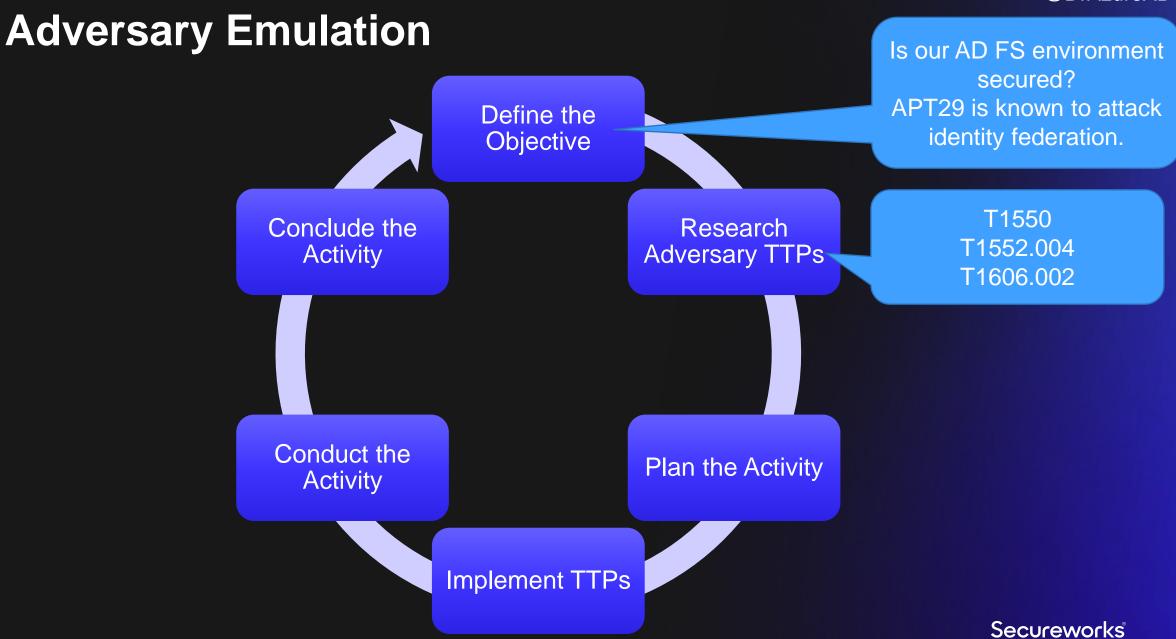
"Why?" The reason for performing the attack.

"How?" Techniques used to achieve the goal of the attack.

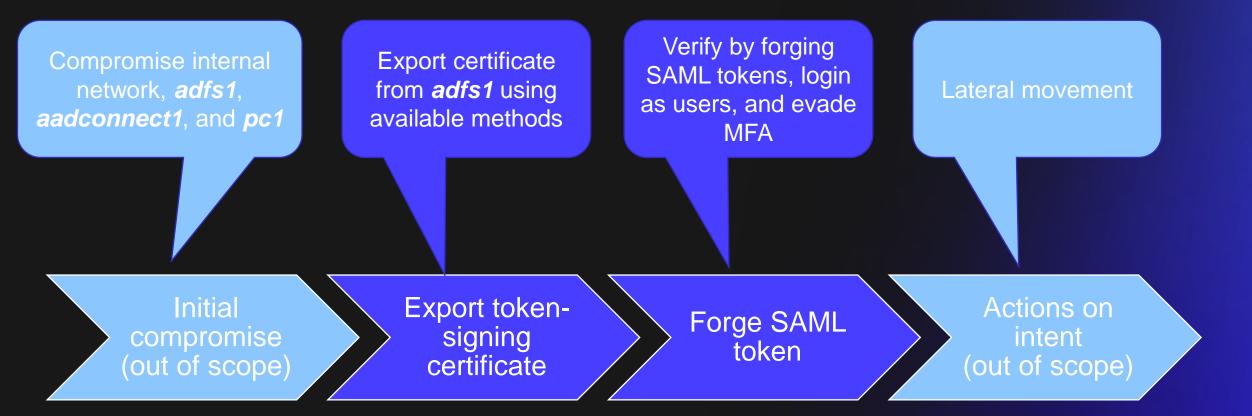
Technical details on how the adversary used the technique.

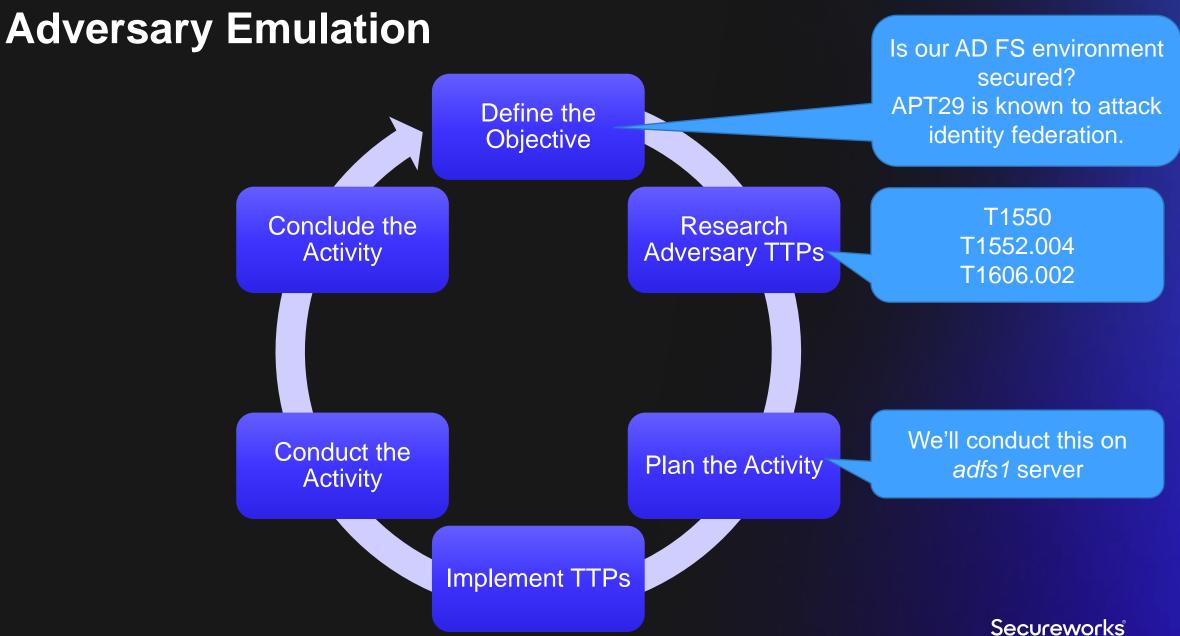
Secureworks

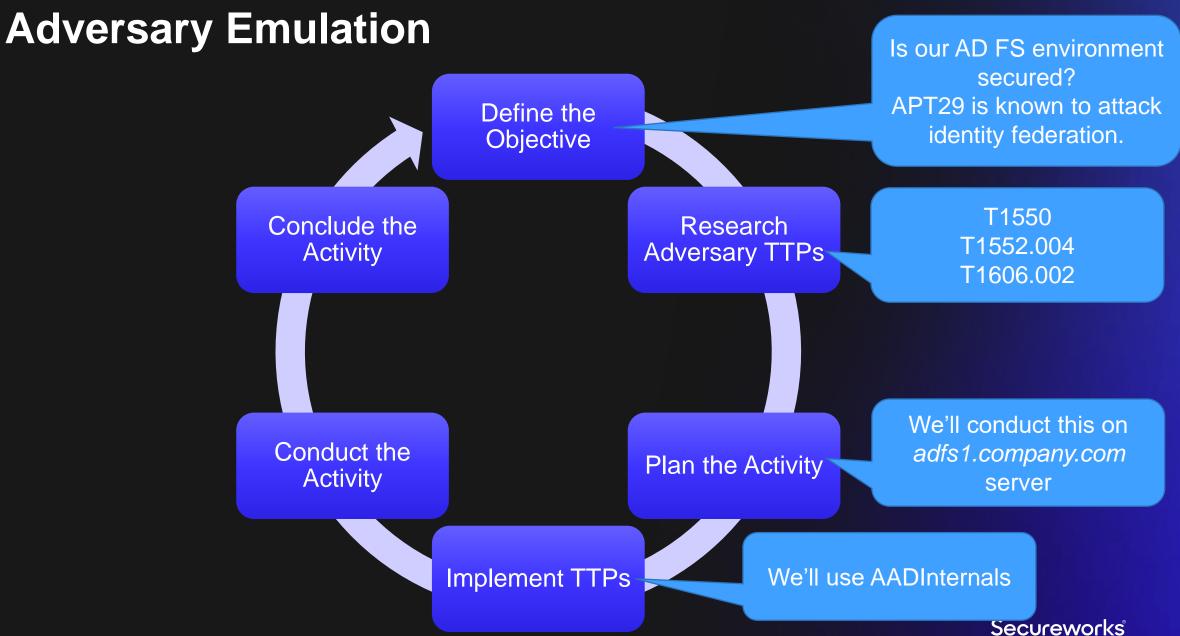
@DrAzureAD



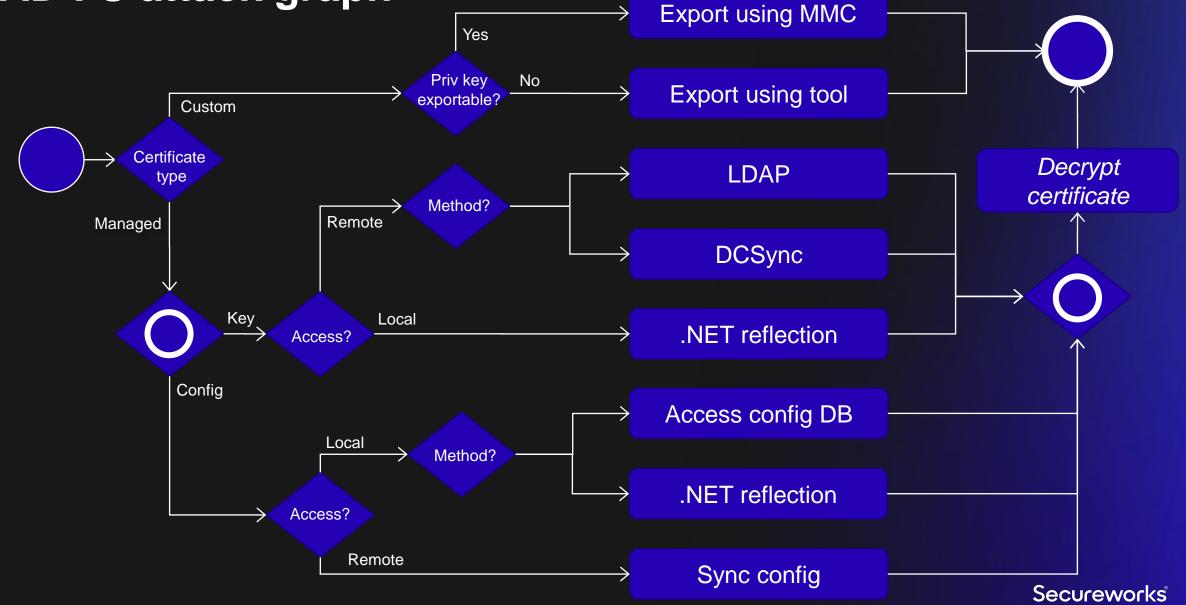
Adversary Emulation Plan







AD FS attack graph



@DrAzureAD **Adversary Emulation** Is our AD FS environment secured? Reporting, APT29 is known to attack Define the recommendations & identity federation. Objective support improvements T1550 Conclude the Research T1552.004 Activity Adversary TTPs T1606.002 We'll conduct this on Conduct the adfs1.company.com Plan the Activity Activity server Execute each TTP. Were they detected? We'll use AADInternals Implement TTPs Were they prevented? Secureworks

Recommendations

- Use unmanaged certificates
- Use Hardware Security Module (HSM)
- Block port 80 to AD FS servers from non-AD FS servers
- Monitor AD FS server events
- Configure Azure AD to reject federated IdP MFA's¹
- Use Pass-through Authentication (PTA)?

1. <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad</u>

Recent research on PTA

T1552.004: Private Keys "steal the identity of PTA agent by exporting the certificate"

> T1071.001: Web Protocols "create an undetectable backdoor"

T1212: Exploitation for Credential Access *"gather credentials"*

T1556: Modify Authentication Process "log in using invalid passwords"

T1498: Network Denial of Service *"perform denial of service attacks"* THREAT ANALYSIS

Azure Active Directory Pass-Through Authentication Flaws

TUESDAY, SEPTEMBER 13, 2022 BY: COUNTER THREAT UNIT RESEARCH TEAM

🎔 in f 🖾

by an organization's

5

Updated: September 20, 2022

Pass-through addition of (PTA) is one of the Azure Active Directory (Azure AD) hybrid identity authentication methods. Photoes on PTA agents installed on one or more on-premises servers. Azure AD uses a certificate-based authentication (CBA) to identify each agent. In May 2022, Secureworks® Sounter Threat Unit[™] (CTU) researchers analyzed how the protocols used by PTA could be exploited. The inducted threat actors could steal the identity of the PTA agent by exporting the certificate to not obtained.

agent to create an undetectable backdoor, allowing threat actors to log in using invalid passwords, gather credentials and performed and performed attacks. Attackers can renew the certificate when comman persistence in the promote for years. A compromised certificate cannot be revoked

researchers shared their findings with Microsoft on May 10, 2022. Microsoft responded on July 2 that PTA is working as intended and gave no indication of plans to address the reported flaws.

Update: On September 20, Microsoft sent an update about their plans to address these issues.

https://www.secureworks.com/research/azure-activedirectory-pass-through-authentication-flaws

Recent research on PTA

PoC for PTA exploitation exist

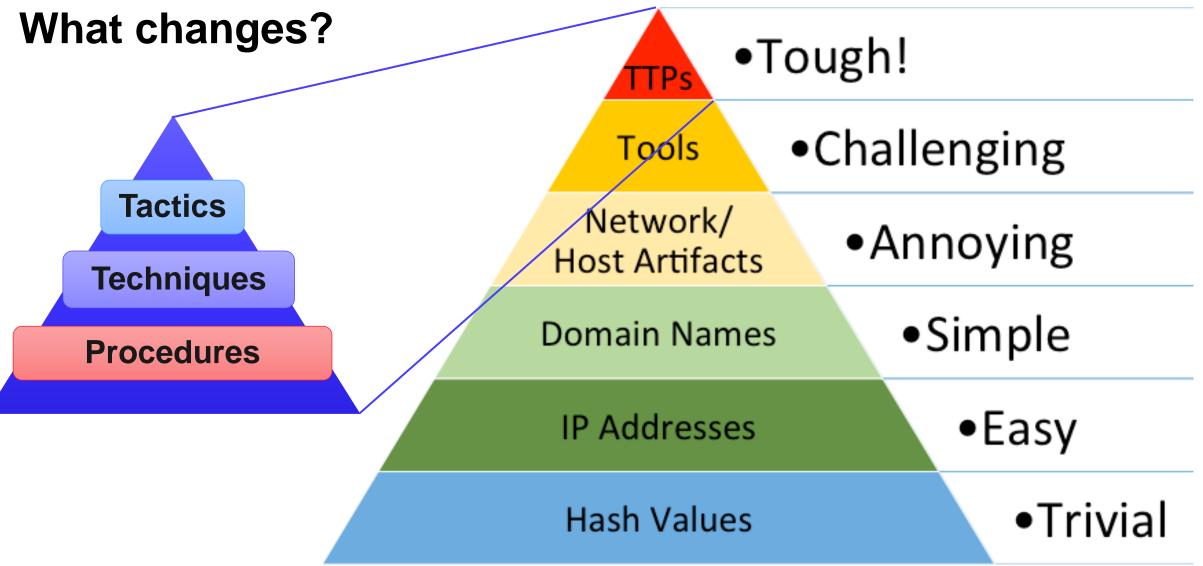
Exploiting Azure AD PTA vulnerabilities: Creating backdoor and harvesting credentials

September 20, 2022

In 13 September 2022, Secureworks published a Threat Analysis: Azure Active Directory Pass-Through Authentication Flaws. The vulnerabilities discovered by our team allows threat actors to gain persistent and undetected access to the target Azure AD tenant.

In this blog post, I'll show how the attack can be conducted using **AADInternals** and standalone Windows server.

https://o365blog.com/post/pta/



Summary

- Adversary emulation helps to protect against specific adversaries that matters to you/your business
- Open-source tools (e.g. AADInternals, Mimikatz,..) can be used to conduct attacks using procedures adversaries are using in real-life
- Before making recommendations, test the alternatives too..

Thank you!



CLOUD IDENTITY SUMMIT '22

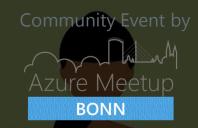
Thu, September 22nd, 2022

00

Ask Me Anything (AMA)

Roundtable discussion and Q&A on experiences from the field and current trends!

Meet the speakers and exchange with members of the community!



Follow us on Twitter

@identitysummit



CLOUD IDENTITY SUMMIT '22

Your Feedback is Important!

https://www.identitysummit.cloud/feedback/

Community Event by



Follow us on Twitter

