Secureworks



Deep-dive to Azure AD Join

@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

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















Contents

- Identities & devices
- Registering & joining devices
- Stealing device identity
- Faking device identity



Recap: identities

Azure AD (AAD) Represents user identity Tenant User **Application** object object Represents device identity Device object

Represents organisation identity

Represents
application
(client) identity

Devices

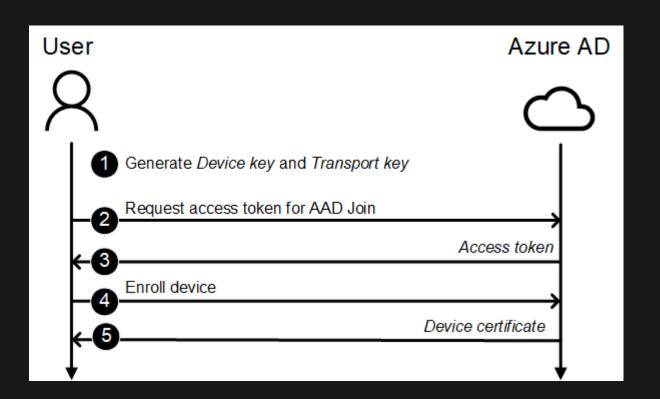
Three join types

Join Type	What	Credentials	Device Management
Registered	Personal PCPersonal/CorporateMobile deviceCloud-only	Microsoft AccountAzure ADLocal account	• Intune
Joined	Corporate PCCloud-only	Azure AD	• Intune
Hybrid Joined	Corporate PCCloud & On-prem	Active Directory	IntuneSCCM

- All device information stored to Azure AD
- Compliance attribute set by MDM

Device join process

- Two set of keys are generated during the join
 - Device certificate: dkpub/dkpriv
 - Transport key: tkpub/tkpriv



Primary Refresh Token (PRT)

- Long-lived refresh token (14 days)
 - Update request signed with the dkpriv
- Requires SessionKey (proof-of-possession key)
 - Encrypted by Azure AD with the tkpub
- Used to (automatically) retrieve access/refresh tokens for Azure AD & Office 365 services
 - Access tokens contain the device claim! (and maybe MFA too)

Certificate locations

- Device certificate *thumbprint* in registry
 - HKLM:\SYSTEM\CurrentControlSet\Control\CloudDomainJoin\JoinInfo
 - HKCU:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WorkplaceJoin\JoinInfo
- Device certificate in machine store
 - Cert:\LocalMachine\My\<thumbprint>
 - Cert:\CurrentUser\My\<thumbprint>
- Device key name in certificate and stored on disk:
 - C:\ProgramData\Microsoft\Crypto\Keys\<keyname>
- Transport key *name* in registry
- Hard coded? No (3) HKLM:\SYSTEM\CurrentControlSet\Control\Cryptography\Ngc\KeyTransp bd0460cca26e8bfae401221e5666af9aaed3528be060534a7e79f32eeff9719e cfc0f173f2be88f14d73677df7beedb055130fea2519b8dc8ab573\5764f8e7da_ a4e17737bd8070136321944fe5e98c1880d424d2d336
- Transport key on disk
 - C:\ProgramData\Microsoft\Crypto\SystemKeys\???

https://o365blog.com/post/deviceidentity/

1ea05

Registry keys "decrypted"

- Registry keys paths are different for Joined & Registered devices
- The path "elements" are SHA256 hashes of Unicode strings of registry values, user's email, etc.

AAD Joined:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Ngc\KeyTransportKey\PerDeviceKeyTransportKey\<idp>\<tenant id>

AAD Registered:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Ngc\KeyTransportKey\<sid>\<idp>\<tenant id>_<user email>

Transport key

- Contains RSA1 blob (public key) and RSA2 (private key)
- Private key encrypted with DPAPI
- To decrypt, elevate to LocalSystem and Unprotect (
 - [Security.Cryptography.ProtectedData]::Unprotect(\$ privateKeyBlob, <entropy>, "LocalMachine")
 - <entropy> = "6jnkd5J3ZdQDtrsu" + null terminator
- To get all RSAParameters, convert from RSA2 to RSA3

Stealing device's identity

- Target device:
 - Compromise the target device
 - Get local admin privileges
 - Export device certificate & device + transport keys



- Attacker's device:
 - Create PRT token using exported certificate and keys
 - Log in as target user



Faking device identity (and compliance?)

"Join" fake device to Azure AD



- Configure target device to use certificate & keys of the fake device
- Log in as target user



Thank you!

Questions?

Secureworks