Secureworks®

Secureworks® Primary Refresh Token (PRT) viewer

@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), MVR

Contact details

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

MVP Microsoft Most Valuable Professional

Microsoft Most Valuable Security Researcher ESTD. 2021 VOLUME

Microsoft Certified Trainer Microsoft MCT Trainer 2022 - 2023

Microsoft 365 Certified Enterprise Administrator Expert

Microsoft Certified Azure Solutions Architect Expert

Microsoft 365 Certified Security Administrator Associate

Microsoft Certified Identity and Access Administrator Associate

Contents

- Introduction
- Installation on Burp Suite
- Preparing target endpoint
- Decrypting and monitoring traffic

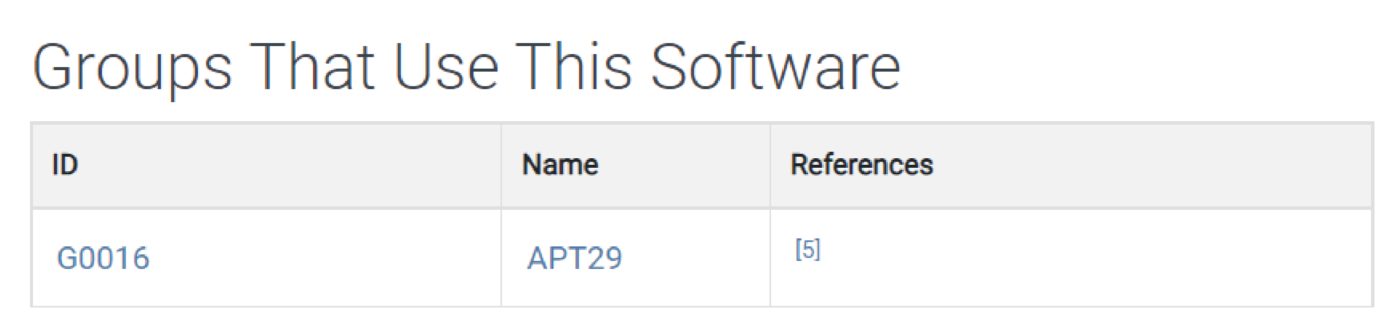
Secureworks® Primary Refresh Token (PRT) viewer

- Opensource add-on for Burp Suite and Fiddler classic
- Available at:

  `https://github.com/secureworks/primary-refresh-token-viewer`
- Helps to monitor traffic between AAD joined devices and Azure AD
- Decrypts:
  - Session key from PRT request
  - Content encrypted with key derived from session key and ctx

AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
  - https://github.com/gerenios/aadinternals
  - https://o365blog.com/aadinternals/
- MITRE ATT&CK
  - https://attack.mitre.org/software/S0677/

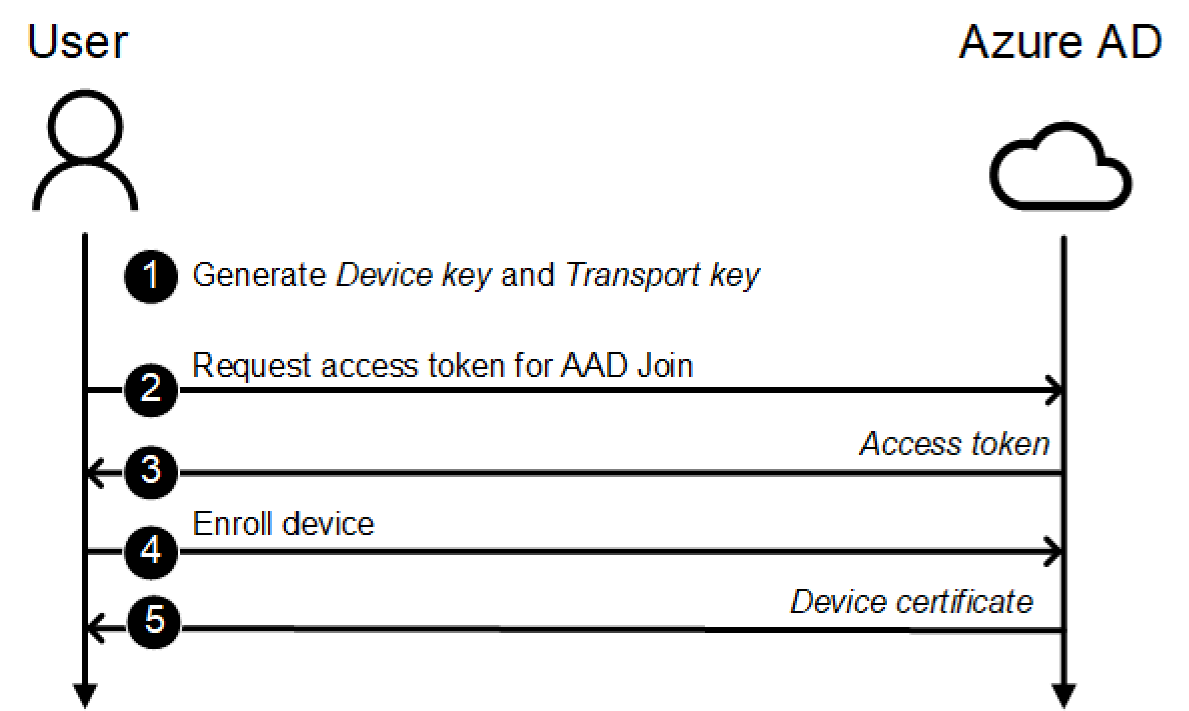


Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

Device join process

- Two key pairs (*dkpub/dkpriv* and *tkpub/tkpriv*) are generated
- Public keys sent to Azure AD
- Device key (certificate) represents the device (*dkpub/dkpriv*)


User
Azure AD
1 Generate *Device key* and *Transport key*
2 Request access token for AAD Join
3 *Access token*
4 Enroll device
5 *Device certificate*

Secureworks®

Primary Refresh Token (PRT)

- Long-lived refresh token (~~14~~ 90 days)
- Updated using the device certificate
- Used to (automatically) retrieve access/refresh tokens for Azure AD & Office 365 services
  - Access tokens contain the device claim!

https://aadinternals.com/post/prt/

Obtaining the PRT

- Requires:
    - Proof-of-identity of the user
    - Proof-of-identity of the device
        - Request signed with device certificate’s *dkpriv*
    - Transport key *tkpriv*
        - Response includes session key, encrypted with *tkpub*

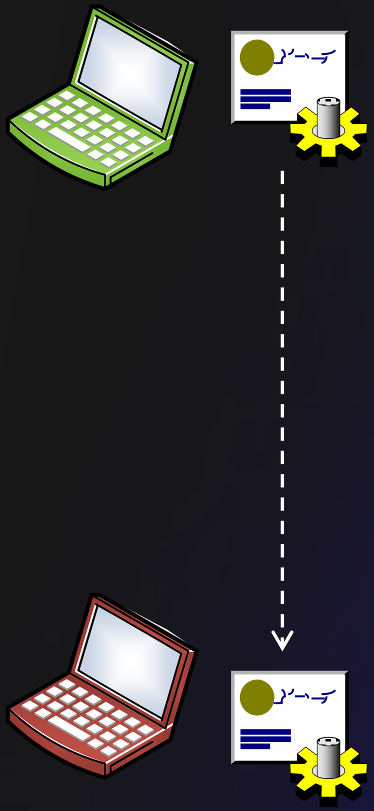
Obtaining tokens with the PRT

- Requires:
    - PRT
    - Session key
        - Request signed with a key derived using KDF/KDFv2
- Response contains access token:
    - User identity
    - Device identity
    - Login method (RSA,WIA,PWD,MFA)

Decrypting and monitoring

- Target device:
  - Configure the target device
  - Export transport key

- Monitoring device:
  - Import transport key



Secureworks®