

SESSION ID: CTF-T09

Cloud CTF 201: Solving Capture-The-Flag Challenges in AWS, Azure, GCP

Jenko Hwong

Threat Research
WideField Security

Luis Rivas

Network System Engineer
Department of Defense

Azure Challenge Walkthrough

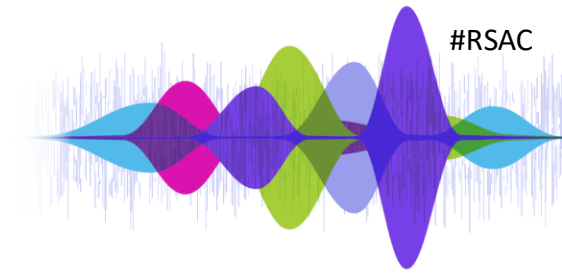
A decorative graphic at the bottom of the slide. It features a series of thin, vertical, light blue lines of varying heights on the left side. To the right of these lines is a series of overlapping, rounded, teardrop-like shapes in various colors: light blue, purple, magenta, green, and light purple. These shapes are arranged in a way that they appear to be part of a larger, abstract pattern, possibly representing a signal or a network.

Many Voices.
One Community.

General

- Hard to Insane Azure Challenge
- Azure TTP focus
- Heavy game theme/puzzles (mixed)
- Tried to use recent real-world TTP
 - User **discovery**
 - OAuth device code **phish**
 - Microsoft SSO (Azure – Apps)
 - Lateral movement / stealth (tenant #2, **deleteItems**)

Starting point



- <http://erebos0.cloudy-daze.com:8080>
- HTTP Auth user: idq
- HTTP Auth pwd: XXXXXXXX

The Map



The Scroll

To cross the threshold into the cerulean skies of **Zurea Terna Di**, seek the **Novitiate's Pegasus Sword askew**. Then fathom how **the White's Hotau Wolf** can be **co-deceived**. The incantations thou requirest were cast by **Razed Dura** or **Anonymise Trio**. The whispered lore to askance traverse is a **foci** on **Wuker's Corse**, while **Signo Ginnels** shall ascendeth thee. Tame the **Viper Cleric's pain** amidst a **tonne** of **tan earth**, and thou shalt be bestowed a revelation and a cryptic **gonfalon**. The Oracle can see **Naga Ram's** true nature.

To gain access into the azure region of **Azure Entra ID**, find the **Apprentice's weak password guess**. Then figure out how **Gandalf's OAuth Flow** can be **Device Code**. The techniques you require were first used by **DrAzureAD** or **Nestoori Synamaa**. The secrets to lateral movement is **SecureWorks FOCI**, while **Single Sign-On** shall escalate you. Control the **Service Principal** in **another tenant**, and you will receive a big insight and an encrypted **flag**. The Oracle can see **anagrams'** true meaning.

The Attack Path

Identity Quest

- Recent, relevant IAM techniques
- Hard, Fun, Feasible
- Azure + Office



1 IDOR (eop)
[Web app + SDK|PS|API]

2 Brute Force (access)
[Web MSFT Portals]

3 OAuth Device Code Phish (access)
[Email + SDK|PS|API]

Insane++ Dials

1. Minimal Clues
2. Use diff client id than Outlook (SW FOCI list)
3. Undelete SP



web app
vm: idq-web-vm-dev2
managed id: idq-web-vm-dev2
rg: identity-quest

SSRF (access/eop)



quandrix@
Guest



gandalf@
Guest

Phishing victim daemon (gandalf@) on web VM: auto checks email, auto device code login w/ MFA, emails response

Tenant 1: Cloudy Daze

cloudydaze.com

Azure Entra ID (discovery)
user enumeration

Azure Blob (discovery)
meeting_20240601.md

sa: idqdevsa
sc: idqdevsc
rg: identity-quest-wizards

Teams Chat (discovery)
merlin, gandalf, quandrix

Office 365

OneDrive File (data)
2 decrypt keys: pt, de

Office 365

Azure Blobs (data)
1 decrypt key: cry
encrypted FLAG: gonfalon

sa: idqdevgandalfsa
sc: idqdevgandalfsc
rg: identity-quest-gandalf

Tenant 2: Cloudy Daze Test

cloudydazetest.onmicrosoft.com

Blob (data)
1 decrypt key: key

sa: idqtest2sa
sc: idqtest2sc
rg: idqtest2

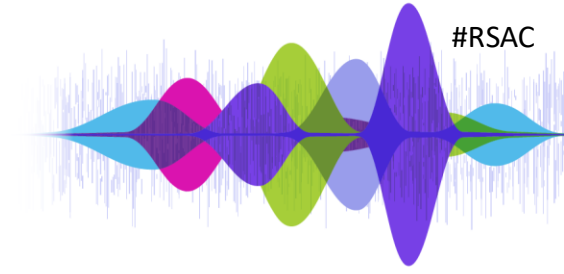
5 Change secret (eop)
sp: sp_test2 (orig: temp delete status, requiring undelete)

Blob (data)
readme.txt (nothing burger)

sa: idqtestsa
sc: idqtestsc
rg: idqtest

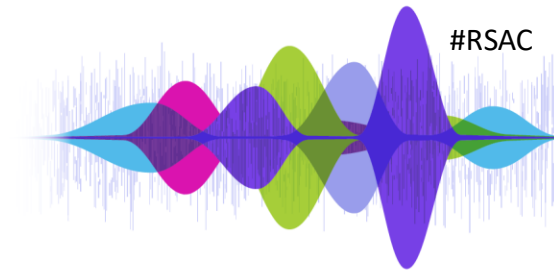
4 Tenant Switch (lateral movement)

Attack Steps



1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys
4. Lateral move: tenant switch
5. Priv esc: service principal takeover -> more decrypt keys
6. Actions: decrypt flag

Attack Steps



1. Web->Azure

- IDOR

`u=0`

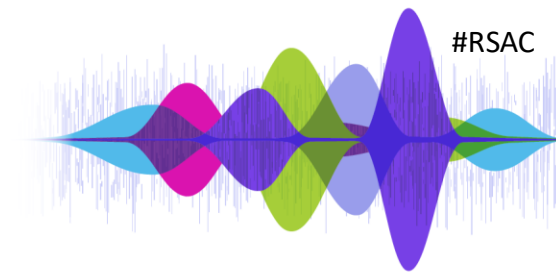
- SSRF -> IMDS

`http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://management.azure.com -H Metadata:true`

- File clues + User Enum

`do_attack_web_1.sh (option 3,2)`

Attack Steps



1. Web->Azure

— File clues + User Enum

`do_attack_web_1.sh` (option 3)

Morgana: One of our very own, Quandrix, seems to have been very lax in his secrets accounts.

Gerald: In Rivia, some of our elves picked obvious secrets that could be guessed. Like home towns and birthdays.

Harold: Or start dates in the Guild. He's as dumb as Tom.

Marvolo: Harold little boy it's almost time for another lightning tattoo. Morgana, what needs to be done about Quandrix.

Rand: I think the problem was that Quandrix knows better and intended to change, but the pen test happened and one of his portal accounts in Zurea got hacked. It was just a testing account...

Merlin: Rand, you know the renegade elves stole some treasure because one of our development wizard realms was connected to our production one... we were lucky our Ignoble Handling sorcerers responded so quickly.

Morgana: Quandrix is prone, like many of our lower creatures, to pick easy to guess not-so-secrets, and never change them, so he's susceptible to brutes who force and spray their way into his mind. But some of his secrets can just be guessed because he tends to use public information easily found in the Terna Di region of Zurea.

Tom: Let me guess, he's still using that school he loves. And some date that everyone knows...

Attack Steps

1. Web->Azure

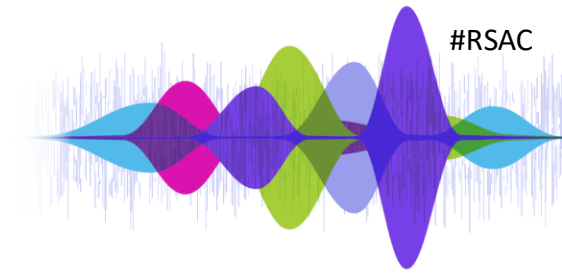
— File clues + User Enum

do_attack_web_1.sh (option 2)

```
{  
  "businessPhones": [  
    "bday: 08/13",  
  ],  
  "displayName": "Quandrix Apprentice",  
  "givenName": "Quandrix",  
  "jobTitle": "School of Mages",  
  "mail": "quandrix@cloudy-daze.com",  
  "mobilePhone": "start: 01/22",  
  "officeLocation": "Strixhaven",  
  "preferredLanguage": null,  
  "surname": "Apprentice",  
  "userPrincipalName": "quandrix@cloudy-daze.com",  
  "id": "c0824d07-6f39-4e45-8fdd-47c85bba7970"  
},
```

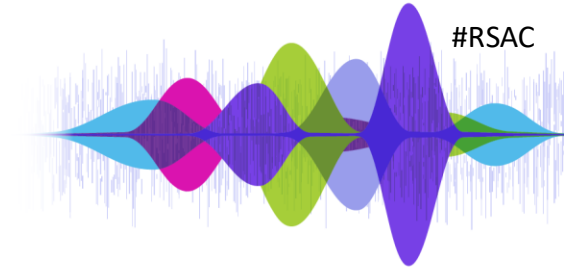
GET <https://graph.microsoft.com/v1.0/users>

Attack Steps



1. Web->Azure
2. User discovery: Guess creds -> quandrix -> Chat discovery

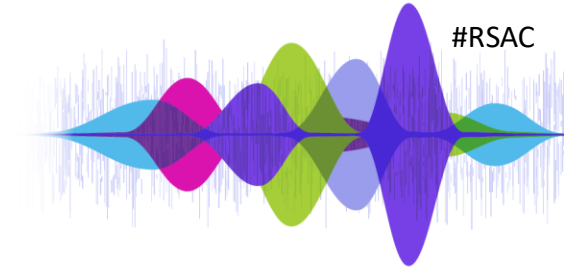
Attack Steps



1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys

`do_attack_2.sh`

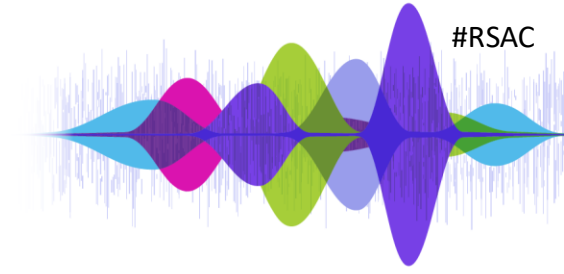
Attack Steps



1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys
4. Lateral move: tenant switch
5. Priv esc: service principal takeover -> more decrypt keys

```
az cli login (merlin @ Test Tenant)  
do_attack_assume_sp_get_blob_3.sh
```

Attack Steps



1. Web->Azure: IDOR -> SSRF -> IMDS -> File clues + User Enum
2. User discovery: Guess creds -> quandrix -> Chat discovery
3. Privileged phish: OAuth device code phish -> Gandalf -> encrypted flag + partial decrypt keys
4. Lateral move: tenant switch
5. Priv esc: service principal takeover -> more decrypt keys
6. Actions: decrypt flag

`do_attack_get_flag_4.sh`