Resilience of the VO membership vetting process

AKA seeing social accounts handled in an satisfying way

Baptiste Grenier

SDIS Officer, IRTF member

2023/06/21

Report on EGI CSIRT activities

TLP:CLEAR Public

A bit of context

- Chit chats between some IRTF members, with the SSC in the background, leading to the idea of testing the vetting process of a cloud VO, using an identity from a social media platform
  - "What is needed to start a VM in fedcloud? A registered account in a VO?
  - "Maybe we should get some social media accounts and check if they get accepted there :-)"
  - "Sure, seem an interesting exercise, let's do it!"

Motivation

Open Science and Open Access do not mean there is no need to control who can use resources and services

- Many **security incidents** caused by the, **possibly on purpose**, **lack of authorisation and vetting** when granting access to resources and services. Social media IdPs, like Google, are providing unlimited accounts allowing to verify an email for free.

  - [EGI-20210318-001] **Proxying of nefarious content** via a misconfigured IaaS platform allowing anyone to create a local account and deploy services.
  - [EGI-20210430-01] **Crypto-mining** on a JupyterHub notebook, access granted without any vetting to every Check-in user.
  - [EGI-20220107-01] **Crypto-mining** on a JupyterHub notebook, access granted without any vetting to every Indigo IAM user. Also possible to access by creating a local account with just a mail verification.
  - [EGI-20220114-01] **Crypto-mining** on a JupyterHub notebook, access granted without any vetting to every Check-in user.

#0: pretext impersonating a researcher in need of cloud resources

Welcome Dr Sobchack

- Dr Walter Sobchack is a researcher, looking for cloud resources to do some analysis in the context of their research
  - **Identity card**
    - Name: Walter Sobchack
    - Title: Dr
    - Institute: Nizhny Novgorod State Academy of Medicine (Russia)
    - Email: dr.walter.sobchack@gmail.com
  - **Research papers - online proofs**
    - https://www.researchgate.net/scientific-contributions/DM-Sobchak-33763131
      - Content already available online, from a real researcher with a similar name
  - **Inspiration: Walter Sobchak character from "The Big Lebowski" movie**
    - https://coenbrothers.fandom.com/wiki/Walter_Sobchak

1: Getting a social media account integrated with Check-in

May options to choose from

- Google, GitHub, ORCID, LinkedIn…
- Decided to go with a **Google account** as it also provides a convenient way to have a **working email address**
  - **Easy to create and manage**
  - **One requirement:** having a phone number used at account creation

1: Dr Walter Sobchack's Google account

An easy first step

- Welcome Dr Sobchack!
  - **Email**: dr.walter.sobchack@gmail.com

#2 getting a Check-in account associated with the GMail account

Check-in account is one email verification away

- Registering and managing EGI Check-in account at https://aai.egi.eu/registry

#3: enrolling to a VO for piloting activities

Looking for "easily" available resources

- See https://docs.egi.eu/users/getting-started/#get-access-to-pilot-allocation

#3: enrolling to a VO for piloting activities

vo.access.egi.eu: a Check-in managed and cloud-enabled VO for piloting activities and the Long Tail of Science

- VO ID Card: https://operations-portal.egi.eu/vo/view/voname/vo.access.egi.eu
- VO managers from EGI Foundation
  - EGI Community Support Team (CST)
    - https://www.egi.eu/egi-foundation/team/#cst
  - EGI Technical Solutions Team (TST)
    - https://www.egi.eu/egi-foundation/team/#tst

  - Members on duty following a rota
  - Reviewing and vetting access requests
  - According to a clearly defined vetting procedure

#3: enrolling to a VO for piloting activities

Investigating public information about the VO

- Cloud Compute EGI Service: https://docs.egi.eu/users/compute/cloud-compute/
  - Supporting sites, images and flavours: https://appdb.egi.eu/store/vo/vo.access.egi.eu

#3: enrolling to a VO for piloting activities

Using Check-in to enroll to the VO

- **Enrolling**: https://aai.egi.eu/registry/co_petitions/start/coef:240

#4: Going through the vetting process

Welcome message and discussing the justification for requesting resources

#4: Going through the vetting process

Checking the Affiliation. Pointing to Dr Sobchak's research on ResearchGate…

DM Sobchak's research while affiliated with Nizhny Novgorod State Academy of Medicine and other places

#4: Going through the vetting process

Not enough trust, please use a higher assurance level Identity Provider

- Well done guys, better not let me in!

#5: Are we done?

Going through the list of available VO in Check-in, opened to self-enrollment

- Currently 118 available VO available for self enrollment

#6: Knocking at heaven's door

Trying to enrolling to the first 25 VOs, requesting or not to write a comment to justify request

#6: Doors staying closed

No VO managers granted access to Walter…

#7: Triggering alerts in EGI Foundation

EGI Foundation Central VO management team getting suspicious

Search: we have a similar

Thread # fedcloud

[redacted] 5 days ago

Hi @Baptiste , we have a similar account to the one above, who has been trying to get access to our infrastructure multiple times. He claimed to be a Russian scientist.
Should I create a GGUS ticket to Check-in or write to ism@ to have the account suspended? I am a bit afraid that someone will approve the request by mistake. (edited)

[redacted] 5 days ago

Wlater Sobchack (dr.walter.sobchack@gmail.com)

```
wsobchack (UID)
2b8782438b6457177fc3dd7ec094e078c5fd85581eff6e5798ffae5aaa17903f@egi.eu (ePUID)
dr.walter.sobchack@gmail.com (Official, Verified)
Groups:
CO:COU:cloudferro.com:members:all
CO:COU:creodias.eu:members:all
CO:COU:datafurn.eosc-hub.eu:members:all
CO:COU:desy-cc.de:members:all
CO:COU:digifarm.io:members:all
CO:COU:vo.i-nergy.eu:members:all
CO:COU:eosc-synergy.eu:members:all
CO:COU:covid19.eosc-synergy.eu:members:all
CO:COU:crystal_channelling_simulation.vo.egi.eu:members:all
CO:COU:d4science.org:members:all
CO:COU:dteam:members:all
CO:COU:ehoney.infn.it:members:all
CO:COU:cloud.egi.eu:members:all
CO:COU:cesga.es:members:all
CO:COU:biinsight.eosc-hub.eu:members:all
CO:COU:benchmark.terradue.com:members:all
CO:COU:belle:members:all
CO:COU:aiidalab-demo.materialscloud.org:members:all
CO:COU:vo.access.egi.eu:members:all
CO:members:active
CO:members:all
```

[redacted] 4 days ago

[redacted] opened the ticket: https://ggus.eu/index.php?mode=ticket_info&ticket_id=159402
But I would also like to get your opinion.
My concern is that the Check-in team takes longer to process the request and, in the meantime, the guy is accepted by any [redacted] Manager by mistake. He could do some damage, not only destroying things but perhaps creating some persistent access and moving laterally.
This guy was not like the previous attempt, where someone requested access to many VOs just to see if he/she was lucky to be accepted. This guy actually used social engineering on us, tried to convince us that he was a [redacted] researcher working on varicella, showed a list of publications, etc. (edited)

- In fact many VOs are managed by the EGI Foundation team
  - They got multiple access requests from the same user
  - => reported to the EGI Foundation Information Security Manager, asking for support

#7: Requesting the account suspension

EGI Foundation Central VO management team taking actions

- Requesting account suspension in GGUS

#7: A VO manager reporting to EGI CSIRT

EGI Foundation Central VO management team getting suspicious

- First report about suspicious activity sent to it-support@egi.eu
- Identifying the pretext's context
- Then forwarding to abuse@egi.eu

Lessons from the exercise

It was both successful (from a defender side) and a failure (from an attacker side)

- **What went well**
  - Dr Sobchak **never got access to any resources**
  - **Vetting** of vo.access.egi.eu was very **effective**
    - Professional tone in communication
    - Following a defined procedure, looking for:
      - Justifications for accessing the resources
      - Justifications on the identity, researcher status and institute
      - Asked for using a Identity Provider providing more assurance
  - **Reporting** dubious activity to the **local security team**
  - Taking **protective measures** (account suspension)
    - Check-in team was reactive, account got blocked
  - A VO manager **reported** suspicious request **to EGI CSIRT**

- **What may be improved**
  - Account suspension request in GGUS should have been managed with the involvement of the local security team and possibly of the EGI CSIRT
  - It's possible to easily discover many VO and try to enroll, hoping that a VO manager may overlook something during the vetting

- **Follow-up**
  - Promoting/sharing VO vetting procedure
  - Discussing how to improve trust and vetting of identities
  - Re-used this approach during the SSC

EGI Security Service Challenge

- Overall goal: **deploying VMs for an attack** spreading across the EGI infrastructure and services
- Some mapping with MITRE ATT&CK knowledge base:
  - Establish Accounts via a Trusted Relationship, interacting with a Command and Control aiming at doing Resource Hijacking
- Persona:
  - Uli Kunkel, **a German staff researcher**
  - Account from an **eduGAIN-federated trusted IdP**
  - **Online presence** to appear more legitimate
    - **A personal page** created
    - Real researchers having similar names and public information, including publications
- **Caught during** the initial **vetting** process
  - **Kudos to the VO managers!**
  - Eventually joined a VO allowing to deploy VMs…

An adventure that involved EGI's "Security dude"

Contact us

baptiste.grenier@egi.eu

EGI CSIRT: security-requests@egi.eu

Get in touch with us

Let's talk. Or
meet in person

www.egi.eu

This work is partially funded by the EU research and innovation programme