Simulation of a large-scale security incident - keep juggling a lot red/blue/purple balls

Daniel Kouřil [1,3]   Sven Gabriel [2,3]

[1]CESNET   [2]Nikhef   [3]EGI CSIRT

Introduction

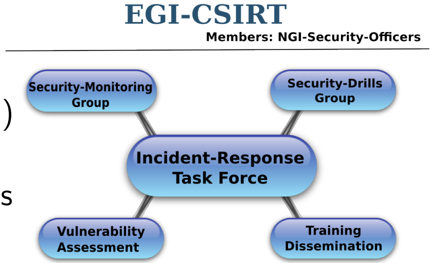
Overview

- Outline of the presentation
- EGI CSIRT
- What is the infrastructure, what are the questions to be answered
- Identities, Access and Red Team introduction
- Attack Infrastructure and CTF
- Results/Conclusions

EGI-CSIRT

EGI CSIRT objective: provide the EGI infrastructure with incident response capabilities across the participating NGIs.

- Project wide coordination of operational security activities.
- Interfacing to other (Grid/NREN/VO, IdP) CSIRTs
- EGI-CSIRT central tasks, security activities coordination


EGI-CSIRT
Members: NGI-Security-Officers
Security-Monitoring Group
Security-Drills Group
Incident-Response Task Force
Vulnerability Assessment
Training Dissemination

What, Why, How I

Goals of the Security Service Challenge (SSC) I, Assessment Security Incident Management

- EGI CSIRT: Test our incident response capabilities, are our procedures ready to deal which a multi Resource Center (RC) incident
- Assess the required collaboration with partner Security Teams (OSG, eduGAIN)
- How does it look at boarders? Collaboration with Identity Providers Security teams
- Does the infrastructure indeed looks the same as the last time we looked at it?

What, Why, How II

Goals of the Security Service Challenge (SSC) II, Assessment of the Incident Response capabilities, Forensic skills.

- Communications: response times, relevant content.
- Containment: act on a compromised account, suspend access to the infra
- Stop, and analyse malicious activities -
- → Capture the flag `https://ctf.egi.eu/`

The Playground

The playground, Context, LHC

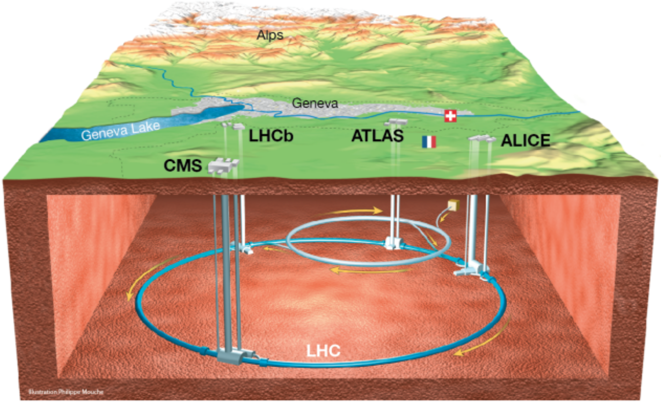
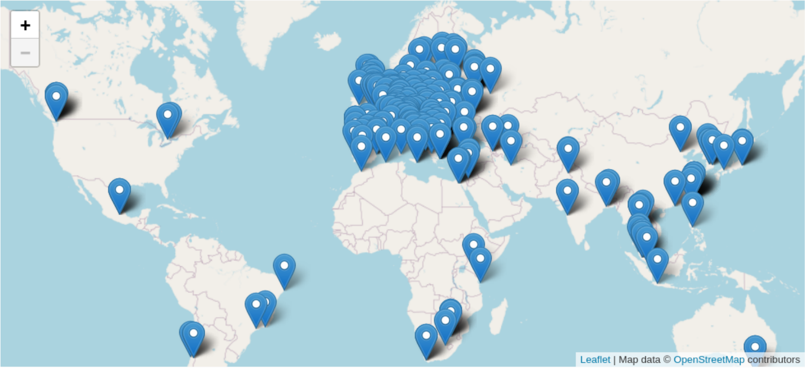


Illustration Philippe Mouche

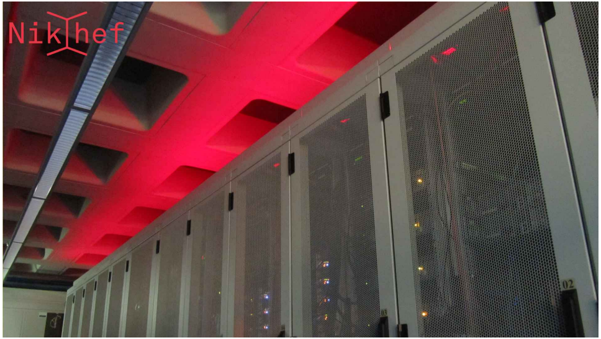
The playground, Context, Resource Centers



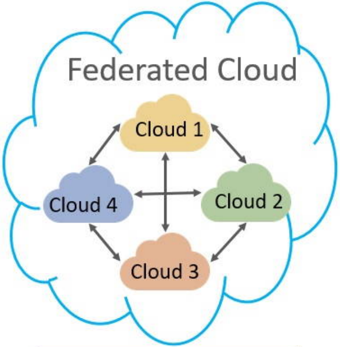
243 sites certified, CMS VO has 4827 users, and can use 52 RCs coordinated by EGI

The playground, type of resources

Compute Clusters



Clouds


Federated Cloud

Cloud 1

Cloud 4

Cloud 2

Cloud 3

Federated Cloud

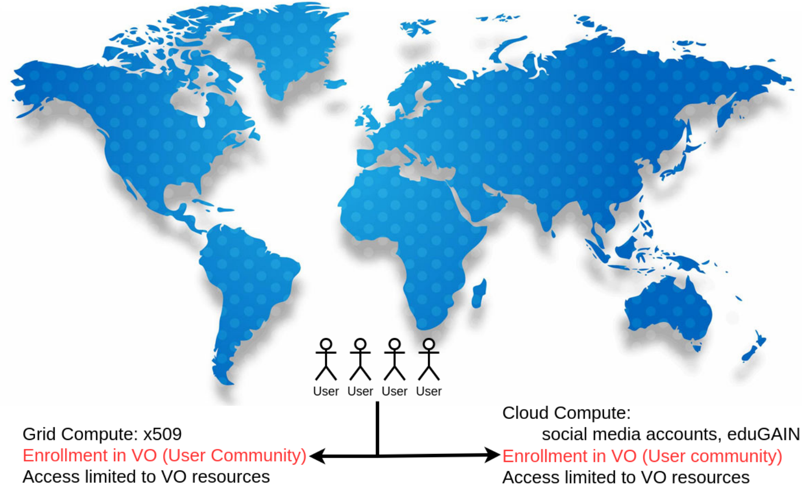
The playground, Organisational Borders

243+ Resource Centers distributed over 40+ countries in WLCG are coordinated through the following organisations:

- OSG `https://osg-htc.org/networking/`, US based RCs
- The Nordic e-Infrastructure Collaboration , `https://neic.no/`, northern Europe.
- EGI `https://egi.eu`, ... the rest

A tempting target for crypto currency mining, d-dosing, ...
To get ready the Incident Response Procedures have to be harmonized across the organisations. .

The playground, The User



Grid Compute: x509
Enrollment in VO (User Community)
Access limited to VO resources

Cloud Compute:
social media accounts, eduGAIN
Enrollment in VO (User community)
Access limited to VO resources

Access to the Playground, Identities

Access, Identity Providers

- x509 certificates, CAs
  - meanwhile often coupled to institutes HR data
  - migration to tokens started.
- IdP proxy (egi-checkin)
  - Federated Identity Providers (eduGAIN)
  - Social Media accounts
  - EGI Check-in serves as a seamless bridge, enabling more than 17,500 registered users to access 150+ services effortlessly, using their own institutional identity providers and community AAI services.

Access, compromised Identities

- x509 certificates, CAs
  - Certification revocation, strict rules on revocation, but possible
- IdP proxy (egi-checkin)
  - eduGAIN provides through SIRTFI a handle for Incident Response
  - good luck with social media accounts

Access through Virtual Organisations

Access, Virtual Organisation

- Users are not granted access to the resources directly, rather they have to join a Virtual Organisation (VO)
- A VO is a group of people (e.g. scientists, researchers) with common interests and requirements, who need to work collaboratively and/or share resources (e.g. data, software, expertise, CPU, storage space) regardless of geographical location.
- VOs can suspend their users based on token, certificate DN.
- RCs decide which VO they support, grant access to (a fraction) of their local resources, RC can block access for individuals, based on their certificate DN.

The Red Team

Red Team, the attack plan

Goals: Use the nice Playground for own purposes

- Crypto Currency Mining (we must not make money from the resources, start own currency (egoin))
- Rent out the resources under our control for DDoS campaigns, ...

Scenario

- Get credentials, and use them for ...
- Deploy an attack infra (command and control system, ...)
- Create a Botnet on the infrastructures
- Does this seem unrealistic? Well, no.

Red Team, the attack plan, needed ingredients

3 Major ingredients

- Credentials that give access to High Throughput computing
- Credentials that gives access to Cloud Resources to host the attack infra
- Attack infra

Get Identities, access to the infrastructure

Access to Compute clusters

x509 credentials registered at CMS VO

- Coordinate with CMS VO to provide credentials used for the SSC

Access to Cloud Infras

Identities from Social Media and Federated Identity Providers (ex. eduGAIN) can be used in egi-checkin (IdP proxy)

Motivation: several incidents with crypto currency mining, hosting of problematic material, lets make this part of the exercise.

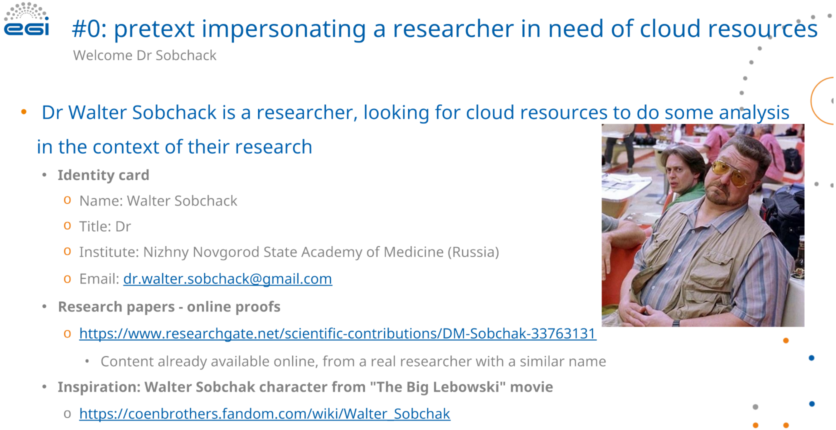
- Social media account, well that's easy ...
- Identity from Federated IdP.
  - Find IdP that wants to collaborate on this security research project, *thanks DFN-AAI*
  - Invent a person, and provide it with some identity.
  - Enrol this identity in a VO that has access to cloud resources.
  - ...see next slides *Resilience of the VO membership vetting process*

What people get to in after work sessions

Every Identity needs some background to stay consistent, lets try this:

Next slides by Baptiste Grenier, Senior Service Delivery and Information Security Officer, EGI.

What people get to in after work sessions



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

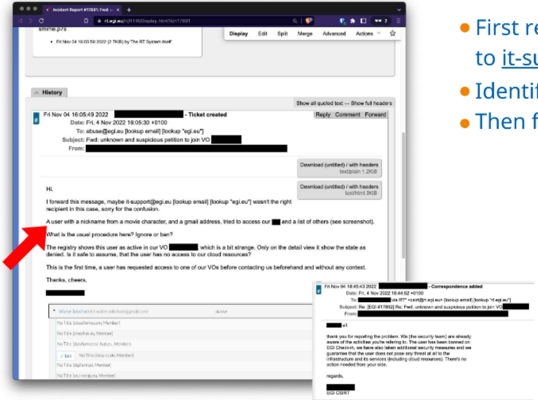
Welcome Dr Sobchack

- 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

What people get to in after work sessions

#7: A VO manager reporting to EGI CSIRT

EGI Foundation Central VO management team getting suspicious



Incident Report #17891: Fwd: u
rt.egi.eu/rt/RTIR/Display.html?id=17891
Display Edit Split Merge Advanced Actions

smime.p7s

- Fri Nov 04 16:05:50 2022 (2.7KiB) by The RT System itself

History
Show all quoted text — Show full headers
Reply Comment Forward

Fri Nov 04 16:05:49 2022 [redacted] - Ticket created

Date: Fri, 4 Nov 2022 16:05:30 +0100
To: abuse@egi.eu [lookup email] [lookup "egi.eu"]
Subject: Fwd: unknown and suspicious petition to join VO [redacted]
From: [redacted]

Download (untitled) / with headers
text/plain 1.2KiB
Download (untitled) / with headers
text/html 3KiB

Hi,

I forward this message, maybe it-support@egi.eu [lookup email] [lookup "egi.eu"] wasn't the right recipient in this case, sorry for the confusion.

A user with a nickname from a movie character, and a gmail address, tried to access our [redacted] and a list of others (see screenshot).

What is the usual procedure here? Ignore or ban?

The registry shows this user as active in our VO [redacted] which is a bit strange. Only on the detail view it show the state as denied. Is it safe to assume, that the user has no access to our cloud resources?

This is the first time, a user has requested access to one of our VOs before contacting us beforehand and without any context.

Thanks, cheers,

[redacted]

Walter Sobchack (drwalter.sobchack@gmail.com) Active
No Title (cloudferro.com, Member)
No Title (creodias.eu, Member)
No Title (datafum.eosc-hub.eu, Member)
✓ Edit No Title (dear-code, Member)
No Title (digifarm.io, Member)
No Title (vo.i-nergy.eu, Member)

Fri Nov 04 18:45:43 2022 [redacted] - Correspondence added

Date: Fri, 4 Nov 2022 18:44:52 +0100
To: [redacted] via RT" <csirt@rt.egi.eu> [lookup email] [lookup "rt.egi.eu"]
Subject: Re: [EGI #17892] Re: Fwd: unknown and suspicious petition to join VO [redacted]
From: [redacted]

[redacted] all

thank you for reporting the problem. We (the security team) are already aware of the activities you're refering to. The user has been banned on EGI Check-in, we have also taken additional security measures and we guarantee that the user does not pose any threat at all to the infrastructure and its services (including cloud resources). There's no action needed from your side.

regards,

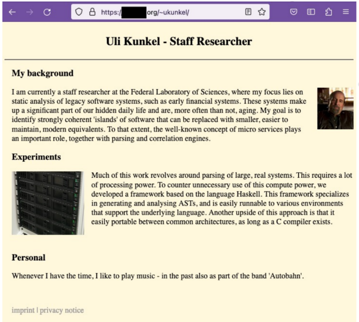
[redacted]
EGI CSIRT

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

What people get to in after work sessions

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...


https:/[redacted]org/~ukunkel/

Uli Kunkel - Staff Researcher

My background

I am currently a staff researcher at the Federal Laboratory of Sciences, where my focus lies on static analysis of legacy software systems, such as early financial systems. These systems make up a significant part of our hidden daily life and are, more often than not, aging. My goal is to identify strongly coherent 'islands' of software that can be replaced with smaller, easier to maintain, modern equivalents. To that extent, the well-known concept of micro services plays an important role, together with parsing and correlation engines.

Experiments

Much of this work revolves around parsing of large, real systems. This requires a lot of processing power. To counter unnecessary use of this compute power, we developed a framework based on the language Haskell. This framework specializes in generating and analysing ASTs, and is easily runnable to various environments that support the underlying language. Another upside of this approach is that it easily portable between common architectures, as long as a C compiler exists.

Personal

Whenever I have the time, I like to play music - in the past also as part of the band 'Autobahn'.

The Attack Infrastructure

Red Team, Find the right people

- Use the usual job submission systems to send a bot.
  - Expert knowledge from various areas.
- Bot connects to C2.
- Command the bots to create noise, that the local teams should detect.

Red Team Engineering

Build a framework to talk to frameworks that talk to frameworks that talk to compute elements that run our malware that returns commands that runs some other file that talks to another framework that looks like actual malware.

Red Team, Start the SSC

Murphy's Law, obviously

- C2 Software breaks spectacularly
    - Reset your database (bad, bad choice)
- Get cought scouting environments
- Miner traceability is sub-optimal

Find the right balance between red & blue

Hide behind `cms.nikhef.de` (as opposed to `nikhef.nl`)

- Let's see how well known Nikhef is as an institute :-)

The Blue-Teams

Goal of the blue team activities

Coordinate security response activities over:

- 4 Organisations (EGI, OSG, eduGAIN, CMS VO).
- 58 Resource Centers (with local security teams).
- 141 gateways to the infra (controlled by the local security teams, proxy gateways controlled by VO).
- 2 proxy gateways that potentially circumvent local access control mechanism.
- Stop 2 Credentials from accessing the infras.

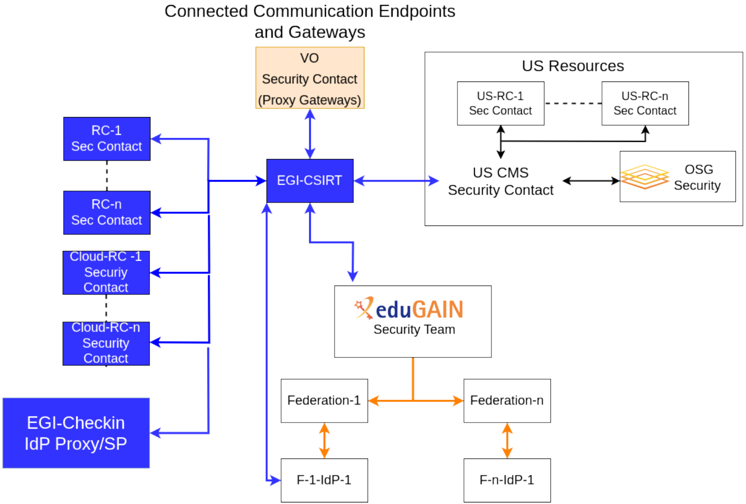
The task

The Task

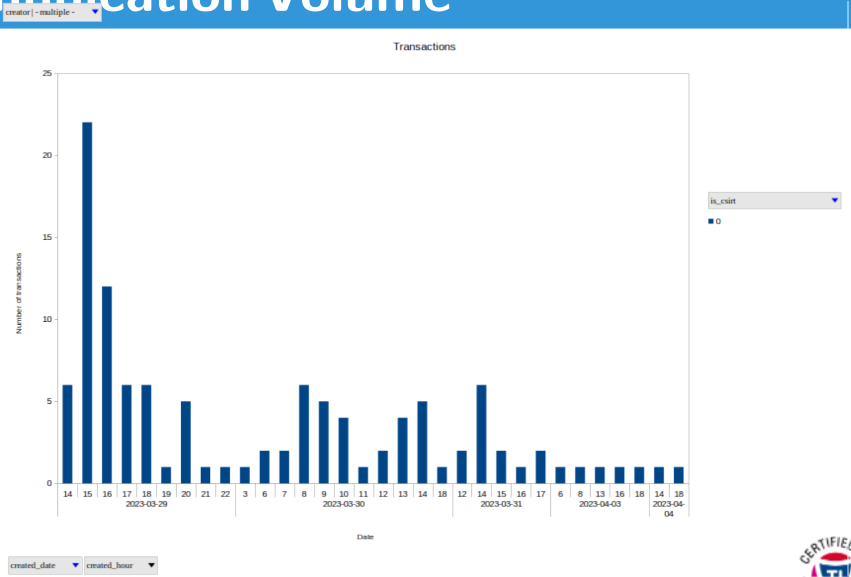
- Identify affected Resource Centers, Organisations.
- Stop malicious processes on the affected Infra.
- Stop/Suspend accounts used to initiate the malicious processes.
- Collect sufficient forensics information to resolve the incident.

The Communication Endpoints

Communication Network



Communication Volume



Blue Team Resources

The coordination, inclusive the assessment of feedback for further intel sharing was done by 2 Persons. **Heavily Understaffed**

The Results

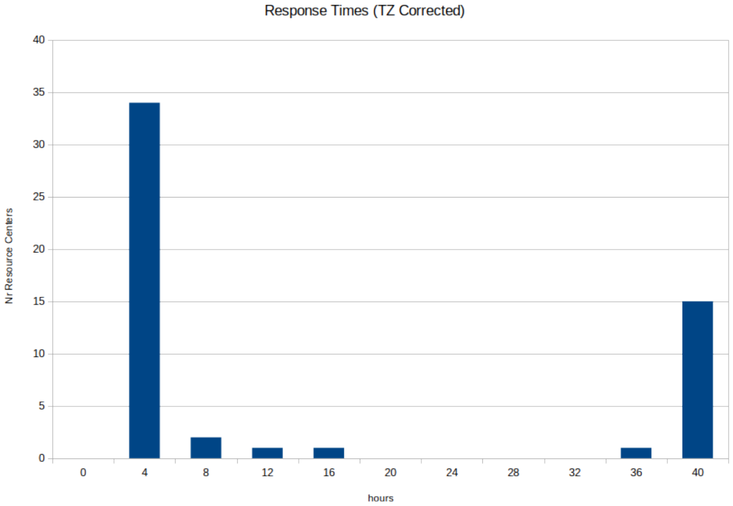
Results, what was evaluated

Goal: Assessment of the Incident Response capabilities at the Resource Centers

- Communications: Response times
- Containment: Stop malicious processes, suspend reported credentials
- Forensics: On/Offline forensics of the malicious processes running at the resource center. Capture The Flag, participation optional.

Resource Centers Response Times

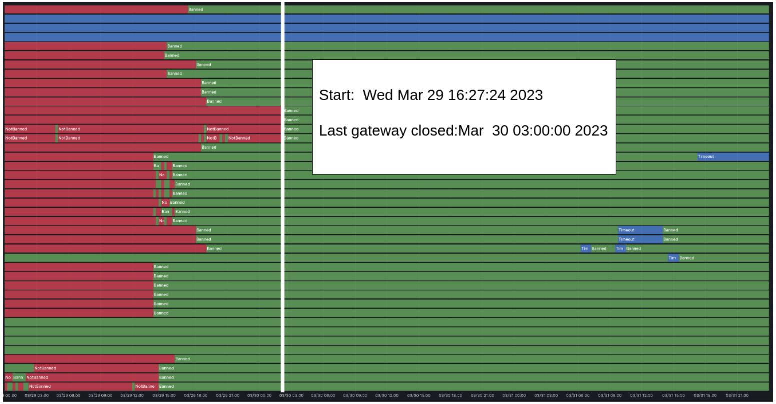
Communications, Response Times



Resource Centers Incident Response capabilities

Containment, Suspend malicious credentials

Gateway system 1, local resource security teams, certificate revoked: Wednesday, March 29, 2023 13:17

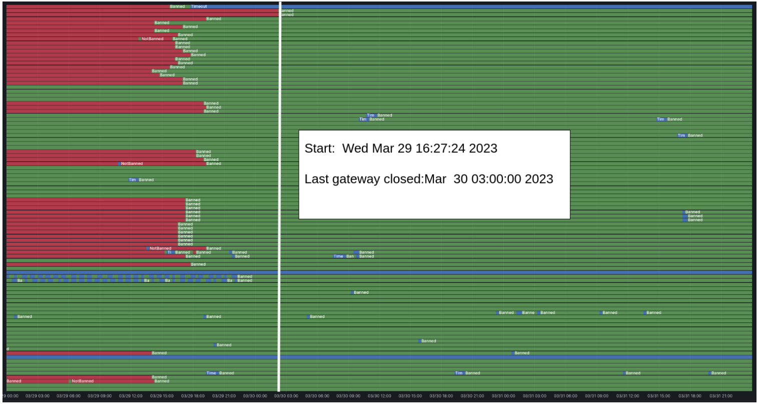


Start: Wed Mar 29 16:27:24 2023

Last gateway closed:Mar 30 03:00:00 2023

Containment, Suspend malicious credentials

Gateway system 2, local resource security teams, certificate revoked: Wednesday, March 29, 2023 13:17

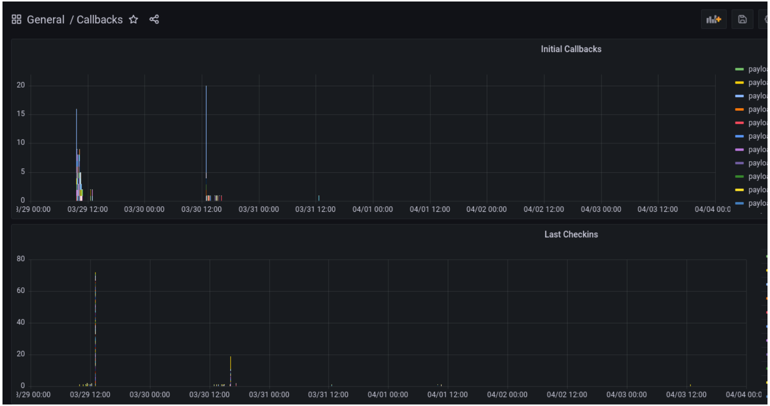


Start: Wed Mar 29 16:27:24 2023

Last gateway closed:Mar 30 03:00:00 2023

Containment, Stop malicious processes

Kill the botnet, local resource security teams. (Lessons learned from earlier campaign, implement self destruct)



Containment on Cloud Infra

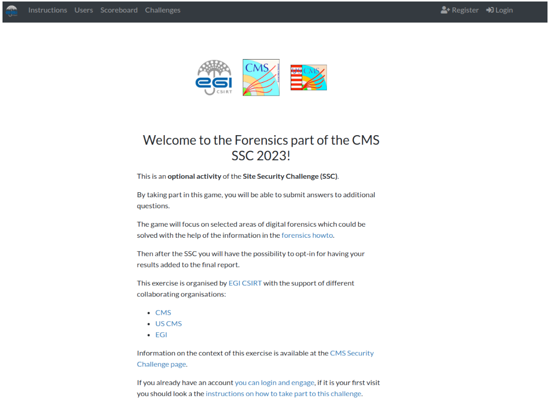
Stop malicious virtual machines. Kill the attack infrastructure, C2, Content delivery network, ...

- Running VMs not affected, needed to be suspended by the local teams..
- Significant delay between invalidating IdP identity at Federated IdP and the lifetime of the token received from infrastructure proxy IdP(already addressed)
- Token Lifetime was an issue.
- (How can we mimick Certificate-Revocation-List functionality from the x509 world in the Federated Identity world?)

Resource Centers forensic capabilities

Capture The Flag, registration

Registration to the CTF is optional, 18 Teams, 39 Users participated.
More on the CTF in the second part of the presentation by Daniel.



Welcome to the Forensics part of the CMS SSC 2023!

This is an **optional activity** of the **Site Security Challenge (SSC)**.

By taking part in this game, you will be able to submit answers to additional questions.

The game will focus on selected areas of digital forensics which could be solved with the help of the information in the forensics howto.

Then after the SSC you will have the possibility to opt-in for having your results added to the final report.

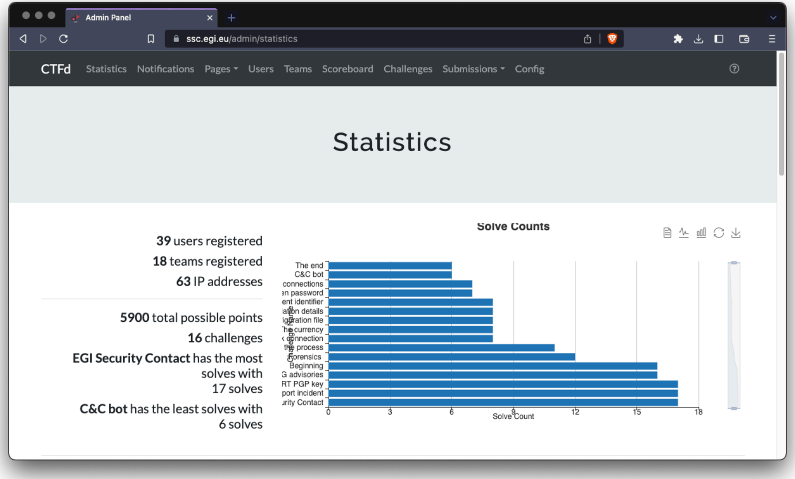
This exercise is organised by EGI CSIRT with the support of different collaborating organisations:

- CMS
- US CMS
- EGI

Information on the context of this exercise is available at the CMS Security Challenge page.

If you already have an account you can login and engage, if it is your first visit you should look a the instructions on how to take part to this challenge.

Capture The Flag, Result statistics



Statistics

39 users registered

18 teams registered

63 IP addresses

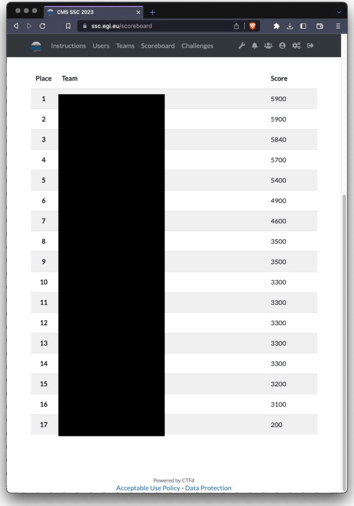
5900 total possible points

16 challenges

EGI Security Contact has the most solves with 17 solves

C&C bot has the least solves with 6 solves

Capture The Flag, Result Scores



Place	Team	Score
1	[redacted]	5900
2	[redacted]	5900
3	[redacted]	5840
4	[redacted]	5700
5	[redacted]	5400
6	[redacted]	4900
7	[redacted]	4600
8	[redacted]	3500
9	[redacted]	3500
10	[redacted]	3300
11	[redacted]	3300
12	[redacted]	3300
13	[redacted]	3300
14	[redacted]	3300
15	[redacted]	3200
16	[redacted]	3100
17	[redacted]	200

Powered by CTFd
Acceptable Use Policy - Data Protection

Sufficient forensics capabilities available in the infrastructure to do a root cause analysis.

Inter organization coordination

Inter organization coordination

EGI/OSG

- Clear handover not implemented, daily meetings to synchronize the activities in the organisations needed.
- Collaboration with IdP worked flawless, identity from federated AAI IdP was only used at one proxy, incident coordination in eduGAIN was challenged only very basic. (eduGAIN CSIRT was informed by IdP!)
- Very good collaboration with CMS Security.

Conclusions

Conclusion, Discussion

- The complexity of the coordination of incident response activities is huge.
- Sufficient manpower needed for the coordination task.
- Plan for inter-organisational meetings at least once a day.
- Work towards automation, monitor the activities as far as possible.
- Various flaws in the response procedures detected and addressed (check efficiency of the current workflow, implement control loops)

CTF

Extension of the exercise

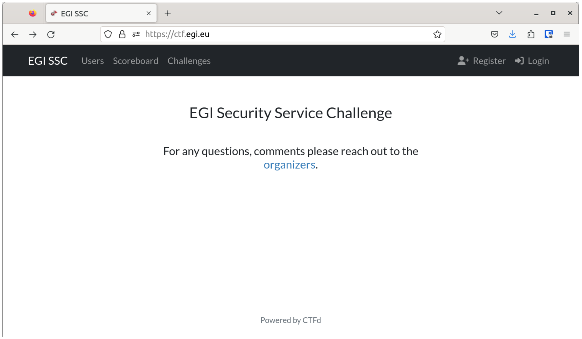
- Primary goal was to check essential security capabilities
  - Collaboration, communication, capability to act, etc.
  - No specific analytical capability is expected/required
- More technical part introduced as optional extension
  - Engage more the administrators and make it more attractive
  - Show the capabilities of common tools/commands
  - Improve the skills
  - Better position the security team

CTF Design

- Site administrators provided with a “malicious” jobs
- The payload was crafted to allow some essential analysis
- A set of exercises derived how for data gathering and analysis
  - Simplified, focusing only on technical bits (*Quick & Dirty Forensics*)
  - The exercise compiled into a CTF scenario, guiding the admins through a few areas

CTF today

- `https://ctf.egi.eu/`
- Registration code: `ISGC`



EGI Security Service Challenge

For any questions, comments please reach out to the organizers.

Powered by CTFd