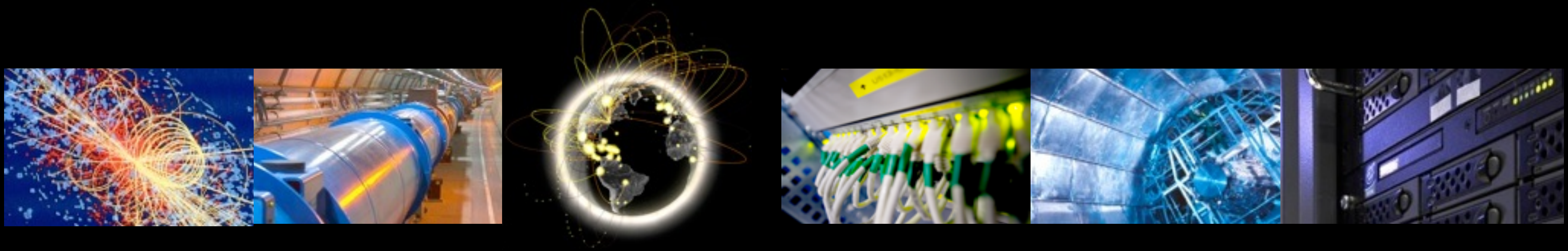
CERN's role in WLCG Security Operations

18-04-2024 / ALICE Workshop



https://indico.cern.ch/event/1355985

Responsibilities

CERN Computer Security

– Local security operations

- Security reviews, incident response, threat intelligence, …

WLCG Security

– Policies (endorsed by the Management Board)

– Recommendations

– Coordination and Incident Response

– Oversee major changes (eg: tokens, federated identities…)

Jose Carlos Luna

jose.carlos.luna@cern.ch

WLCG Security Officer

EGI IRTF

– Incident Response

– Vulnerability evaluation and tracking

– Policies and procedures

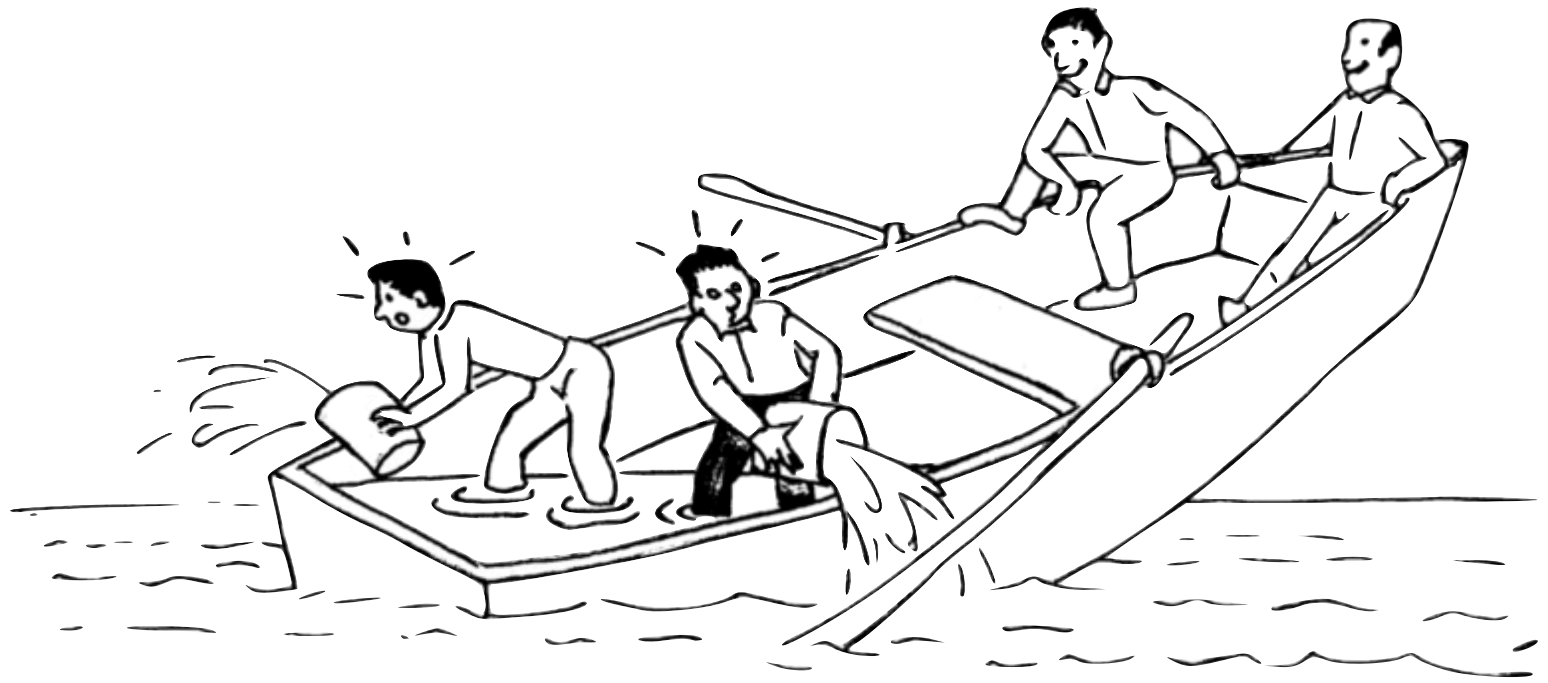
Pau Cutrina

pau.cutrina@cern.ch

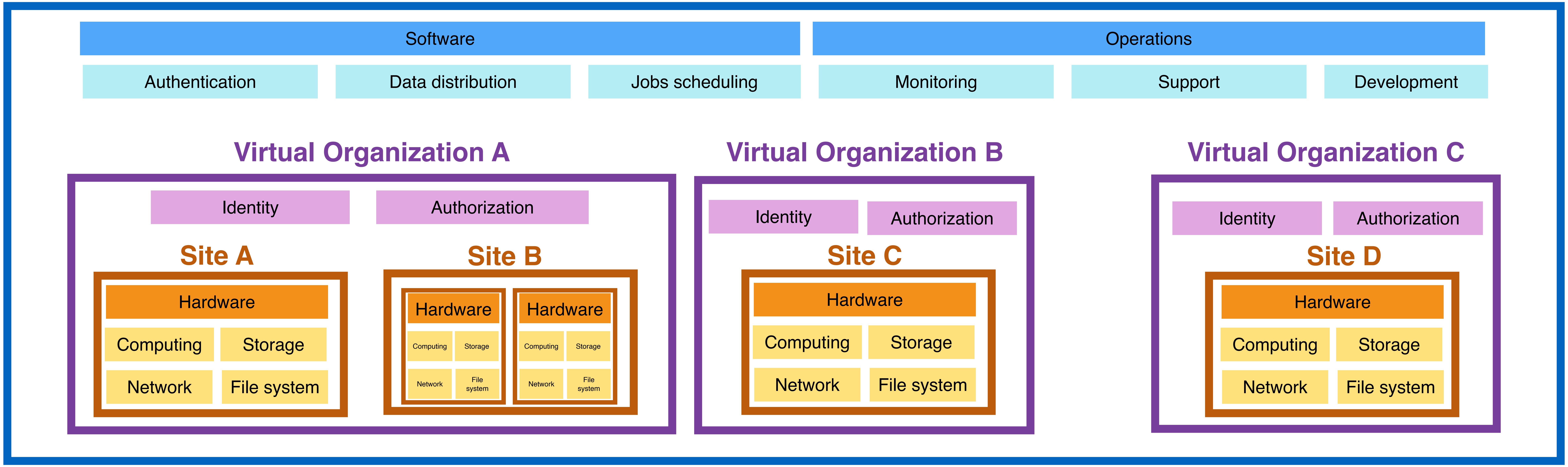
EGI IRTF Lead

Security model - WLCG

- Layered based model
  - Grid infrastructure
    - Resources are **shared**, so connected
    - Security teams at different levels



WLCG (EGI+OSG)



Software | Operations

Authentication | Data distribution | Jobs scheduling | Monitoring | Support | Development

Virtual Organization A

Identity | Authorization

Site A

Hardware: Computing, Storage, Network, File system

Site B

Hardware: Computing, Storage, Network, File system

Hardware: Computing, Storage, Network, File system

Virtual Organization B

Identity | Authorization

Site C

Hardware: Computing, Storage, Network, File system

Virtual Organization C

Identity | Authorization

Site D

Hardware: Computing, Storage, Network, File system

WLCG	World LHC Computing Grid
EGI	European Grid Infrastructure
OSG	Open Science Grid

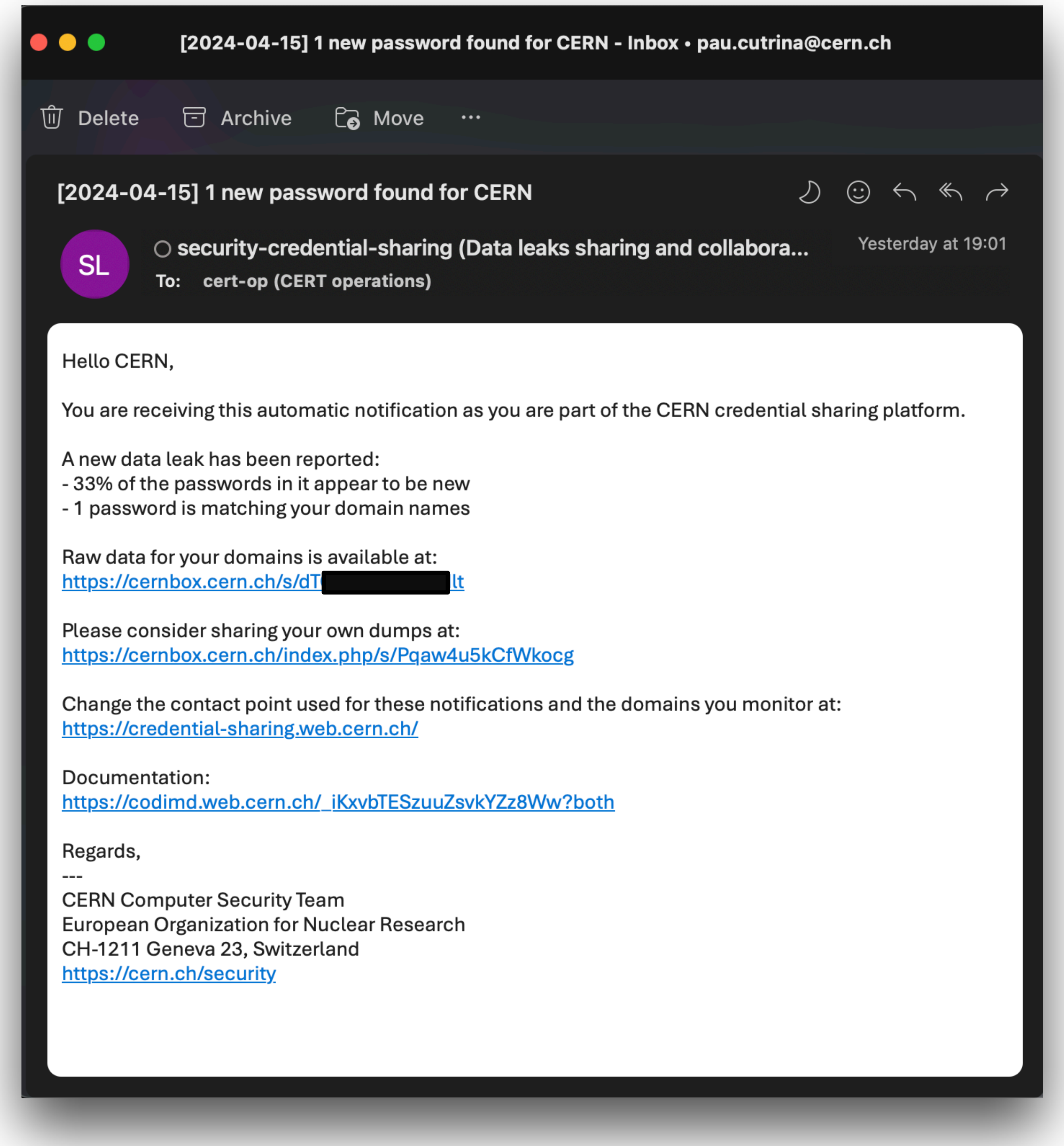
https://twiki.cern.ch/twiki/bin/view/LCG/WLCGOperationsWeb; https://wlcg-public.web.cern.ch/

Activities

- Incidents Response (IR)
  - IR coordination
  - EGI Policies and Procedures
    - I.e. criteria for sites suspension
  - Communication channels
    - Email, RT, Mattermost, Keybase, …
  - Constant updates (advisories)
- Communications Challenge
  - Security contacts up-to-date
  - Procedures associated
- Vulnerabilities
- SSC

Initiatives

- Credential Sharing: Give us your **domain** and **email** and we will notify you.
- Advisories
- MISP
- WLCG SOC WG



[2024-04-15] 1 new password found for CERN - Inbox • pau.cutrina@cern.ch

[2024-04-15] 1 new password found for CERN

SL ○ security-credential-sharing (Data leaks sharing and collabora... Yesterday at 19:01
To: cert-op (CERT operations)

Hello CERN,

You are receiving this automatic notification as you are part of the CERN credential sharing platform.

A new data leak has been reported:
- 33% of the passwords in it appear to be new
- 1 password is matching your domain names

Raw data for your domains is available at:
https://cernbox.cern.ch/s/dT[redacted]lt

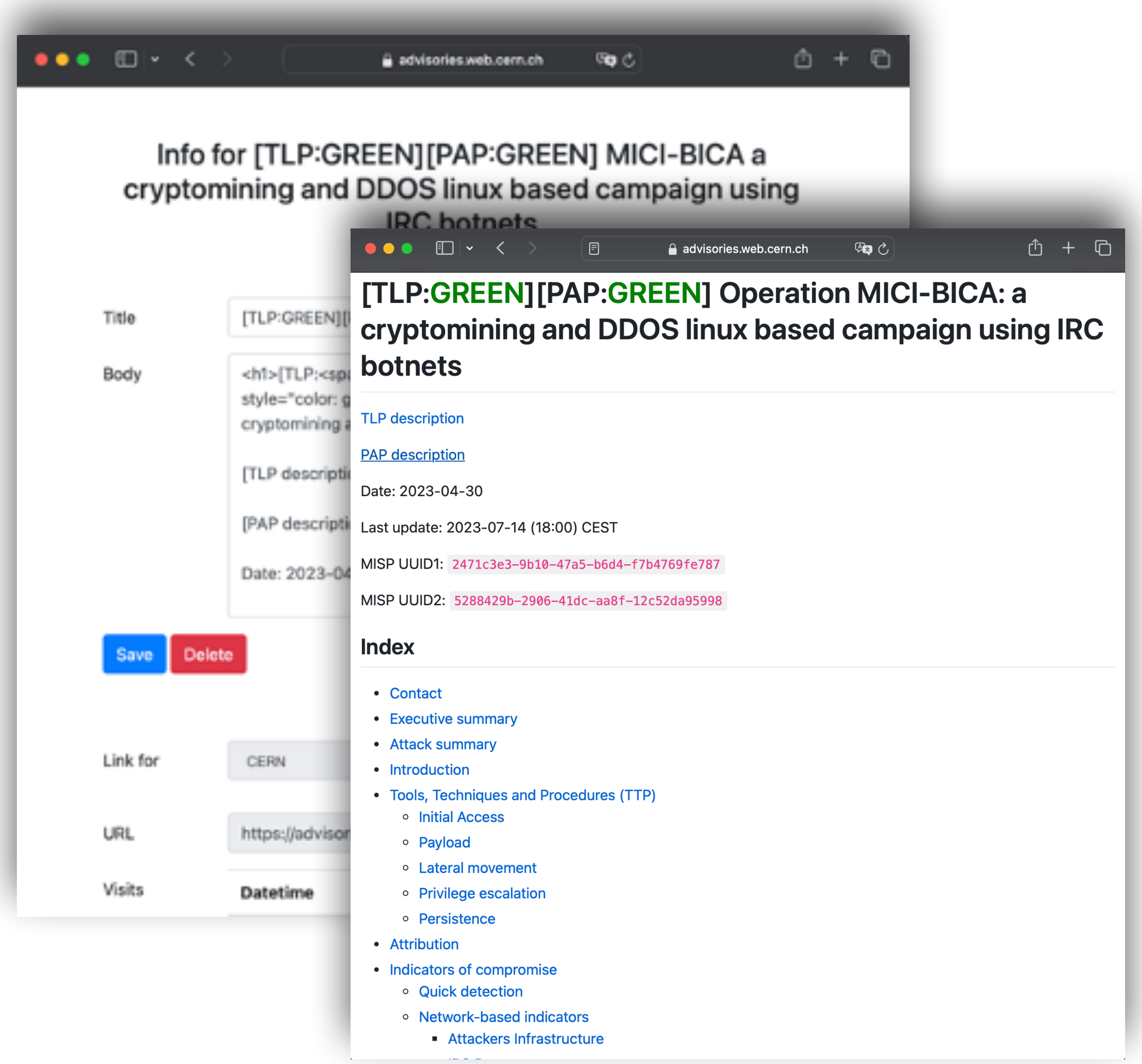
Please consider sharing your own dumps at:
https://cernbox.cern.ch/index.php/s/Pqaw4u5kCfWkocg

Change the contact point used for these notifications and the domains you monitor at:
https://credential-sharing.web.cern.ch/

Documentation:
https://codimd.web.cern.ch/_iKxvbTESzuuZsvkYZz8Ww?both

Regards,

CERN Computer Security Team
European Organization for Nuclear Research
CH-1211 Geneva 23, Switzerland
https://cern.ch/security



advisories.web.cern.ch

Info for [TLP:GREEN][PAP:GREEN] MICI-BICA a cryptomining and DDOS linux based campaign using IRC botnets

Title [TLP:GREEN][

Body <h1>[TLP:<spa
style="color: g
cryptomining a

[TLP descripti

[PAP descripti

Date: 2023-04

Link for CERN

URL https://advisor

Visits Datetime

advisories.web.cern.ch

[TLP:GREEN][PAP:GREEN] Operation MICI-BICA: a cryptomining and DDOS linux based campaign using IRC botnets

TLP description

PAP description

Date: 2023-04-30

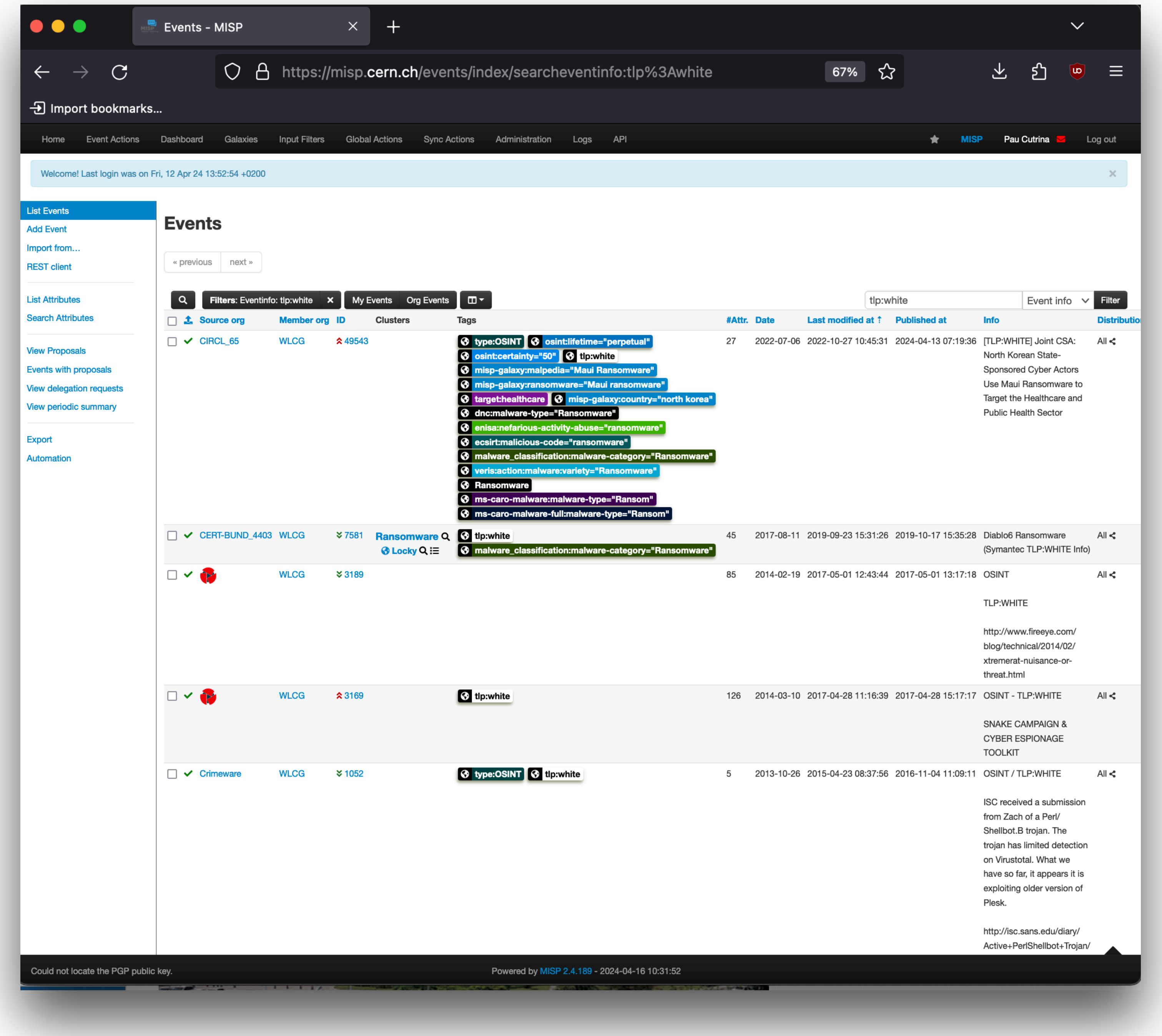
Last update: 2023-07-14 (18:00) CEST

MISP UUID1: `2471c3e3-9b10-47a5-b6d4-f7b4769fe787`

MISP UUID2: `5288429b-2906-41dc-aa8f-12c52da95998`

Index

- Contact
- Executive summary
- Attack summary
- Introduction
- Tools, Techniques and Procedures (TTP)
  - Initial Access
  - Payload
  - Lateral movement
  - Privilege escalation
  - Persistence
- Attribution
- Indicators of compromise
  - Quick detection
  - Network-based indicators
    - Attackers Infrastructure



https://misp.cern.ch/events/index/searcheventinfo:tlp%3Awhite

Welcome! Last login was on Fri, 12 Apr 24 13:52:54 +0200

Events

Filters: Eventinfo: tlp:white

tlp:white Event info

Source org	Member org	ID	Clusters	Tags	#Attr.	Date	Last modified at	Published at	Info	Distribution
CIRCL_65	WLCG	49543		type:OSINT osint:lifetime="perpetual" osint:certainty="50" tlp:white misp-galaxy:malpedia="Maui Ransomware" misp-galaxy:ransomware="Maui ransomware" target:healthcare misp-galaxy:country="north korea" dnc:malware-type="Ransomware" enisa:nefarious-activity-abuse="ransomware" ecsirt:malicious-code="ransomware" malware_classification:malware-category="Ransomware" veris:action:malware:variety="Ransomware" Ransomware ms-caro-malware:malware-type="Ransom" ms-caro-malware-full:malware-type="Ransom"	27	2022-07-06	2022-10-27 10:45:31	2024-04-13 07:19:36	[TLP:WHITE] Joint CSA: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector	All
CERT-BUND_4403	WLCG	7581	Ransomware Locky	tlp:white malware_classification:malware-category="Ransomware"	45	2017-08-11	2019-09-23 15:31:26	2019-10-17 15:35:28	Diablo6 Ransomware (Symantec TLP:WHITE Info)	All
	WLCG	3189			85	2014-02-19	2017-05-01 12:43:44	2017-05-01 13:17:18	OSINT TLP:WHITE http://www.fireeye.com/blog/technical/2014/02/xtremerat-nuisance-or-threat.html	All
	WLCG	3169		tlp:white	126	2014-03-10	2017-04-28 11:16:39	2017-04-28 15:17:17	OSINT - TLP:WHITE SNAKE CAMPAIGN & CYBER ESPIONAGE TOOLKIT	All
Crimeware	WLCG	1052		type:OSINT tlp:white	5	2013-10-26	2015-04-23 08:37:56	2016-11-04 11:09:11	OSINT / TLP:WHITE ISC received a submission from Zach of a Perl/Shellbot.B trojan. The trojan has limited detection on Virustotal. What we have so far, it appears it is exploiting older version of Plesk. http://isc.sans.edu/diary/Active+PerlShellbot+Trojan/	All

Could not locate the PGP public key.

Powered by MISP 2.4.189 - 2024-04-16 10:31:52

https://wlcg-soc-wg.docs.cern.ch/

Upcoming Actions

- Possibilities
  - Technical trainings (forensics, pentest, operations, …)
  - Simulation of incident to review procedures
  - Assessment security status. Security policies to checklist.
  - Communications challenges to the VOs
  - Random audits
  - Workshops
  - Regular meetings
  - Etc.

Questions?

Jose.Carlos.Luna@cern.ch
Pau.Cutrina@cern.ch