# NGSOTI (Next Generation Security Operator Training Infrastructure)

## Introduction to Incident Response

CIRCL
Computer Incident
Response Center
Luxembourg

Co-funded by
the European Union

TEAM CIRCL

*TLP:CLEAR*

info@circl.lu

2025-01-28

# Outline

Welcome

CIRCL background and services

Introduction

Practical aspects

Incident Response Contractors Evaluation

# Welcome and Introduction

## Interactions during the training

- Collaboration during the training.
- Interrupt the training at any point in time if you have important questions.
- Write your questions in the hdoc.
- Use the collaborative notes to share information.
- collaborative notes that can be downloaded and converted in docx or PDF.

# Welcome

## Interactions with the audience

- Round table.
- Purpose make this training useful.
- What are your area of expertise?
- What do you expect from this course?

# CIRCL background and services

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL[1]) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the **private sector**, communes and non-governmental entities in Luxembourg.
- Started operation under Economic Interest Group in September 2010.
- Under NIS regulation (duties defined in the law of 28 may 2019 defined in Mémorial A $N^o$ 372 of the 31 May 2019).

[1] `https://www.circl.lu/`

# CIRCL background and services

## CIRCL Missions 1/2

- Provide a **systematic and pragmatic response** facility to cyber security incidents.
- **Support economical sector** to recover quickly and efficiently from cyber security incidents.
- Minimize cyber security incident-based losses, theft of information and disruption of services.

# CIRCL background and services

## CIRCL Missions 2/2

- **Gather information/intelligence related to incident handling** to better prepare future incidents management and provide optimized protection for systems and data.
- Coordinate communication among national and international incident response teams[2] during security emergencies and to help prevent future incidents.
- Provide a security related **information sharing community** and warning system for national ICT users and international partners.
- Foster knowledge and awareness exchange[3] in cyber security.

[2] FIRST.org, CSIRTs network, TF-CSIRT...

[3] `https://www.circl.lu/pub/`

## CIRCL Services - Incident Coordination

- Incident handling[4] for reported ICT incidents via different medium (e.g. International CSIRT channel, national incident report,...).
- Incident identification and triage.
- Technical investigation including information correlation (e.g. Security vulnerability/incidents matching, similar incident resolution,...).
- Incident coordination might also include vulnerability handling and **coordinated vulnerability disclosure**[5] (e.g. software vulnerability related to an incident).

[4] https://www.circl.lu/opendata/statistics/

[5] https://www.circl.lu/pub/responsible-vulnerability-disclosure/

## CIRCL and Open Source Tooling

- From the early beginning of CIRCL, **developing tools and software** for our use-cases should be available to others[6].
- For all software developed, associated **services**[7] are available.
- **Producing intelligence** from the services available.
- In 2024, CIRCL maintain more than 14 open source projects[8] (250+ official git repositories).

[6] *Public Money, Public Code*

[7] publicly accessible or restricted access services

[8] `https://opensource-metrics.circl.lu/`

# CIRCL background and services

## MISP Project and CIRCL

- CIRCL **leads the development** of the Open Source MISP threat intelligence platform[9] which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing**.
- Private sector such as the financial sector can request access to one or more information sharing communities operated by CIRCL.

[9] `https://www.misp-project.org/`

# CIRCL background and services

## MISP communities management and hosting

- CIRCL provides **different level of MISP hosting** for communities such as CSIRTs, financial sector, mobile operator sector, banking regulator which can include:
  - Dedicated virtual or physical MISP instance hosted in Luxembourg;
  - MISP software stack maintenance;
  - Managing organisation and communities;
  - Bootstrapping information and intelligence from feeds or other communities;

# CIRCL background and services

## What is MISP?

- MISP is a **threat information sharing** platform that is free & open source software.
- A tool that **collects** information from partners, your analysts, your tools, feeds.
- Normalises, **correlates**, **enriches** the data.
- Describe and structure complex TTPs[10], course of action or custom intelligence.
- Allows teams and communities to **collaborate**.
- **Feeds** automated protective tools and analyst tools with the output.

[10] Tactics, techniques, and procedures.

# CIRCL background and services

## MISP Project - ecosystem overview

- An open standard[11], training materials.
- Classification libraries[12] & encyclopedia[13] (from threat-actor databases to MITRE ATT&CK).
- **MISP-specific tools**: Python Wrapper, Enrichment service, misp-guard for air-gapped system, etc.
- **Integration and workflows**: OpenAPI, Workflow blueprints, misp-modules (300+ enrichments), etc.
- Open data & OSINT Feeds.

[11] https://www.misp-standard.org/

[12] https://www.misp-project.org/taxonomies.html

[13] https://www.misp-project.org/galaxy.html

Plethora of content for **different objectives** and **use-cases**

- **MISP Book**[14] User guide for day-to-day usage.
- `MISP/misp-training`[15] Main repository for any documentation, training materials or conference talks.
- `MISP/misp-training-lea` Complete e-learning course for Law enforcement.
- **Training video** Topical, feature-focused or 4h e-learning session.
- **Others** Cheatsheets, Best practices, guidelines, compliance[16], etc...

[14] https://www.circl.lu/doc/misp/

[15] https://github.com/MISP/misp-training

[16] https://misp-project.org/compliance/

# CIRCL background and services

## Cerebrate

- Cerebrate[17] [18] is an open source platform meant to act as a trusted **contact information provider**.
- Main objectives are **community management** and **local tool orchestration**.
- **IAM centric design** including users provisioning.
- Local tool **management** and **inter-connection** (e.g. MISP).

[17] https://www.cerebrate-project.org/

[18] https://cerebrate.misp-project.org

# CIRCL background and services

## Pandora

- Pandora[19] [20] is an analysis framework to discover **whether a file is suspicious and to conveniently show the results**.
- This tool was created out of a partnership with the CERT of a bank in need of a local tool in order **to avoid leaking sensitive information** toward third-parties.
- CIRCL develops the open source project, along with operating a public instance for the community and supporting organisations wanting to operate local instances.

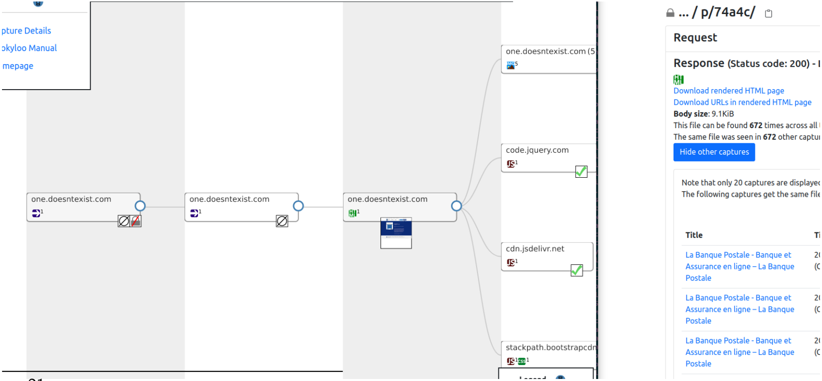
[19] `https://github.com/pandora-analysis`

[20] `https://pandora.circl.lu/`

# CIRCL background and services

## Lookyloo

- Lookyloo[21] [22] is **a safe environment to check, review and analyse urls**.
- This forensic tool can be used to analyse potential phishing website but also legitimate sites for understanding the interactions.



**Response** (Status code: 200) - I

Download rendered HTML page
Download URLs in rendered HTML page
**Body size:** 9.1KiB
This file can be found **672** times across all
The same file was seen in **672** other captu

Note that only 20 captures are displayed
The following captures get the same file

| Title | Ti |
|---|---|
| La Banque Postale - Banque et Assurance en ligne – La Banque Postale | 2( (C |
| La Banque Postale - Banque et Assurance en ligne – La Banque Postale | 2( (C |
| La Banque Postale - Banque et Assurance en ligne – La Banque Postale | 2( (C |

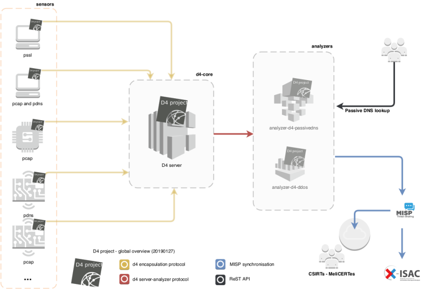
[21] https://github.com/Lookyloo

[22] https://lookyloo.circl.lu/

# CIRCL background and services

## D4 Project

- D4 Project[23] is a **large-scale distributed sensor** network to monitor DDoS and other malicious activities relying on an open and collaborative project.

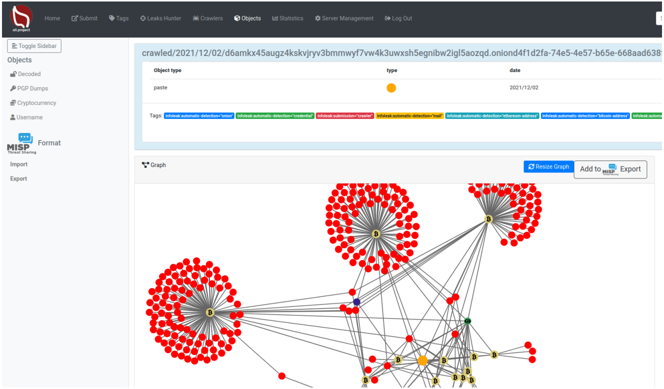


[23] https://www.d4-project.org/

# CIRCL background and services

## AIL Project

- AIL Project[24] is an open source framework to collect, crawl, dig and analyse unstructured data. The framework can be used to find **information leaks**, intelligence, insights and much more. The open source framework includes crawling services (for Tor, I2P) or feeders for specific sources (Telegram, fediverse).



crawled/2021/12/02/d6amkx45augz4kskvjryv3bmmwyf7vw4k3uwxsh5egnibw2igl5aozqd.oniond4f1d2fa-74e5-4e57-b65e-668aad638

| Object type | type | date |
|---|---|---|
| paste | ● | 2021/12/02 |

Tags: infoleak:automatic-detection="onion" infoleak:automatic-detection="credential" infoleak:submission="crawler" infoleak:automatic-detection="mail" infoleak:automatic-detection="ethereum-address" infoleak:automatic-detection="bitcoin-address" infoleak:automa

[24] https://ail-project.org/

# CIRCL background and services

## Typo Squatting

- Typo Squatting[25] is a service to generate, find and assess existing **fake domain used by adversaries**.
- Can be used as a **standalone Python library**[26] for integration with other tools.
- **Publicly accessible** service to run queries and download the results.
- Support many (20+) domain generation algorithms, automatic MISP integration and false-positive detections.

[25] `https://typosquatting-finder.circl.lu/`

[26] `https://github.com/ail-project/ail-typo-squatting`

# CIRCL background and services

## Hashlookup

- Hashlookup[27] [28] is a public API to lookup hash values against **known databases of file hashes**.
  - include NSRL dataset along with more than 100 sources such as CDNjs, major Linux distributions, snap repositories...
- The service is publicly accessible service or can be used as Bloomfilter datasets to off-line lookups.
- Typical usage: During digital forensic investigation to give context and information about the files extracted.

[27] https://hashlookup.io

[28] https://hashlookup.circl.lu/

# CIRCL background and services

## PassiveDNS, PassiveSSL, PassiveSSH

Services providing valuable information during investigation and scenario re-construction.

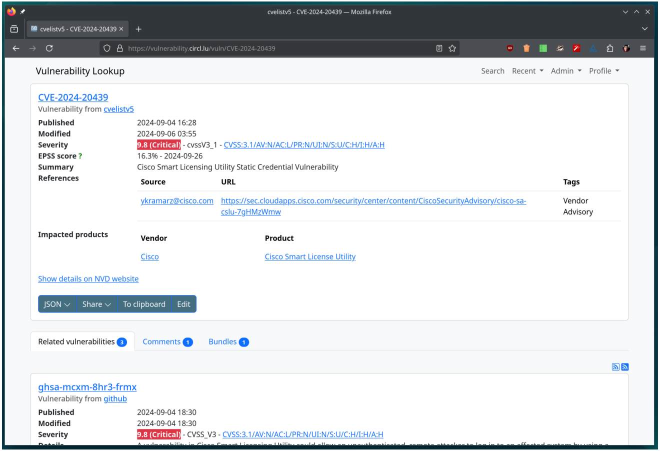
- **PassiveDNS**: Historical DNS records database.
- **PassiveSSL**: Historical database of X.509 certificates (query per IP address, certificates).
- **PassiveSSH**: Historical database of SSH keys & fingerprint (query per IP, fingerprints, banners).

CIRCL Passive SSL

Passive SSH

# CIRCL background and services

## Vulnerability lookup



cvelistv5 - CVE-2024-20439 — Mozilla Firefox
cvelistv5 - CVE-2024-20439
https://vulnerability.circl.lu/vuln/CVE-2024-20439
Vulnerability Lookup
Search
Recent
Admin
Profile

CVE-2024-20439

Vulnerability from cvelistv5

| | |
|---|---|
| **Published** | 2024-09-04 16:28 |
| **Modified** | 2024-09-06 03:55 |
| **Severity** | 9.8 (Critical) - cvssV3_1 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **EPSS score ?** | 16.3% - 2024-09-26 |
| **Summary** | Cisco Smart Licensing Utility Static Credential Vulnerability |

**References**

| Source | URL | Tags |
|---|---|---|
| ykramarz@cisco.com | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw | Vendor Advisory |

**Impacted products**

| Vendor | Product |
|---|---|
| Cisco | Cisco Smart License Utility |

Show details on NVD website

ghsa-mcxm-8hr3-frmx

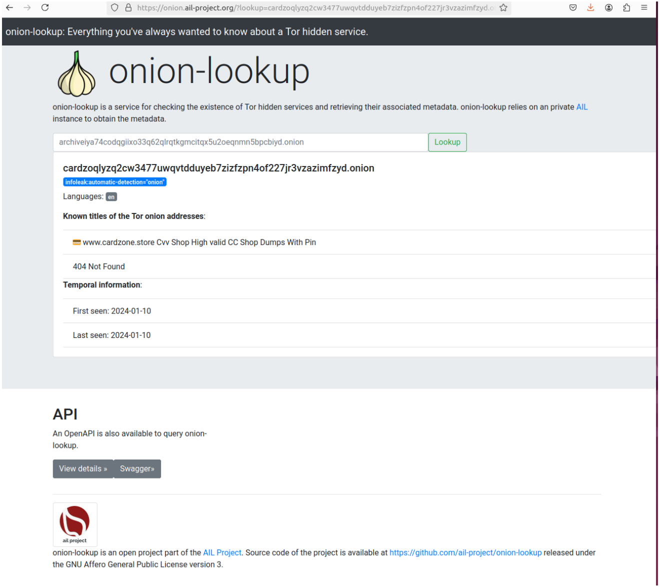
Vulnerability from github

| | |
|---|---|
| **Published** | 2024-09-04 18:30 |
| **Modified** | 2024-09-04 18:30 |
| **Severity** | 9.8 (Critical) - CVSS_V3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **Details** | A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a |

**Figure:** A vulnerability with its details, correlations, comments, and bundles.

# CIRCL background and services

## Onion lookup



https://onion.ail-project.org/?lookup=cardzoqlyzq2cw3477uwqvtdduyeb7zizfzpn4of227jr3vzazimfzyd.o

onion-lookup: Everything you've always wanted to know about a Tor hidden service.

onion-lookup

onion-lookup is a service for checking the existence of Tor hidden services and retrieving their associated metadata. onion-lookup relies on an private AIL instance to obtain the metadata.

archiveiya74codqgiixo33q62qlrqtkgmcitqx5u2oeqnmn5bpcbiyd.onion

cardzoqlyzq2cw3477uwqvtdduyeb7zizfzpn4of227jr3vzazimfzyd.onion

infoleak:automatic-detection="onion"

Languages: en

**Known titles of the Tor onion addresses**:

- 💳 www.cardzone.store Cvv Shop High valid CC Shop Dumps With Pin
- 404 Not Found

**Temporal information**:

- First seen: 2024-01-10
- Last seen: 2024-01-10

### API

An OpenAPI is also available to query onion-lookup.

onion-lookup is an open project part of the AIL Project. Source code of the project is available at https://github.com/ail-project/onion-lookup released under the GNU Affero General Public License version 3.

# Introduction

## Dependencies of incident response training

- On the capabilities of the team
  - In house incident response.
  - Rely on external entities.
  - Critical: Evaluation of the received data / reports.
- On the infrastructure
  - On premises with local IT.
  - On IT integrator.
  - Using cloud infrastructure.
  - Using software as a service (SaaS).
- Bring your Own device policy.
- ...

# Introduction

## High level view

- Definition and importance of incident response.
- Common types of cybersecurity incidents (e.g., malware, phishing, ransomware, data leaks, president fraud).
- Overview of incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned).
- Creation and testing of incident response playbooks

## Incident Response Team (IRT) Roles and Responsibilities

- Incident Response Team (IRT) Roles and Responsibilities → clearly defined borders.
- Roles in an IRT: Incident Manager, Security Analysts, Forensic Experts, Legal, and PR team.
- Importance of cross-functional collaboration.
- Defining the chain of command and communication channels.

# Introduction

## Preparation Phase

- Developing and maintaining an Incident Response Plan (IRP).
- Setting up tools for monitoring and detection (SIEM, IDS/IPS, firewalls).
- Importance of regular updates to documentation and procedures.
- Training exercises (e.g., tabletop exercises, simulations).
- Data backup and recovery procedures.

# Introduction

## Detection and Analysis

- Identifying signs of potential incidents (e.g., unusual activity, system alerts).
- Log analysis and alert correlation techniques.
- Use of automated detection tools.
- Initial triage and prioritization of incidents based on severity.

# Introduction

## Containment Strategies

- Short-term containment: isolating affected systems to prevent further spread.
- Long-term containment: patching vulnerabilities, monitoring for persistence.
- Importance of minimizing business disruption while containing threats.

# Introduction

## Eradication and Recovery

- Removing the root cause of the incident (malware, compromised accounts).
- Verifying system integrity and security.
- Safe restoration of systems and services.
- Ensuring the incident does not recur.

# Introduction

## Post-Incident Activities

- Conducting a thorough post-incident analysis (forensic investigation, root cause analysis).
- Documenting lessons learned and updating the Incident Response Plan.
- Reporting to stakeholders, including executives and regulatory bodies.
- Reviewing and refining security measures.

# Introduction

## Communication and Reporting

- Developing internal and external communication strategies.
- Prepare crisis communication.
- Setup out of band communication channels. The other ones could be intercepted or disrupted.
- Clear communication channels between IT, management, and external partners.
- Regulatory compliance: Reporting incidents to authorities as required (GDPR, NIS,NIS2, DORA etc.).
- Inspect the regulator reports in advance and make sure that you can get all the data.

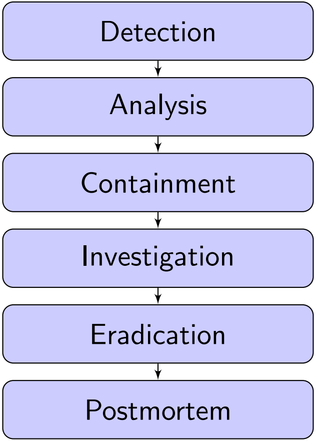
# Introduction

## Continuous Improvement

- Regular review and updates to the IRP based on lessons learned.
- Ongoing training for team members to stay updated on evolving threats.
- Scheduling regular mock drills and simulations based on real data.

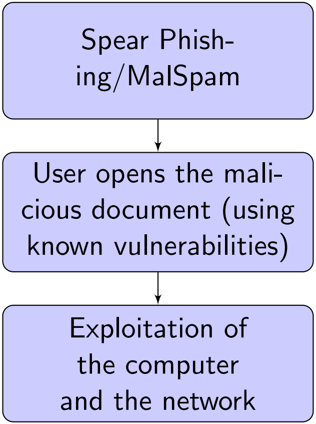
# Introduction

An overview to incident response



# Practical aspects

Nowadays, how is the attacker compromising a PC?


Spear Phishing/MalSpam
User opens the malicious document (using known vulnerabilities)
Exploitation of the computer and the network

# Practical aspects

## Consequences (I)

**Ransomware**

- Malware enumerates and encrypts local and remote files using strong encryption.
- To get the key in order to decrypt, a ransom is asked to be paid.

Questions

- **How to detect? Why detection matters?**
- Should I pay? And what are the consequences?
- How to recover?
- "I have a backup but never tested to restore it!" equals to "I have no backup!"
- How to block similar threats in the future?

# Practical aspects

## Consequences (II)

**Targeted malware**

- Malware to support the activities of an attacker focusing on a specific objective.

Questions

- **How to detect? When is such a targeted attack usually detected?**
- How to recover (remediation) from such an attack (including lateral movement and exploitation)?
- Attackers tend to remain in the infrastructure for weeks or even months before being detected.

# Practical aspects

## Detection (the most common)

- External indicators (e.g. IOCs[29] shared with third-parties).
- Anomalies detected by internal or external people to the organization.
- Performance or stability anomalies detected internally.
- FP[30] incidents usually cross-checked via various sources.
- (careful) Analysis of logs produced by network or security devices/software.

[29] CIRCL MISP

[30] False positives

# Practical aspects

## Detection means gathering, checking and data mining

- Minimal internal team is required to ensure the adequate detecting within your organization.
- Ticketing software (e.g. RTIR) is required to track down incidents/indicators.
- Evaluate case management tools such as flowintel[31]
- The internal team can rely on ”Public Resource Teams”, ”Internal Teams” and ”Commercial Teams” to operate.

[31] `https://github.com/flowintel/flowintel`

# Practical aspects

## A source of detection - An example with McAfee log files

```
Would be blocked by Access Protection rule (rule is currently
not enforced) DDDDDD\U0XXXXX C:\WINNT\Explorer.EXE
C:\DOCUME~1\U0XXXXX\LOCALS~1\Temp\Temporary Directory 1
for Waterpump_update.zip\Analysis Results Upd.exe Common
Standard Protection: Prevent common programs from running
files from the Temp folder Action blocked: Execute
```

- The antivirus didn't detect the malicious files (A/V doesn't detect targeted attacks) but
- Behaviour of the malicious program was detected but not blocked.
- Sending weekly or daily this log to the local IRT[32].

[32] Incident Response Team

# Practical aspects

## Minimal logging recommendations

- Logs are usually a common source of initial detection (e.g. application crashing[33], incoherent access logs).
- Keeping the raw logs is a must (e.g. some security tools modify logs or extraction of raw logs is difficult).
- Having a minimal logging infrastructure keeping raw logs is the basis (before any SIEM integration).
- Don't forget to log "outsourced" services.
- Test your logging infrastructure (e.g. can you find a specific IP address relationship with a MAC address or an username).

[33] Crash dump analysis `https://github.com/neolea/neolea-training-materials/tree/master/e.205-dfir-elf-analysis`

# Practical aspects

## Detection - how to deal with false positives?

If you receive an indicator detecting a potential incident, we have no guarantee to be accurate.

- Collecting the incident reports in a ticketing system helps to reduce the time to process FP events.
- Sometimes the event itself is accurate (e.g. a server is no more responding) but does not lead to a security incidents.
- It's not uncommon to have an event (initially classified as FP) to become a real incident after some times.

# Practical aspects

## Increase detection rate (and reduce analysis time)

Profiling networks and systems is a way to measure expected profile of running systems.

- File integrity check (e.g. default binaries checksum of internal software) is critical to detect unknown binaries and improve analysis time.
- Network profiling (e.g. bytes over time) of internal systems.
- Understand and define normal behavior of networks, systems and applications (e.g. which TCP ports are used by your internal software?).
- Keeping logs[34] is critical especially because incidents might not be discovered within months.

[34] log retention policy

# Practical aspects

## Outsourcing and incident handling

Outsourcing is introducing an additional layer of complexity in case of incident handling. You might consider the following when a part of your IT infrastructure is outsourced:

- The outsourcing providers must provide a feed of raw logs that can be used for analysis on request (in time!) or constantly (preferred).
- Clocks in the outsourcing must be synchronised and using consistent timestamps.
- The local IRT should not only rely on the information provided by the outsourcing provider (Hello Microsoft!)

# Analysis - The Order of Volatility (OOV)

The expected life-time of data :

| Type of Data | Life Span |
|---:|---:|
| Registers or cache | Nanoseconds |
| Main Memory | Ten Nanoseconds |
| Network State | Milliseconds |
| Running Processes | Seconds |
| Disk | Minutes |
| Backup Medias | Years |
| CD-ROMS or printouts | Tens of years |

*Sometimes a small process trace can explain more than 50 gigabytes of a single backup...*

# Practical aspects

## Incident Analysis - Theory

- Broad definition of (computer) forensic analysis : *"Forensic analysis involves the preservation, identification, extraction, documentation and interpretation of computer data"*
- *To reach those goals, the forensic specialists follow clear and well-defined methodologies. Flexibility is highly required when encountering the unusual.*
- *Have a look into Forensic training material to see what it is about.*[35]

[35] `https://www.circl.lu/services/forensic-training-materials/`

- Acquire the evidence without altering or modifying the original source.
- Authenticate that you gathered the evidence in a proper way.
- Analyze the non-original collected data without modifying it.

# Practical aspects

## Incident Analysis - Methodology

- Act always in ways that you can easily explaing to a court.
- Think twice before doing any action on the collected data.
- Take notes of everything not only the action taken but also any discoveries.
- First rule: Stay calm.
- Second rule: Limit risk but keep OOV in mind.
- Third rule: Never work on real data.

# Practical aspects

## Notification during incident handling

During incident analysis, IRT should notify the appropriate individuals in order to perform the analysis.

- (default) Head of information security and related IT staff (including system owners) or external support IRT.
- (if the incident might generate publicity) Public affairs or communication team.
- (if legal impact) Legal department.
- (if appropriate) Law enforcement.

You must be prepared to support ”out-of-band” communication methods if the incident targets the communication infrastructure.

# Practical aspects

## Containment strategy

Containment is critical to avoid collateral damage from an incident. Containment strategies depend on various factors like:

- Requirements of evidence preservation.
- Detection by the attackers of the containment (e.g. change of password).
- Service availability.
- Resources required to implement the containment.
- Be aware of your security tools and policies (e.g. USB port blocker) when an acquisition is required with contained evidences.

# Practical aspects

## Gathering evidence: memory acquisition

- If the system is **not** running, recovering hibernation file/crash dumps/pagefiles from disk.
- If the system is running and accessible, acquire memory with win32dd/win64dd (or RamCapturer or DumpIt or KnTDD).
  - win32dd.exe -l[0—1] memory.dump
- If the system is running but not accessible, hardware techniques using Firewire/DMA access limited to the first 4GB of memory.

- Systems are not always physically accessible.
- Some of the tools can save to a share the memory dump or use an encrypted network tunnel (e.g. over SSH).
- Remote acquisition over the network is not always recommended.
- Remote access and storing the raw dump file locally is an acceptable solution.

```
psexec.exe \\remotesys -e -w c:\ c:\\win32dd.exe c:\\winlocal.
```

# Practical aspects

## Memory acquisition of virtualized systems

- VMware ESX (and related products)
  - .vmem, .vmss and .vmsn files need to be collected for memory analysis.
- VirtualBox
  - via the debugvm command (vboxmanage debugvm dumpguestcore –filename dump.elf)
  - strip elf part to get raw data

```
head -c $(($size+$off)) dump.elf | tail -c +$(($off+1)) > dum
```

# Practical aspects

## Gathering evidence: memory acquisition - risks

- Memory acquisition is performed with administration privileges.
  - If the system is suspicious (and infected), the credentials used might be abused/gathered by the attacker.
- Still better than user-space tools like Process Explorer (e.g. malware rootkits).
- Don't do acquisition when huge processes are running in memory (e.g. AntiVirus full scan, disk indexing).
- Don't forget that some malware detect memory acquisition tools.
- Disk acquisition should be done just after memory acquisition (comparing disk/memory is useful).

# Practical aspects

## Gathering evidence: disk acquisition

- The objective is to acquire an exact copy of the raw suspected disks.
- Forensic analysis will be performed on the acquired disks and never on the original disks.
    - Physical disk acquisition using hardware equipment with write-block like Tableau or similar equipments.
    - Software disk acquisition using a bootable CD (e.g BackTrack/Kali Linux) with dd, dd_rescue, dcfldd or aimage or live (if disk encrypted).

```
dcfldd if=/dev/sda hash=md5,sha256 hashwindow=20G
    md5log=md5.txt sha256log=sha256.txt hashconv=
    after bs=512 conv=noerror,sync split=20G
    splitformat=aa of=sda.dd
```

- Preserve and label original evidence in a safe place.

# Practical aspects

## Pitfalls in disk acquisition

- Using a physical write-blocker is a must to limit the destruction of the evidences.
- A raw disk acquisition is a disk intensive operation and might break the disk.
  - Cooling is critical (e.g. avoid places where there are no fresh air flows).
  - Vibration of the disk should be limited (e.g. put the disk on a stabilized support).
- Prepare a set of forensic disks with an adequate capacity for your future acquisitions.

# Practical aspects

## Analysis of the evidence: memory analysis

- Unstructured analysis (e.g. grep, strings) → easy for analysis checking but out-of-context.
- File carving → quick extraction of contiguous data for files or executables.
- Structured analysis → interpretation of operating system data structure, kernel-user space separation.
  - Volatility[36], Mandiant Redline.

[36] https://volatilityfoundation.org/

# Practical aspects

## Analysis of the evidence: disk analysis

- Unstructured analysis (e.g. grep, strings) → easy for analysis checking but out-of-context.
- File carving → quick extraction of contiguous data for files or executables.
- Structured analysis → interpretation of file-systems (NTFS, ext3/ext4, UFS)
  - Autopsy and The Sleuth Kit[37], Digital Forensics Framework[38].
  - Plaso[39] - a Python-based backend engine for the tool log2timeline.

[37] http://www.sleuthkit.org/

[38] http://www.digital-forensic.org/

[39] https://github.com/log2timeline/plaso

# Practical aspects

## Malware analysis - complexity

- What's the exact definition of a malware? (from remote access tool to custom payload used in targeted attacks)
- Malware is not only payload on Windows machines (but also for instance active malicious JavaScript, repurposed software, bundled software)
- Linux malware analysis training material.[40]
- It's context dependent.

[40] https://github.com/neolea/neolea-training-materials/tree/master/e.205-dfir-elf-analysis

# Practical aspects

## Malware - analysis

During forensic analysis or other activities during the investigation, various suspicious files might be found that could be malware.
Two different approaches can be used:

- Static analysis
  - File characteristics (known operating system file? meta-information? Known in the local baseline?)
  - Result from multiple A/V detection
  - Results from dissasembly
- Dynamic analysis[41]
  - Executing malware in a controlled environment to understand behavior
  - Logging API calls
  - Intercepting and logging network access
- Usually a combination is used to overcome limitations of dynamic and static analysis (e.g. Anti-VM/debug, Turing's Halting problem, target specific requirements)

[41] NGSOTI Kunai sandbox

# Practical aspects

## Indicators usage - a circular approach

- From new indicators (from forensic analysis or malware analysis).
- Indicators like IP addresses, URLs, ASN can be checked in proxy logs, netflow records, firewall logs.
- Indicators like mutexes, file hashes, services, yara rules can be checked on systems directly.
- Those indicators can be used to scope new detections.
- Share indicators early in MISP → automation

# Incident Response Contractors Evaluation

Example: Webshell discovered on Microsoft Exchange Server

## Incident Report

The server was patched and emails are functional.

## Evaluation

- What went wrong?

# Incident Response Contractors Evaluation

Example: Webshell discovered on Microsoft Exchange Server

## Incident Report

The server was patched and emails are functional.

## Evaluation

- What went wrong?
- No evidences were collected.
- No forensic analysis was made.
- Webshell is still usable.

# Incident Response Contractors Evaluation

Example: Webshell discovered on Microsoft Exchange Server

## Incident Report

The files were removed, the server was updated and emails are functional.

## Evaluation

- What went wrong?

# Incident Response Contractors Evaluation

Example: Webshell discovered on Microsoft Exchange Server

## Incident Report

The files were removed, the server was updated and emails are functional.

## Evaluation

- What went wrong?
- No evidences were collected.
- No forensic analysis was made.
- Attackers might have done lateral movement.
- Other backdoors might be available to the attacker.

# Incident Response Contractors Evaluation

Example: Defaced website

### Incident Report

A snapshot of the virtual machine was restored.

### Evaluation

- What went wrong?

# Incident Response Contractors Evaluation

Example: Defaced website

## Incident Report

A snapshot of the virtual machine was restored.

## Evaluation

- What went wrong?
- No evidences were collected.
- No forensic analysis was made.
- Attackers might have still access.

# Incident Response Contractors Evaluation

Example: Compromised VPN gateway

## Incident Report

The VPN gateway was reset, the configuration was restored. Remote access is functional.

## Evaluation

- What went wrong?

# Incident Response Contractors Evaluation

Example: Compromised VPN gateway

## Incident Report

The VPN gateway was reset, the configuration was restored. Remote access is functional.

## Evaluation

- What went wrong?
- No evidences were collected.
- No forensic analysis was made.
- No checks for lateral movements were made.
- Attacker's access to the infrastructure remains functional.

# References and Contact

- https://circl.lu/pub
- https://misp-project.org
- https://ail-project.org
- https://lookyloo.circl.lu
- https://pandora.circl.lu
- https://vulnerability.circl.lu/recent
- https://onion.ail-project.org/
- https://www.circl.lu/services/passive-dns/
- https://www.circl.lu/services/passive-ssl/
- https://typosquatting-finder.circl.lu/
- https://www.d4-project.org/
- https://hashlookup.io
- contact: info@circl.lu, (+352) 247 88444