M&NTIS PLATFORM

SupSec Seminar

Log Analysis Blueteam CTF

CTF organized by
Malizen and AMOSSYS

AMOSSYS
EXPERT IN CYBERSECURITY

Blueteam CTF Context

MonkeyMoney is a NFT startup

Provides a market place to sell NFT (“monkeys”)

MonkeyMoney IT system security was not a priority…

Attack Day : January the 19th

Starting from 15h53, users cannot open a Windows session : AD server not reachable

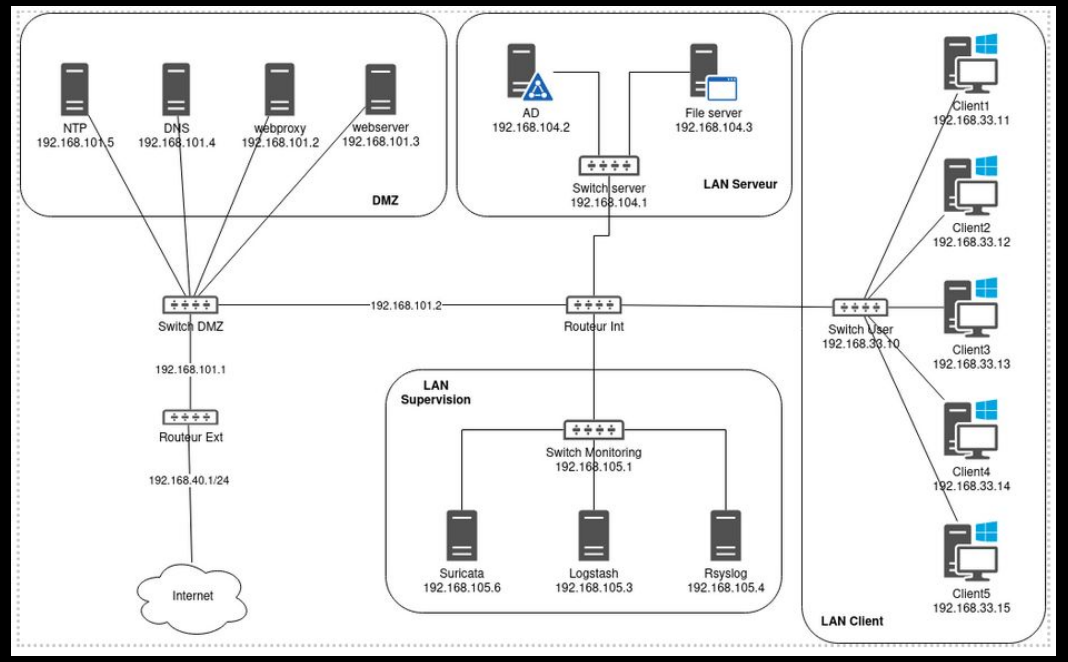
Local connexion by admin to the AD server and… bim !

The day after

Your are an incident response analyst from CERTIFLEX

MonkeyMoney provides you with

- IT system topology
- Explanation of log collection chain
- And logs…



The challenge

For the challenge, logs are provided

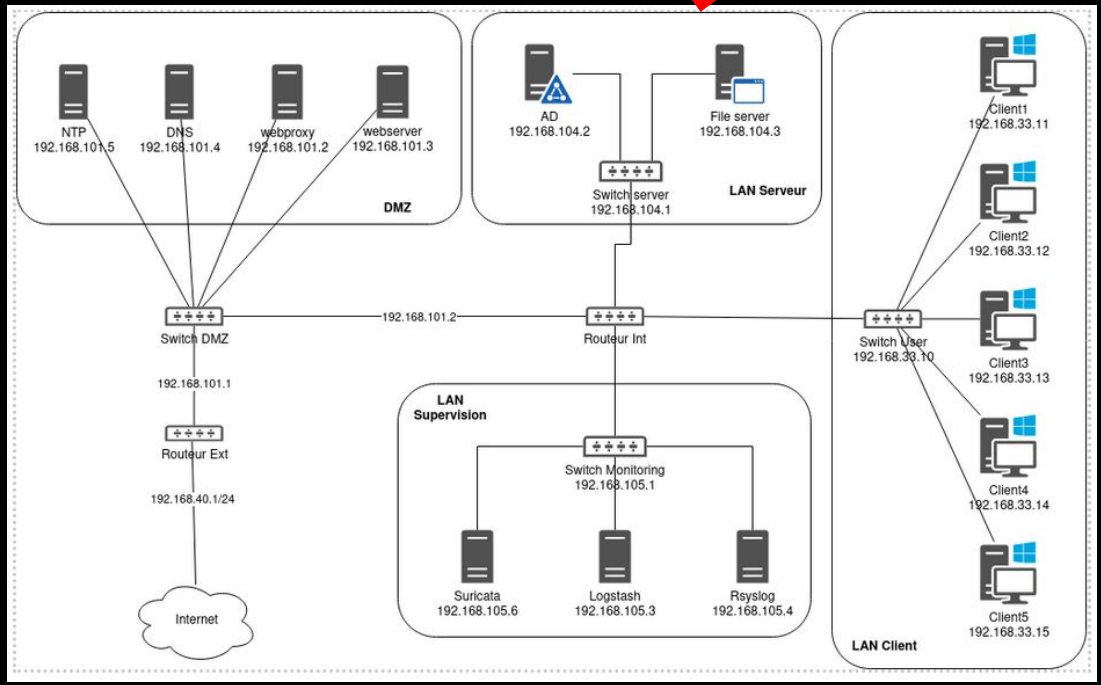
- as raw syslog files
- and either through Kibana (Elastic) : AMOSSYS competition
- or Malizen Investigation Platform : Malizen competition

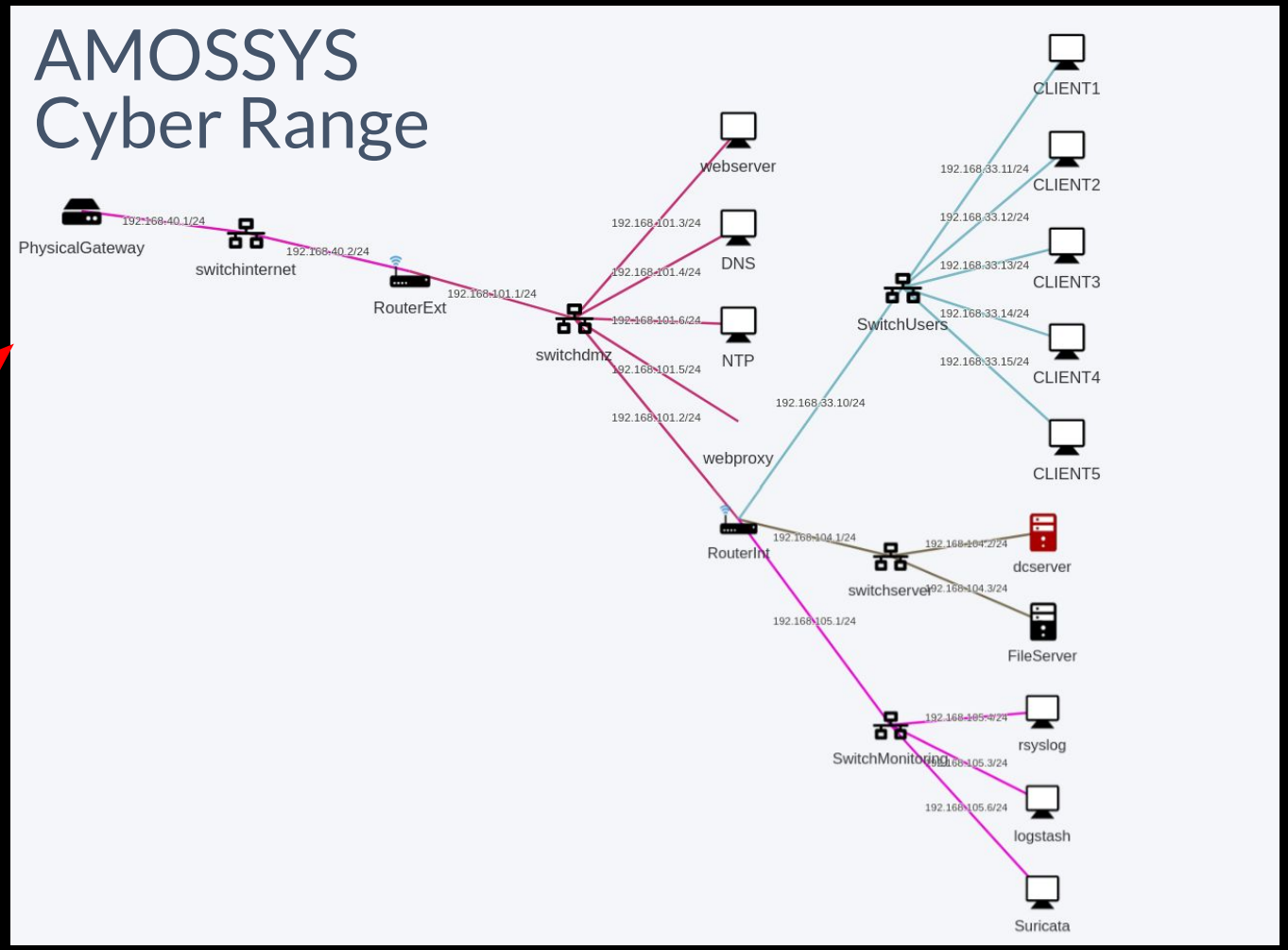
```
$ wc */*
     517  …    CLIENT1/beats.log
     844  …    CLIENT2/beats.log
     544  …    CLIENT3/beats.log
     599  …    CLIENT4/beats.log
    1059 …    CLIENT5/beats.log
    1037 …    dcserver/beats.log
   21077…    DNS/beats.log
      19  …    FileServer/beats.log
   85602 …    Suricata/beats.log
    7719 …    webproxy/beats.log
     210  …    webserver/beats.log
  119243 …    total
```

Dataset generation : Behind the scene

Emulating IT system topology

Infrastructure as Code





Emulating life

On top of the emulated IT system

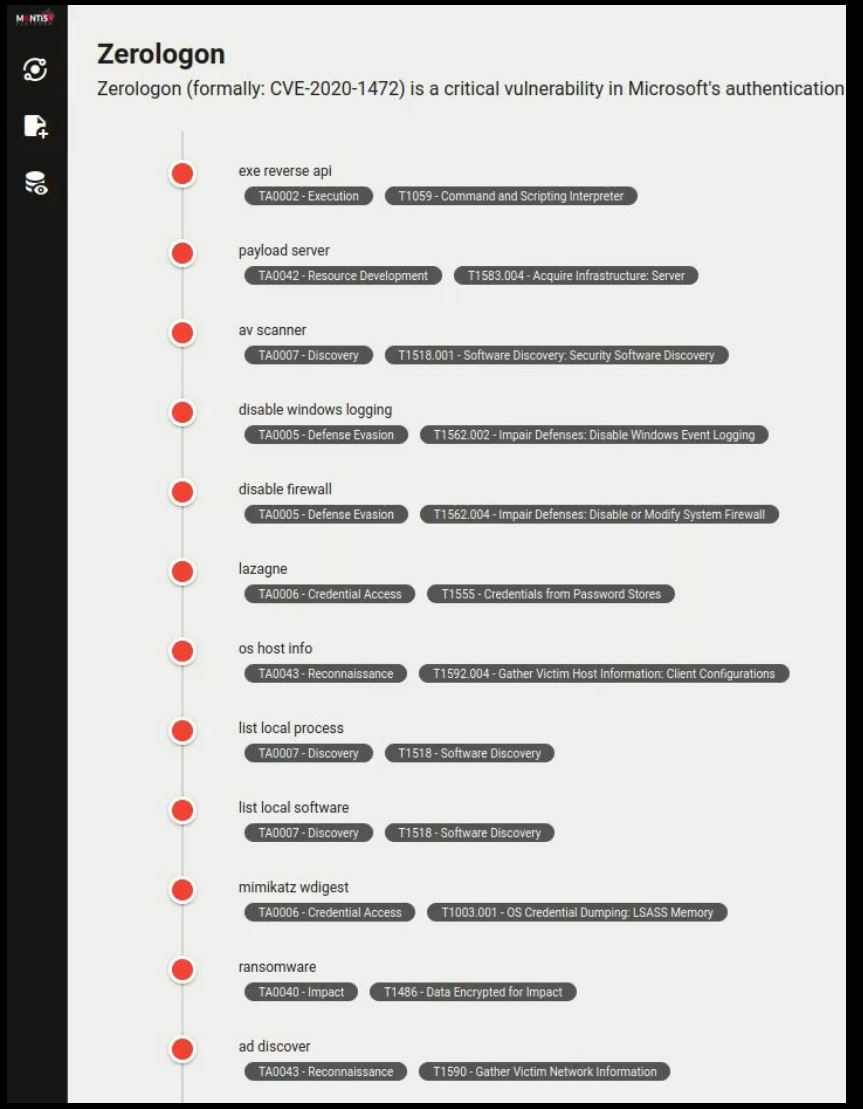
- provisioning of artefacts and data on all endpoints
- provisioning of weaknesses
- realistic legitimate user activity on desktop endpoints
  - agent-less
  - mostly automated :)

Emulating a threat actor

Attack execution : expert system with pre- and post- conditions, and graph traversal

Attack scenario

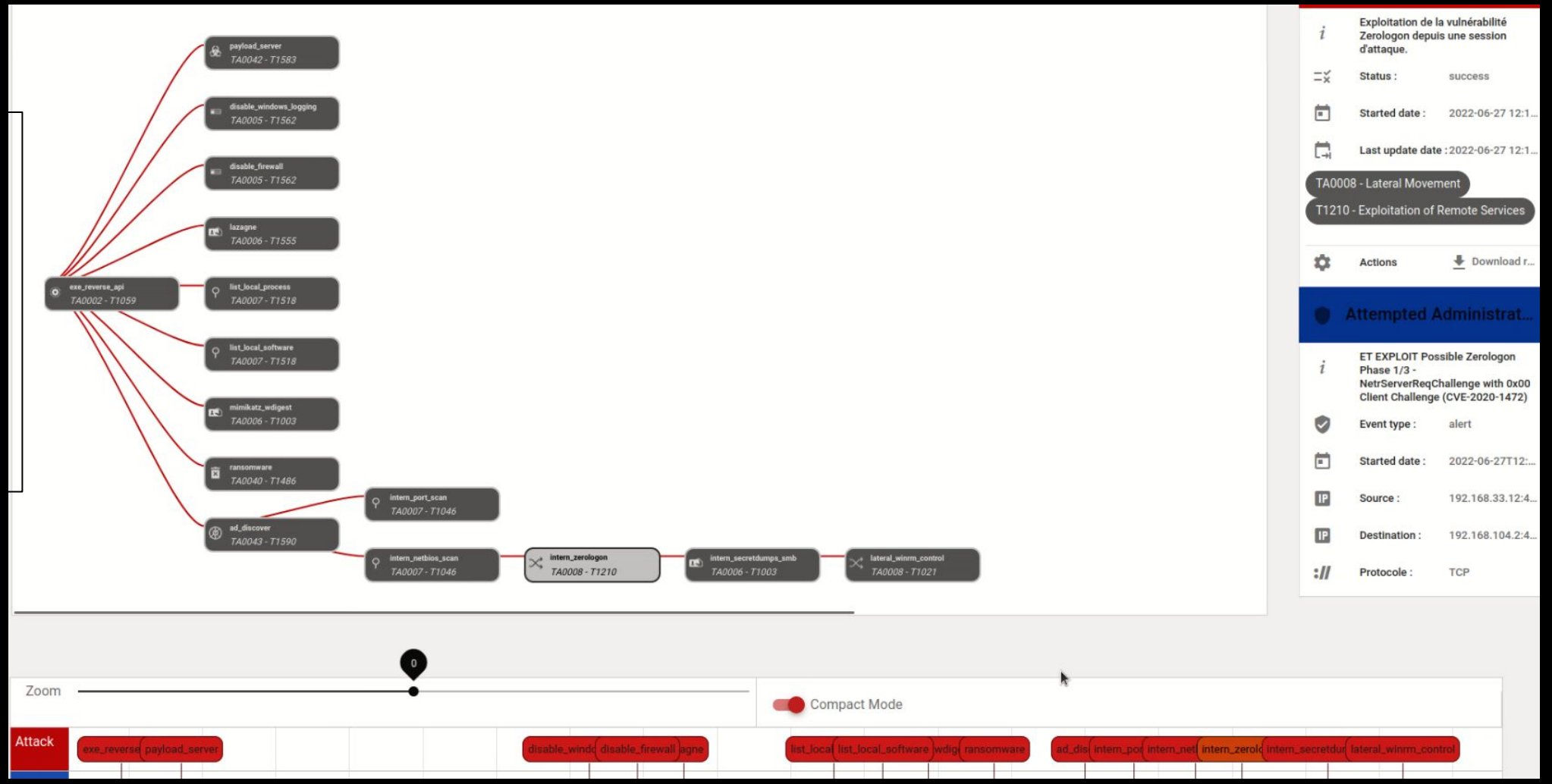
- Log4Shell Tomcat exploitation from internet
  - 1105_000_001
- Connexion to C&C to retrieve orders
- Local discovery
  - 1518_000_001
- Lateral move to User LAN with scheduled task fetching Powershell script from Tomcat web server
- Multiple local discovery steps
  - 1007_000_001 / 1518_000_001
- Multiple network discovery steps
  - 1590_000_001 / 1046_000_002 / 1046_000_003
- Compromise of AD server with Zerologon exploit
  - 1046_000_003
- Ransomware deployed on AD server



Validating the defense : Explainability of attack steps

Attack report containing metadata of attack steps

Attack scenario visualization



M&NTIS Platform

Platform for testing efficiency of security products and SOC/CERT capabilities

Adversary Emulation on Cyber Range

Execution of real attack scenarios

- Attacker infrastructure
- Execution of TTPs on targeted system (MITRE ATT&CK)
- CTI/IoC injection from attack reports

Use cases: live testing and dataset generation

Financial support by DGA MI and AID

contact: frederic.guihery@amossys.fr