SAHER
Cyberthreat supervision platform based on open source tools
SAHER

• Technical Plateform

• Open Source tools

• Developed by the ISAC team

• Real-time cyber attack monitoring
SAHER architecture

MRTI

Collect

Process

Share

DDoS Attack

TTP, IoC

Community

SOC Team

Incident Team

Awareness

Training Cyber drill, Saher magazine
SAHER

- Services’s availability supervision (POP, SMTP, DNS, HTTP...)
- IP REPUTATION
- Detection of massive attacks (DDoS, Mining, IoT, …)
- Behaviour study of attackers
- DDoS Attack
SAHER Tools

- Threat intel
- Firewall
- Web SSO
- VPN

- {php} IPAM
- ZABBIX
- 【RT】I【R】
- re:dash
- Mattermost

- IP Manager
- Monitoring
- Request Tracker
- Dashboard

- MISP
- SURICATA
- TheHive
- elastic
- Nextcloud

- Threat Sharing
- IDS
- Case Manager
- Elastic stack
- Doc Sharing
SAHER Feeds

76 Reports:
- Blacklist IP
- Accessible RDP, SMB, SSH, FTP, Hadoop
- …
SAHER

- Services’s availability supervision (POP, SMTP, DNS, HTTP...)
- IP REPUTATION
- Detection of massive attacks (DDoS, Mining, IoT, ...)
- Botnet Detection
- Active Monitoring
- DDoS Attack
- Behaviour study of attackers
SAHER :: Botnet detection

filebeat

DNS 1

DNS 2

DNS 3

DNS n

Input  Filter  Output

logstash

Elasticsearch

Database of over 37k malicious domains
Screenshot dashboard

Number of botnet per day

List of detected botnets

Number of unique IP addresses

Total Botnet

Details of malicious domains / botnets

Malicious domains
SAHER::Active Monitoring

Organization 1

Organization 2

Organization n

Stack

Stack

Stack

tunCERT
SAHER::Active Monitoring
SAHER :: continuous supervision..

1. Watch & Research
   Security bulletins
   New CVEs published

2. Analysis & identification
   Vulnerability tests
   Severity of the vulnerability

3. Actions
   Notification of concerned organisms
   Reporting / generation of vulnerability notices

4. Monitoring & control
   Check whether the recommendations have been implemented
SAHER :: Use Case proxy logon

- 200 Exchange Servers
- Several vulnerable servers
- Several compromised servers (with webshell)
- https://www.ansi.tn/fr/tuncert/les-vulnerabiltes/microsoft-exchange-server-11
Timeline ProxyLogon/Microsoft Exchange

- **03/03/2021**: Alert Bulletin publication
  - tunCERT

- **07/03/2021**: Updating sensors
  - Identification of IP through shodan

- **08/03/2021**: Task Force

- **13/03/2021**: Exploitation of vulnerabilities (shadowserver)
  - Warning

- **15/03/2021**: Internal Meeting
  - (SOC/CSIRT/ISAC/PENTEST)
  - Action Plan
  - Notification of concerned organisms

- **16/03/2021**: Intervention with organisations

**A continuous work...**
Thank you