QUAND DES RSSI COLLABORENT ...

(SUR UNE PLACE DE MARCHÉS D'IOC COMMUNAUTAIRE)

Emmanuel Mesnard -- Université de Reims Champagne-Ardenne
Damien Berjoan -- ESUP Portail
Fabrice Prigent -- Université Toulouse Capitole
Yves Agostini -- Université de Lorraine

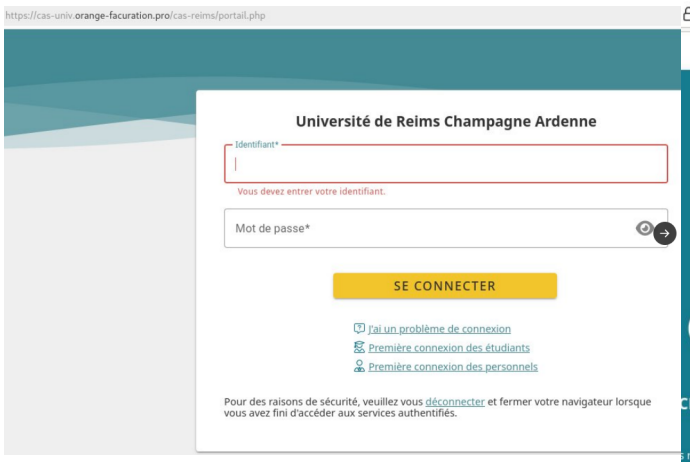
PHISHING

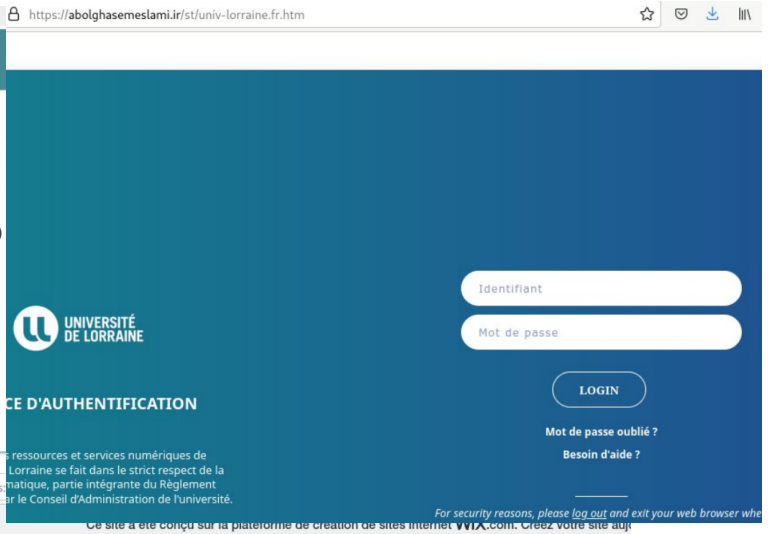
RANSOMWARE

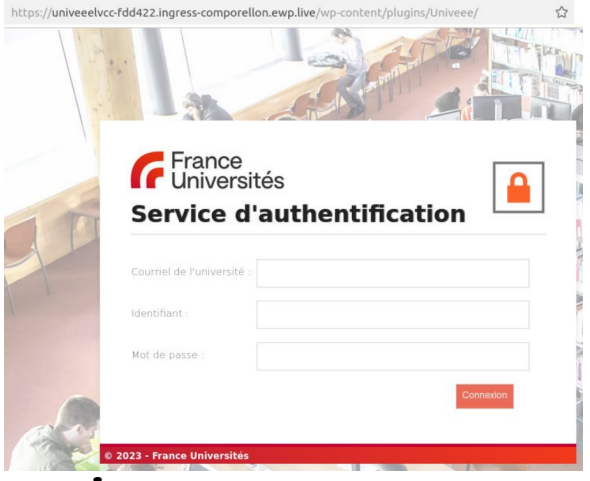
INFOSTEALER

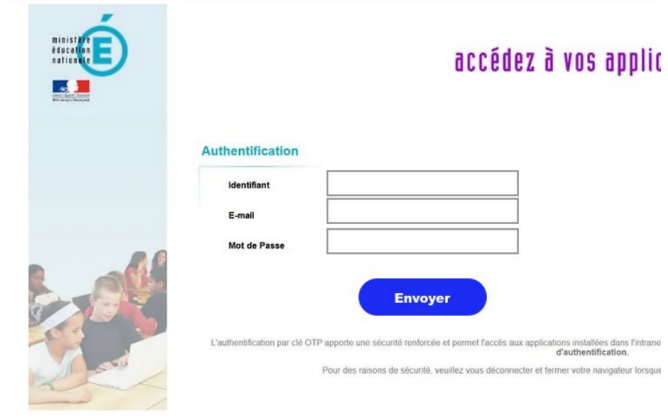
BUSINESS DES MALWARES

PHISHING





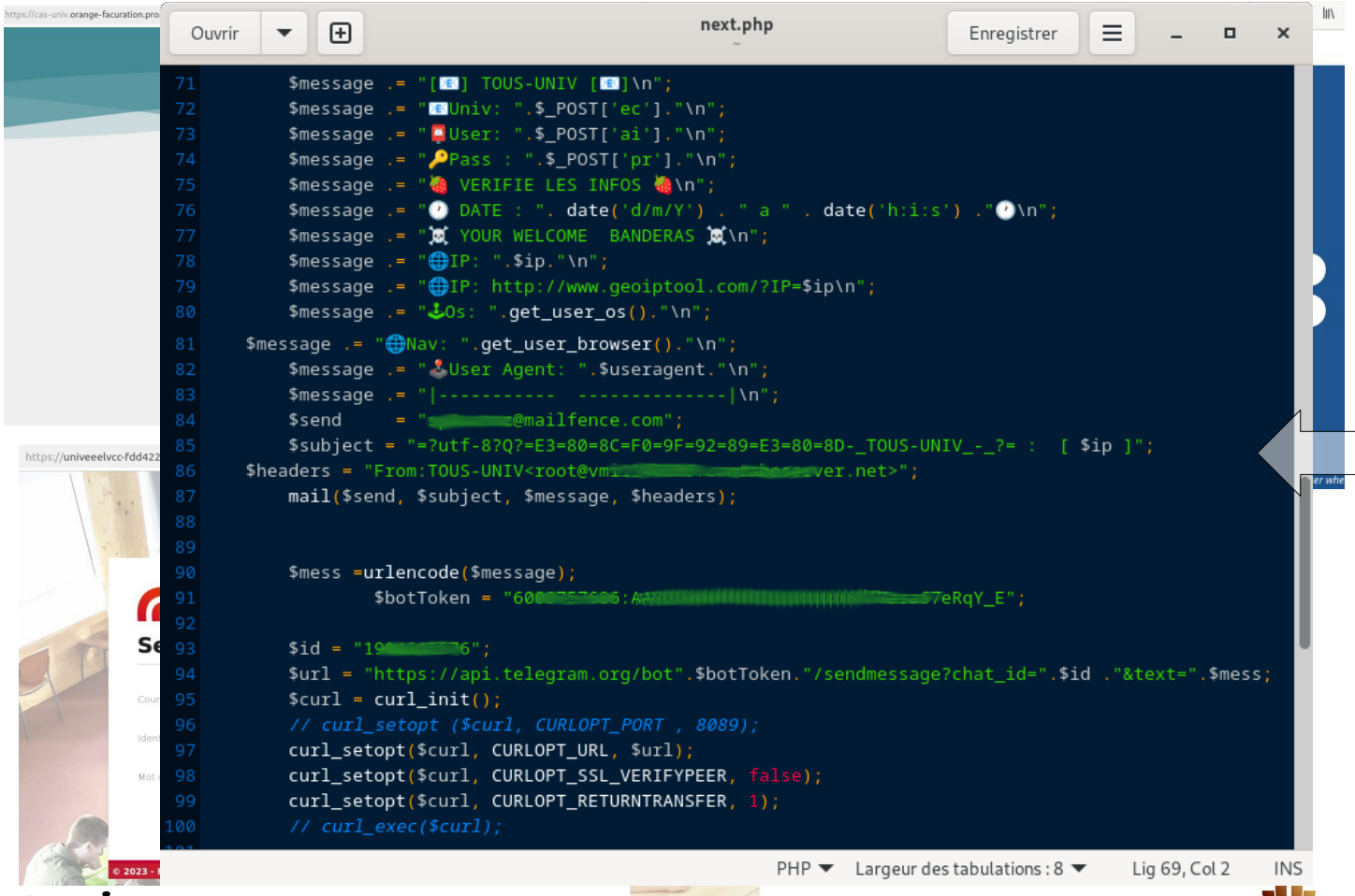




Escroquerie historique

Nos utilisateurs doivent apprendre à lire une URL … systématiquement !

PHISHING

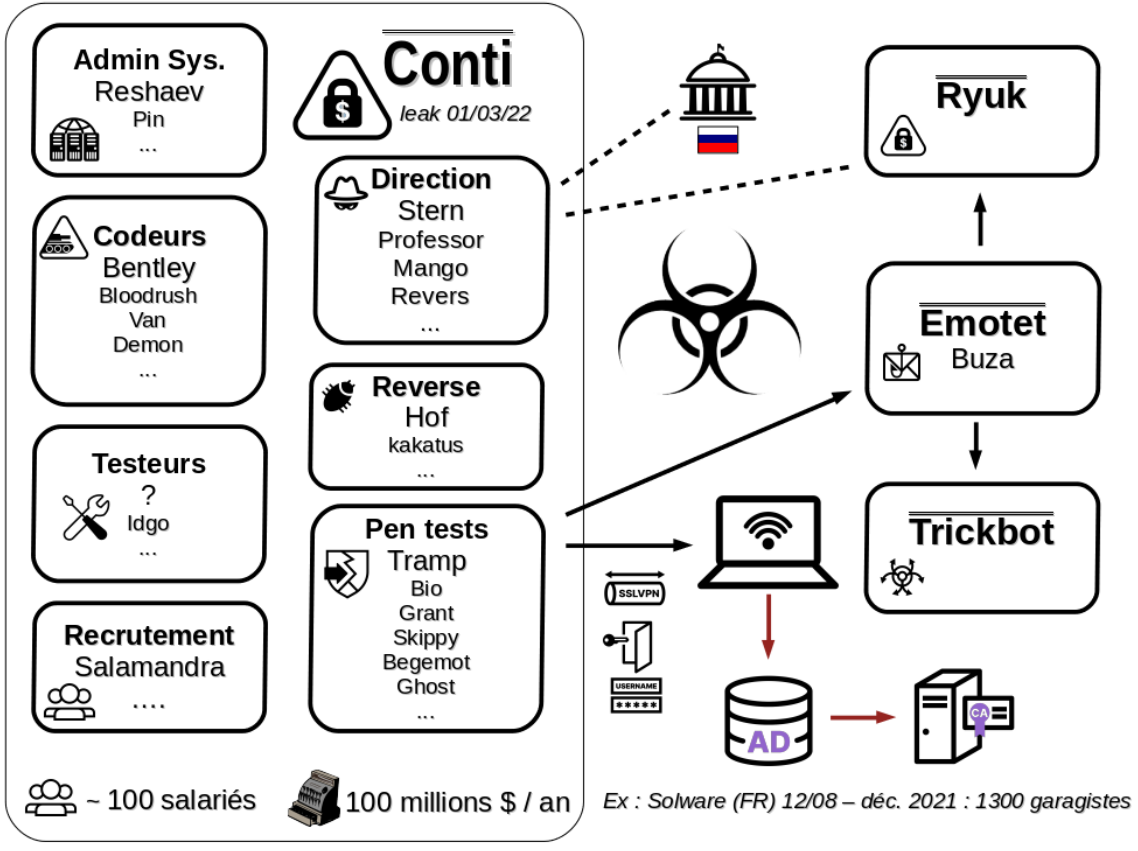


Escroquerie historique

Nos utilisateurs doivent apprendre à lire une URL … systématiquement !

Kits standard avec transmission vers mail & canal Telegram

LE GROUPE CONTI



Dévoilé en mars 2022

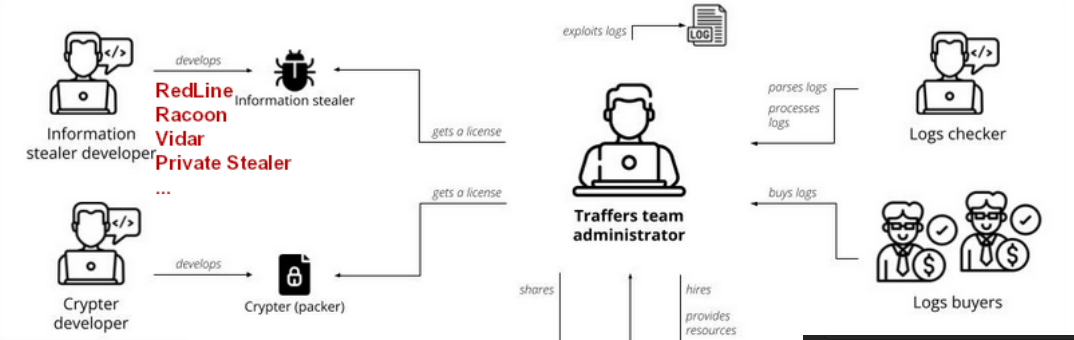
- Salariés et organisés en équipes
- Collaborations entre divers groupes

Ryuk : ransomware
Trickbot : troyen
Emotet : mails piégés

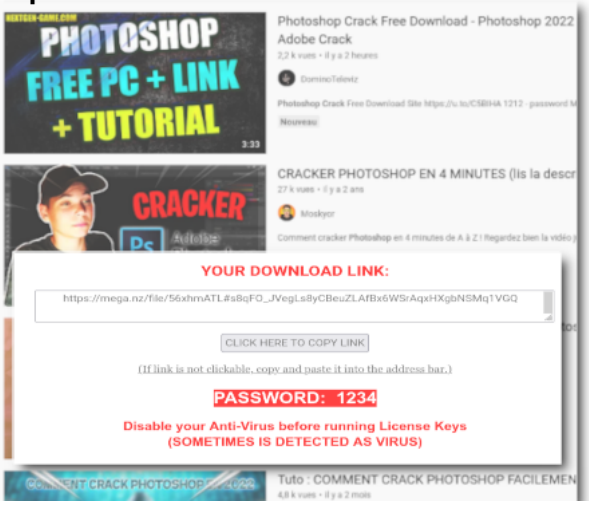
TRAFFERS

Трафферер

29 août 2022

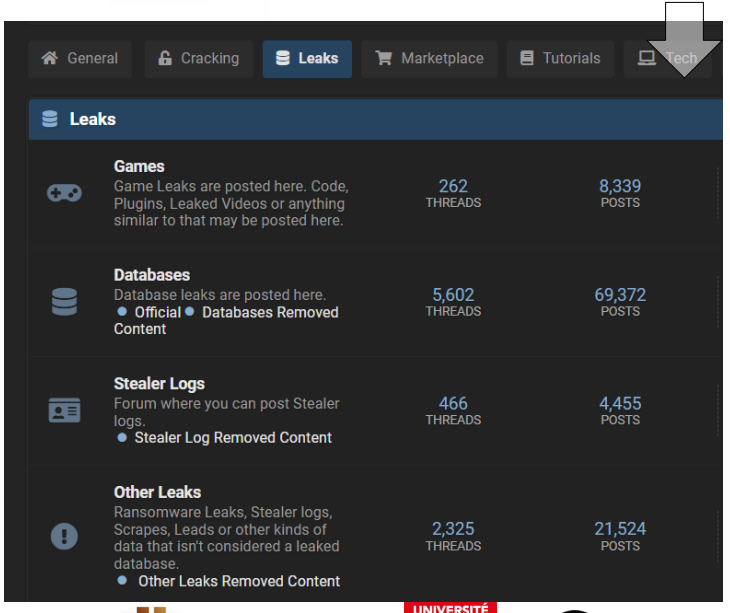


Opération 911



Dévoilé en août 2022

- Diffusion d'**infostealers**
- Vente de « logs »



jres RENNES 2024

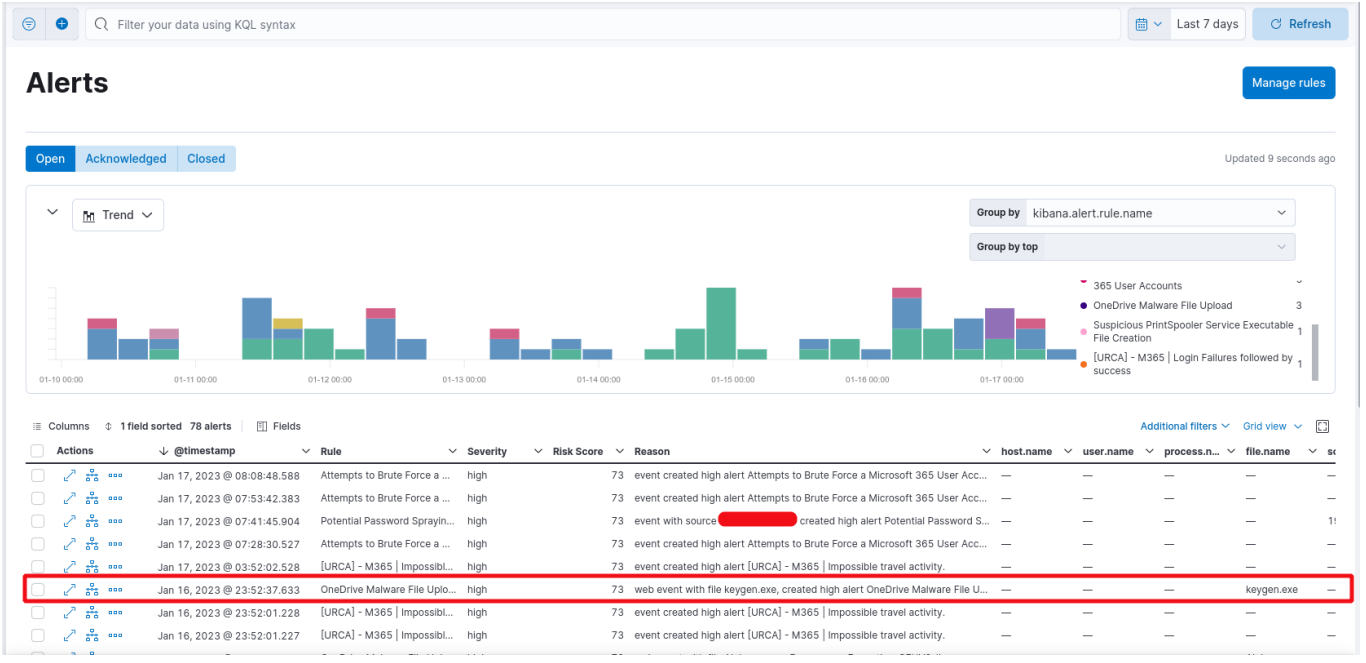
Université de Reims Champagne-Ardenne · esup portail · Université Toulouse Capitole · Université de Lorraine

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE
ESUP PORTAIL
UNIVERSITÉ TOULOUSE CAPITOLE
UNIVERSITÉ DE LORRAINE

CONTEXTES UNIVERSITAIRES

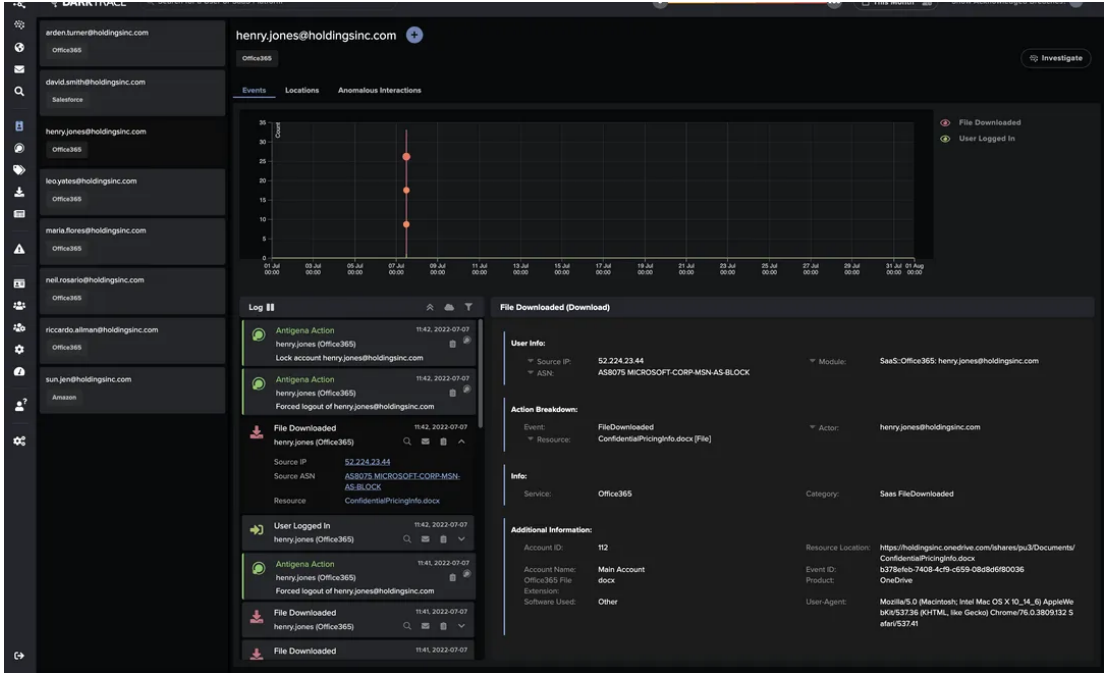
UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

- 30 000 étudiants, 4 000 personnels, 5 villes
- Détections : SIEM Elastic / Sonde NDR / Rspamd



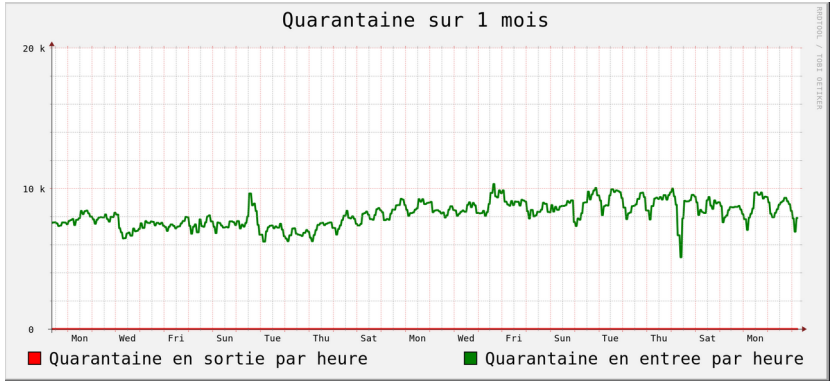
CONSORTIUM ESUP PORTAIL

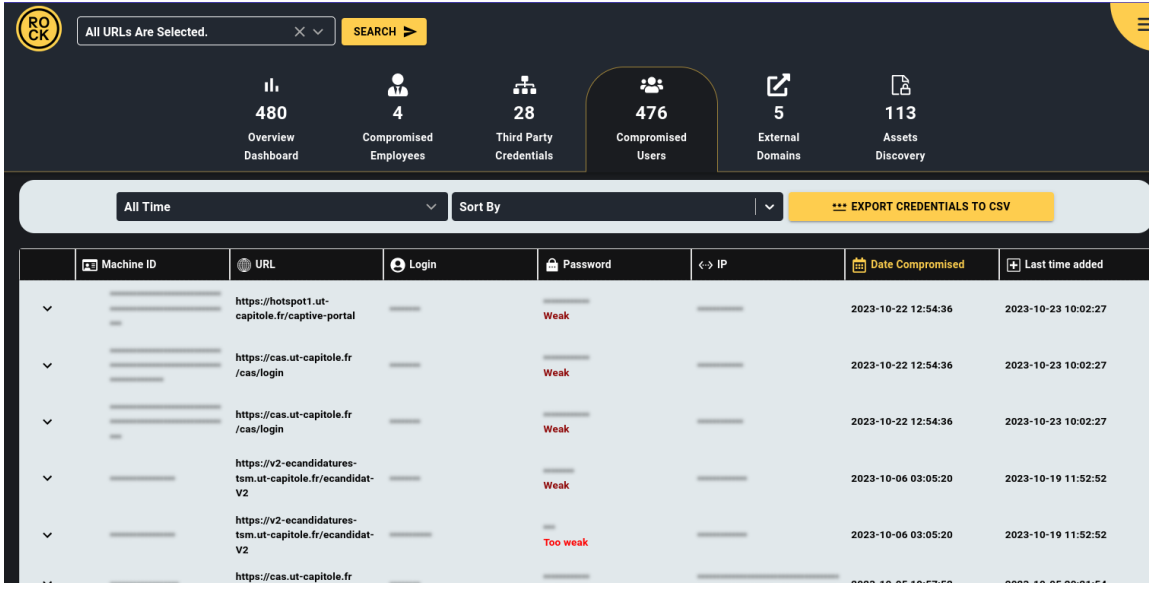
- Services pour une centaine d'établissements de l'ESR
- Détections : sonde NDR



UNIVERSITÉ TOULOUSE CAPITOLE

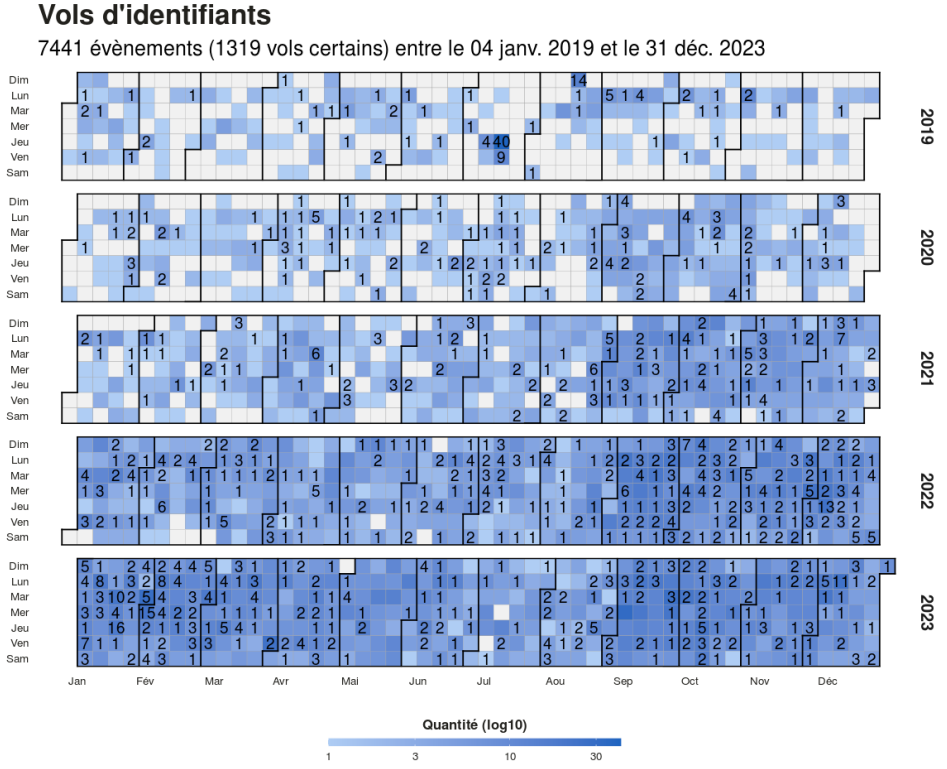
- 20 000 étudiants, 1 500 personnels
- Détections : honeypots, « logs » infostealers

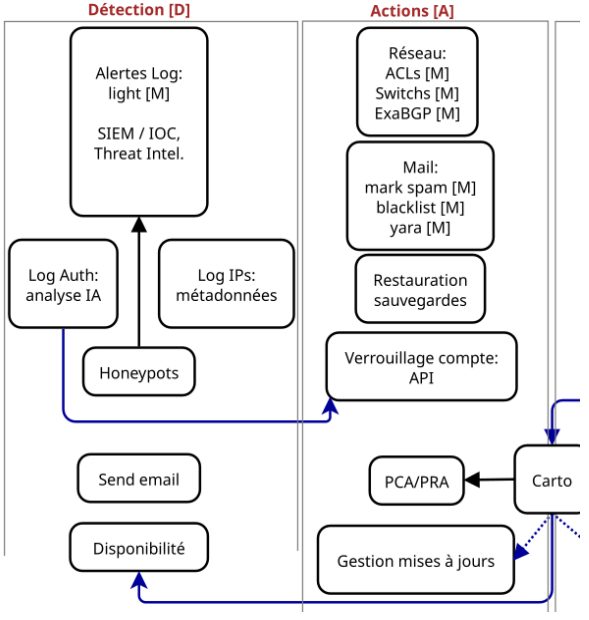




UNIVERSITÉ DE LORRAINE

- 60 000 étudiants, 9 000 personnels, 2 métropoles, 11 villes
- Détections : SMSI / analyse des logs de connexions





DES CONTEXTES DIVERS

DES MODES DE DÉTECTIONS,
DES MODES D'ACTIONS DIVERS

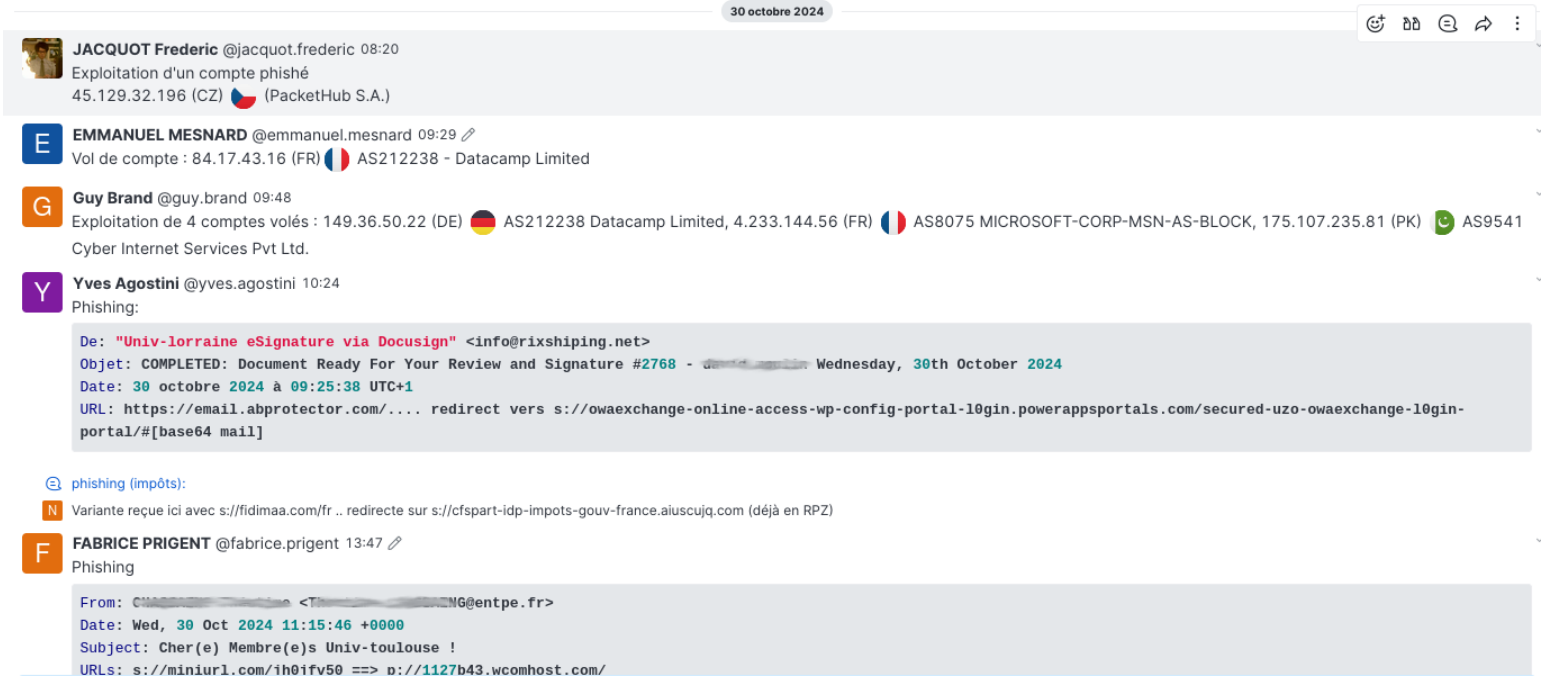
Nous sommes tous «ciblés»
Avec les mêmes techniques, par les mêmes escrocs,...

ROCKETCHAT
À VENIR…

PARTAGES D’IOC

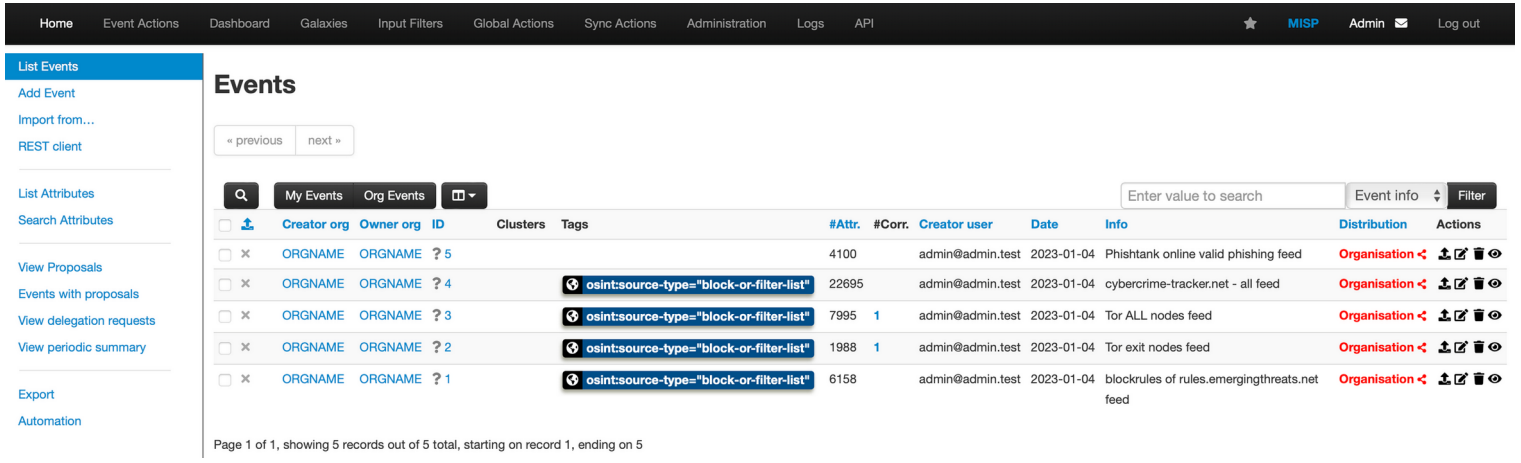
ROCKET CHAT : HTTPS://ROCKET.ESUP-PORTAIL.ORG/GROUP/SSI_IOC

- Depuis 2022, 30 établissements, 6 très actifs



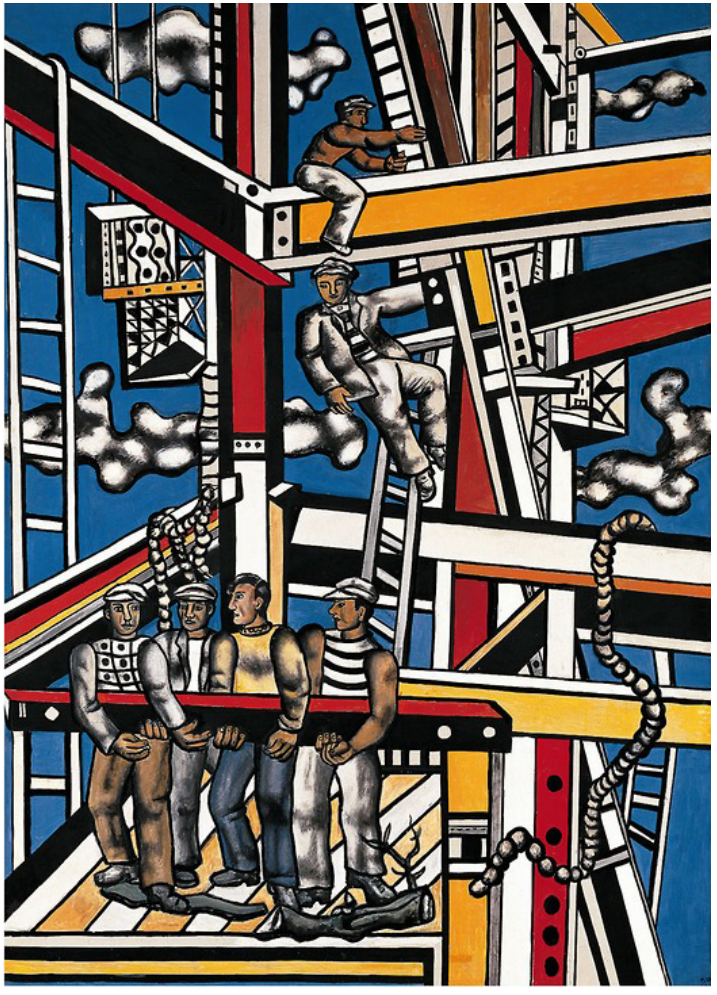
À VENIR

- MISP :



- Intégrations aux outils locaux ? Actions automatisées ?
- Définition des conditions d'accès ?

=> Qui souhaite participer à un groupe de travail ?



Merci pour votre attention

Questions ?

«Les constructeurs» - Fernand Léger – 1950