



jires

RENNES 2024

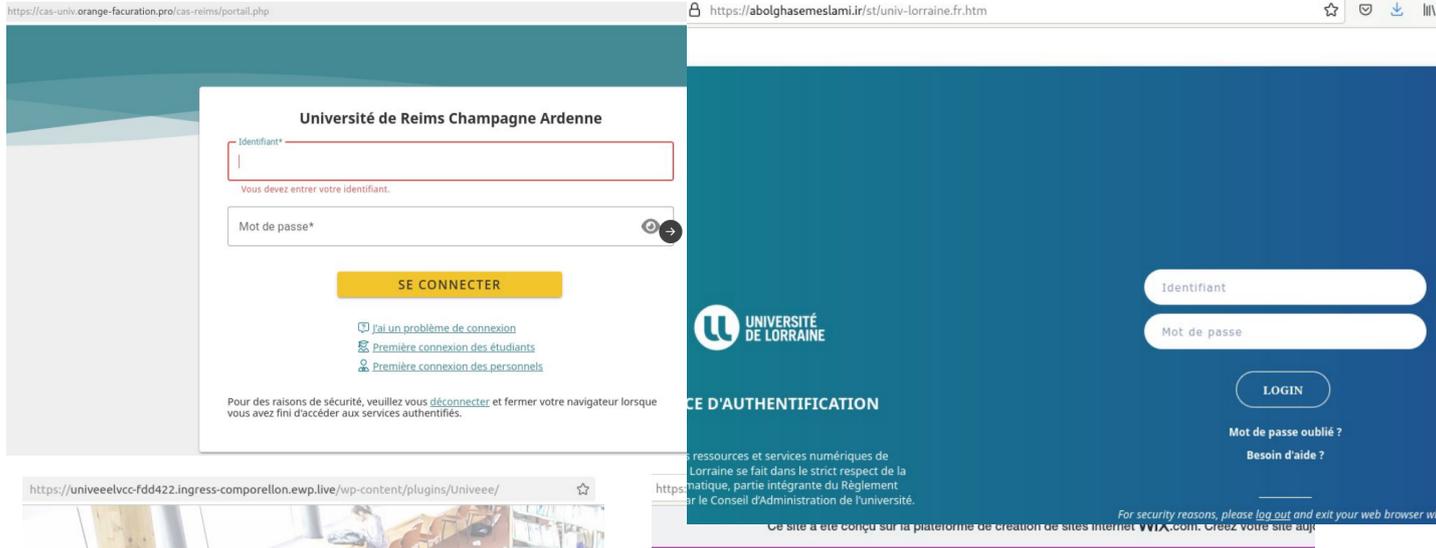
QUAND DES RSSI COLLABORENT ... (SUR UNE PLACE DE MARCHÉS D'IOC COMMUNAUTAIRE)

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

PHISHING
RANSOMWARE
INFOSTEALER

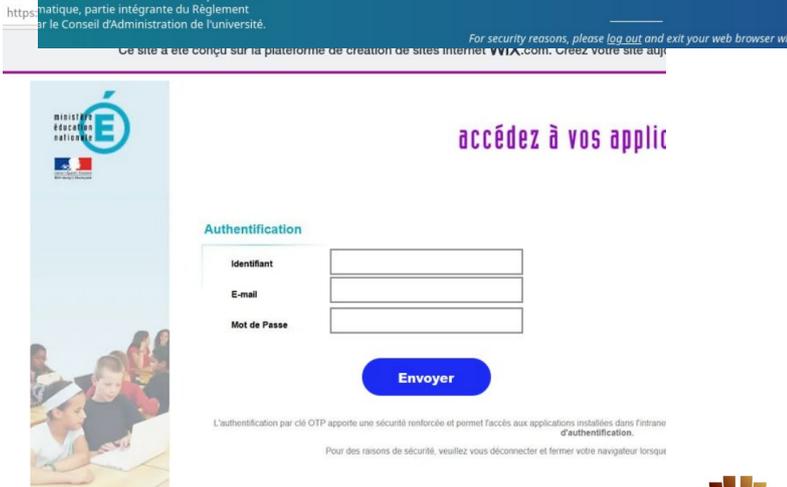
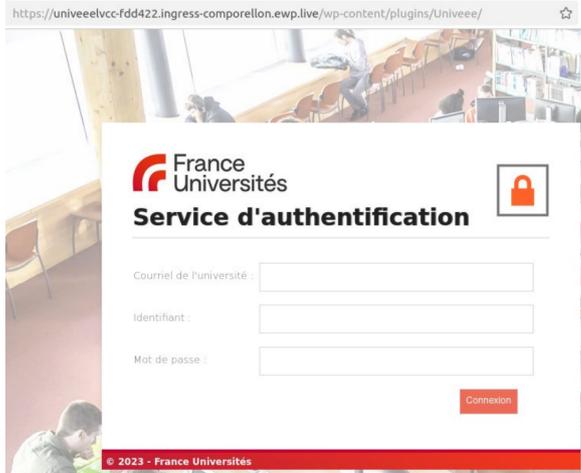
BUSINESS DES MALWARES

PHISHING

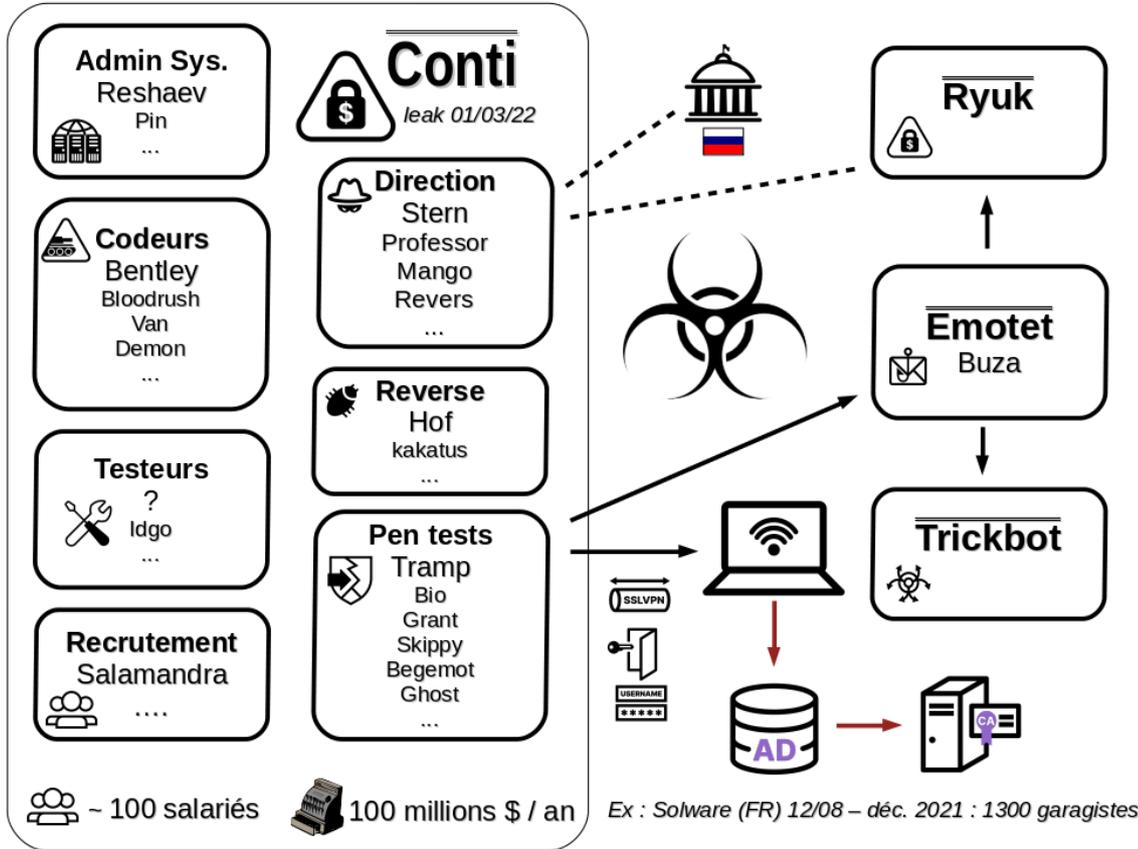


Escroquerie historique

Nos utilisateurs doivent apprendre à lire une URL ... systématiquement !



LE GROUPE CONTI



Dévoilé en mars 2022

- Salariés et organisés en équipes
- Collaborations entre divers groupes

Ryuk : ransomware

Trickbot : troyen

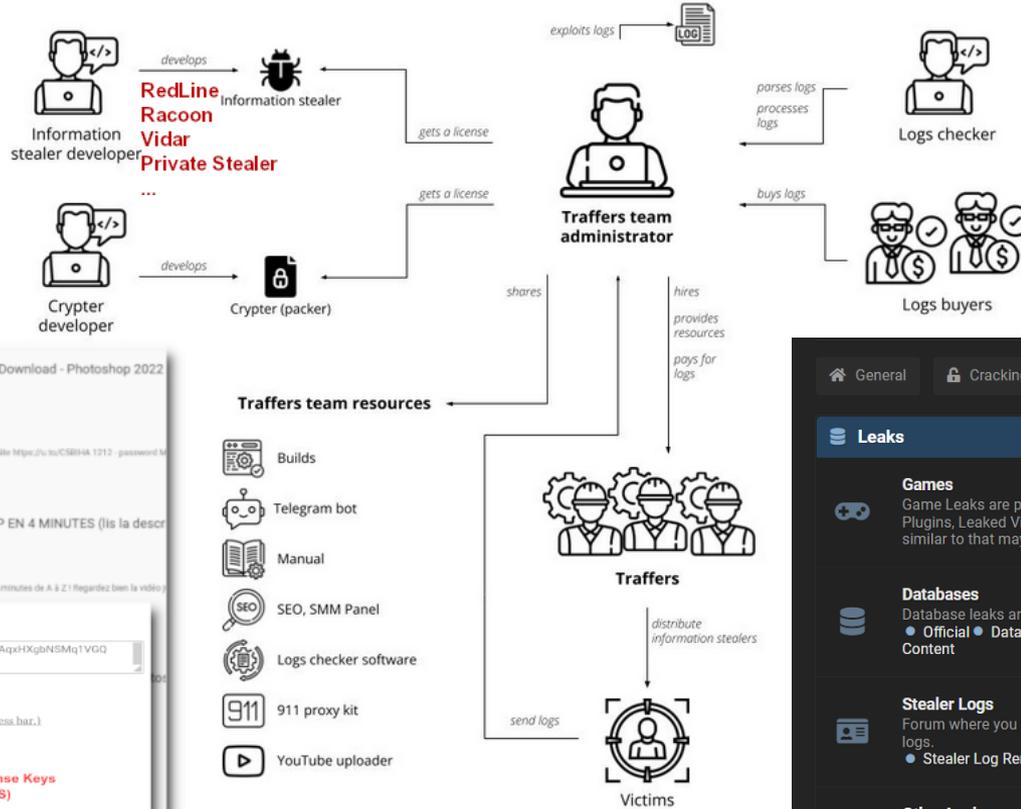
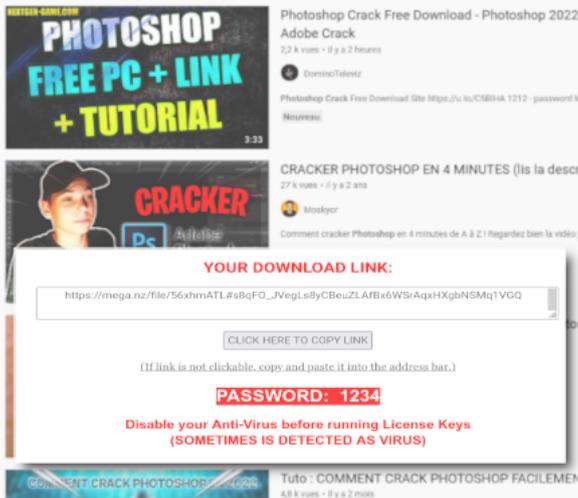
Emotet : mails piégés

TRAFFERS

Траффер

29 août 2022

Opération 911



Dévoilé en août 2022

- Diffusion d'infostealers
- Vente de « logs »

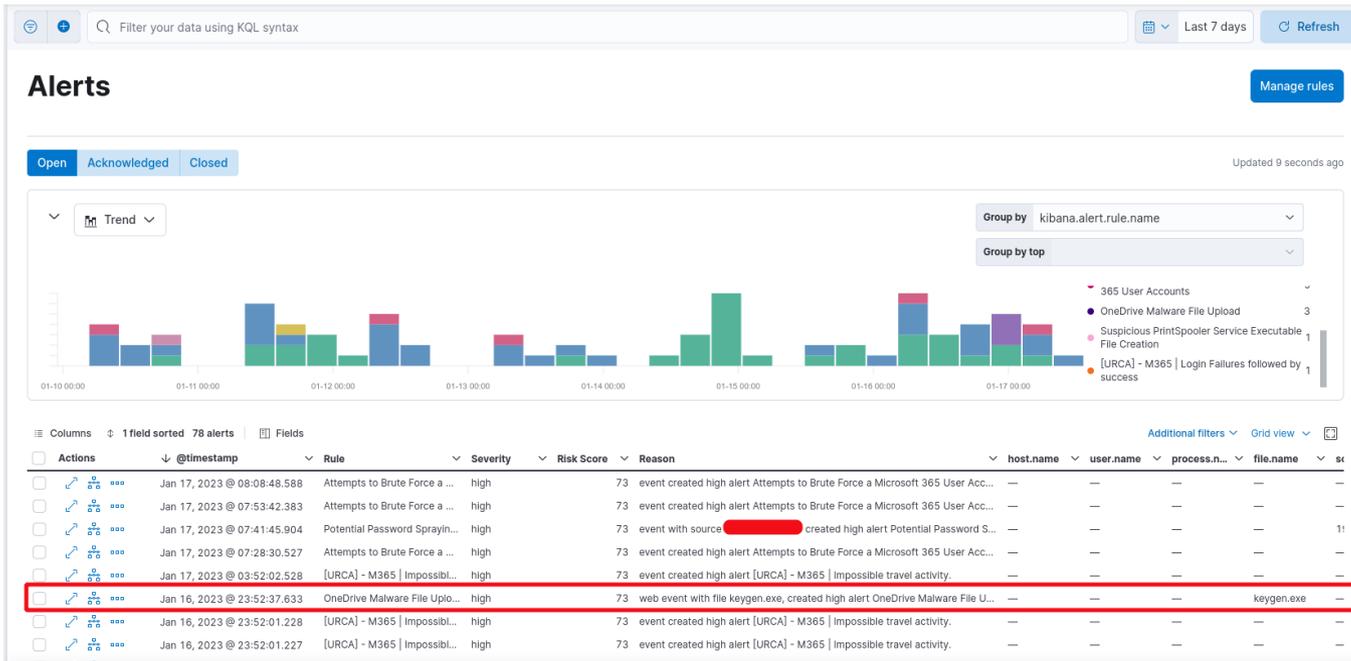
Category	Description	Threads	Posts
Games	Game Leaks are posted here. Code, Plugins, Leaked Videos or anything similar to that may be posted here.	262	8,339
Databases	Database leaks are posted here. Official Databases Removed Content	5,602	69,372
Stealer Logs	Forum where you can post Stealer logs. Stealer Log Removed Content	466	4,455
Other Leaks	Ransomware Leaks, Stealer logs, Scrapes, Leads or other kinds of data that isn't considered a leaked database. Other Leaks Removed Content	2,325	21,524

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



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

The screenshot displays a security dashboard for the user henry.jones@holdingsinc.com. On the left, a list of users is shown. The main area features a timeline with a graph showing activity over time. Below the graph, there are detailed event logs for the user, including:

- Artigena Action:** Lock account henry.jones@holdingsinc.com
- Artigena Action:** Forced logout of henry.jones@holdingsinc.com
- File Downloaded:** ConfidentialPricingInfo.docx
- User Logged In:** henry.jones (Office365)
- Artigena Action:** henry.jones (Office365)
- File Downloaded:** henry.jones (Office365)
- File Downloaded:** henry.jones (Office365)

The right side of the dashboard shows a 'File Downloaded (Download)' section with details for the user info, action breakdown, and additional information.

The top screenshot shows an alert titled 'External Connection' with a 100% detection rate. The details include:

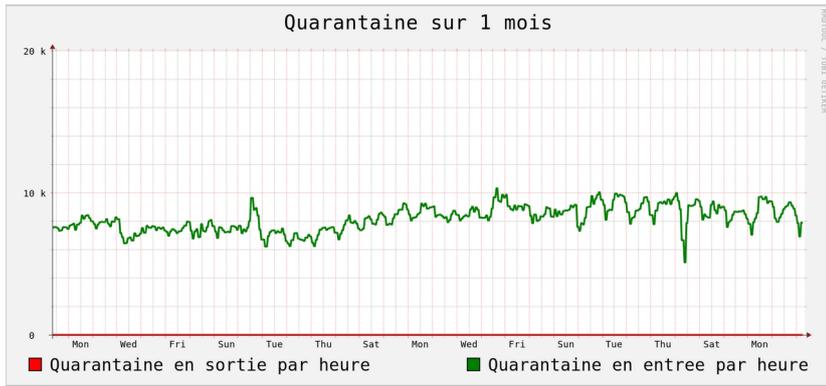
- Inoculation source: Darktrace:Antigena Email:Fake Portal
- ASN: AS16276 OVH SAS
- Hostname: projects.ayomi.fr
- To: 135.125.37.226
- Inoculation description: Host was observed in a phishing link identified by Antigena Email, which points to a fake login portal used for credential harvesting. Inoculation classified this phishing email as a possible fake generic notification.
- Inoculation strength: 50

The bottom screenshot shows an alert titled 'SMB Read Success' with a 30% detection rate. The details include:

- Event message share: \\dfs-ma-.../devu file=Handicap10-...-APPEL A PROJET UNIVERSITE EXCELLENCE INCUSIVE:RESANA - plateforme et mot de passe...docx version=smb2 account=magali.lastricani
- Event ID: ConfidentialPricingInfo.docx
- Product: OneDrive
- User Agent: Mozilla/5.0 (Microsoft; Intel Max OS X 10.14.0; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3909.132 Safari/537.41

UNIVERSITÉ TOULOUSE CAPITOLE

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

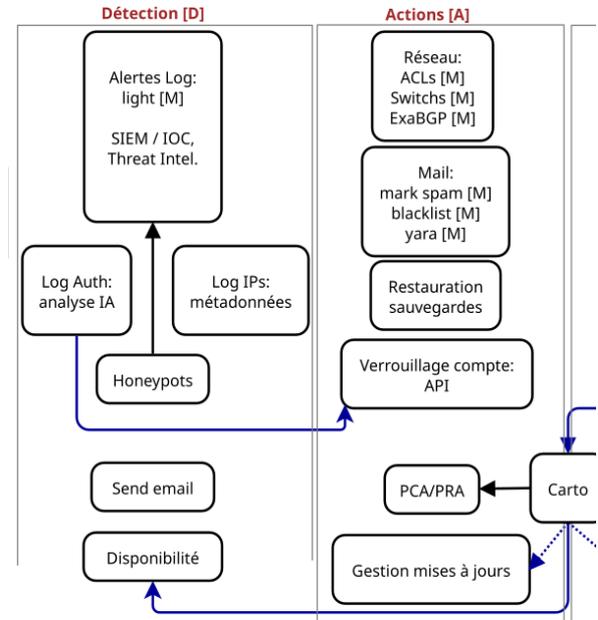
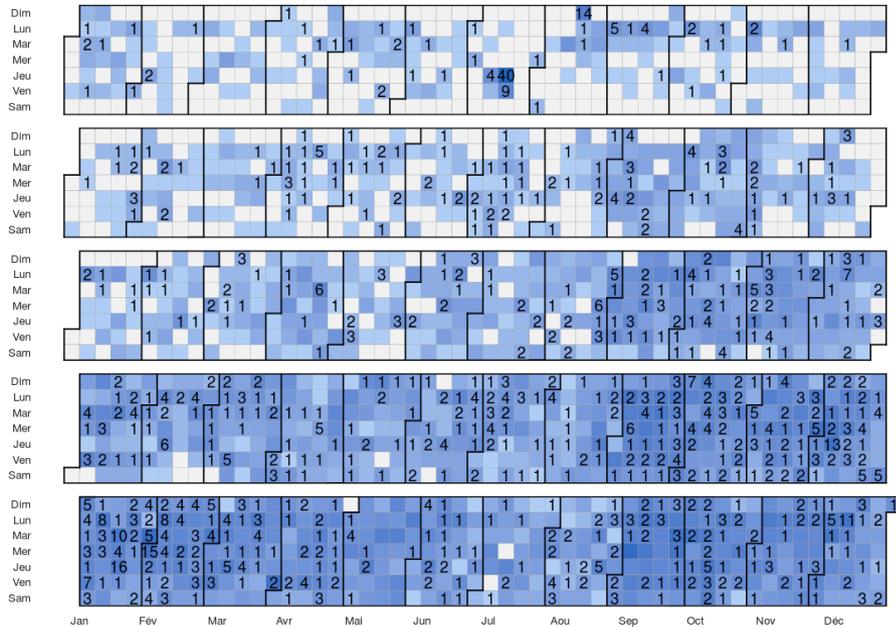


Machine ID	URL	Login	Password	IP	Date Compromised	Last time added
...	https://hotspot1.ut-capitole.fr/captive-portal	...	Weak	...	2023-10-22 12:54:36	2023-10-23 10:02:27
...	https://cas.ut-capitole.fr/cas/login	...	Weak	...	2023-10-22 12:54:36	2023-10-23 10:02:27
...	https://cas.ut-capitole.fr/cas/login	...	Weak	...	2023-10-22 12:54:36	2023-10-23 10:02:27
...	https://v2-ecandidatures-tsm.ut-capitole.fr/ecandidat-V2	...	Weak	...	2023-10-06 03:05:20	2023-10-19 11:52:52
...	https://v2-ecandidatures-tsm.ut-capitole.fr/ecandidat-V2	...	Too weak	...	2023-10-06 03:05:20	2023-10-19 11:52:52
...	https://cas.ut-capitole.fr

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

Vols d'identifiants

7441 évènements (1319 vols certains) entre le 04 janv. 2019 et le 31 déc. 2023



DES CONTEXTES DIVERS

DES MODES DE DÉTECTIONS,
DES MODES D'ACTION DIVERS

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

ROCKETCHAT
À VENIR...

PARTAGES D'IOC

◆ Depuis 2022, 30 établissements, 6 très actifs

30 octobre 2024

JACQUOT Frederic @jacquot.frederic 08:20
Exploitation d'un compte phishé
45.129.32.196 (CZ) 🇨🇪 (PacketHub S.A.)

EMMANUEL MESNARD @emmanuel.mesnard 09:29 ✎
Vol de compte : 84.17.43.16 (FR) 🇫🇷 AS212238 - Datacamp Limited

Guy Brand @guy.brand 09:48
Exploitation de 4 comptes volés : 149.36.50.22 (DE) 🇩🇪 AS212238 Datacamp Limited, 4.233.144.56 (FR) 🇫🇷 AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, 175.107.235.81 (PK) 🇵🇰 AS9541
Cyber Internet Services Pvt Ltd.

Yves Agostini @yves.agostini 10:24
Phishing:

De: "Univ-lorraine eSignature via DocuSign" <info@rixshipping.net>
Objet: COMPLETED: Document Ready For Your Review and Signature #2768 - [redacted] Wednesday, 30th October 2024
Date: 30 octobre 2024 à 09:25:38 UTC+1
URL: <https://email.abprotector.com/...> redirect vers s://owaexchange-online-access-wp-config-portal-10gin.powerappsportals.com/secured-uzo-owaexchange-10gin-portal/#[base64 mail]

🔍 phishing (impôts):
🇺🇸 Variante reçue ici avec s://fidimaa.com/fr .. redirecte sur s://cfspart-idp-impots-gouv-france.aiuscuqj.com (déjà en RPZ)

FABRICE PRIGENT @fabrice.prigent 13:47 ✎
Phishing

From: [redacted] <[redacted]@entpe.fr>
Date: Wed, 30 Oct 2024 11:15:46 +0000
Subject: Cher(e) Membre(e)s Univ-toulouse !
URLs: s://miniurl.com/ih0ifv50 ==> p://1127b43.wcomhost.com/

◆ MISP :

The screenshot displays the MISP 'Events' page. The left sidebar contains navigation options like 'List Events', 'Add Event', 'Import from...', 'REST client', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'View periodic summary', 'Export', and 'Automation'. The main area shows a table of events with the following data:

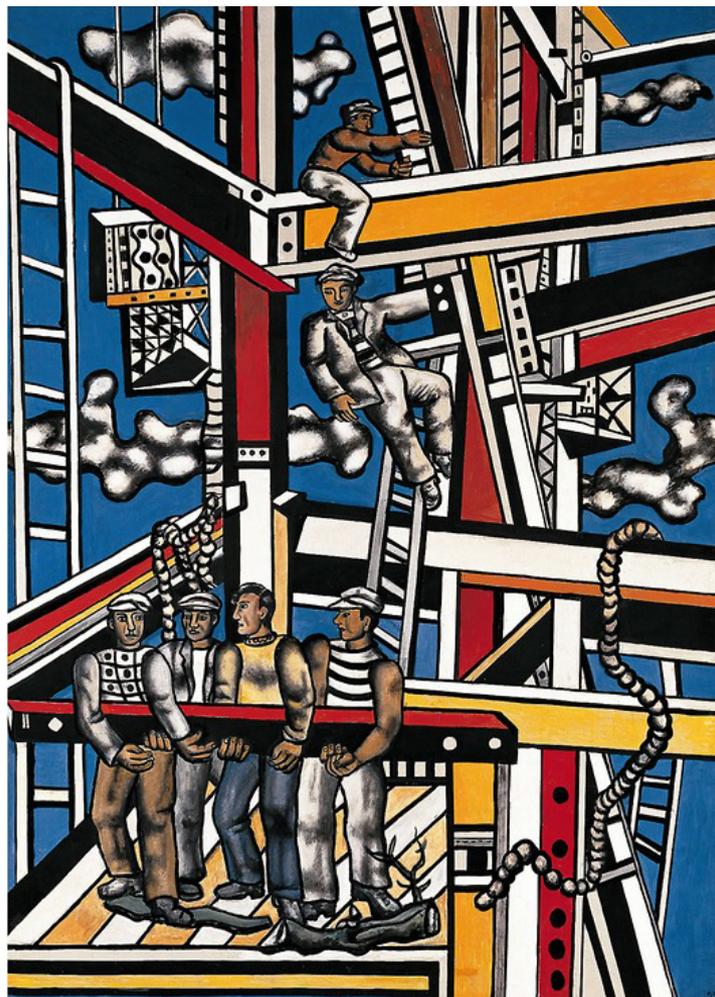
<input type="checkbox"/>	<input type="checkbox"/>	Creator org	Owner org	ID	Clusters	Tags	#Attr	#Corr	Creator user	Date	Info	Distribution	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	? 5			4100		admin@admin.test	2023-01-04	Phishtank online valid phishing feed	Organisation <	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	? 4		osint:source-type="block-or-filter-list"	22695		admin@admin.test	2023-01-04	cybercrime-tracker.net - all feed	Organisation <	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	? 3		osint:source-type="block-or-filter-list"	7995	1	admin@admin.test	2023-01-04	Tor ALL nodes feed	Organisation <	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	? 2		osint:source-type="block-or-filter-list"	1988	1	admin@admin.test	2023-01-04	Tor exit nodes feed	Organisation <	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	? 1		osint:source-type="block-or-filter-list"	6158		admin@admin.test	2023-01-04	blockrules of rules.emergingthreats.net feed	Organisation <	

Page 1 of 1, showing 5 records out of 5 total, starting on record 1, ending on 5

◆ 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