



# Investiguer et détecter la menace du phishing Adversary-in-The-Middle

Grégoire CLERMONT  
Quentin BOURGUE

27 mars 2024

# Qui sommes- nous ?

## Threat Detection & Research (TDR), Sekoia.io



**Grégoire CLERMONT**

*CTI & Detection Analyst*

grégoire.clermont@sekoia.io



**Quentin BOURGUE**

*Lead Cybercrime Analyst*

quentin.bourgue@sekoia.io

# Plan de la présentation

- 1 Phishing Adversary-in-The-Middle :  
la technique et l'écosystème
- 2 Investigation des campagnes  
et identification des kits de  
phishing
- 3 De la détection à la  
remédiation

# Phishing Adversary-in-The-Middle : la technique et l' écosystème

# Le phishing, aujourd'hui



1

De : **Sekoia System Maintenance** <notifications@getanyprivateinfo.com>  
Date: ven, 2 févr. 2024 à 13:01  
Subject: Resolve Now: Limited Storage Preventing Email Activity - @sekoia.fr  
To: <@sekoia.fr>



Your mailbox has reached its capacity



@sekoia.fr mailbox is unable to send or receive messages due to limited storage.

Please visit your email portal to resolve this matter by freeing up space.

To create additional space, click the "Free-up Space" button below.

Free-up Space

Mailbox address: @sekoia.fr

This e-mail is covered by the Electronic Communications Privacy Act, 18 U.S.C. 2510-2521 and is legally privileged.

Disclaimer

2

Étapes de redirections, anti-bot, CAPTCHA

3

sekoia

← a1@sekoia.fr

Enter password

Because you're accessing sensitive info, you need to verify your password.

Password

Forgot my password

Sign in

Pages de phishing AiTM usurpant la charte graphique de la victime (dynamique)

# Fonctionnement de la technique Adversary-in-The-Middle



Phishing  
“classique”  
devenu obsolète  
avec le MFA

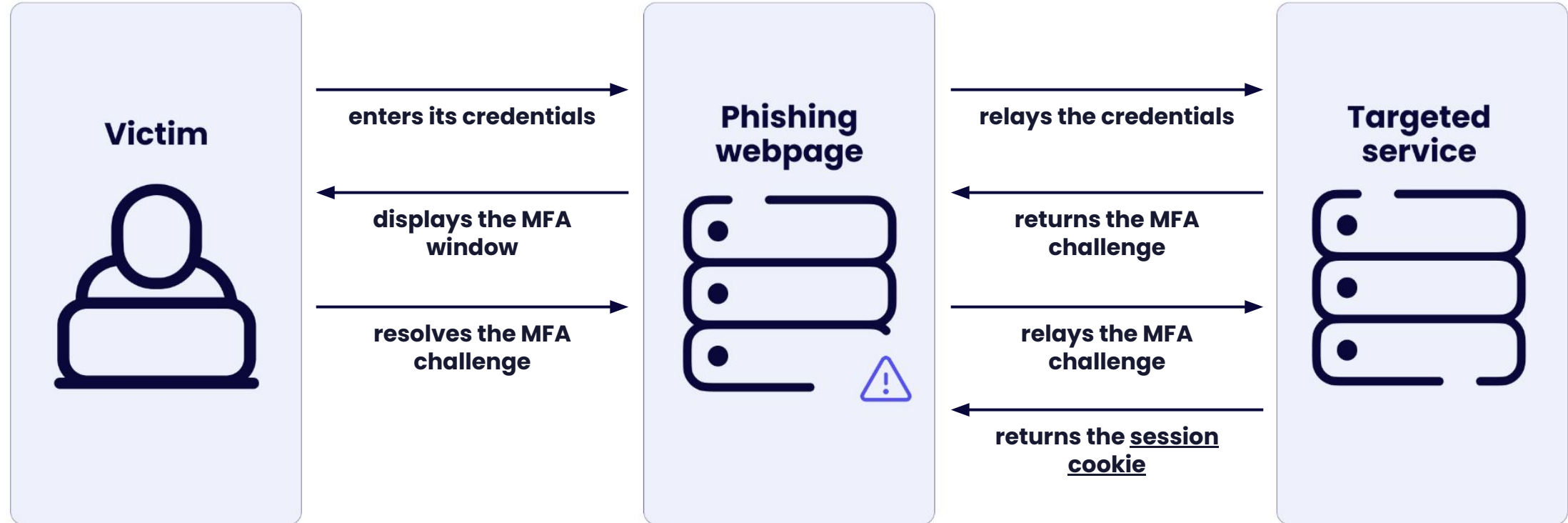


Authentification  
multifacteur  
(MFA)  
→ Résolution d'un  
challenge unique



Bypass du MFA  
avec le phishing  
AiTM

# Fonctionnement de la technique Adversary-in-The-Middle



# Écosystème cybercriminel associé au Phishing-as-a-Service



Pages de phishing AiTM  
clé en main pour  
\$120 à \$1000 par  
mois



Promotion et  
vente sur  
Telegram (bots)



Acteurs majeurs :

- EvilProxy
- Caffeine
- NakedPages
- Tycoon 2FA
- Greatness



# Écosystème cybercriminel associé au Phishing-as-a-Service



Name: Office 2FA Cookie Stealer (30 Days, Never Red Screen)

## ANTI-RED 2FA OFFICE LINKS

### Requires:

- ◆ Domain

### Page Features:

- ◆ Auto Capture 2FA Cookies (Phone and Microsoft Authenticator app).
- ◆ Available with Offline 2FA Attachment.
- ◆ Available with Redirect Attachment.
- ◆ Link Statistics.
- ◆ Auto Grab victim number where the 2fa code was sent.
- ◆ One Time (ON/OFF).
- ◆ Block Countries (ON/OFF).
- ◆ Custom Page Title (ON/OFF).
- ◆ Telegram ID.
- ◆ Custom Redirect Link.
- ◆ Dynamic Codes.
- ◆ Auto Grab Email (Normal, Base64).
- ◆ Auto Fetch Custom Logos. Backgrounds.

Price: \$400



**Caffeine**  
(670+ abonnés)

@evilproxy [Phishing as a Service]

✓ Our phishing pages are 100% identical!

You get LOGIN, PASSWORD, COOKIES and more info about user

!! Мы можем помочь вам повысить устойчивость к фишинговым атакам. Фишинг как услуга (PhaaS) - это программа повышения осведомленности о безопасности для всех сотрудников организации.

Наши симуляции фишинга поддерживаются программной платформой собственной разработки. В частности, наше бэкэнд-приложение предлагает полный набор функций, необходимых для проведения фишинговых кампаний:

!! We can help you improve your resilience against phishing attacks. Phishing as a Service (PhaaS) is a security awareness program for all employees of the organization.

Our phishing simulations are supported by an in-house developed software platform. In particular, our backend application offers the full set of functionalities required to conduct phishing campaigns: Get a demo completely free 1 day!

### ✓ + Services:

- ◆ google.com 10/20/31 days = 250/450/600\$ ( <https://youtu.be/o-xWNwTmyps> )
- ◆ microsoft 10/20/31 days = 150/250/400\$ (Hotmail, CORP, Remote SSO, ADFS) ( [https://youtu.be/dim\\_lfqTy64](https://youtu.be/dim_lfqTy64) )
- ◆ icloud.com 10/20/31 days = 150/250/400\$ (auto token/cookies refresh up to 2 days with internal tool)
- ◆ dropbox.com 10/20/31 days = 150/250/400\$ (also sign in with google)
- ◆ github.com 10/20/31 days = 150/250/400\$
- ◆ linkedin 10/20/31 days = 150/250/400\$
- ◆ yandex.ru 10/20/31 days = 150/250/400\$
- ◆ facebook.com 10/20/31 days = 150/250/400\$
- ◆ yahoo.com 10/20/31 days = 150/250/400\$

**EvilProxy**  
(3100+ abonnés)

Saad Tycoon Group 🚀

Latest Update 🚀🚀🚀

Introducing our brand-new Anti-Bot feature, designed to keep your URLs super safe! 🛡️🔒

Mode 1: 🚀 **STRONG MODE** 🚀 Highly recommended for ultimate protection! No chance of detection, and your link stays strong for months! 🛡️🔒

Mode 2: 🚫 **LOW ANTI-BOT** 🚫 Not recommended, but if you like living on the edge! Higher chance of detection, and if your URL gets caught, you'll have to pay for a domain change. 🌐🔗 Also, we can't predict how long your link will last in this mode. 🕒🔒

Choose wisely, go for the best protection, and keep your links secure with TeMa Tycoon's Anti-Bot update! 🌐🔒

🛡️🔒 Ready to level up your security? Follow these simple steps to tweak your Anti-Bot settings in the admin panel:

🔑 **Login:** Head to your admin panel and log in with your credentials.

⚙️ **Settings:** Navigate to the "Settings" section.

🛡️ **Anti-Bot Level:** Look for the "Anti-Bot" option and click on it.

⚙️ **Adjust Settings:** Choose your desired Anti-Bot level from the options available. Whether you want robust protection or a lighter touch, it's all at your fingertips!

💾 **Save Changes:** Don't forget to save your changes before leaving the panel.

Voilà! You've successfully fine-tuned your Anti-Bot settings for enhanced security. 🌐🔒 Stay safe online!

**Tycoon 2FA**  
(450+ abonnés)

Naked Pages Announcement

!! READ THIS AND UNDERSTAND PLEASE !!

WITH NAKEDPAGES YOU GET ACCESS TO OUR BOT AND CAN USE

copy  
INBUILT REDIRECT/PHP REDIRECT  
ATTACHMENT/OFFLINE ATTACHMENT  
DIRECT LINKS

ALL IN THE POWER OF YOUR HANDS

WE HAVE 2 TYPES OF LICENSE

NORMAL LICENSE: 300\$  
RENEW @: 200\$

VIP LICENSE: 1K\$  
RENEW @: 700\$

FOR NORMAL LICENSE YOU CAN USE ALL OUR PUBLIC PAGES LIST BELOW:

copy  
Office(With 2fa bypass and cookies)  
Outlook(+2fa bypass and cookies)  
Yahoo + 2fa bypass + cookies  
Aol + 2fa bypass + Cookies  
Dropbox + 2fa bypass + Cookies  
Ionos + 2fa bypass + Cookies  
Rackspace + 2fa bypass + Cookie  
-----Email Cookie Capture-----  
(You get email access cookies to bypass 2fa for: Gmail(IF VIP), aol, yahoo, outlook, office)  
  
adobex (Adobe Theme Capture Email Then Email cookies)  
onedrivex (Onedrive Theme Capture Email Then Email cookies)  
emailx (Plaid Capture Email Then Email cookies) (For banks)  
autox (Automatic Capture Email From Autograb Then Email cookies)

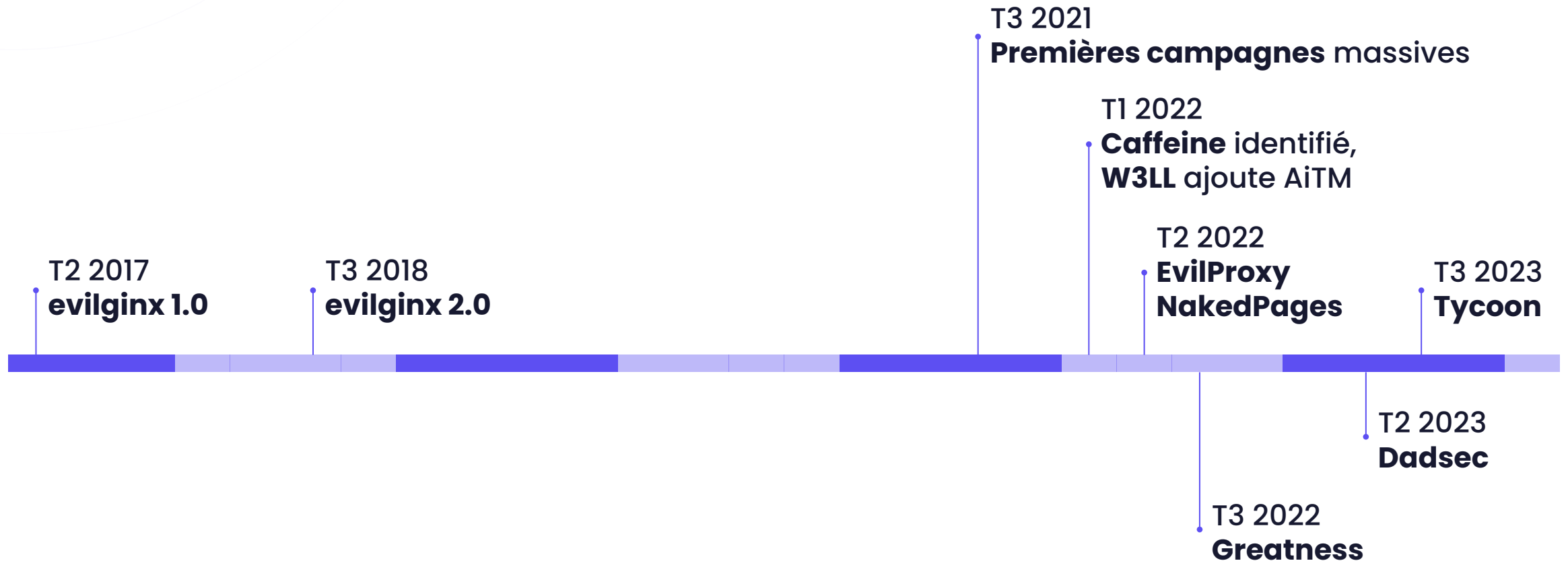
**NakedPages**  
(4400+ abonnés)

# Fonctionnalités des kits vendus en PhaaS



- Ciblage des services spécifiques (Microsoft, Gmail, Dropbox...)
- Collecte des mots de passe, adresses email, adresses IP, navigateurs
- Relai des challenges 2FA et collecte des cookies de session
- Récupération automatique de la charte graphique de l'organisation
- Exfiltration vers Telegram
- Protection des pages avec un CAPTCHA, Cloudflare, anti-bot

# Écosystème cybercriminel associé au Phishing-as-a-Service



# Investigation des campagnes et identification des kits de phishing

# Investigation des kits de phishing AiTM



## Objectifs (contexte, CTI, recherche, etc.)

- Analyser une campagne de phishing
- Contextualiser une page de phishing
- Illuminer l'infrastructure associée
- Dénicher des nouvelles menaces émergentes

# Investigation des kits de phishing AiTM



1

The screenshot shows the urlscan.io interface for a scan of **i9152.cisele0.com**. The domain is associated with IP **172.67.162.203** (United States) and is hosted on **CLOUDFLARENET, US**. The scan was performed on March 03, 2024, at 2:37:06 am UTC. The effective URL is **https://i9152.cisele0.com/NOZcbtTxxEiGj/**. The summary indicates that the website contacted 4 IPs in 3 countries across 5 domains to perform 5 HTTP transactions. The main IP is 172.67.162.203. The TLS certificate was issued by E1 on February 28th, 2024, and is valid for 3 months. The scan shows that **shorturl.at** was scanned 6060 times on urlscan.io. The urlscan.io verdict is "No classification". The page title is **rQdxWXndQt**. The screenshot shows a loading page with a yellow background and a message: "Just a moment, we're working on getting this page ready for you. This page is running browser checks to ensure your security."

## Caractéristiques pertinentes :

- URLs de redirection
- Contenu
- Titre de la page
- Hébergement
- Ressources contactées

Analyse rapide de l'URL de phishing : **urlscan.io** ou **console du navigateur web** (bac à sable)

# Investigation des kits de phishing AiTM



2

urlscan.io Home Search Live API Blog Docs Pricing Corine

Sponsored by SecurityTrails A Recorded Future Company

Search for domains, IPs, filenames, hashes, ASNs

server:cloudflare page.title.keyword: /[a-zA-Z]{10}/ filename:"jquery-3.6.0.min.js" AND "turnstile/v0/api.js" Search Help

Search results (100 / 611, sorted by date, took 200ms) Showing All Hits Details: Hidden

URL	Age	Size	IPs	🏠
dlh8vxdpla.dx9no.com/v10h507mtr/	Public 2 minutes 49 KB 6 5 1	🇺🇸		
rsx.ritheran.com/586Z/	Public 38 minutes 48 KB 5 4 1	🇺🇸		
kwua.knanumck.com/ninaphan/	Public 53 minutes 48 KB 5 4 2			
fuyici.otandord.ru/uskylega/	Public 2 hours 51 KB 7 6 2	🇺🇸		
f662p.emorasp8.com/220e/NzQyODI2OC9mcm9udGVuZC9qdXBpdGVyL2ZpbGVtYW5hZ2VvL2luZGV...	Public 2 hours 48 KB 5 3 1	🇺🇸		
05ui.acruitel.ru/bialblo/	Public 2 hours 49 KB 5 4 1	🇺🇸		
picuke.tleymnab.com/aramairf/	Public 3 hours 49 KB 5 4 1	🇺🇸		
picuke.tleymnab.com/aramairf/	Public 3 hours 49 KB 5 4 1	🇺🇸		
f662p.emorasp8.com/220e/	Public 3 hours 48 KB 7 5 1	🇺🇸		
f662p.emorasp8.com/220e/	Public 3 hours 48 KB 5 4 1	🇺🇸		
v12w7ymtol1.com/i011bwh/	Public 3 hours 48 KB 5 4 1	🇺🇸		
26jt2.yonque1.com/42wkJYSK0ykb/	Public 3 hours 49 KB 5 4 2	🇺🇸		
svz.8j3h2.com/y2X6/	Public 3 hours 48 KB 5 4 1	🇺🇸		
2l1s2.coustor.com/543K4TJij8t8/	Public 6 hours 49 KB 5 4 1	🇺🇸		

server:cloudflare

page.title.keyword: /[a-zA-Z]{10}/

filename:"jquery-3.6.0.min.js"

filename:"turnstile/v0/api.js"



+ de 600 résultats sur 21 jours

+ de 175 noms de domaine

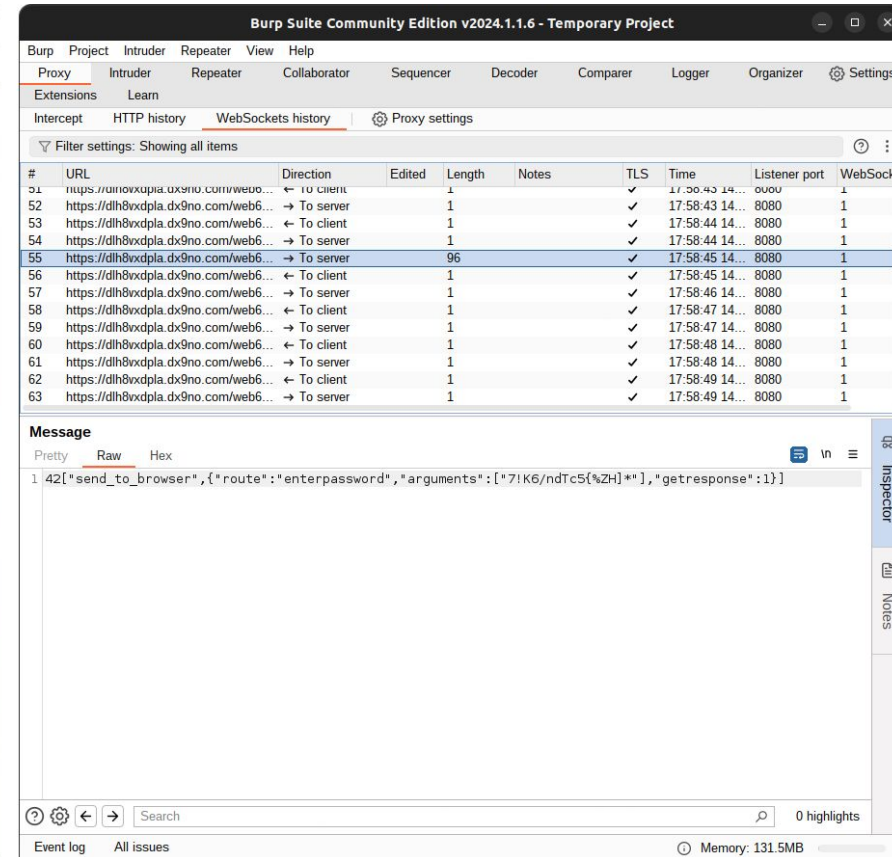
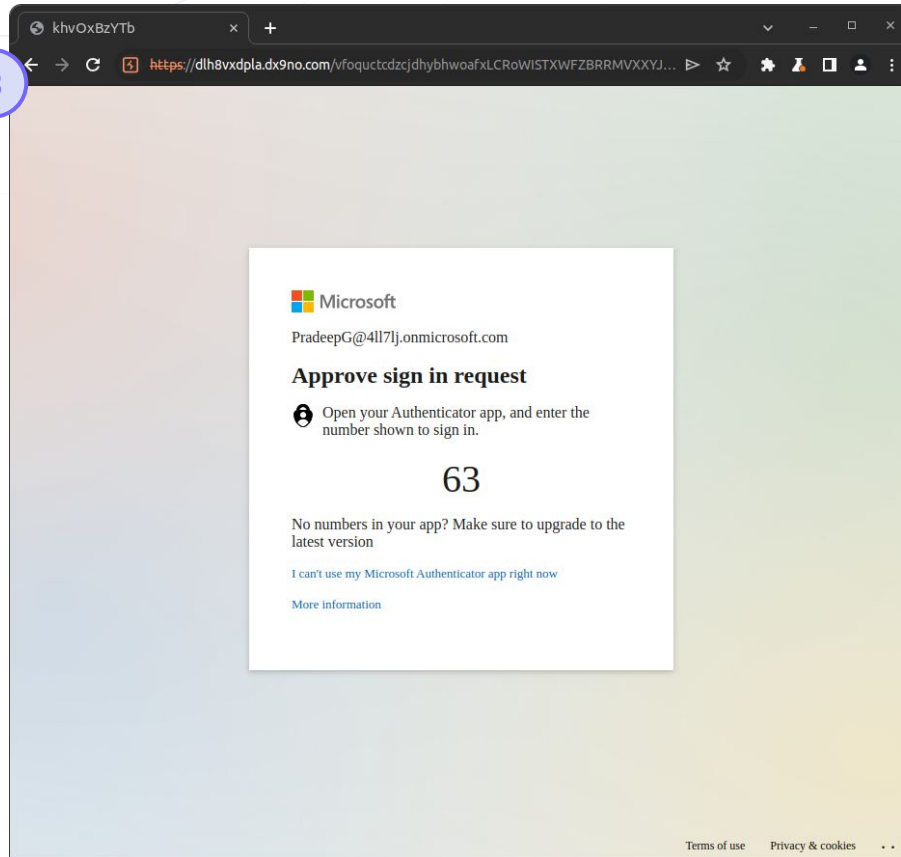
**Pivot** à partir des éléments caractéristiques (titre, ressources requêtées, domaines contactés, etc.)



# Investigation des kits de phishing AiTM



3



Analyse poussée avec **Burp Suite** en jouant l'attaque (avec un compte test)



# Investigation des kits de phishing AiTM



4

Microsoft Azure

Search resources, services, and docs (G+)

la-corine-admin@fic.on...  
M365 SANDBOX

Home > La Corine

## La Corine | Sign-in logs

User

Search

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview. →

Date : Last 24 hours Show dates as : Local User contains a3a10b46-138c-452c-81d8-77d723a55040 Add filters

Date	User	Application	Status	IP address	Authentication requirem...
3/14/2024, 6:20:48 PM	La Corine	OfficeHome	Success	104.252.183.15	Multifactor authentication
3/14/2024, 6:20:45 PM	La Corine	OfficeHome	Interrupted	104.252.183.15	Multifactor authentication
3/14/2024, 6:19:28 PM	La Corine	OfficeHome	Failure	104.252.183.15	Multifactor authentication
3/14/2024, 5:58:54 PM	a3a10b46-138c-452c-81d8-7...	OfficeHome	Interrupted	188.127.227.138	Single-factor authentication
3/14/2024, 5:55:48 PM	a3a10b46-138c-452c-81d8-7...	OfficeHome	Failure	142.252.171.60	Single-factor authentication

SPUR

104.252.183.15

This IP is hosted in a datacenter.

104.252.183.15 DATACENTER

GREEN FLOID LLC AS204957

SPUR

142.252.171.60

This IP is hosted in a datacenter.

142.252.171.60 DATACENTER

GREEN FLOID LLC AS204957

Analyse des **tentatives de connexion** à partir des journaux d'Azure → adresse IP

# Investigation des kits de phishing AiTM



5

Scanned	Detections	File type	Name
2023-07-06	3 / 59	PHP	ott/sms.php
2023-07-05	2 / 58	PHP	ott/assets/bg.php
2023-07-05	2 / 58	PHP	ott/assets/c.php
2023-07-05	2 / 59	PHP	ott/assets/e.php
2023-07-05	2 / 57	PHP	ott/assets/f.php
2023-07-05	2 / 58	PHP	ott/assets/fi.php
2023-07-05	2 / 59	PHP	ott/assets/i.php
2023-07-09	2 / 58	PHP	ott/assets/k.php
2023-07-05	2 / 59	PHP	ott/assets/lg.php
2023-07-05	2 / 58	PHP	ott/assets/sc.php
2023-07-05	2 / 58	PHP	ott/assets/signop.php
2023-07-10	2 / 58	PHP	ott/login.php
2023-07-05	2 / 59	PHP	ott/phoneappnotif.php
2023-07-05	2 / 58	PHP	ott/phoneappotp.php
2023-07-05	2 / 58	PHP	ott/process.php
2023-07-05	2 / 58	PHP	ott/twoawayoff.php
2023-07-05	2 / 58	PHP	ott/twoawaysms.php
2023-07-05	2 / 58	PHP	ott/validate.php
2023-07-05	2 / 59	PHP	ott/verification.php
2023-07-05	1 / 58	PHP	ott/assets/jquery.php
2023-07-05	1 / 58	PHP	ott/assets/style3.php
2023-07-05	1 / 58	PHP	ott/list.php
2023-07-05	1 / 59	PHP	ott/p/index.php
2023-07-05	1 / 59	PHP	ott/p/logout.php

*/login.php : fake login page*

*/process.php : fonctions principales*

*/validate.php : Cloudflare Turnstile*

*/verification.php : challenges MFA*

*/p/index.php : construction des pages HTML*

En pivotant sur les fichiers :

- noms
- hashes
- contenu



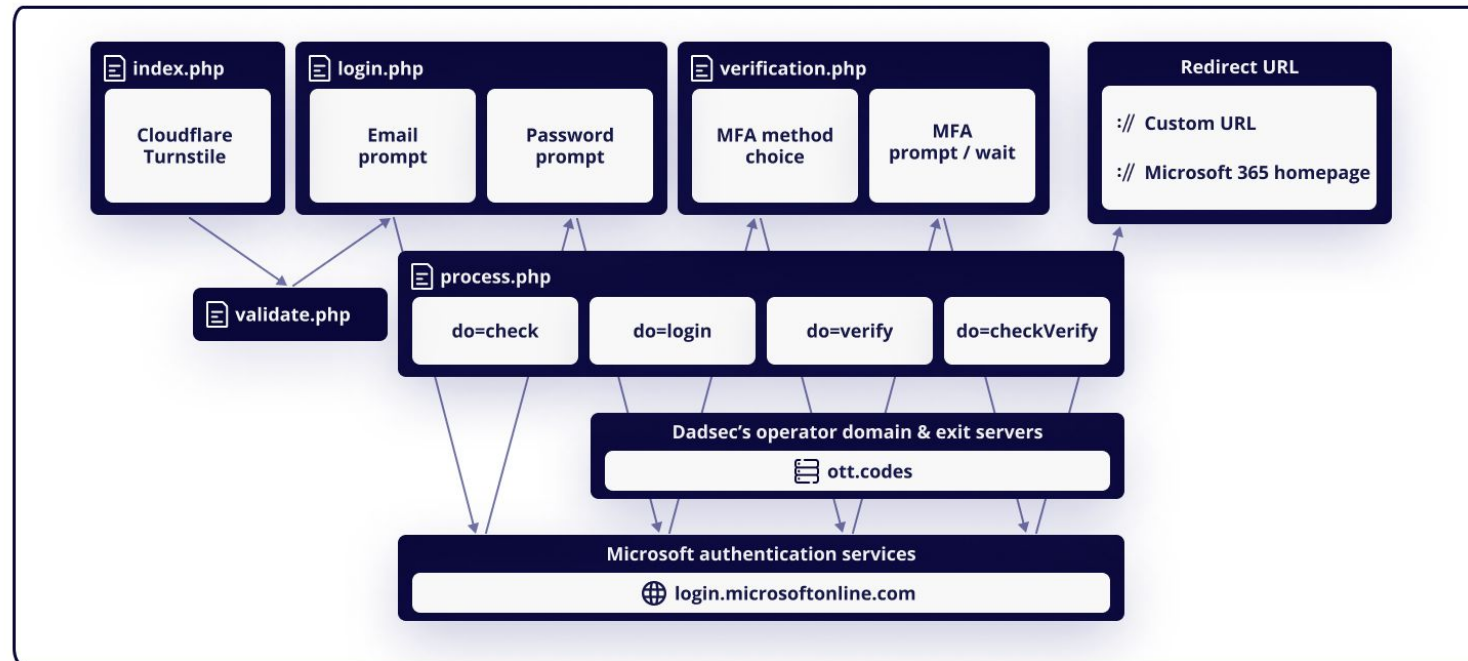
Code source (ZIP ou RAR)  
disponible sur VirusTotal

Recherche du **code source**, ayant potentiellement fuité sur **VirusTotal**

# Analyse des kits de phishing



## Code workflow of the *Dadsec OTT* AiTM phishing kit



# Suivi des infrastructures



## Heuristiques de recherche proactives, à partir

- De l'empreinte des serveurs
- Des certificats TLS
- De la réponse HTTP du serveur sur des chemins
- ...

→ Illumination des infrastructures à partir des services de scan (Shodan, Censys) et nos outils internes

The screenshot shows the Censys search interface. The search query is `services:(port:3000 and banner_hashes="sha256:577d61201b43f8bd52426b083d88a326f64a69492dd9361d9fc5c7d8f882d053")`. The results show 778 hosts. The left sidebar shows filters for Labels (remote-access, default-landing-page, database, file-sharing, email) and Autonomous System (ASGHOSTNET, DIGITALOCEAN-ASN, IS-AS-1, AKAMAI-LINODE-AP, Akamai Connected Cloud). The main list shows hosts with their IP addresses, operating systems, and services. A detailed view of a host (5.230.77.70) is shown on the right, displaying the response to a GET request via Socks to the path `http://5.230.77.70:3000/v404/static/stat.css`. The response includes headers like `Accept-Ranges: bytes`, `Cache-Control: public, max-age=0`, and `Content-Type: text/css; charset=UTF-8`. The body content shows CSS rules for background, font-family, color, and padding.

*exemple d'heuristique pour le PhaaS NakedPages*

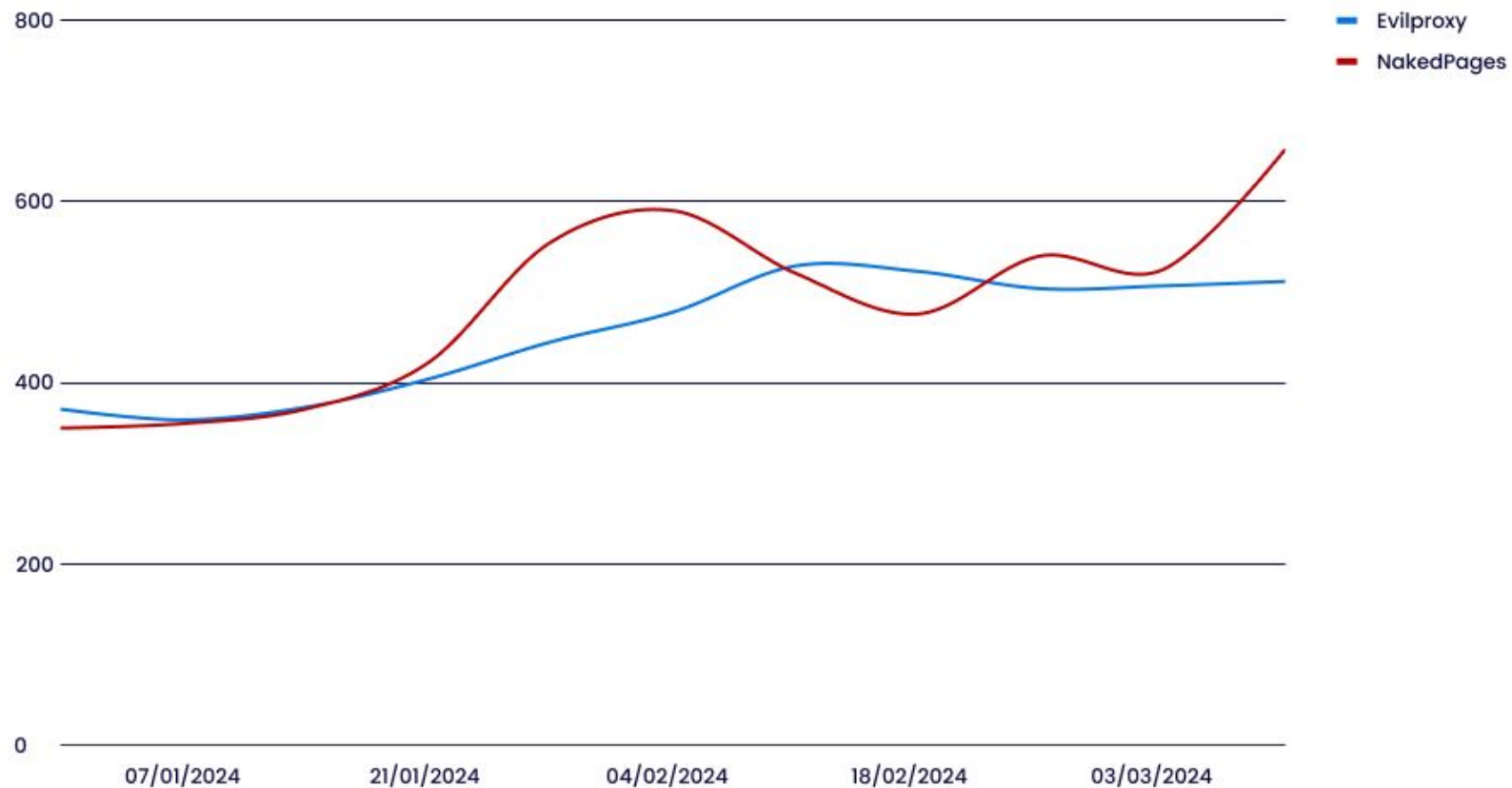
```
body {
  background: #f5f5dc;
  font-family: 'Courier New', Courier, monospace;
  color: #333;
  line-height: 1.6;
}

.container {
  margin: auto;
  color: red;
  width: 50%;
  padding: 20px;
}
```

# Suivi des infrastructures



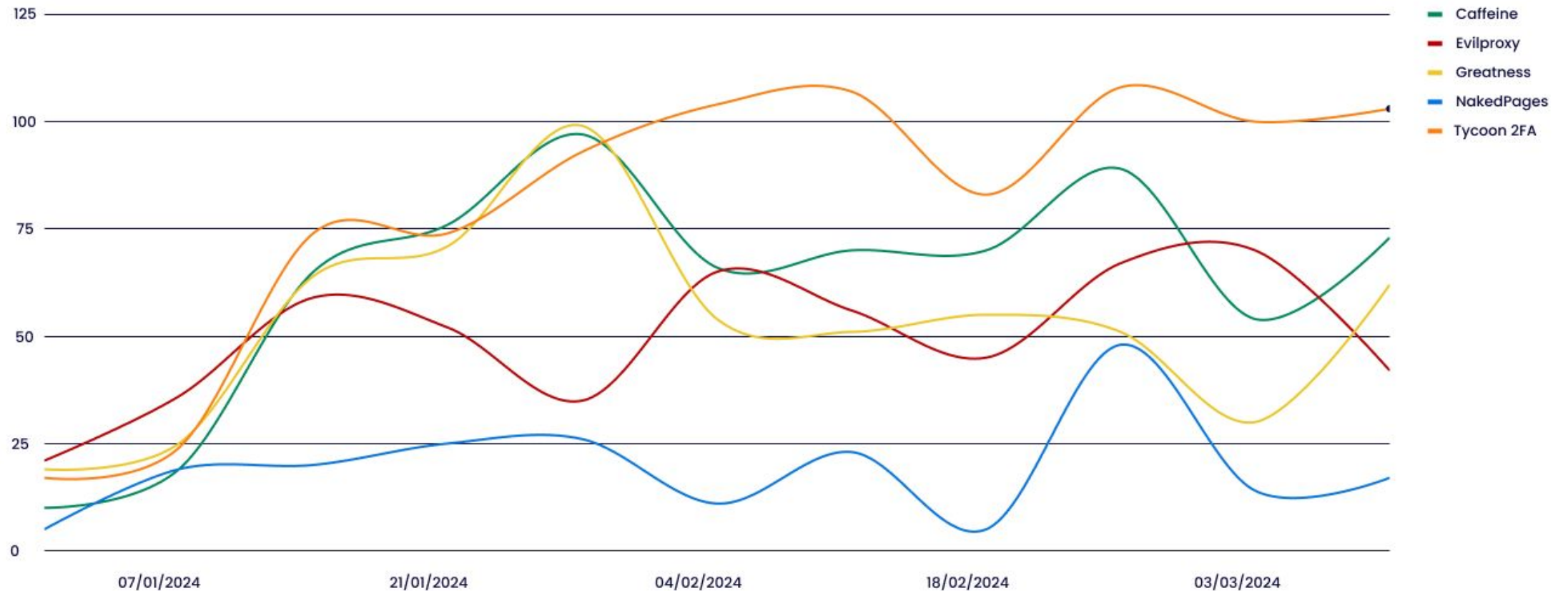
Nombre de serveurs C2 actifs pour Evilproxy et NakedPages en 2024 (heuristiques proactives)



# Suivi des infrastructures



Nombre de domaines de phishing détectés par semaine pour Caffeine, Evilproxy, Greatness, NakedPages et Tycoon 2FA (heuristiques urlscan.io)





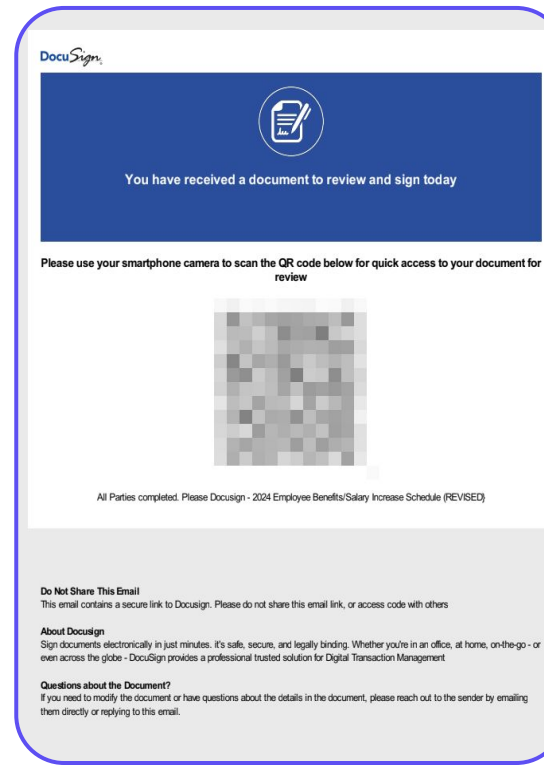
# Suivi des campagnes de phishing



Analyse automatique des QR codes par la sandbox VirusTotal Jujubox

→ Heuristique de recherche sur le comportement :

PDF > browser > Turnstile



PDF malveillant contenant un QR code



Page de phishing protégé par Cloudflare Turnstile

# Suivi des campagnes de phishing



behavior:"--start-maximized --single-argument" behavior_network:challenges.cloudflare.com type:pdf				
FILES - 20 / 2.7 K Pro +1.1 K results				
		Sort by	Filter by	Export
		Detections	Size	First seen
				Last seen
				Submitters
<input type="checkbox"/>	EAA836E50585C5FFB784FE727E682E4701696131167E077265EA4063398852 pdf DocuSign_PayoutStatement_USER robert.condon.pdf	Tycoon 2FA	24-03-22 3:38:58	1
<input type="checkbox"/>	2F7F78F0689A332DB802F533C2075C18FA1E206D77198FD5D384DCB07EE40195 pdf Salesforce Connector's Document.pdf	Greatness	24-03-22 4:55:21	1
<input type="checkbox"/>	01462074983D11789BC49FAE29187F627F541E61F22AEAF0C13E46848C08F58D pdf Employee benefit for celso.marcandali.pdf	(offline)	24-03-21 3:08:06	1
<input type="checkbox"/>	C209D61E1E98BF30A10E8DB39225DD43F4F1E39E2CAD31997D43F82622905CFA pdf Ksgroup_HLZ3RAKL98541.pdf	NakedPages	24-03-21 2:21:42	1
<input type="checkbox"/>	DB2287118034C293A290F843C97D9C96993ECD6350E88BD0568F05686827531 pdf DocuSign Benefit and Payroll for agreeer.pdf	NakedPages	24-03-21 2:08:15	1
<input type="checkbox"/>	9B6462822BF23291DC0CC0039582F38D06DF0889C3488F5007936DEBABB3D9 pdf Benefits Policy Update for nick.goodman.pdf	NakedPages	24-03-21 1:54:38	1
<input type="checkbox"/>	4B032EA968FED968A13FAAC359DC1D52AB2F6D045D0837910079A802D7FEC pdf DocuSign_PayoutStatement_USER ccaiazzo.pdf	Tycoon 2FA	24-03-21 1:10:54	1
<input type="checkbox"/>	BBA56C073BFFD8EC9DF3B647D48F19321D2119928A6D5FF3608460507D75A8F pdf Benefits Policy Update for kristywheel.pdf	NakedPages	24-03-21 9:19:01	1
<input type="checkbox"/>	0064732778963E581BE4400F2E58DD2DAB4D4C0A7C9FC868EC5F2E68203472CE pdf Benefits Policy Update for smatthews.pdf	NakedPages	24-03-21 9:09:43	1
<input type="checkbox"/>	61638146A5D2C060989E48249F8AB1888316F902468683FAA7CCBCBCA763E pdf ATT0001-5.pdf	Greatness	24-03-21 8:51:26	1
<input type="checkbox"/>	C1A89CABF49FC8F214CDD9D30A155F5008180A14C8303E62EA56242C4A1990FF pdf Thu 21st March-plans.pdf	Greatness	24-03-21 8:40:53	1
<input type="checkbox"/>	6A86BFAFADC1771820A9104159221C04E148538C7D82F8BB8A421A19365AEAF1 pdf Final Distribution.pdf	NakedPages	24-03-21 8:18:43	1
<input type="checkbox"/>	326FF9A410D99F9B9F39851B984E1F746F02AF581A1DE5AF5AC9157316D3672C pdf Employee Benefits Plan for Ntash (1).pdf	Caffeine	24-03-21 6:43:14	1

type:pdf

behavior:"--start-maximized --single-argument"  
behavior\_network:challenges.cloudflare.com



+ de 2700 résultats  
sur 3 mois

Découverte du PhaaS  
"Tycoon 2FA"



# De la détection à la remédiation



# Stratégies de détection



- Indicateurs : tracking (pro)actif des domaines, adresses IP...
- Détections spécifiques à chaque kit (structure d'URL, HTML...)
- **Journaux d'authentification**
- **Ressource canari** dans la page de connexion
- **Journaux de proxy HTTP** ou de navigation web
- Actions courantes post-compromission

# Journaux d'activités liés à l'authentification



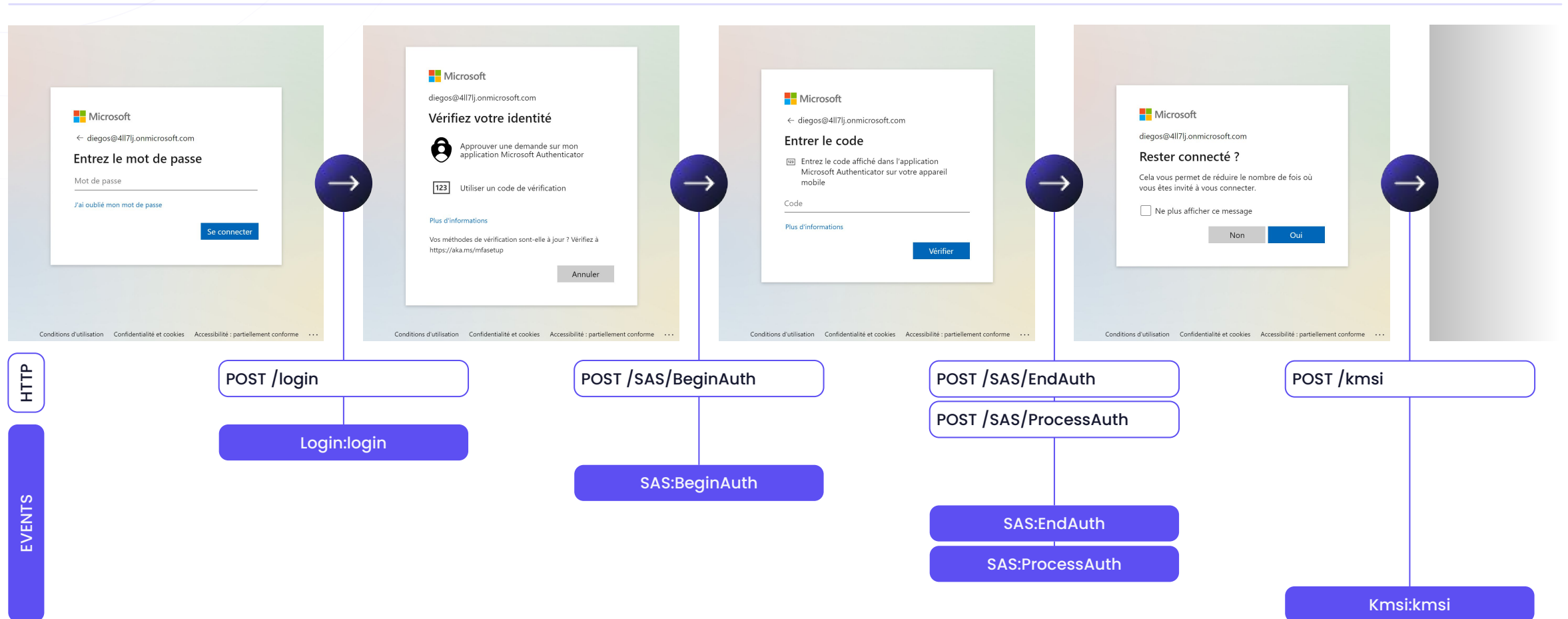
	Journaux d'activité <b>Entra ID</b> SignInLogs	Journal d'audit <b>Microsoft 365</b> UserLoggedIn / UserLoginFailed
détails de contexte	enrichis	minimaux
étapes de l'authentification	non	oui
ID de session	non	oui
collecte SIEM	historiquement plus complexe	plus simple

ID de pivot

properties.id  
properties.originalRequestId

Id  
IntraSystemId

# Journaux d'activités liés à l'authentification



# Opportunités de détection




RequestType	UserAgent	InterSystemsId
Login:login	Chrome/78.0.3904.108	e8c36924-4998-4180-9bbf-2cea5660f7f0
Cmsi:Cmsi		e8c36924-4998-4180-9bbf-2cea5660f7f0
SAS:BeginAuth	Chrome/105.0.0.0	e8c36924-4998-4180-9bbf-2cea5660f7f0
SAS:EndAuth	Chrome/105.0.0.0	e8c36924-4998-4180-9bbf-2cea5660f7f0
SAS:ProcessAuth		e8c36924-4998-4180-9bbf-2cea5660f7f0
Kmsi:kmsi	Chrome/78.0.3904.108	e8c36924-4998-4180-9bbf-2cea5660f7f0

## Anomalie de **User-Agent**


- absent
- variations au sein d'une même authentification
- ancien

*exemple d'authentification via Caffeine*

# Opportunités de détection



AS399629 – BL Networks



Country	 United States ⓘ
Website	<a href="https://blnwx.com">blnwx.com</a>
Hosted domains	12,619
Number of IPv4	12,288
Number of IPv6	0
ASN type	Hosting



RequestType	ClientIP	ASN (enrichissement)	Pays (enrich.)	InterSystemsId
Login:login	109.121.41.176	AS215622 - MECRA BILISIM	Serbie	b3b092e0-ed9-...
SAS:BeginAuth	64.52.80.237	AS399629 - BL Networks	États-Unis	b3b092e0-ed9-...
SAS:EndAuth	64.52.80.237	AS399629 - BL Networks	États-Unis	b3b092e0-ed9-...
SAS:ProcessAuth	38.45.71.91	AS174 - Cogent Communications	États-Unis	b3b092e0-ed9-...

## Anomalies d'adresse IP

- datacenter (*blacklist*)
- variations au sein d'une même authentification
- pays ou AS inhabituel (*whitelist*)
- proxy résidentiel (*threat intel*)



38.45.71.91

This IP is contributing bandwidth to  
PACKETSTREAM\_PROXY. Anonymized traffic is  
mixed with legitimate traffic from this network.

# | Opportunités de détection



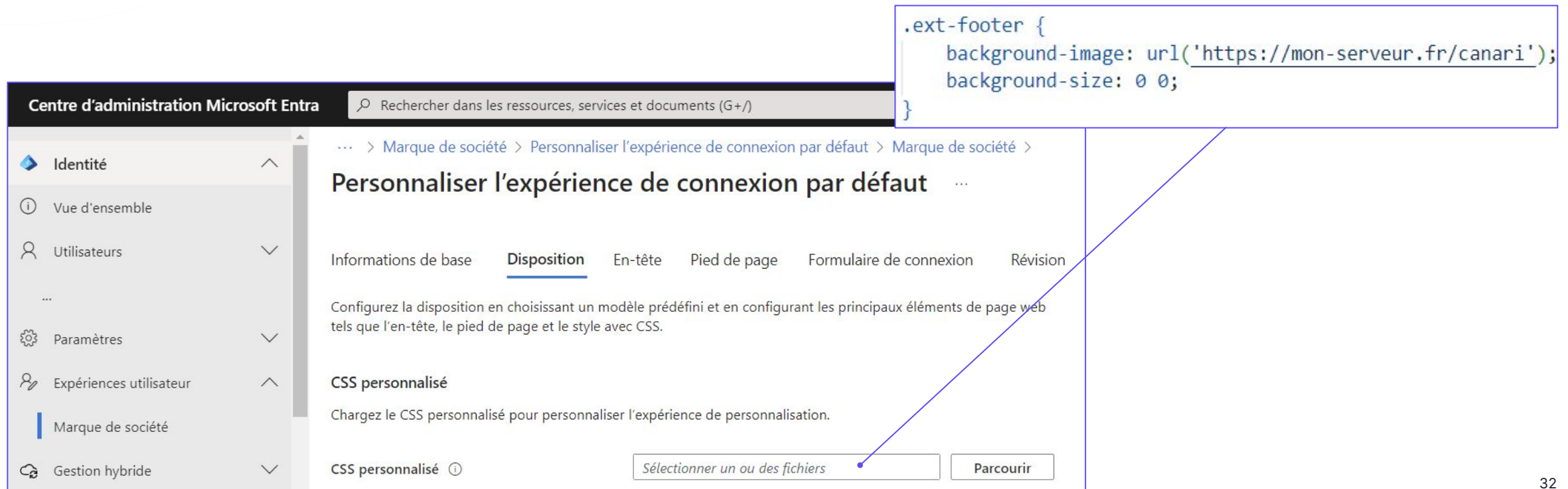
Signal faible : **ID d'application cliente**

ApplicationId	Nom	Kits
4765445b-32c6-49b0-83e6-1d93765276ca	OfficeHome	EvilProxy, Caffeine, Tycoon, ...
00000002-0000-0ff1-ce00-000000000000	Office 365 Exchange Online	NakedPages
72782ba9-4490-4f03-8d82-562370ea3566	Office 365	Dadsec

# Opportunités de détection



## URL canari via CSS personnalisé (HTTP Referer)



The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains the navigation menu with 'Identité' selected. The main content area is titled 'Personnaliser l'expérience de connexion par défaut' and has tabs for 'Informations de base', 'Disposition', 'En-tête', 'Pied de page', 'Formulaire de connexion', and 'Révision'. The 'Disposition' tab is active, showing instructions to configure the layout by choosing a predefined model and configuring web page elements like the header, footer, and CSS. Below this, there is a section for 'CSS personnalisé' with a description and a button to 'Sélectionner un ou des fichiers'. A callout box points to this button, displaying the following CSS code:

```
.ext-footer {  
    background-image: url('https://mon-serveur.fr/canari');  
    background-size: 0 0;  
}
```



# Opportunités de détection



## Journaux de proxy HTTP ou de navigation web

`https://login.microsoftonline.com/common/SAS/BeginAuth` **légitime**

12:37:35.000	GET	https://login.cliquez-sur-ouvrir.info/organizations/oauth2/v2.0/authorize?client_id=476544
12:37:40.000	POST	https://login.cliquez-sur-ouvrir.info/common/GetCredentialType?mkt=fr
12:37:41.000	POST	https://login.cliquez-sur-ouvrir.info/common/instrumentation/dssostatus
12:37:50.000	POST	https://login.cliquez-sur-ouvrir.info/common/login
12:37:55.000	POST	https://login.cliquez-sur-ouvrir.info/common/SAS/BeginAuth <b>proxy</b>
12:38:09.000	POST	https://login.cliquez-sur-ouvrir.info/common/SAS/EndAuth
12:38:09.000	POST	https://login.cliquez-sur-ouvrir.info/common/SAS/ProcessAuth
12:38:12.000	POST	https://login.cliquez-sur-ouvrir.info/kmsi

# | Investigation d'une compromission



## **Session ID** (journaux Microsoft 365)

- AzureActiveDirectory, Exchange : `DeviceProperties.SessionId`
- SharePoint, OneDrive : `AppAccessContext.AADSessionId`

# Investigation d'une compromission

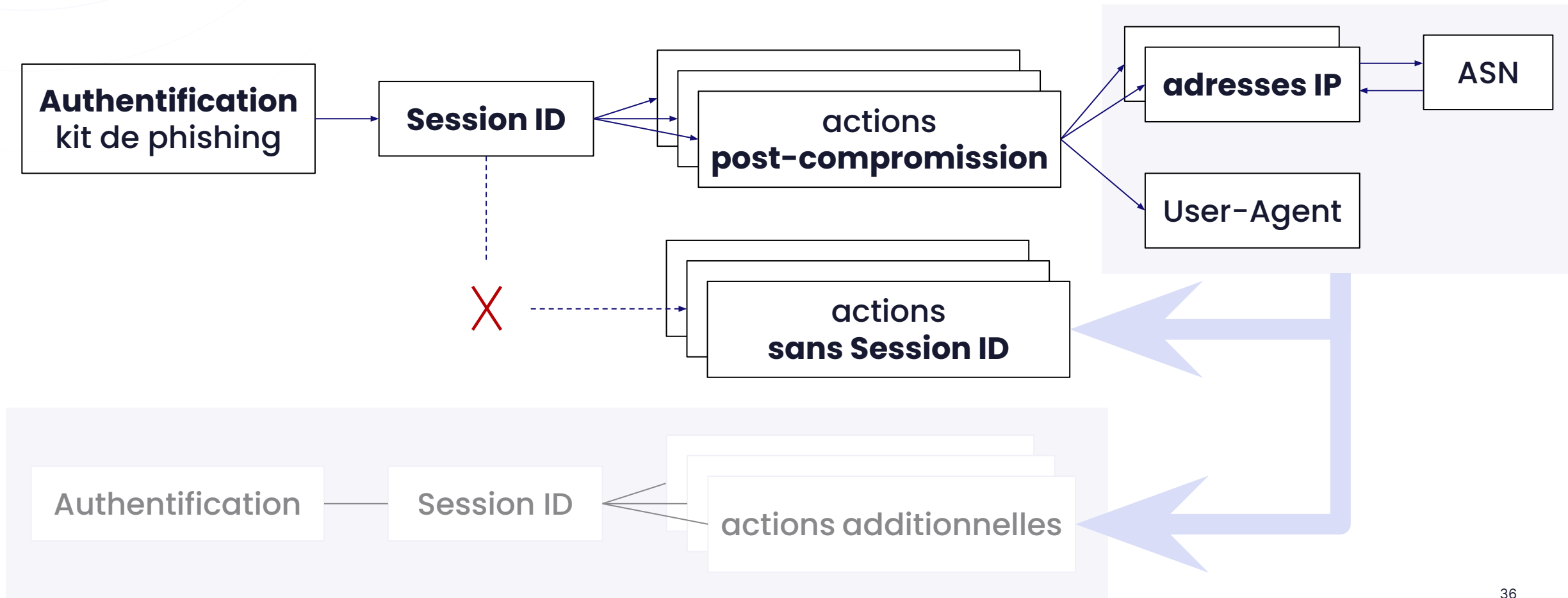


## Session ID (journaux Microsoft 365)

- AzureActiveDirectory, Exchange : `DeviceProperties.SessionId`
- SharePoint, OneDrive : `AppAccessContext.AADSessionId`

CreationTime	Workload	Operation	RequestType	Session ID	UserAgent	ClientIP
Vendredi 16:08	AzureActiveDirectory	UserLoggedIn	Login:login	849aaae2-fbf1-4b7a-a37d...	Windows Chrome/115	38.45.71.91
...						
Lundi 13:55	AzureActiveDirectory	UserLoggedIn	Login:reprocess	849aaae2-fbf1-4b7a-a37d...	macOS Chrome/122	91.196.69.67
...						
Lundi 13:56	OneDrive	FileAccessed		849aaae2-fbf1-4b7a-a37d...		91.196.69.67
...						
Lundi 14:07	Exchange	Update				91.196.69.67

# Investigation d'une compromission



# Remédiation et prévention



## Remédiation

- **révoquer les sessions** et changer le mot de passe
- inspecter les **méthodes de MFA**

## Prévention

- **MFA résistante au phishing** (clé de sécurité FIDO2, certificat...)
- Accès conditionnel : **exiger appareil inscrit** auprès de Entra ID

# Merci !



*[blog.sekoia.io](https://blog.sekoia.io)*



**Grégoire CLERMONT**

*CTI & Detection Analyst*

[gregoire.clermont@sekoia.io](mailto:gregoire.clermont@sekoia.io)



**Quentin BOURGUE**

*Lead Cybercrime Analyst*

[quentin.bourgue@sekoia.io](mailto:quentin.bourgue@sekoia.io)