Cozy Bear et Wicked Panda

Introduction aux vecteurs d'attaque des animaux fantastiques

GUIDE
Baptiste Audidier

Nomenclature

Rappels de cours:

- **APT**: Menace Persistante avancée
- **Zero Day**: vulnérabilité non corrigée
- **Exploit**: script exploitant une vulnerabilité
- **MITRE ATT&CK:** Inventaire des tactiques et techniques des cyberattaquants
- **OPSEC**: Sécurité de l'opération
- **OSINT**: Sources d'information Open Source

Wicked Panda

Énumération de domaines

python sublist3r.py -d domain.fr

MITRE ATT&CK T1595.003

GITHUB Sublist3r

• Scan actif de vulnérabilités

python jexboss.py -host http://server.fr

MITRE ATT&CK T1595.002

GITHUB JexBoss

Nmap

OneForAll

Scan passif de technologies

domain:domain.fr product:gitlab

MITRE ATT&CK T1596.005

Shodan

Exploitation d'applications publiques

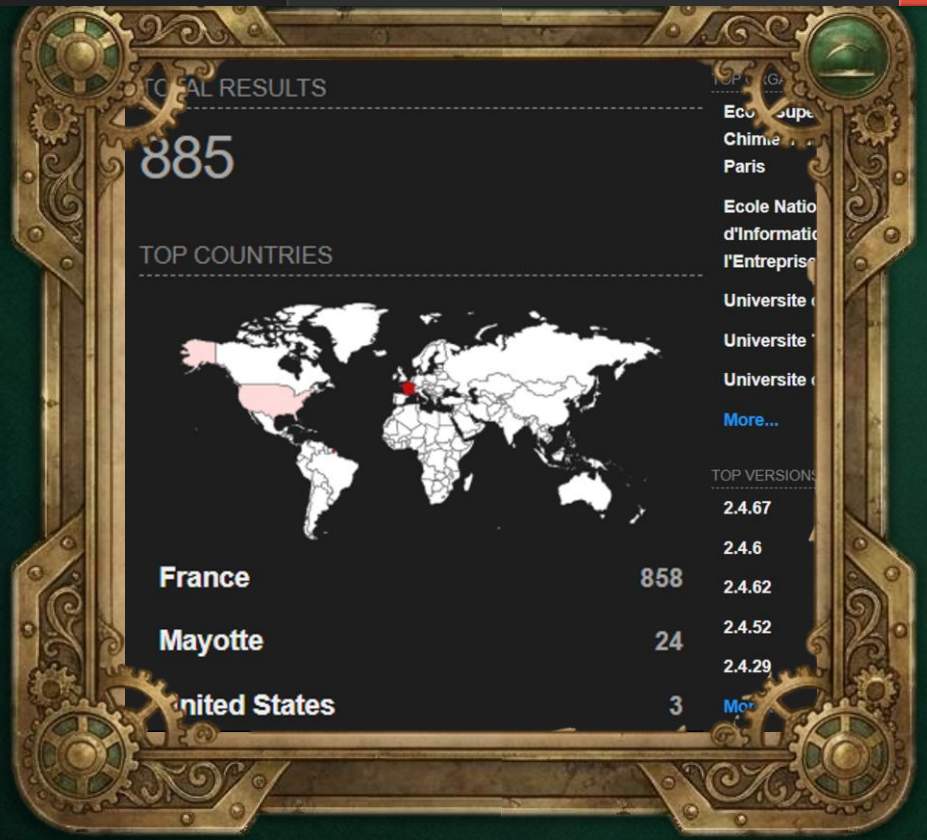
sqlmap -u http://target.fr?id=1 -p "id"

MITRE ATT&CK T1190

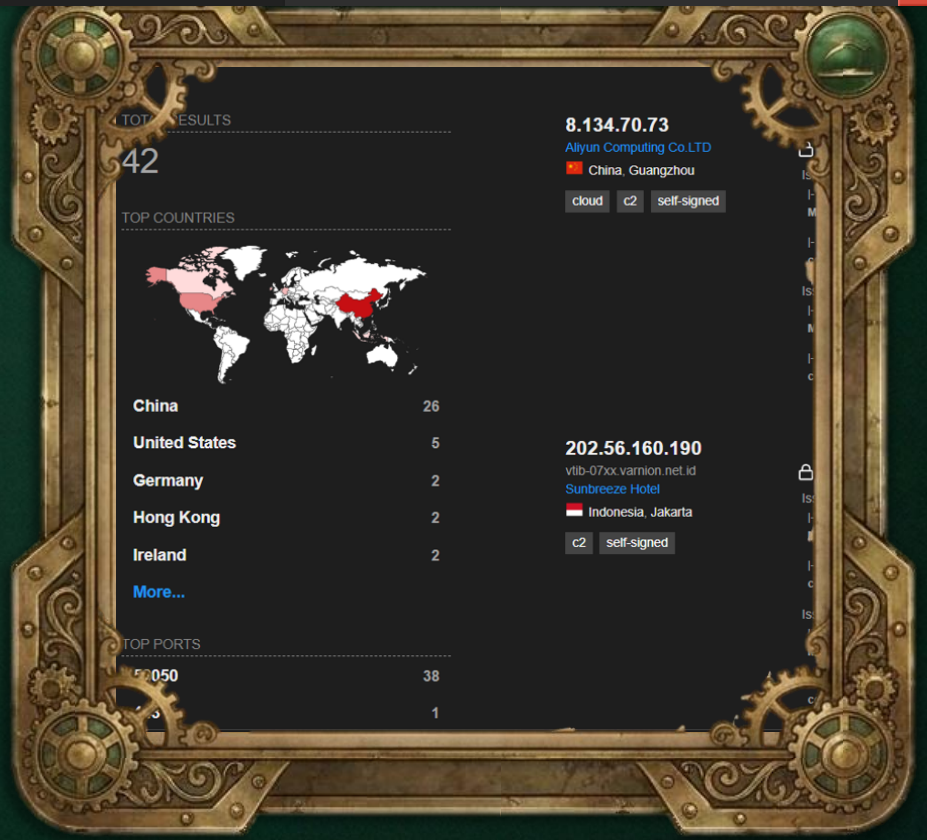
GITHUB SQLMap

Shodan

SHODAN net:193.54.0.0/15 product:Apache



SHODAN ssl.cert.issuer.cn:"Major Cobalt Strike"



OSINT 100% passive

Lister les URLs indexées par des crawlers comme archive.org

Waybackurls

```
waybackurls domain.fr |
sort -u | tee
waybackurls.txt
```

Gau

```
gau --subs domain.fr |
sort -u | tee gau.txt
```

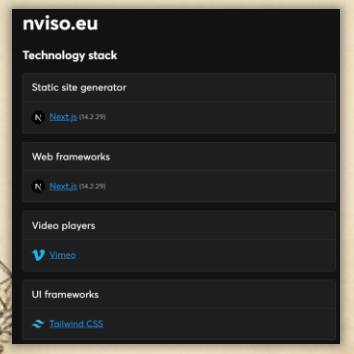
Chercher par mots-clefs les urls intéressantes

```
cat waybackurls.txt
gau.txt 2>/dev/null \
  | sort -u \
  | rg -i
'(oauth|openid|oidc|au
thorize|token|login|log
out|signin|callback|red
irect|postlogout|msal|a
dal)' \
  | tee
auth_related_urls.txt
```

Visualiser les urls

URLScan

Noter les technologies et versions



Wappalyzer

CVE-2026-50751

Découverte et observation

CVSS Meta Temp Score
8.3
Current Exploit Price (≈)
$1k-$2k
CTI Interest Score
0.00

EPSS Score: 0.41152
EPSS Percentile: 0.98486

VulDB

Scan Shodan

Shodan

net:"193.54.0.0/15" product:"Check Point"

TOTAL RESULTS
10

TOP PORTS

18264	4
264	3
443	3

TOP ORGANIZATIONS

Universite Numerique Ile-de-France	5
Renater	3
MJENR-DATACENTERS	1
Universite Claude Bernard - Lyon 1	1

Détection & Exploitation

```
$ python3 watchTowr-vs-Check-Point-CVE-2026-50751.py -rh vpn.example

watchTowr-vs-Check-Point-CVE-2026-50751.py

(*) Check Point IKEv1 Remote-Access VPN certificate-auth by

- McCaulay (@_mccaulay) of watchTowr (@watchTowrcyber)

CVEs: [CVE-2026-50751]

[#] CVE-2026-50751 Check Point IKEv1 Remote-Access certificate-auth
[+] Self-signed cert (untrusted); signature will be invalid (no priv
[#] Connecting via udp ...
[#] Authenticating as 'watchtowr' with the forged certificate + inva
[#] Decrypting...
[+] Gateway Internal IP: 172.31.255.128
[+] [BYPASSED] Gateway authenticated us as "watchtowr". CVE-2026-507
```

GITHUB watchtowr labs

ExploitDB

Known Exploited Vulnerability

CISA KEV

CHECK POINT | SECURITY GATEWAY

CVE-2026-50751

Check Point Security Gateway Improper Authentication Vul
authentication vulnerability in IKEv1 key exchange that could a
authentication and establish a remote access VPN connection

Related CWE: CWE-287

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Additional Notes +

Cozy Bear

- Authentifiants volés

```
h8mail -t
target@example.com
```

MITRE ATT&CK T1078.004 · Dehashed · H8mail · Have I been Pwnd

Vol de jetons

```
trufflehog git https://github.com/cnrs/repo
```

MITRE ATT&CK T1566.001 · GITHUB Trufflehog · BadSecrets

Scan passif de certificats

```
https://crt.sh/?q=dom
ain.fr
```

MITRE ATT&CK T1596.003 · Security Trails · Virus Total

Profilage

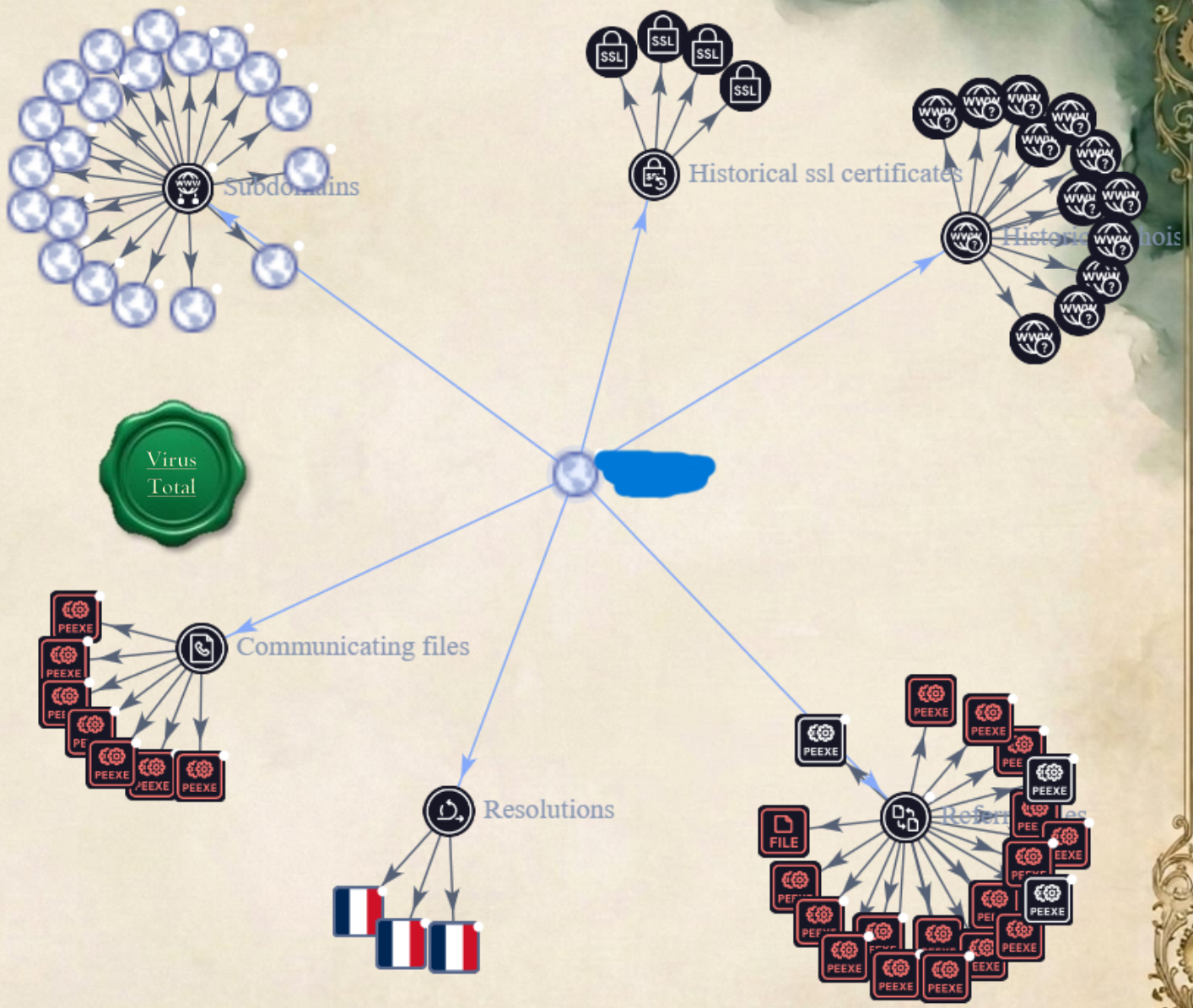
```
ghunt email
private.email@gmail.com
```

MITRE ATT&CK T1589 · Hunter.io

VirusTotal

```
root@kali:~#
```

- Sous-domaines
- Certificats SSL
- Fichiers référençant le domaine
- Fichiers communicants avec le domaine

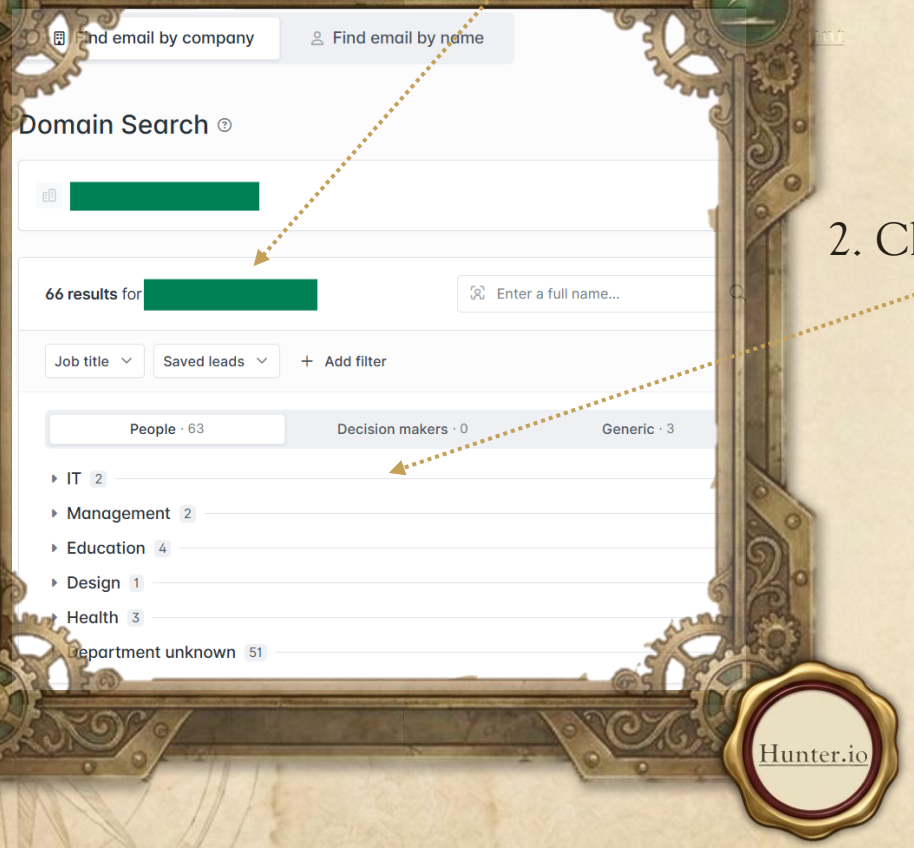


Profiling & Leaks

1. Lister les emails

```
┌──(alchemist㉿kali)-[~]
└─$ ghunt email
private.email@gmail.com
```

GHunt



Hunter.io

2. Choisir une cible

3. Se renseigner

...ent.com/
...K_

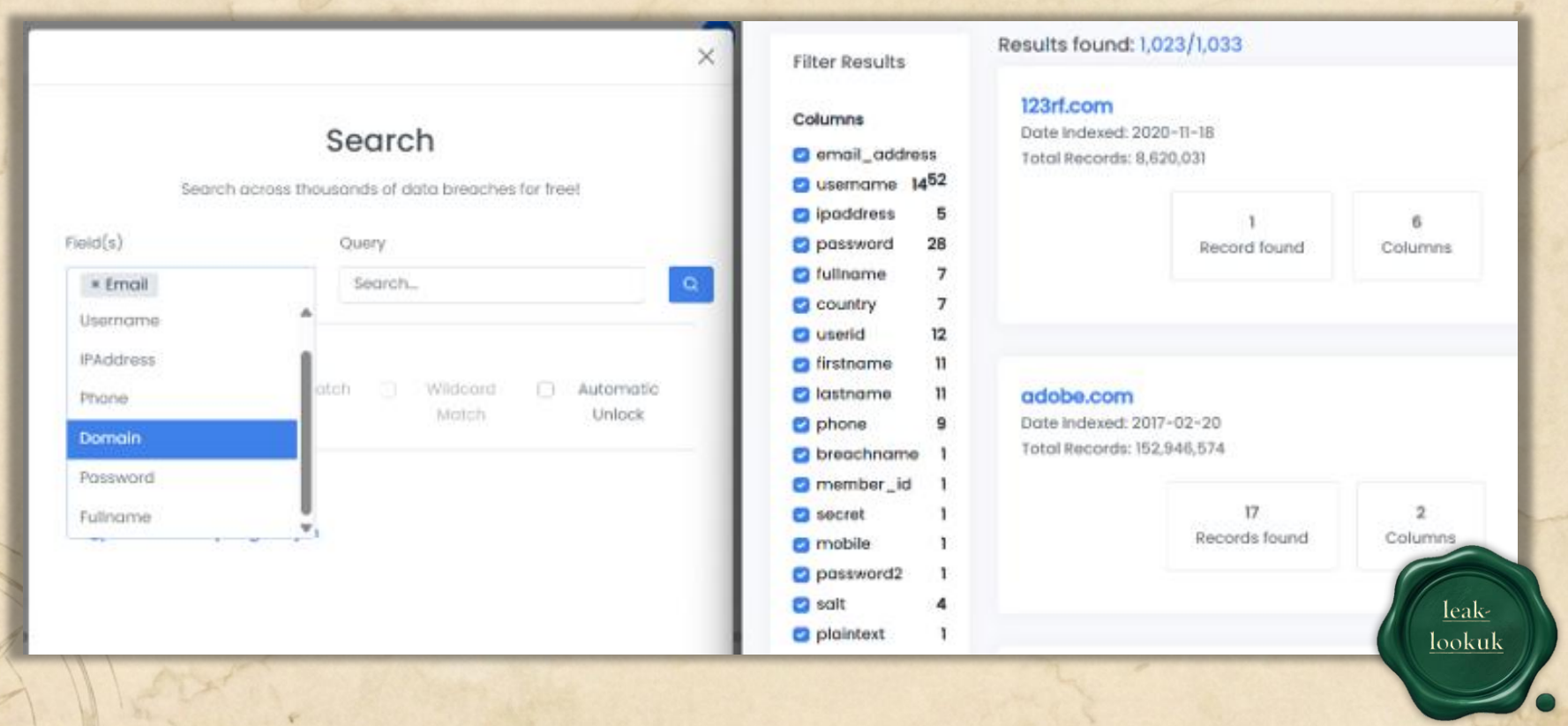
Last profile edit : 2026/06/01 22:23:14 (UTC)

[+] Activated Google services :
- Youtube
- Photos
- Maps
- Meet

Profile page : https://www.google.com/maps/contrib/113165654383606939471/reviews

[Statistics]
Reviews : 4
Photos : 47
Answers : 102
Places added : 1
Facts checked : 2

Profiling & Leaks



Sous-domaines intéressants

- test2fa.domaine.fr
- ftp.domaine.fr
- sshserv.domaine.fr
- mysql-db.domaine.fr
- listes.domaine.fr
- smtp.domaine.fr

OSINT Azure

- Tenant ID
- Utilisation de jetons JWT
- Jetons signés avec un algorithme solide
- Kerberos

MITRE ATT&CK T1592.004

https://login.microsoftonline.com/domain.fr/v2.0/.well-known/openid-configuration

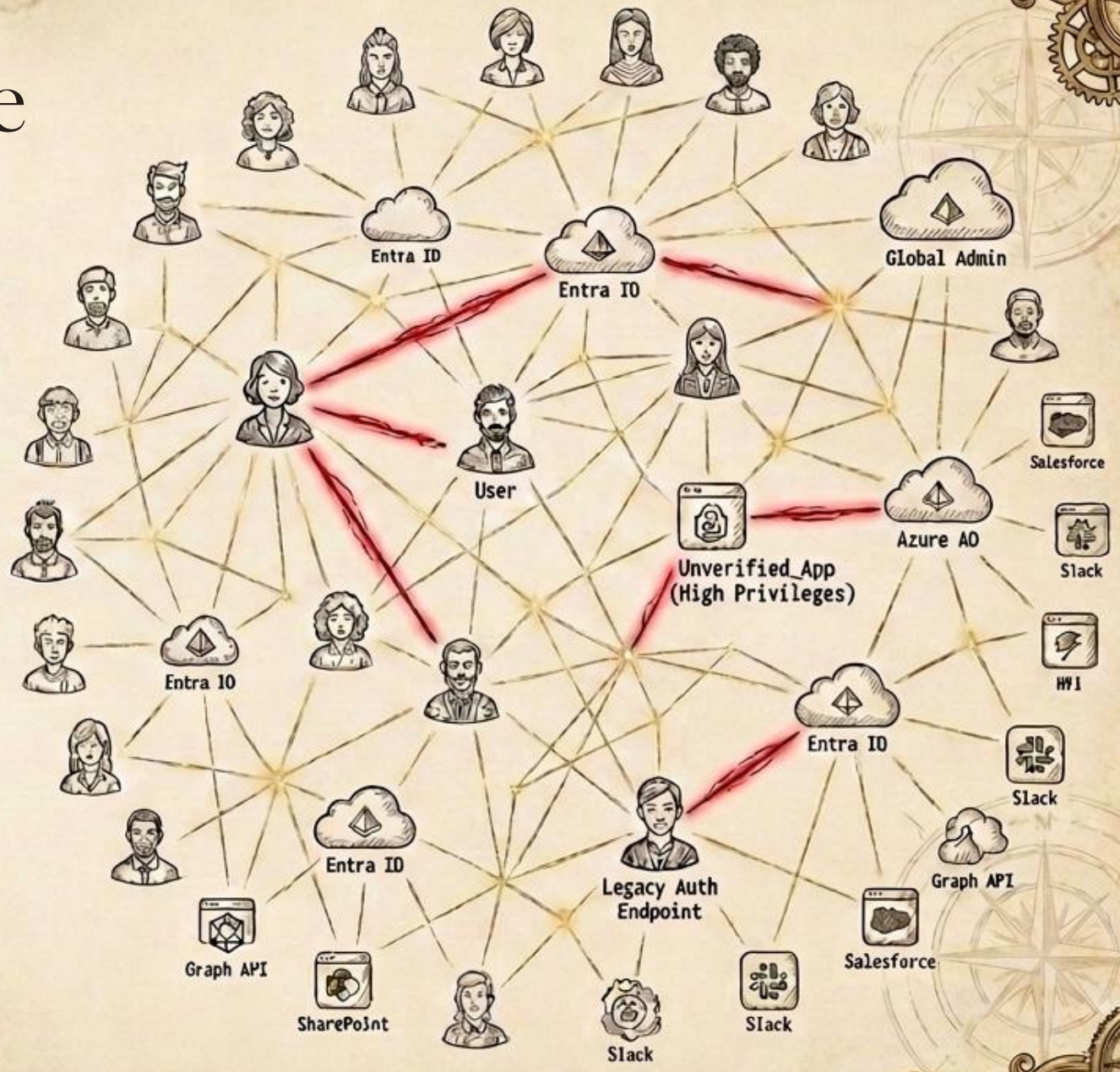
Azure accrobranche

Point d'entré

- Password spraying
- Comptes de test sans MFA
- Proxy résidentiel

Persistance

- Anciennes applications de test
- Permission "Mail.ReadWrite"
- Ajout de certificats



BBot

BBOT MODULES LIST

ajaxpro	aspnet_bin_exposure	baddns	baddns_direct	baddns_zone	badsecrets	bucket_amazon
bucket_digitalocean	bucket_firebase	bucket_google	bucket_google	bucket_microsoft	bypass403	bypass403
dnsbrute	dnsbrute_mutations	dnscommonsrv	ffuf	ffuf_shortnames	dotnetnuke	ffuf
ffuf	filedownload	fingerprintx	gitlab_com	gitlab_com	gitlab_com	gitlab_onprem
gitlab_com	gitlab_onprem	gowitness	hunt	hunt	httpx	hunt
legba	iis_shortnames	lightfuzz	ntlm	ntlm	newsletters	ntlm
nuclei	oauth	oauth	paramminer_cookies	paramminer_headers	paramminer_headers	portscan
reflected_parameters	retirejs	robots	sslcert	sslcert	sslcert	url_manipulation
telerik	anubisdb	anubisdb	wafw00f	wafw00f	wafw00f	wpscan
affiliates	apkpure	asn	bufferoverrun	bufferoverrun	bufferoverrun	builtwith
c99	censys_dns	censys_ip	code_repository	code_repository	code_repository	credshed
crt	crt_db	dehashed	dnscaa	dnscaa	dnscaa	fullhunt
dnsdumpster	dnstllsrpt	docker_pull	extractous	extractous	extractous	fullhunt
git_clone	gitdumper	github_codesearch	hackertarget	hackertarget	hackertarget	hunterio
ip2location	ipneighbor	ipstack	myssl	myssl	myssl	otx
pgp pgp	portfilte	postman	shodan_idb	shodan_idb	shodan_idb	skymem
social	subdomain	dar	urlscan	urlscan	viewdns	wayback
asset_inventory	csv	emails	http	http	mysql	neo4j
nmap_xml	pminej	python	slack	slack	splunk	sqlite
stdout	subdomain	txt	web_parameters	web_parameters	web_report	websocket
cloudcheck	dnsresolve	aggregate	aggregate	excavate	speculate	unarchive

Questions

(si il reste le temps)