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

OneFor All

Exploitation d'applications publiques

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

MITRE ATT&CK T1190

GITHUB SQLMap

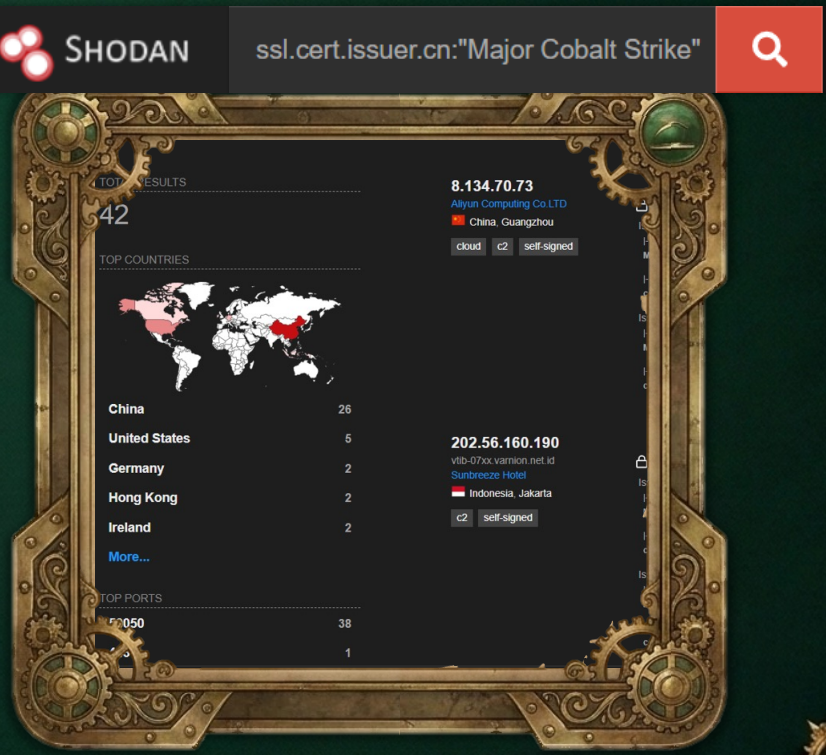
Scan passif de technologies

domain:domain.fr product:gitlab

MITRE ATT&CK T1596.005

Shodan

Shodan scanne tout le monde



OSINT 100% passive

Lister les URLs indexées par des crawlers comme archive.org

Waybackurls

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

Gau

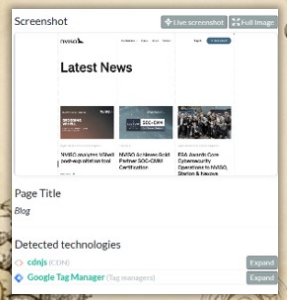
```
gau --subs domain.fr |
sort -u | tee gau.txt
```

Chercher par mots-clefs les urls intéressantes

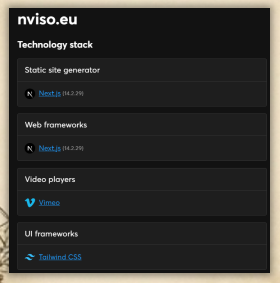
```
cat waybackurls.txt
gau.txt 2>/dev/null \
  | sort -u \
  | rg -i
'(oauth|openid|oidc|au
thorize|token|login|log
out|signin|callback|red
irect|postlogout|msal|a
dal)' \
  | tee
auth_related_urls.txt
```

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

Shodan

Scan Shodan

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

TOTAL RESULTS
10

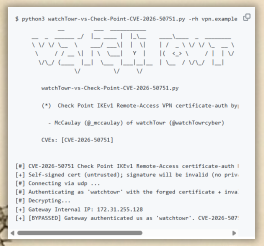
TOP PORTS

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



GITHUB watchtowr labs

ExploitDB

CISA KEV

Known Exploited Vulnerability

CHECK POINT | SECURITY GATEWAY

CVE-2026-50751

Check Point Security Gateway Improper Authentication Vul
authentication vulnerability in IKEv1 key exchange that could 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

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=domain.fr

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

Profilage

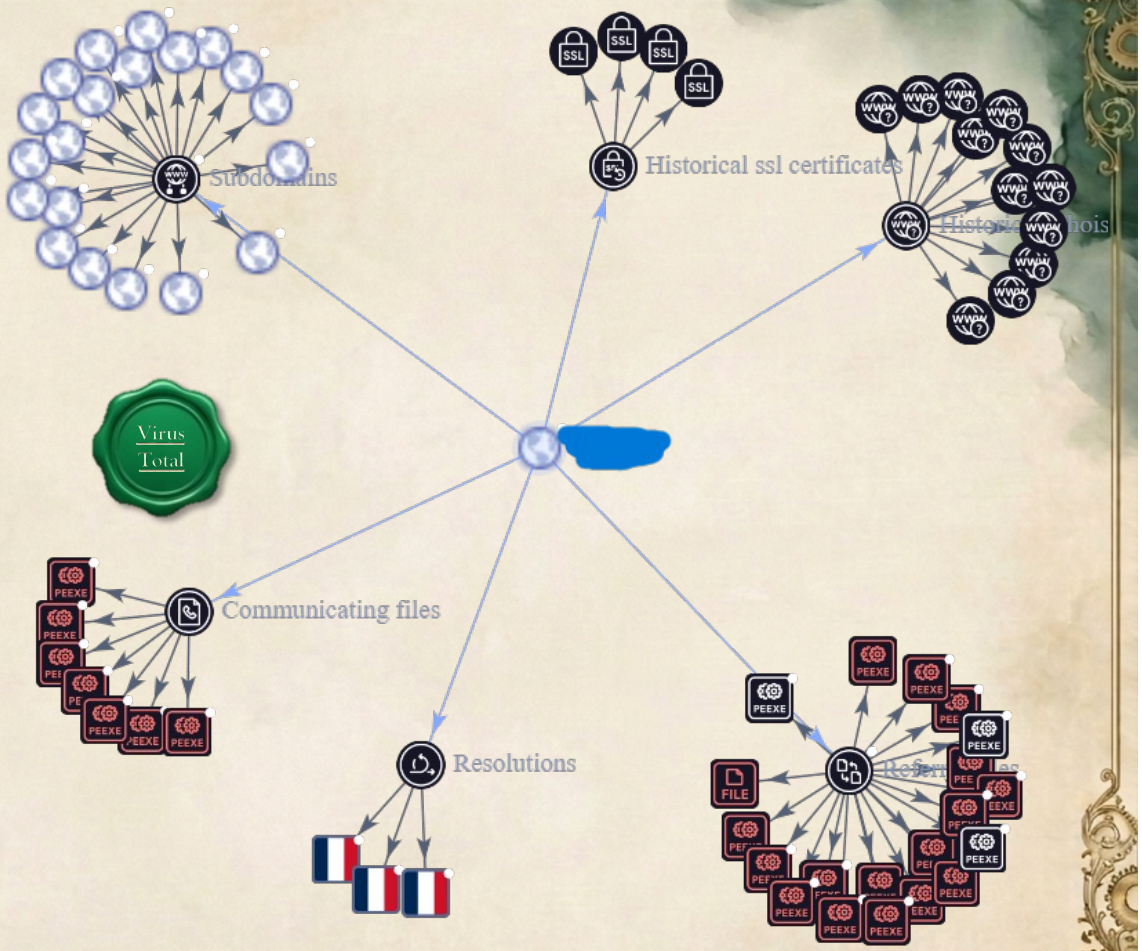
ghunt email private.email@gmail.com

MITRE ATT&CK T1589 · Hunter.io

VirusTotal

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

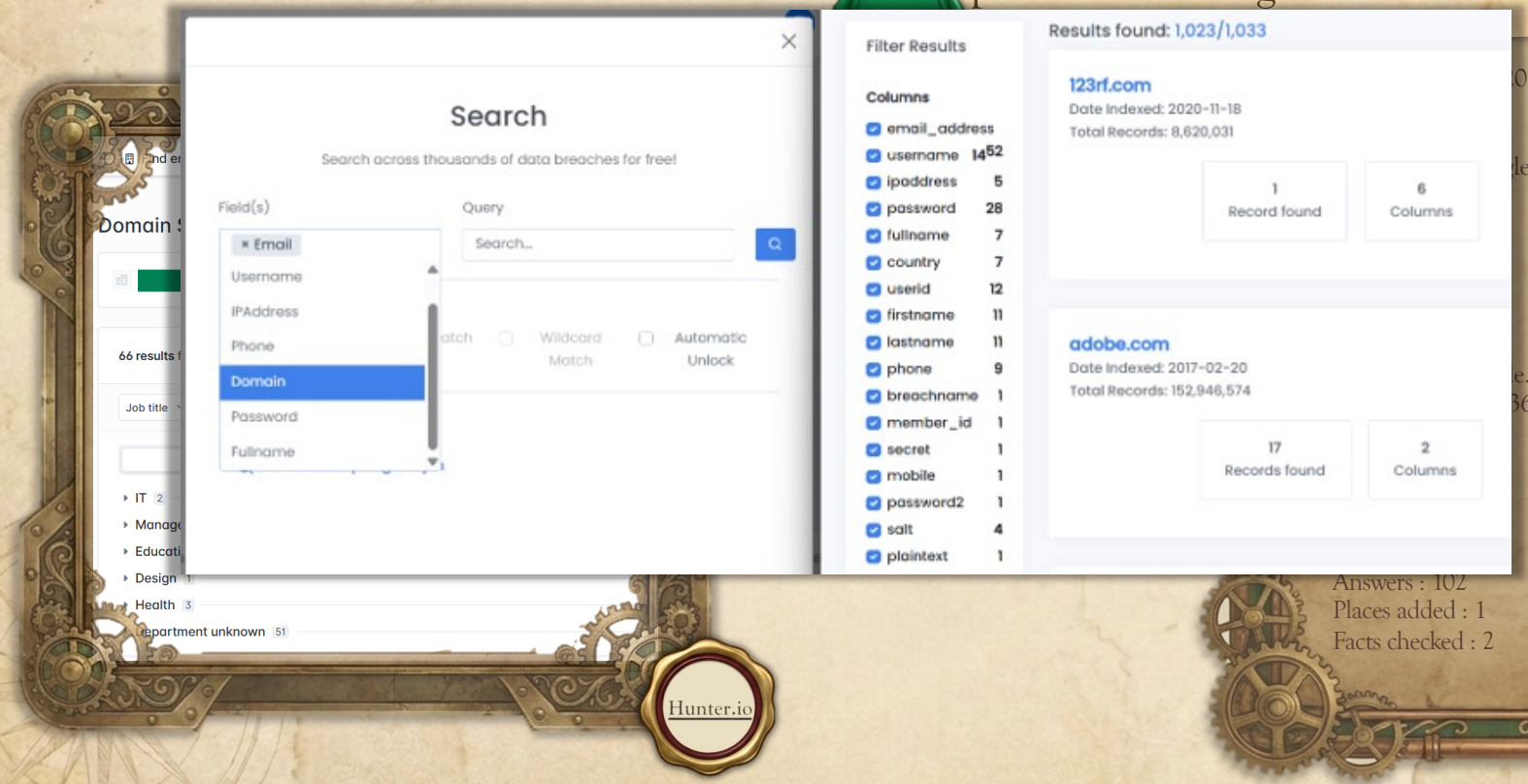
- Sous-domaines
- Certificats SSL
- Fichiers référençant le domaine
- Fichiers communicants avec le domaine



Profiling & Leaks

1. Lister les emails

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



Answers : 102
Places added : 1
Facts checked : 2

Sous-domaines intéressants

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

OSINT Azure

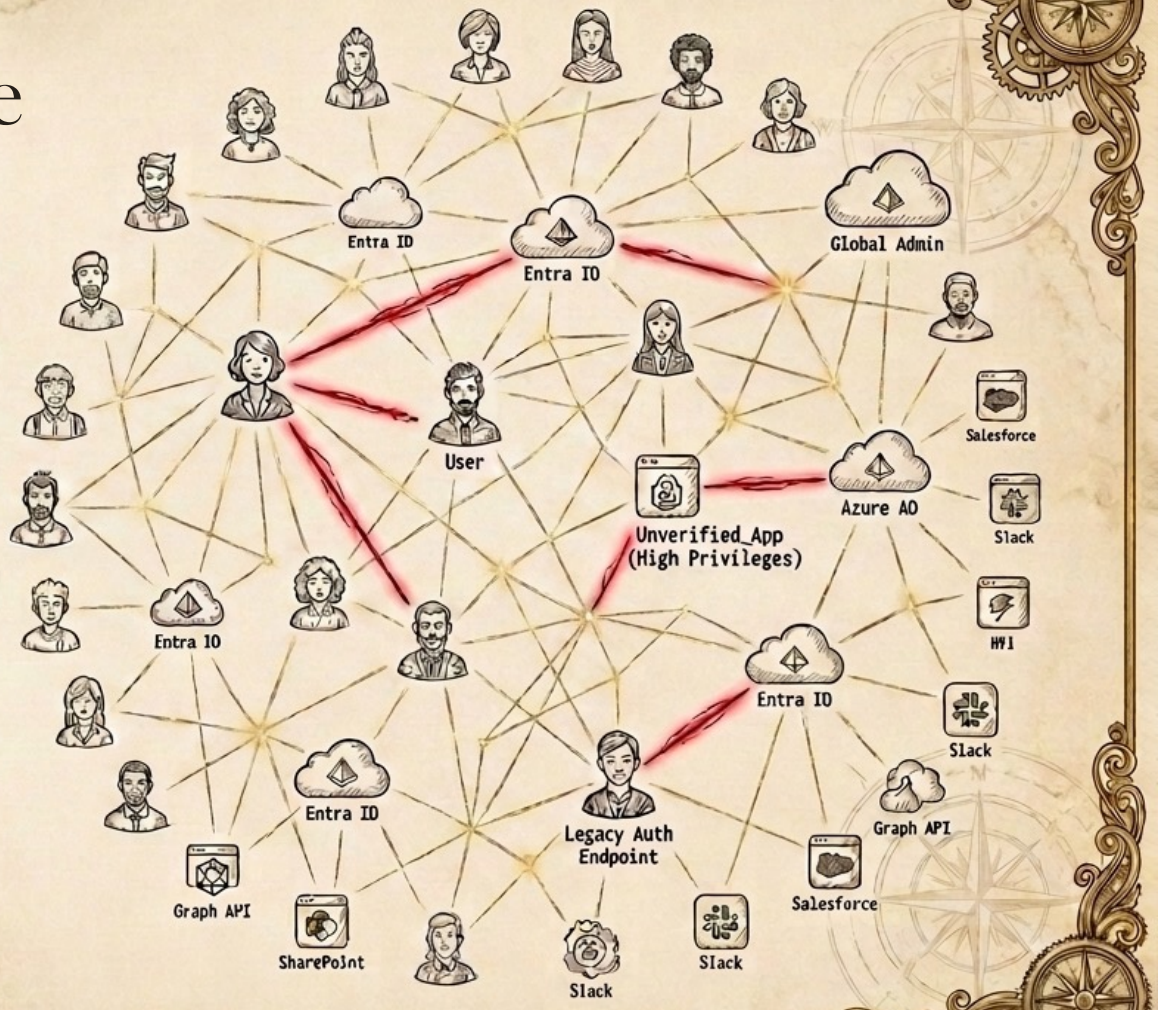
- Tenant ID
- Utilisation de jetons JWT
- Jetons signés avec un algorithme solide
- Kerberos


```
{
  "token_endpoint":
"https://login.microsoftonline.com/<tenant_id>/oauth2/v2.0/token",
  "token_endpoint_auth_methods_supported":[
    "client_secret_post",
    "private_key_jwt",
    "client_secret_basic",
    "self_signed_tls_client_auth"
  ],
  "jwks_uri":
"https://login.microsoftonline.com/<tenant_id>/discovery/v2.0/keys",
  "id_token_signing_alg_values_supported":["RS256"],
  "response_types_supported":["code","id_token","code id_token","id_token
token"
  ],
  "scopes_supported":[
    "openid"
```


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”



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	gitdumper	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_params	paramminer_headers	portscan
reflected_parameters	retirejs	robots	smuggler	sslcert	sslcert	url_manipulation
telerik	anubisdb	anubisdb	subdomains	trufflehog	wafw00f	wpscan
affiliates	apkpure	asn	azure_tenant	bucket_file_enum	bufferoverrun	builtwith
c99	censys_dns	censys_ip	certspotter	dnsbrute	code_repository	credshed
crt	crt_db	dehashed	dnsbrute	dnsbrute_mutations	dnscaa	fullhunt
dnsdumpster	dnstllsrpt	docker_pull	dockerhub	emailformat	extractous	fullhunt
git_clone	gitdumper	github_codesearch	github_org	github_workflows	hackertarget	hunterio
ip2location	ipneighbor	ipstack	myssl	otx	myssl	otx
pgp pgp	portfilte	postman	postman_download	rapiddns	shodan_idb	skymem
social	subdomain	dar	filedownload	urlscan	viewdns	wayback
asset_inventory	csv	emails	http	http	mysql	neo4j
nmap_xml	pmine	python	python	slack	splunk	sqlite
stdout	subdomain	s	txt	web_parameters	web_report	websocket
cloudcheck	dnsresolve	aggregate	aggregate	excavate	speculate	unarchive

Questions

(si il reste le temps)