
Les APT
Advanced Persistent Threats
APT
19 mai
Gérard PELIKS
Béatrice LAURENT
Abdelnahen SENOUSSAOUI
Les “Lundi de la Cybersécurité“

1


Quel est le problème ?
2

2

## Légende urbaine

Lorsqu'une TPE/PME est piratée,
elle est victime de ses lacunes en cybersécurité

Lorsqu'une grande organisation est piratée,
elle est victime d'une **APT**

**Les conflits géopolitiques sont à l'origine d'une flambée des APT soutenues par des États et du hacktivisme**

+58 % en 2024 par rapport à 2023

3

3

## Les attaques par APT (Advanced Persistent Threats)

### Les cyberattaques persistantes

*Définition* : Cyberattaque qui met en œuvre des moyens humains et techniques importants pour infiltrer durablement les systèmes d'information vitaux d'une organisation...

**Furtives**


**Ciblées**

**Durables**

4

4

## Les phases des attaques par APT

- Ingénierie sociale
- Attaque
- Etablissement d'un canal
- Elévation de privilège
- Expansion latérale
- Exfiltration des données
- Destruction du maliciel

5

5

## Les phases des attaques par APT

- **Ingénierie sociale**
- Attaque
- Etablissement d'un canal
- Elévation de privilège
- Expansion latérale
- Exfiltration des données
- Destruction du maliciel

6

6

## Reconnaissance passive



Réseaux sociaux

Darknet

*Image tirée d'une présentation du CLUSIF*

7

7

## Reconnaissance active : Les cibles

À l'accueil

Au standard

Ingénierie sociale

Help Desk

8

8

## Contre-mesures : Taisez-vous, formez-vous


**La sensibilisation de tous est indispensable !**

9

9

## Les phases des attaques par APT

- Ingénierie sociale
- Attaque
- Etablissement d'un canal
- Elévation de privilège
- Expansion latérale
- Exfiltration des données
- Destruction du maliciel

10

10

## C'est quoi ce mail débile ???

Envoyer | De | À: beatrice.laurent@lundi-cyber.fr; abdel@universite-paris-cite.fr | Cc: | Objet: Lundis de la Cybersécurité : TRÈS IMPORTANT, mail que je vais envoyer à mes listes

Invitation-Lundi-Cybe-Nol1.pdf 357 Kb

Bonjour,

Nos Lundis de la Cybersécurité se feront désormais **les jeudis** et plus les lundis.
Nos abonnés vont être avertis dans les heures qui viennent.

Les raisons de ce changement de date et d'horaire sont expliqués dans le lien et dans le PDF attaché :
https://192.23.14.1/lesnouveauxlundiscyber.com

Merci de votre compréhension.

Béatrice, Ahmed et Gérard

11

11

## Le Phishing et ses variantes

**Le Smishing**

par SMS

**Le Vishing**

par la voix

**Le Quishing**

**Tu es tombée dans le panneau par un mail de Phishing**

**Béatrice ! ☹**

12

12

## Tu as cliqué ! : Trop tard : petit clic et grosse claque !


*Tiré d'une présentation de la gendarmerie nationale*

**Le clic de trop (ça arrive à tout le monde ☹**
**mais il ne faut pas être comme tout le monde**

13

13

## Vous avez cliqué ! : C'était un mail piégé


14

14

## Cette attaque en Spear Phishing, qui a fait ça ?

15

15

## Demande d'aide à cybermalveillance.gouv.fr


16

16

Service d'assistance

Victime d'une cybermalveillance ?

Démarrer un diagnostic

## Comment signaler un mail frauduleux ?

Sachez tout d'abord qu'**au moindre doute, il ne faut donner aucune information** et **ne cliquer sur aucun lien**. Ils pourraient vous rediriger vers un site frauduleux. De même, si le mail suspect contient une pièce jointe, ne l'ouvrez pas, elle pourrait abriter un virus. Ensuite, **si vous avez identifié un email comme étant un mail frauduleux, il est important de le signaler** que vous soyez ou non tombé dans le piège. En effet, signaler un phishing permet de limiter le nombre de victimes et peut aider à identifier le cybercriminel à l'origine de l'arnaque.

Pour signaler un phishing par email aux services compétents, il existe plusieurs alternatives. Dans tous les cas, veillez à conserver les preuves et, en particulier, le message d'hameçonnage reçu. Pour signaler efficacement une tentative de phishing, il est important de transmettre le plus d'informations possible.

### 1. Signaler un mail de phishing sur Signal Spam

Si vous avez reçu un mail suspect, vous pouvez **le signaler sur la plateforme** Signal Spam. Il s'agit d'un

17

## Ce sont les Russes !


18

18

## La Russie multiplie les cyberattaques contre la France


En quatre ans, les pirates russes de **Fancy Bear (APT28)** ont visé une dizaine d'entités françaises sensibles

L'ANSSI a publié un rapport sur l'activité du groupe de cyberespionnage **lié au renseignement russe (le GRU).**

Fancy Bear a ciblé ou compromis une dizaine d'entités françaises sensibles, dont des ministères, des organisations de défense...

19

19

## Document de l'ANSSI

**29 avril 2025**


**https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-006.pdf**

20

20

## … et les autres …


21

21

## Exemples de groupes APT

Les APT sont portées principalement par des groupes de pirates financés par **la Russie, la Chine, l'Iran et la Corée du Nord**

- **APT41 :** Chine, vol du code source de produits stratégiques US.
- **APT38 :** Corée du Nord, transactions SWIFT, vol dans les institutions financières.
- **APT28 - Fancy Bear : Russie, contre l'OTAN et les entreprises de défense US.**
- **APT39** : Iran, concentrées sur des pays du Moyen-Orient


22

22

**Chine :**

- **APT1 (Comment Crew, PLA Unit 61398)** : Un des groupes les plus anciens et notoires, connu pour des attaques d'espionnage économique à grande échelle.
- **APT3 (Gothic Panda, Buckeye)** : Ciblant les secteurs de l'aérospatiale, des communications et de la technologie.
- **APT10 (MenuPass, Stone Panda)** : Vise les secteurs de la technologie, de l'automobile et de la pharmacie.
- **APT17 (Deputy Dog, Elderwood)** : Impliqué dans de nombreuses campagnes d'espionnage.
- **APT19 (Deep Panda, C0d0so0)** : Connu pour cibler les entreprises et les cabinets d'avocats.
- **APT27 (Emissary Panda)** : Vise divers secteurs, y compris le gouvernement et la défense.
- **APT31 (Judgment Panda, Zirconium)** : Ciblant les secteurs de l'aérospatiale, des télécommunications et le gouvernement.
- **APT41 (Winnti)** : Mêle espionnage et activités de cybercriminalité financière.
- **Volt Typhoon** : Se concentre sur les infrastructures critiques aux États-Unis et en Asie-Pacifique.
- **Flax Typhoon** : Ciblant des organisations aux États-Unis.
- **Salt Typhoon (GhostEmperor, FamousSparrow)** : Ciblant les réseaux de communication critiques.

**Russie :**

- **APT28 (Fancy Bear, Sofacy)** : Lié au renseignement militaire russe (GRU), connu pour cibler des gouvernements, des organisations militaires et politiques.
- **APT29 (Cozy Bear, The Dukes)** : Associé au service de renseignement étranger russe (SVR), ciblant des gouvernements et des organisations diplomatiques.
- **Sandworm (Voodoo Bear)** : Lié au GRU, connu pour des attaques destructrices contre des infrastructures critiques.
- **Turla (Snake, Venomous Bear)** : Groupe sophistiqué ciblant des entités gouvernementales et diplomatiques.
- **Gamaredon (Primitive Bear)** : Ciblant principalement l'Ukraine.

23

23

**Iran :**

- **APT33 (Elfin, Refined Kitten)** : Vise les secteurs de l'aérospatiale et de l'énergie.
- **APT35 (Charming Kitten, Phosphorus)** : Ciblant la recherche médicale, les infrastructures et les élections.
- **APT39 (Chafer, Remix Kitten)** : Ciblant les télécommunications et d'autres secteurs au Moyen-Orient.

**Corée du Nord :**

- **Lazarus Group (APT38)** : Connu pour des vols financiers, des cyberattaques destructrices et des opérations d'espionnage.
- **Kimsuky** : Se concentre sur la collecte de renseignements en Corée du Sud et dans la région.
- **APT43** : Mène des activités d'espionnage et de cybercriminalité pour soutenir les intérêts nord-coréens.

**Autres groupes notables :**

- **Equation Group** : Un groupe très sophistiqué, dont certains liens suggèrent une affiliation avec les États-Unis.
- **APT40 (TEMP.Periscope)** : Un groupe chinois ciblant divers secteurs, notamment l'ingénierie et la marine.
- **Blind Eagle (APT-C-36)** : Un groupe d'espionnage ciblant principalement la Colombie.
- **Bahamut** : Un groupe de mercenaires cybernétiques.

**Avec eux, ça fait mal… !!!**

24

24

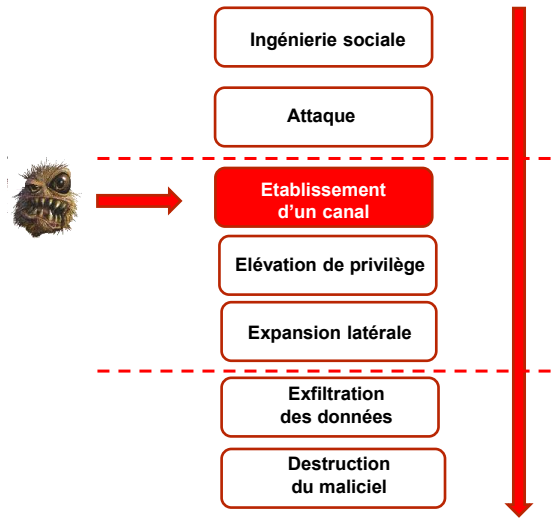
## Et en France, on fait quoi pour lutter contre ?


https://www.linkedin.com/posts/dgsi-securite-interieure_vid%C3%A9o-apt28-activity-7328063987319791637-CbS1

25

25

## Les phases des attaques par APT

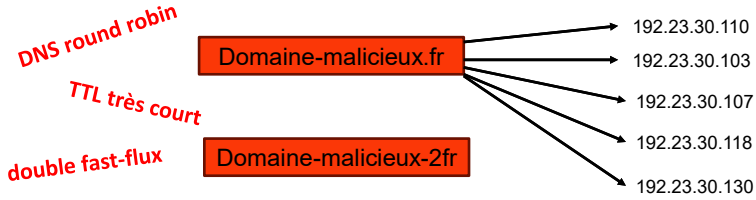



26

26

## Le Fast Flux DNS pour brouiller les pistes

- **Une attaque par changement fréquent des adresses IP données par un DNS**
- Avec un réseau à flux rapide, les **botnets** déplacent chaque adresse IP en quelques minutes seulement
- Bloquer quelle adresse IP ?
- Très difficiles à détecter, difficiles à éliminer

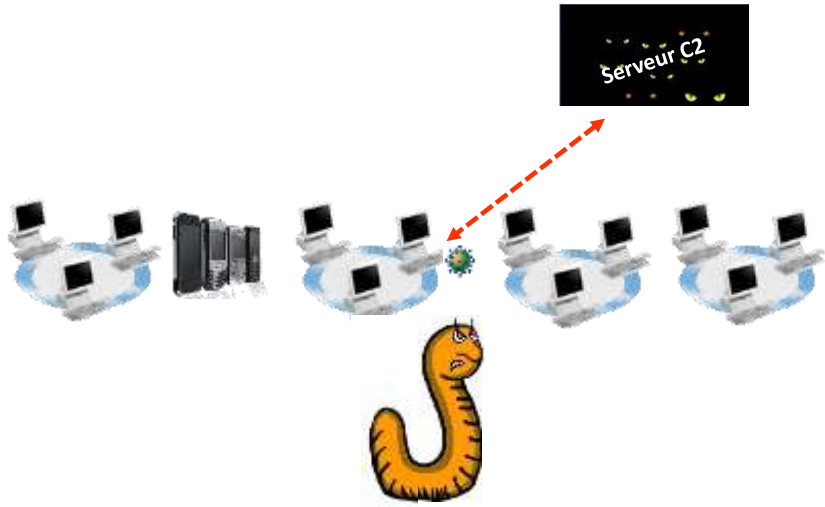



https://www.orange-business.com/fr/blogs/securite/securite-des-reseaux/fast-flux-et-double-fast-flux-techniques-de-resilience-de-sites-douteux

27 *Jean-François Audenard – Groupe Orange*

27

## Attaques par APT : Le maliciel se met à jour




28

28

## Les phases des attaques par APT


Ingénierie sociale

Attaque

Etablissement d'un canal

Elévation de privilège

Keylogger

Pass the hash

Man in the middle

ARP spoofing

29

29

## Contre-mesures : contrôle des privilèges

INTERDATA

PING CASTLE

Audit de l'Active Directory

BALABIT

WALLIX

Si vous n'avez pas détecté une attaque en APT à ce stade…

**Après c'est trop tard !**

30

30

## Les phases des attaques par APT

mimikatz

NDR

- Ingénierie sociale
- Attaque
- Etablissement d'un canal
- Elévation de privilège
- Expansion latérale
- Exfiltration des données
- Destruction du maliciel

Scan de ports

nmap

Zero-days

Remote Desktop Protocol

PsExec

Secure Shell

RemCom

xCmdSvc

31

31

## La prolifération des RATs !!!


PiXie

Quasar

FlawedAmmyy

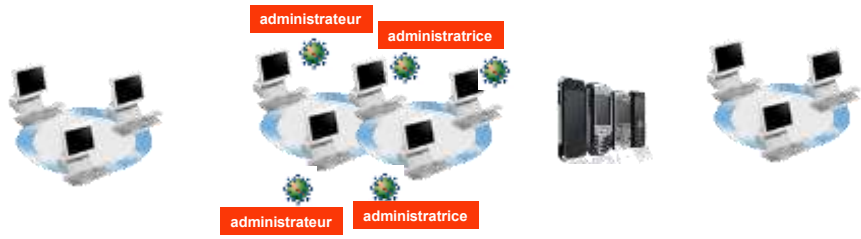
**Remote Access Troyans**

Cheval de Troie d'accès à distance

32

32

## Seuls les contaminés vont être pillés de leurs secrets




33

33

## Les phases des attaques par APT

mimikatz

psexec

ngrok

anydesk

procdump

powershell

Ingénierie sociale

Attaque

Etablissement d'un canal

Elévation de privilège

Expansion latérale

Exfiltration des données

Destruction du maliciel

0day

nmap

nslookup

Port TCP 443 : HTTPS

Port TCP 990 : FTPS

SNOWLIGHT

VShell

34

34

## L'exfiltration des données : La stéganographie

R : 00100110

V : 11001101

B : 10000110

On utilise un bit de chaque octet RVB qui compose chaque pixel de l'image. La dégradation est invisible à l'oeil nu...
On utilise ces bits pour cacher un document de 1/8e de la taille de l'image.

35

35

## Cacher un message dans une image couleur

36

36

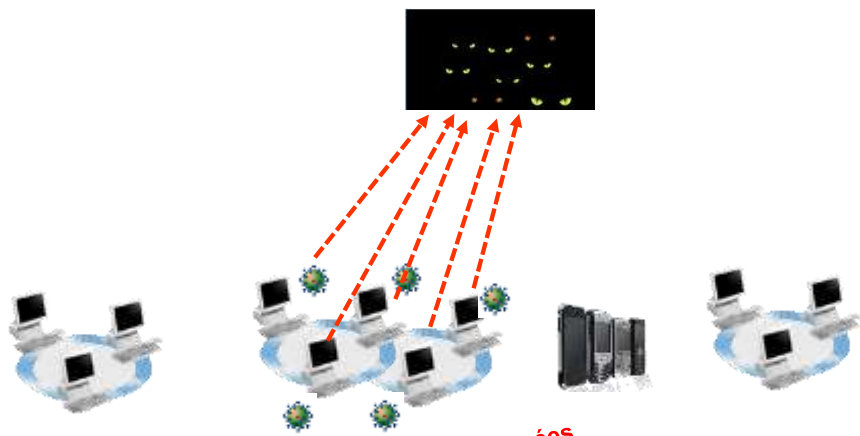
## L'exfiltration des données : La stéganographie


Ports TCP 443 (HTTPS) et 990 (FTPS)

37

37

## L'exfiltration des données



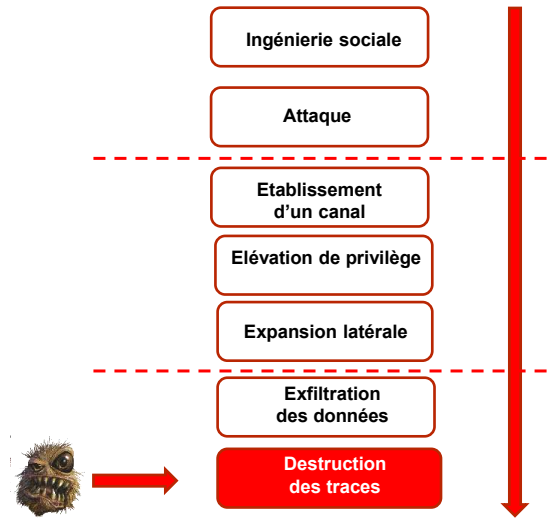
Compression, chiffrement des données

Suppression des historiques

38

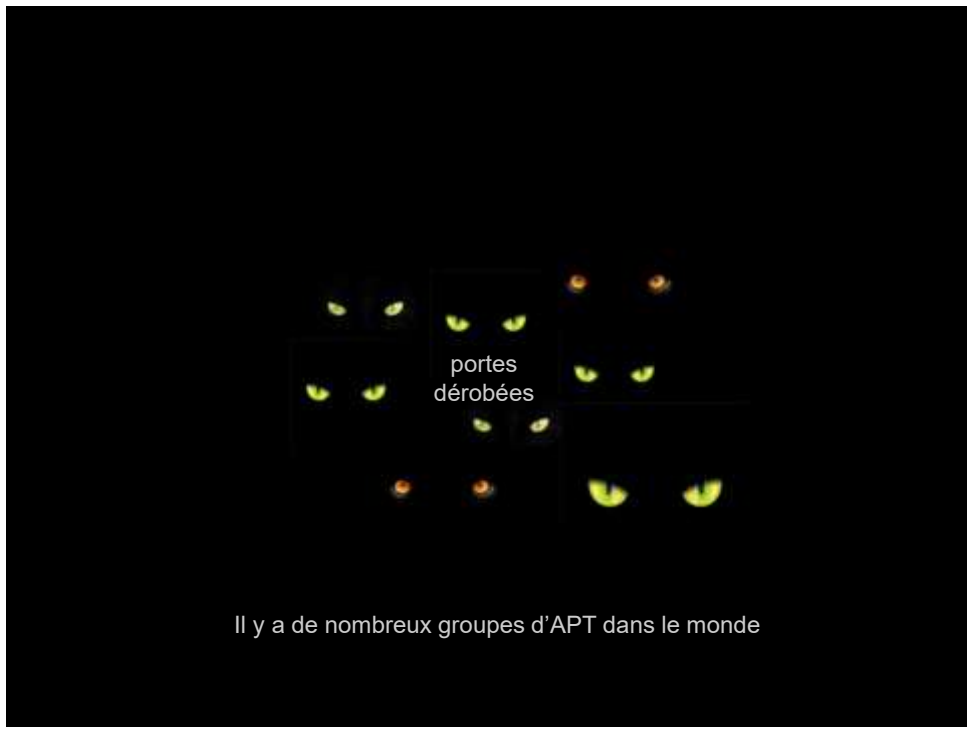
38

## Les phases des attaques par APT




39

39




40

Une fois les dommages constatés…

En moyenne, vous constatez les dommages…
…très longtemps après le début de l'attaque…

et vous devez en avertir la CNIL avant 72 heures,
une fois les dommages constatés…

# RGPD oblige !!!

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Conséquences juridiques et sanctions réglementaires

41

41

Revenons à la réalité…

Béatrice n'aurait pas cliqué!!!

Devant le mail débile, elle m'aurait téléphoné

Et l'attaque en APT aurait échoué ☺

C'était un scénario fictif, bien entendu ☺
Les noms de domaines utilisés sont aussi fictifs

beatrice.laurent@lundi-cyber.fr; abdel@universite-paris-cite.fr


42

42

## Que faire contre les APT ???


- **Threat Intelligence : Détecter les signes d'une attaque**
  - Anomalies dans les données sortantes ;
  - élévation de privilèges sans raison ;
  - comportements inhabituels de comptes utilisateurs ;
  - accumulations de fichiers inconnus et envois…

43

## Que faire contre les APT ???


Sensibiliser **tout** votre personnel (y compris celui de l'accueil, du help desk…)

- Compartimenter votre information
- Mettre à jour les correctifs
- Mettre en œuvre les édifices de sécurité (DLP, SIEM, SOC, ZTNA …)
- Préparer une cellule de crise, et entrainement

44

## Que faire contre les APT ??? : Les signaler


45

## Contre-mesures : Les édifices de sécurité

- Le DLP
- Le SIEM
- Le SOC
- La cellule de crise APT
- L'assurance cyber

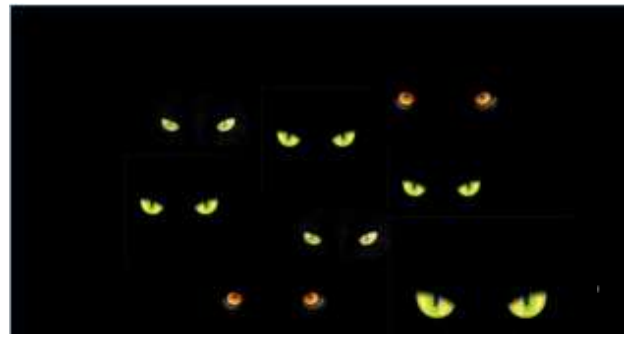
**Favoriser la résilience**

**Directives et Règlements : NIS2, DORA, CRA…**

46

46

## Les tuiles qui protègent de la pluie ont toutes été posées par beau temps



**Méfiez-vous des APT**

Ne soyez pas une organisation piratée

47

47

## La cybersécurité, avant l'attaque, c'est trop cher après l'attaque c'est trop tard

**Merci pour votre attention!**

Maintenant, **le quart d'heure des Associations**,
avec : **Claire ALBERIO**

Je vous retrouve après pour les questions / réponses

48

48