RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

PANORAMA DE LA MENACE INFORMATIQUE

La menace ? Des capacités au service d'une intention, qui saisissent une opportunité

- Nombre d'intrusions avérées observées par l'ANSSI dans les systèmes d'information :
  - 2020 : 786 ;
  - 2021: 1082

Intentions :

- Gain financier ;
- Espionnage ;
- Déstabilisation.

- Des attaquants aux capacités en constante progression;
- Des intentions persistantes et un usage de plus en plus décomplexé;
- De nombreuses faiblesses exploitées.

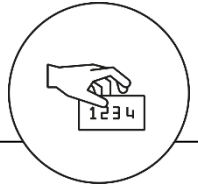
Des acteurs offensifs aux capacités en constante progression

Acteurs cybercriminels spécialisation et professionnalisation

Ex: Les bullets Proof Hoster

Acteurs étatiques de moins en moins identifiables

- *outils non-caractéristiques;*
- *partage d'outils entre différents modes opératoires réputés liés à des États;*
- *technique Living-of-the-Land.*



Acteurs privés un écosystème qui se développe rapidement

Ex: NSO Group

Des intentions persistantes et un usage de plus en plus décomplexé

Espionnage: première finalité !

- En 2021, 14 opérations de cyberdéfense traitées par l'ANSSI étaient liées à des opérations d'espionnage ;
- Détournement de cadres juridiques :
  - *Logiciel GoldenTax en Chine*
  - *Extraterritorialité (Cloud Act, FISA, ITAR)*

Gain financier :

- *USA (2021) : Rançongiciel Darkside sur Colonial Pipeline*

Des attaques informatiques mises à profit **d'opérations déstabilisation**.

- *Campagne Ghostwriter attribuée à la Russie par l'Allemagne et l'Union européenne et à la Biélorussie par l'éditeur de sécurité FireEye*
- *Inde (2021) : **Prépositionnement** sur le réseau électrique*

De nombreuses faiblesses exploitées

- Exploitation massive de vulnérabilités par différents type d'acteurs
- Exploitation à des fins malveillantes des nouveaux usages numériques (ex:Cloud)
- Attaques indirectes *via* la *supply chain*
- Faible sécurisation des données entrainant des *leaks* massifs

CVE les plus exploitées en 2021

Incidents ANSSI		
1	CVE-2021-26855	Microsoft Exchange
2	CVE-2021-26857	
3	CVE-2021-26858	
4	CVE-2021-27065	
5	CVE-2018-13379	Fortinet
6	CVE-2021-21985	VMWare
7	CVE-2021-22893	Pulse

Incidents CISA		
1	CVE-2021-26855	Microsoft Exchange
2	CVE-2021-26857	
3	CVE-2021-26858	
4	CVE-2021-27065	
5	CVE-2021-22893	Pulse
6	CVE-2021-22894	
7	CVE-2021-22899	
8	CVE-2021-22900	
9	CVE-2021-27101	Accellion
10	CVE-2021-27102	
11	CVE-2021-27103	
12	CVE-2021-27104	
13	CVE-2021-21985	VMWare
14	CVE-2018-13379	Fortinet
15	CVE-2020-12812	
16	CVE-2019-5591	

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

WWW.CERT.SSI.GOUV.FR