Une brève histoire de la cyber-sécurité

Pr. Gilles Grimaud - Université de Lille - Faculté des sciences et technologies

cnrs Université de Lille Inria centralelille IMT Nord Europe École Mines-Télécom IMT-Université de Lille

Une brève histoire de la cyber-sécurité

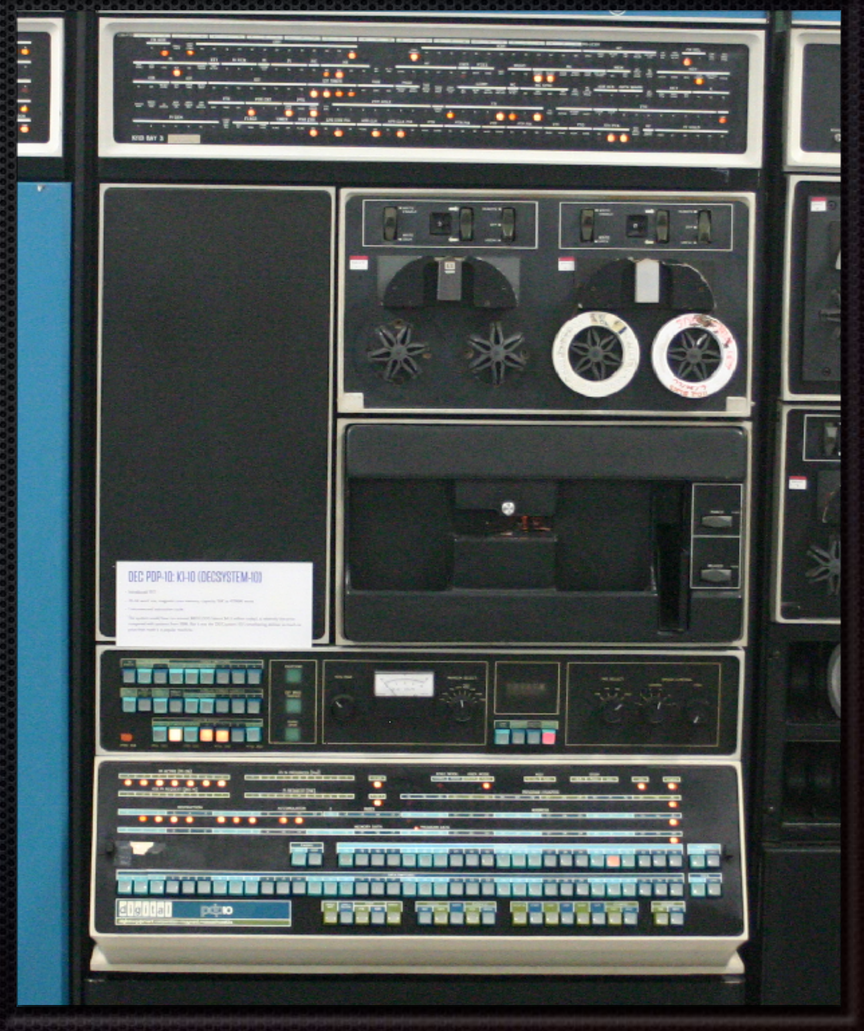
- -1980 : les précurseurs
- 1980-2000 : l’ère des hackers
- 2000- : Internet et la cyber-criminalité
- état des lieux

Les précurseurs

1971 : Creeper

« I'M THE CREEPER:
CATCH ME IF YOU CAN »
ARPANET/DPD

⇝ Reaper



Les précurseurs

1971 : Creeper

« I’M THE CREEPER:
CATCH ME IF YOU CAN »
ARPANET/DPD

⇝ Reaper

1973 : Cyber-braquage

NY Union Dime vs Mr R.S. Para

⇝ 20 000 $ d’amende

Les précurseurs

1971 : Creeper

« I'M THE CREEPER:
CATCH ME IF YOU CAN »
ARPANET/DPD

⇝ Reaper

1973 : Cyber-braquage

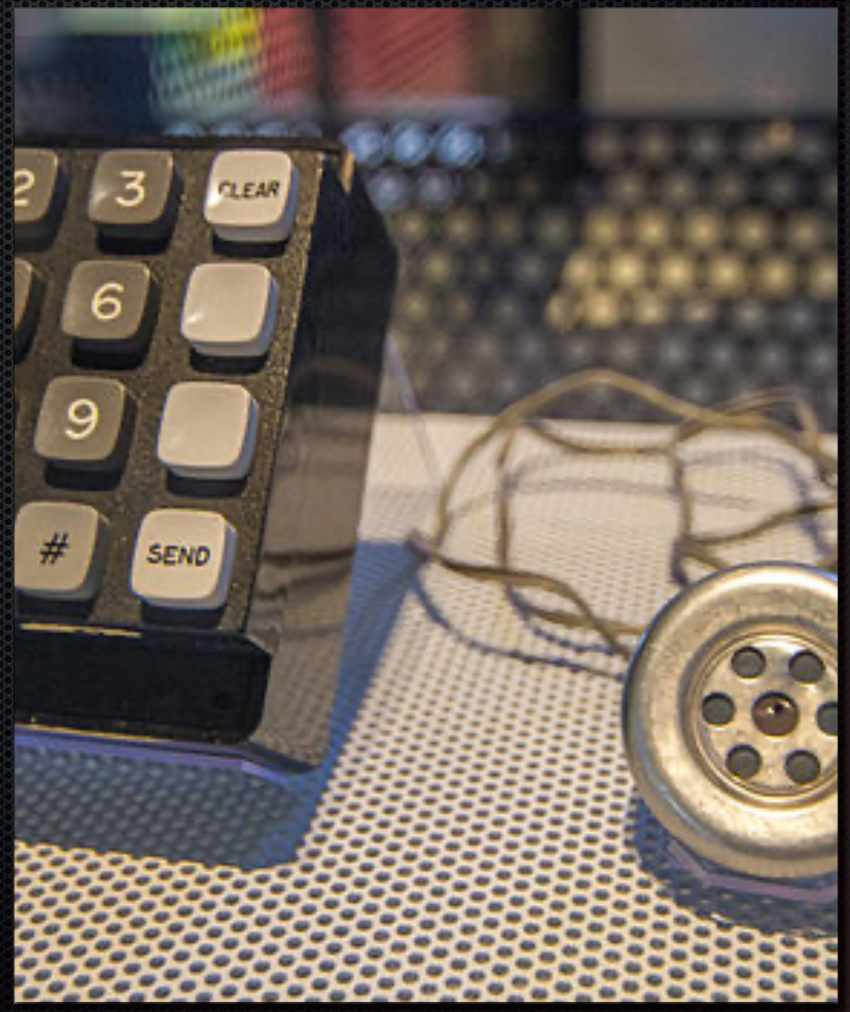
NY Union Dime vs Mr R.S. Para

⇝ 20 000 $ d'amende

1975 : Blue Box Phreaks

Mr Draper

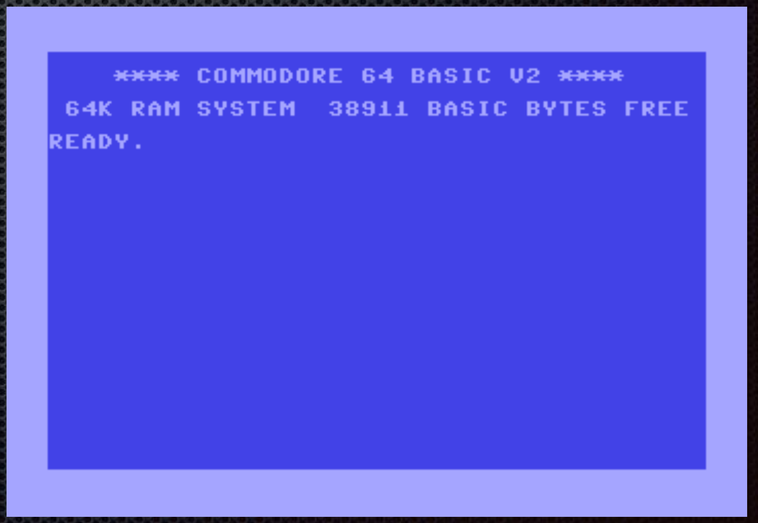
⇝ 2 ans de prison



L’ère des Hackers

1980 : L’informatique grand publique

Une (sous?)culture émerge :
jeux vidéos, bidouillage, programmation maison…



1981 : Création du Chaos Computer Club

L’ère des Hackers

1985 : Crackers, swappers, cheaters, lamers…

- copy parties
- compétitions / émulations

L’ère des Hackers

1986 : Première épidémie documentée
Première épidémie sur « compatible PC »
Vecteur d’infection « la disquette »

1987 : Anti-virus
Premiers virus éradiqués sur PC

1988 : Premiers anti-virus commerciaux

" Theory of self-reproducing automata "

L’ère des Hackers

1988 : Réponse pénale

La loi Godfrain du 5 février 1988

L’ère des Hackers

1997 : Rétro-ingénierie terminal de paiement

Il trouve la clef (cryptographique) publique

1998 : « Négociation » GIE Carte Bancaire

Démonstration publique d’une YesCard

2000 : Jugement

« coupable de falsification de cartes bancaires et d'introduction frauduleuse dans un système automatisé de traitement ».

⇝ 10 mois de prison

Serge Humpich

Internet et la cyber-criminalité

2000 : L'informatique grand publique devient :

1. un support multimédia ;
2. massivement interconnecté ;
3. supportant un nombre croissant de transactions commerciales.

Internet et la cyber-criminalité

1999 : Napster & la numérisation de l'information
Partage à grande échelle de fichiers audio mp3

2001 : Torrent
Partage de fichiers pair-à-pair

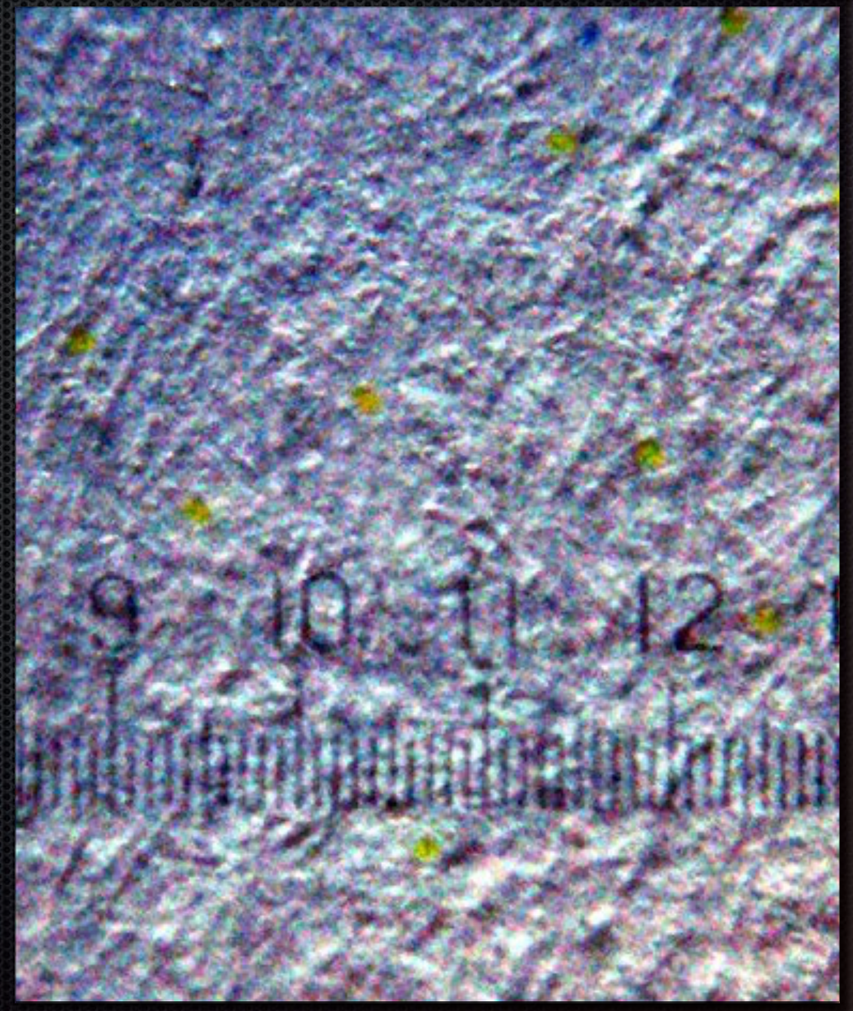
2003 : The Pirate Bay
Espace de partage de fichiers
(audio, video, application, jeu…)

Internet et la cyber-criminalité

1998 : Tatouage numérique

Stéganographie

Suivi de copyright



Internet et la cyber-criminalité

1999 : Common Vulnerabilities and Exposures

Dictionnaire systématique des failles de sécurité et d'exploits répertoriés pouvant entraîner la perte de contrôle d'un système informatique :
exemple CVE-2019-14095

CVE-ID	
CVE-2019-14095	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Buffer overflow occurs while processing LMP packet in which name length parameter exceeds value specified in BT-specification in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8016, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9379, QCA9886, QCM2150, QCN7605, QCS404, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://www.qualcomm.com/company/product-security/bulletins/march-2020-bulletin

Internet et la cyber-criminalité

1995 : Premier programme de Bug Bounty

Les entreprises payent pour les ingénieurs qui trouvent des failles de sécurité dans leurs logiciels (Netscape).

2013 : Google, Facebook, Microsoft…

Facebook et Microsoft produisent des cartes bancaires « bug bounty » pour récompenser des exploits ;

Google étend son programme de bug bounty aux logiciels opensource « critique ».

Notion de faille de sécurité logicielle

Une illustration grand publique ?

Internet et la cyber-criminalité

White hat, Grey hat, Black hat

. . .

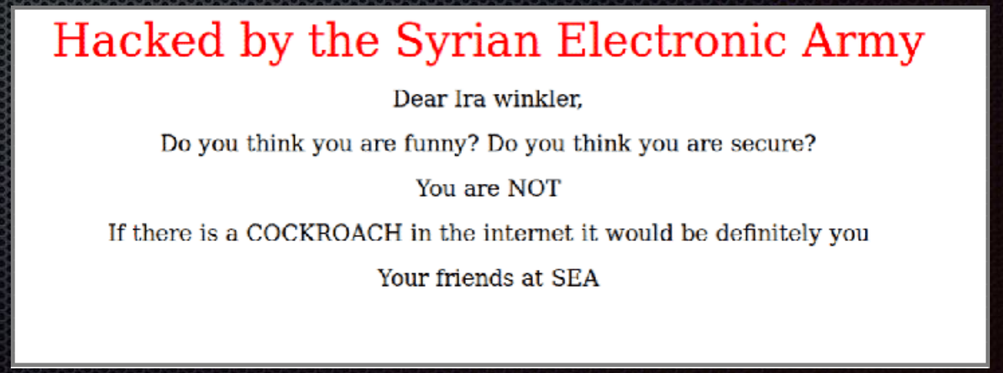
Internet et la cyber-criminalité

1996 : Defacement (défiguration?) du site web du département de la justice américaine.

Hacker Activistes = Hacktivistes

2014 : Le défacement de RSAConference

Les clefs du royaume…



Internet et la cyber-criminalité

2001 : Hameçonnage (Phishing)

Contre-façon de site web (ou mail, sms, …)

- vol d'identité ;
- accès à des informations privées (compte bancaire…) ;
- …

Attaques homographes : example.com example.com

Internet et la cyber-criminalité

2002 : Lancement du réseau TOR

Vie privée vs Anonymat

Commercialisation de VPNs et des Proxys

Internet et la cyber-criminalité

2010 : Notion d’emprunte numérique

Electronic Frontier Foundation annonce 18,1 bits d’entropie.

https://amiunique.org

https://coveryourtracks.eff.org

Internet et la cyber-criminalité

2007 : Débridage du premier iPhone : « *Jailbreaking* »

- contourner les limitations d'opérateurs ;
- contourner les limitations d'utilisations ;
- permettre le chargement d'applications piratées…

20% des iPhones en France.
à ne pas confondre avec le fait de désimlocker son téléphone.

« Rooter » un android, Jailbreak de switch, PS4…

Internet et la cyber-criminalité

2004 : Botnets, scans, spams et DDoS

Botnet, mot-valise construit a partir de robot et réseau.

- propagation de logiciels malveillants (extension du botnet) ;
- propagation de spams ;
- utilisation de CPUs « gratuits » : minage de cryptomonnaies ;
- Attaques distribuées en dénie de service.

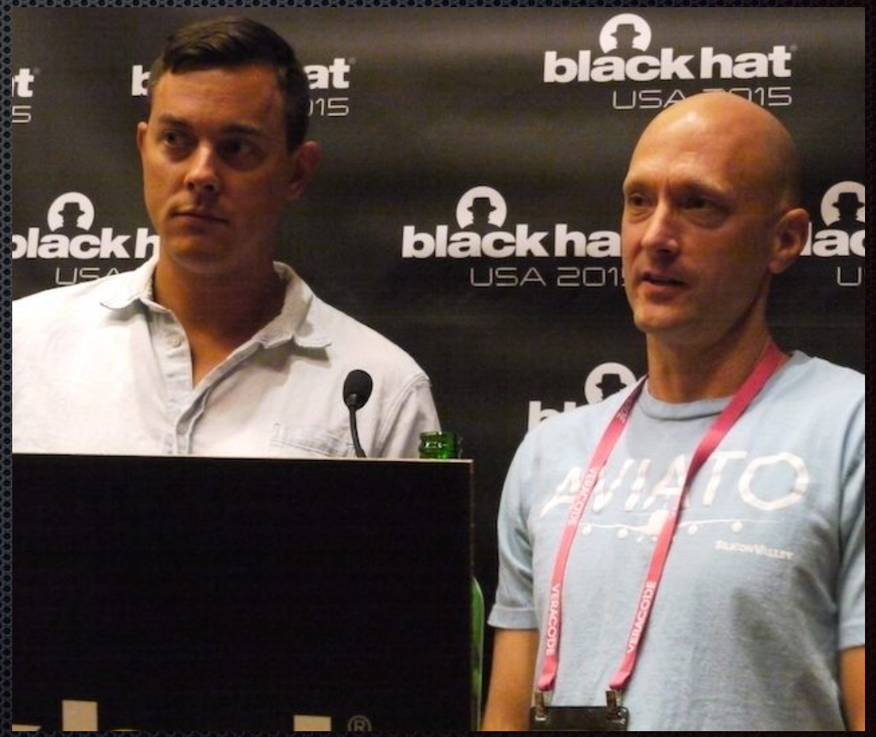
2016 : Le cas de Mirai & DDoS

Attaque en dénie de service : 620Gb/s (Netflix, twitter)
Attaque en dénie de service : 1Tb/s (OVH)

Internet et la cyber-criminalité

Crimes sans fils…

2012 : Hack d'un pacemaker
2015 : Prise de contrôle à distance d'une Jeep Cheeroke

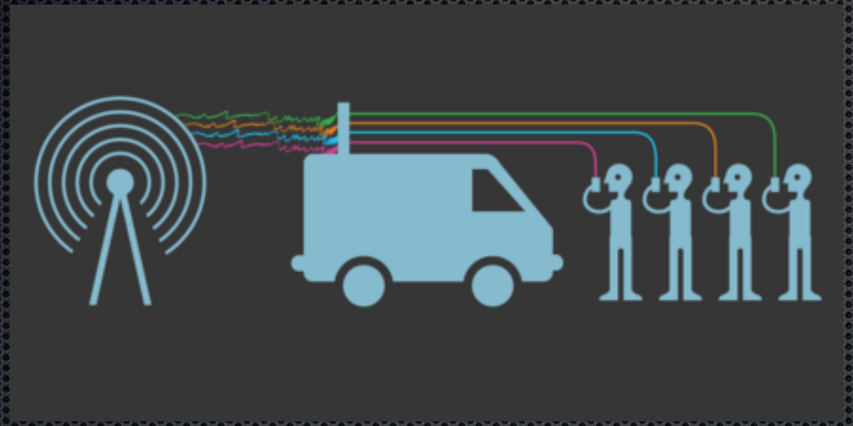


Mais pas sans trace :
2010 : Notion de « preuves numériques »
Utilisation d'informations numériques pour aider à établir les faits.
2021 : « Analyse forensique des écosystèmes intelligents communicants de l'internet des objets » doctorat de l'IRCGN

Internet et la cyber-criminalité

2003 : 1er IMSI Catcher commercialisé

Terrorisme, prisons, surveillance…



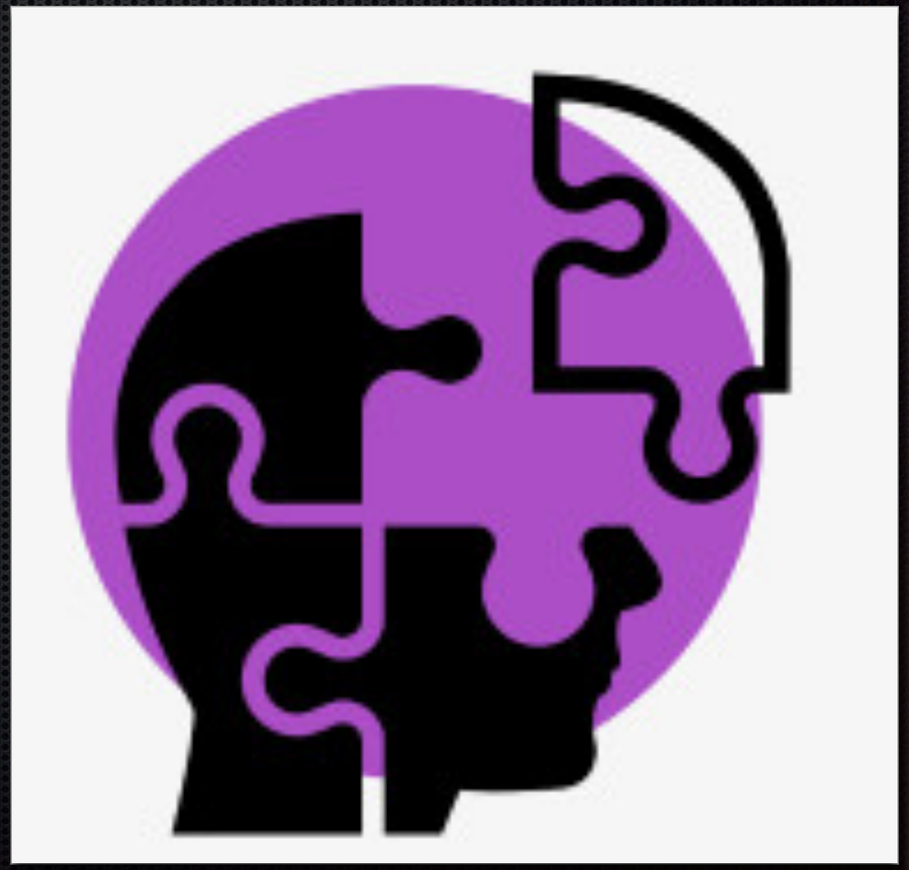
2010 : un IMSI-Catcher maison à 1500 $

Internet et la cyber-criminalité

2005 : Intelligence Community Directive 301

- OSInt ;
- GEOInt ;

Exploitation de données et méta-données publiques…



Internet et la cyber-criminalité

2003 : Le Grand Pare-feu chinois

Censure ;

Traçage ;

Espionnage.

Internet et la cyber-criminalité

2007 : 1er acte de cyber-guerre

Paralyser les infrastructures d'état de l'Estonie.

2010 : Stuxnet

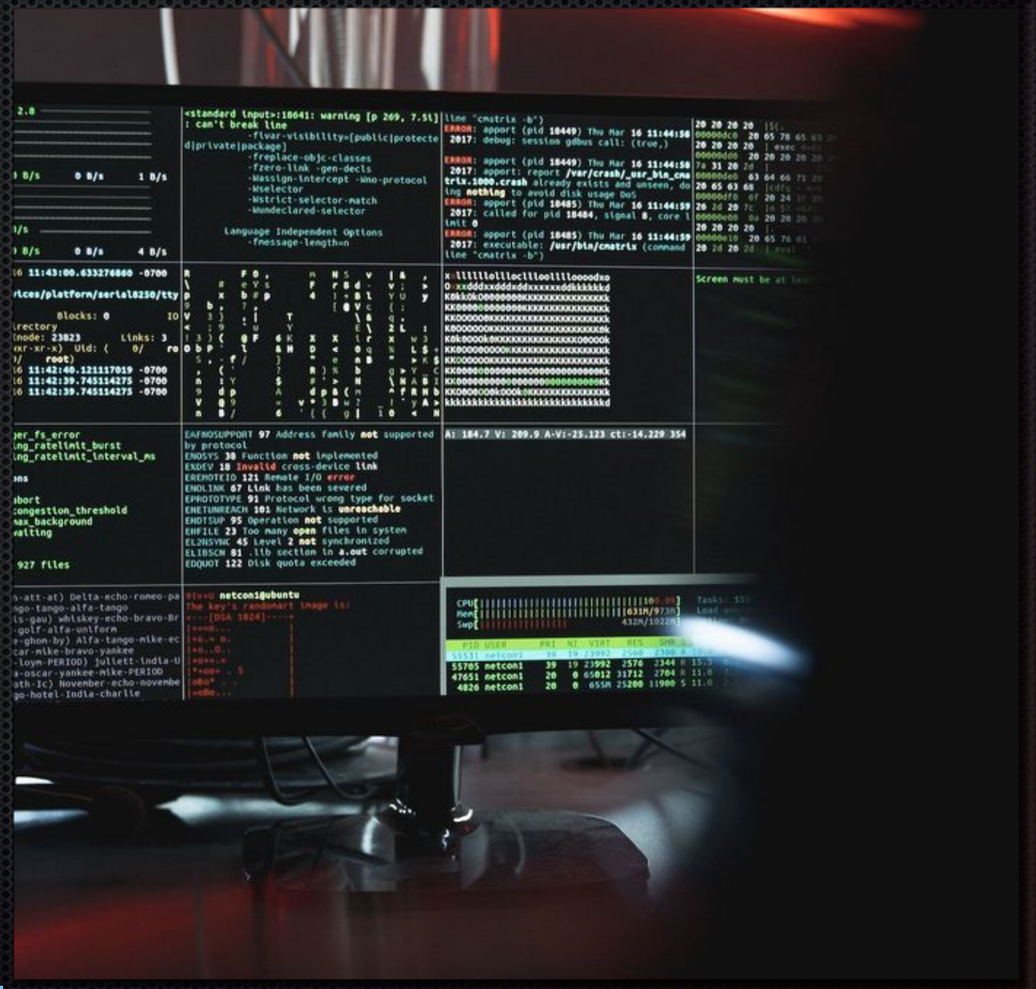
Virus conçu pour détruire les équipements nucléaires iraniens.

2017 : NotPetya malware

Attaque de l'économie ukrainienne.

2022 : Foxblade

Microsoft rapporte une attaque ciblée la veille de l'invasion russe.



État des lieux

cyber-menaces des organisations criminelles

- vol de données privées, mots de passe, données bancaires… (hameçonnage) ;
- rétro-ingénierie, vol de propriété industrielle,
- commerce de failles de sécurité « *Zero-Day* » ;
- botnets, spams, denis de service ;
- trafic d'e-réputation, campagne de calomnie ;
- criminalité : trafics de produits illicites, ramçongiciels, pédo-pornographie.

État des lieux

Cyber-sécruité et le secteur privé

- Antivirus, Pare-feux et Système de Détection d'Intrusions ;
- *Zero-Day* et *Bug-Bounty* ;
- Audit de sécurité, *Pentesting* ;

- Appropriation de données de la vie privée (traçage) ;
- Espionnage industriel ;
- …

État des lieux

Cyber-sécurité et organismes d'état

- lutte contre la cyber-criminalité ;
  - enquête sous pseudonyme,
  - exploitation d'indices numérique,
  - radio-identification ;

- Intelligence open-source ;

- espionnage d'état, industriel ;
- Armes de guerre, guerre hybride ;
- Censure, Désinformation, …


CYBER SECURITY
INFORMATION
FUTURE
CONNECTION
DATA
CONTACT
ELECTRONIC
INFO
SEARCH
NETWORK
WWW
TODAY
AREA
CONNECT
COMMUNITY
VIRTUAL
CYBER
GLOBAL
INNOVATION
ACCESS
RELATION
TECHNOLOGY
WEB
SOURCE
PROVIDER
SPEED
NUMBER