Évolution et industrialisation des cyberattaques

Clusis - 5à7 en ligne

Janvier 2025

EVOLINK Security

Sylvain Porchet

EVOLINK Thinking Solutions Together

Industrialisation des cyberattaques

RaaS, *Ransomware-as-a-Service*

1. Introduction RaaS
2. Deep dive Raas

TTPs, *Tactics, Techniques, and Procedures* (TTP)

3. Introduction TTPs
4. Deep dive TTPs

À l'aube de l'ère numérique, **les cyberattaques étaient l'œuvre de hackers isolés**, motivés par la curiosité ou le vandalisme.

Aujourd'hui, la cybercriminalité s'est **industrialisée,** formant un **écosystème complexe** de **groupes organisés** et de cybercriminels **spécialisés**

Les prémices

1970-1980

- Les premiers actes de cybercriminalité étaient souvent liés à des piratages informatiques rudimentaires, comme le phreaking (piratage des réseaux téléphoniques) ou la création des premiers virus informatiques (1982,**1987**).

- Le terme "cybercrime" est encore très peu utilisé, mais les bases de ce qui allait devenir une nouvelle forme de criminalité étaient posées.

L’émergence

1990

- Le terme **"cybercrime"** ("cybercriminalité") commence à être utilisé pour décrire ces délits commis via des réseaux informatiques.

- En 1997, le **Conseil de l’Europe** a commencé à travailler sur une convention pour lutter contre la cybercriminalité, aboutissant à la **Convention de Budapest sur la cybercriminalité** en 2001.

La professionnalisation

2000

- Les cybercriminels ont commencé à **s'organiser en réseaux structurés**, utilisant des outils de plus en plus sophistiqués.

- Des **marchés noirs en ligne ont émergé**, facilitant la vente de données volées, de logiciels malveillants et de services de piratage.

L'industrialisation

2010

- Le cybercrime est devenu une véritable industrie, avec des revenus estimés à des **milliards** de dollars.
  Coûts: 114mrd/2010 600 mrd/2018*

- Les attaques sont désormais automatisées, ciblées et souvent menées par des groupes criminels organisés ou des États-nations.

*Sources:
Symantec (2011), Norton Cybercrime Report.
McAfee (2018), Rapport de synthèse

L’industrialisation hyperconnectée

2020

- Le cybercrime est devenu une **menace systémique** **et hyperconnectée.**
  Les attaques sont désormais **massives, sophistiquées et multiformes**, exploitant IA, IoT et infrastructures cloud.

  Coûts : 8K mrd. pour 2023, 9.22K mrd. Projeté 2024*

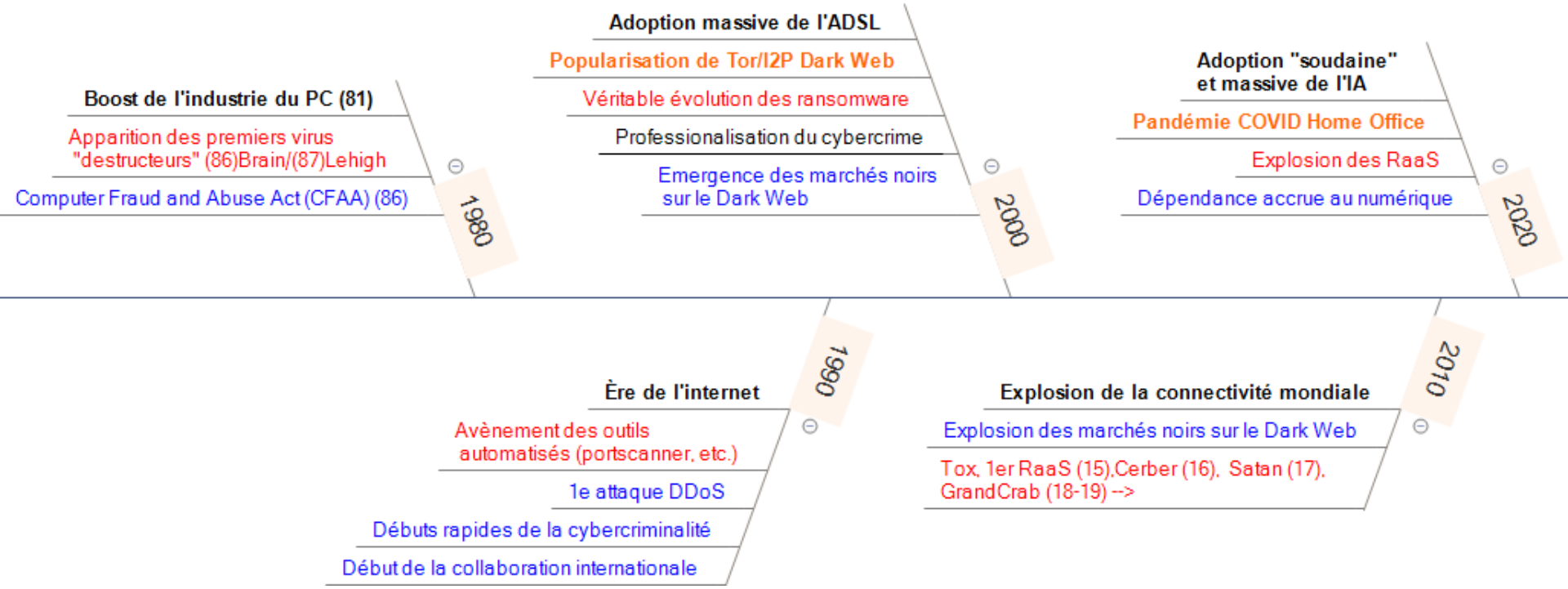
* source: Amma Fleck (2024). Cybercrime Expected To Skyrocket in Coming Years
Une projection d’octobre 2023 de Cybersecurity Ventures, faisait état de 9.5K

Échelle de grandeurs

États-Unis :	26 185 mrd de dollars
Chine :	21 643 mrd de dollars
Cybercrime	9 220 mrd de dollars
Japon :	4 365 mrd de dollars
Allemagne :	4 120 mrd de dollars
Inde :	3 820 mrd de dollars
Suisse:	834 mrd. de dollars

Source: Business Cool. (2024) Classement PIB 2024 : les pays les plus riches du monde

Les accélérateurs au fil du temps.



Les accélérateurs au fil du temps.

	Crise du Coronavirus. Dimension sanitaire		Crime conventionnel		Cybercrime		Indice niveau d'exposition au risque cyber[33]	Fragile States Index[34]
	Nombre de malades (au 30/09/2020)[35]	Nombre de décès / million d'habitants (au 30/09/2020)[36]	En hausse	En baisse	En hausse	En baisse		
États-Unis	7 433 558	638	Homicides	X	X		0,145	38,3
Royaume-Uni	453 264	620	Trafic de drogue, violences domestiques	X	X		0,207	38,3
Mexique	738 163	597	Crime organisé, homicides, vols...		X		0,483	67,2
Russie	1 176 286	142	Crime organisé	X	X		0,528	72,6
Inde[37]	6 305 643	71		X	X		0,597	75,3
Singapour	57 765	5		X	X		0,231	26,3
Malaisie (KL)	11 224	4		X	X		0,293	57,6

Source: IHEMI. (2025). Évolution du crime et du cybercrime durant la pandémie de coronavirus

Métriques « pandémiques».

1) Aux États-Unis, depuis le début de l'épidémie, le nombre de cyberincidents quotidiens déclarés auprès de l'Internet **Crime Complaint Center** (IC3) est passé de 1000 à 4000.

2) Le créateur de l'entreprise de cybersécurité MonsterCloud estime, quant à lui, que **les attaques par ransomware** auraient augmenté de **800%** depuis le début de la pandémie

Sources:
Maggie Miller. (2020) FBI sees spike in cybercrime reports during coronavirus pandemic.
Prnewswire. (2020) Top Cyber Security Experts Report. site prnewswire.com

Stu (KnowBe4) stu-knowbe4 **Brand Representative** Thai Pepper — May 2015

As we predicted in our whitepaper "Your Money or Your Life/Files", there is now shake-and-bake criminal ransomware that aspiring Internet criminals can put together in a few minutes. Meet 'Tox', Ransomware for the rest of us.

In short, you can now go to this TOR website "for criminals by criminals", roll your own ransomware for free, and the site takes a 20% kickback of every Bitcoin ransom payment.

Jim Walter at McAfee Labs commented: "The packaging of malware and malware-construction kits for cybercrime "consumers" has been a long-running trend. Various turnkey kits that cover remote access plus botnet plus stealth functions are available just about anywhere. Ransomware, though very prevalent, has not yet appeared in force in easy-to-deploy kits. But now we have Tox–and it's free."

Tox is not going to to be the last criminal malware to embrace this model. You can expect new strains, built with more features, better quality and different encryption and evasion methods. This is only the beginning.

And as always, stepping employees through effective security awareness training is a must these days. Find out how affordable this is, and be pleasantly surprised. Reviews at the tab.

Warm regards, Stu

@KnowBe4

Source: https://community.spiceworks.com/t/its-heeere-criminal-ransomware-as-a-service/407309

Rétrospective de l'industrialisation par apparition des services

1. DDoS-as-a-Service (2000)
2. Bulletproof Hosting (2000)
3. Phishing-as-a-Service (2004)
4. Spam-as-a-Service (2004)
5. Botnets-as-a-Service (2007)
6. Exploit Kits-as-a-Service (2010)
7. Crimeware-as-a-Service (2010)
8. Ransomware-as-a-Service (2018 (2015))

2015 Le grand virage

2015 un tournant

À partir de 2015 :

Les **groupes criminels organisés** ont commencé à **investir massivement** dans le cybercrime, voyant son potentiel lucratif.

Ils ont adopté des méthodes professionnelles, avec des équipes spécialisées (développeurs, analystes, financiers) et des infrastructures techniques robustes.

Les cybercriminels et les mafias traditionnelles.

Les mafias traditionnelles **occupent une place de plus en plus importante** dans l'écosystème de la cybercriminalité.

Motivations:

Maximisation des profits.

Réduction des risques.

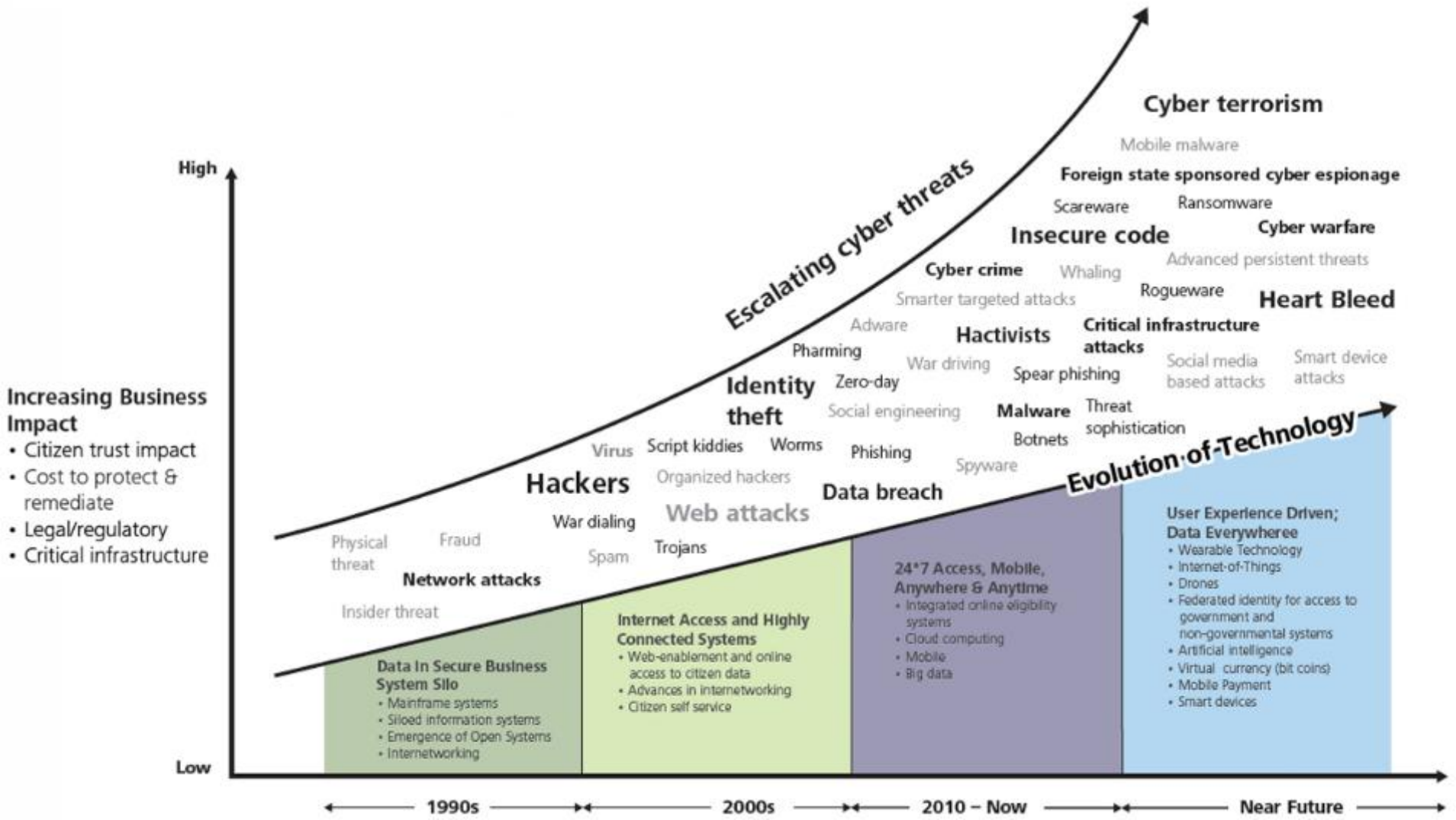
Ceci va augmenter **l'exponentialité** de la dynamique de l'industrialisation

Les mafias ont besoin des cybercriminels pour blanchir une partie de leurs revenus illégaux.

Les cybercriminels ont besoin des mafias et de leur logistique pour convertir la monnaie numérique en monnaie fiduciaire.

Interdépendance des systèmes

Synoptique de l’évolution



Source: Deloitte-NASCIO Cybersecurity Study (2014). *State government at risk: Time to move forward*

RaaS


Javier Diaz
Security Team Coordinator
Cybersecurity Specialist
javier.diaz@swisscom.com
Anthony Ferzoco
ICT Security Operation Engineer
Cybersecurity Specialist
anthony.ferzoco@swisscom.com

TTPs (Tactics, Techniques, and Procedures)
TTPs (Tactiques, Techniques et Procédures)

TTPs (Tactics, Techniques, and Procedures)

Dans le monde réel.

Ensemble de méthodes et de stratégies utilisées par les forces armées pour mener à bien leurs opérations.

Elles englobent l'ensemble des actions,
depuis la **planification** jusqu'à **l'exécution**,
en passant par l'évaluation.

TTPs (Tactics, Techniques, and Procedures)

- **Dans le monde de la cybersécurité.**

  Comme les militaires étudient les **tactiques**, **techniques** et **procédures** de leurs adversaires, les équipes SecOps analysent les TTP des cybercriminels.

Pour:

- **Comprendre** le modus operandi des attaquants :
  Identifier les méthodes utilisées, les outils privilégiés, les vecteurs d'attaque favoris.
- **Anticiper les menaces** :
  Prédire les prochaines attaques, mettre en place des mesures de prévention adaptées.
- **Détecter les intrusions** :
  Les TTP font référence pour détecter les activités suspectes.
- **Réagir efficacement** : Une fois une attaque détectée, la connaissance des TTP permet de mettre en œuvre les **mesures de réponse** les plus appropriées.

TTPs (Tactics, Techniques, and Procedures /Tactiques, techniques et procédures)

Tactics = Objectifs généraux ou le "**pourquoi**" des actions d'un attaquant.
->Ce que l'attaquant veut accomplir

Obtenir un accès initial à un système

Maintenir une présence persistante

Exfiltrer des données sensibles

TTPs (Tactics, Techniques, and Procedures /Tactiques, techniques et procédures)

Techniques = Détaillent le "**comment**" les tactiques sont mises en œuvre.
->Méthode utilisée pour accomplir

Exploiter une vulnérabilité
Campagne de phishing
Installation d'un Keylogger

TTPs (Tactics, Techniques, and Procedures /Tactiques, techniques et procédures)

Procedures = Décrivent les détails spécifiques, ou la manière dont une technique est mise en œuvre.
->Action pratique

Exploiter la faille CVE-2023xyz
Configurer un site web factice imitant une page de connexion
Utiliser une macro malveillante pour écrire un mail à l'insu d'un utilisateur

Exemple complet.

Cyberattaque visant une entreprise :

- Tactique : Escalade des privilèges.
- Technique : Voler des informations d'identification (credentials).
- Procédure : Utilisation de scripts PowerShell pour extraire les mots de passe en clair depuis la mémoire d'un système.

Les TTPs constituent un outil essentiel pour :

Analyser et **contrer** les cybermenaces,

notamment dans le cadre de méthodologies comme **MITRE ATT&CK**, **Cyber Kill Chain**, ou d'autres cadres de réponse aux incidents.

Sylvain Porchet
RSSI/CISO
Responsable département sécurité
Head of security departement
sylvain.porchet@evolink.ch
Tél. +41 58 255 77 55
Tél. direct: +41 58 255 77 64
www.evolink.ch

Sylvain Porchet
contact@porchet.org
https://www.linkedin.com/in/sporchet/

Sharekey
ID : 8NBKLQY5
https://app.sharekey.com/member/8NBKLQY5

www.evolink.ch

EVOLINK Security

EVOLINK
Security