الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team

TUNISIA
CYBER SECURITY
& CLOUD EXPO

Malware as a Service

MaaS

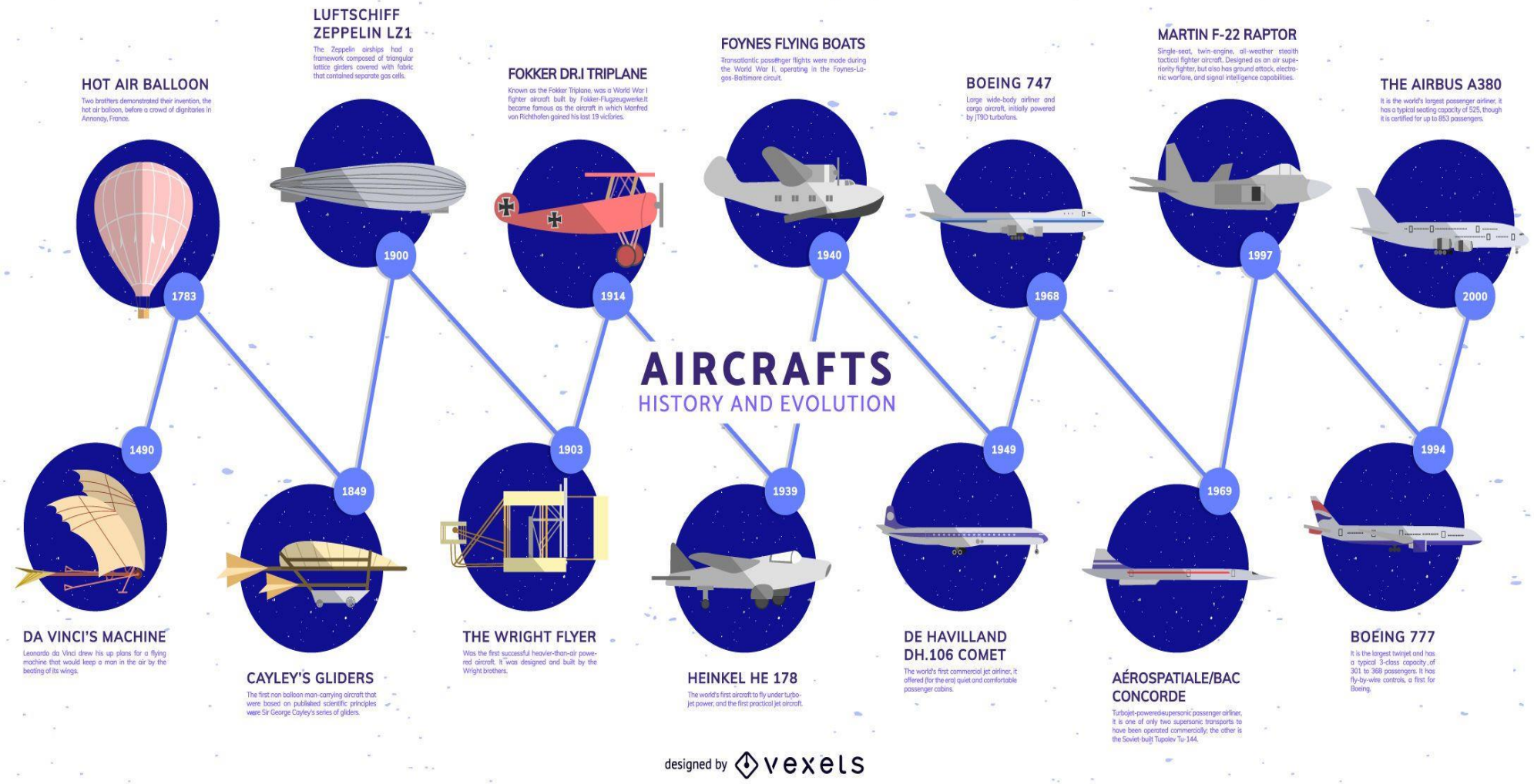
BENMABROUK Mohamed Ali

Chargé de la Direction de Réponse aux Urgences Informatiques et Assistance - ANSI

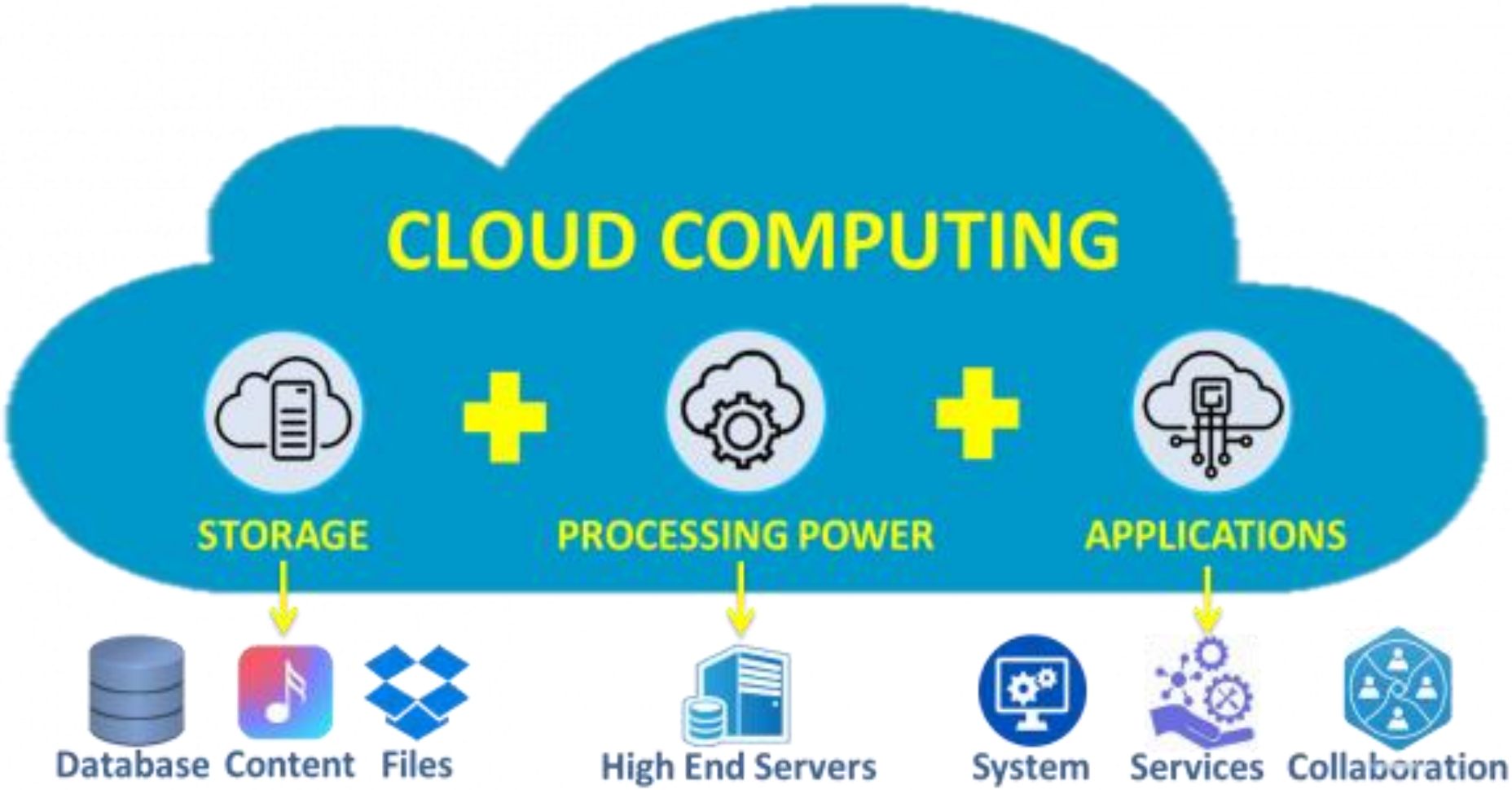
Plan

- Introduction
- Histoire: cloud computing, malware
- Maas
- Caas
- IA
- Solutions

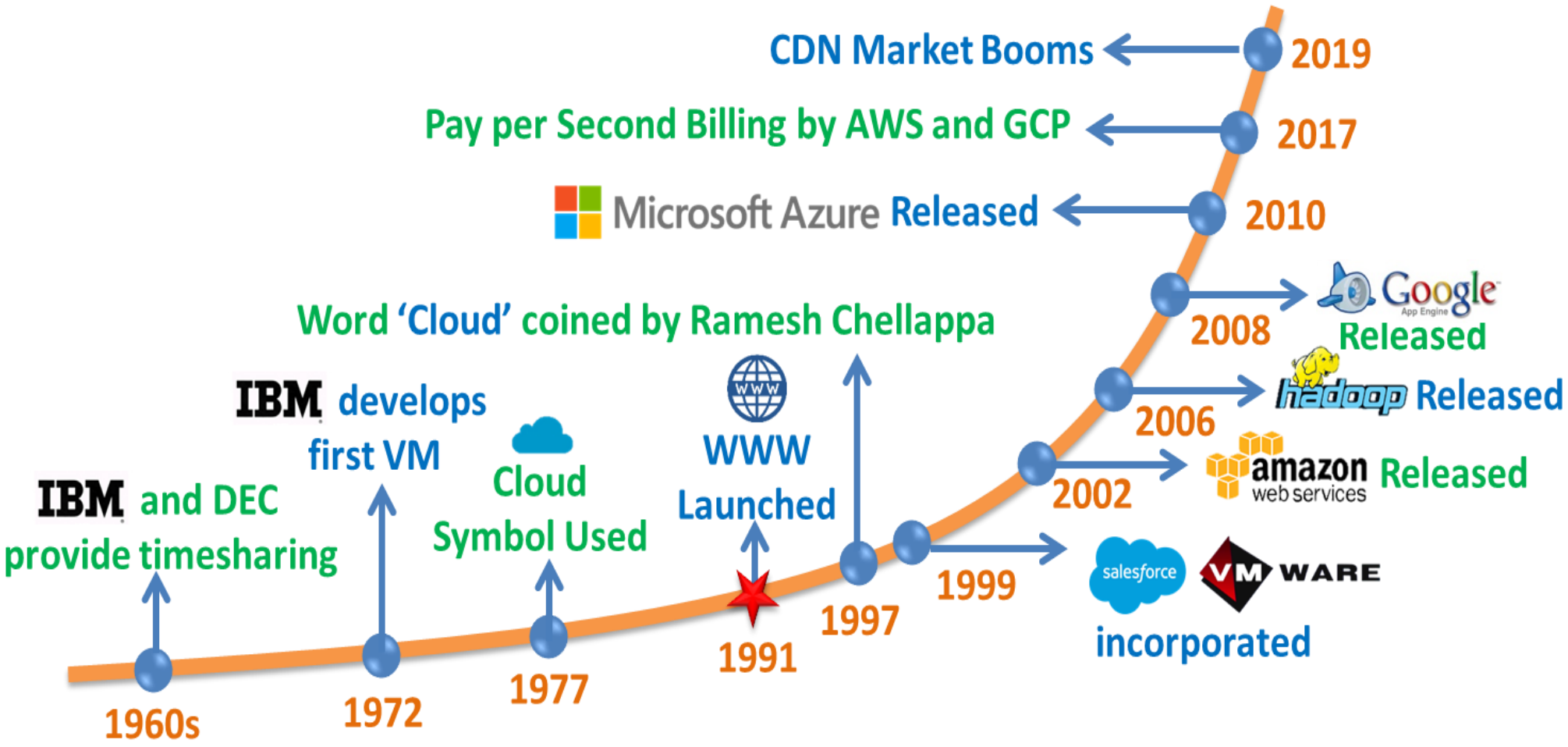
Introduction



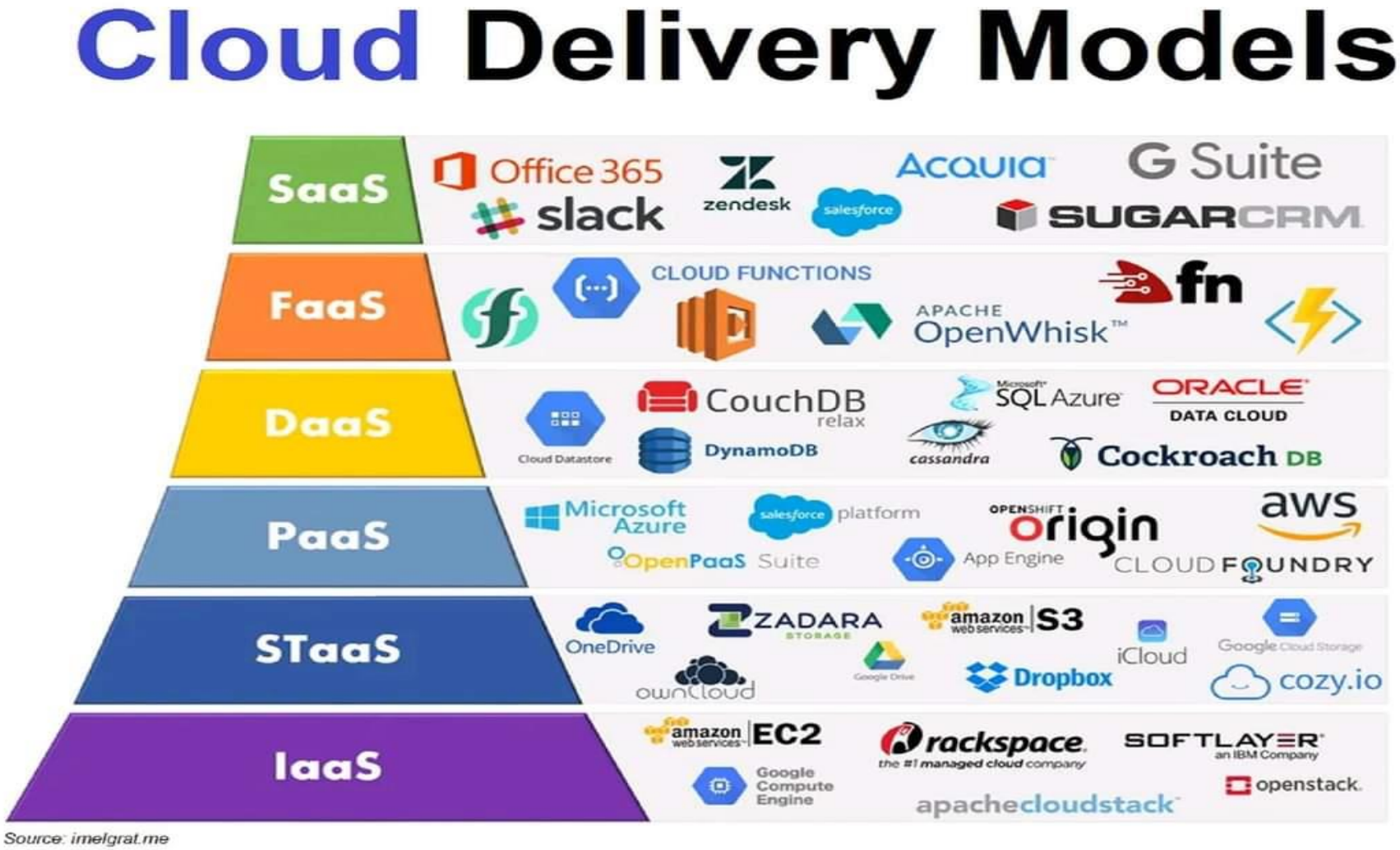
Histoire - Cloud Computing



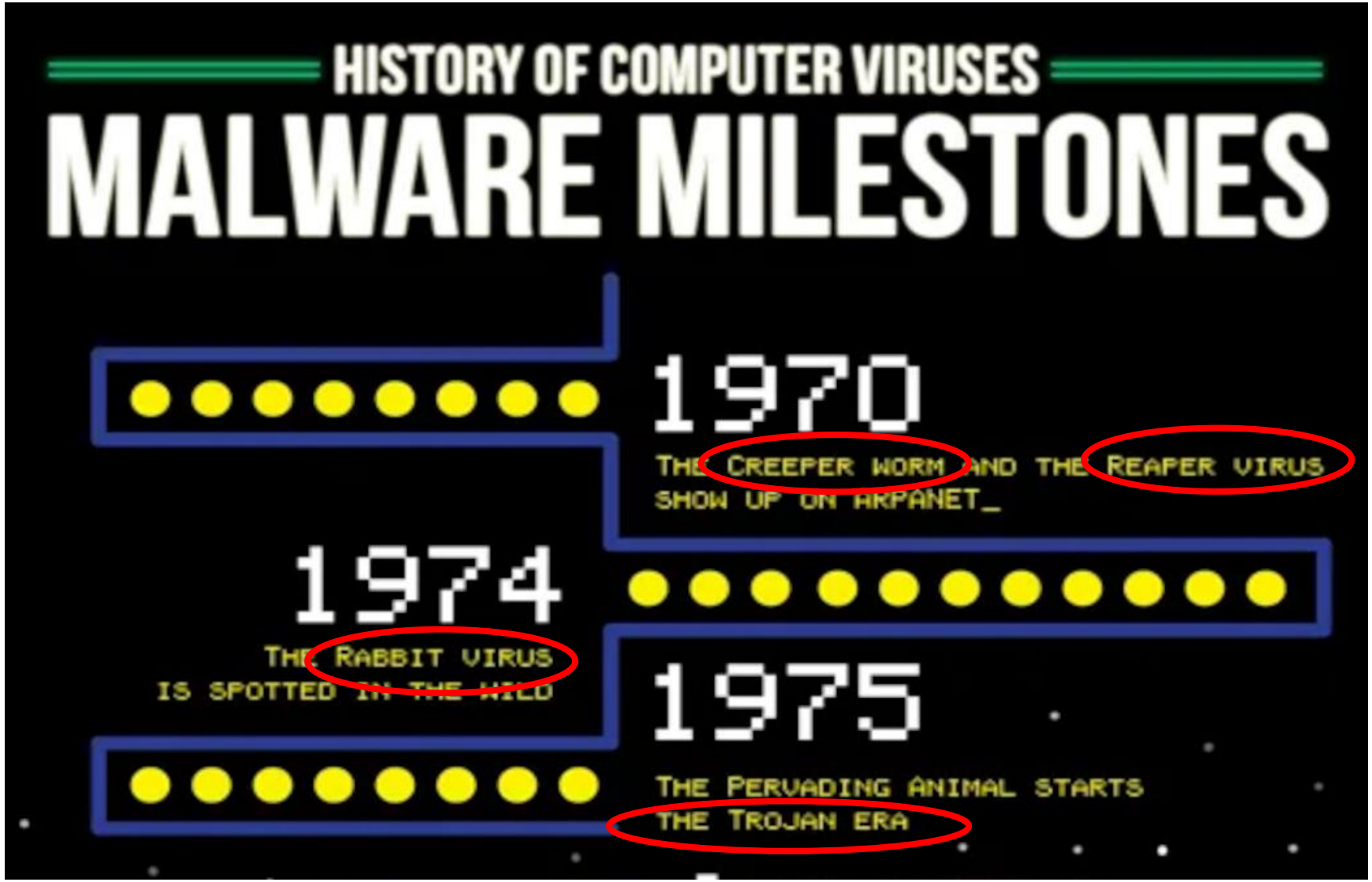
Histoire - Cloud Computing



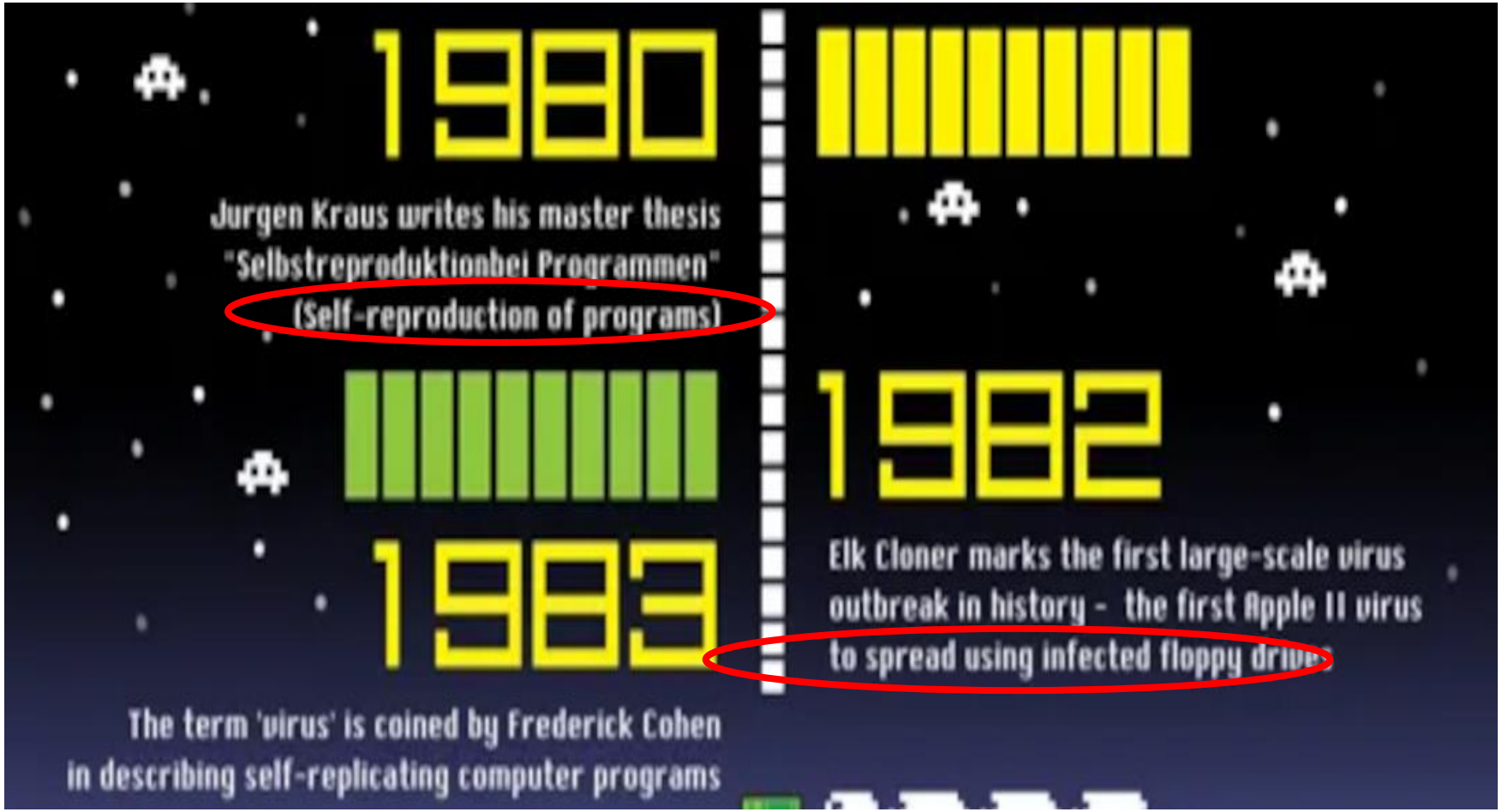
Histoire - Cloud Computing



Histoire des Malwares- Les premières années



Histoire des Malwares- Les premières années



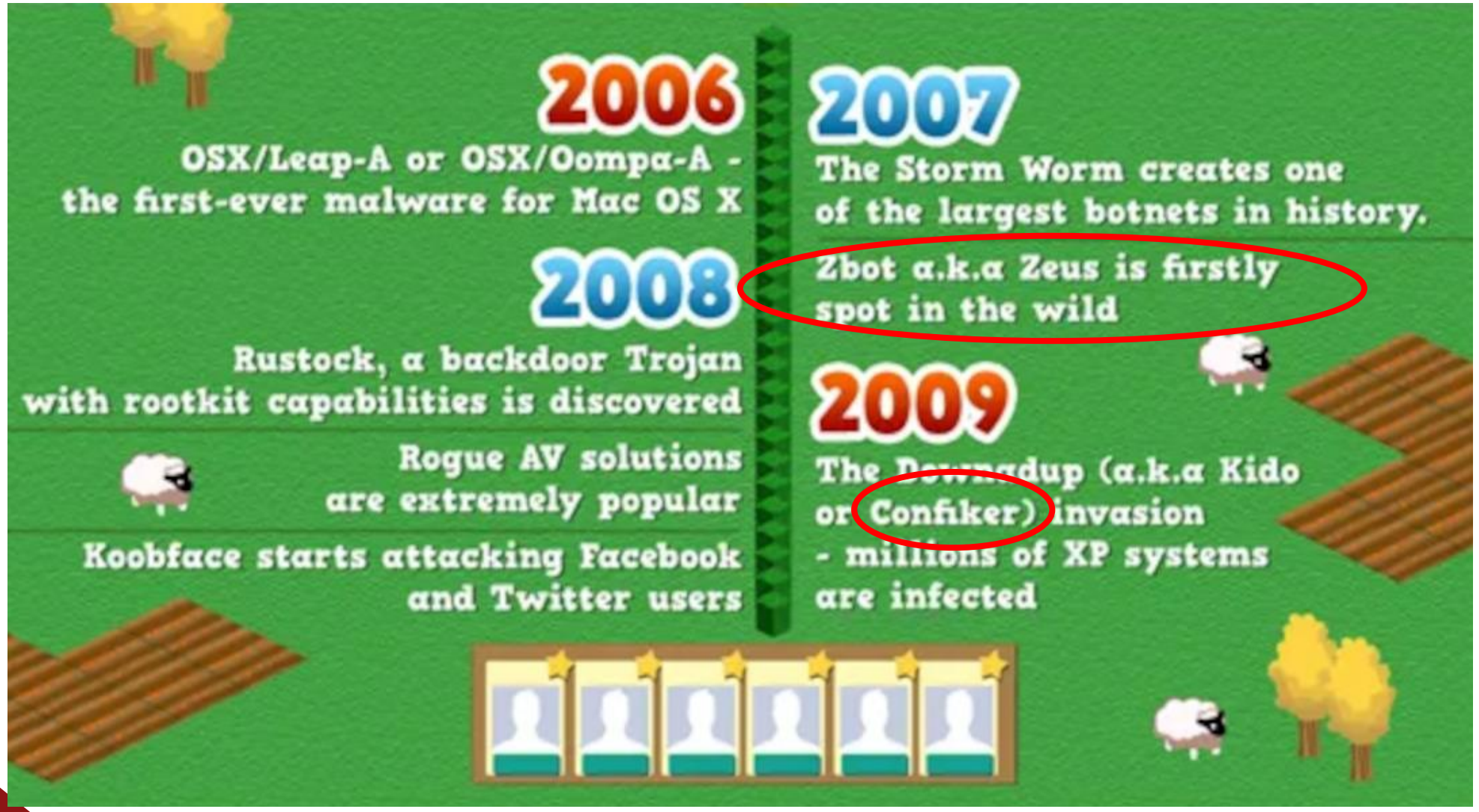
Histoire des Malwares- Les premières années

Histoire des Malwares- Les premières années

Histoire des Malwares- Les premières années

Histoire des Malwares — Toolkits et et les taux d'infection étonnants

Histoire des Malwares — Toolkits et et les taux d'infection étonnants



Histoire des Malwares – Sophistiqué, Espionnage + Cyber-armes

Histoire des Malwares – Sponsorisé, sophistiqué et rentable

2011/12: Reveton

Figure 4: Reveton Ransom Screen with MoneyPak instructions

Histoire des Malwares – Sponsorisé, sophistiqué et rentable

2013: CryptoLocker - the arrival of cryptocurrency as a payment option

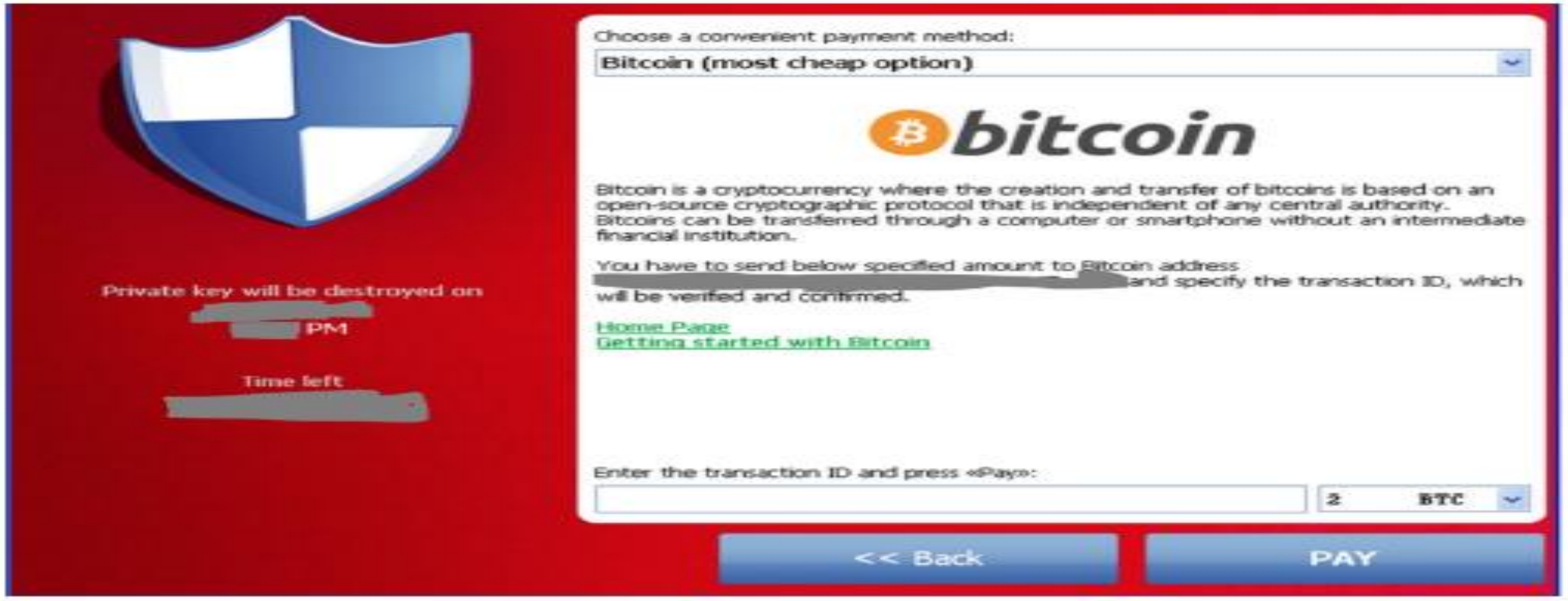
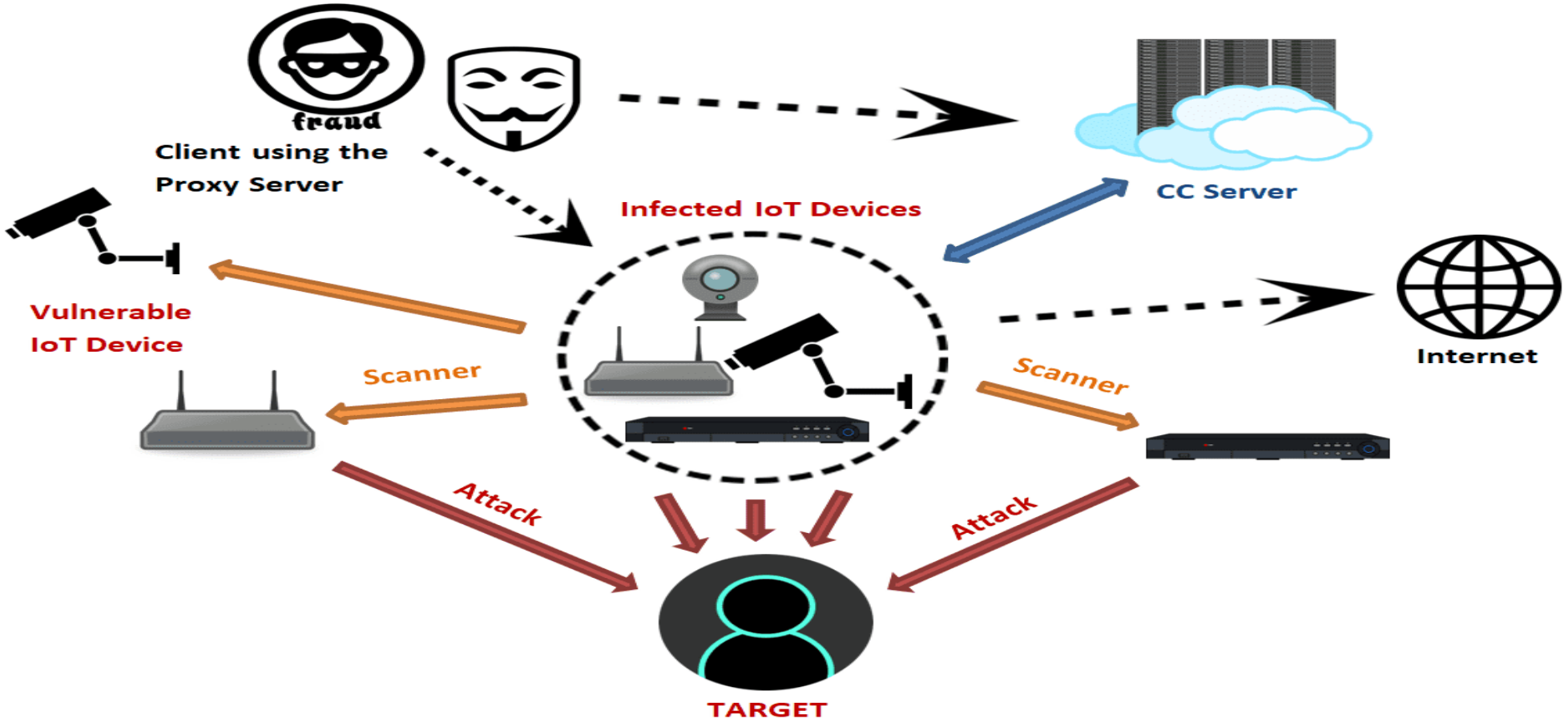


Figure 6: CryptoLocker bitcoin ransom demand

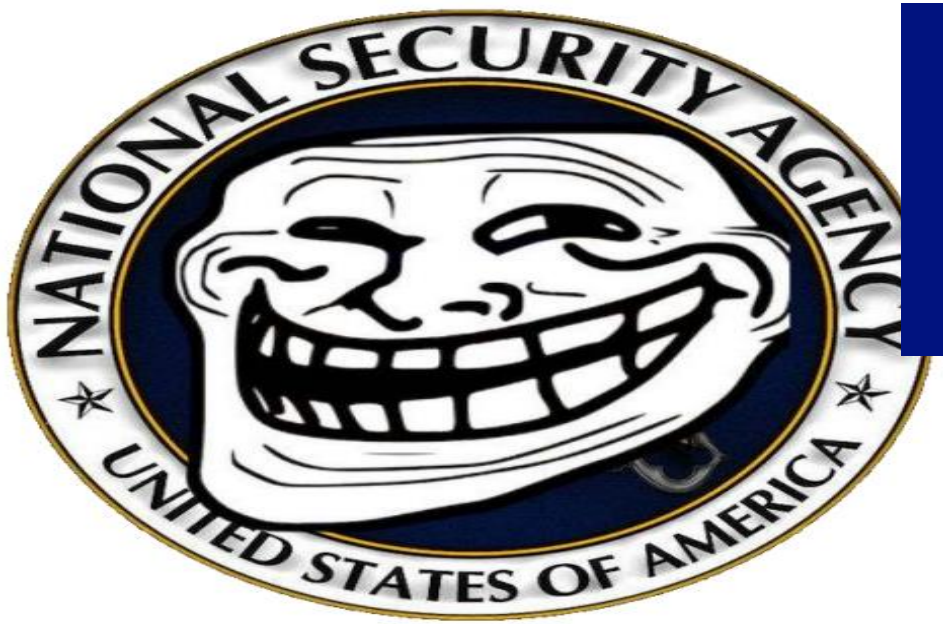
Histoire des Malwares – Sponsorisé, sophistiqué et rentable

2016: Mirai – First Botnet to target IoT devices



Histoire des Malwares – Sponsorisé, sophistiqué et rentable

2017: ShadowBrokers (NSA), WannaCry, Petya/NotPetya,and not disclosing vulnerabilities

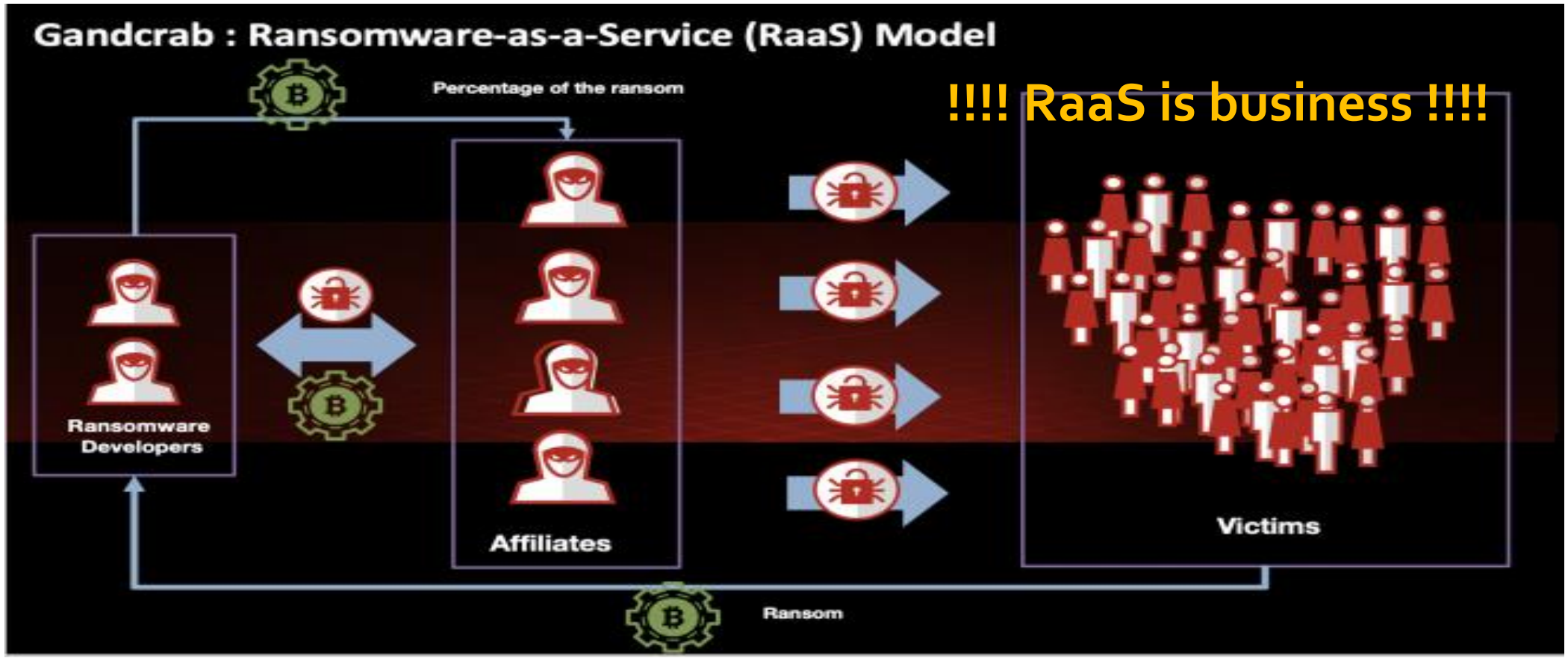


Histoire des Malwares – Sponsorisé, sophistiqué et rentable

2017/2018: XMRig - Mining for crypto

Histoire des Malwares – Sponsorisé, sophistiqué et rentable

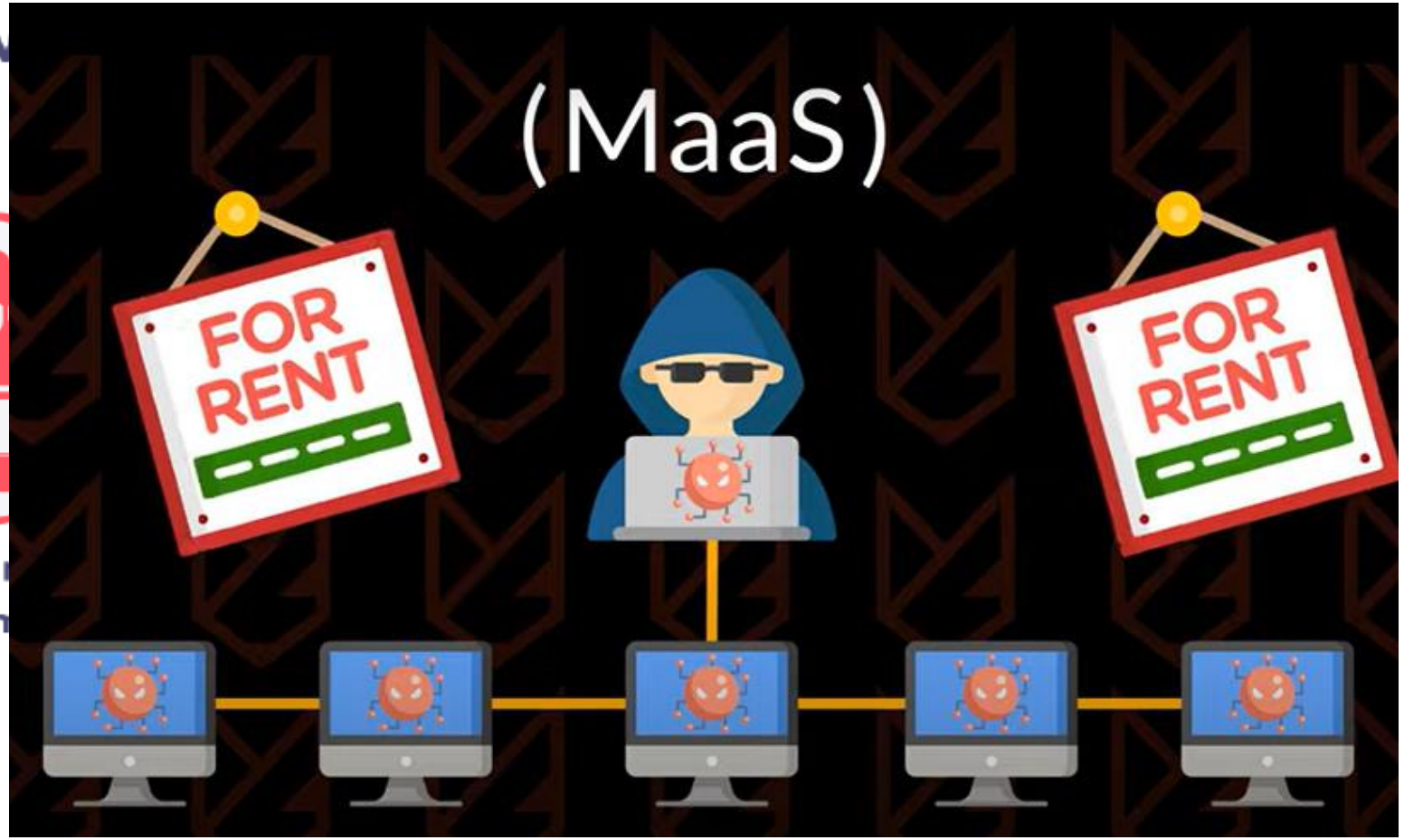
2019: GandCrab and the emergence of **Ransomware as a Service**



2021: Malware as a Service (MaaS)

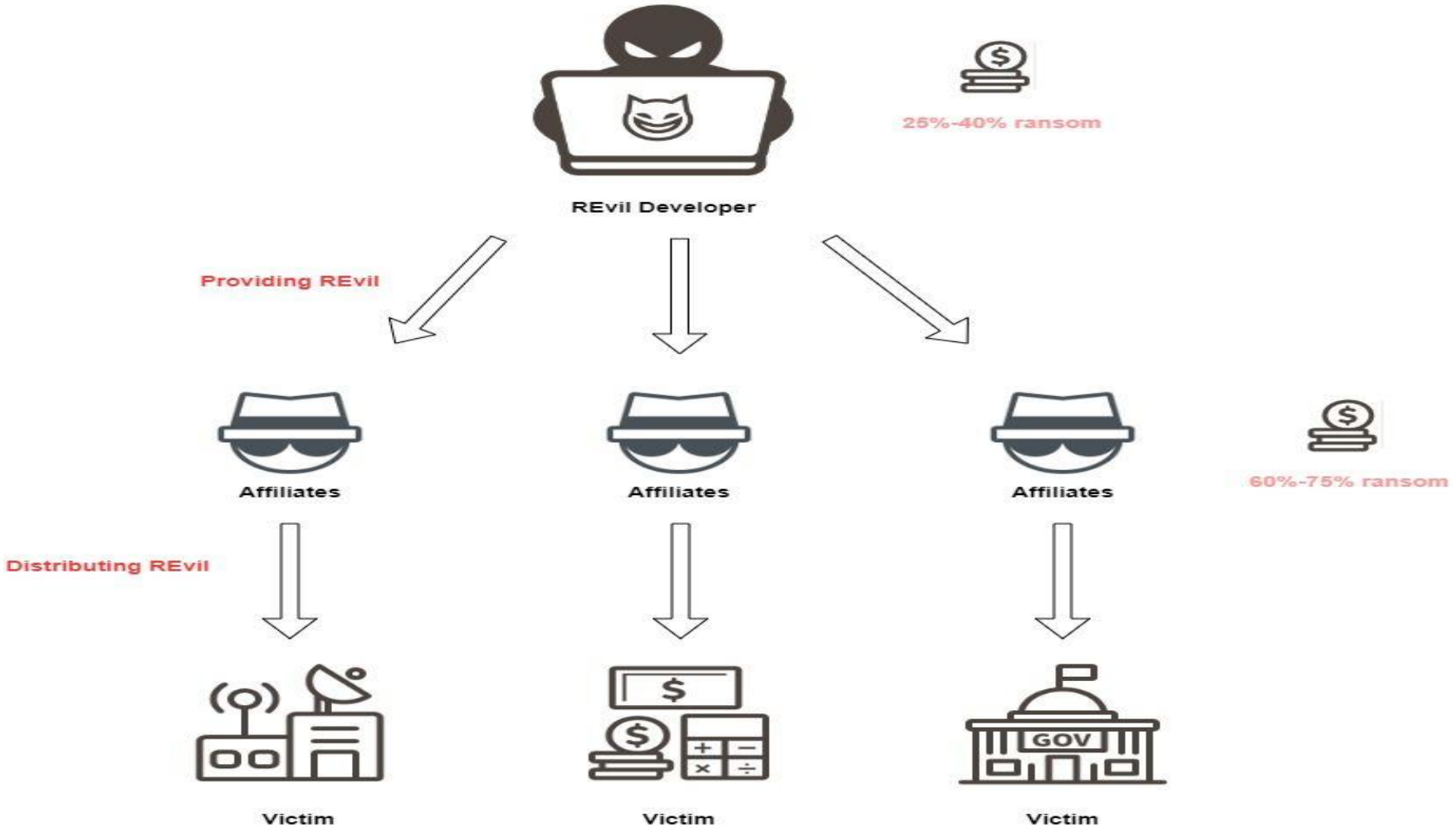
Malw

Malwa
developm

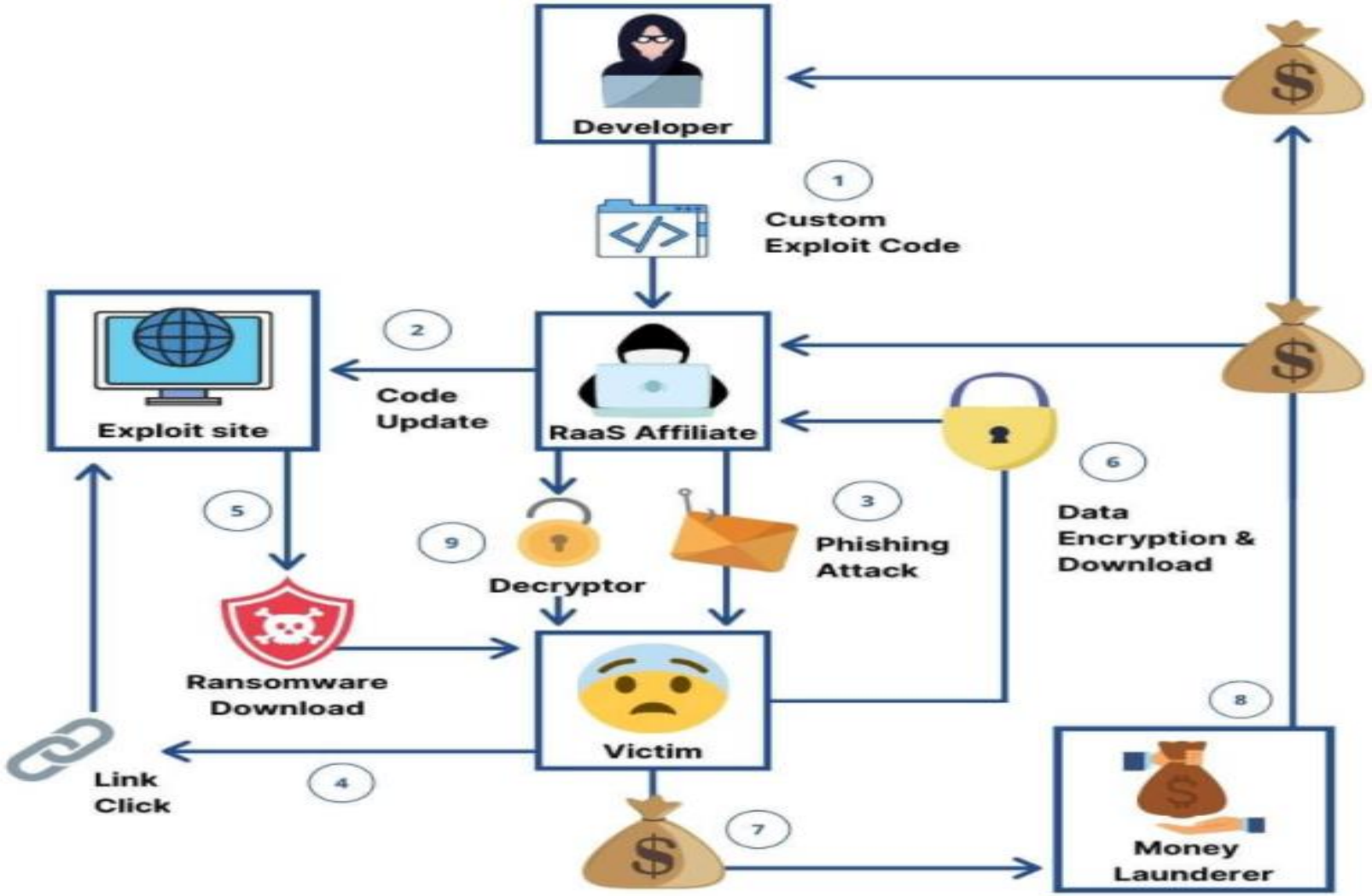


Exemple de Maas : DarkSide ($5 million)

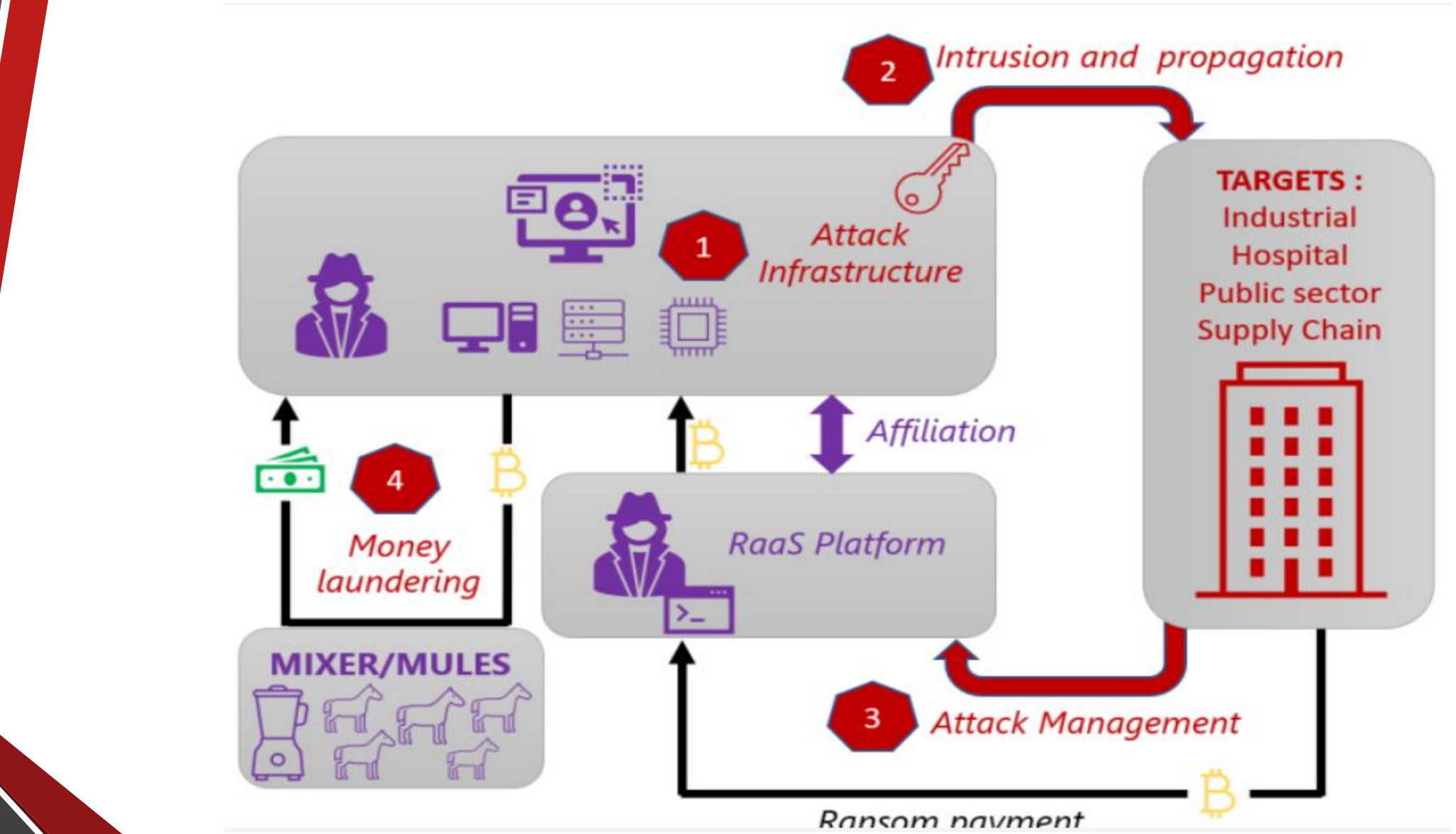
Exemple de Maas : Revil ($11 million)



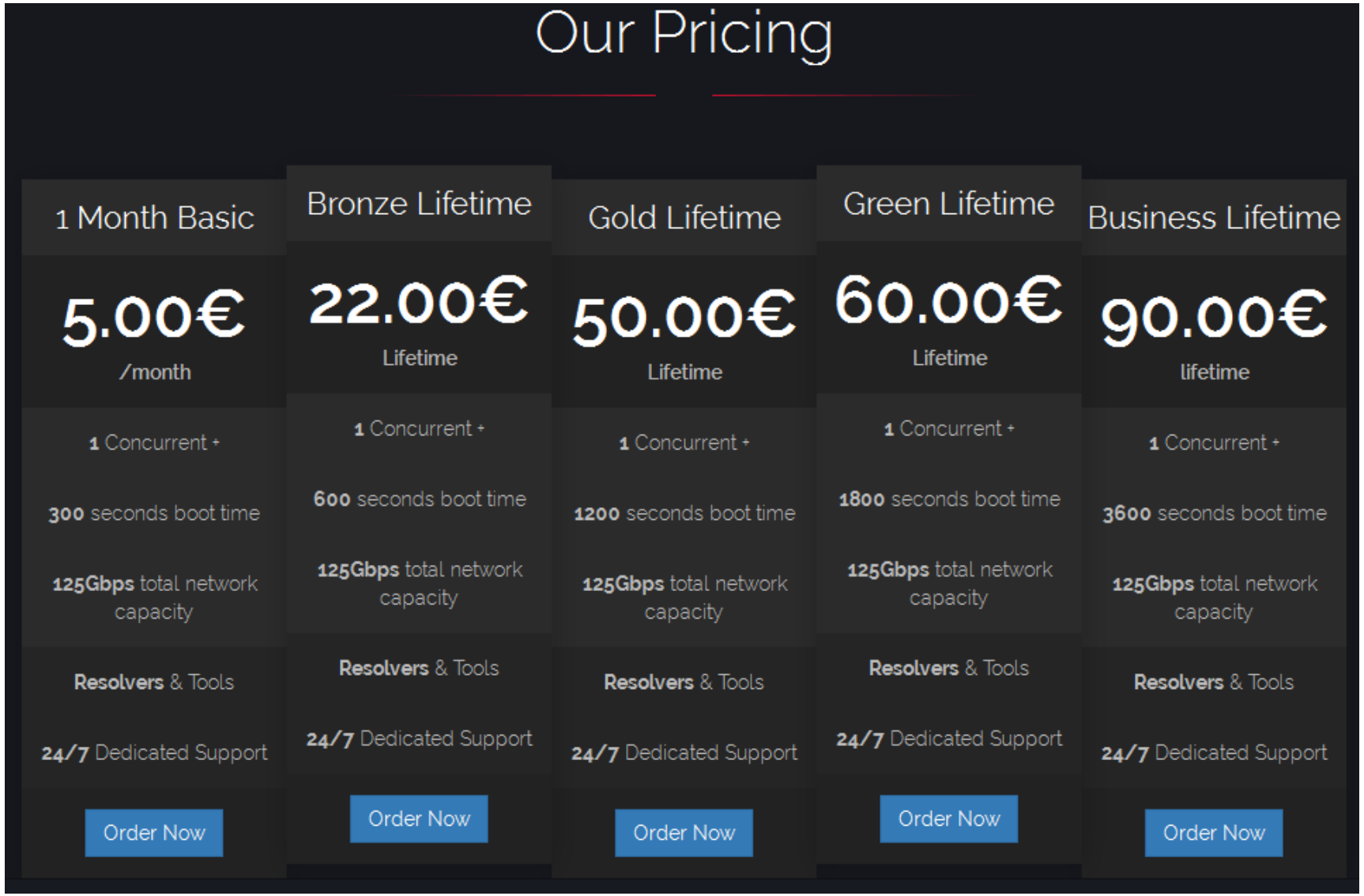
Exemple de Maas : LockBit



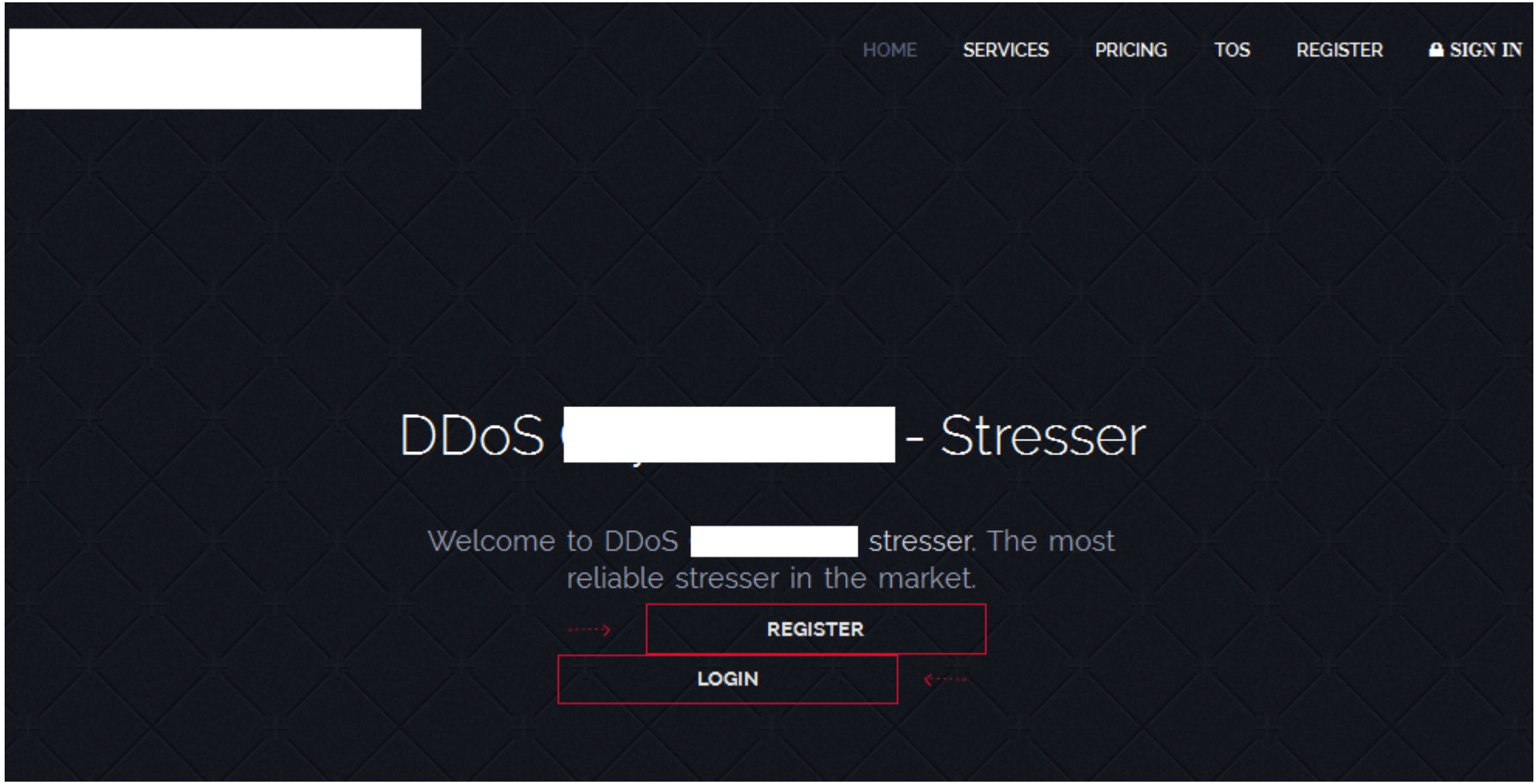
Exemple de Maas : Conti ($180 million)



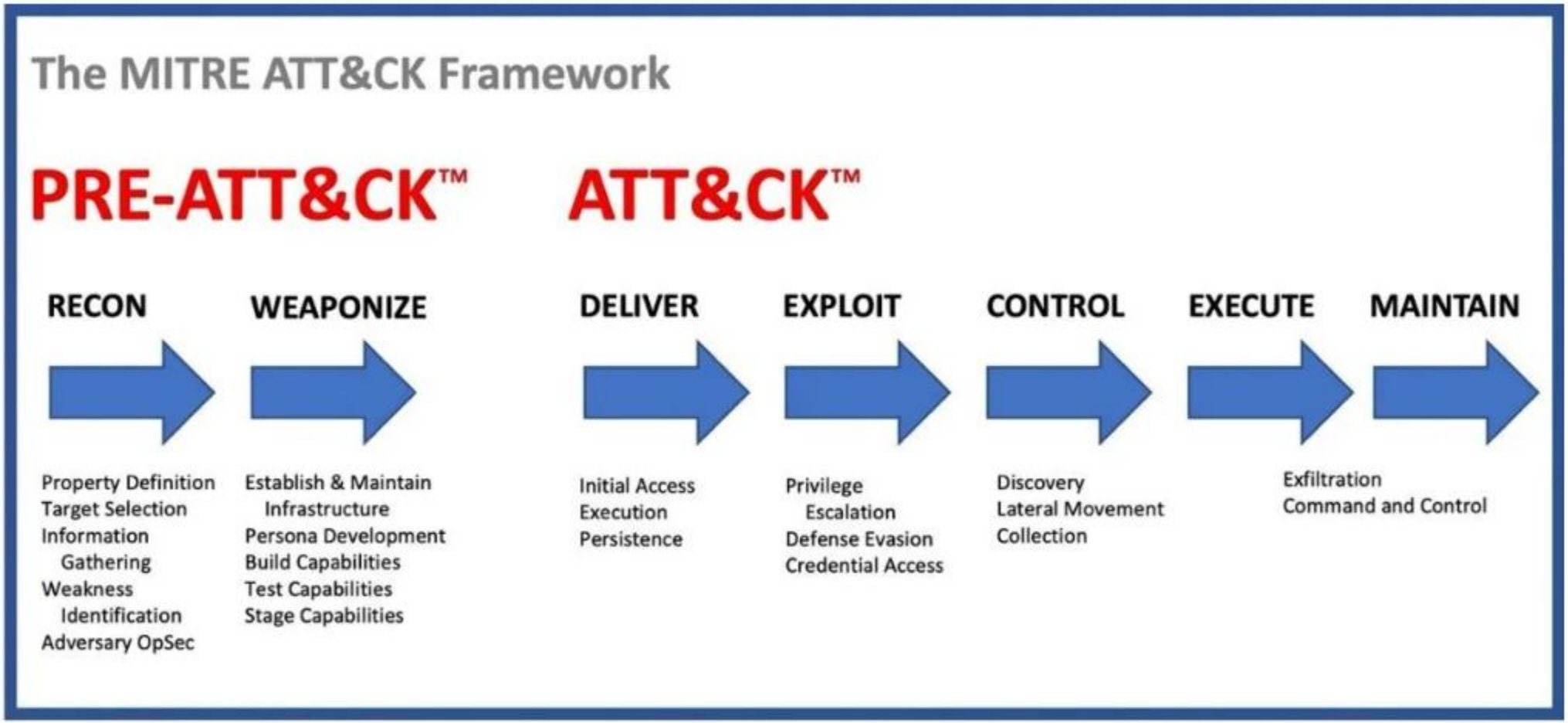
DDoS as a Service



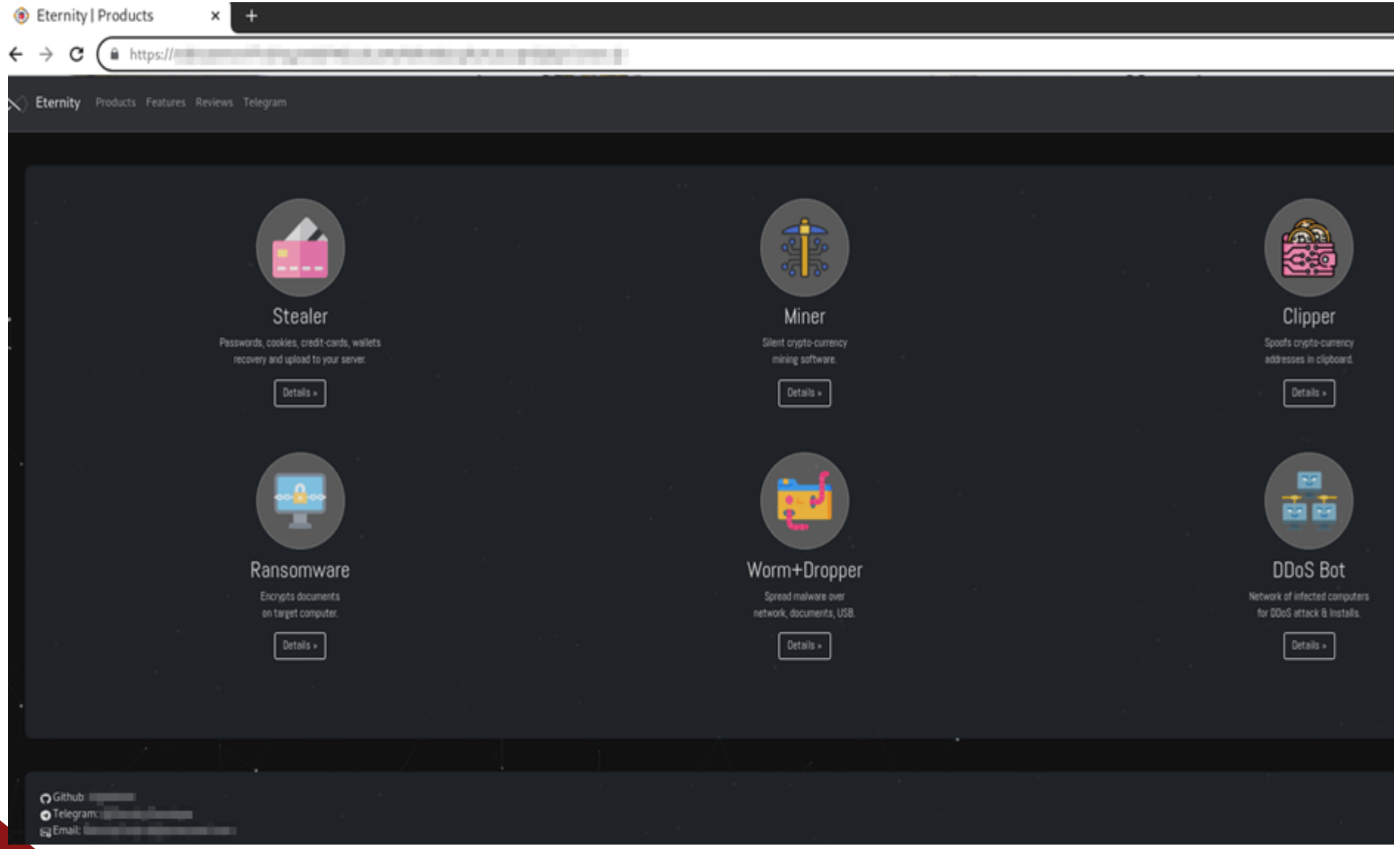
DDoS as a Service - Exemple



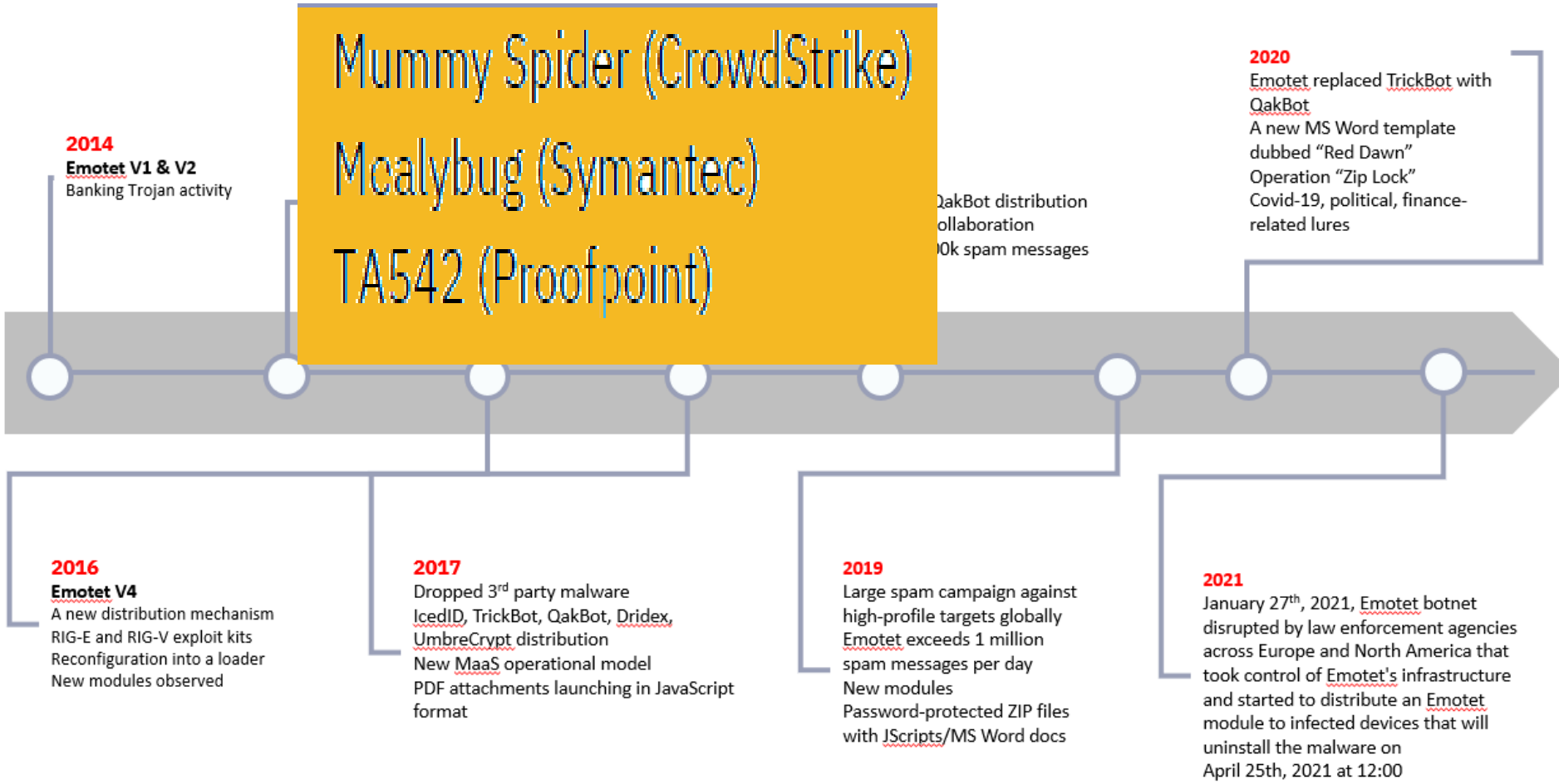
2021/2022: Crime-as-a-Service (CaaS)



2022: Crime-as-a-Service (CaaS)



Caas - Exemple : Emotet Family



IA: Social Engineering – BEC - Phishing

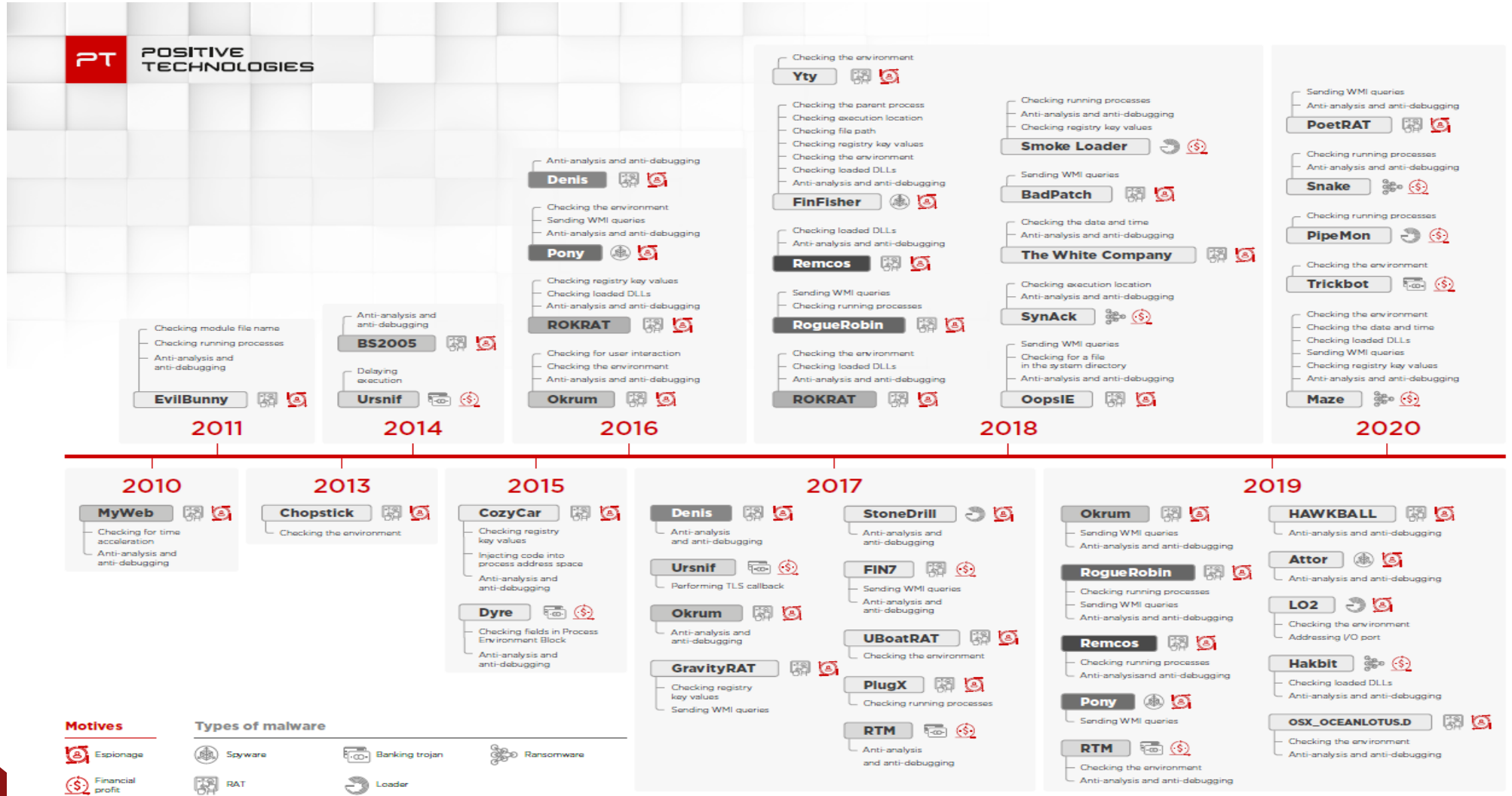
IA: Evasion Technics

A Malware Obfuscation AI Technique to Evade Antivirus Detection in Counter Forensic Domain

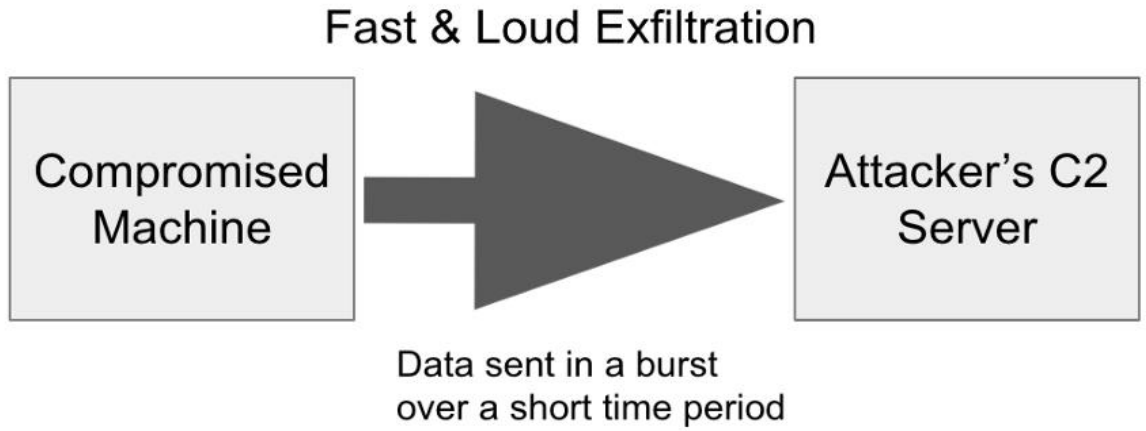
In this paper, we introduce multiple techniques consists of four stages that aid a malware; to **avoid anti-malware tools,** these techniques were mainly developed to provide a **high evasion rate against anti-malware systems via dynamic analysis techniques**. The evasion rate success of our samples were tested through (Kaspersky, Virustotal and Virusscan), then the result of our experiment were compared with other obfuscation techniques to stand on the success level of the experiment as well as extracting the strength and weakness points for any possible future works.

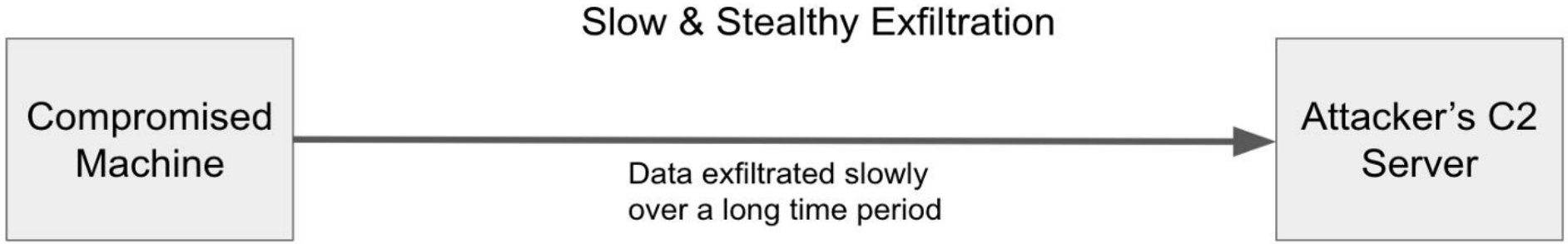
https://link.springer.com/chapter/10.1007/978-3-030-52067-0_27

IA: Evasion Technics

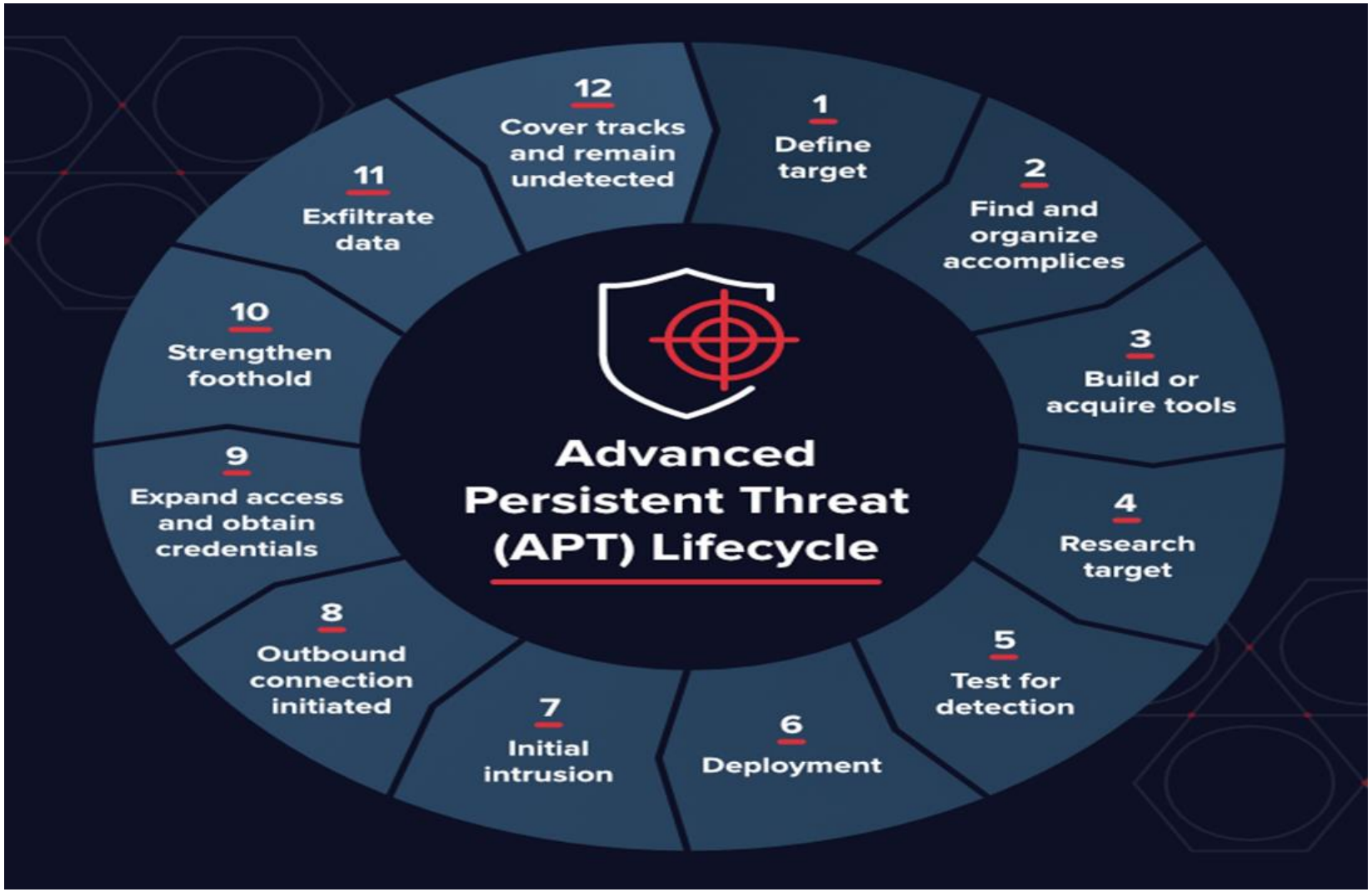


IA: Data Exfiltration





APT


Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected

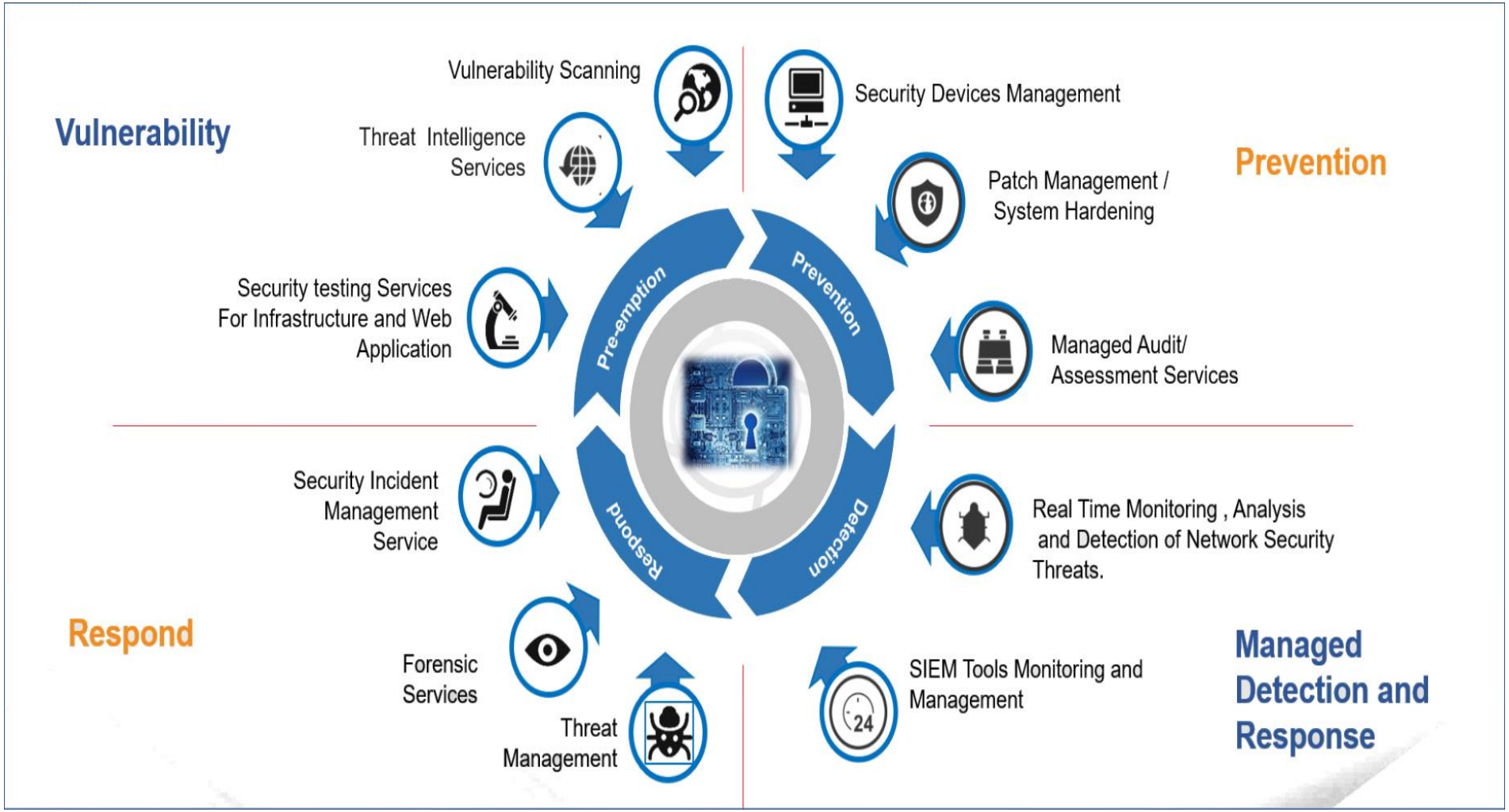
Cyber War

Conti siding with Russia over the invasion of Ukraine

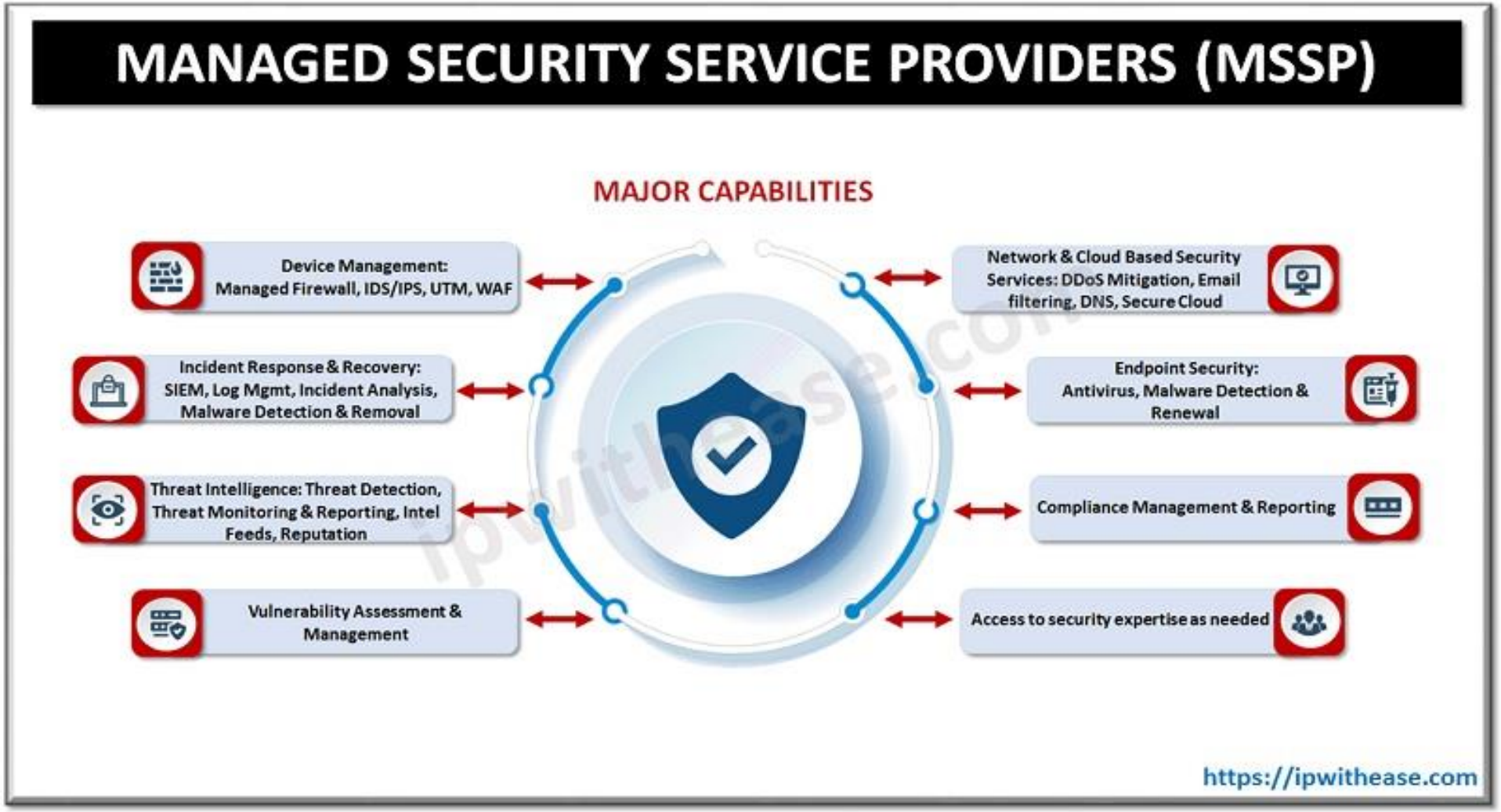
Source: BleepingComputer

Solutions ?

Solutions: Protection contre Cybercrime



Solutions: MSSP



Solutions: Cybersecurity as a service

Global Cybersecurity As A Service Market Trends, Applications, Analysis, Growth, And

Security as a Service (SECaaS) Overview

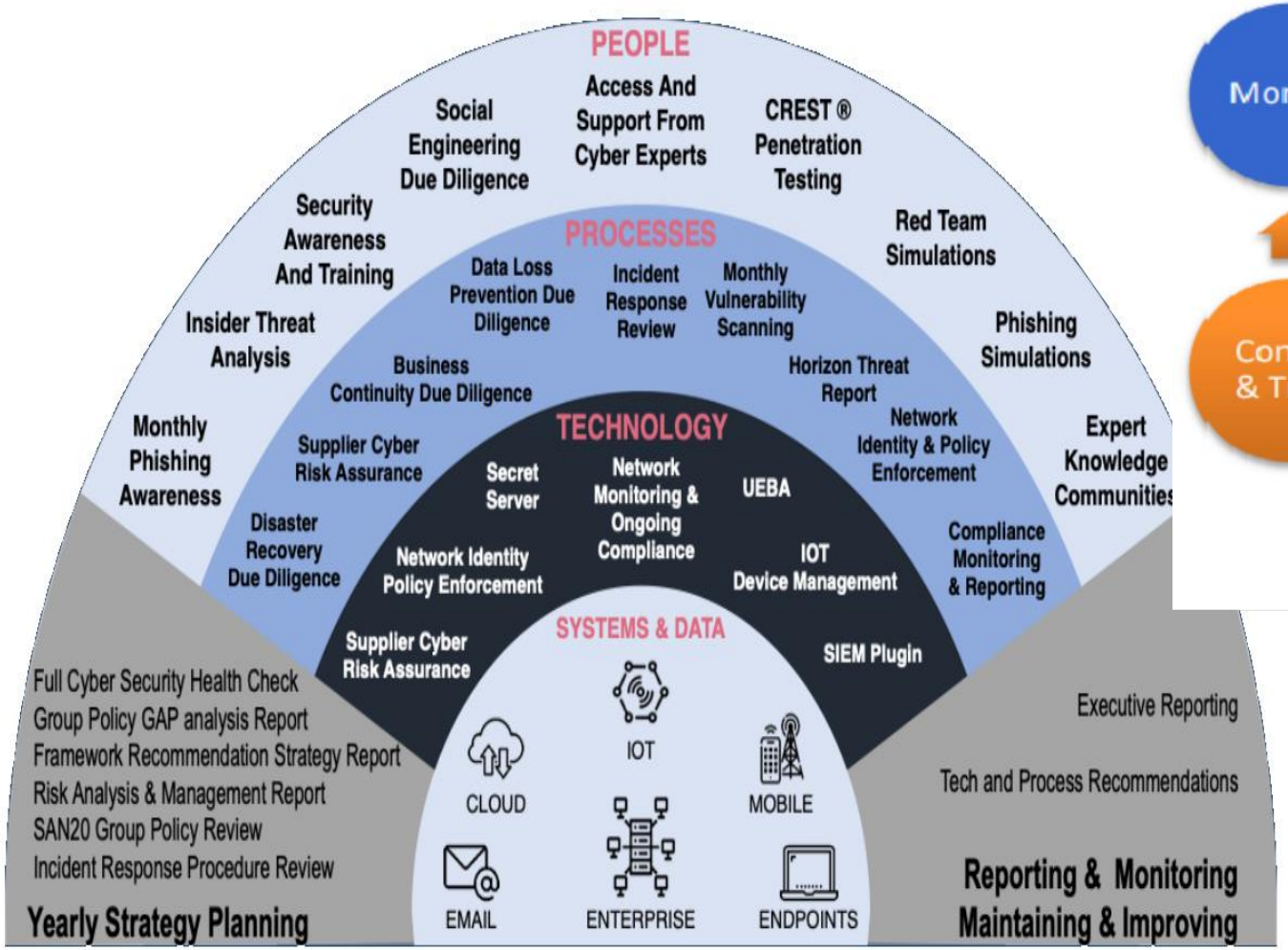
This slide depicts the overview of security as a service that helps organizations to outsource cybersecurity services from cloud providers, including its main components such as remote users, web data, internet, and web security as a service.

- Cloud-based approach for outsourcing cybersecurity services
- Subscription-based security service hosted by cloud providers, like Software as a Solution
- Method to relieve the in-house security team's obligations, expand security demands as the organization develops, and avoid the expenses and upkeep of on-premise alternatives
- Cloud-based solutions have become increasingly popular for corporate infrastructures
- Add text here
- Add text here

Types

- Continuous Monitoring, Data Loss Prevention (DLP), Email Security, Antivirus Management, Spam Filtering, Intrusion Protection, Security Assessment, Network Security, and so on
- Add text here

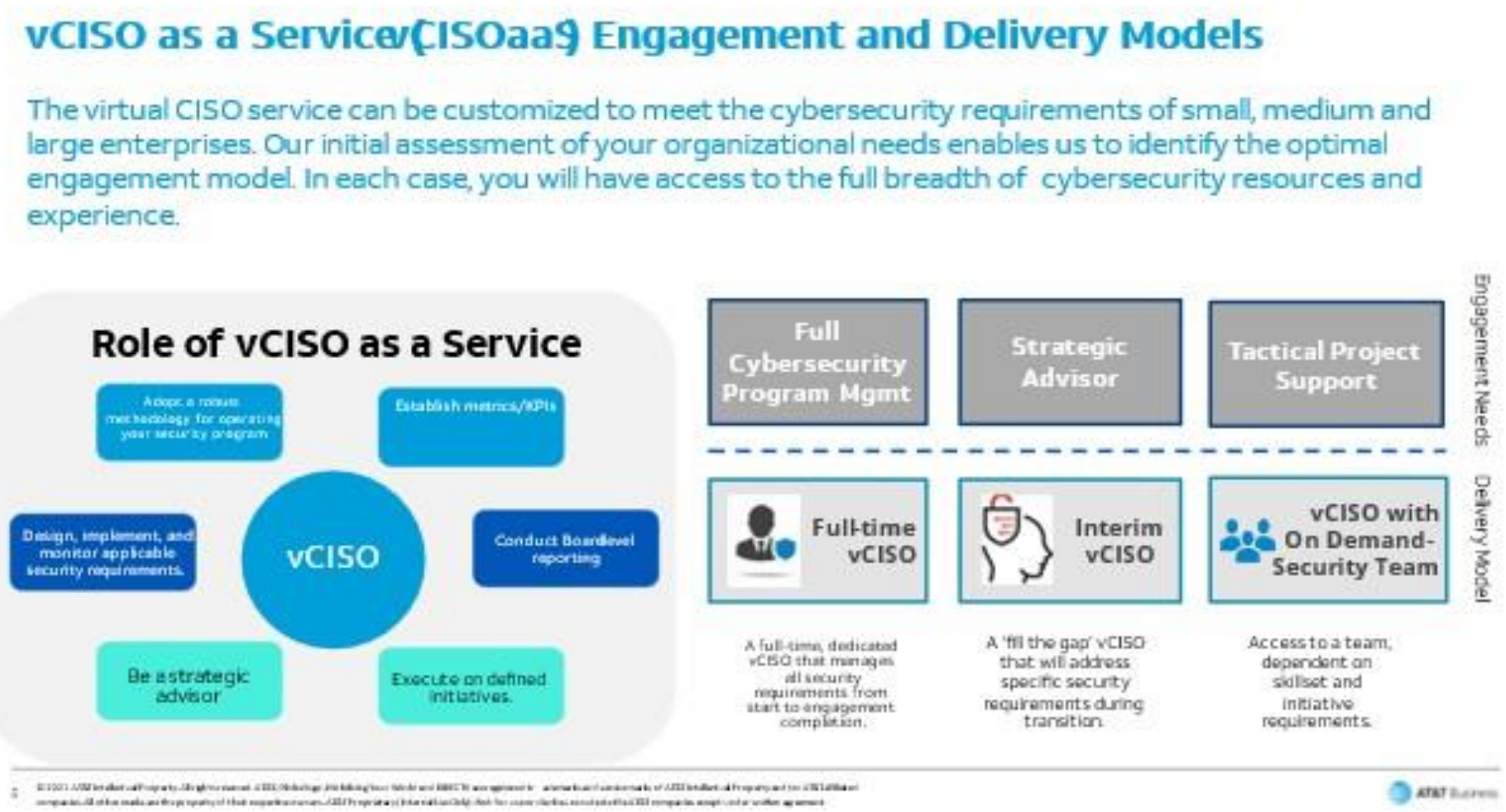
Solutions: Cybersecurity as a service



Solutions: Cybersecurity as a service

Company Type	Monthly Subscriptions Starting From:			
	Small	Medium	Large	Enterprise
	< 250*	< 500*	< 1000*	> 1000*
Monthly Subscription	Starting from $3k-6k+	Starting from $6k-10k+	Starting from $10k-20k+	Starting from $20k to 50K+

2022: A lasting trend: CISO As a Service



CTI aaS

KEY FEATURES

CONTEXTUALIZED THREAT INTELLIGENCE

- Customer exposure scanning - data leakage, attack anticipation
- Threat landscape - advisory reports
- Vulnerability details pertaining to customer's technology stack
- Identification and take down of phishing domain

CONTEXTUALIZED IOC'S

- Customer and industry specific IoC
- Consumption of IoC - feed integration in existing security products

COMPREHENSIVE THREAT INDICATOR SCORING METHODOLOGY

- Providing high confidence IoC reducing false positives
- Powered by AI and machine learning to analyses massive amount of threat intel data

A COMPREHENSIVE PLATFORM INTEGRATED WITH COMMERCIAL AND OPEN SOURCE THREAT INTEL

- Centralize and contextualize variety of threat data
- Machine learning and AI based search platform to search across dark web, social media and underground forums
- Based around open standards for consumption by existing security tools

Merci de votre attention

Q&A