

Malware as a Service

MaaS

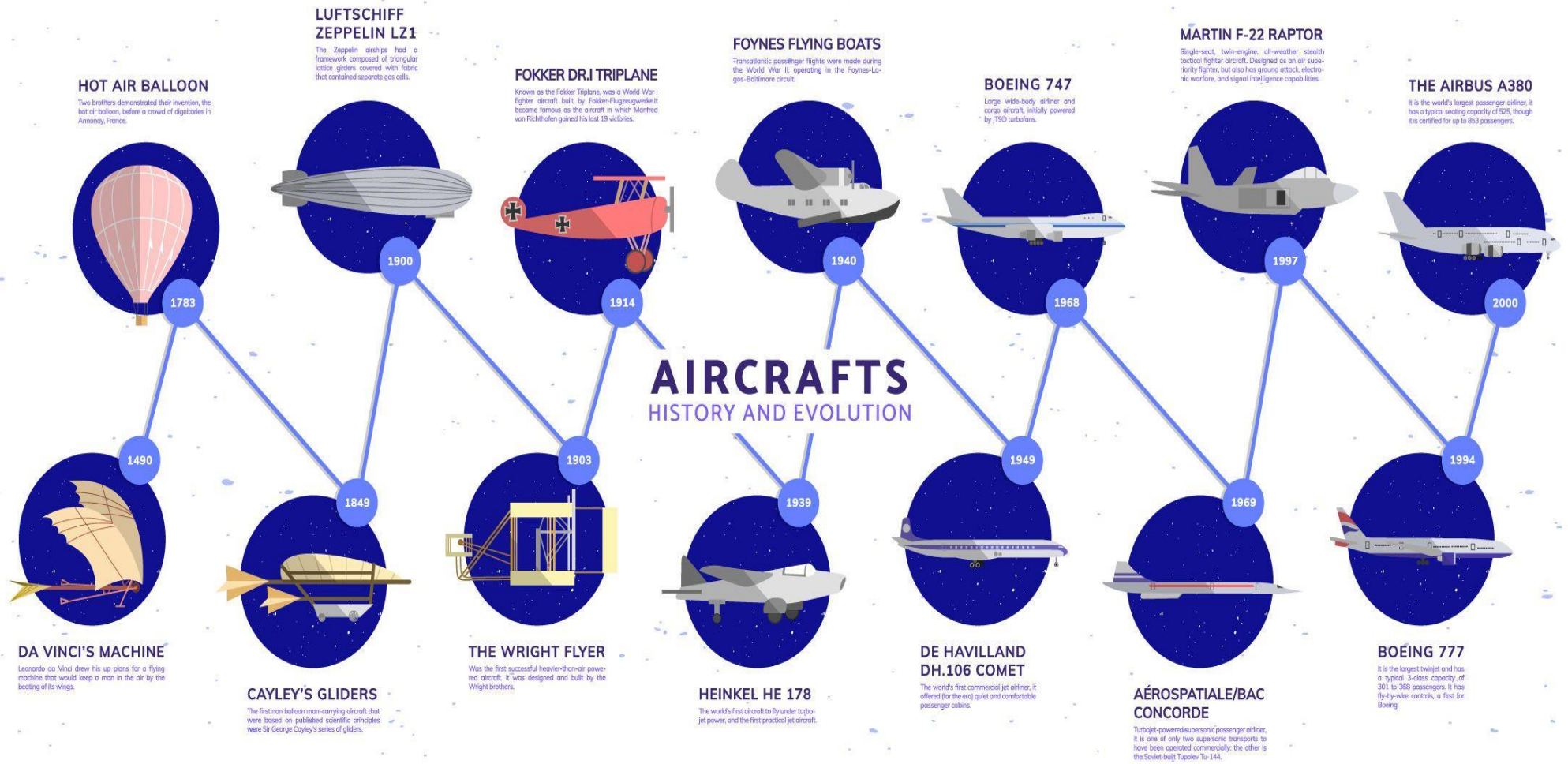
BENMABROUK Mohamed Ali

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

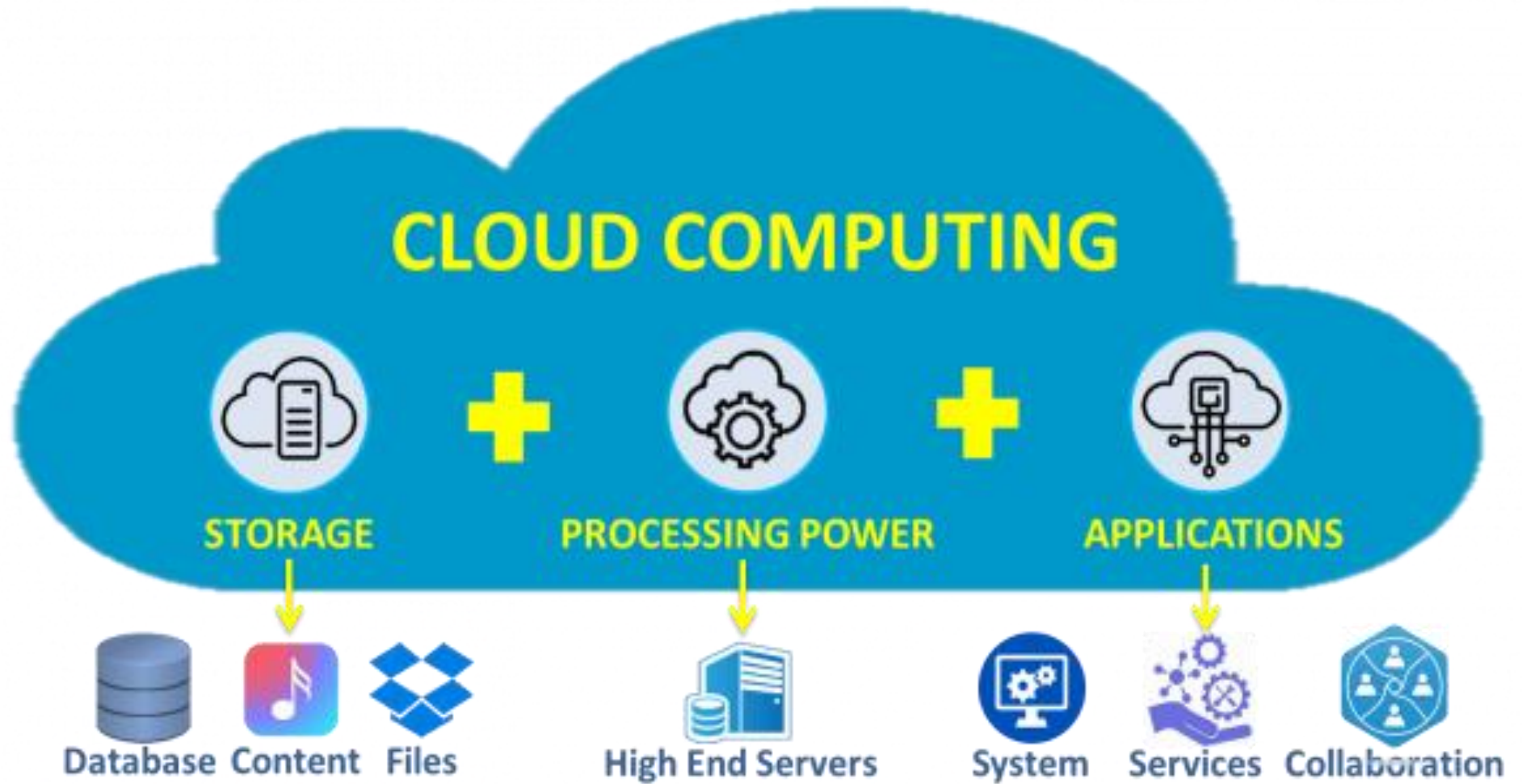
Plan

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

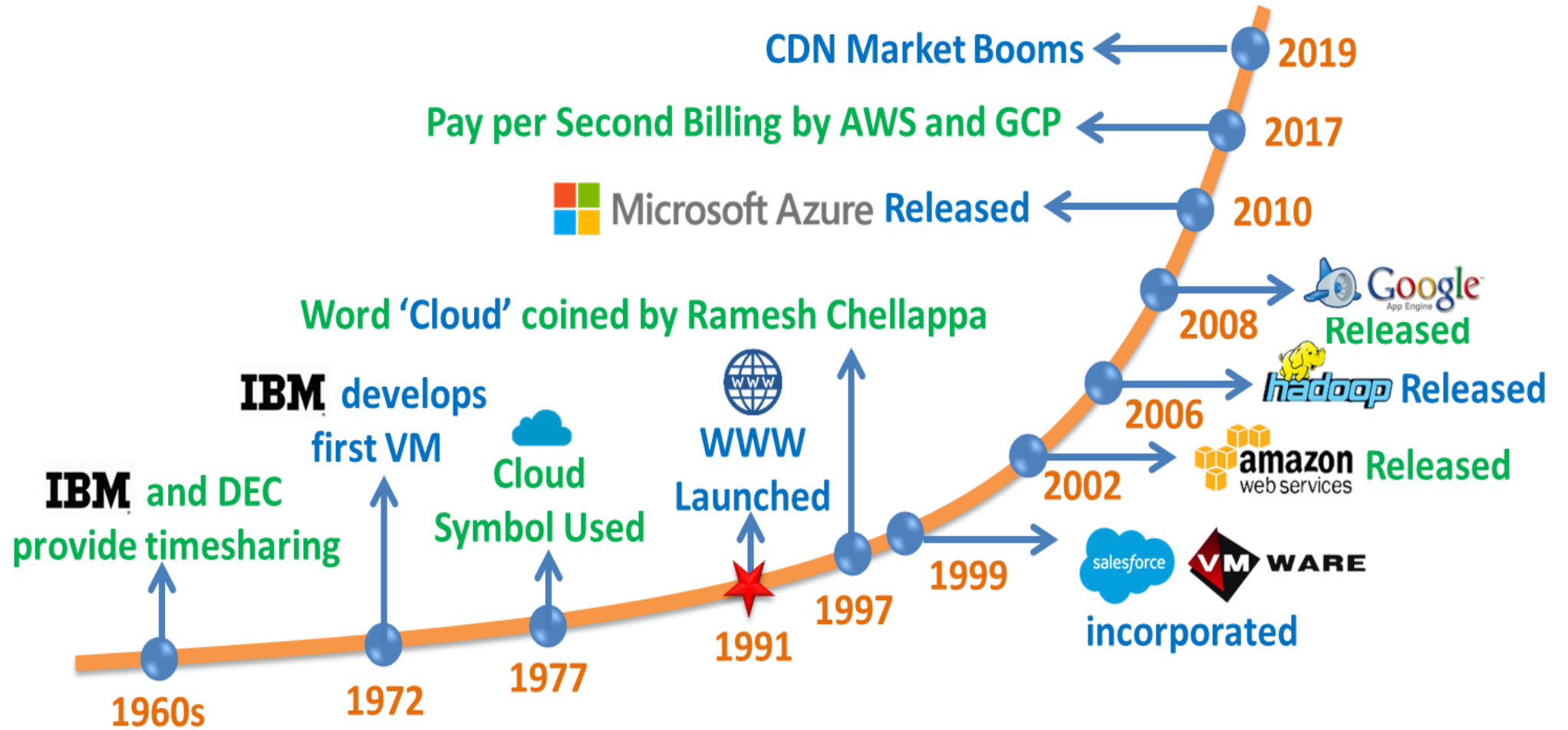
Introduction



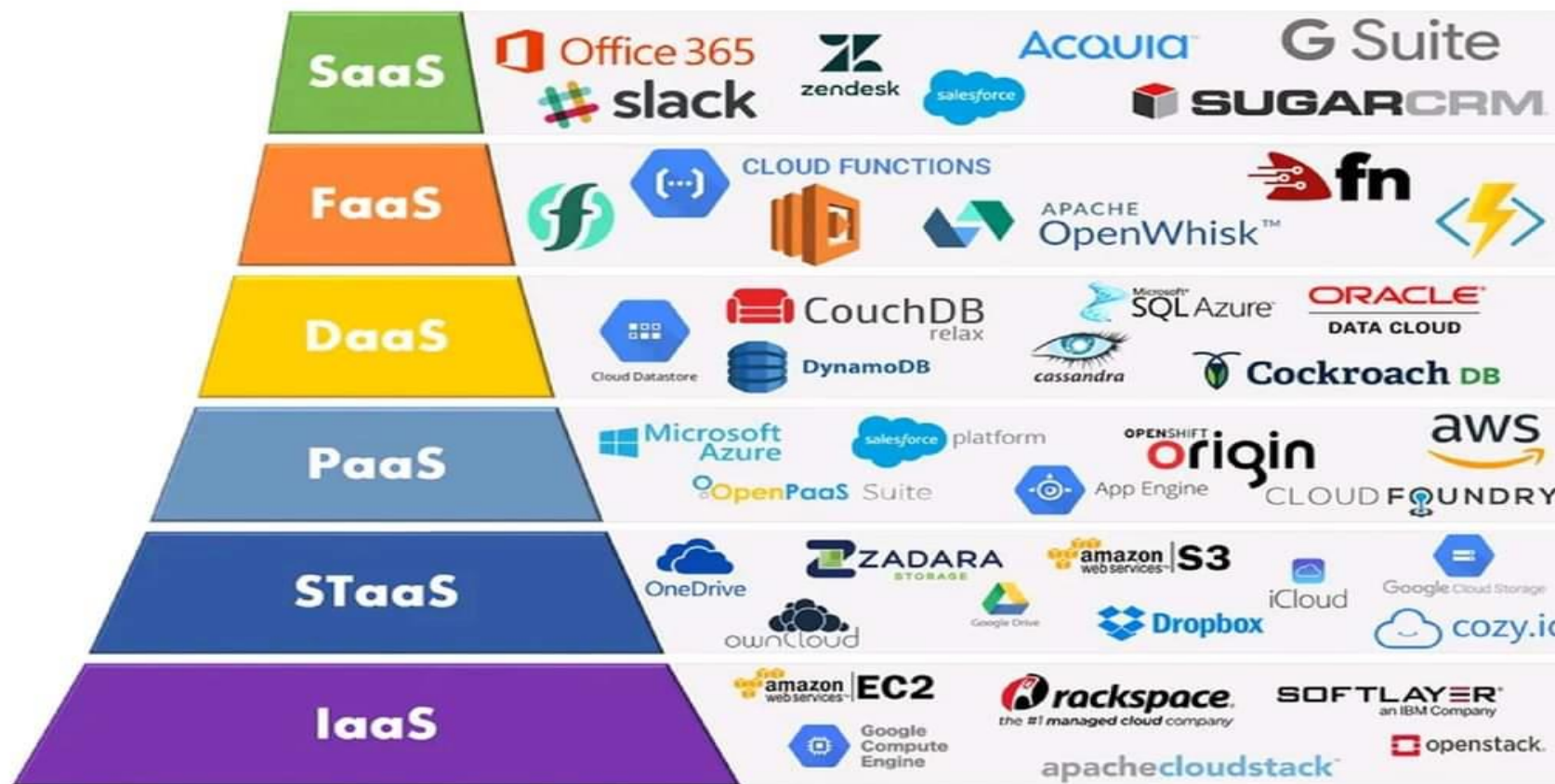
Histoire - Cloud Computing



Histoire - Cloud Computing

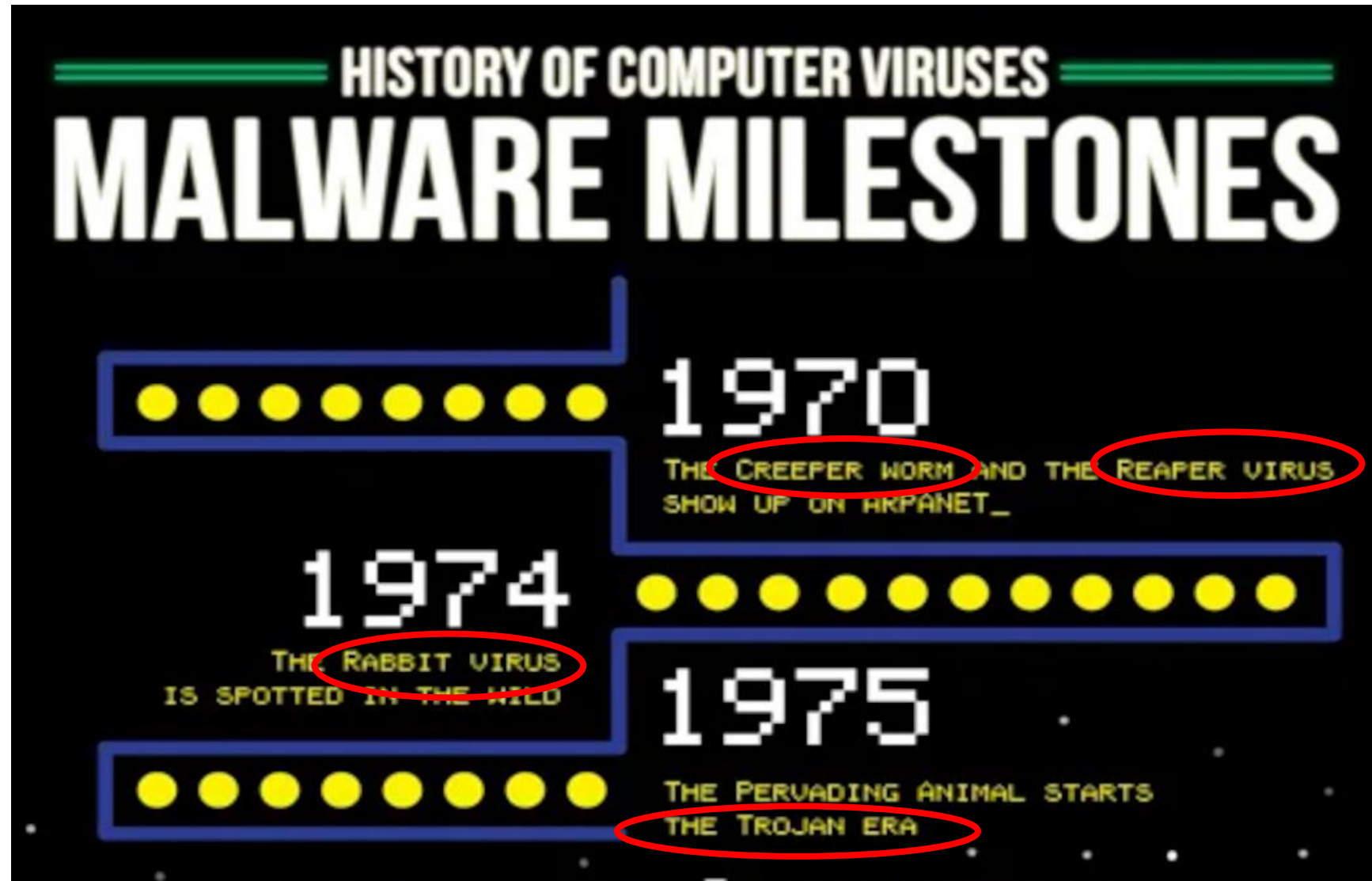


Cloud Delivery Models

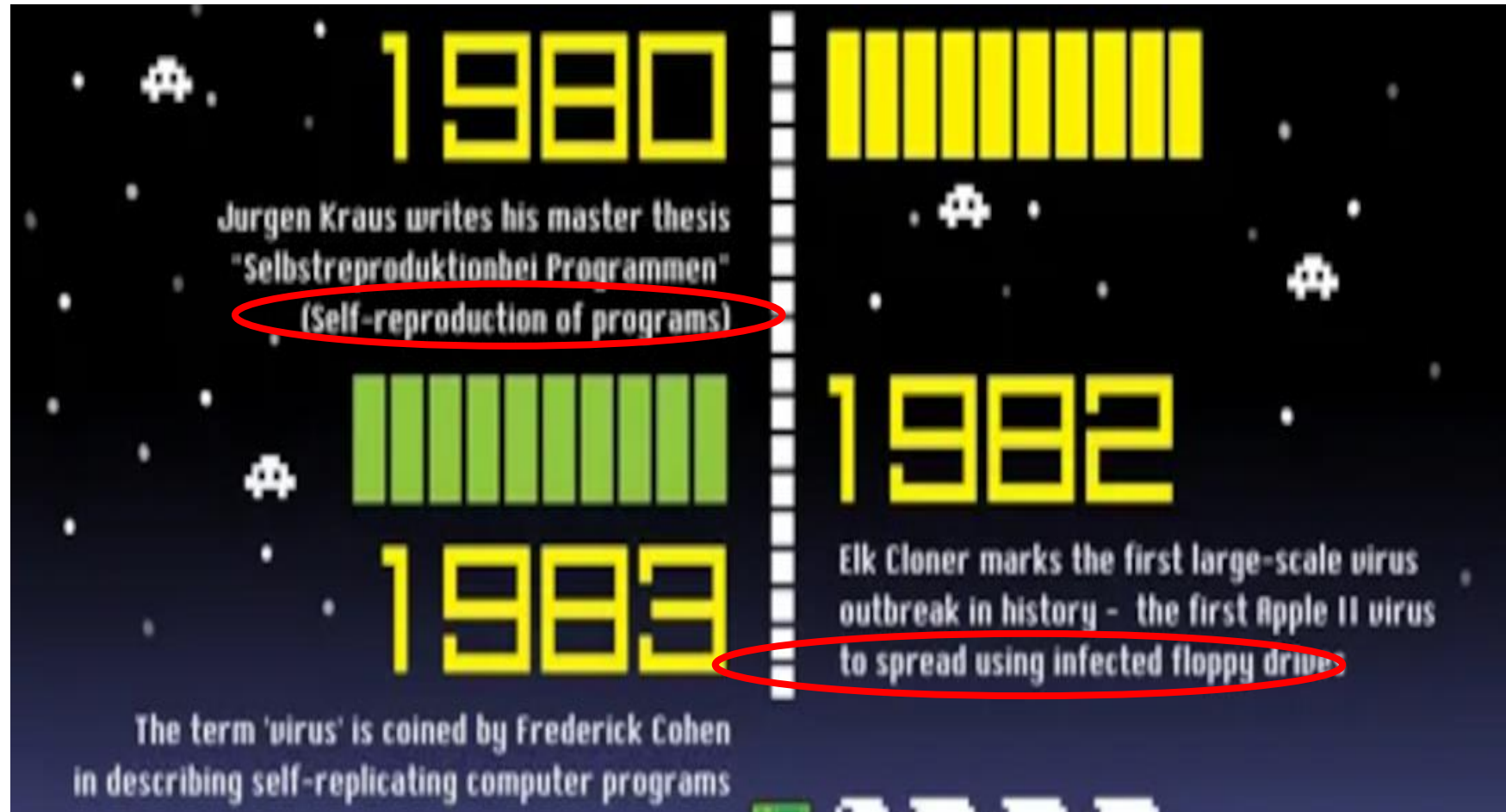


Source: imelgrat.me

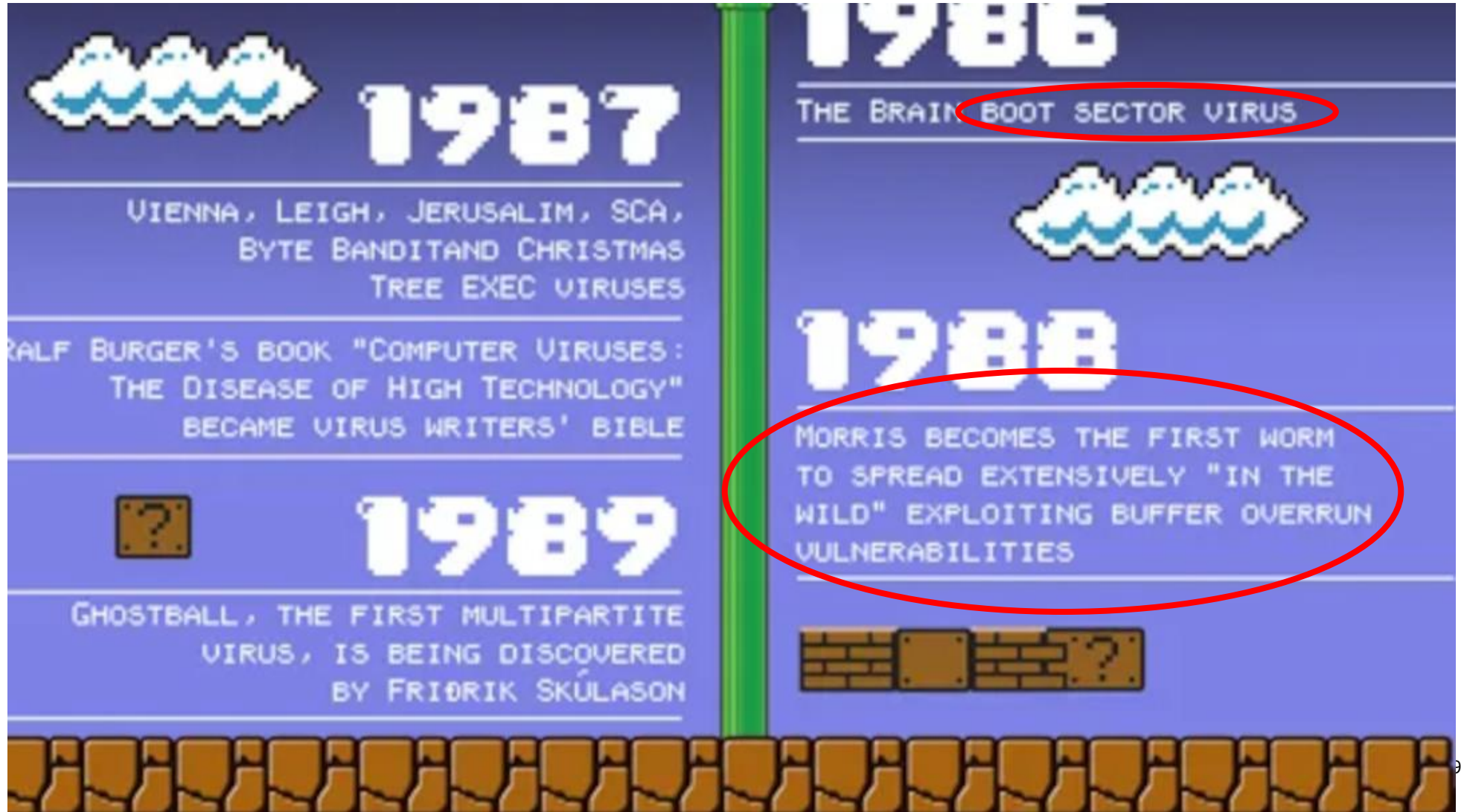
Histoire des Malwares- Les premières années



Histoire des Malwares- Les premières années



Histoire des Malwares- Les premières années



Histoire des Malwares- Les premières années



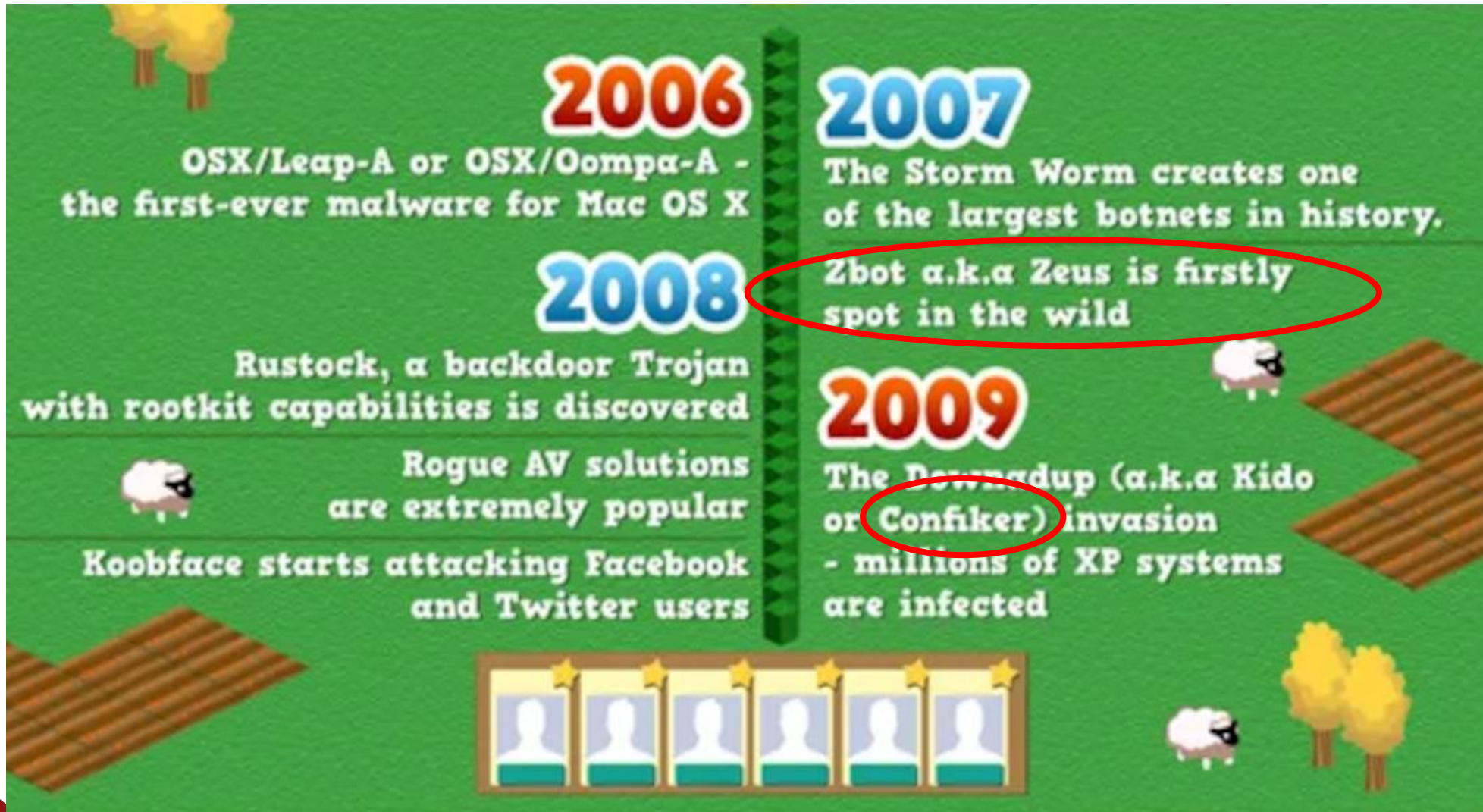
Histoire des Malwares- Les premières années



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

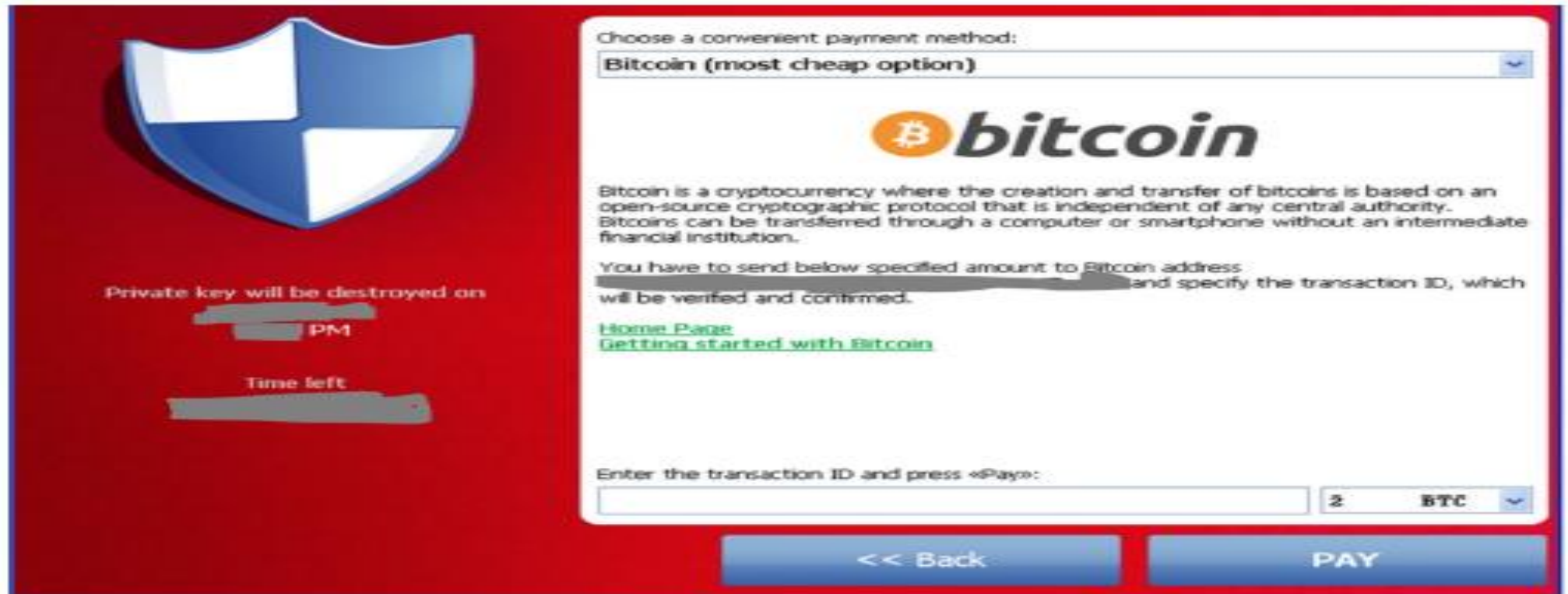
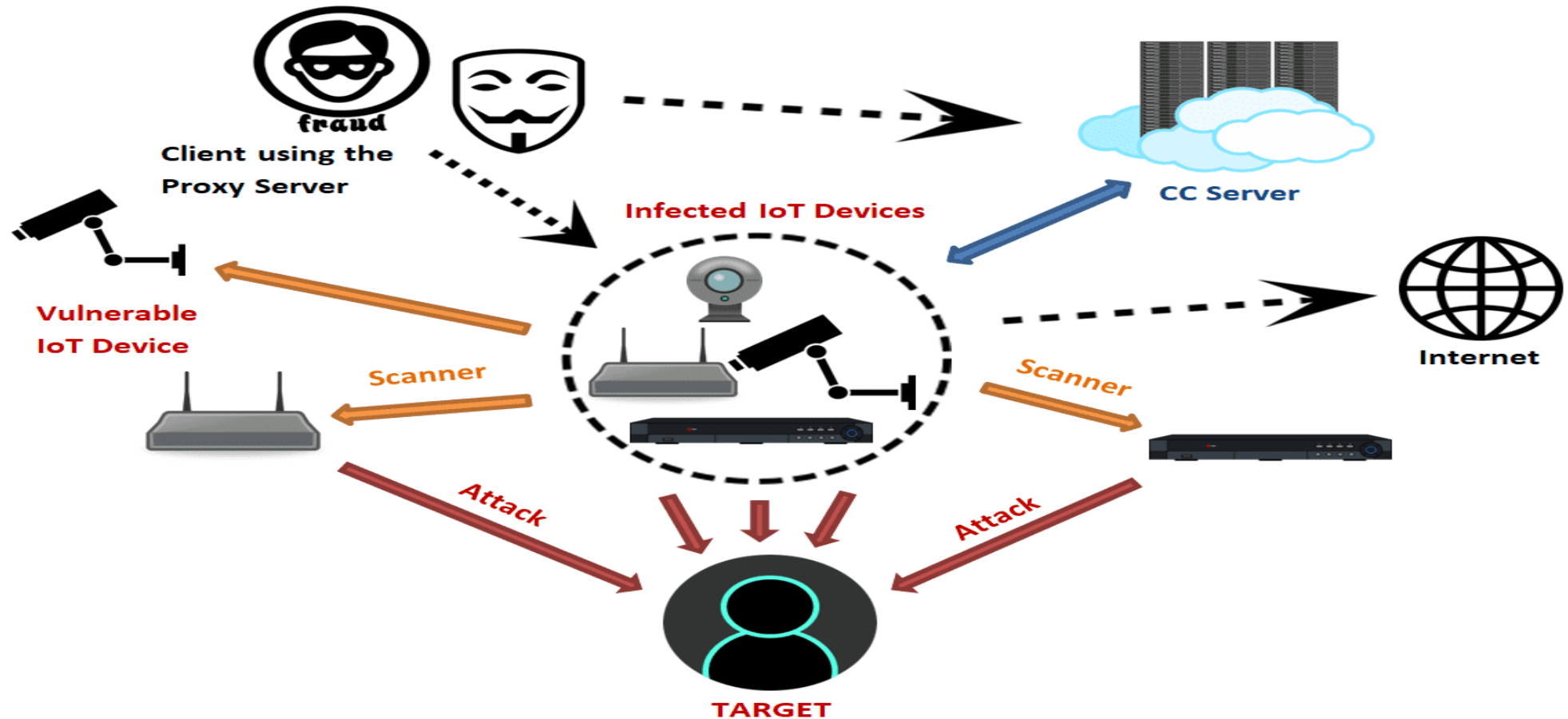


Figure 6: CryptoLocker bitcoin ransom demand

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



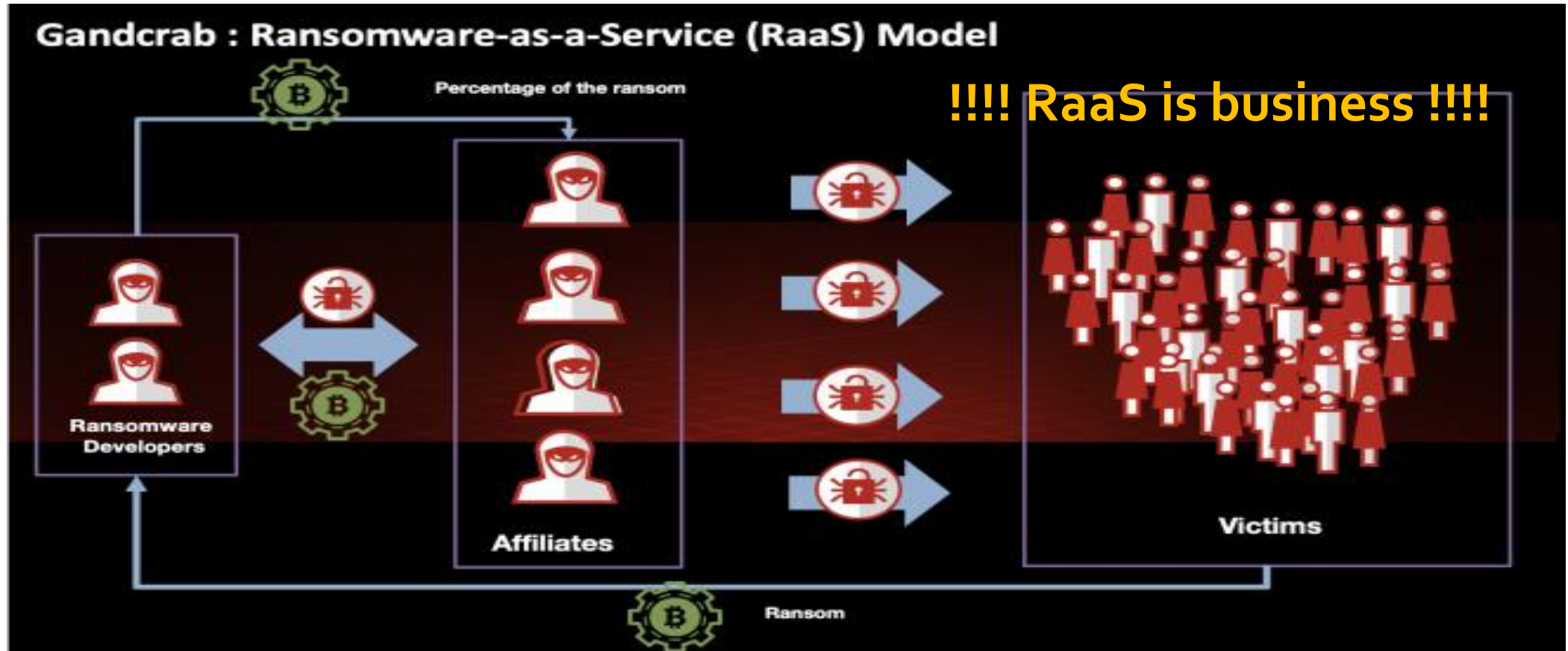
Histoire des Malwares – Sponsorisé, sophistiqué et rentable

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)



Exemple de Maas : DarkSide (\$5 million)



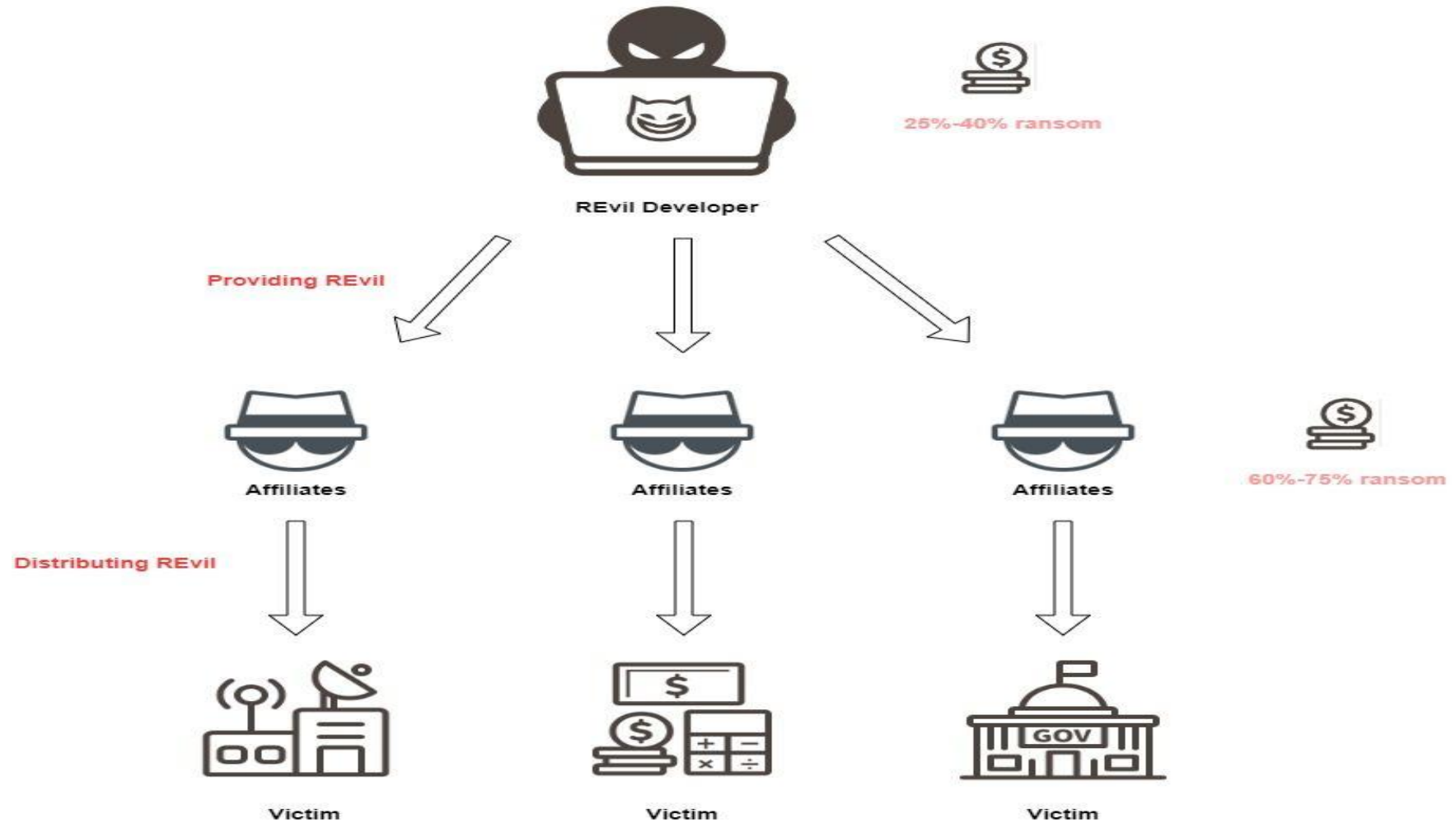
WANTED
REWARD OF UP TO
\$10,000,000.00 USD
FOR INFORMATION LEADING TO THE LOCATION, ARREST, AND/OR
CONVICTION OF OWNERS/OPERATORS/AFFILIATES OF THE



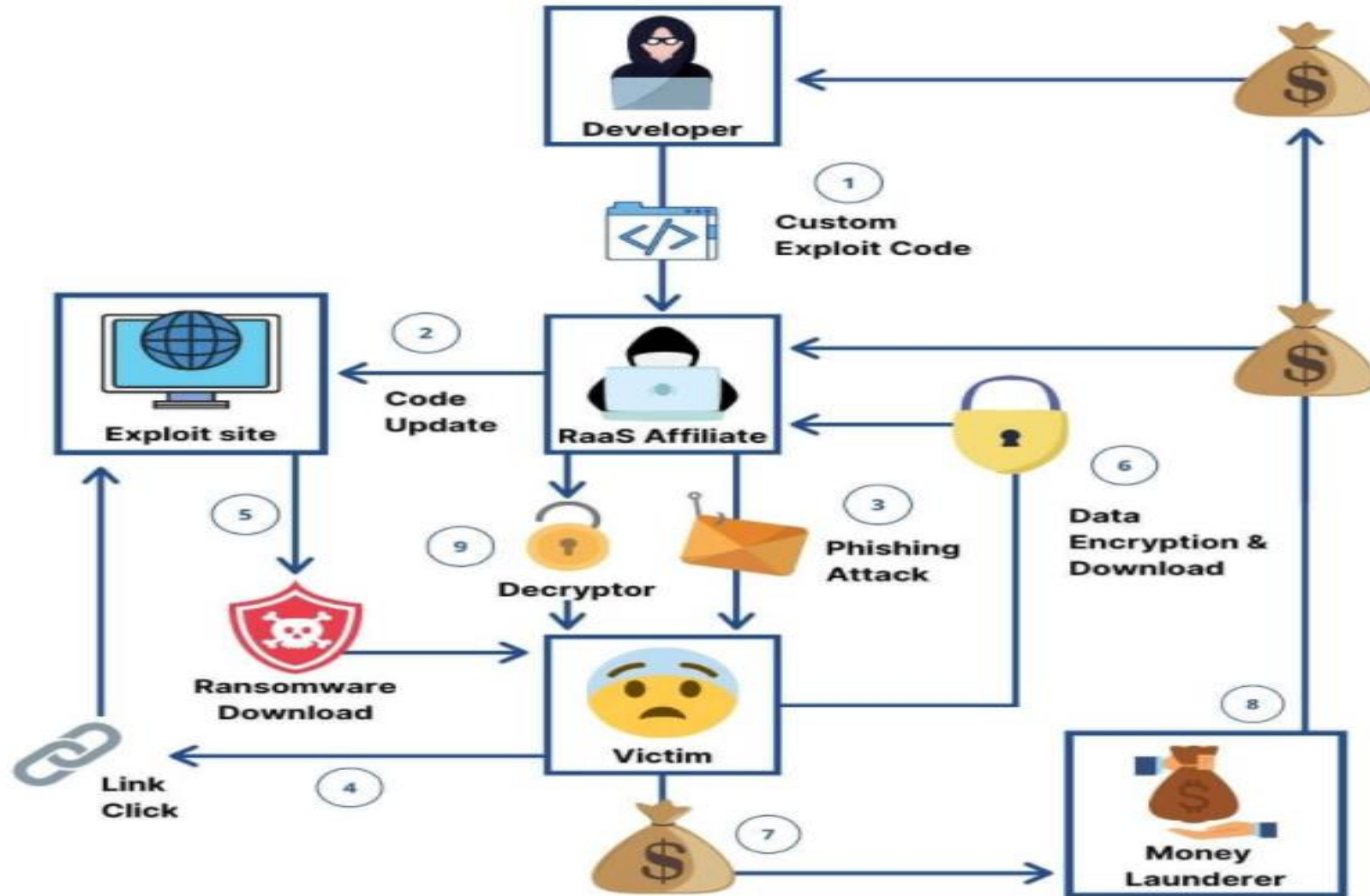
**DarkSide Ransomware
As a Service Group**

SUBMIT TIPS VIA TELEPHONE OR THE FBI WEBSITE BELOW
**Follow-on contacts to be established through
WhatsApp, Telegram, Signal, or other platform
of reporting party's choosing**

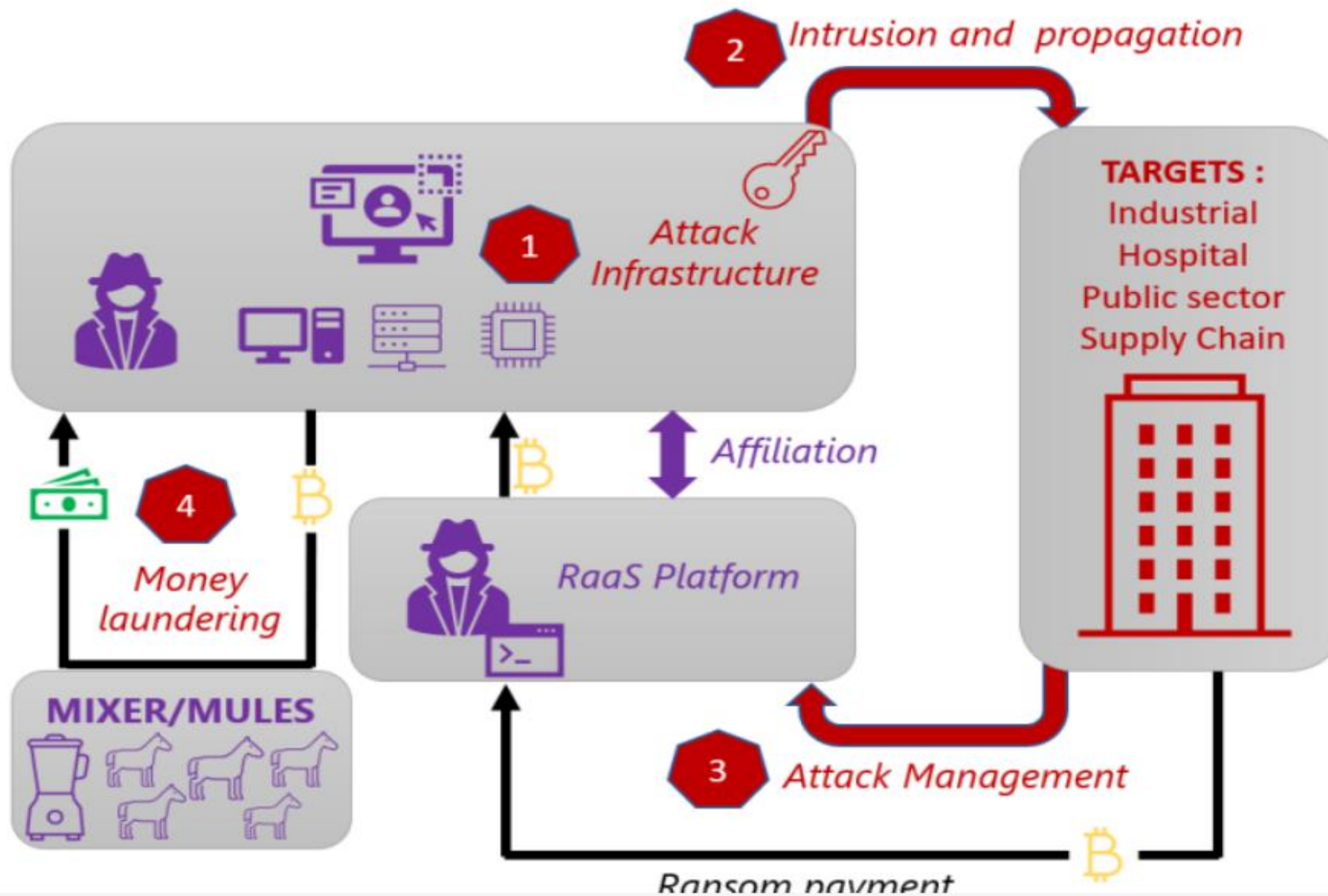
Exemple de Maas : Revil (\$11 million)



Exemple de Maas : LockBit



Exemple de Maas : Conti (\$180 million)

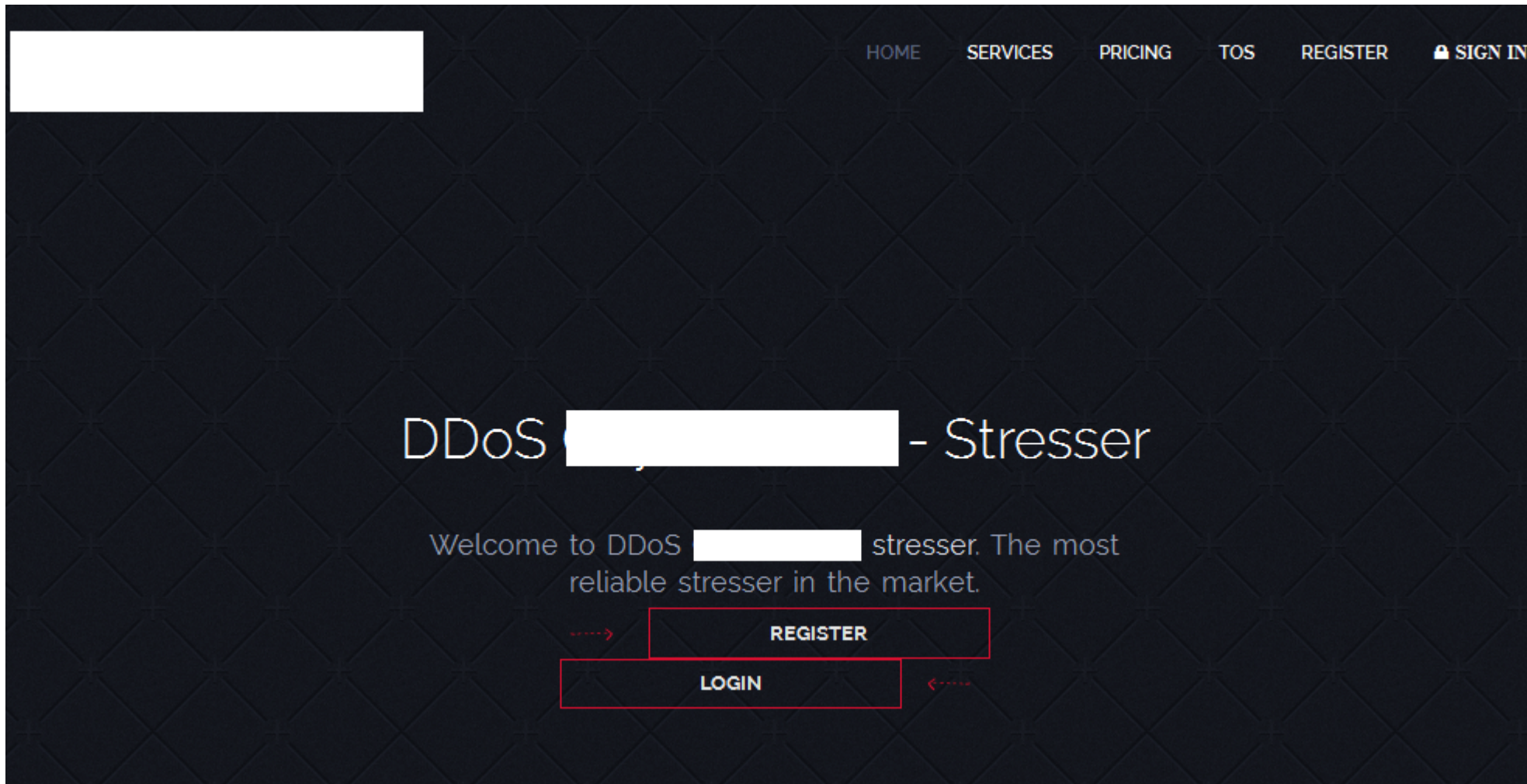


DDoS as a Service

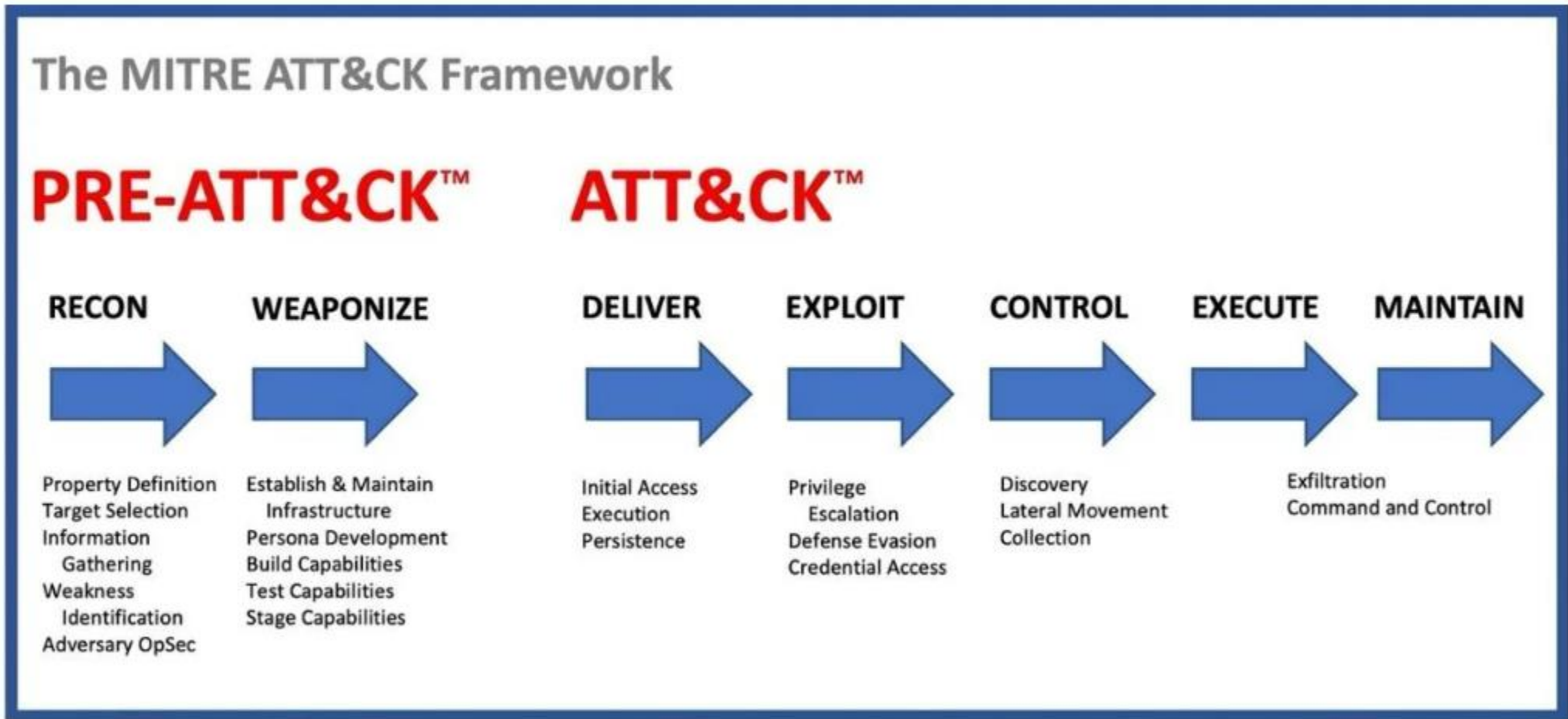
Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

DDoS as a Service - Exemple



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



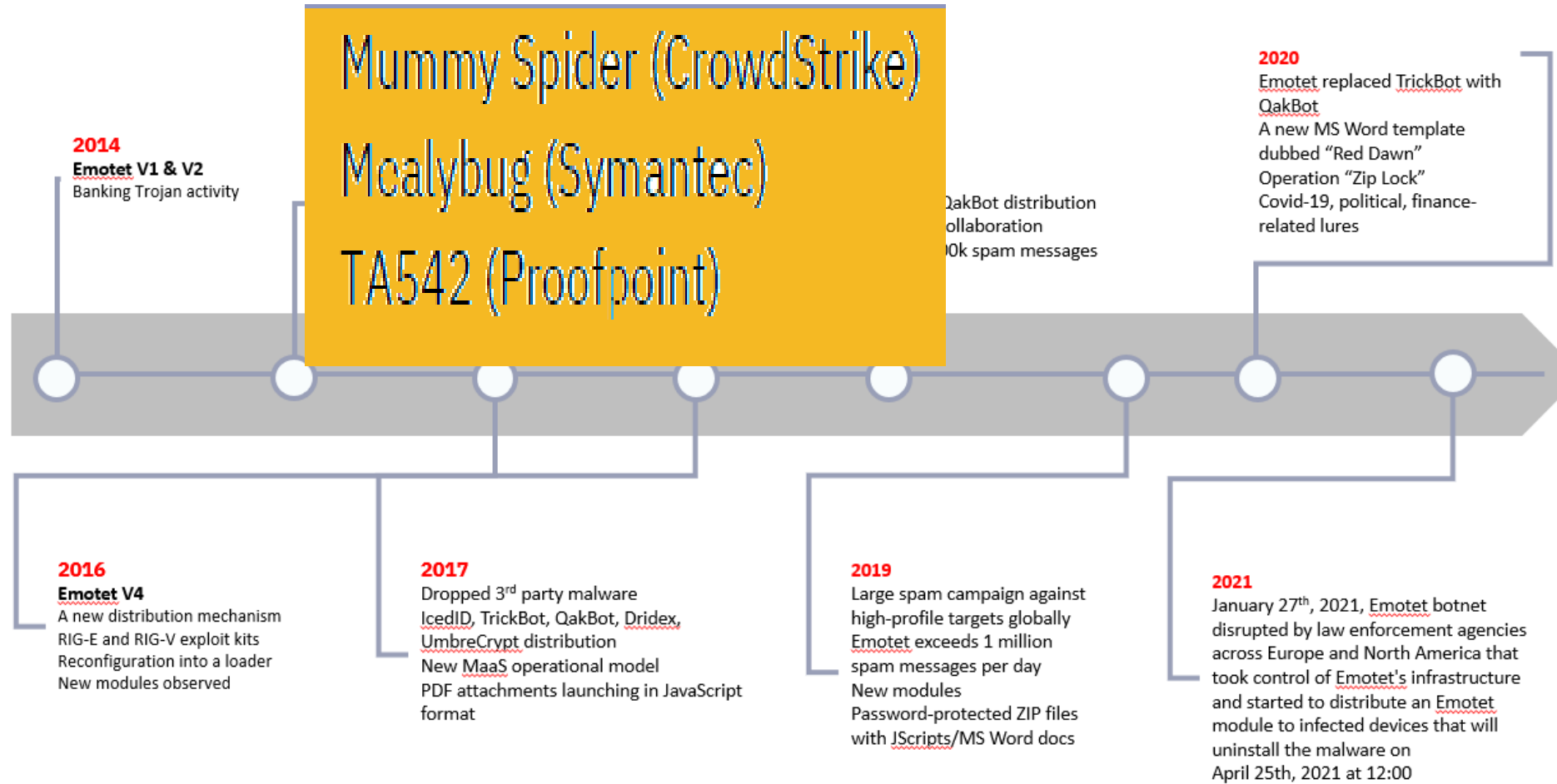
2022: Crime-as-a-Service (CaaS)

The screenshot shows a web browser window with the URL <https://eternity.cc/>. The page title is "Eternity | Products". The navigation menu includes "Eternity", "Products", "Features", "Reviews", and "Telegram". The main content area displays six malware products in a grid:

- Stealer**: Passwords, cookies, credit-cards, wallets recovery and upload to your server. [Details »](#)
- Miner**: Silent crypto-currency mining software. [Details »](#)
- Clipper**: Spoofs crypto-currency addresses in clipboard. [Details »](#)
- Ransomware**: Encrypts documents on target computer. [Details »](#)
- Worm+Dropper**: Spread malware over network, documents, USB. [Details »](#)
- DDoS Bot**: Network of infected computers for DDoS attack & installs. [Details »](#)

At the bottom of the page, there are social media links for GitHub, Telegram, and Email.

Caas - Exemple : Emotet Family



IA: Social Engineering – BEC - Phishing



IA: Evasion Technics

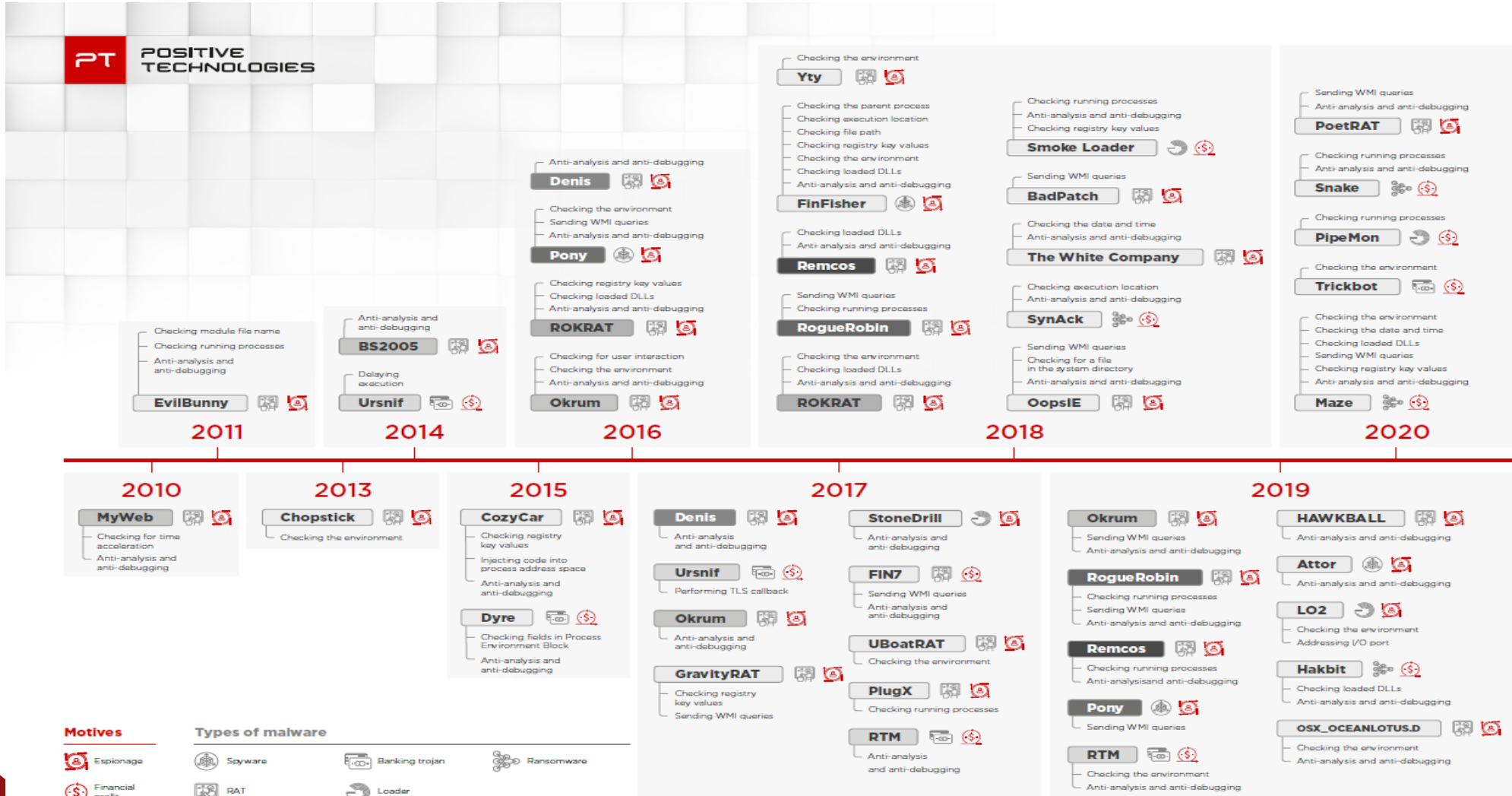
A Malware Obfuscation AI Technique to Evade Antivirus Detection in Counter Forensic Domain

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

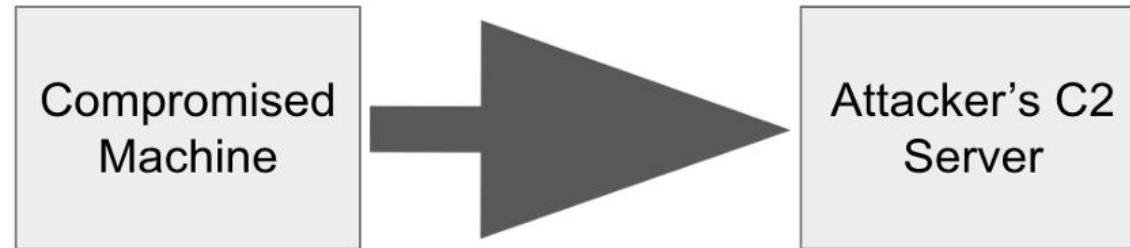


IA: Evasion Technics



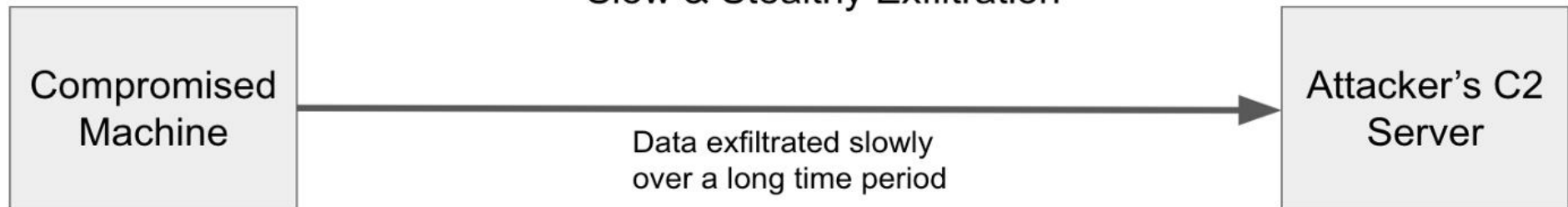
IA: Data Exfiltration

Fast & Loud Exfiltration



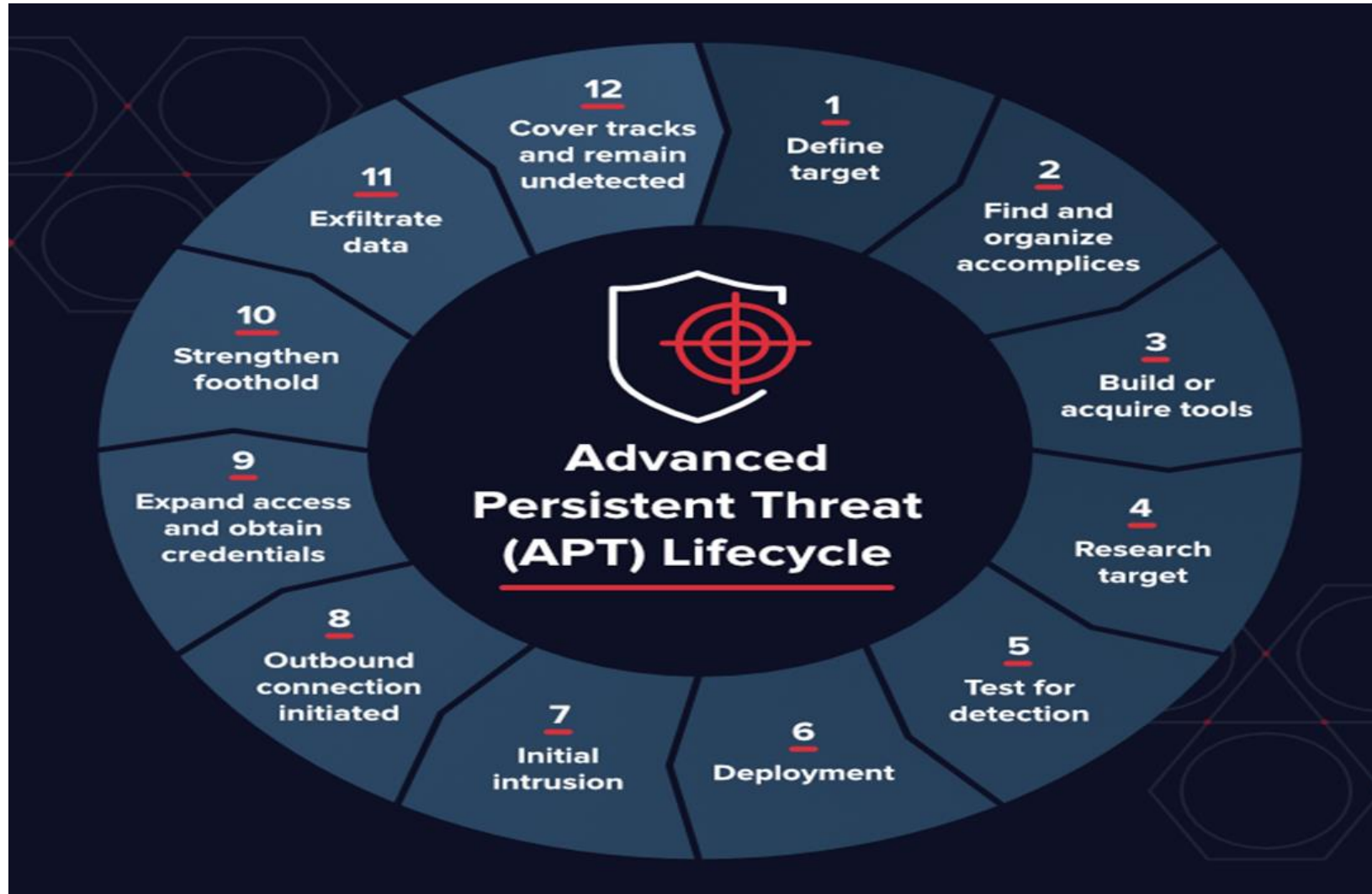
Data sent in a burst
over a short time period

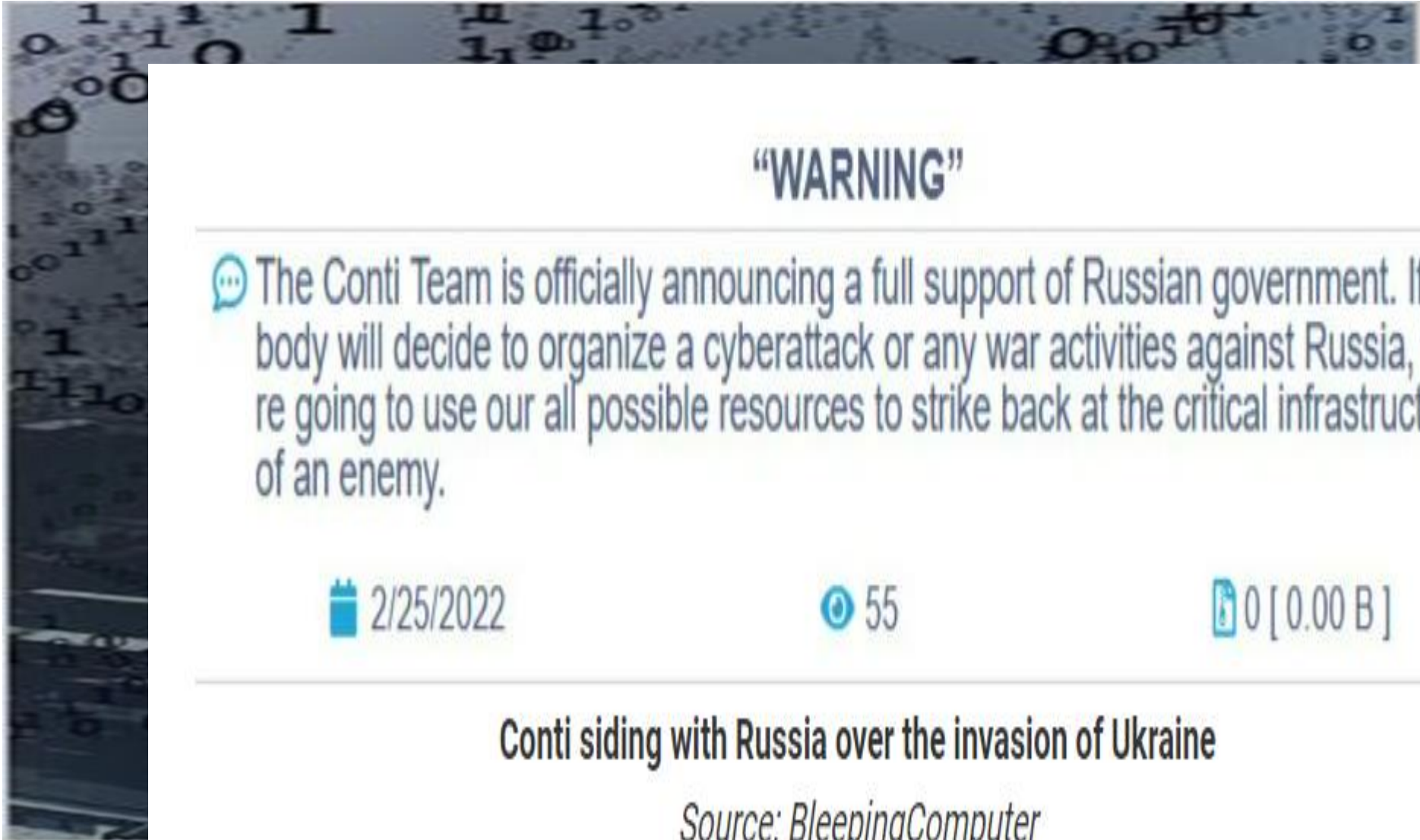
Slow & Stealthy Exfiltration



Data exfiltrated slowly
over a long time period

APT





“WARNING”

🗨 The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

📅 2/25/2022

💬 55

✉️ 0 [0.00 B]

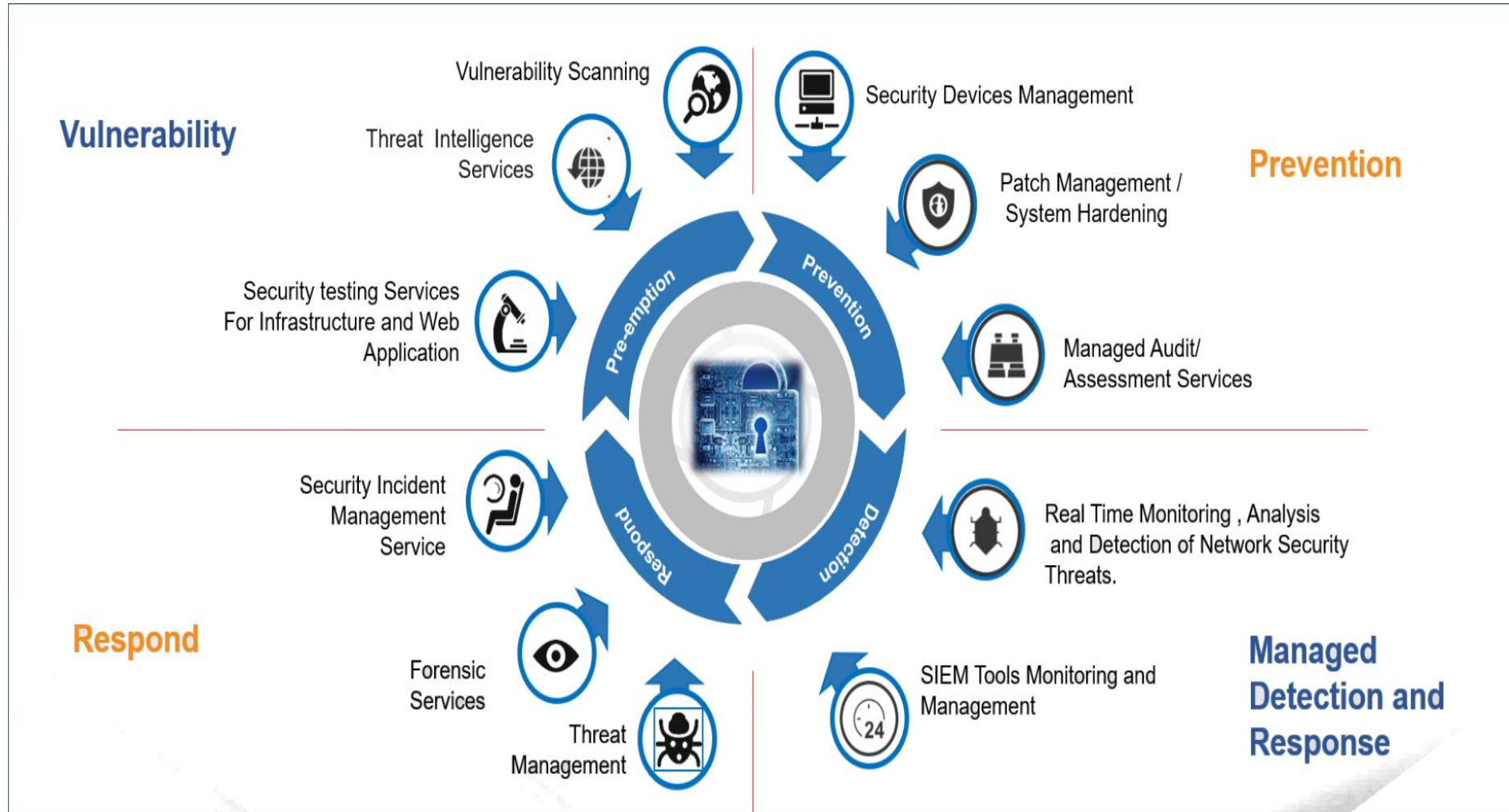
Conti siding with Russia over the invasion of Ukraine

Source: *BleepingComputer*

Solutions ?



Solutions: Protection contre Cybercrime



MANAGED SECURITY SERVICE PROVIDERS (MSSP)

MAJOR CAPABILITIES



Solutions: Cybersecurity as a service



Global Cybersecurity As A Service Market Trends, Applications, Analysis, Growth, And Forecast: 2019 To 2027

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.



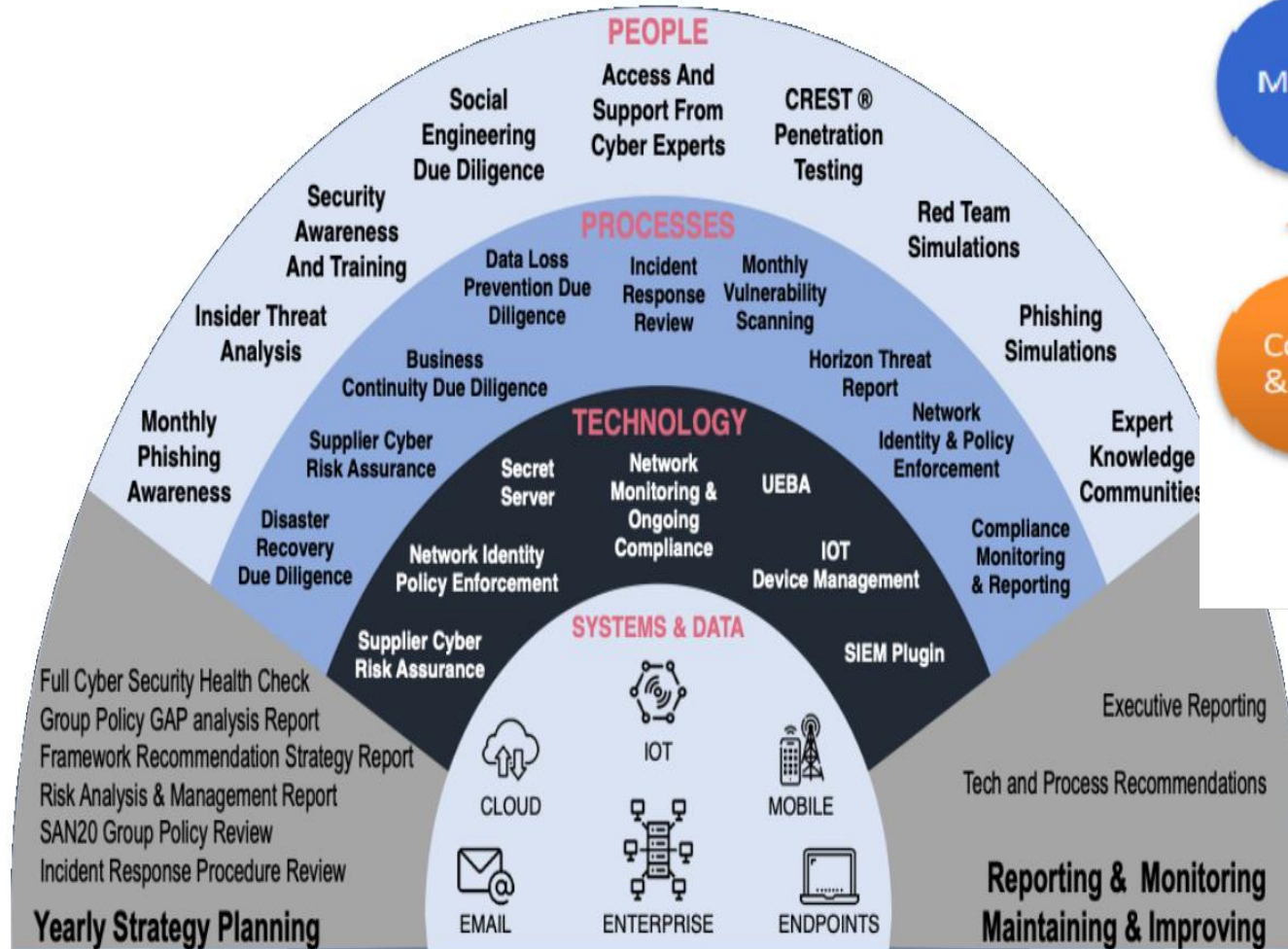
- Cloud-based approach for outsourcing cybersecurity services
- Subscription-based security service hosted by cloud providers, like Software as a Solution
- Method to relieve the in-house security team's obligations, expand security demands as the organization develops, and avoid the expenses and upkeep 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

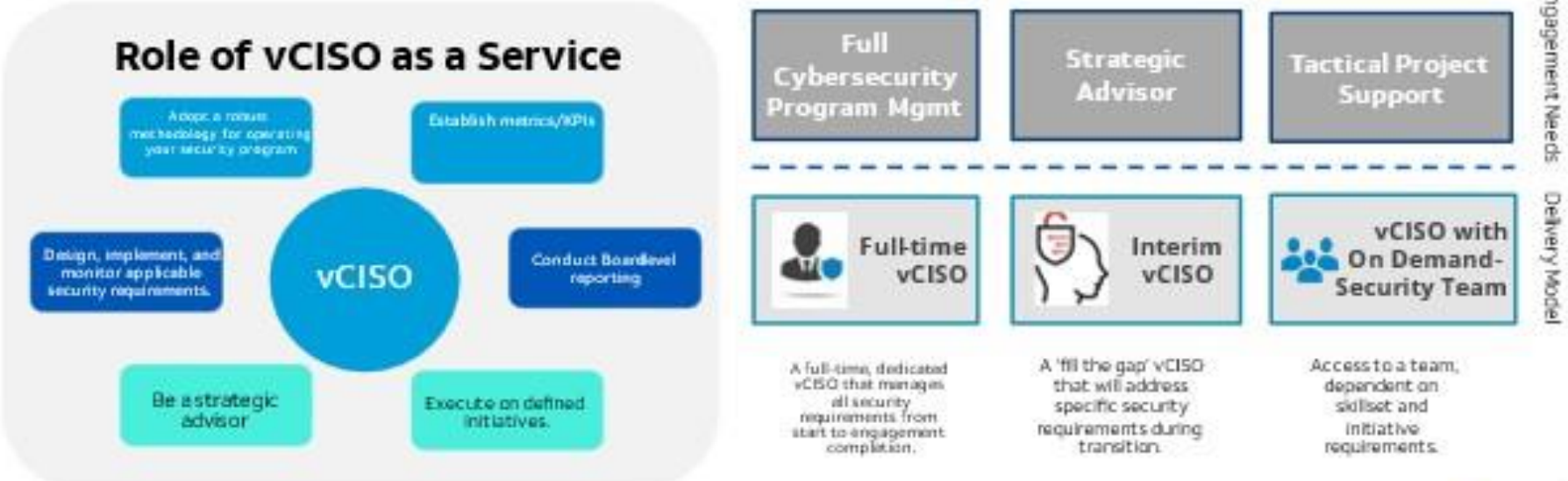


Solutions: Cybersecurity as a service

Monthly Subscriptions Starting From:				
Company Type	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+

vCISO as a Service Engagement and Delivery Models

The virtual CISO service can be customized to meet the cybersecurity requirements of small, medium and large enterprises. Our initial assessment of your organizational needs enables us to identify the optimal engagement model. In each case, you will have access to the full breadth of cybersecurity resources and experience.



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