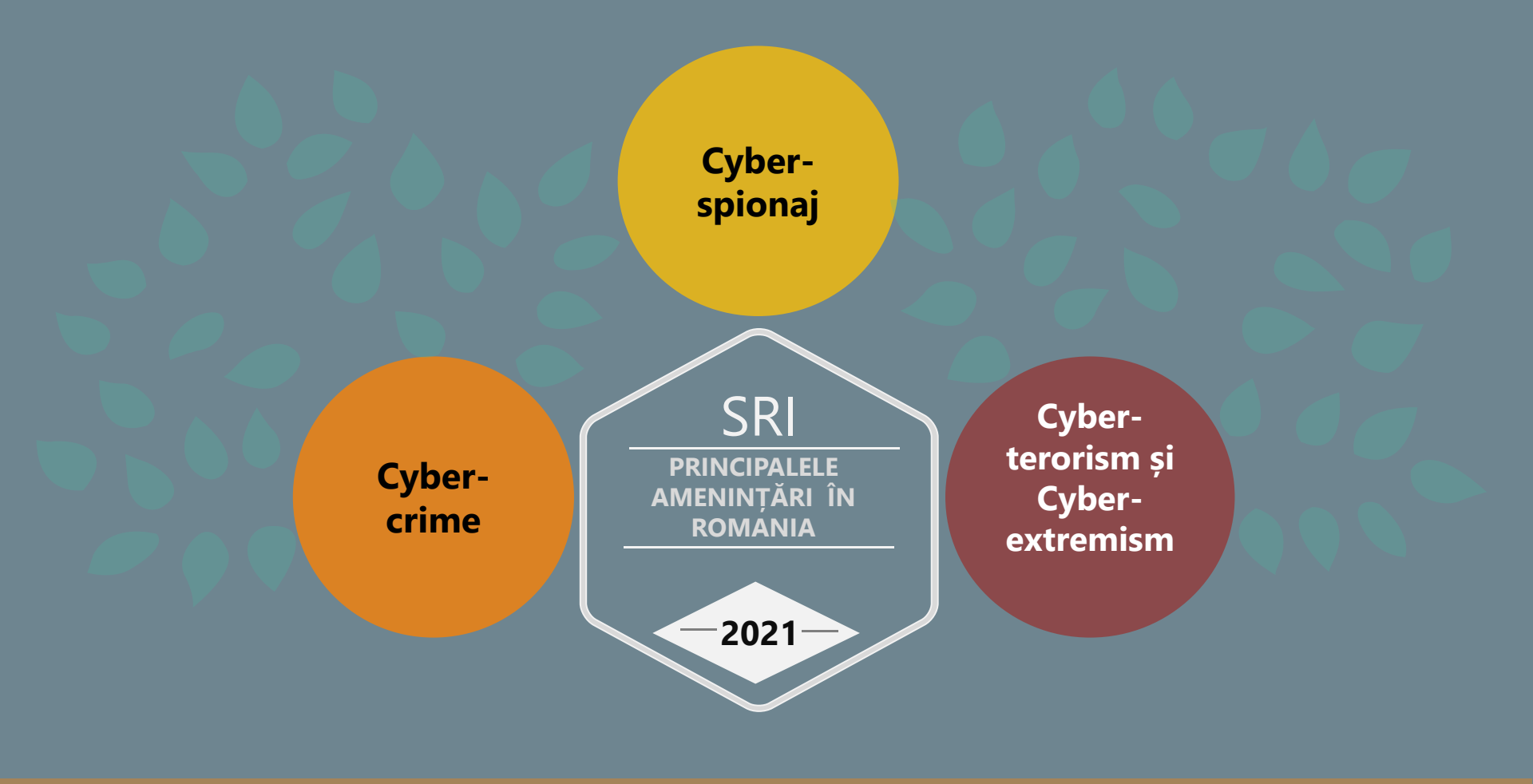
Business as a service vs cybercrime as a service

- *Impactul cybercrime asupra mediului privat* -

GOVNET Conferences

„White Collar Crime and Corporate Fraud – 2022"


Cyber-
spionaj
Cyber-
crime
SRI
PRINCIPALELE
AMENINȚĂRI ÎN
ROMANIA
2021
Cyber-
terorism și
Cyber-
extremism

Amenințarea cibernetică

STATALE

Motivație: **strategică**

Atacurile cibernetice vizează **domeniile strategice** în vederea exfiltrării de informații confidențiale

CRIMINALE

Motivație: **financiară**

Atacurile vizează compromiterea confidențialității datelor gestionate la nivelul **sistemelor informatice asociate serviciilor financiar-bancare** sau utilizarea infrastructurii afectate ca instrument în derularea de alte atacuri cibernetice

TERORISTE ȘI EXTREMISTE

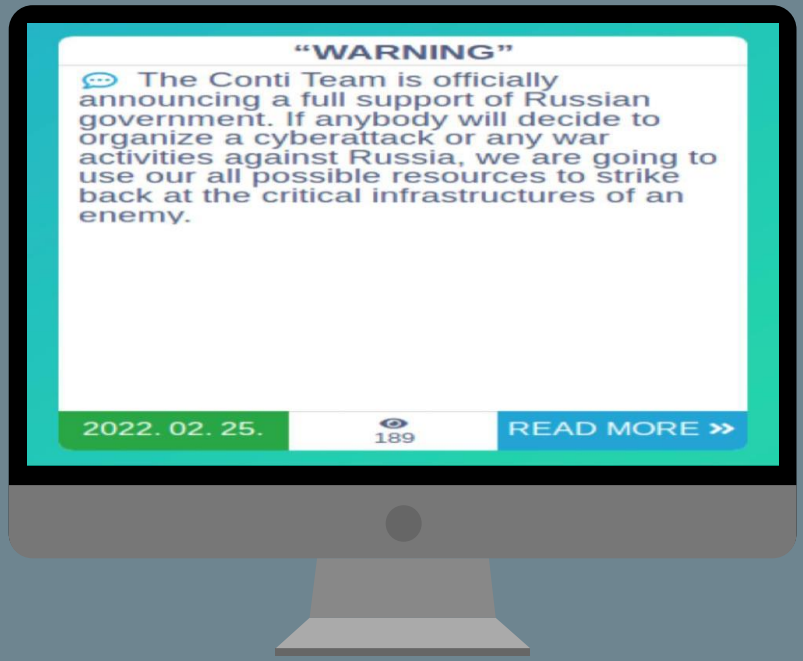
Motivație: **ideologică**

Atacurile vizează **sisteme informatice cu nivel scăzut de securitate cibernetică**

Atacurile cibernetice motivate ideologic se remarcă prin puternic impact mediatic

Ransomware

- atac cibernetic de tip ransomware – atacatorii urmăresc blocarea accesului victimelor la sistemele informatice și criptarea datelor acestora;
- atacatorii solicită plata unei răscumpărări în monedă virtuală pentru a reda victimei accesul la propriile date;
- grupările de cybercrime s-au orientat către exfiltrarea de date anterior criptării și amenințarea victimelor cu publicarea acestora - *double extersion*.



Phobos, Conti, LockBit, REvil

Ransom DDoS

Ransom → DDoS

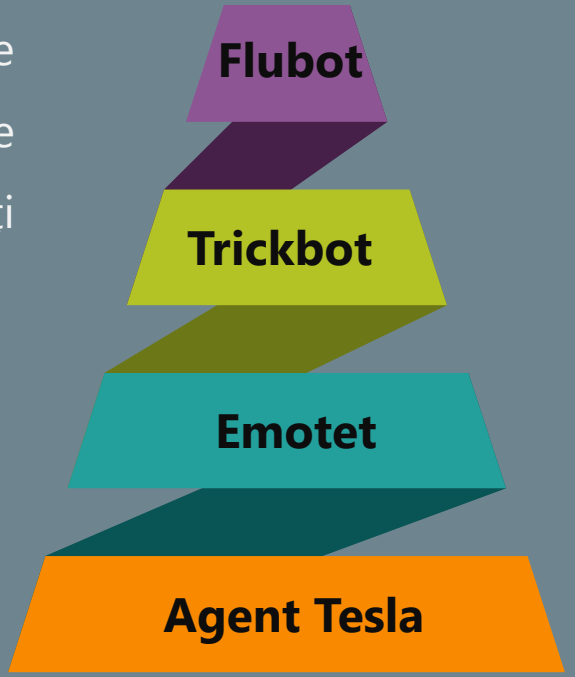
Atac cibernetic în care victimele sunt amenințate cu indisponibilizarea propriilor sisteme prin atacuri de tip ***DDoS*** în situația în care nu este plătită răscumpărarea în termenul solicitat.

Atacatorii impersonează grupări de criminalitate cibernetică notorii și chiar actori statali, pentru a fi percepuți de victime ca fiind o reală amenințare.

Troian

Software aparent legitim, care prezintă o serie de funcționalități nelegitime, ce permit atacatorului să controleze total sau parțial sistemele infectate și să deruleze activități specifice criminalității cibernetice:

- rularea/blocarea/oprirea proceselor;
- exfiltrarea de fișiere;
- furtul de credențiale de acces și date sensibile;
- captarea șirurilor de caractere introduse de la tastatură;
- realizarea de capturi de ecran.



Cryptojacking

Aplicațiile de tip *cryptominner* au o complexitate redusă. În prezent, acest tip de aplicație nu este foarte întâlnit, întrucât veniturile pe care le poate asigura sunt reduse.

Exemplu: Coinminer

Atac cibernetic ce presupune compromiterea unor sisteme informatice în scopul utilizării resurselor acestuia pentru minarea de criptomonedă.

Business as a service vs cybercrime as a service

- *Impactul cybercrime asupra mediului privat* -

GOVNET Conferences

„White Collar Crime and Corporate Fraud – 2022"