AMENINȚĂRILE CIBERNETICE LA ADRESA ROMÂNIEI

CYBERSECURITY FORUM, ***12 Martie 2019 – București***

**** Multiple operațiuni cibernetice ofensive la adresa infrastructurilor IT&C cu valențe critice din România.***

TURLA / Wipbot

DOMENII ȚINTĂ

- guvernamental, afaceri externe, energie, cercetare, media

OBIECTIVE

- exfiltrare de informații, asigurare persistență în cadrul infrastructurilor critice

MODUS OPERANDI

- tehnici de inginerie socială, *spearphishing, watering hole*

TEHNOLOGII AVANSATE

- vulnerabilități *„0-day”*, infrastructură complexă de atac

TURLA / Wipbot

!! Nedetectabil de nicio soluție de securitate cibernetică existentă pe piață

!! Multiple campanii de atac în 2018

APT28 / Sofacy

DOMENII ȚINTĂ
- apărare, securitate națională, afaceri externe și interne, comunicații, energie

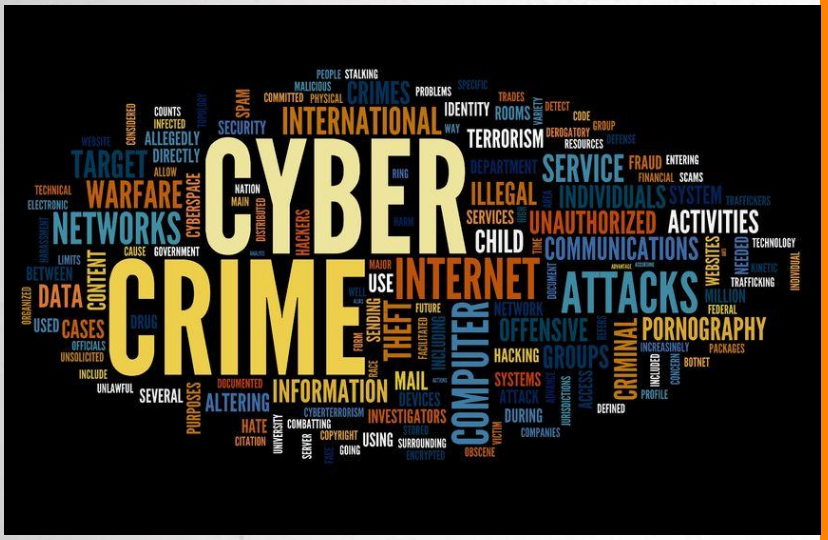
OBIECTIVE
- *reconnaissance*, compromitere infrastructuri IT&C, exfiltrare de informații, persistență în sistemul victimă

MODUS OPERANDI
- *spearphishing, watering hole websites, drive-by download*

TEHNOLOGII AVANSATE
- vulnerabilități „*0-day*”, infrastructură complexă de atac

**** De asemenea, multiple campanii de atac în 2018***

CRIMINALITATE CIBERNETICĂ



❖ CARBANAK / Cobalt Strike

- **actor cibernetic** asociat unor **grupări de criminalitate cibernetică de sorginte estică**, responsabil pentru **atacuri cibernetice care au vizat instituții financiar-bancare**;

„**Serviciul Român de Informații**, prin unitatea specializată în cyberintelligence – **CENTRUL NAȚIONAL CYBERINT** – deține date și informații certe, inclusiv de ordin tehnic, că asupra unor **instituții financiare** din România au avut loc atacuri cibernetice de amploare în perioada **iunie – august a acestui an.**”

Comunicat de presă SRI – 18 august 2018

TERORISM CIBERNETIC

"On 25-26 April 2018 a simultaneous multinational takedown, coordinated by ***Europol's EU IRU*** *and with the support of Eurojust and the Belgian Federal Prosecutor, led to the seizure of digital evidence by law enforcement from Bulgaria (Cybercrime Department in General Directorate Combatting Organised Crime), France (SDAT-SDLC),* ***Romania (Directorate for Countering Organised Criminality – Terrorism Investigation Unit with the support of the Romanian Intelligence Service)****, and the seizure of IS servers in the Netherlands (Dutch National Police – Internet Referral Unit together with the Belgian Federal Judicial Police – East-Flanders), Canada and the USA. Meanwhile, the United Kingdom (Counter Terrorism Internet Referral Unit)* ***took the lead in the referral process of top-level domain registrars abused by IS****."*

Comunicat de presă EUROPOL - 28 aprilie 2018

Exerciții de securitate cibernetică

CyDEx17

70 participanți

30 jucători

40 observatori

CyDEx18

91 participanți

41 jucători

51 observatori

8-10 OCTOMBRIE 2018

Lucrăm cu…

- 2015-2018: European Cyber Security Challenge
- CYBERINT în cooperare cu organizații publice și private.
- 2016, 2017 – echipa Romaniei a fost vicecampioană

- 6 ani în NATO - Cyber Coalition – Core Planning team.
- configurarea Cyber Range
- dezvoltarea *„the Big Scenario"*
- dezvoltare software specific

Peste 5000 de ore lucrate/an!

Module de securitate cibernetică pre/universitatare

Mediu universitar – cursuri postuniversitare în securitate cibernetică în domenii precum administrarea rețelele IT&C, dispozitivele mobile, managementul incidentelor de securitate cibernetică, analiza malware, analiza de tip forensics, securitatea infrastructurilor critice IT&C.

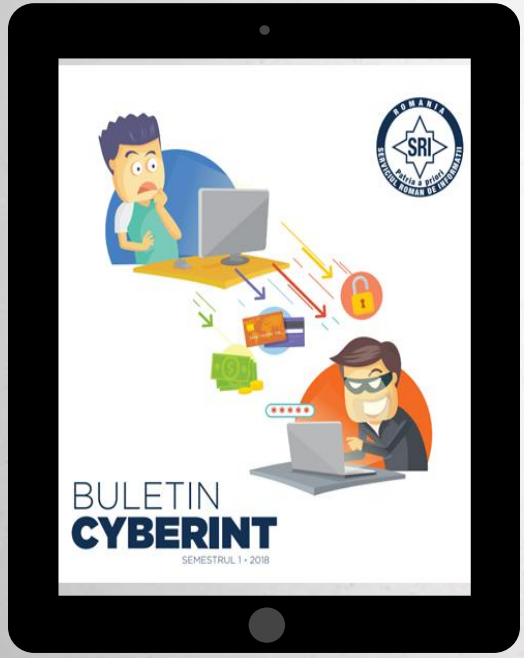
Mediu preuniversitar – module de securitate cibernetică cu accent pe aceleași arii precum cele universitare, însă cu nivel mai redus de complexitate.

Ce știe laptopul / telefonul despre tine?

- Nume & adresă
- Parole
- Apeluri telefonice, mesaje text
- Localizarea geografică
- Fișierele recente / șterse
- Numărul cardurilor de credit, informațiile conturilor bancare
- Istoricul Web

Inginerie socială...
Deoarece manipularea unui individ se realizează mult mai ușor decât compromiterea unei întregi instituții

Awareness



Consolidarea securității cibernetice

Eforturi susținute


ROMANIA
CENTRUL NATIONAL
CYBERINT
SERVICIUL ROMAN DE INFORMATII

Mulțumesc!