2017 HIGHLIGHTS

CERT-RO

ROMÂNIA 1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

Raportul CERT-RO privind evoluția amenințărilor cibernetice este rezultatul unei analize asupra informațiilor colectate și procesate de instituție pe parcursul anului 2017. Acesta este destinat managerilor, experților de securitate din organizațiile publice și private, cât și decidenților politici, cercetătorilor, organizațiilor neguvernamentale și cetățenilor. Raportul include taxonomia CERT-RO utilizată pentru clasificarea alertelor și incidentelor.

./1 CONTEXT

GDPR

Strategia de securitate cibernetică UE

Directiva NIS

Anul 2017 a fost unul dinamic în ceea ce privește evoluția amenințărilor cibernetice, atât prin prisma atacurilor cibernetice cu impact major asupra serviciilor societății informaționale, cât și prin prisma pierderilor de date confidențiale la scară largă. Tendința globală cu privire la diversificarea amenințărilor și vulnerabilităților isi mentine caracterul ascendent, concomitent cu o creștere semnificativa a numărului de dispozitive conectate la internet.

Ca urmare, autoritățile naționale și actorii privați își extind eforturile de prevenție și mitigare. Începând cu luna mai a acestui an, Directiva NIS va fi transpusă în legislația națională, concomitent cu intrarea in vigoare a Regulamentului General pentru Protecția Datelor. Acestea vor determina organizațiile vizate să adopte măsuri tehnice și procedurale adecvate, precum implementarea unor măsuri minime de securitate și mecanisme pentru raportarea incidentelor grave.

./2 EVOLUȚIA AMENINȚĂRILOR LA NIVEL GLOBAL

Malware

- Malware rezident doar în RAM (fileless)
- Utilizarea uneltelor software pre-instalate (living off the land)
- Independență față de acțiunea utilizatorilor (click less)
- Malware-ul ce țintește sistemele MAC OS este în creștere
- Exploatarea vulnerabilităților din hardware sau firmware
- Exploatarea lanțului de aprovizionare (supply chain attacks)

Ransomware

- Atacuri țintite
- Ransomware-as-a-service (Raas)
- Wipeware
- Atacuri asupra dispozitivelor medicale (MEDJACK)

Botnets

- Migrarea către dispozitivele IoT
- Mașinile virtuale reprezintă mai nou o țintă

DoS/DDoS

- Atacurile DDoS înregistrează o evoluție ascendentă
- Atacuri DDoS în valuri (Pulse Wave Attacks)
- Costurile serviciilor de tip DDoS as-a-service sunt în continuă scădere –
- Serviciile de schimb de monezi virtuale (Bitcoin Exchange) sunt printre ținte
- Câteodată atacurile DDoS maschează alte tipuri de atacuri

Phishing

- Atacuri țintite (spear phishing)
- Phishing care livrează malware
- Utilizarea de mecanisme de evitare a detecției

./3 EVOLUȚIA AMENINȚĂRILOR LA NIVEL NAȚIONAL

138M ALERTE

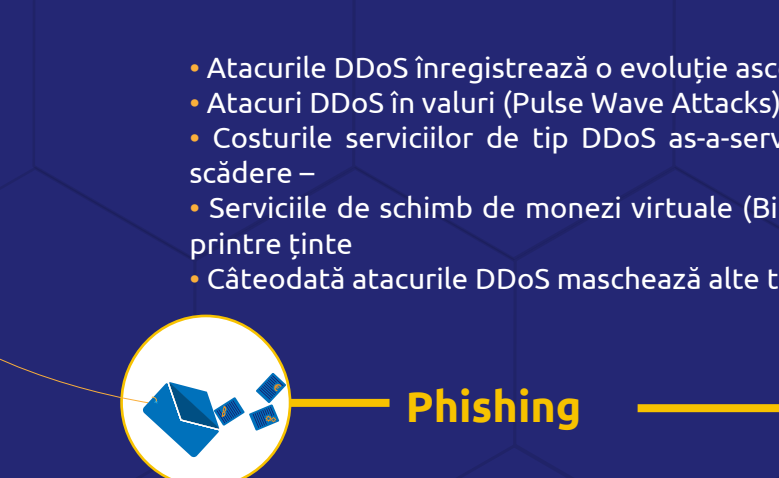
2.89M IP-uri (34%)

83% SISTEME VULNERABILE

25% CREȘTERE ÎN NR. DE ALERTE

1.7k DOMENII .RO

Top 10 tipuri de malware specifice spațiului cibernetic românesc



138,217,026 alerte de securitate cibernetică



Numărul alertelor colectate de CERT-RO



Citiți întregul raport aici

www.cert.ro
cooperation@cert.ro
+4031-6202187
Blv. Mareșal Averescu, nr. 8-10, 011455 București, România