Ca urmare a activităților desfășurate la nivelul **Centrului de răspuns al MAI la incidente de securitate IT (CERT-INT)**, instituit în cadrul **Direcției Generale de Protecție Internă**, de la începutul anului 2022 în spațiul cibernetic al ministerului au fost observate multiple agresiuni informatice, acestea menținându-se în continuare la un nivel ridicat.

Astfel, în această perioadă au fost colectate și corelate 6.390.496.695 evenimente de sistem, din care au fost extrase și analizate aproximativ 5.682 alerte de securitate, fiind identificate diferite acțiuni cibernetice ofensive, manifestate prin atacuri cibernetice și activități informaționale malițioase în mediul online.

Atacurile au debutat cu acțiuni de recunoaștere a suprafeței de atac, în vederea identificării unor vulnerabilități tehnologice și au continuat cu **atacuri de tip scam, phishing, spear-phishing, smishing sau malspam, pentru propagarea unor aplicații malițioase de tip ransomware (WannaCry, Strictor etc.), infostealer (Qbot, Lokibot,Emotet, Agent tesla etc.), remote access trojan – RAT (Remcos, Cryxos, etc.) sau botnet (Andromeda, Mirai etc.) și DDoS (atât volumetrice, cât și la nivel de aplicație)**.

În cadrul campaniilor de agresiuni informatice, care de cele mai multe ori exploatau subiectul agresiunilor militare din Ucraina, atacatorii vizau obținerea unor beneficii pecuniare, compromiterea credențialelor de acces ale utilizatorilor sau indisponibilizarea temporară a unor servicii sau resurse informatice.

Prezintă caracter de noutate în această perioadă identificarea unor **atacuri cibernetice complexe**, care vizau propagarea prin email a unor **aplicații malware sofisticate sau exploatarea unor vulnerabilități critice de tip „*zero day*”**, în cadrul cărora entități rău intenționate urmăreau compromiterea resurselor informatice, realizarea unor canale de comunicații la distanță către serverele de comandă și control și exfiltrarea datelor anumitor utilizatori de la nivelul ministerului.

Vectorul de atac predominant este în continuarea mesageria electronică (email-ul), iar în urma analizării tehnicilor, tacticilor și procedurilor de atac, precum și coroborării indicatorilor de compromitere obținuți din cercetarea agresiunilor cu alte surse de informații, s-a evidențiat posibilitatea ca acestea să fie desfășurate de amenințări persistente avansate de tip APT.

În perioada de referință au fost observate diverse campanii de dezinformare în mediul online, desfășurate prin promovarea unor narative false în cadrul platformelor/grupurilor specifice cu referire la site-urile Poliției Române, Poliției de Frontieră sau Departamentului pentru Situații de Urgență, având ca scop amplificarea artificială a percepției stării de nesiguranță sau de insecuritate, scăderea încrederii populației în capacitatea autorităților statului român de a se apăra în fața unor astfel de atacuri cibernetice, precum și supradimensionarea activităților malițioase întreprinse de atacatori.

Agresorii apelează la diferite detalii tehnice, de cele mai multe ori fără nicio relevanță, pentru promovarea unor așa-zise atacuri cibernetice desfășurate asupra resurselor

web ale instituțiilor publice din România, menite să asigure creșterea reputației acestora și să evidențieze neputința autorităților publice de a se proteja.

Pentru a face față actualelor provocări de securitate Centrul de răspuns al MAI la incidente de securitate IT a desfășurat în această perioadă activități de monitorizare a securității infrastructurii cibernetice a MAI, prin intermediul instrumentelor specifice, în vederea identificării și contracarării cu celeritate a oricăror forme de manifestare a amenințărilor informatice.

Totodată, DGPI **cooperează activ**, atât cu structurile ministerului, cât și cu toate celelalte instituții cu capabilități și responsabilități în domeniul securității cibernetice de la nivel național, pentru identificarea și adoptarea celor mai bune măsuri de securitate, bune practici în domeniu și soluții în prevenirea, detectarea și contracararea atacurilor cibernetice.