DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Comunicat de presă

București, 1 Mai 2022

Continuă atacurile cibernetice de tip **DDoS (Distributed Denial-of-Service)** auto-asumate de gruparea **pro-rusă Killnet** asupra unor site-uri web din România, atacuri motivate de acțiunile de sprijin ale României pentru Ucraina, în contextul invaziei acestui stat de către Federația Rusă.

Directoratul Național de Securitate Cibernetică (DNSC) colaborează cu administratorii site-urilor web impactate, cu instituțiile abilitate și cu parteneri internaționali pentru investigarea și contracararea acestor atacuri.

Se observă o diversificare a atacurilor prin utilizarea unor noi metode care vizează infectarea cu aplicații malware de tip ransomware a sistemelor informatice ale organizațiilor deja atacate prin DDoS. În acest context, tehnicile utilizate de atacatori includ **spear phishing** și **spoofing.**

Atacatorii cibernetici transmit **mesaje pe email, WhatsApp, Signal, Telegram, Messenger, Slack,** etc. pretinzând că sunt o sursă / persoană de încredere, pentru a convinge victimele potențiale să divulge informații confidențiale, date personale sau să efectueze acțiuni care permit preluarea controlului unor infrastructuri sau dispozitive informatice de către atacatori.

Pentru a încerca să inducă în eroare potențialele victime și pentru o rată de succes mai ridicată, atacatorii intenționează să utilizeze inclusiv adrese de email sau conturi de utilizator falsificate ca aparținând unor instituții publice sau organizații cunoscute din România.

Recomandăm prudență în cazul în care se recepționează mesaje ce au următoarele caracteristici:

- Sunt prezentate ca fiind solicitări urgente, inclusiv din partea autorităților;
- Sunt ciudat formulate și apar ca provenind de la o sursă sau persoană "de încredere";
- Includ linkuri sau atașamente care nu au fost solicitate;
- Cer furnizarea unor date cu caracter personal sau tehnice (parole, PIN, IP etc.).

Pentru a limita riscul infectării cu ransomware și a evita criptarea sau distrugerea datelor, este obligatorie și realizarea de copii de siguranță (backup) pentru site-uri, baze de date sau orice alt tip de date expuse în mediul Internet, precum și stocarea acestor copii în locații separate.

Un ghid de securitate cibernetică pe care îl puteți folosi este disponibil la:

https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021

Persoană de contact pentru presă: Mihai Rotariu | mihai.rotariu@dnsc.ro | 0740 066 866