CERT-RO avertizeaza asupra unui val de atacuri de tip sextortion via e-mail, în România

Specialistii Centrului National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO) au înregistrat, recent, multiple notificari si alerte privind un val de emailuri transmise din partea unor grupari infractionale mai multor utilizatori din România, în care sunt continute mesaje de tip Sextortion Scam Email.

"Destinatarii mesajelor de tip Sextortion Scam Email sunt anuntati, în mod fals, ca dispozitivul pe care îl folosesc a fost infectat cu malware si ca infractori cibernetici au preluat controlul asupra acestuia", atentioneaza expertii.

Fenomenul de Sextortion Scam Email a fost observat în România, sustine sursa citata.

"Utilizatorii sunt notificati fie ca au fost filmati cu camera web a dispozitivului utilizat în ipostaze intime, fie vizitând site-uri cu continut pornografic, cu amenintarea ca o înregistrare video urmeaza a fi trimisa catre toate contactele din agenda utilizatorului, pentru a afecta reputatia potentialei victime. Infractorii cer o suma de aproximativ 1.300 de dolari, în criptomoneda, într-un termen de 50 de ore. Spre deosebire de cazuri anterioare, atacatorii nu ofera o 'dovada' pentru a demonstra controlul asupra dispozitivului compromis sau veridicitatea celor scrise. Prin aceasta metoda se urmareste declansarea unei reactii de panica a posibilei victime cu scopul de a o determina sa plateasca suma ceruta în cel mai scurt timp", se subliniaza în comunicatul de presa al CERT-RO, transmis miercuri AGERPRES.

Potrivit expertilor, practic, infractorii cibernetici transmit astfel de mesaje în mod nediscriminatoriu si automatizat, la un numar foarte mare de adrese de email, asteptând ca unii dintre destinatari, inclusiv din România, sa reactioneze la email si sa intre în dialog cu gruparea infractionala.

"Se mizeaza exclusiv pe faptul ca unii utilizatori vor dori sa îsi protejeze reputatia si vor plati suma ceruta, fara a cere o alta opinie din partea unei persoane avizate. Pentru a monetiza pe seama efortului depus, atacatorii nu au nevoie sa convinga fiecare utilizator, ci doar un mic procent al acestora. Nu raspundeti niciodata la email-uri de acest tip si informati imediat expertii IT sau cyber din organizatia dumneavoastra", sfatuiesc specialistii CERT-RO.

Pe lista recomandarilor pe care le fac expertii se afla: nu raspundeti niciodata la email-uri de acest tip, primite de la persoane necunoscute; contactati departamentul IT al institutiei/organizatiei dumneavoastra, pentru a le cere sprijinul, verificati sursa email-ului primit, de fiecare data când vi se pare ceva suspect; acordati o atentie sporita corectitudinii gramaticale a textului din email - lipsa unor diacritice, greseli de sintaxa si o exprimare nenaturala, sunt semne ca s-au folosit instrumente de traducere automata din alta limba; în cazul în care ati efectuat o astfel de plata si acum realizati ca totul a fost o pacaleala, va recomandam sa notificati deopotriva CERT-RO si Politia Româna pentru a depune o plângere; evitati sponsorizarea criminalitatii cibernetice.

Raportarea catre CERT-RO se poate realiza fie pe adresa de e-mail alerts@cert.ro, fie prin numarul unic 1911.