CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO

ALERTĂ: val de atacuri de tip sextortion scam via email

CERT-RO a înregistrat recent multiple notificări și alerte privind un val de emailuri transmise din partea unor grupări infracționale.

Destinatarii mesajelor de tip SEXTORTION SCAM EMAIL sunt anunțați, în mod fals, că dispozitivul pe care îl folosesc a fost infectat cu malware și că infractorii cibernetici au preluat controlul asupra acestuia.

Nu răspundeți niciodată la email-uri de acest tip și informați imediat experții IT sau cyber din organizația dumneavoastră!

SEXTORTION SCAM EMAIL observat în România

Utilizatorii sunt notificați fie că au fost filmați cu camera web a dispozitivului utilizat în ipostaze intime, fie vizitând site-uri cu conținut pornografic, cu amenințarea că o înregistrare video urmează a fi trimisă către toate contactele din agenda utilizatorului, pentru a afecta reputația potențialei victime.

Infractorii cer o sumă de aproximativ 1.300 de dolari, în criptomonedă, într-un termen de 50 de ore.

Spre deosebire de cazuri anterioare, atacatorii nu oferă o 'dovadă' pentru a demonstra controlul asupra dispozitivului compromis sau veridicitatea celor scrise. Prin această metodă se urmărește declanșarea unei reacții de panică a posibilei victime cu scopul de a o determina să plătească suma cerută în cel mai scurt timp.

Practic, infractorii cibernetici transmit astfel de mesaje în mod nediscriminatoriu și automatizat, la un număr foarte mare de adrese de email, așteptând ca unii dintre destinatari să reacționeze la email și să intre în dialog cu gruparea infracțională.

Se mizează exclusiv pe faptul că unii utilizatori vor dori să își protejeze reputația și vor plăti suma cerută, fără a cere o altă opinie din partea unei persoane avizate. Pentru a monetiza pe seama efortului depus, atacatorii nu au nevoie să convingă fiecare utilizator, ci doar un mic procent al acestora.

Recomandări

- Nu răspundeți niciodată la email-uri de acest tip, primite de la persoane necunoscute.
- Contactați departamentul IT al instituției/organizației dumneavoastră, pentru a le cere sprijinul.
- Verificați sursa email-ului primit, de fiecare dată când vi se pare ceva suspect.
- Acordați o atenție sporită corectitudinii gramaticale a textului din email - lipsa unor diacritice, greșeli de sintaxă și o exprimare nenaturală, sunt semne că s-au folosit instrumente de traducere automată din altă limbă.
- În cazul în care ați efectuat o astfel de plată și acum realizați că totul a fost o păcăleală, vă recomandăm să notificați deopotrivă CERT-RO și Poliția Română (pentru a depune o plângere).
- Evitați sponsorizarea criminalității cibernetice!

alerts@cert.ro

Telefon 1911