Bitdefender a descoperit un nou grup de infractori cibernetici care ataca infrastructuri critice la granitele României

Un nou grup activ de atacatori cibernetici, ce sprijina interesele Federatiei Ruse, este implicat în atacuri asupra infrastructurilor-cheie din regiunea extinsa a Marii Negre, tintele confirmate fiind institutii judiciare si guvernamentale din Georgia, precum si un furnizor de energie electrica din Republica Moldova, sustin expertii în securitate cibernetica ai Bitdefender.

Acestia subliniaza, într-un comunicat de presa transmis, marti, ca metodele folosite de catre grupul Curly COMrades sunt: accesul prelungit în retele, furtul de date si mascarea traficului prin site-uri web legitime, ce ar putea fi replicate si împotriva organizatiilor românesti, inclusiv din domenii ca energie, transport sau administratie publica.

"Investigatia a evidentiat folosirea unor tehnici avansate de persistenta, infrastructuri de acces redundante si un nou tip de instrument de atac, MucorAgent. Acesta utilizeaza o metoda de persistenta fara precedent în cercetarile companiei, care exploateaza o componenta standard a Windows pentru a se reactiva în mod imprevizibil si discret. Atacurile observate în state vecine sau apropiate geografic reprezinta un posibil indicator al amenintarilor care pot viza România. Granitele fizice nu mai limiteaza riscurile cibernetice, iar proximitatea geografica, legaturile economice si infrastructurile interconectate fac necesara o monitorizare permanenta si o capacitate de reactie rapida din partea companiilor si institutiilor românesti", se arata în comunicat.

În acest context, specialistii Bitdefender recomanda monitorizarea permanenta a activitatilor neobisnuite din retea si blocarea traficului catre servere externe suspecte, alaturi de restrictionarea utilizarii instrumentelor de administrare la distanta atunci când nu sunt strict necesare.

Totodata, este nevoie de implementarea de solutii de detectie si raspuns la incidente, precum EDR (Endpoint Detection and Response), respectiv XDR (Extended Detection and Response), care monitorizeaza în timp real activitatea din retea si din sistemele interne, identifica comportamente suspecte si permit reactie rapida; pentru organizatiile fara echipe interne dedicate de securitate.

În plus, o alta recomandare vizeaza apelarea la servicii de tip MDR (Managed Detection and Response), care pun la dispozitie echipe externe specializate care ofera monitorizare non-stop, investigare si raspuns la atacuri.

"Atacurile observate în state vecine sau apropiate geografic reprezinta un posibil indicator al amenintarilor care pot viza România. Granitele fizice nu mai limiteaza riscurile cibernetice, iar proximitatea geografica, legaturile economice si infrastructurile interconectate fac necesara o monitorizare permanenta si o capacitate de reactie rapida din partea companiilor si institutiilor românesti", subliniaza expertii.

Bitdefender ofera solutii superioare de preventie, detectie si raspuns la incidente de securitate cibernetica. Laboratoarele companiei descopera sute de noi amenintari informatice în fiecare minut si valideaza zilnic 50 de miliarde de interogari privind amenintarile. Tehnologiile Bitdefender sunt licentiate catre peste 200 dintre cele mai cunoscute branduri de securitate din lume.

Fondata în anul 2001, compania are clienti în peste 170 de tari si birouri pe toate continentele.