Bitdefender: România si alte state din Asia Centrala si Europa, vizate de o campanie de spionaj cibernetic

Producatorul global de solutii de securitate cibernetica Bitdefender avertizeaza asupra unei campanii de spionaj cibernetic în desfasurare, orchestrata de o grupare specializata inclusiv în furt de date sensibile, ce vizeaza entitati guvernamentale si diplomatice din Asia Centrala si Europa, inclusiv România.

"UAC-0063 este o grupare specializata în spionaj cibernetic si furt de date sensibile. Activa înca din 2022, UAC-0063 a început sa vizeze tinte din Asia Centrala, iar acum si-a extins activitatea si în Europa. Printre tinte se numara ambasade si institutii guvernamentale din Germania, Olanda, Marea Britanie, Georgia si România. Atacatorii au dezvoltat o tehnica avansata de atac, bazata pe documente Word compromise. Aceste fisiere sunt distribuite prin e-mailuri de tip phishing si contin macro-uri infectate care, odata activate, instaleaza amenintari informatice pe dispozitivele victimelor. În unele cazuri, atacatorii au reutilizat documente autentice furate anterior de la institutii diplomatice", atentioneaza expertii Bitdefender, într-un comunicat de presa transmis, miercuri, AGERPRES.

Potrivit sursei citate, odata infectat, dispozitivul începe sa transmita date catre serverele atacatorilor si poate fi folosit pentru noi atacuri asupra altor tinte.

Atacurile UAC-0063 au fost confirmate si în România, unde au fost identificate tentative de infectare folosind variante mai sofisticate ale amenintarii informatice, sustin specialistii în securitate cibernetica. Astfel, pe data de 4 aprilie 2024, o versiune compilata a acestuia, protejata prin tehnici avansate de camuflare a codului, a fost detectata pe un sistem din tara.

"CERT-UA (Institutia de Raspuns la Incidente de Securitate Cibernetica din Ucraina) atribuie UAC-0063 gruparii ruse APT28 (BlueDelta), însa fara dovezi tehnice clare. Desi atacatorii folosesc tactici similare cu cele ale APT28, nu exista înca o confirmare definitiva. Totusi, faptul ca atacurile vizeaza entitati diplomatice si guvernamentale din regiuni de interes pentru Rusia ridica semne de întrebare cu privire la posibila motivatie geopolitica a acestor operatiuni", noteaza Bitdefender.

În acest context, pentru a combate eficient amenintarile cibernetice, fie trecute, prezente sau viitoare, este esentiala o strategie de securitate bazata pe mai multe niveluri de protectie.

Potrivit expertilor, primul pas în reducerea riscului de atac este minimizarea suprafetei de expunere. "Gestionarea proactiva a riscurilor, prin evaluari de vulnerabilitate si scenarii de amenintare, ajuta la identificarea si eliminarea punctelor slabe înainte ca acestea sa fie exploatate de atacatori precum UAC-0063", subliniaza compania.

De asemenea, pe zona de protectie, este nevoie de implementarea mai multor straturi de securitate pentru dispozitive si utilizatori îngreuneaza semnificativ accesul atacatorilor.

"Chiar daca solutiile de securitate detecteaza anomalii, echipele de securitate trebuie sa le investigheze si sa actioneze rapid. Lipsa personalului specializat sau a resurselor poate duce la întârzieri în raspuns si permite atacatorilor sa îsi continue operatiunile. Solutiile de threat intelligence ofera informatii esentiale despre atacuri cibernetice. Bitdefender IntelliZone este o platforma intuitiva care centralizeaza aceste informatii si actorii implicati si ofera analistilor de securitate acces la servicii avansate de analiza malware", se precizeaza în comunicat.

Bitdefender este un lider recunoscut în domeniul securitatii IT, cu clienti în peste 170 de tari si birouri pe toate

continentele.