

## Bitdefender: România și alte state din Asia Centrală și Europa, vizate de o campanie de spionaj cibernetic

**Producatorul global de soluții de securitate cibernetică Bitdefender avertizează asupra unei campanii de spionaj cibernetic în desfășurare, orchestrată de o grupare specializată inclusiv în furt de date sensibile, ce vizează entități guvernamentale și diplomatice din Asia Centrală și Europa, inclusiv România.**

"UAC-0063 este o grupare specializată în spionaj cibernetic și furt de date sensibile. Activa încă din 2022, UAC-0063 a început să vizeze ținte din Asia Centrală, iar acum și-a extins activitatea și în Europa. Printre ținte se numără ambasade și instituții guvernamentale din Germania, Olanda, Marea Britanie, Georgia și România. Atacatorii au dezvoltat o tehnică avansată de atac, bazată pe documente Word compromise. Aceste fișiere sunt distribuite prin e-mailuri de tip phishing și contin macro-uri infectate care, odată activate, instalează amenințări informatice pe dispozitivele victimelor. În unele cazuri, atacatorii au reutilizat documente autentice furate anterior de la instituții diplomatice", atenționează experții Bitdefender, într-un comunicat de presă transmis, miercuri, AGERPRES.

Potrivit sursei citate, odată infectat, dispozitivul începe să transmită date către serverele atacatorilor și poate fi folosit pentru noi atacuri asupra altor ținte.

Atacurile UAC-0063 au fost confirmate și în România, unde au fost identificate tentative de infectare folosind variante mai sofisticate ale amenințării informatice, susțin specialiștii în securitate cibernetică. Astfel, pe data de 4 aprilie 2024, o versiune compilată a acestuia, protejată prin tehnici avansate de camuflare a codului, a fost detectată pe un sistem din țară.

"CERT-UA (Instituția de Răspuns la Incidente de Securitate Cibernetică din Ucraina) atribuie UAC-0063 grupării ruse APT28 (BlueDelta), însă fără dovezi tehnice clare. Deși atacatorii folosesc tactici similare cu cele ale APT28, nu există încă o confirmare definitivă. Totuși, faptul că atacurile vizează entități diplomatice și guvernamentale din regiuni de interes pentru Rusia ridică semne de întrebare cu privire la posibilă motivație geopolitică a acestor operațiuni", notează Bitdefender.

În acest context, pentru a combate eficient amenințările cibernetică, fie trecute, prezente sau viitoare, este esențială o strategie de securitate bazată pe mai multe niveluri de protecție.

Potrivit experților, primul pas în reducerea riscului de atac este minimizarea suprafeței de expunere. "Gestionarea proactivă a riscurilor, prin evaluări de vulnerabilitate și scenarii de amenințare, ajută la identificarea și eliminarea punctelor slabe înainte ca acestea să fie exploatare de atacatori precum UAC-0063", subliniază compania.

De asemenea, pe zona de protecție, este nevoie de implementarea mai multor straturi de securitate pentru dispozitive și utilizatori îngreunează semnificativ accesul atacatorilor.

"Chiar dacă soluțiile de securitate detectează anomalii, echipele de securitate trebuie să le investigheze și să acționeze rapid. Lipsa personalului specializat sau a resurselor poate duce la întârzieri în răspuns și permite atacatorilor să își continue operațiunile. Soluțiile de threat intelligence oferă informații esențiale despre atacuri cibernetică. Bitdefender IntelliZone este o platformă intuitivă care centralizează aceste informații și actorii implicați și oferă analiștilor de securitate acces la servicii avansate de analiză malware", se precizează în comunicat.

Bitdefender este un lider recunoscut în domeniul securității IT, cu clienți în peste 170 de țări și birouri pe toate

continentele.