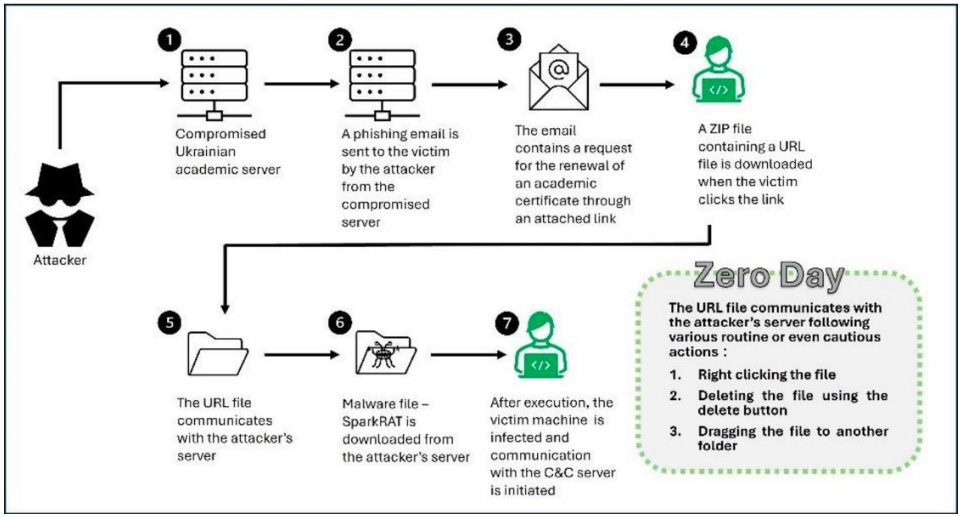
Raport consolidat eveniment cibernetic

CVE-2024-43451- „Right-Click to Hack”

CVE-2024-43451 este o vulnerabilitate zero-day activ exploatată, care vizează utilizatorii ***Windows***, în special în Ucraina. Această vulnerabilitate permite atacatorilor să utilizeze fișiere URL pentru a executa acțiuni malițioase prin simpla interacțiune a utilizatorului, cum ar fi un *click dreapta, tragerea sau ștergerea fișierului*. Descoperirea a fost realizată de echipa ClearSky Cyber Security, care a constatat că fișierele malițioase erau distribuite de pe un site guvernamental ucrainean și erau utilizate într-o campanie de phishing.



Informații suplimentare

Vector de atac și exploatare	• **Fișier URL malițios:** vectorul de infecție începe cu un fișier **Zip** conținând un fișier **PDF** și un fișier cu extensia .url sunt utilizate pentru a deschide adrese web și conțin o secțiune [InternetShortcut] care definește locația URL-ului.. Interacțiunea cu fișierul **URL** declanșează o comunicare cu serverul atacatorului, stabilind o conexiune **SMB.** • **Obținerea Hash-urilor NTLM**: Atunci când un fișier .url încearcă să acceseze un server SMB controlat de atacator, sistemul Windows trimite hash-ul **NTLM** al utilizatorului, permițând atacatorilor să folosească această valoare în atacuri de tip **„Pass-the-Hash”** pentru a compromite resursele Windows**.** • **Metoda de activare:** exploatarea este declanșată prin click dreapta, tragere sau ștergere, ceea ce face vulnerabilitatea extrem de periculoasă și ușor de activat accidental de către utilizatori.
Actori implicați	Conform ClearSky, se suspectează că actorii amenințării sunt legați de gruparea **UAC-0194**, cunoscută pentru afiliațiile sale rusești. Infrastructura de rețea asociată atacului include IP-uri conectate la un furnizor rus de VPS, care acceptă plăți cu criptomonede, indicând încercări de a ascunde activitățile.
Impact și malware distribuit	• **Malware asociat**: Vulnerabilitatea a fost folosită pentru a distribui diverse tipuri de malware, inclusiv Redline Stealer și SparkRAT. Redline Stealer este utilizat pentru a fura date sensibile, iar SparkRAT pentru controlul sistemului compromis. • **Compromiterea resurselor Windows**: Exploatarea oferă atacatorilor acces la resursele Windows sensibile, compromițând securitatea sistemului fără ca utilizatorii să fie nevoiți să introducă parole.
Răspuns și măsuri de atenuare	Microsoft a lansat un patch pe 12 noiembrie 2024 pentru a corecta această vulnerabilitate. Utilizatorii sunt încurajați să aplice actualizările de securitate cât mai rapid posibil.
IOC	ClearSky a publicat IoCs, incluzând hash-uri SHA-256 și adrese IP, precum IP-ul 92.42.96[.]30, asociat cu Saltu[.]Cloud, un furnizor rus de VPS. Administratori de rețea și profesioniști în securitate cibernetică sunt sfătuiți să monitorizeze aceste IoCs.
Fluxul de atac	1. Victima descarcă un fișier ZIP malițios care conține un fișier .url și un fișier aparent legitim, cum ar fi un PDF. 2. Victima interacționează cu fișierul .url (prin click dreapta, ștergere, drag and drop etc.), activând vulnerabilitatea. 3. Fișierul .url inițiază o conexiune SMB către un server C2 controlat de atacatori, care captează hash-ul NTLM al victimei. 4. Atacatorii folosesc hash-ul NTLM în atacuri de tip „Pass-the-Hash” pentru a se autentifica în rețeaua organizației și pentru a răspândi malware, precum Redline Stealer sau SparkRAT.
Tipuri de malware distribuite	**Redline Stealer**: Această aplicație malițioasă este cunoscută pentru capacitatea sa de a fura informații sensibile, inclusiv parole stocate, date de autentificare, detalii despre carduri de credit și criptomonede. Redline poate exfiltra datele și poate trimite rapoarte complete către atacatori.

	SparkRAT: SparkRAT este un remote access trojan (RAT) capabil de control total al sistemului infectat. Acesta permite atacatorilor să monitorizeze activitatea victimei, să descarce și să execute fișiere, să controleze camerele și microfoanele și să efectueze capturi de ecran.
Măsuri de detecție	**Monitorizare SMB** • **Monitorizarea cererilor SMB neobișnuite**: Configurați alarme pentru cereri SMB care se conectează la domenii necunoscute sau IP-uri suspecte. Întrucât vulnerabilitatea CVE-2024-43451 utilizează SMB pentru a trimite hash-uri NTLM către serverul atacatorului, monitorizarea atentă a acestui protocol este esențială. • **Auditarea autentificărilor NTLM**: Configurați logarea și monitorizarea pentru autentificările NTLM, în special în afara domeniului rețelei organizației, pentru a detecta tentativele de autentificare cu hash-uri compromise. **Analiza logurilor de evenimente Windows**: • **Evenimente legate de fișierele URL**: Monitorizați evenimentele legate de crearea, accesarea și manipularea fișierelor .url. Evenimentele pot fi analizate pentru a detecta utilizarea neobișnuită a acestor fișiere, care ar putea semnala exploatarea vulnerabilității. • **Conexiuni SMB cu IP-uri externe**: Logurile de evenimente Windows pot fi analizate pentru conexiuni SMB inițiate către IP-uri externe. Conexiunile SMB externe sunt rare în medii securizate și pot fi un indicator al unei încercări de capturare a hash-urilor NTLM. **Endpoint Detection and Response (EDR)**: • **Detectarea comportamentului suspicios**: EDR-urile pot detecta și alerta asupra activităților neobișnuite, cum ar fi execuția unui fișier .url ce inițiază conexiuni externe. • **Blocarea execuției automatizate a fișierelor .url**: Configurați EDR-ul pentru a restricționa sau alerta la execuția fișierelor .url descărcate din surse externe. **Indicatori de Compromitere (IoCs)** • **Hash-uri de fișiere și domenii suspecte**: Utilizați hash-urile SHA-256 și IP-urile publicate de ClearSky și alte surse de inteligență cibernetică pentru a detecta potențialele activități malițioase legate de această vulnerabilitate. • **Lista de blocare**: Adăugați IP-ul și alte domenii suspecte în lista de blocare a rețelei pentru a preveni conexiunile cu infrastructura atacatorului.

Recomandări generice	1. **Aplicarea Patch-urilor**: Asigurați-vă că toate patch-urile de securitate de la Microsoft sunt instalate pentru a atenua vulnerabilitatea CVE-2024-43451. 2. **Educația utilizatorilor**: Instruirea utilizatorilor să nu interacționeze cu fișiere necunoscute și să fie precauți în cazul descărcării de fișiere din surse nesigure. 3. **Monitorizarea IoCs**: Folosiți IoCs furnizate de ClearSky pentru a detecta activitățile asociate cu această vulnerabilitate în rețeaua organizației. 4. **Restricționarea accesului SMB**: Implementați măsuri de control pentru a restricționa accesul la SMB, reducând riscul de capturare a hash-urilor NTLM.

Resurse externe

https://securityonline.info/right-click-to-hack-zero-day-cve-2024-43451-vulnerability-targets-windows-users/