Raport consolidat eveniment cibernetic

Amenințarea cibernetică GamaCopy și tacticile sale

Un nou actor cibernetic, denumit GamaCopy, a fost identificat utilizând tactici similare cu cele ale grupului de hacking Gamaredon, aliniat cu Kremlinul. Acest actor a inițiat atacuri cibernetice care vizează entități vorbitoare de limbă rusă, folosind metode avansate de livrare și acces la distanță. Campania a fost atribuită unui cluster de amenințări cunoscut și sub denumirea de Core Werewolf, care utilizează instrumente și tehnici similare pentru a ascunde adevărata lor identitate.

Informații suplimentare

Metode de livrare a malware-ului	❖ **Canal de livrare:** Atacurile utilizează arhive auto-extractibile (SFX) create cu 7-Zip pentru a livra fișiere malițioase. ❖ **Conținut malițios**: Fișierele includ UltraVNC configurat pentru acces la distanță, un script batch care livrează sarcina utilă, și un document PDF utilizat ca diversiune. ❖ **Evitarea detectării**: Executabilul UltraVNC este denumit "OneDrivers.exe" pentru a imita un fișier Microsoft legitim.
Exploatarea vulnerabilităților	❖ **Porturi utilizate**: UltraVNC este configurat să folosească portul 443 pentru a imita traficul legitim HTTPS. ❖ **Tehnici de obfuscare**: Utilizarea comenzii EnableDelayedExpansion și a altor tehnici de scripting pentru a ascunde activitățile malițioase.
Comparații cu Gamaredon și Core Werewolf	GamaCopy adoptă tacticile, tehnicile și procedurile utilizate de grupurile menționate. Exemple includ: ❖ Folosirea arhivelor SFX pentru instalarea și executarea UltraVNC. ❖ Instrumente open-source utilizate pentru a ascunde amprenta atacurilor.
Impactul atacurilor	**Efecte economice** ❖ Pierderi financiare pentru organizațiile afectate, datorită furtului de date și costurilor de remediere. ❖ Perturbarea operațiunilor, inclusiv a infrastructurilor critice. **Impact asupra reputației**

	❖ Afectarea începerii colaborărilor în cadrul organizațiilor compromise. ❖ Creșterea ne întrecerii în utilizarea tehnologiilor open-source suspecte.
Context geopolitic	**Influența războiului ruso-ucrainean** Războiul a amplificat activitatea grupurilor cibernetice, multe dintre acestea vizând infrastructuri critice și organizații militare. GamaCopy și grupuri similare profită de vulnerabilitățile tehnologice și sociale pentru a compromite ținte strategice. **Imitarea tacticilor statale** Deși GamaCopy nu este confirmat ca fiind susținut direct de un stat, tactica sa de a imita Gamaredon sugerează un scop strategic: confuzia și distragerea atenției investigatorilor.
Măsuri de protecție și recomandări	**Detectarea și prevenirea** ❖ Monitorizarea fișierelor SFX: Implementarea de soluții AV care pot analiza arhivele auto-extractibile. ❖ Controlul traficului de rețea: Detectarea conexiunilor suspecte care utilizează portul 443. ❖ Autentificarea robustă: Utilizarea autentificării multifactor pentru a preveni accesul neautorizat. **Educația utilizatorilor** ❖ Organizarea de sesiuni regulate de conștientizare privind phishing-ul și metodele de inginerie socială utilizate de atacatori.

Resurse externe

https://thehackernews.com/2025/01/gamacopy-mimics-gamaredon-tactics-in.html