DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ALERTĂ
30.03.2022

UNCLASSIFIED / NECLASIFICAT

Campanie cibernetică malițioasă cu malware de tip Trojan Stealer via email

Vă informăm că, începând cu data de 25 martie 2022, este în desfășurare o **campanie cibernetică malițioasă cu malware de tip Trojan Stealer, via email**, care vizează instituții de stat și private din România.

MODUS OPERANDI

Atacatorii impersonează instituții publice sau companii private din România folosind liste de adrese de email existente în calculatoarele atacate pentru a transmite și propaga mesaje ce conțin linkuri infectate precum:

hxxps://onedrive[.]live[.]com/download?cid=204A4E2E2BFCF3CA&resid=204A4E2E2BFCF3CA%21110&authkey=AD5eSXevs3QExIU

Prin accesarea linkului respectiv este descărcat un fișier *Excel Macro* (de tip ***Trojan Stealer***) după care, odată cu activarea funcției *Macro*, este instalat un program malițios cu ajutorul căruia **sunt extrase date din sistemul informatic**.

RECOMANDĂRI

Se recomandă, în primul rând, **verificarea adresei reale de mail a expeditorului** de pe care sunt transmise mesajele prin suprapunerea cursorului peste adresa expeditorului (caz în care trebuie să apară același expeditor).

Acțiunea trebuie întreprinsă mai ales în situația în care mesajul pare să vină de la o persoană legitimă, cunoscută, având un conținut identic cu cel al unui email primit anterior, fără a exista motive ca acesta să fi fost transmis din nou de la aceeași expeditor.

În același timp, **trebuie avuți în vedere** următorii pași:

- Implementarea de urgență a politicii DMARC la nivel de domeniu, măsura fiind necesară întrucât filtrele *anti-phishing* și *anti-spam* sunt cele mai eficiente în momentul implementării acestei politici. Astfel, pot fi evitate încă din fază incipientă atacurile care vizează infrastructurile cibernetice.
- Verificarea fluxului de mesaje email, în vederea identificării celor care conțin linkul malițios ***hxxps://onedrive[.]live[.]com/download?cid=AA923B0E0F7A6594&resid=AA923B0E0F7A6594%21107&authkey=ABibU7JaU8GKdaY*** ori altele similare (ce aparțin domeniului onedrive.live.com), specifice acestei campanii malițioase.
- În situația în care sunt identificate astfel de mesaje email, se impune verificarea sistemelor informatice pe care au fost deschise, în vederea stabilirii posibilelor infecții.
- Actualizarea filtrelor anti-spam (sa-learn).

Atașăm un ghid destinat administratorilor de domeniu pentru implementarea politicii DMARC, în varianta scurtă și extinsă. De asemenea, insistăm pentru implementarea următoarelor măsuri de securitate cibernetică cu caracter general:

- **Sporirea vigilenței,** care este principalul atu avut oricând la dispoziție de către un utilizator obișnuit. Trebuie manifestată atenție la verificarea emailurilor primite, în special a celor care conțin atașamente! Virusul ***Trojan Stealer*** este încă activ, se propagă prin intermediul emailului și vizează deopotrivă **persoane fizice, instituții publice** sau **companii private**.
- În cazul existenței unor suspiciuni legate de veridicitatea conținutului mesajului, **se impune verificarea autenticității informațiilor oferite** de către presupusul expeditor direct cu acesta, utilizând alt canal de comunicare (preferabil telefonul).
- **Scanarea cu o soluție de securitate** instalată pe dispozitiv, sau cu una disponibilă gratis online, pentru **link-urile sau atașamentele suspecte** din căsuța dvs. de mail. Nu uitați să aplicați la timp update-urile pentru aceste soluții de securitate!
- Scanarea cu antivirus nu este suficientă însă. ***Trojan Stealer*** nu este ușor de identificat și interceptat, deoarece **eludează de multe ori soluțiile antivirus** convenționale.
- Implementarea de **filtre la gateway-ul de email** pentru a înlătura e-mailurile cu indicatori cunoscuți de spam sau malware și pentru a bloca adresele IP suspecte din firewall.
- **Emailurile suspecte trebuie raportate departamentului IT** pentru izolare și investigare. Verificați periodic regulile contului de e-mail, ce pot fi setate pentru redirecționarea automată a tuturor mesajelor, ceea ce ar putea duce la o scurgere de date, dacă există o infecție.
- Pentru a vă proteja eficient împotriva ***Trojan Stealer***, trebuie să vă concentrați în principal pe poarta principală de acces a malware-ului: comunicarea prin e-mail. ***Trojan Stealer*** **se ascunde adesea în fișierele Microsoft Office și are nevoie de macrocomenzi** pentru a putea instala malware-ul dorit, este logic să nu le permiteți. Dacă totuși nu vă puteți desfășura activitatea fără macrocomenzi, este posibil să le permiteți numai celor semnate.
- **Actualizarea de urgență a** sistemelor de operare, programelor antivirus, browserelor web, clienților de e-mail și a programelor de tip Office.
- **Accesul la rețea ar trebui monitorizat continuu** de către cei responsabili din Departamentele IT, deoarece astfel se poate determina în timp util dacă a apărut o infecție cu **Trojan Stealer**.
- **Dezactivarea serviciilor neutilizate**. **Trojan Stealer** profită adesea de vulnerabilitățile identificate în serviciile care rulează în background, pentru a se răspândi pe alte computere din rețea. Remote Desktop Protocol (RDP), tehnologia care ne permite lucrul de la distanță, este un astfel de exemplu. Utilizatorilor li se recomandă să dezactiveze astfel de servicii dacă nu sunt necesare, pentru a împiedica malware-ul să le exploateze și să se propage în rețea.
- **Instalarea unei soluții de control al aplicațiilor.** Utilizatorii pot lua în considerare instalarea unui astfel de software care oferă listă albă de aplicații și/sau directoare. Astfel, se permite rularea exclusiv a programelor aprobate, în timp ce se restricționează altele. Este o practică bună de securitate pentru a proteja un sistem informatic.
- **Nu ezitați să contactați Directoratul**, în cazul în care suspectați că grupul sau contul dumneavoastră de Signal a fost compromis sau a fost subiectul unui atac.

alerts@dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #awareness