DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ALERTĂ
28.06.2022

E-mail-uri cu atașamente malițioase care folosesc identitatea vizuală ANAF

UNCLASSIFIED / NECLASIFICAT

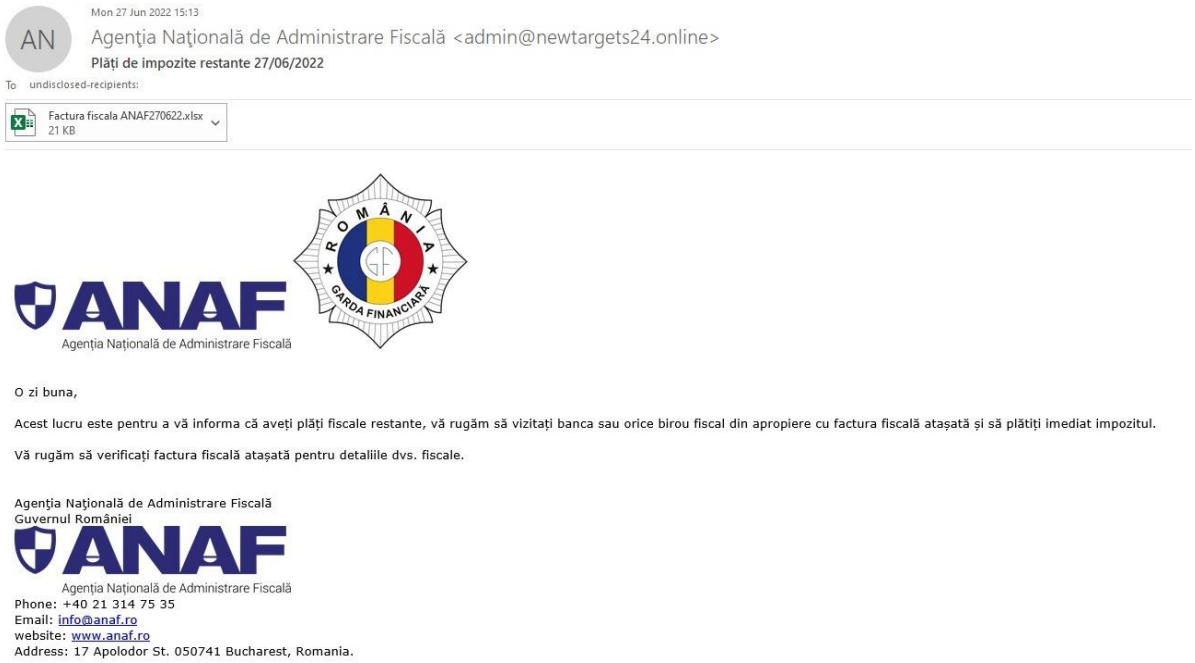
În ultimele zile, Directoratul Național de Securitate Cibernetică (DNSC) a observat o creștere notabilă a utilizării malware-ului **LokiBot** în atacuri propagate prin intermediul serviciului de e-mail.

Infractori cibernetici folosesc identitatea vizuală a Agenției Naționale de Administrare Fiscală (ANAF) pentru a transmite prin intermediul unor e-mail-uri cod malițios. Mulți utilizatori au observat că este vorba despre un atac și nu un e-mail legitim din partea autorității și au notificat autoritățile.

Descriere

Metoda de atac - e-mail-uri nesolicitate care copiază identitatea vizuală a unor instituții sau organizații cu reputație – este des folosită de atacatori pentru a oferi potențialelor victime un scenariu plauzibil, mizând în același timp pe emoționarea utilizatorului pentru a-l face mai puțin vigilent.

În acest caz, textul folosit de atacatori face referire la acest stimul psihologic încă de la început, destinatarii e-mail-ului fiind anunțați că au 'plăți restante fiscale', iar pentru a verifica situația trebuie să acceseze 'factura fiscală atașată'. Odată descărcat și accesat, atașamentul duce la infectarea dispozitivului cu malware-ul LokiBot.



Mon 27 Jun 2022 15:13

AN Agenţia Naţională de Administrare Fiscală <admin@newtargets24.online>

Plăți de impozite restante 27/06/2022

To undisclosed-recipients:

Factura fiscala ANAF270622.xlsx
21 KB

ANAF
Agenția Națională de Administrare Fiscală

ROMÂNIA
GARDA FINANCIARĂ

O zi buna,

Acest lucru este pentru a vă informa că aveți plăți fiscale restante, vă rugăm să vizitați banca sau orice birou fiscal din apropiere cu factura fiscală atașată și să plătiți imediat impozitul.

Vă rugăm să verificați factura fiscală atașată pentru detaliile dvs. fiscale.

Agenția Națională de Administrare Fiscală
Guvernul României

ANAF
Agenția Națională de Administrare Fiscală

Phone: +40 21 314 75 35
Email: info@anaf.ro
website: www.anaf.ro
Address: 17 Apolodor St. 050741 Bucharest, Romania.

Impact

LokiBot, cunoscut și sub denumirile alternative de *Lokibot*, *Loki PWS* și *Loki-bot* - utilizează o variantă de malware tip troian, având ca scop principal furtul de informații sensibile, cum ar fi nume de utilizator, parole, portofele de criptomonede și alte credențiale. Reușește să facă acest lucru prin utilizarea unui *keylogger* care monitorizează activitatea din browser și de pe calculator, reușind să înregistreze informațiile tastate pe dispozitivul infectat.

Actorii cibernetici rău intenționați folosesc de obicei LokiBot pentru a viza sistemele de operare Windows și Android și de multe ori distribuie malware-ul prin intermediul atașamentelor malițioase anexate unor e-mail-uri nesolicitate, site-uri web malițioase, mesaje text sau platforme de mesagerie.

Remediere

Principalele recomandări pe care echipa DNSC le oferă în astfel de cazuri se referă în primul rând la prevenție. De fiecare dată când primiți un mesaj nesolicitat, trebuie să fiți atenți și să verificați sursa mesajului primit. În acest caz, dacă se accesau informațiile din *header*-ul mail-ului, se putea observa că mesajul a fost transmis de pe domeniul **newtargets24.online** și nu de pe anaf.ro.

Mai departe, dacă utilizatorul era atent la textul mesajului, observa că este cel mai probabil tradus automatizat în română dintr-o limbă străină, deoarece există greșeli clare de exprimare care pot fi identificate imediat. Formula inițială de adresare din mail (‘o zi bună’) este una des utilizată în încheierea unui mesaj, nu la începutul lui. În continuare, textul sună extrem de ciudat, ceea ce ar fi trebuit să ridice serioase semne de întrebare destinatarului (‘Acest lucru este pentru a vă informa’) cu privire la legitimitatea acestui mail.

În plus, dacă utilizatorul analiza atașamentul din e-mail cu o soluție de securitate existentă pe dispozitiv, ori una disponibilă gratis online (ex: VirusTotal), își putea da imediat seama că este vorba despre un fișier infectat cu malware.

Pentru a antrena utilizatorii din România să identifice și să evite astfel de atacuri cu malware, Directoratul Național de Securitate Cibernetică, Poliția Română și Asociația Română a Băncilor, alături de parteneri din zona privată precum Microsoft Romania, BIT SENTINEL, ATTACK Simulator, ANIS sau Dekeneas au lansat modulul ANTI-MALWARE din cadrul campaniei de conștientizare la nivel național sigurantaonline.ro. Acest site este un instrument util utilizatorilor de toate vârstele pentru a-și îmbunătăți igiena de securitate cibernetică.

Recomandări pentru utilizatori

- Fiți atenți la deschiderea atașamentelor de e-mail, chiar dacă atașamentul este așteptat și expeditorul pare să fie cunoscut! Verificați mereu sursa reală a mesajului din *header*-ul e-mail-ului primit;
- Folosiți o soluție de securitate pe dispozitive, actualizată la zi;
- Actualizați frecvent sistemului de operare și programele/aplicațiile folosite;
- Puneți în aplicare autentificarea multi-factor pentru conturile folosite, iar acolo unde nu este posibil, folosiți parole unice, puternice și complexe;

Recomandări pentru organizații

- Pentru a evita răspândire malware-ului în rețea, dezactivați serviciile de partajare de fișiere și imprimante. Dacă aceste servicii sunt absolut necesare, utilizați parole puternice sau autentificare Active Directory;
- Restricționați capacitatea (permisiunilor) utilizatorilor de a instala și rula aplicații software nedorite. Nu adăugați utilizatori în grupul administratorilor locali, cu excepția cazului în care este absolut necesar;

- Puneți în aplicare o politică clară de stabilire a parolelor puternice pentru conturile folosite de angajați;
- Activați un firewall personal pe stațiile de lucru ale agenției, configurat pentru a refuza solicitările de conectare nesolicitate;
- Dezactivați serviciile inutile de pe stațiile de lucru și serverele organizației;
- Scanați și eliminați atașamentelor suspecte de e-mail;
- Monitorizați obiceiurile de navigare pe web ale utilizatorilor și restricționați accesul la site-uri cu conținut nefavorabil;
- Fiți atenți atunci când utilizați suporturi externe (USB stick, HDD extern, CD-uri, etc);
- Scanați toate software-urile descărcate de pe internet înainte de execuție;
- Mențineți un nivel de informare optim al angajaților cu privire la cele mai recente amenințări și puneți în aplicare listele adecvate de control al accesului.

Surse

CISA

SigurantaOnline

DNSC – Ghid de Securitate cibernetică

alerts@dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #awareness