Raport consolidat eveniment cibernetic

njRat

njRAT (alias Bladabindi) este un troian de acces la distanță folosit pentru a controla mașinile infectate. njRAT, la fel ca mulți troieni de acces la distanță, funcționează pe principiul **reverse backdoor**. După crearea malware-ului (clientul) și deschiderea acestuia, serverul atacatorului primește o solicitare din partea clientului. După o conexiune reușită, atacatorul poate controla computerul victimei trimițând comenzi către server iar clientul le procesează.

După infectarea malware-ul se copiază în **„TEMP", „APPDATA", „USERPROFILE"**. De asemenea, se poate copia în fișiere **.exe**, pentru a se asigura că va fi activat de fiecare dată când victima pornește computerul.

Troianul njRAT are câteva trucuri în mânecă pentru a evita detectarea de către programele antivirus. De exemplu, folosește mai multe obfuscatoare **.NET** pentru a-și obstrucționa codul. O altă tehnică pe care o folosește acest malware este deghizarea într-un proces critic, blocând capacitatea utilizatorului de a-l închide.

Informații suplimentare

TIP	***Troian***
Instrumente pentru analiză	Pentru scanarea rețelei – Wireshark, TCPDUMP, Angry IP Scanner Pentru scanarea de viruși și malware – Software antivirus existente Analiză și detectare procese- Lordpe, Sysmon , Procces Hacker
Recomandări împotriva infectării:	• **Endpoint Security:** njRat este o variantă de malware cunoscută și stabilită, deci o soluție de securitate a punctelor terminale ar trebui să fie capabilă să identifice și să prevină infectarea. • **Email Scanning:** e-mailurile de tip phishing sunt una dintre metodele principale pe care njRat le folosește pentru a se propaga. • **Web Security:** O soluție de securitate web poate identifica și bloca conținutul rău intenționat înainte de a putea fi descărcat pe dispozitiv. • **Removable Media Security:** njRat este, de asemenea, capabil să se răspândească prin intermediul unităților USB infectate. • **Account Security:** njRat are capacitatea de a efectua înregistrarea tastelor și de a fura acreditările utilizatorului. Implementarea celor mai bune practici de securitate a contului poate face dificil pentru atacatori să folosească aceste acreditări compromise pentru a-și atinge obiectivele.

IOC	**IP addresses** 172.67.135.130 185.199.109.133 144.126.144.223 192.121.87.108 193.42.33.179 5.35.153.131 **URLs** https://pastebin.com/raw/UgsiXFgH https://pastebin.com/raw/YKgY3s0H https://pastebin.com/raw/rdmzbeYW https://pastebin.com/raw/Hu1K7Y4W https://pastebin.com/raw/VGGi28kN https://pastebin.com/raw/jxx7yjgK http://troia23.duckdns.org:1177/ https://pastebin.com/raw/Xde8ekvN https://pt.textbin.net/download/insdj4bhn2 https://pastes.io/download/g4enqwgps4 https://pastebin.com/raw/Hu1K7Y4W https://pastebin.com/raw/VGGi28kN https://pastebin.com/raw/jxx7yjgK https://6ded-177-50-200-148.ngrok-free.app/ https://pastebin.com/raw/vZM3LPTw https://pt.textbin.net/download/rcd5ihynxw
Recomandări generice	• **Izolarea dispozitivului compromis** -Identificați dispozitivul sau sistemele suspecte și izolați-le de rețeaua principală. Izolarea poate fi efectuată prin deconectarea fizică a dispozitivelor sau restricționarea accesului acestora la rețea. • **Scanarea și curățarea dispozitivelor compromise -** Înainte de a începe scanarea pentru sistemelor Windows este necesar de dezactivat ***System Restore*** pentru a permite scanarea totala a calculatorului. Utilizați un antivirus actualizat pentru a șterge fișierele detectate ca ***Backdoor.MSIL.BLADABINDI.THA***. Dacă fișierele detectate au fost deja curățate, șterse sau puse în carantină nu este necesar niciun pas suplimentar • **Curățarea registrului** - Ștergeți valorile registrului (***fiți atenți editarea incorectă a Windows Registry poate duce la defecțiuni ireversibile ale sistemului***). Curățați Registrul pentru oricare dintre valorile manipulate. Manipulările de registru a botnet-ului constau în crearea cheii cu un nume ciudat ***„[kl]” într-un stup HKEY_CURRENT_USER\Software\32*** cu valoarea unui set aleatoriu de caractere și cifre. • **Resetarea dispozitivelor la starea implicită -** În cazul dispozitivelor care nu pot fi curățate sau încredințate, luați în considerare resetarea acestora la setările implicite de fabrică. Asigurați-vă că după resetare toate parolele implicite sunt schimbate și actualizate. • **Reevaluarea securității rețelei -** Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.