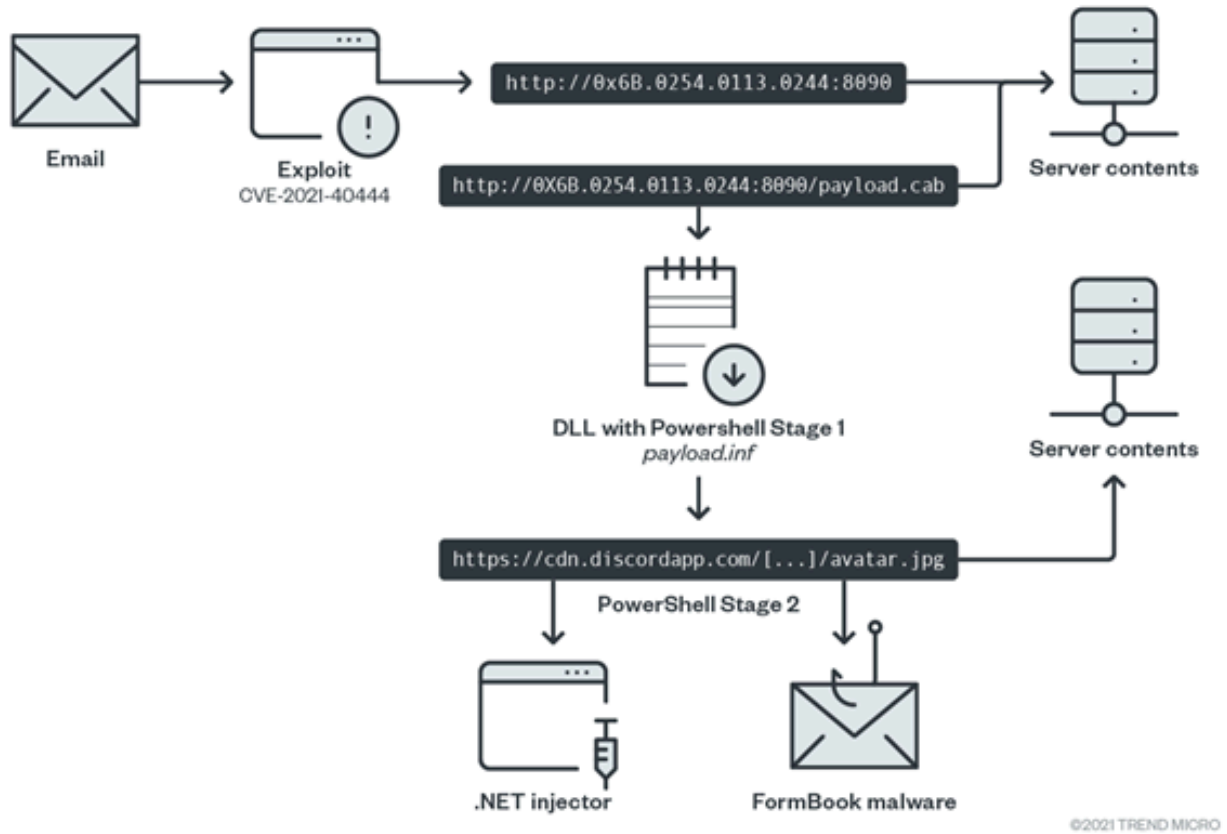
Raport consolidat eveniment cibernetic

FormBook

FormBook este un infostealer cu trăsături de troian și botnet. Deși principalul său rol este de infostealer, poate avea mai multe funcționalități periculoase: furt de credențiale, informații de autentificare, date din browsere sau aplicații. În unele cazuri, poate fi utilizat ca parte a unui botnet pentru a compromite mai multe sisteme și pentru a le folosi în campanii de atac, precum distribuirea de spam sau lansarea de atacuri DDoS.



Răspândire prin email a FormBook, utilizând vulnerabilitatea CVE-2021-40444

Informații suplimentare

TIP	***Infostealer***
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
Infectare	FormBook cel mai des este răspândit prin e-mail utilizând o gamă largă de mecanisme de infectare și se poate conține într-o serie de atașamente ca fișiere : **PDF, doc, RTF, png, zip, exe, rar.** El profită de diferite vulnerabilități a sistemului ca: **CVE-2012-0158, CVE-2017-1182, CVE-2017-0199, CVE-2021-40444.** După infectare, virusul se copie și redenumește într-un director care diferă în funcție de privilegiile utilizatorului. Dacă se folosește un cont de administrator, virusul se instalează fie în **%ProgramFiles%**, fie în **%CommonProgramFiles%**. Dacă privilegiile nu sunt, atunci virusul se va copia în **%TEMP%** sau **%APPDATA%**.
IOC	**IP adrese publice** 82.180.175.114 172.67.177.75 154.23.147.231 206.188.193.90 152.199.21.175 54.150.239.82 172.67.160.165 178.20.227.11 154.80.192.235 **Hash** 71e33ab4047596129fe18f2d2304254b1ff0128096e3a8b07f75f779afd130b7 48006427b80726e2434323dd1b06e988912741080e00c29b2913a3749e50755c 8acf4c88e097cfcba3bfa08c24884c446bb943f5a3b5eb610f50db67574de771 **Domene** 1385.net 02s-pest-control-us-ze.fun amilablackwell.online commerce-74302.bond 458881233.men

Detectare	• Folosiți o soluție Endpoint Detection and Response (EDR) pentru a identifica infecțiile și a iniția procesul de remediere • Monitorizează activitatea rețelei în căutarea unor conexiuni externe neobișnuite, în special către servere C&C utilizate de botnet. • Scanați sistemul cu o soluție antivirus actualizată. • identificați prezența folderului cu numele static **„3r9Pk-75”** sau a bibliotecelor malware specifice (ex. **wininet.dl**).
Recomandări generice	• **Izolarea dispozitivului compromis** - Identificați dispozitivul sau sistemele suspecte care ar putea face parte din botnet și izolați-le de rețeaua principală. Izolarea poate fi efectuată prin: deconectarea fizică a dispozitivelor sau restricționarea accesului acestora la rețea. • **Întreruperea comunicării cu serverul de comandă și control (C&C)** - Blocați traficul de ieșire către adresele IP cunoscute asociate cu serverele de comandă și control ale botnet-ului, le găsiți în descrierea din Anexă. Pentru aceasta utilizați firewall-uri sau soluții de filtrare a traficului. • **Actualizarea software-ului și a sistemelor (patch &update)** - Asigurați-vă că toate dispozitivele și sistemele din rețea sunt actualizate la cele mai recente versiuni, inclusiv sistemele de operare, aplicațiile și software-ul de securitate. Acest lucru ajută la remedierea vulnerabilităților cunoscute și la prevenirea reinfectării. • **Scanarea și curățarea dispozitivelor compromise** - Utilizați un antivirus actualizat și soluții anti-malware pentru a scana toate dispozitivele compromise în căutarea amenințărilor. Eliminați sau izolați fișierele și programele malware identificate. • **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. • **Analiza log-urilor** - Analizați log-urile de securitate pentru a identifica activitatea suspectă și modelele de atac. Astfel puteți afla dacă unele porturi au rămas deschise sau sunt configurate greșit, iar remedierea acestor vulnerabilități va ajuta la creșterea nivelului de securitate din rețeaua locală. • **Reevaluarea securității rețelei** - Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.