Distribuirea malware-ului Noodlophile Stealer & XWorm prin site-uri AI false

<table>
<tr><td>Descrierea generală</td><td colspan="3">O campanie de malware activă exploatează popularitatea instrumentelor AI pentru a păcăli utilizatorii să descarce fișiere infectate. Atacatorii creează site-uri false care pretind a fi platforme AI de generare video, promovate prin reclame pe Facebook și postări virale.
Utilizatorul este instruit să încarce un fișier pentru a primi o versiune „AI generată”, însă descarcă un fișier .zip care conține executabile malițioase.</td></tr>
<tr><td colspan="4">Conținutul arhivei și componentele malware</td></tr>
<tr><td rowspan="11">Variante de denumiri</td><td>Denumire posibilă</td><td colspan="2">Observații</td></tr>
<tr><td>MachineAI.mp4.exe</td><td colspan="2">Înlocuire ordinii cuvintelor</td></tr>
<tr><td>GenerateVideoAI.exe</td><td colspan="2">Eliminarea extensiei false .mp4</td></tr>
<tr><td>AI_Video_Generator_Pro_2025.mp4.exe</td><td colspan="2">Adăugarea unor detalii „credibile”</td></tr>
<tr><td>CapCutAI2025.mp4.exe</td><td colspan="2">Se asociază cu aplicații video reale (ex. CapCut)</td></tr>
<tr><td>DeepDreamFX_VideoAI.mp4.exe</td><td colspan="2">Folosire de termeni legați de AI (DeepDream etc.)</td></tr>
<tr><td>AICore.dll</td><td colspan="2">DLL folosită pentru execuția codului</td></tr>
<tr><td>Document.docx</td><td colspan="2">BAT obfuscat, deghizat ca fișier Word</td></tr>
<tr><td>Document.pdf</td><td colspan="2">Arhivă RAR în Base64, mascată ca fișier PDF</td></tr>
<tr><td>meta / images.exe</td><td colspan="2">Utilitar WinRAR ce extrage fișierele în fundal</td></tr>
<tr><td>Randomuser2025.txt</td><td colspan="2">Script Python obfuscat ce încarcă Noodlophile Stealer și/sau XWorm în memorie</td></tr>
<tr><td>srchost.exe</td><td colspan="2">Loader Python ce finalizează execuția și injectarea malware-ului</td></tr>
<tr><td>RunMeToStartAI.mp4.exe</td><td colspan="2">Incitarea utilizatorului să execute fișierul</td></tr>
<tr><td rowspan="6">Extensii dublu mascate sau ascunse</td><td>Exemplu fișier</td><td>Ce este de fapt</td><td>Explicație</td></tr>
<tr><td>videoAI.mp4.exe</td><td>Executabil Windows</td><td>Pare fișier video, dar e .exe</td></tr>
<tr><td>documentAI.pdf.exe</td><td>Executabil Windows</td><td>Pare fișier PDF</td></tr>
<tr><td>presentationAI.ppt.scr</td><td>Script autoexecutabil</td><td>Mascat ca PowerPoint</td></tr>
<tr><td>cvAI.docx.bat</td><td>Script de comandă</td><td>Mascat ca document Word</td></tr>
<tr><td>genAI.jpg.js</td><td>Script JavaScript (browser)</td><td>Pare imagine dar lansează cod</td></tr>
<tr><td>Funcționalitate malware</td><td colspan="3">❖ Noodlophile Stealer
• Tip: Informație Stealer
○ Comportament:
✓ Exfiltrare acreditive browser
✓ Furt portofele crypto
✓ Trimiterea datelor prin Telegram Bot
✓ Colectare fișiere locale și date sensibile
❖ XWorm RAT (opțional)
• Tip: Remote Access Trojan
○ Tehnici de evaziune:
✓ Shellcode injection
✓ PE hollowing</td></tr>
</table>

Distribuirea malware-ului Noodlophile Stealer & XWorm prin site-uri AI false

	✓ Persistență și control la distanță
Vector de livrare	Promovare prin *Facebook Ads* și postări virale Site-uri care imită interfețe *AI* (ex. „Dream AI Generator") Arhive .zip mascate ca fișiere media/video

Tactici, Tehnivi și Proceduri (TTPs) – MITRE ATT&CK

Tactică	Tehnică	Cod MITRE	Descriere
Execuție	User Execution via Double Extension	T1204.002	Utilizatorul execută .exe mascat ca .mp4
Persistență	Registry Run Keys	T1547.001	Adăugare în registry pentru lansare automată
Exfiltrare	Exfiltration Over Web Service	T1567.002	Trimitere date prin Telegram Bot
Recunoaștere	System Information Discovery	T1082	Colectare date despre sistemul infectat
Comandă și control	Application Layer Protocol: Telegram	T1071.001	Canal C2 prin aplicație populară

Recomandări de securitate	1. Evitați site-urile necunoscute care oferă aplicații *AI* 2. Verificați extensiile fișierelor descărcate (ex. .exe mascat ca .mp4) 3. Rulați un antivirus actualizat 4. Monitorizați sistemul pentru procese neobișnuite (ex. srchost.exe) 5. Inspectați conexiunile *Telegram* suspecte 6. Utilizați un mediu sandbox pentru analiza fișierelor necunoscute
Măsuri de răspun și remediere	1. Izolare imediată a endpoint-urilor infectate 2. Ștergerea fișierelor suspecte și curățarea registrului 3. Resetarea tuturor conturilor compromise 4. Revizuirea traficului *Telegram* și blocarea *C2* 5. Scanare completă cu *EDR/XDR* 6. Actualizarea politicilor de securitate privind descărcările *AI* nevalidate
Referință	https://securityonline.info/ai-tools-turn-trojan-fake-video-platforms-drop-noodlophile-stealer-and-xworm-payloads/