Operation ForumTroll

Descriere	Kaspersky a identificat o campanie de spionaj denumită *Operation ForumTroll* care exploatează un zero-day în Google Chrome (CVE-2025-2783) pentru a obține execuție de cod la distanță și a scăpa din sandbox, permițând astfel livrarea succesivă a unui loader și a unui spyware sofisticat (componenta finală identificată de Kaspersky ca fiind *Dante* / produs comercial Memento Labs). Exploatarea se realiza prin simpla vizitare a unei pagini web-malware distribuite prin e-mailuri de tip phishing direcționate. Impact: compromitere silentioasă a posturilor care vizitează link-urile (RCE → escaladare din sandbox → persistenta + exfiltrare documente), folosită pentru colectare de date sensibile (documente office), keylogging și controle C2 criptate.
Indicatori-cheie	✓ Vulnerabilitate exploatată: CVE-2025-2783 (Chrome sandbox escape prin manipulare/validare incorectă a pseudo-handle-urilor Windows). ✓ Chrome patched: Chrome 134.0.6998.177 / .178 (remediu publicat). ✓ Tehnici folosite: validator WebGPU (ECDH) → loader în font/JS falsificate → COM hijacking (override CLSID, twinapi.dll) → încărcare DLL malitioasă → spyware (LeetAgent loader + Dante ca payload final). ✓ Comunicări C2: HTTPS cu multiple straturi de obfuscare; infrastructură suprapusă cu CDN (Fastly) observată. ✓ Ținte: instituții media, universități, centre de cercetare, organizații financiare și guvernamentale, în principal în Rusia și Belarus (campanie cu lure legat de „Primakov Readings”).
Lanțul atacului (TTP)	✓ Phishing targetat — e-mail în limba rusă, conține link scurt/efemer spre site fals care imită pagina forumului Primakov Readings. ✓ Landing page / Validator — pagină web care folosește WebGPU pentru a valida „vizitatorul uman”; efectuează ECDH pentru a decripta următorul stadiu ascuns în fișiere JS / font. ✓ Exploit CVE-2025-2783 — eroare de logic în gestionarea pseudo-handlurilor Windows (ex. -2 returnat de GetCurrentThread()) permisă prin IPC Chrome → escalate sandbox → execuție în proces browser. ✓ Loader multi-stadiu — validator → loader (deobfuscare) → payload în formă binară criptată; loader verifică prezența în procese țintă și decriptează doar în contexte specifice (stealth). ✓ Persistență — COM hijacking prin suprascrierea/înregistrarea CLSID-urilor (ex: twinapi.dll CLSID) astfel încât procese legitime să încarce DLL-uri malițioase. ✓ Payload final — LeetAgent (loader/spyware) care instalează/lansează Dante (Memento Labs); capabilități: keylogging, colectare și exfiltrare documente (.doc/.xls/.pdf/.pptx), comenzi remote; antidebugging, anti-sandbox, VMProtect packing; configurații criptate (XOR + AES-256-CBC), key bound to HWID. ✓ Comunicare & exfiltrare — conexiuni HTTPS cu multiple straturi de obfuscare, folosind infrastructuri legitime/CDN (Fastly) pentru camuflare
Analiza tehnică	
Mecanism de exploatare	Problema centrală este o validare logică insuficientă a pseudo-handle-urilor Windows (ex: valoarea -2 de la GetCurrentThread() sau alte pseudo-handle valori), care, prin mecanisme IPC nevalidate, permite ca un renderer sandboxed să provoace comportament nedorit/execuție în procesul browserului sau alt proces cu privilegii mai mari. Aceasta este o sandbox escape prin logica IPC.
Validator	Validatorul folosește WebGPU (API grafic modern) pentru a forța execuția unor operațiuni criptografice (ECDH) în browser și a decripta stadiul următor (payload ascuns în resurse aparent inofensive: scripturi, fonturi). Aceasta complică analiza statică și reduce detectabilitatea.
Persistență (COM hijacking)	Atacatorii suprascriu sau reînregistrează CLSID în registry astfel încât apeluri legitime la componente COM (în special legate de twinapi.dll) să conducă la încărcarea DLL-urilor

	malițioase. Această tehnică oferă încărcare în contexte privilegiate și reutilizare a mecanismelor legitime OS.
Malware final — LeetAgent & Dant	✓ *LeetAgent*: componente de control (comenzi cu ID-uri în leetspeak), keylogging, colectare extensii documente, comunicații C2 criptate. ✓ *Dante* (Memento Labs): arhitectură modulară, tehnici anti-analiză (VMProtect, anti-debug, anti-sandbox), configurare criptată (XOR + AES-256-CBC), key-binding la hardware. Legătura la Memento Labs se bazează pe similarități de cod, infrastructură și tehnici; Kaspersky a identificat această legătură.
IoC	✓ Regiștri / Registry • Modificări la chei CLSID/COM asociate twinapi.dll sau alte CLSID neașteptate: HKCR\CLSID\{...} schimbări recente — comparați cu backup de inventar. • Chei de autorun/Run care încarcă DLL-uri necunoscute. ✓ Fișiere / Procese • Fișiere DLL noi încărcate de procese legitime (explorer.exe, svchost.exe, orice proces asociat twinapi). • Executabile/ DLL cu semnături VMProtect sau binare packate strâns. • Fișiere cu nume/și/sau timestamp-uri ce conțin pattern-uri obfuscated JS/font payload decode. ✓ Rețea • Conexiuni HTTPS ieșire către domenii noi sau rotații frecvente, folosind Fastly/CDN-like IP ranges; monitorizare eșantionată a SNI/Host header în TLS (unde e posibil). • Trafic cu payload mici, criptate, din procese de user-land (browser) către host-uri externe. ✓ Comportament • Procese browser care lansează activități neobișnuite (spawn de procese native, scriere în registry, încărcare DLL în procese de sistem). • Detectare keylogging: hook-uri în procese UI sau API hooking. ✓ Sugestii de căutări (Elastic/SIEM / EDR) • Events: ProcessCreate where ParentImage is chrome.exe AND child loads *.dll into explorer.exe|svchost.exe within short time window. • Registry: changes to HKCR\CLSID* where LastWriteTime in timeframe scan. • Network: TLS connections to dynamic hostnames resolved to Fastly IP space shortly after suspicious process spawn.
Semnale EDR / XDR	✓ Alertare la *chrome.exe* care face RPC/IPC către alte procese sau scrie/execuă binare în *%TEMP%* ori *%AppData%* în sesiune web. ✓ Detectare modificări ale CLSID/COM registration: generare alertă dacă *HKCR\CLSID\{*}* este creat/actualizat de procese non-admin sau neobișnuite. ✓ Detectare execuție de cod de tip Dynamic DLL load (LoadLibrary) în procese legate de *twinapi.dll* sau în contexte sistem.
Măsuri de remediere și atenuare	✓ Acțiuni imediate • Se actualizează Google Chrome la versiunea 134.0.6998.177/178 sau mai nouă. • Se izolează sistemele suspecte și se colectează artefactele (RAM, jurnale EDR, evenimente Sysmon). • Se rulează scanări complete cu soluția EDR/antivirus și se verifică modificările în HKCR\CLSID. • Se resetează parolele și se revocă token-urile conturilor afectate. ✓ Corective • Se elimină intrările COM hijack și se restaurează cheile CLSID legitime. • Se șterg fișierele și DLL-urile malițioase identificate. • Se verifică integritatea sistemului și se aplică ultimele patch-uri OS și aplicații. ✓ Preventive • Se activează politici de control aplicații (AppLocker/WDAC) pentru blocarea încărcării DLL-urilor neautorizate.

	• Se dezactivează temporar WebGPU pe stațiile critice. • Se configurează monitorizarea permanentă a modificărilor COM/Registry și a proceselor derivate din chrome.exe. • Se implementează filtrare egress și alertare pe conexiuni HTTPS anormale.
Referință	https://securityonline.info/kaspersky-exposes-chrome-zero-day-rce-cve-2025-2783-delivering-memento-labs-spyware-in-forumtroll-campaign/ https://securelist.com/operation-forumtroll/115989/?utm_source=chatgpt.com