AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Sulmi i zinxhirit të furnizimit që shfrytëzon infrastrukturën e përditësimit të Notepad++ për shpërndarjen e malware-ve

Data: 04/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Studiuesit e sigurisë kanë identifikuar një sulm shumë të sofistikuar qe synon zinxhirin e furnizimit, i cili i atribuohet një grupi APT të sponsorizuar nga shteti.

Informacione Teknike

Fushata abuzoi me infrastrukturën e kompromentuar që hostonte shërbimin zyrtar të përditësimit Notepad++ për të ofruar në mënyrë selektive një back door të personalizuar më parë, të padokumentuar, të quajtur Chrysalis, te viktimat e synuara.

Komprometimi nuk buronte nga dobësitë në vetë kodin burimor të Notepad++. Në vend të kësaj, sulmuesit arritën akses në nivel infrastrukture te ofruesi i përbashkët i hostimit, duke mundësuar përgjimin selektiv dhe ridrejtimin e trafikut të përditësimit të destinuar për notepad-plus-plus.org. Kjo i lejoi aktorit keqdashës të shpërndante ngarkesa të dëmshme të përditësimit te viktimat e zgjedhura me kujdes pa shkaktuar zbulim të gjerë.
Fushata ishte aktive nga qershori 2025 deri të paktën në nëntor-dhjetor 2025, duke synuar organizatat e lidhura me objektivat historike të spiunazhit të Lotus Blossom, duke përfshirë qeverinë, telekomunikacionin, aviacionin, infrastrukturën kritike dhe sektorët e medias.
Në thelb të këtij operacioni ishte Chrysalis, një backdoor e personalizuar me shumë funksione, e ofruar përmes një zinxhiri ngarkues me shumë faza, duke shfrytëzuar ngarkimin anësor të DLL, shellcode të enkriptuar, pjesët e brendshme të padokumentuara të Windows (Microsoft Warbird) dhe një përzierje të malware të personalizuar me mjete të dobishme si Metasploit dhe Cobalt Strike. Kjo fushatë demonstron një evolucion të qartë në artin e Lotus Blossom dhe nxjerr në pah rrezikun e vazhdueshëm që paraqesin sulmet e synuara të zinxhirit të furnizimit kundër ekosistemeve të besuara të softuerëve.

Qasja Fillestare dhe Kompromentimi i Zinxhirit të Furnizimit
• Sulmi filloi nga një kompromentim i serverit të përbashkët të pritjes që hostonte infrastrukturën e përditësimit të Notepad++, konkretisht pikës fundore përgjegjëse për kthimin e URL-ve të shkarkimit të përditësimit.
• Sipas analizës forensike dhe regjistrave të ofruesit të pritjes:
o Serveri ishte i kompromentuar në mënyrë aktive deri më 2 shtator 2025.
o Edhe pse qasja direkte e serverit humbi pas mirëmbajtjes, kredencialet për shërbimet e brendshme mbetën të ekspozuara deri më 2 dhjetor 2025, duke mundësuar ridrejtimin e vazhdueshëm të trafikut.
• Sulmuesit ridrejtuan në mënyrë selektive trafikun e përditësimeve për domeinin notepad-plus-plus.org në serverat e kontrolluar nga sulmuesi, duke kthyer manifeste përditësimesh keqdashëse.
• Synimi ishte shumë selektiv, në përputhje me spiunazhin e sponsorizuar nga shteti dhe jo me shpërndarjen masive të programeve keqdashëse.

Pika kyçe: Asnjë provë nuk sugjeron shfrytëzimin e kodit të aplikacionit Notepad++; dobësia qëndronte në kontrollet e pamjaftueshme të verifikimit të përditësimeve në versionet më të vjetra të kombinuara me kompromentimin e infrastrukturës.

Treguesit e Kompromentimit janë përcjellë ne dokumentin e Excel-it

Rekomandime

AKSK rekomandon :

1. Përditësoni menjëherë Notepad++
o Instaloni manualisht versionin 8.9.1 ose më të ri
o Sigurohuni që certifikata dhe verifikimi i nënshkrimit WinGup është i aktivizuar

2. Proactive Threat Hunting IOC)
o Kryeni investigime të synuar nëpër pikat fundore, serverat dhe telemetrinë e rrjetit duke përdorur Treguesit e Kompromisit (IOC) të shoqëruara me këtë fushatë.
o Kërkoni për path-e të njohura të skedarëve, hash-e, aktivitet ngarkimi anësor i DLL-ve, artefakte të qëndrueshmërisë së shërbimit/regjistrit dhe zinxhirë të dyshimtë të ekzekutimit të proceseve