TLP: CLEAR

Cybersecurity Report

21.04.2025 - 02.05.2025

Stories

Zadné vrátka NodeJS infikujú používateľov prostredníctvom overení CAPTCHA

V marci 2025 výskumníci zo Trustwave SpiderLabs odhalili sofistikovanú malvérovú kampaň, ktorá inštaluje NodeJS backdoor cez falošné CAPTCHA obrazovky na kompromitovaných webových stránkach. Útok, súvisiaci s aktivitou KongTuke aktívnou od septembra 2024, začína návštevou infikovaného webu, kde škodlivý JavaScript zozbiera systémové údaje a kontaktuje C2 server. Ten odošle falošnú CAPTCHA výzvu, a pri jej vyplnení sa na pozadí spustí PowerShell príkaz, ktorý nainštaluje NodeJS a škodlivý kód YaNB (Yet Another NodeJS Backdoor). Tento malvér umožňuje ovládanie systému, krádež dát a udržanie prístupu cez úpravu registra, pričom sa maskuje ako aktualizácia prehliadača. Používa XOR šifrovanú komunikáciu, techniky na obchádzanie virtualizačného prostredia a môže sťahovať ďalšie škodlivé moduly. Hoci nie je priradené konkrétne CVE ani CWE, kampaň vykazuje vysokú úroveň sofistikovanosti a objavuje sa aj v iných hrozbách ako Mispadu a Lumma.

https://cybersecuritynews.com/new-stealthy-nodejs-backdoor-infects-users/

Phishing-as-a-service nástroje obchádzajú viacfaktorové overenie pomocou útokov typu adversary-in-the-middle

Vznikol rozsiahly podzemný trh s phishingovými nástrojmi, ktoré umožňujú útočníkom obchádzať bežné formy multifaktorového overenia (MFA), ako sú SMS kódy, e-maily alebo autentifikačné

aplikácie. Tieto útoky využívajú techniku adversary-in-the-middle (AitM), pri ktorej útočník umiestni proxy server medzi obeť a cieľovú webstránku. Výskumníci zo Cisco Talos upozorňujú, že dostupné phishing-as-a-service nástroje ako Tycoon 2FA, Rockstar 2FA, Evilproxy, Greatness a Mamba 2FA poskytujú hotové balíky vrátane falošných prihlasovacích stránok a skriptov na zachytenie prihlasovacích údajov aj jednorazových kódov. Útoky často začínajú podvodnou správou o tom, že účet bol kompromitovaný, a vyzývajú obeť, aby sa čo najskôr prihlásila na falošný odkaz, ktorý sa vizuálne podobá oficiálnej adrese. Takto útočník v reálnom čase zachytí prihlasovacie údaje aj druhý faktor, čím získa plný prístup k účtu napriek zapnutému MFA.

https://arstechnica.com/security/2025/05/phishing-attacks-that-defeat-mfa-are-easier-than-ever-so-what-are-we-to-do/

Útok zneužíva zraniteľnosť v Google OAuth a prechádza bezpečnostnými kontrolami Gmailu

Bol odhalený sofistikovaný phishingový útok, ktorý zneužíva zraniteľnosť v systéme Google OAuth a obchádza bezpečnostné filtre Gmailu vrátane DKIM overenia. Útočník vytvorí OAuth aplikáciu s vloženou phishingovou správou, ktorú následne Google sám odošle ako platne podpísané upozornenie z adresy no-reply@google.com. Táto správa obsahuje odkaz na subdoménu google.com, ktorá imituje prihlasovaciu stránku. Vývojár Nick Johnson z ENS bol medzi cieľmi a upozornil, že ide o tzv. DKIM replay attack. Google potvrdil problém a pripravuje opravu. Útok zneužíva dôveru v oficiálne autorizačné procesy namiesto klasických falošných stránok.

https://cybersecuritynews.com/googles-oauth-system-flaws/

GPT-4 vytvorilo funkčný exploit pre kritickú SSH zraniteľnosť v Erlang/OTP ešte pred zverejnením PoC

Bezpečnostný výskumník Matt Keeley demonštroval, že umelá inteligencia (GPT-4) dokáže vytvoriť funkčný exploit pre závažnú

zraniteľnosť ešte pred zverejnením verejného proof-of-concept (PoC). V prípade CVE-2025-32433, kritickej chyby s hodnotením CVSS 10.0 v SSH implementácii Erlang/OTP, GPT-4 nielen pochopilo popis chyby, ale aj identifikovalo opravnú zmenu v kóde, porovnalo ju s predchádzajúcou verziou, lokalizovalo zraniteľnosť a napísalo a odladilo funkčný exploit. Zraniteľnosť umožňuje neautentifikované vzdialené spustenie kódu s vysokými oprávneniami v dôsledku nesprávneho spracovania správ SSH protokolu počas úvodného spojenia. Keeley spustil analýzu po tweete výskumníkov z Horizon3.ai, ktorí zmienili existenciu PoC bez jeho zverejnenia. O deň po zverejnení chyby už viacerí výskumníci publikovali vlastné exploity, vrátane AI-asistovaného PoC od Platform Security.

https://cybersecuritynews.com/chatgpt-creates-working-exploit-for-cves/

Malvérna kampaň cieli na Docker a obchádza detekciu viacvrstvovou obfuskáciou

Bezpečnostní výskumníci z Darktrace a Cado Security Labs odhalili malvérnu kampaň zameranú na Docker prostredia, ktorá zneužíva nesprávne nakonfigurované alebo verejne prístupné služby na spustenie škodlivých kontajnerov. Útok sa začína spustením kontajnera z Docker Hubu s obrazom kazutod/tene:ten, ktorý spúšťa skript ten.py ukrytý vo vrstvách obrazu. Tento skript používa zreťazenú obfuskáciu: reverzovanie base64 reťazcov, ich dekompresiu cez zlib a následné spustenie – opakované 63-krát, kým sa odhalí finálny škodlivý kód. Namiesto klasického ťaženia kryptomeny cez nástroje ako XMRig malvér simuluje prevádzku uzla pre decentralizovanú sieť teneo.pro, aby získaval interné tokeny Teneo Points odmeňujúce aktivitu. Útočníci tak profitujú bez výrazného využitia systémových zdrojov a bez typických indikátorov ťaženia. Tento trend ukazuje posun od známych kryptominovacích nástrojov k zneužívaniu legitímnych platforiem.

https://cybersecuritynews.com/new-malware-hijacking-docker-images/
