TLP: CLEAR

Cybersecurity Report

16.06.2025 - 29.06.2025

Stories

Globálna malvérová kampaň zneužíva NFC platby na finančné podvody

Bezpečnostní výskumníci odhalili novú malvérovú kampaň NGate, ktorá cieli na NFC platobné systémy a zaznamenala 35-násobný nárast útokov v prvej polovici 2025. Útoky začali v Česku a rýchlo sa rozšírili globálne, pričom využívajú nástroj NFCGate, pôvodne určený na výskum, teraz zneužitý na reálne NFC relay útoky. Kampaň začína SMS phishingom, nasadením falošnej PWA aplikácie a následnou hlasovou manipuláciou obetí, ktoré sú presvedčené, aby priložili platobnú kartu k telefónu. NGate tak na diaľku prenesie NFC dáta k útočníkovi, ktorý ich vie okamžite zneužiť na platby bez fyzickej prítomnosti karty. Útoky sa ďalej vyvinuli do tzv. Ghost Tap schém, kde sú údaje obetí hromadne využívané cez automatizované Android zariadenia.

https://cybersecuritynews.com/eset-warns-of-nfc-data-for-contactless-payments/

Pokročilá APT kampaň zneužívajúca ClickOnce na útoky proti energetickému sektoru

Kampaň OneClik predstavuje novú sofistikovanú APT hrozbu zameranú na energetický, ropný a plynárenský sektor, kde útočníci zneužívajú technológiu Microsoft ClickOnce na doručenie škodlivého kódu. Útok začína phishingovými e-mailmi smerujúcimi obete na falošné diagnostické weby hostované cez Azure Blob Storage, odkiaľ sa spúšťajú škodlivé ClickOnce manifesty. Malware pozostáva z .NET načítača OneClikNet a zadných vrát RunnerBeacon napísaných v Go,

pričom komunikácia prebieha cez legitímne služby ako AWS CloudFront, API Gateway a Lambda, čo výrazne sťažuje detekciu. Zadné vrátka využívajú RC4 šifrovanie a MessagePack protokol na ovládanie infikovaných systémov, vrátane spúšťania shell príkazov, skenovania portov, tunelovania cez SOCKS5 a manipulácie s tokenmi.

https://cybersecuritynews.com/apt-hackers-abuse-microsoft-clickonce/

Nový malvér, ktorý pomocou prompt injection manipuluje s modelmi umelej inteligencie pri spracovaní vzorky

Výskumníci odhalili nový škodlivý kód s názvom Skynet, ktorý ako prvý dokumentovane využíva techniku prompt injection na oklamanie AI nástrojov používaných pri analýze malvéru. Skynet bol anonymne nahratý na VirusTotal v júni 2025 z Holandska a predstavuje dôkazový koncept zameraný na zneužitie veľkých jazykových modelov ako GPT-4 či Gemini, ktoré bezpečnostné tímy používajú na automatizovanú detekciu hrozieb. V C++ kóde bol ukrytý špeciálny prompt, ktorý sa snaží model donútiť, aby ignoroval pôvodné inštrukcie a označil kód za neškodný. Hoci testy ukázali, že moderné AI modely odolali tejto injekcii, samotný výskyt tejto techniky poukazuje na nový trend, v ktorom útočníci cielia priamo na AI vrstvy bezpečnostných systémov.

https://cybersecuritynews.com/new-malware-spotted-in-the-wild-using-prompt-injection/

Hackeri využívajú penetračný framework TeamFiltration na získanie prístupu k účtom Microsoft Teams, OneDrive, Outlook a ďalším

V kampani UNK_SneakyStrike útočníci zneužívajú legitímny nástroj TeamFiltration, pôvodne určený na bezpečnostné testovanie Office 365, na prevzatie tisícok Microsoft cloud účtov naprieč stovkami organizácií. Útoky využívajú funkcie nástroja na enumeráciu používateľov, password spraying a získavanie tokenov v rámci Microsoft OAuth aplikácií ako Teams, OneDrive či Outlook. Prístup si útočníci udržiavajú nahrávaním škodlivých súborov do OneDrivu,

ktoré maskujú ako bežné dokumenty. Väčšina prevádzky pochádza z USA, Írska a Británie a využíva infraštruktúru AWS. Vďaka technikám ako rotácia regiónov a spätné tiché fázy sú útoky efektívne a ťažko odhaliteľné.

https://cybersecuritynews.com/hackers-leverage-teamfiltration-pentesting-framework/

Pokročilé zneužitie .NET na skrytý malvér

Kybernetické hrozby sa posúvajú na novú úroveň, keď útočníci čoraz častejšie zneužívajú legitímne .NET frameworky na maskovanie malvéru. Nový nástroj WEAPONIZE_DOTNET, integrovaný v MacroPack Pro, umožňuje útočníkom transformovať nástroje ako Rubeus, SeatBelt, SharpDPAPI či SharpHound do ťažko odhaliteľných škodlivých payloadov. Využíva pri tom slabinu .NET architektúry, kde zostáva veľká časť symbolov zachovaná aj po kompilácii, čo uľahčuje obfuskáciu. Framework využíva pokročilé techniky ako prepis PInvoke na DInvoke (volanie API funkcií až za behu), dynamické mapovanie pre prípad použitia reflexie, a úplné embedovanie kódu, čím sa škodlivý kód nikdy neuloží na disk. Tento prístup efektívne obchádza antivírusy aj behaviorálnu analýzu a funguje na systémoch od Windows 7 po Windows 11.

https://cybersecuritynews.com/researchers-obfuscated-weaponized-net-assemblies/
