CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

DECEMBER 2025

TLP: CLEAR

Kybernetickým priestorom v decembri 2025 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Europol s partnermi rozložili kryptomenový mixér Cryptomixer

Orgány činné v trestnom konaní zo Švajčiarska a Nemecka spolu s Europolom a Eurojustom rozložili službu Cryptomixer, ktorú kyberzločinci používali na pranie nezákonne získaných kryptomien.

2 Rusko zablokovalo aplikácie FaceTime a Snapchat

Rusko zablokovalo prístup k aplikáciám FaceTime a Snapchat, pretože ruský štátny úrad zodpovedný za dohľad nad komunikačnými službami, informačnými technológiami a masmédiami Roskomnadzor tvrdí, že tieto aplikácie boli používané na organizovanie teroristických útokov, verbovanie zločincov a na páchanie podvodov a iných trestných činov proti občanom krajiny.

3 Spear-phishingová kampaň ruskej UTA0355 zneužíva tematiku bezpečnostných konferencií v Európe

Spoločnosť Volexity zverejnila informácie o spear-phishingovej kampani ruskej skupiny UTA0355, ktorej cieľom je kompromitácia prostredí Microsoft a Google.

4 Výskumníci zaznamenali prvý prípad zneužitia zraniteľnosti React2Shell na nasadenie ransomvéru Weaxor

S-RM zverejnili informácie o prvom prípade zneužitia kritickej zraniteľnosti React2Shell na infekciu zariadenia ransomvérom Weaxor.

5 Skupina Dragonforce sa prihlásila k ransomvérovému útoku na stavebnú spoločnosť Váhostav

Hackerská skupina DragonForce sa prihlásila k ransomvérovému útoku na slovenskú stavebnú spoločnosť Váhostav.

6 Spoločnosť ESET zverejnila analýzu podvodných kampaní NOMANI

Spoločnosť ESET vo svojom Threat Report H2 2025 upozornila na 62-percentný nárast falošných investičných schém NOMANI, ktoré sú propagované prostredníctvom sociálnych sietí Facebook, YouTube a podobne.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti jednotka CSIRT.SK v mesiaci december riešila typicky najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK.

Okrem bežných phishingových kampaní sa vyskytla kampaň na klientov Tatra banky využívajúca techniku quishing. Jedná sa o použitie QR kódov smerujúcich na podvodné webstránky. CSIRT.SK vykonala analýzu poskytnutého obsahu.

V decembri Vládna jednotka CSIRT riešila v spolupráci s partnermi kybernetický útok na Ministerstvo hospodárstva SR, o ktorom informovali viaceré médiá. V rámci vykonaných úkonov riešenia bezpečnostného incidentu vrátane prebiehajúcej forenznej analýzy zaistených kybernetických stôp boli zistené viaceré skutočnosti, ktoré mali za následok narušenie integrity, dôvernosti, dostupnosti informácií, resp. informačných systémov a mali dopad na kontinuitu činností organizácie. V rámci preventívnych opatrení bol preverený výskyt indikátorov kompromitácie, získaných pri analýze incidentu, v rámci iných organizácií v konštituencii CSIRT.SK. Jednotka naďalej rieši spoločne s partnerskou SK-CERT tento kybernetický bezpečnostný incident, kde naďalej prebiehajú všetky operácie pre jeho vyriešenie od detekcie až po obnovu systémov.

CSIRT.SK v rámci získavania informácií z verejných zdrojov objavila závadný obsah na webe patriacom organizácii v konštituencii CSIRT.SK. Organizácii odporučia preveriť kompromitáciu prostredníctvom rozhrania wp-login.php, skontrolovať účty a oprávnenia, zabezpečiť sanáciu webu, zmeniť prístupy a zakázať verejný prístup k wp-login.php.

Jednotka v decembri prijala a preverovala informáciu o vážnom a pokračujúcom podozrení na bezpečnostný incident týkajúci sa verejne dostupného rozhrania API, čo viedlo k masívnemu úniku osobných údajov. Toto rozhranie aktívne zneužívali podvodníci, ktorí pre získanie kompletných osobných údajov klientov organizácie nepotrebovali autentifikáciu, autorizáciu ani API kľúč. Nahlasovateľ dodal tiež informácie o následnom zneužívaní získaných osobných údajov.

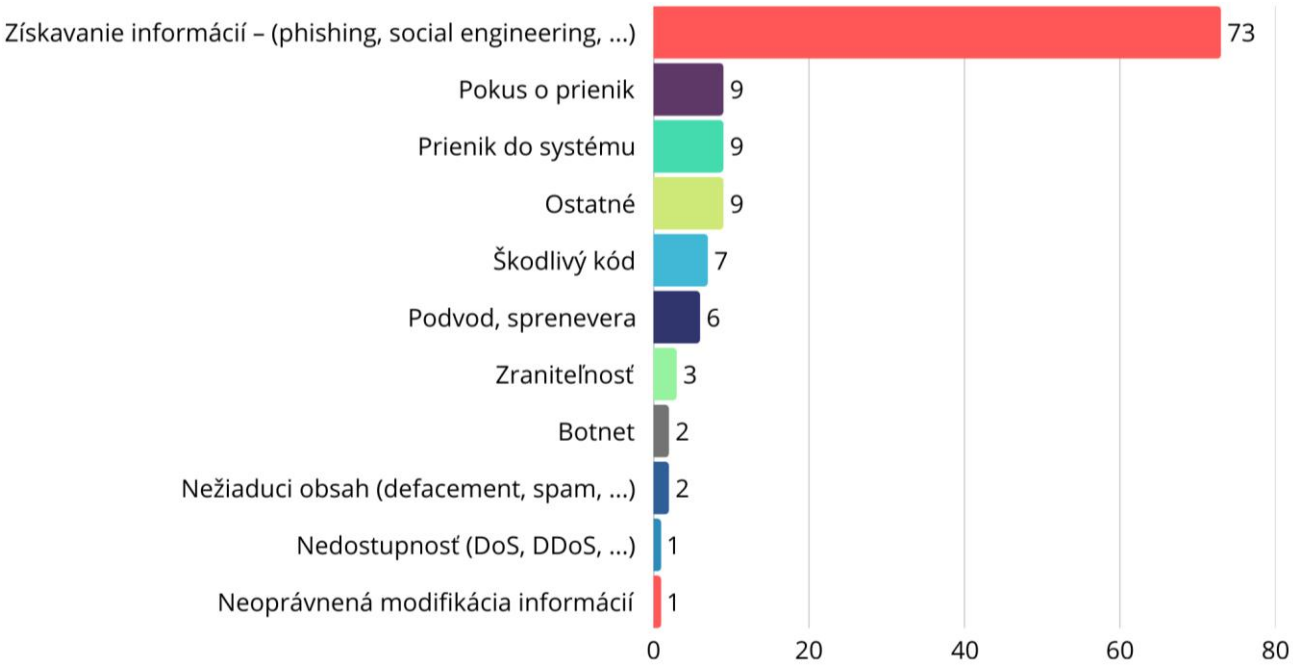
Ministerstvo financií SR poskytlo informácie o kybernetickom bezpečnostnom útoku typu DDoS, teda úmyselnej snahe vyvolať nedostupnosť služby, ktorý bol zaznamenaný na informačnom systéme súvisiacom so službou cenyslovensko.sk. Organizácia prijala okamžité technické opatrenia na zníženie dopadu útoku. Neboli zistené žiadne narušenia týkajúce sa dôvernosti a integrity dát.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén, ktorú monitoruje modul Domino.

CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných škôl. V decembri jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre

zamestnancov Výskumnej agentúry a študentom Gymnázia Augusta Horislava Škultétyho vo Veľkom Krtíši a Spojenej školy v Modrom Kameni.

VJ CSIRT poskytuje tiež školenia a cvičenia pre svoju konštituenciu v rámci výcvikového strediska Kyberaréna.



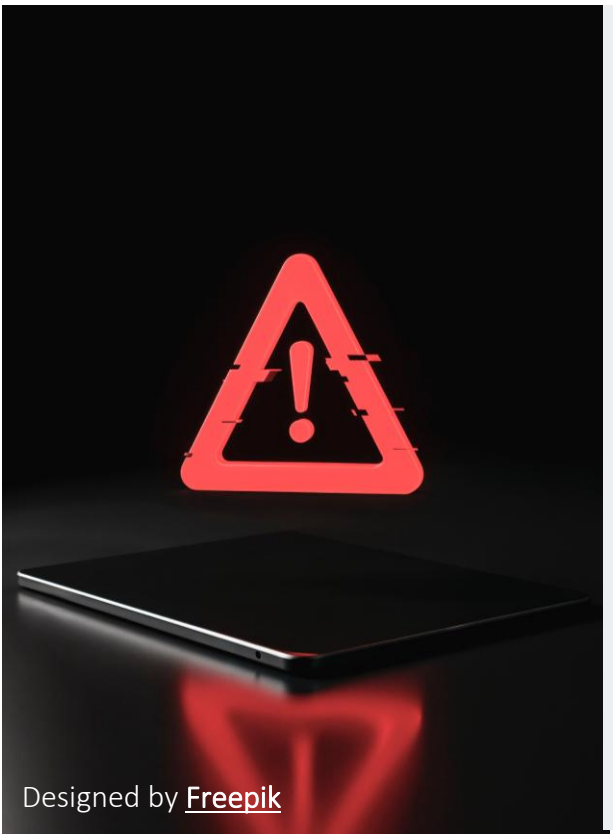
VÝZNAMNÉ UDALOSTI VO SVETE

Europol s partnermi rozložili mixér kryptomien Cryptomixer

Orgány činné v trestnom konaní zo Švajčiarska a Nemecka spolu s Europolom a Eurojustom rozložili službu Cryptomixer, ktorú kyberzločinci používali na pranie nezákonne získaných kryptomien. Počas razie v Zürichu, ktorá sa uskutočnila medzi 24. a 28. novembrom 2025 zaistili participujúce zložky tri servery, doménu *cryptomixer.io* a cez 12 TB dát. Zároveň zmrazili vyše 25 miliónov € v kryptomenách. Od roku 2016 služba Cryptomixer spracovala viac ako 1,3 miliardy € z trestnej činnosti, vrátane obchodovania s drogami a zbraňami, podvodov, ransomvérových útokov a krádeží platobných kariet.

OpenAI zaznamenala celosvetový výpadok služieb ChatGPT

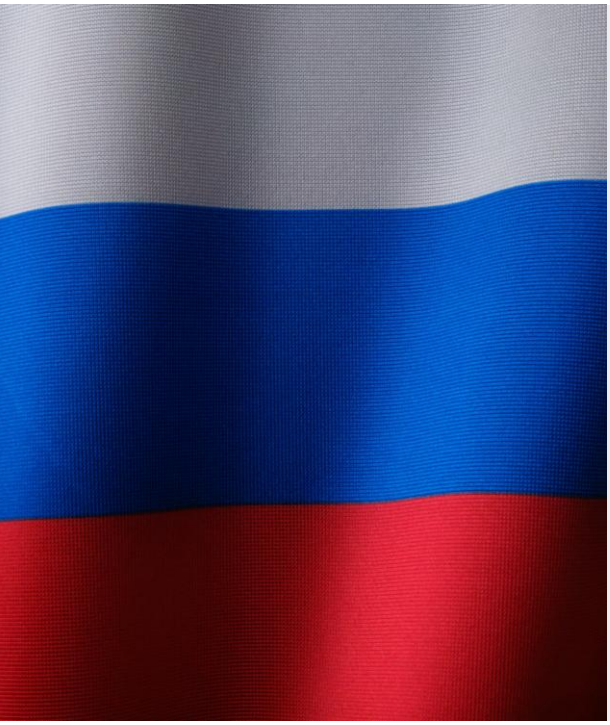
Spoločnosť OpenAI zaznamenala celosvetový výpadok služieb ChatGPT. Problémy u používateľov vznikli pri pokuse prístupu k chatu, načítavanie odpovedí sa zasekávalo a bolo zaznamenané miznutie histórie rozhovorov. Portál DownDetector, ktorý sa zameriava na detekciu výpadkov služieb, zaznamenal problémy u viac ako 30 000 používateľov. Spoločnosť OpenAI v ranných hodinách potvrdila, že eviduje zvýšenú chybovosť pri prístupe k službe a intenzívne pracuje na jej odstránení. Od 15:14 ET bola služba čiastočne obnovená, i keď v obmedzenom režime.



NCSC-UK spustilo testovaciu fázu služby pre rozposielanie adresných varovaní na zraniteľné systémy

Britské národné centrum kybernetickej bezpečnosti NCSC-UK spustilo pilotnú prevádzku služby Proactive Notifications, ktorej cieľom je informovať organizácie v rámci Británie o zraniteľnostiach v ich infraštruktúrach. Samotnú službu poskytuje spoločnosť Netcraft a varovania sú založené na dátach získaných z otvorených zdrojov a skenovania internetu. NCSC informovalo, že všetky varovania budú prichádzať z domény netcraft.com, nebudú obsahovať žiadne prílohy, ani požadovať platby alebo akékoľvek citlivé informácie. Centrum zároveň zdôraznilo, že varovania nebudú pokrývať všetky systémy a zraniteľnosti a organizácie by sa nemali spoliehať výhradne na túto službu. NCSC už prevádzkuje službu Early Warning, kde organizácie adresne upozorňuje na hrozby, podozrivé a škodlivé aktivity cieliace na ich infraštruktúru. Služba Proactive Notifications má varovať pred rizikami a služba Early Warning už pred zachytenými aktivitami priamo cielenými na organizáciu.

VÝZNAMNÉ UDALOSTI VO SVETE

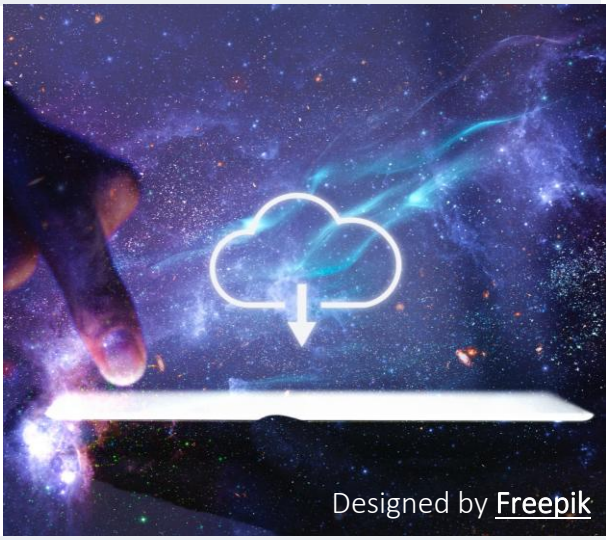


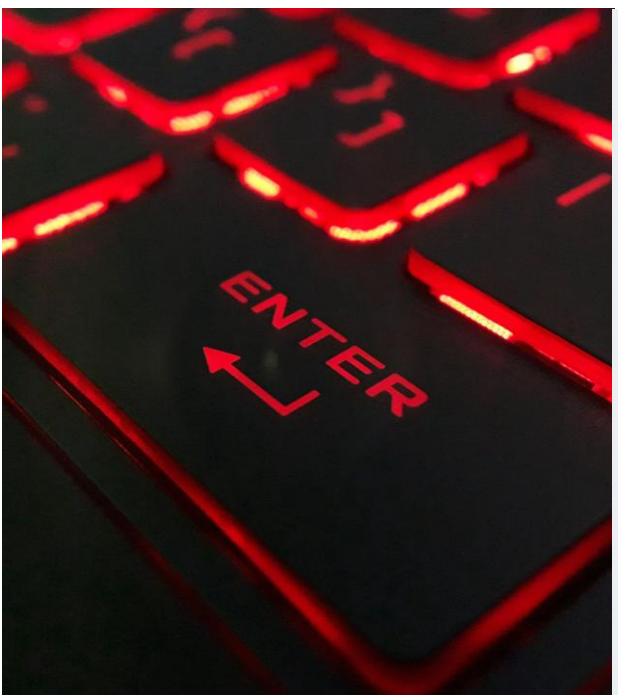
Rusko zablokovalo aplikácie FaceTime a Snapchat

Rusko zablokovalo prístup k aplikáciám FaceTime a Snapchat, pretože ruský štátny úrad zodpovedný za dohľad nad komunikačnými službami, informačnými technológiami a masmédiami Roskomnadzor tvrdí, že tieto aplikácie boli používané na organizovanie teroristických útokov, verbovanie zločincov a na páchanie trestných činov proti občanom krajiny. Snapchat prestali používatelia oficiálne využívať od 10. októbra 2025. FaceTime tak patrila k posledným veľkým video-komunikačným službám, ktoré ešte fungovali v krajine po obmedzeniach aplikácií WhatsApp či Telegram. Nedávno úrad s odvolaním sa na šírenie LGBT propagandy a extrémistického materiálu zablokoval aj online hraciu platformu Roblox. Aplikácie Viber a Signal sú v Rusku blokované už od roku 2024. Ruská vláda tak pokračuje v kampani proti zahraničným platformám, a zároveň propaguje vlastnú aplikáciu MAX, ktorá podľa kritikov môže slúžiť na sledovanie používateľov.

Cloudflare zaznamenala výpadok služieb v súvislosti s motiváciou zraniteľnosti React2Shell

Spoločnosť Cloudflare v piatok 5. decembra 2025 opätovne zaznamenala približne 3-hodinový rozsiahly výpadok služieb, ktorý spôsobil zobrazenie chybovej hlášky „*500 Internal Server Error*“ na približne 28 % všetkej HTTP prevádzky. Spoločnosť vylúčila kybernetický útok a za príčinu problému označila nové bezpečnostné opatrenia (nové pravidlá pre Web Application Firewall) zavedené v súvislosti s mitigáciou aktívne zneužívanej kritickej zraniteľnosti React2Shell (CVE-2025-55182) v knižniciach JavaScript React a Next.js.





Spoločnosť GreyNoise zachytila pokusy o prienik do VPN portálov Palo Alto

Výskumníci z GreyNoise zverejnili informácie o kampani zameranej na prienik do VPN portálov Palo Alto GlobalProtect a skenovanie API endpointov SonicWall SonicOS. Kampaň začala 2. decembra 2025 z približne 7 000 IP adries infraštruktúry nemeckého poskytovateľa IT služieb 3XK Tech GmbH, ktorý prevádzkuje vlastnú BGP sieť a ponúka hostingové služby. Podarilo sa stotožniť 3 klientske profily, ktoré spoločnosť zachytila aj pri útokoch koncom septembra, v polovici októbra a novembra 2025. Palo Alto vyhlásila, že ide o útoky na heslá hrubou silou a tzv. password spraying a vylúčila existenciu zraniteľností. Administrátorom odporúčame v rámci bezpečnostného monitoringu detegovať podozrivé správanie v rámci autentifikácie do portálov a blokovať dostupné indikátory kompromitácie.

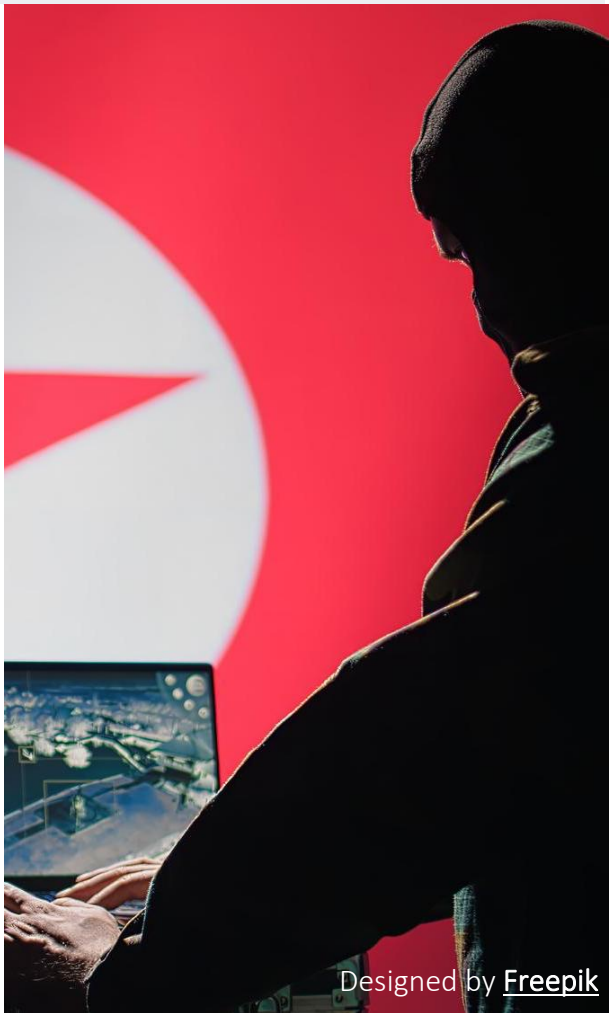
VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosť Amazon narušila a zdokumentovala aktivity ruských skupín asociovaných s GRU

Tím Amazon Threat Intelligence zdokumentoval aktivity ruských štátom sponzorovaných skupín súvisiace s útokmi na energetický sektor, kritickú infraštruktúru a cloudovú sieťovú infraštruktúru západných krajín v období rokov 2021 až 2025. Na základe prekryvu infraštruktúry s APT44 tím útoky atribuuje ruskej vojenskej spravodajskej službe GRU. Na prvotný prienik do systémov zneužívali primárne nesprávnu konfiguráciu sieťových zariadení a verejne dostupných manažmentových zariadení, pričom možno súčasne pozorovať pokles aktivít súvisiacich so zneužívaním zraniteľností. Tento postup má nižšiu mieru detekcie. Primárnymi cieľmi boli priemyselné routre, VPN koncentrátory, remote access gateway, sieťové manažmentové zariadenia, kolaboračné a wiki platformy, ako aj cloudové manažmentové systémy. Po ich kompromitácii zneužívali natívne funkcie pre zachytávanie paketov a zo zachytenej prevádzky extrahovali prihlasovacie údaje. Tie sa prostredníctvom techniky tzv. credential replay snažili zneužiť na získanie hlbšieho prístupu do systému. Pred prechodom do fázy laterálneho šírenia si vytvárali perzistentný prístup zostavením spojenia na IP adresy pod ich kontrolou.

Severokórejské skupiny aktívne zneužívajú React2Shell na šírenie nového malvéru EtherRAT

Výskumníci zo spoločnosti Sysdig zverejnili informácie o aktivitách skupín, ktoré aktívne zneužívajú kritickú zraniteľnosť CVE-2025-55182 (React2Shell) v protokole RSC Fligh na šírenie nového malvéru EtherRAT. Malvér v rámci C2 komunikácie zneužíva smart kontrakty siete Ethereum, využíva 5 rôznych mechanizmov zaistenia perzistencie na platforme Linux a sťahuje vlastnú inštanciu Node.js. Útok začína zneužitím zraniteľnosti React2Shell na vykonanie Base64-kódovaného príkazu rozhrania shell, ktorý sa snaží stiahnuť ďalší skript a následne ho spustiť. Tento skript vytvára skrytý priečinok, do ktorého sťahuje a extrahuje legitímnu inštanciu Node.js. Následne dochádza k vytvoreniu šifrovaného škodlivého obsahu a obfuskovaného JavaScript droppera, ktoré spúšťa Node.js. Dropper prostredníctvom zabudovaného kľúča AES-256-CBC dešifruje obsah a zapíše ho do ďalšieho skrytého JavaScript súboru. Ten predstavuje samotný malvér EtherRAT. Zachytená aktivita vykazuje podobnosť s kampaňami Contagious Interview, ktoré sú typické pre severokórejské APT skupiny. Výskumníci z OpenSourceMalware zároveň upozornili, že v rámci týchto kampaní možno pozorovať postupný odklon od zneužívania balíkov NPM ku Microsoft Visual Studio Code, kde útočníci zneužívajú konfiguračný súbor tasks.json.



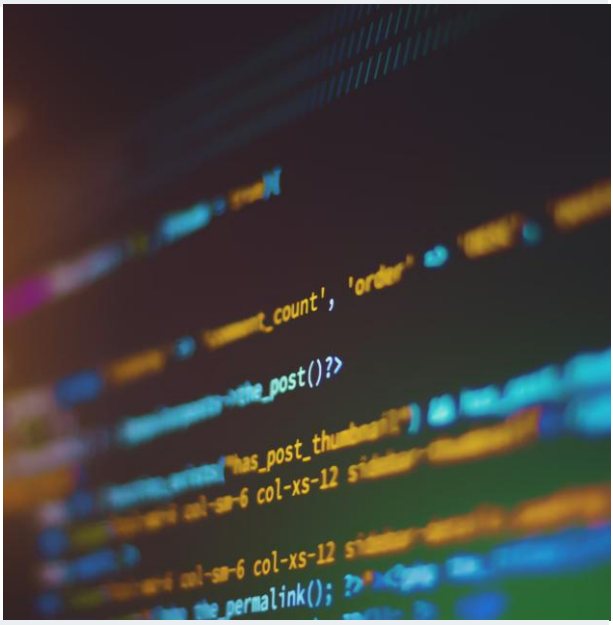
VÝZNAMNÉ UDALOSTI VO SVETE

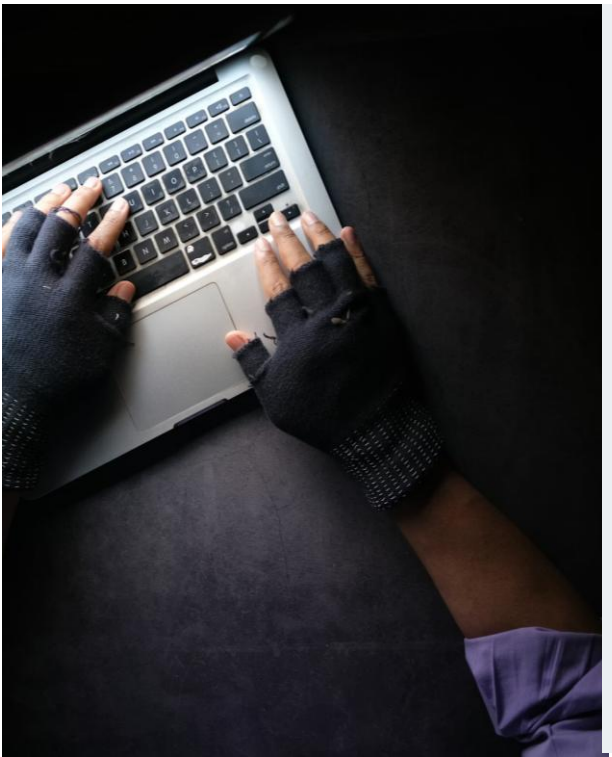
Spear-phishingová kampaň ruskej UTA0355 zneužíva tematiku bezpečnostných konferencií

Spoločnosť Volexity zverejnila informácie o spear-phishingovej kampani ruskej skupiny UTA0355, ktorej cieľom je kompromitácia prostredí Microsoft a Google. Útočníci za týmto účelom vytvárajú phishingové stránky a rozposielajú e-maily s tematikou uznávaných bezpečnostných konferencií v Európe, kde sa počas registračného procesu snažia získať prístup do účtov obetí. Kampane zneužívajú Oauth a Device Code Authentication. Útočníci navádzajú potenciálne obete aj prostredníctvom správ cez komunikačné platformy.

Útočníci pokračujú v intenzívnom zneužívaní kritickej zraniteľnosti React2Shell

Spoločnosti Palo Alto Networks a NTT Security zverejnili výsledky analýzy útokov zameraných na zneužívanie kritickej zraniteľnosti React2shell (CVE-2025-55182), v rámci ktorých došlo k nasadeniu nových linuxových zadných vrátok KSwapDoor a ZnDoor. Tieto vytvárajú internú mesh sieť na komunikáciu medzi kompromitovanými servermi a komunikáciu šifrujú silnými algoritmami. Obsahuje funkcie pre obchádzanie firewallov, vytvorenie interaktívneho shellu, vzdialené vykonanie príkazov, operácie so súborovým systémom, spustenie SOCKS5 proxy a port forwardingu a rôzne skenovacie funkcie využívané pri laterálnom pohybe v sieti.





Výskumníci zaznamenali prvý prípad zneužitia zraniteľnosti React2Shell na nasadenie ransomvéru Weaxor

S-RM zverejnila informácie o prvom prípade zneužitia kritickej zraniteľnosti React2Shell na infekciu zariadenia ransomvérom Weaxor. Na základe dostupných informácií ide o menej sofistikovanú skupinu s oportunistickým cielením na verejne dostupné servery, ktorá dáta len šifruje a požaduje relatívne nízke výkupné. Útočníci po zneužití zraniteľnosti a získaní prístupu spustili obfuskovaný PowerShellový skript, ktorý nasadil Cobalt Strike beacon. Následne deaktivovali Windows Defender a spustili ransomvér. Útoky boli limitované priamo na koncové body so zraniteľnosťou React2Shell a útočník nevykonával laterálny pohyb. Za účelom maskovania svojej aktivity a komplikácie procesu obnovy zmazal shadow kópie a event logy. Zariadenie bolo následne kompromitované nezávisle iným útočníkom.

VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosť ESET zverejnila analýzu podvodných kampaní NOMANI s tematikou falošných investičných schém

Spoločnosť ESET vo svojom Threat Report H2 2025 upozornila na 62-percentný nárast falošných investičných schém NOMANI, ktoré sú propagované prostredníctvom sociálnych sietí Facebook, YouTube, a podobne. ESET v roku 2025 zablokovala vyše 64 000 URL adries asociovaných s týmto typom podvodu, pričom majoritné množstvo detekcií bolo zaznamenaných v Českej republike, Japonsku, Slovenskej republike, Španielsku a Poľsku. Kampaň bola prvýkrát zdokumentovaná v decembri 2024 a jej špecifikom bol malvertisement prostredníctvom sociálnych sietí, posty zneužívajúce identitu známych spoločností a AI generované videá známych osobností, ktoré nabádali na investície do neexistujúcich investičných platforiem s vysokou návratnosťou investovaných prostriedkov. Pri žiadosti o výber investovaných prostriedkov od obetí žiadali ďalšie poplatky alebo poskytnutie citlivých údajov ako sú fotografie dokladov alebo čísla bankových kariet. Útočníci obete následne cielili aj prostredníctvom scam kampaní, kde sa vydávali za pracovníkov Europolu, Interpolu a iných finančných inštitúcií a ponúkali im pomoc so získaním svojich financií.

Falošné domény MAS (Microsoft Activation Scripts) zneužívané na šírenie malvéru Cosmali Loader

Etickí hackeri kompromitovali riadiaci server malvéru Cosmali Loadera a upravili ho tak, aby na infikovaných zariadeniach zobrazil vyskakovacie upozornenie informujúce obeť o kompromitácii. Typosquattingová doména get.activate[.]win, napodobňujúca doménu get.activated.win referencovanú v oficiálnom MAS (Microsoft Activation Scripts) nástroji, distribuovala PowerShell skripty slúžiace na šírenie malvéru Cosmali Loader. Vyskakovacie okná reportovalo viacero používateľov na sieti Reddit a ich výskyt bol potvrdený aj bezpečnostnými výskumníkmi na sieti X. Útočníci sa spoliehali na nepozornosť používateľov vedúcu k preklepom. Cosmali Loader je zneužívaný na šírenie kryptominerov a RAT malvéru XWorm. Spoločnosť Microsoft považuje open-source nástroj MAS za pirátsky nástroj pre aktiváciu OS Windows bez zakúpenej licencie. Na prebiehajúcu kampaň upozornil aj prevádzkovateľ nástroja, MassGravel. Aktivátory a cracky zostávajú populárnym spôsobom šírenia malvéru.

VÝZNAMNÉ UDALOSTI VO SVETE

Skupina DragonForce sa prihlásila k ransomvérovému útoku na slovenskú stavebnú spoločnosť Váhostav

Hackerská skupina DragonForce sa prihlásila k ransomvérovému útoku na slovenskú stavebnú spoločnosť Váhostav. Získala takmer 225 GB interných dát, spustila sedemdňové odpočítavanie pred ich zverejnením, a následne údaje skutočne publikovala na darkwebe. Únik citlivých informácií môže mať vážne právne, reputačné aj bezpečnostné dôsledky, najmä vzhľadom na skutočnosť, že spoločnosť je kľúčovým dodávateľom pri veľkých štátnych infraštruktúrnych projektoch.

Útok na dodávateľský reťazec modulu Trust Wallet pre Chrome viedol ku krádeži kryptomien v hodnote 7 miliónov dolárov

Zakladateľ spoločnosti Binance, Changpeng Zhao, potvrdil, že 24. decembra útočníci vydali kompromitovanú aktualizáciu rozšírenia Trust Wallet pre prehliadač Chrome. Bližšie nešpecifikovaným útočníkom sa v rámci útoku na dodávateľský reťazec podarilo odcudziť kryptomeny z takmer 3 000 kryptopeňaženiek v celkovej hodnote 7 miliónov dolárov. Trust Wallet je populárna kryptopeňaženka vo forme rozšírenia pre Chrome alebo mobilnej aplikácie, ktorá umožňuje ukladanie, správu a interakciu s kryptomenami na rôznych blockchainoch a komunikáciu s decentralizovanými aplikáciami dApps. Krátko po reportovaní škodlivej aktivity po inštalácii verzie 2.68.0 bola v tichosti vydaná zabezpečená verzia 2.69.0. Škodlivá verzia obsahovala súbor JavaScript 4482.js, ktorého cieľom bolo zneužiť legitímnu analytickú knižnicu PostHog na exfiltráciu citlivých údajov na externú doménu pod kontrolou útočníka. Doména bola zaregistrovaná len pár dní pred samotným incidentom. Zachytené boli aj nadväzujúce phishingové kampane s tematikou bezpečnostnej záplaty pre odstránenie zraniteľnosti, ktoré však slúžili len na ďalšie získanie seedov a krádež kryptomien.

VÝZNAMNÉ UDALOSTI VO SVETE

- India nariadila povinnú predinštaláciu vládnej aplikácie Sanchar Saathi do všetkých smartfónov.
- CISA zverejnila analýzu čínskych zadných vrátok BrickStorm pre platformu VMware.
- TOP 5 hrozieb v oblasti bezpečnosti webových aplikácií, ktoré charakterizujú rok 2025.
- FBI varuje pred kampaňami vydierania s tematikou falošných únosov podložených upravenými fotografiami a videami.
- Výskumníci zverejnili analýzy androidového malvéru FVNcBot, SeedSnatcher a ClayRAT.
- AI odhaľuje rozsiahlu malvérovú sieť 5 000 domén zameranú na čínsky trh.
- Microsoft rozširuje Bug Bounty Program na všetky systémy a služby s potenciálnym vplyvom na jeho služby.
- Výskumníci zverejnili analýzy nových phishingových platforiem BlackForce, GhostFrame, InboxPrime AI a SpiderMan.
- Google začiatkom roka 2026 ukončí službu Dark Web Report.
- Hackeri odcudzili údaje prémiových používateľov služby Pornhub a zneužili ich na vydieranie.
- Interpol v rámci operácie Sentinel rozložil ransomvérové skupiny aktívne v Afrike.
- Útočníci v roku 2025 zneužili prihlasovacie údaje z úniku služby LastPass z roku 2022 na krádež kryptomien.
- Čínska APT skupina Evasive Panda zneužíva útoky typu DNS poisoning na šírenie backdooru MgBot.
- Rumunská energetická spoločnosť Complexul Energetic Oltenia sa stala obeťou ransomvérového útoku skupiny Gentlemen.
- Európska vesmírna agentúra (ESA) potvrdila kompromitáciu externých serverov.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

ASUS opravil kritickú zraniteľnosť v routeroch série DSL

Spoločnosť ASUS vydala bezpečnostné aktualizácie firmvéru routerov série DSL, ktoré opravujú kritickú zraniteľnosť. Zraniteľnosť CVE-2025-59367 možno zneužiť na získanie neoprávneného prístupu do systému a úplné narušenie dôvernosti, integrity a dostupnosti zariadenia.

Kritická zraniteľnosť React Server Components umožňuje vykonávať kód

Vývojári platformy JavaScript React opravili kritickú zraniteľnosť v React Server Components, ktorá umožňuje vzdialené vykonávanie kódu na serveri. Zasiahnuté sú viaceré balíčky npm, vrátane platformy Next.js. Zraniteľnosť dostala pomenovanie React2Shell.

Kritická zraniteľnosť Apache Tika umožňuje injektovať XML

Vývojári Apache Tika vydali opravné aktualizácie pre viacero modulov, do ktorých je možné injektovať externé entity XML. Zneužitím opravenej zraniteľnosti môže útočník získať schopnosť čítať citlivé dáta alebo vzdialene vykonávať kód.

Apple opravila aktívne zneužívané zraniteľnosti svojich OS a prehliadača

Apple vydala aktualizácie na opravu dvoch zero-day zraniteľností, ktoré sa nachádzajú v nástroji WebKit prehliadača Safari a ďalších prehliadačov na iOS a knižnici ANGLE pre Google Chrome pre Mac. CVE-2025-43529 umožňuje vykonávanie ľubovoľného kódu a možno ju zneužiť spracovaním škodlivého webového obsahu. Zraniteľnosť môže viesť k poškodeniu pamäte.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti FreePBX umožňujú získať kontrolu nad systémom

Vývojári FreePBX opravili jednu kritickú a dve vysoko závažné zraniteľnosti v aplikácii FreePBX Endpoint Manager. Kritická zraniteľnosť umožňuje obísť autentifikáciu, zatiaľ čo ostatné dve dovoľujú získavať a meniť dáta v SQL databáze a nahrávať ľubovoľné súbory.

Aktívne zneužívaná zraniteľnosť SonicWall SMA1000

Spoločnosť SonicWall vydala bezpečnostné aktualizácie pre zariadenia SonicWall SMA1000, ktoré opravujú aktívne zneužívanú zraniteľnosť. Zraniteľnosť strednej závažnosti CVE-2025-40602 spočíva v nedostatočnej autorizácii v rámci konzoly AMC (Application Management Console) a lokálny útočník by ju mohol zneužiť na eskaláciu privilégií.

Kritická zraniteľnosť Hewlett Packard Enterprise OneView

Spoločnosť HPE varuje pred kritickou zraniteľnosťou manažmentovej platformy OneView, ktorá umožňuje vzdialené vykonávanie kódu.

MongoBleed: aktívne zneužívaná zraniteľnosť MongoDB server umožňuje čítať pamäť

Vývojári MongoDB Server opravili vysoko závažnú zraniteľnosť umožňujúcu vzdialenému neautentifikovanému útočníkovi manipulovať s premennými v hlavičkách požiadaviek a získavať tak citlivé informácie z pamäte na halde (angl. heap) v rámci operačnej pamäte. Zraniteľnosť je aktívne zneužívaná.

MESAČNÍK ZRANITEĽNOSTÍ NOVEMBER 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3018.html