CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

MAREC 2026

TLP: CLEAR

Kybernetickým priestorom v marci 2026 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Nová phishingová kampaň imituje služby štátnych inštitúcií.

Vládna jednotka CSIRT získala informácie o nových podvodných webstránkach, ktoré sa snažia napodobniť vzhľad a funkcie oficiálnych elektronických služieb štátu. Ide o novú phishingovú / smishingovú kampaň.

2 Poľské jadrové výskumné centrum sa stalo terčom kyberútoku

Poľské Národné centrum jadrového výskumu (NCBJ) bolo cieľom kybernetického útoku, ktorý bezpečnostné systémy včas zachytili a zablokovali.

3 Ruské skupiny kompromitujú účty na platformách WhatsApp a Signal

Holandské informačné služby MIVD (Netherlands Defence Intelligence and Security Service) a AIVD (Netherlands General Intelligence and Security Service) varujú pred phishingovou kampaňou ruských štátom sponzorovaných skupín zameranou na predstaviteľov vlády, vojenský personál a žurnalistov. Cieľom kampane je špionáž a získavanie citlivých údajov.

4 Skupina teampcp kompromituje populárne softvérové balíky a produkty

Vývojári Skupina TeamPCP vedie niekoľkofázovú eskalujúcu kampaň zameranú na kompromitáciu softvérového dodávateľského reťazca. Útočníci zneužívajú dôveryhodné distribučné kanály (PyPI, GitHub, NPM, Docker Hub) a kompromitujú populárne nástroje a knižnice (Trivy, KICS, LiteLLM, Telnyx).

5 Čínsky CNCERT varuje o rizikách AI frameworku OpenClaw

Čínsky tím CNCERT (China's National Computer Network Emergency Response Technical Team) vydal varovanie pred rizikami používania open-source AI agentového frameworku OpenClaw.

6 Skupina ShinyHunters kompromitovala systémy Európskej komisie

Európska komisia vyšetruje kybernetický útok na svoje účty v cloude spoločnosti Amazon, pri ktorom útočník získal neautorizovaný prístup k časti cloudovej infraštruktúry. Útočník odcudzil viac ako 350 GB dát, vrátane databáz a informácií viazaných na účty zamestnancov či e-mailové systémy.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci marec riešil 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.

V marci jednotka CSIRT.SK na základe vzájomnej spolupráce s partnermi a monitorovania externých zdrojov zaevidovala podozrivú webovú stránku. Vizuálne spracovanie stránky napodobňovalo dizajn legitímnych služieb Sociálnej poisťovne. Ku predmetnej aktivite neboli v tom čase evidované žiadne hlásenia, čo vyplývalo z pravdepodobnej skutočnosti, že kampaň ešte nebola spustená (len v príprave). Sociálnej poisťovni jednotka poskytla detailné informácie získané analýzou prípadu. V rámci odporúčaní bola aj príprava koordinovaného informovania verejnosti.

Podobné kampane v štádiu príprav zachytila VJ CSIRT aj voči Ministerstvu vnútra SR. Webstránky pripravované na novú vlnu phishingovej/smishingovej kampane mali vizuálne spracovanie napodobňujúce dizajn legitímnych služieb a organizácií spadajúcich pod Ministerstvo vnútra SR. Súčasťou kampane boli tiež fyzicky rozmiestnené letáčiky s vizuálnom oznámení bratislavskej mestskej polície, informujúce vodičov náhodných zaparkovaných vozidiel o fiktívnych pokutách. Na podvodné stránky odkazovali QR kódy na letáčikoch. Informácie o kampani publikovala CSIRT.SK aj na svojom webe. Fotografiu podvodného letáčiku umiestneného na okne vozidla jednotke poskytol súkromný nahlasovateľ. V rámci vzájomnej spolupráce jednotka informovala aj partnerské organizácie.

CSIRT.SK sa v marci stretol aj s hlásením podozrivej URL s podvodnou webstránkou. Táto bola propagovaná na sociálnej sieti Facebook, kde si na ňu podvodník zaplatil reklamu. Jednotka s partnermi preverila prístupy z lokalít organizácií vo svojej konštituencii. Deň po zahájení procesu riešenia incidentu už bola podozrivá webová stránka nedostupná. Na sociálnych sieťach sa často vyskytujú podvodné príspevky. Buďte obozretní pri interagovaní s reklamami na sociálnych sieťach, pretože útočníkom stojí za to zaplatiť si reklamný príspevok, aby získali väčší dosah svojich podvodných kampaní.

V marci identifikovala organizácia v konštituencii CSIRT.SK na základe dodaných indikátorou kompromitácie a vlastnej analýzy jedno koncové zariadenie, z ktorého bolo vykonané úspešné spojenie na škodlivú IP adresu. Z nej bol stiahnutý binárny súbor. Organizácia vykonala okamžitú zmenu prihlasovacích údajov a škodlivú doménu zablokovala. Predmetné IP adresy so škodlivým obsahom boli zablokované aj v sieti Govnet. Zariadenie bolo zaistené a spolu s odhaleným škodlivým obsahom bolo predmetom forenznej analýzy. O niekoľko dní neskôr organizácia identifikovala ďalšie podozrivé zariadenie, ktoré vykazovalo znaky kompromitácie. Aj toto zariadenie bolo izolované a organizácia vykonala zmenu prístupových údajov používateľa. Analýza ukázala, že vektor prieniku bol phishingový e-mail so škodlivou prílohou, ktorá bola podrobené malvérovej analýze. Jednotka požiadala organizáciu o reinštaláciu zariadení, a zároveň odporučila kontrolu mailboxov všetkých zamestnancov na prítomnosť predmetného škodlivého emailu. Ďalšie kompromitované zariadenia už neboli identifikované. Krátko nato nahlásila kybernetický bezpečnostný incident, ktorý mal všetky známky tejto prebiehajúcej kampane, ďalšia organizácia. Jednotka požiadala o poskytnutie vzoriek podozrivého e-mailu, vykonala analýzu a poskytla zistenia a odporúčania pre zníženie dopadu incidentu.

CSIRT.SK v marci informovala organizácie vo svojej konštituencii o kampani šíriacej škodlivý kód typu infostealer/RAT. Analýza preukázala, že išlo o infostealer známy ako Agent Tesla. Na základe tohto varovania jednotku kontaktovalo viacero organizácií, ktoré pomohli rozšíriť sadu identifikovaných indikátorov kompromitácie. Tieto jednotka zaviedla do svojej zdieľanej inštancie platformy MISP (služba Afrodita). Vo všetkých nahlásených prípadoch došlo k zastaveniu útoku už v prvej fáze. Ak bol škodlivý súbor otvorený, CSIRT.SK odporučil dané zariadenie preinštalovať pre odstránenie potenciálnej perzistencie.

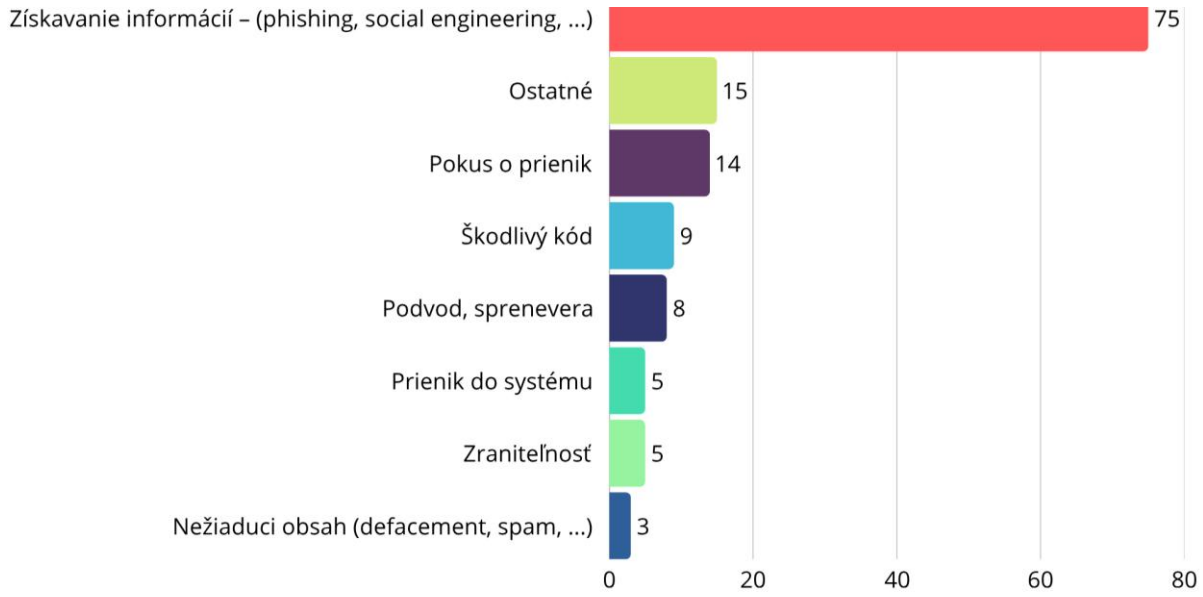
V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles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

V rámci služby Ares boli vykonané penetračné testy 5 webových aplikácií a jeden audit konfigurácie podľa tzv. CIS benchmarks. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

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 marci jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Mestskej časti Petržalka, Bratislava a spoločnosti KOMVak vodárne a kanalizácie mesta Komárna a.s.. Prednášala aj študentom SPŠ dopravnej v Trnave, Obchodnej akadémie a Strednej zdravotníckej školy v Považskej Bystrici, Strednej odbornej školy stavebnej v Nitre, SOŠ pedagogickej v Modre a Strednej zdravotníckej školy v Dunajskej Strede.

Členovia tímu CSIRT.SK prednášali aj na študentskej konferencii „Moderné technológie v automatizácii“, ktorú organizovala v Bratislave SPŠ strojnícka Fajnorka. Prispeli témami bezpečnosti priemyselných zariadení a internetu vecí.

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



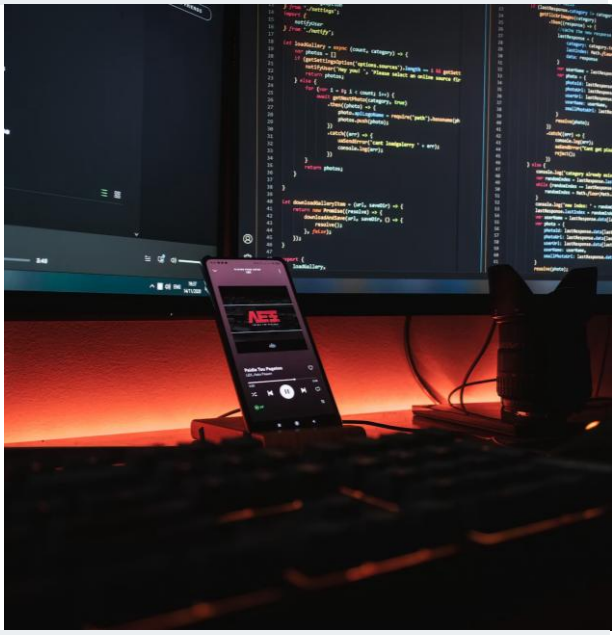
VÝZNAMNÉ UDALOSTI VO SVETE

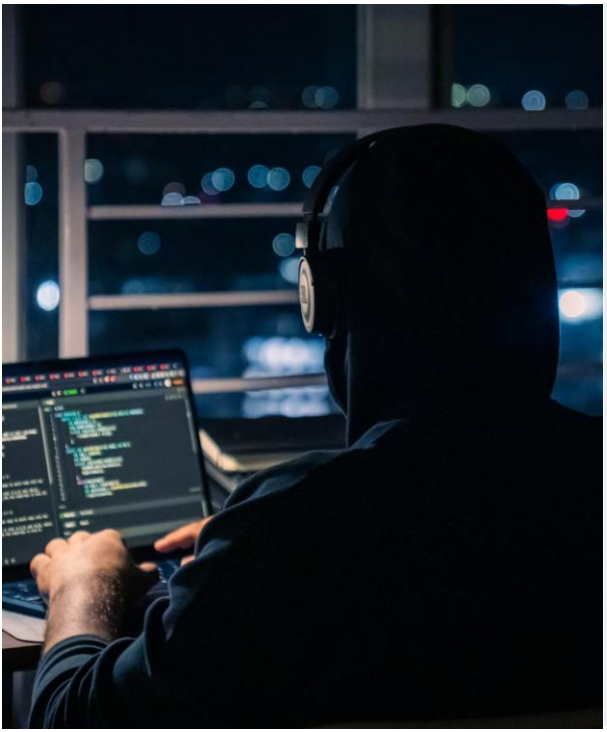
Nová phishingová kampaň imituje služby štátnych inštitúcií. Podvodníci lepia aj nálepky na autá

VJ CSIRT získala informácie o nových podvodných webstránkach, ktoré sa snažia napodobniť vzhľad a funkcie oficiálnych elektronických služieb štátu. Ide o novú phishingovú /smishingovú kampaň, ktorá sa môže v nasledujúcich dňoch objavovať plošne. Útočníci používajú dôveryhodne vyzerajúce domény, platené certifikáty, aj funkčné odkazy na skutočné informačné stránky a služby. Tým sa snažia zvýšiť dôveryhodnosť falošných stránok a zvýšiť tak šancu vylákania osobných a prihlasovacích údajov alebo platobných informácií, či priamo podvodom docieliť prevod finančných prostriedkov.

Skupina TeamPCP kompromituje populárne softvérové balíky a produkty

Skupina TeamPCP vedie niekoľkofázovú eskalujúcu kampaň zameranú na kompromitáciu softvérového dodávateľského reťazca. Útočníci zneužívajú dôveryhodné distribučné kanály (PyPI, GitHub, NPM, Docker Hub) a kompromitujú populárne nástroje a knižnice (Trivy, KICS, LiteLLM, Telnyx), čím obchádzajú tradičné bezpečnostné mechanizmy. Cieľom skupiny je distribúcia malvéru, ktorý následne umožňuje krádež prihlasovacích údajov, kompromitáciu prostredí CI/CD a krádež kryptomien. V niektorých prípadoch vykonáva aj deštruktívne útoky, aktuálne zamerané proti Iránu. Kampane skupiny TeamPCP predstavujú vysoké riziko pre organizácie využívajúce open-source nástroje a knižnice.





Výskumníci zdokumentovali aktivity hacktivistických skupín súvisiacich s konfliktom v Iráne

Nedávna eskalácia konfliktu na Blízkom východe sa preniesla aj do kyberpriestoru. Analytici zo spoločnosti Radware v období od 28. februára do 2. marca 2026 zaznamenali 149 DDoS útokov, ktoré zasiahli 110 subjektov. Hlavnými aktérmi tejto digitálnej ofenzívy sú hacktivistické skupiny DieNet, Keymous+ a NoName057(16). Útoky sa sústredili najmä na kritickú infraštruktúru, vládny, finančný a telekomunikačný sektor. 107 útokov cielilo na región Blízkeho východu, najmä Kuvajt, Izrael a Jordánsko, no nevyhli sa im ani Spojené arabské emiráty, Bahrajn, Katar, Saudská Arábia a Omán. Zasiahnuté boli aj európske organizácie. Bezpečnostní experti varujú, že tento nárast kybernetických útokov odráža rozširujúci sa digitálny front konfliktu a vyzývajú organizácie, aby posilnili obranné mechanizmy proti útokom typu DDoS.

VÝZNAMNÉ UDALOSTI VO SVETE

NCSC-UK varuje pred zvýšeným rizikom kybernetických útokov Iránu a proiránsky orientovaných skupín

NCSC-UK v súvislosti s aktuálnou situáciou na Strednom východe varovala pred zvýšeným rizikom kybernetických útokov zo strany Iránu. Jednalo sa o adresné varovanie pre subjekty, ktoré buď priamo alebo prostredníctvom dodávateľského reťazca pôsobia v tomto regióne. Napriek tomu, že väčšina územia Iránu nemá v dôsledku nariadenia vlády internetové pripojenie, štátom sponzorované skupiny a proiránsky orientované hackerské skupiny naďalej predstavujú riziko. Výstraha obsahovala odporúčania voči DDoS útokom, phishingovým kampaniam a útokom na priemyselné riadiace systémy.

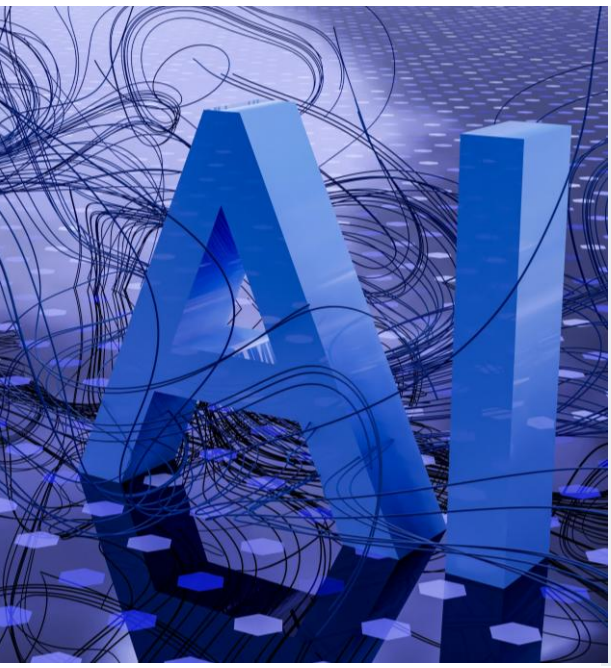
Europol a FBI s partnermi rozložili kyberkriminálne fórum LeakBase

FBI spolu s Europolom a ďalšími orgánmi zo 14 krajín vykonali koordinovanú medzinárodnú akciu Operation Leak, v rámci ktorej rozložili kyberkriminálne fórum LeakBase. Išlo o jednu z najväčších online platforiem na predaj ukradnutých dát a hackingových nástrojov. Orgány zaistili databázu fóra, účty a príspevky používateľov, ich platobné údaje, súkromné správy a IP adresy. Zatkli viacerých podozrivých v rôznych krajinách. Fórum, ktoré bolo voľne dostupné na webe, obsahovalo archívy stoviek miliónov kompromitovaných prihlasovacích údajov a citlivých informácií, už zobrazuje oznámenie o jeho zaistení OČTK.

Útočníci zneužívajú doménu .ARPA a reverzné IPv6 DNS na presmerovanie obetí

Výskumníci zo spoločnosti Infoblox zaznamenali phishingovú kampaň, v ktorej útočníci zneužívajú reverzné DNS zóny ARPA pre IPv6 na obchádzanie bezpečnostných filtrov. Najprv získajú blok IPv6 adries v rámci tunelu IPv6, následne získajú kontrolu nad príslušnou reverznou DNS zónou, ktorú zaregistrujú ako doménu .ip6.arpa a namiesto štandardných PTR záznamov vytvoria záznamy A, ktoré smerujú na infraštruktúru s phishingovými stránkami. Vo phishingových e-mailoch používajú odkazy alebo obrázky odkazujúce na reverzné IPv6 DNS názvy generované z adresného priestoru, čo sťažuje detekciu. V niektorých prípadoch zneužívajú infraštruktúru poskytovateľov ako Cloudflare alebo Hurricane Electric. Po kliknutí systém obeť presmeruje cez traffic distribution system na phishingovú stránku alebo legitímny web, aby sťažil detekciu.

VÝZNAMNÉ UDALOSTI VO SVETE

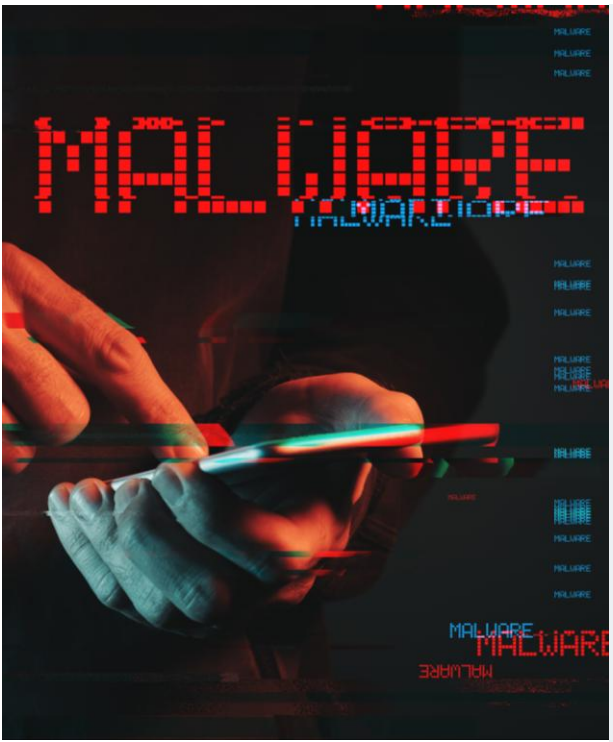


Útočníci zneužívajú AI vyhľadávanie Microsoft Bing na promovanie škodlivých repozitárov GitHub obsahujúcich malvér

Útočníci vytvorili falošné repozitáre na GitHube, ktoré sa vďaka Bing AI zobrazovali ako odporúčaný zdroj na stiahnutie verzie pre Windows. Inštalačné návody v týchto repozitároch navádzali používateľov spustiť príkazy, ktoré namiesto legitímnej aplikácie stiahli malvér – najmä infostealery a proxy nástroje určené na krádež citlivých údajov. Útočníci zvyšovali dôveryhodnosť svojich repozitárov kopírovaním legitímneho kódu z iných projektov a vytvorením organizácie na GitHube s názvom pripomínajúcim oficiálny projekt OpenClaw. Kampaň ukazuje, ako môžu útočníci zneužiť dôveryhodné platformy ako GitHub a zároveň manipulovať výsledky AI vyhľadávania na šírenie malvéru.

Úprava hlavičiek ZIP v rámci novej metódy Zombie ZIP umožňuje obchádzanie ochrán

Bezpečnostný výskumník predstavil techniku Zombie ZIP, ktorá umožňuje útočníkom skryť malvér v špeciálne upravenom archíve ZIP a obísť bezpečnostné kontroly. Útočník upraví hlavičku archívu tak, aby pole *method* označilo dáta ako nekomprimované, hoci ich algoritmus Deflate v skutočnosti komprimuje. Testy na platforme VirusTotal ukázali, že technika dokázala obísť 50 z 51 antivírusových nástrojov. Štandardné nástroje na extrakciu ako 7-Zip alebo WinRAR archív často označia ako poškodený, zatiaľ čo špeciálny loader dokáže obsah správne dekomprimovať a spustiť.



Nová technika maskovania škodlivého obsahu pred AI na báze renderovania webového obsahu

Výskumníci z LayerX demonštrovali novú techniku ukrytia škodlivého kódu na báze renderovania fontov, ktorá dokáže ukryť škodlivé inštrukcie pred AI analyzátormi. AI totiž webové stránky analyzuje ako štruktúrovaný text, zatiaľ čo webové prehliadače vytvárajú vizuálnu reprezentáciu pre používateľa. Práve renderovacia vrstva môže úplne zmeniť viditeľný obsah a význam bez modifikácie samotnej štruktúry DOM. Uvedenú techniku bolo podľa výskumníkov v decembri 2025 možné zneužiť na obídenie detekčných mechanizmov modelov ChatGPT, Claude, Copilot, Gemini, Leo, Grok, Perplexity, Sigma, Dia, Fellou a Genspark. Okrem spoločnosti Microsoft označili ostatní oslovení výrobcovia zraniteľnosť ako mimo rozsah (out of scope), pretože úspešnosť mechanizmu je podmienená interakciou obete a sociálnym inžinierstvom.

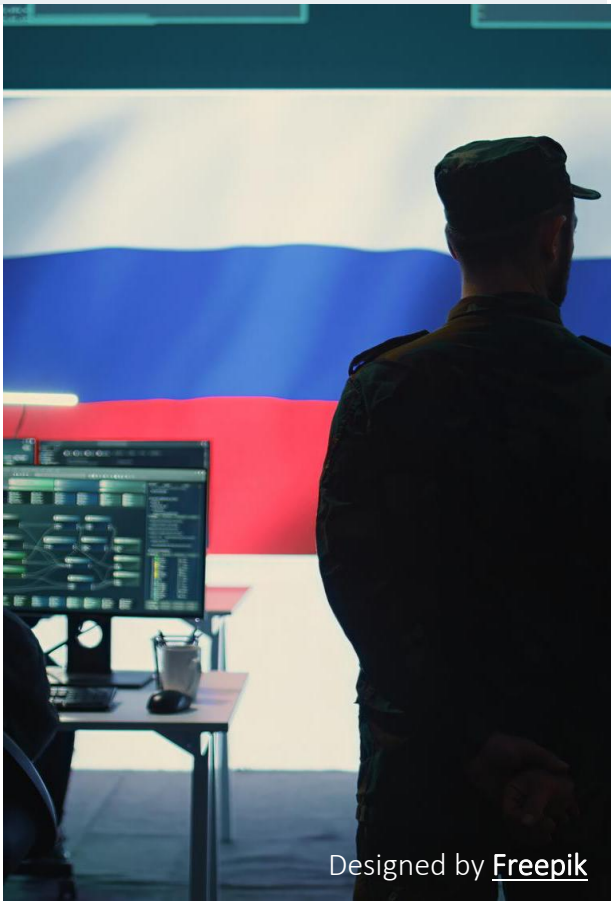
VÝZNAMNÉ UDALOSTI VO SVETE

Zneužívanie OAuth na presmerovanie obetí v phishingových kampaniach

Spoločnosť Microsoft varuje pred phishingovou kampaňou zameranou na subjekty v sektore verejnej správy, v rámci ktorej útočníci zneužívajú chybové presmerovania OAuth na obídenie bezpečnostných mechanizmov e-mailovej ochrany a webového prehliadača. Útočníci vytvoria škodlivé aplikácie OAuth v rámci vlastného Microsoft Entra ID alebo tenantu Google Workspace a nastavia presmerovanie v prípade chybnej autentifikácie na požadovanú URL. Do phishingových e-mailov vkladajú URL so špeciálnymi parametrami *scope*, *state* a *prompt=none*, ktoré automaticky vedú k neúspešnej autentifikácii, čo spustí presmerovací proces zneužívajúci legitímnu infraštruktúru. Phishingové e-maily s rôznou tematikou obsahujú škodlivé URL priamo v tele alebo v PDF prílohe. Šírené sú nástrojmi na hromadné rozposielanie e-mailov a vlastnými nástrojmi útočníkov vyvinutými v Python alebo Node.js. Zaznamenané boli aj prípady presmerovania na phishingové stránky využívajúce platformy attacker-in-the-middle ako EvilProxy, ktoré umožňujú zachytávanie platných relačných cookies zneužiteľných na obchádzanie MFA ochrany. Útočníci však používajú tiež presmerovania na stránky pre stiahnutie škodlivého archívu ZIP obsahujúceho súbor .LNK, ktorý spúšťa skript PowerShell pre fingerprinting obete a DLL side-loading malvéru.

Ruské štátom sponzorované skupiny kompromitujú účty na WhatsApp a Signal

Holandské informačné služby MIVD (Netherlands Defence Intelligence and Security Service) a AIVD (Netherlands General Intelligence and Security Service) varujú pred phishingovou kampaňou ruských štátom sponzorovaných skupín zameranou na predstaviteľov vlády, vojenský personál a novinárov, ktorej cieľom je špionáž a získavanie citlivých údajov. Útočníci obete kontaktujú prostredníctvom správ na platformách WhatsApp a Signal. Zneužívaním legitímnych mechanizmov autentifikácie a párovaním zariadení následne kompromitujú používateľské účty, čo im umožňuje prístup ku kontaktom a správam obete. Zaznamenané boli aj prípady, kedy útočník následne zmenil telefónne číslo asociované s daným kontom na Signal. Jedna kampaň spočíva v rozposielaní upozornení na podozrivú aktivitu a registráciu služby na novom zariadení a druhá v zneužití QR kódov na spárovanie ďalšieho zariadenia. Pridanie párovaného zariadenia je ťažšie detegovateľné, pretože nedochádza k odhláseniu používateľa. Používateľa by mali byť obozretní, nezdieľať citlivé informácie prostredníctvom aplikácií a pravidelne kontrolovať aktivitu a zoznam spárovaných zariadení.



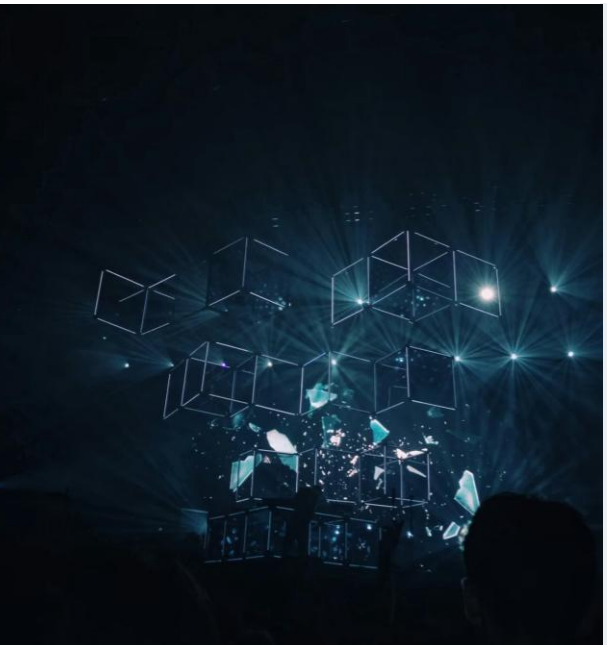
VÝZNAMNÉ UDALOSTI VO SVETE

Výskumníci demonštrovali zneužitie „Agentic Blabbering“ výstupov AI prehliadačov na tvorbu phishingového obsahu obchádzajúceho ich detekciu

Výskumníci z Guardio demonštrovali zneužitie tzv. „Agentic Blabbering“ agentového AI prehliadača Perplexity Comet na vytvorenie phishingového formuláru prostredníctvom OpenAI ChatGPT a Cursor, ktorý Comet následne už nevedel rozpoznať a vyplnil by ho. Pojem Agentic Blabbering označuje výstupy AI prehliadača, kde AI popisuje, čo vidí, čo sa deje, ako vyhodnocuje informácie a čo plánuje ďalej vykonať. Analýzou týchto výstupov možno prostredníctvom GAN (Generative Adversarial Network) upraviť phishing spôsobom obchádzajúcim bezpečnostné mechanizmy prehliadača.

Europol s partnermi rozložil kriminálnu proxy sieť SocksEscort tvorenú kompromitovanými routermi

Europol a partnerské organizácie z viacerých krajín v rámci medzinárodnej operácie Operation Lightning, rozložili botnet SocksEscort, ktorý využíval malvér AVRecon na kompromitovanie malých domácich a podnikových zariadení na poskytovanie anonymného smerovania škodlivej sieťovej premávky. Sieť slúžila kyberzločincom mimo iného pri krádežiach kryptomien, podvodoch, útokoch ransomvérom, DDoS, či na šírenie detskej pornografie. Pri operácii úrady zadržali 23 serverov, prevzali kontrolu nad 34 doménami a zmrazili kryptomeny v hodnote miliónov dolárov a jej prevádzku zastavili.



Čínsky CNCERT varuje pred rizikami AI frameworku OpenClaw a čínska vláda zakazuje jeho nasadenie

Čínsky tím CNCERT (China's National Computer Network Emergency Response Technical Team) vydal varovanie pred rizikami používania open-source AI agentovéj platformy OpenClaw. Varovanie upozorňuje na nedostatočné zabezpečenie inštancií v predvolenej konfigurácii a inherentné riziko rôznych foriem útokov typu prompt injection založených na spracovaní špeciálne vytvorených webových stránok. Efektívne sú útoky typu IDPI (Indirect Prompt Injection) a XPIA (Cross Domain Prompt Injection). Podľa agentúry Bloomberg čínska vláda s odkazom na tieto riziká zakázala použitie OpenClaw vo vládnej infraštruktúre a bankovom sektore.

VÝZNAMNÉ UDALOSTI VO SVETE

Poľské jadrové výskumné centrum sa stalo terčom kyberútoku

Poľské Národné centrum jadrového výskumu (NCBJ) čelilo kybernetického útoku, ktorý bezpečnostné systémy včas zachytili a zablokovali. Útok nepoškodil ani nenarušil prevádzku jadrového reaktora MARIA, ktorý sa používa na vedecké experimenty a výrobu medicínskych izotopov. Vyšetrovanie odhalilo neoverené indikátory naznačujúce možné spojenie s infraštruktúrou v Iráne, hoci táto atribúcia sa ešte nepotvrdila. Kybernetický útok poukázal na rastúce hrozby pre kritickú infraštruktúru a zdôraznil potrebu zvýšenej kybernetickej ochrany zariadení kritickej infraštruktúry.

Holandské ministerstvo financií potvrdilo prienik do IT systémov a kompromitáciu zamestnancov

Holandské ministerstvo financií potvrdilo, že sa 19. marca 2026 stalo obeťou kybernetického útoku, v rámci ktorého útočníci prenikli do niektorých informačných systémov. Bližšie informácie o spôsobe prieniku a rozsahu incidentu neboli zverejnené s odvolaním sa na prebiehajúce vyšetrovanie. V rámci incidentu malo dôjsť aj ku kompromitácii zamestnancov ministerstva.

Útočníci kompromitovali systémy Európskej komisie a exfiltrovali 350 GB dát

Európska komisia vyšetruje kybernetický útok na svoje cloudové účty Amazon, pri ktorom útočníci získali neautorizovaný prístup k časti cloudovej infraštruktúry. Odcudzili viac ako 350 GB dát, vrátane databáz a informácií viazaných na účty zamestnancov či e-mailové servery. Útočníci avizovali, že odcudzené dáta zverejnia neskôr, bez nároku na výkupné. Komisia bezodkladne prijala opatrenia na zmiernenie následkov a v súčasnosti interne vyšetruje príčinu aj rozsah kompromitácie.

VÝZNAMNÉ UDALOSTI VO SVETE

- Samsung v súvislosti s obvineniami z neoprávneného zberu dát aktualizuje pravidlá ochrany súkromia.
- Útok na dodávateľský reťazec prostredníctvom rozšírenia Chrome QuickLens zameraný na šírenie ClickFix a krádež kryptopeňaženiek.
- Europol s partnermi rozložil kyberkriminálnu decentralizovanú platformu The Com.
- Ukrajinský občan obvinený z prevádzkovania AI služby pre generovanie falošných dokladov OnlyFake.
- Iránske dronové útoky poškodili dátové centra AWS v UAE a Bahrajne.
- Europol s partnermi narušil činnosť phishing-as-a-service platformy Tycoon2FA.
- Phishingové kampane ruskej APT28 šíria nové druhy malvéru BadPaw a MeowMeow.
- Europol s partnermi rozložil organizovanú skupinu špecializujúcu sa na finančné podvody prostredníctvom online gamblingových platforiem.
- Microsoft varuje pred rastúcim zneužívaním AI a agentových systémov v rámci kybernetických útokov.
- FBI potvrdila prienik do systému pre správu súdnych rozhodnutí ohľadom sledovania a odpočúvania.
- Iránske skupiny zneužívajú kompromitované IP kamery na monitoring nepriateľa, BDA a cielenie kinetických operácií.
- Google Cloud Threat Horizons Report poskytuje prehľad o aktuálnych hrozbách a útokoch na cloudové systémy.
- Ruská APT28 v rámci útokov na vojenský personál Ukrajiny súčasne nasadzuje Covenant aj BeardShell.
- Meta predstavila rodičmi spravované kontá WhatsApp pre deti do 13 rokov.
- Britská vláda v rámci stratégie boja proti kyberkriminalite spustila Online Crime Centre.
- Google za rok 2025 v rámci programu bug bounty vyplatila odmeny vo výške vyše 17 miliónov dolárov.
- APT28 Roundcube Toolkit zneužitý v rámci útokov na ukrajinskú vládu.
- FBI zaistila webovú stránku skupiny Handala.

- Útočníci zneužívajú Microsft Azure Monitor na rozposielanie phishingových e-mailov.
- FBI v rámci Operation Alice zaistila 373 000 darknetových stránok promujúcich obsah so zneužívaním detí.
- OČTK v rámci medzinárodnej akcie narušili činnosť najväčších DDoS botnetov.
- OpenAI predstavila cloudové úložisko súborov pre ChatGPT.
- V USA odsúdili ruského hackera za poskytovanie IAB služieb ransomware-as-a-service skupine Yanluowang.
- Ruské OČTK zatkli údajného administrátora kyberkriminálneho fóra LeakBase.
- Phishingová kampaň zameraná na používateľov Tiktok For Business.
- Iránska skupina Handala kompromitovala osobný účet na Gmail riaditeľa FBI.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Keď z administrátorských funkcií vznikne RCE: prípadová štúdia OTRS Community Package Design

Bezpečnostní analytici CSIRT.SK objavili chybu v dizajne tiketovacieho systému OTRS Community. Táto bezpečnostná chyba umožňuje vykonávanie ľubovoľného kódu.

Kritická zraniteľnosť Cisco Catalyst SD-WAN Controller/Manager

Spoločnosť Cisco opravila kritickú zraniteľnosť vo svojom produkte Catalyst SD-WAN Controller/Manager. Chybu zabezpečenia aktívne zneužívajú útočníci na obídenie autentifikácie a získanie prístupu ku konfiguračnému rozhraniu.

Riešenie advanced endpoint security od TrendAI obsahuje kritické zraniteľnosti

Spoločnosť TrendAI (nové meno vetvy spoločnosti Trend Micro enterprise business) vydalo bezpečnostné aktualizácie pre svoje riešenie advanced endpoint security Apex One. Tie opravujú 8 zraniteľností z ktorých 2 sú vyhodnotené ako kritické.

Kritická zraniteľnosť Junos OS Evolved dovoľuje vykonávať kód ako root

Spoločnosť Juniper Networks opravila kritickú zraniteľnosť platformy On-Box Anomaly Detection vo svojich routeroch série PTX. Zraniteľnosť umožňuje bez autentifikácie vzdialene vykonávať kód s oprávneniami používateľa root.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti v Cisco Secure FMC a SCC umožňujú vzdialené vykonanie kódu

Spoločnosť Cisco vydala bezpečnostné aktualizácie nástroja pre manažment firewallov Secure Firewall Management Center (FMC) a Security Cloud Control (SCC) Firewall Management, ktoré opravujú 2 kritické zraniteľnosti umožňujúce obídenie prihlásenia, eskaláciu oprávnení a vzdialené vykonanie kódu.

Závažné zraniteľnosti Cisco Catalyst SD-WAN Manager

Spoločnosť Cisco opravila 5 závažných zraniteľností v Catalyst SD-WAN Manager. Tieto útočníkom umožňujú manipulovať so súbormi, získavať informácie, obchádzať prihlásenie, či eskalovať svoje oprávnenia. Cisco potvrdila, že útočníci aktívne zneužívajú dve z opravených zraniteľností.

Kritická zraniteľnosť modulu WordPress User Registration & Membership

Spoločnosť WPEverest vydala bezpečnostnú aktualizáciu svojho modulu User Registration & Membership pre WordPress, ktorá opravuje aktívne zneužívanú kritickú zraniteľnosť CVE-2026-1492. Vzdialený neautentifikovaný útočník ju môže zneužiť na vytvorenie administrátorského účtu.

Kritická zraniteľnosť v HPE Aruba Networking AOS-CX umožňuje reset administrátorského hesla

Spoločnosť HPE (Hewlett Packard Enterprise) vydala balík aktualizácií operačného systému prepínačov série Aruba CX, ktorý okrem iných opravuje jednu kritickú zraniteľnosť. CVE-2026-23813 umožňuje útočníkovi bez akýchkoľvek prihlasovacích údajov obísť autentifikáciu webového manažmentového rozhrania.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Veeam opravuje kritické zraniteľnosti produktu Backup & Replication

Spoločnosť Veeam vydala bezpečnostné aktualizácie zálohovacieho riešenia Backup & Replication, ktoré opravujú 7 zraniteľností, z čoho 5 je označených ako kritické. Vzdialenému autentifikovanému útočníkovi umožňujú vykonávanie kódu, obídenie bezpečnostných prvkov a manipuláciu so súbormi, eskaláciu privilégií a získanie prihlasovacích údajov.

Zero-day zraniteľnosti Google Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie svojho webového prehliadača Chrome, ktoré opravujú dve aktívne zneužívané vysoko závažné zraniteľnosti. Neautorizovanému útočníkovi po ich zneužití umožňujú zapisovať do pamäte a vzdialene vykonávať kód.

Apple opravili zraniteľnosť komponentu WebKit umožňujúcu obídenie politiky Same Origin

Spoločnosť Apple vydala bezpečnostné aktualizácie svojich operačných systémov iOS, iPadOS a macOS, ktoré opravujú zraniteľnosť komponentu WebKit. Zraniteľnosť spočíva v chybe mechanizmu CORS, ktorá vyplýva z nedostatočného overovania vstupov v rámci Navigation API.

Kritická zraniteľnosť GNU InetUtils telnetd umožňuje vzdialené vykonanie kódu

Bezpečnostní výskumníci zverejnili informácie o kritickej zraniteľnosti v GNU InetUtils telnetd. CVE-2026-32746 sa nachádza v handleri LINEMODE SLC (Set Local Characters) a umožňuje zápis do pamäte mimo povolených hodnôt.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zneužívaná zraniteľnosť Zimbra Collaboration Suite dovoľuje perzistentné XSS

CISA pridala do katalógu aktívne zneužívaných zraniteľností (KEV) vysoko závažnú zraniteľnosť Zimbra Collaboration Suite. CVE-2025-66376 umožňuje neautentifikovanému útočníkovi vykonávať útoky typu XSS cez e-maily vo formáte HTML.

Kritická zraniteľnosť ScreenConnect umožňuje prístup k reláciám

Spoločnosť ConnectWise opravila kritickú zraniteľnosť v produkte ScreenConnect, ktorá umožňuje útočníkom získať prístup ku kryptografickému materiálu inštancie, a spolu s ním k aktívnym reláciám. Útočník môže tiež získať zvýšené oprávnenia. Spoločnosť pozorovala pokusy o zneužitie zraniteľnosti.

Kritické zraniteľnosti Citrix NetScaler ADC a Gateway

Spoločnosť Citrix na základe interných kontrol objavila a opravila kritickú zraniteľnosť produktov Citrix NetScaler ADC a Gateway, ktorá umožňuje čítanie pamäte mimo povolené hodnoty. Zároveň opravila vysoko závažnú zraniteľnosť vedúcu ku zámene relácií používateľov.

Útočníci zneužívajú kritickú zraniteľnosť F5 BIG-IP APM

Spoločnosť F5 opravila kritickú chybu zabezpečenia na zariadeniach BIG-IP APM, ktorá môže viesť ku vykonaniu kódu na diaľku za nešpecifikovaných podmienok.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť WordPress Smart Slider 3 umožňuje krádež dát

Bezpečnostní výskumníci upozornili na kritickú zraniteľnosť v doplnku Smart Slider 3 pre WordPress, ktorý je aktívny na viac ako 800 000 webových stránkach. Zraniteľnosť umožňuje akémukoľvek autentifikovanému používateľovi vrátane úrovne subscriber čítať ľubovoľné súbory na serveri.

MESAČNÍK ZRANITEĽNOSTÍ MAREC 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3294.html