CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

FEBRUÁR 2026

TLP: CLEAR

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CSIRT.SK

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

1 Kyberbezpečnostná hra „Fakt alebo mýtus“

Vládna jednotka CSIRT spustila interaktívnu hru, ktorá prostredníctvom 30 otázok testuje znalosti používateľov o aktuálnych kybernetických hrozbách a spôsoboch ochrany. Súčasná hra je venovaná laickej verejnosti. VJ CSIRT pripravuje ďalšie úlohy pre pokročilejších používateľov. Cieľom je informovať o častých mýtoch, s ktorými sa v rámci svojej činnosti VJ CSIRT stretáva.

2 Notepad++ potvrdil hackerský útok na svoje systémy

Vývojári populárneho editoru s otvoreným zdrojovým kódom Notepad++ potvrdili, že útočníci kompromitovali ich infraštruktúru automatických aktualizácií od júna do decembra 2025.

3 Microsoft zavádza nástroj Sysmon ako súčasť operačných systémov Windows

Microsoft v rámci programu Windows 11 Insider Preview predstavil integráciu nástroja Sysmon priamo do operačného systému. Ide o veľmi populárny nástroj určený na obohacovanie záznamov o udalostiach.

4 Rusko začalo aktívne blokovať používanie Whatsapp a Telegram

Ruská vláda sa snaží úplne zablokovať prístup k aplikáciám na posielanie správ WhatsApp a Telegram pre používateľov v krajine ako súčasť širšieho tlaku na kontrolu internetu.

5 Železničná spoločnosť Eurail potvrdila únik citlivých údajov zákazníkov

Spoločnosť Eurail B.V., so sídlom v Holandsku, oznámila, že útočník získal prístup k údajom cestovateľov a dáta ponúka na predaj na dark webe.

6 Platby ransomvéru klesli na rekordne nízku úroveň aj pri náraste útokov v roku 2025

Spoločnosť Chainalysis zverejnila analýzu platieb ransomvérovým skupinám za rok 2025.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci február 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.

CSIRT.SK sa vo februári stretla s niekoľkými podvodnými kampaňami. Jednou z nich bola séria e-mailov cielená na zamestnancov dôležitej štátnej inštitúcie. Útočníci sa pokúšali zneužiť nepozornosť obetí odosielaním správ z falošných adries vo formáte *meno.priezvisko.organizácia(@)outlook.com*. Imitovali identitu reálnych zamestnancov a v správach oslovovali prijímateľov s cieľom začať podvodnú komunikáciu.

Vo februári sa tím CSIRT.SK stretol s podvodnou kampaňou zneužívajúcou meno spoločnosti Websupport. Útočníci šírili podvodný e-mail s odkazom na falošnú platobnú bránu, kde klientov spoločnosti informovali o ukončení služieb vzhľadom na neuhradené platby. Klienti si mali služby, resp. hosting svojich webstránok obnoviť platbou platobnou kartou. Jednotka vykonala analýzu vzorky predmetného e-mailu a kontaktovala správcov hostingu so žiadosťou o odstránenie phishingovej webovej stránky zo svojich serverov. Rovnako informovala o kampani aj firmu Websupport.

Vládna jednotka CSIRT na základe otvorených zdrojov a verejne dostupných vyhlásení zahraničných bezpečnostných orgánov varovala ohľadne zvýšeného rizika kybernetických útokov najmä v podobe DDoS kampaní zameraných na ciele v súvislosti so zimnými olympijskými hrami v Milano-Cortina 2026. Pravdepodobným aktérom zachytených útokov bola proruská hacktivistická skupina NoName057(52), ktorá už v minulosti realizovala útoky motivované geopolitickými udalosťami a politickými postojmi štátov podporujúcich Ukrajinu.

Organizácia v konštituencii CSIRT.SK nahlásila vo februári kompromitáciu konta zamestnanca, ku ktorej došlo prelomením 2FA overovania. Z konta následne útočník rozposlal hromadný e-mail do celej EÚ, vrátane Slovenska. Partner k predmetnému incidentu uviedol ako možný spôsob kompromitácie 2FA tzv. "hands on keyboard phishing". Organizácia získala vzorku rozposielaného phishingového e-mailu a informovala všetkých príjemcov o e-mailovej hrozbe, pričom nezaznamenala žiadne ďalšie podozrivé pokusy o prihlásenie.

Štátna organizácia informovala CSIRT.SK o úspešnom prihlásení používateľa z pekingskej IP adresy (Čína) do konta Microsoft Office365 prostredníctvom komerčnej VPN ServerMania. Táto IP adresa bola viackrát reportovaná v rámci verejných databáz ako škodlivá. Jednotka odporučila štandardné kroky v rámci riešenia incidentu, teda blokovanie konta obete minimálne do zmeny hesla a do zrušenia všetkých aktívnych relácií s ním spojených. Organizácia v rámci investigácie odhalila ďalšie úspešné prihlásenie používateľa (destinácia Peking) do O365 prostredníctvom komerčnej VPN Sharktech.

Február priniesol aj incident spojený s kompromitáciou webového sídla štátnej organizácie. Útok na hostovací server sa odohral formou „injection php-fpm“. Škody sa podarilo minimalizovať a služby obnoviť v pôvodnej kvalite. Nasledujúci deň však organizácia zaznamenala ďalší útok s použitím metódy bruteforce (slovníkový útok) na službu SSH. Táto bola bez ich vedomosti sprístupnená do internetu bez

obmedzení ako aj ich zariadenia firewall, ktoré boli vypnuté. Po týchto odhaleniach prijala náležité opatrenia, obnovila vypadnuté služby a vykonala hardening zasiahnutého servera.

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.

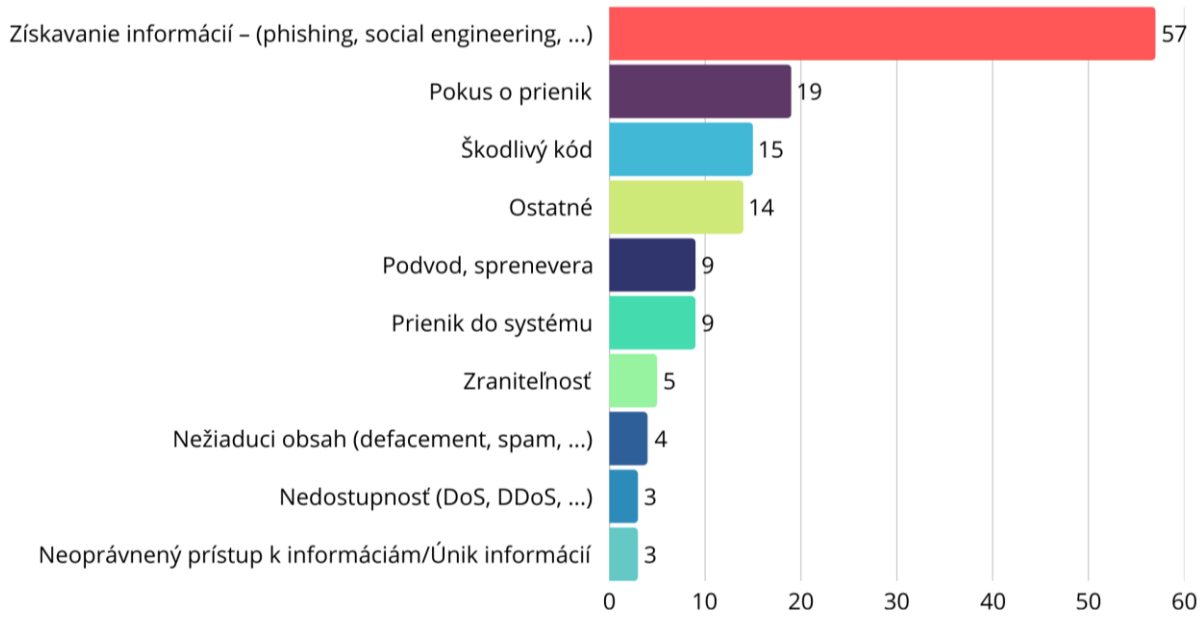
V rámci služby Ares prebiehalo penetračné testovanie piatich webových aplikácií. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

Vo februári CSIRT.SK plošne varoval svoju konštituenciu ohľadom útoku na dodávateľský reťazec, resp. aktualizačný server nástroja Notepad++, nad ktorým sofistikovaný útočník získal kontrolu. Jednotka informovala aj o zraniteľnosti CVE-2026-21509 v balíku Microsoft Office, ktorú v rámci rozsiahlej kampane aktívne zneužívala ruská štátom sponzorovaná skupina APT 28.

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. Vo februári jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Inštitútu pre pracovnú rehabilitáciu občanov so zdravotným postihnutím v Bratislave. Prednášala aj študentom Strednej priemyselnej školy strojníckej (Fajnorka) v Bratislave, Strednej odbornej školy dopravy a služieb v Nových Zámkoch a Strednej odbornej školy stavebnej- Építészeti Szakközépiskola v Nových Zámkoch. Prednášky pre učiteľov prebehli v Spojenej škole Modrý Kameň a na Gymnáziu Augusta Horislava Škultétyho vo Veľkom Krtíši.

Člen tímu CSIRT.SK prezentoval vo februári jednotku v rozhovore v rámci podcastu SHARE na portáli Zive.aktulity.sk.

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



VÝZNAMNÉ UDALOSTI VO SVETE

Kyberbezpečnostná hra „Fakt alebo Mýtus“

Vládna jednotka CSIRT spustila interaktívnu hru, ktorá prostredníctvom 30 otázok testuje znalosti používateľov o aktuálnych kybernetických hrozbách a spôsoboch ochrany. Hra zdôrazňuje potrebu správnej prevencie a revízie bezpečnostných opatrení. Cieľom je zvýšiť povedomie zamestnancov a verejnosti o kybernetických hrozbách a podporiť bezpečné správanie pri práci s IT systémami.

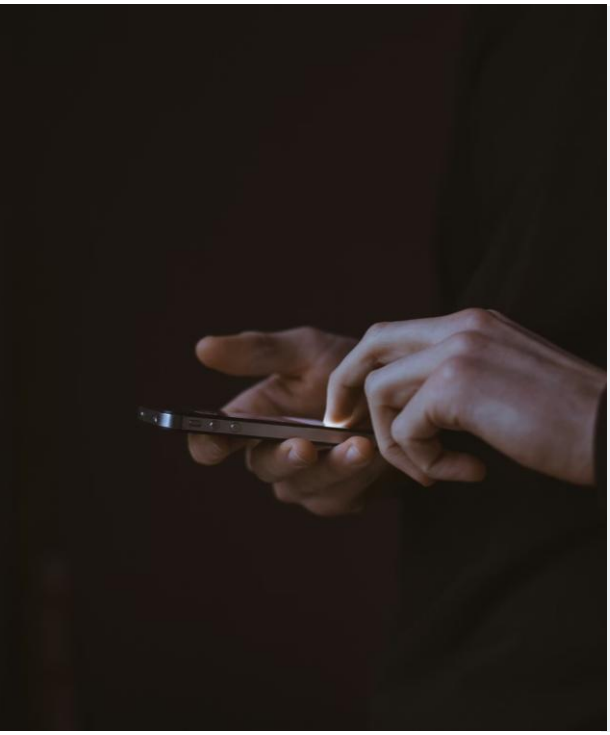
CERT-PL zverejnil report z útokov na energeticky sektor z decembra 2025

CERT-PL zverejnil rozsiahly report dokumentujúci útoky ruskej štátom sponzorovanej skupiny Static Tundra na energetický sektor PL z decembra 2025. Static Tundra je známa väzbami na ruskú FSB. Výskumníci spoločností Eset a Dragos však útoky atribuovali ruským skupinám Sandworm a Electrum, čo poukazuje na zložitosť a chúlostivosť procesu atribúcie. Útočníci na prienik do systémov zneužili platné prihlasovacie údaje z minulosti a taktiež bezpečnostné zraniteľnosti perimetrových zariadení Fortinet Fortigate. Následne vykonali enumeráciu dostupných systémov a technológií ICS, ktoré znefunkčnili modifikáciou firmvéru, zmenou konfiguračných nastavení alebo inštaláciou malvéru, vrátane wiperov DynoWiper a LazyWiper. Skupina svoje aktivity maskovala použitím siete TOR a kompromitovaných zariadení s poľskými aj zahraničnými IP adresami. Samotný wiper neobsahoval funkcionalitu pre zabezpečenie perzistencie ani komunikáciu s C2, čo naznačuje čistú orientáciu na deštrukciu systémov. V rámci infraštruktúry sa zamerali aj na získanie prihlasovacích údajov do Microsoft 365, ktoré následne zneužili na prienik do služieb Exchange, Teams a SharePoint. Na nich vyhľadávali informácie súvisiace s modernizáciou OT technológií, SCADA systémami a technicko-prevádzkovými operáciami.

IAB Európska Komisia, Holandsko a Fínsko potvrdili rozsiahlu kompromitáciu systémov v dôsledku zneužitia zraniteľnosti v Ivanti EPMM

Európska Komisia, Holandsko a Fínsko potvrdili kompromitáciu dôležitých systémov, ku ktorej došlo v dôsledku zneužitia kritických zraniteľností CVE-2026-1281 a CVE-2026-1340 v Ivanti Endpoint Manager Mobile. Spoločnosť Shadowserver eviduje vyše 50 verejne dostupných inštancií, ktoré boli s vysokou pravdepodobnosťou kompromitované. Ivanti aktualizovala svoje varovanie a doplnila nástroj pre kontrolu artefaktov a indikátorov kompromitácie systémov.

VÝZNAMNÉ UDALOSTI VO SVETE

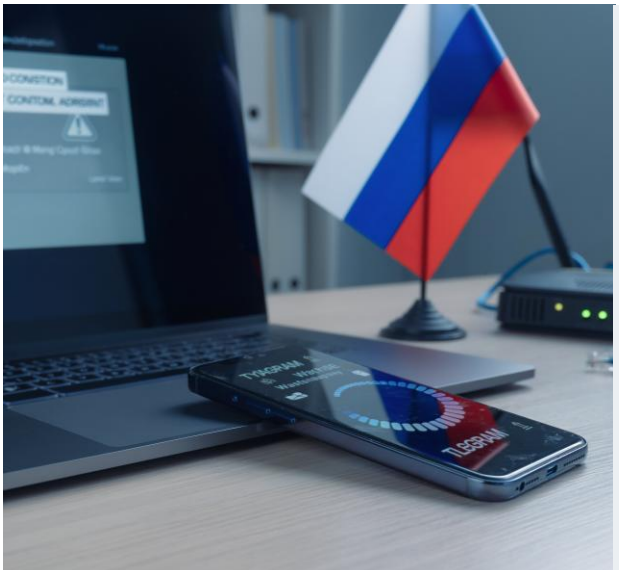


Google zverejnil analýzu a odporúčania voči vishingovej kampani ShinyHunters

Skupina ShinyHunters a prepojené skupiny cielenými telefonátmi (vishing) a falošnými firemnými prihlasovacími stránkami získavajú prihlasovacie údaje a kódy viacfaktorovej autentifikácie (MFA) do Single Sign-On (SSO) služieb ako Okta, Microsoft Entra alebo Google SSO. Po získaní prístupov sa prihlasujú do legitímnych dashboardov SSO, kde vidia, ku ktorým SaaS aplikáciám má používateľ prístup. Prenikajú do cloudových služieb ako Salesforce, Microsoft 365, SharePoint, Slack, DocuSign či Google Drive, odkiaľ exfiltrujú citlivé dáta a používajú ich na vydieranie alebo ďalšiu krádež. Útočníci často registrujú falošné domény imitujúce legitímne firemné služby, aby zvýšili dôveryhodnosť. Na zabezpečenie perzistencie môžu útočníci do systému pridať aj vlastné zariadenie pre MFA. Tento typ útoku umožňuje kompromitovať celú spoločnosť cez jeden účet SSO, čo predstavuje vysoké riziko pre podnikovú bezpečnosť.

Ruská skupina APT28 zneužíva zero-day zraniteľnosť v Microsoft Office

CERT-UA a ZSCALER zverejnili informácie o aktivitách ruskej štátom sponzorovanej skupiny APT28 súvisiacich s aktívnym zneužívaním zero-day zraniteľnosti CVE-2026-21509 v Microsoft Office. Útočníci rozosielajú tzv. spear-phishingové e-maily obsahujúce škodlivé prílohy formátu RTF, ktorých cieľom je infekcia zariadení obetí dvomi verziami dropperov. Prvá distribuuje malvér MiniDoor, ktorý e-maily preposiela na adresy útočníka zriadené na doménach *outlook.com* a *proton.me*. Druhá verzia distribuuje loader Pixynetloader slúžiaci na doručenie implantu Grunt frameworku Covenant. Zneužitie Grunt skupinou APT28 v septembri 2025 zdokumentovali výskumníci zo spoločnosti Sekoia. Výskumníci evidujú útoky cielené na Ukrajinu, Slovensko a Rumunsko.



Rusko začalo aktívne blokovať používanie WhatsApp a Telegram

Ruská vláda sa snaží úplne zablokovať prístup k aplikácii WhatsApp pre používateľov v krajine ako súčasť širšieho tlaku na kontrolu internetu. Úrady tvrdia, že tieto opatrenia prijali v záujme boja proti kriminalite, podvodom a údajnej neochote sprístupňovať údaje OČTK. Spoločnosť Meta označila blokovanie za ohrozenie bezpečnosti a súkromia používateľov. Mnohí obyvatelia Ruska však tieto obmedzenia v praxi obchádzajú pomocou VPN, pričom zásahy proti Telegramu vyvolávajú domácu kritiku vzhľadom na jeho význam pre verejnú, opozičnú aj vojenskú komunikáciu.

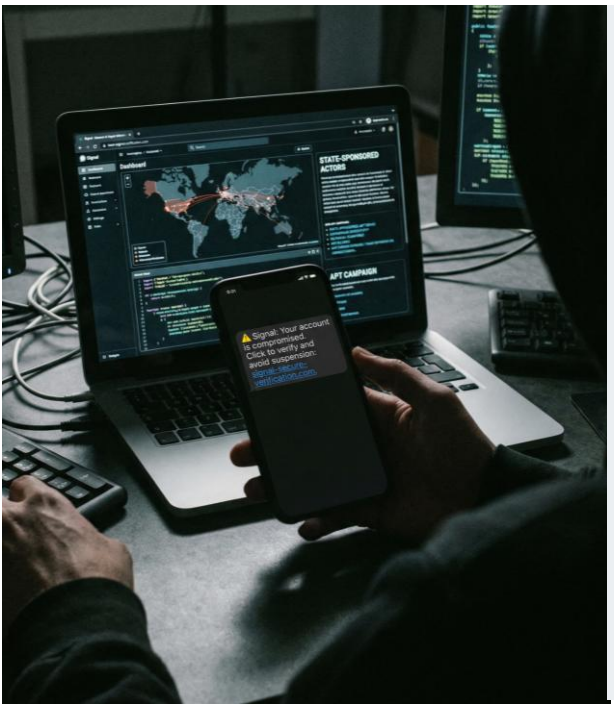
VÝZNAMNÉ UDALOSTI VO SVETE

Notepad++ potvrdil útok na svoje systémy

Vývojári populárneho textového editoru s otvoreným zdrojovým kódom, Notepad++, potvrdili, že útočníci kompromitovali ich infraštruktúru automatických aktualizácií od júna do decembra 2025. Nezávislí experti pripisujú útok čínskej štátnej hackerskej skupine, ktorá zmenila tok aktualizácií, a takto distribuovala konkrétnym používateľom škodlivé aktualizácie a súbory namiesto legitímnych. Útočníci zneužili slabé overovanie v nástroji WinGup a presmerovali aktualizácie na svoje servery. V útoku pokračovali až do 2. decembra 2025, kedy vývojári zamedzili ich prístup. Medzitým Notepad++ migroval na nový hosting, resetoval kompromitované poverenia, posilnil verifikáciu certifikátov a digitálnych podpisov v aktualizáciách verzie 8.8.9 a plánuje ďalšie zlepšenia.

Microsoft zavádza nástroj Sysmon ako súčasť operačných systémov Windows

Microsoft v rámci programu Windows 11 Insider Preview predstavil integráciu nástroja Sysmon priamo do operačného systému. Nástroj zaznamenáva zadefinované udalosti priamo do tzv. Windows Event logov. Spoločnosť informovala o svojom pláne v novembri 2025. Sysmon je kritickým nástrojom, ktorý využívajú špecialisti v rôznych oblastiach kybernetickej bezpečnosti. Jeho využitie v rozsiahlych infraštruktúrach vyžadovalo manuálnu inštaláciu. Nástroj bude v predvolenej inštalácii vypnutý a používatelia ho musia explicitne aktivovať prostredníctvom ovládacieho panela alebo príkazu PowerShell. Pred aktiváciou integrovanej verzie je potrebné odstrániť manuálne nainštalované verzie.



Nemecko varuje pred phishingovou kampaňou zameranou na kompromitáciu účtov Signal

Nemecké bezpečnostné úrady vydali varovanie pred sofistikovanou phishingovou kampaňou, v ktorej pravdepodobne štátom sponzorovaní aktéri cielia na účty komunikačnej platformy Signal vysokopostavených osôb (politikov, vojenských dôstojníkov, diplomatov a investigatívnych novinárov). Využívajú pri tom metódy sociálneho inžinierstva bez potreby nasadenia malvéru či zneužitia zraniteľností. Útočníci sa vydávajú za oficiálnu podporu pre aplikáciu Signal alebo chatbot. Ich cieľom je vylákať od obetí overovací SMS kód, PIN kód k aplikácii alebo ich prinútiť k naskenovaniu QR kódu. Tak získajú buď plnú kontrolu nad účtom, alebo prístup k chatom a kontaktom cez nové pripojené zariadenie. Varovanie zdôrazňuje, že platforma nikdy neoslovuje používateľov týmto spôsobom a obetiam hrozí kompromitácia komunikácie a kontaktov.

VÝZNAMNÉ UDALOSTI VO SVETE

Google zverejnil analýzu zneužívania Gemini AI zo strany štátom sponzorovaných skupín

Google Threat Intelligence Group analyzovala prípady, v ktorých štátom sponzorované skupiny z Číny, Iránu, Severnej Kórey a Ruska využívajú generatívne modely AI vrátane Gemini na podporu svojich operácií. Útočníci používajú AI na prieskum cieľov, tvorbu phishingových správ, generovanie a ladenie kódu, výskum zraniteľností a automatizáciu úloh. Google zároveň zaznamenala pokusy o tzv. „model distillation“, pri ktorých útočníci extrahujú znalosti z modelu s cieľom replikovať jeho schopnosti. Spoločnosť uvádza, že nespozorovala prelomenie bezpečnostných hraníc modelov, ale eviduje ich zneužívanie ako nástroja na zefektívnenie existujúcich kybernetických aktivít a prijíma opatrenia na detekciu a obmedzenie takéhoto správania.

Železničná spoločnosť Eurail potvrdila únik citlivých údajov zákazníkov

Spoločnosť Eurail B.V., so sídlom v Holandsku, oznámila, že útočník získal prístup k údajom cestovateľov a dáta ponúka na predaj na dark webe. Vzorové ukážky dát sú k dispozícii na platforme Telegram. Eurail vyšetruje rozsah incidentu, pričom medzi dotknuté údaje môžu patriť mená, dátumy narodenia, kontaktné údaje, čísla pasov, bankové údaje a informácie súvisiace s programom DiscoverEU. Spoločnosť informovala príslušné úrady podľa GDPR a odporučila zákazníkom zmeniť heslá a sledovať finančné účty.

Diesel Vortex realizuje phishingové kampane na logistické spoločnosti a prepravcov v USA a EÚ

Finančne motivovaná skupina Diesel Vortex sa špecializuje na phishingové útoky na prepravné a logistické spoločnosti v USA a EÚ. Od septembra 2025 získala vyše 1649 prihlasovacích údajov do rôznych podporných platforiem. Vďaka konfiguračnej chybe sa podarilo nájsť databázu SQL, logy z Telegramových webhook-ov a konceptuálnu mapu zachytávajúcu komplexný ekosystém útočníka, ktorý zahŕňa call centrum, e-mailovú podporu, programátorov a špecialistov na vyhľadávanie kontaktov obetí. Podľa informácií ide o arménsky hovoriacu skupinu s infraštruktúrou v Rusku. Phishingové e-maily skupina rozposiela cez službu Zoho SMTP a Zeptomail a na obchádzanie bezpečnostných prvkov zneužíva homoglyfické útoky pomocou znakov v cyrilike. Skupina využíva aj vishing a infiltráciu do Telegramových kanálov obetí, double brokering, krádež materiálu a jeho prepravu inou spoločnosťou za finančný zisk.

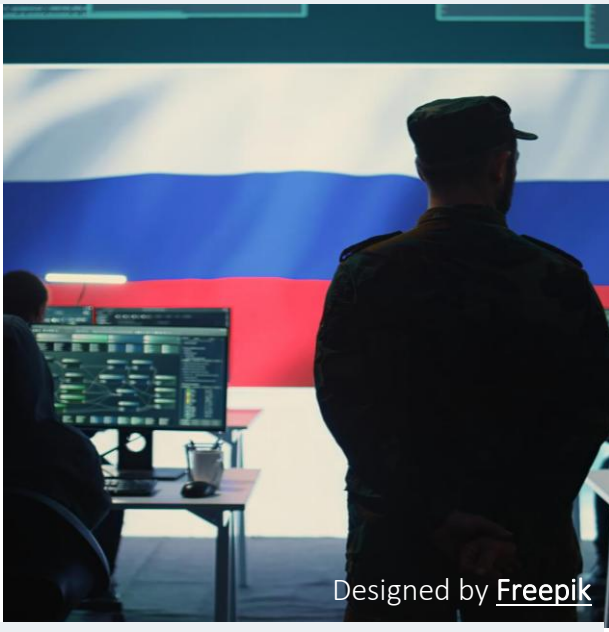
VÝZNAMNÉ UDALOSTI VO SVETE

Ruská skupina UAC-0050 cieli na finančné inštitúcie v Európe

Ruská skupina UAC-0050 rozšírila svoje cielenie z Ukrajiny na finančné inštitúcie v Európe. Cieľom skupiny zostáva špionáž, získavanie finančných prostriedkov a psychologické operácie. Zo podvrhnutých domén rozosielajú phishingové e-maily obsahujúce linky na stiahnutie škodlivého archívu ZIP z platformy na zdieľanie súborov PixelDrain. Cieľom je inštalácia ruského softvéru na vzdialený prístup RMS (Remote Manipulator System), ktorý útočníkom umožňuje získanie kontroly nad zariadením prostredníctvom princípu LOTL (Living Off The Land). V rámci útokov na Ukrajinu skupina za týmto účelom zneužívala malvér LiteManager alebo Remcos RAT.

Ruská skupina APT28 v rámci spear-phishingovej kampane Operation MacroMaze zneužíva webhook[.]site

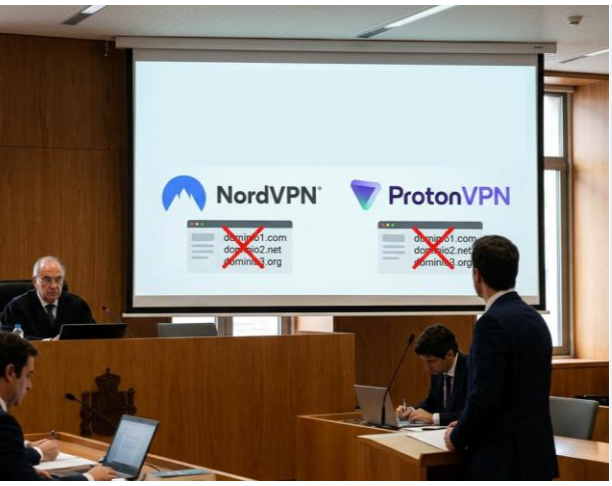
Ruská štátom sponzorovaná skupina APT28 v období medzi 25. septembrom 2025 a januárom 2026 realizovala e-mailovú spear-phishingovú kampaň Operation MacroMaze. Kampaň sa opierala o základné nástroje a zneužívanie legitímnych služieb pre vytvorenie infraštruktúry a exfiltráciu dát. Správy obsahovali špeciálne vytvorený dokument, ktorý po otvorení kontaktuje doménu *webhook[.]site*, a následne funguje ako dropper ďalšieho malvéru. Skupina zlepšuje maskovanie aktivít a opäť zneužíva webové prehliadače v tzv. headless režime.



Platby ransomvéru klesli na rekordne nízku úroveň aj pri náraste útokov v roku 2025

Spoločnosť Chainalysis zverejnila analýzu platieb ransomvérovým skupinám za rok 2025. Napriek signifikantnému nárastu počtu ransomvérových a vydieračských útokov zaznamenali približne 28-percentný pokles počtu obetí, ktoré zaplatili výkupné. Tento trend potvrdzuje aj súhrnná správa spoločnosti Coveware, podľa ktorej podiel obetí platiacich výkupné klesá najmä vďaka lepšej pripravenosti organizácií, dostupnosti záloh a rastúcemu právnemu tlaku neplatiť útočníkom. V reakcii na tento vývoj sa útočníci čoraz viac zameriavajú na krádež dát a vydieračské taktiky namiesto samotného šifrovania systémov. Initial Access Brokers (IAB) zarobili približne rovnaké sumy v rokoch 2024 aj 2025.

VÝZNAMNÉ UDALOSTI VO SVETE



Španielsko nariadilo NordVPN a ProtonVPN blokovanie 16 domén pre nelegálne streamovanie bez ich účasti na pojednávaní

Španielsky súd udelil preventívne opatrenia spoločnostiam NordVPN a ProtonVPN a nariadil poskytovateľom VPN zablokovať 16 webových stránok využívaných na nelegálne streamovanie zápasov LaLiga. Spoločnosti poskytujúce VPN služby uviedli, že o konaní nedostali predchádzajúce oznámenie a nemohli sa brániť pred vydaním príkazu.

VÝZNAMNÉ UDALOSTI VO SVETE

- Výskumník odhaľuje únik fotiek zo súkromných profilov na Instagrame.
- OČTK v rámci akcie Operation Switch Off rozložili nelegálne platformy pre streamovanie TV.
- Greynoise zachytila skenovanie a enumeráciu Citrix Netscaler a Citrix ADC Gateway.
- Útočníci pokračujú v aktívnom zneužívaní CVE-2025-11953 v knižnici NPM @react-native-community/cli.
- CISA pasívne pridáva príznaky zneužitia zraniteľností ransomvérovými skupinami do svojej databázy KEV.
- Microsoft v apríli 2027 ukončí podporu EWS API na MS 365 a Exchange Online.
- Nový nástroj s otvoreným zdrojovým kódom Tirith analyzuje škodlivosť príkazov kopírovaných do terminálu.
- CISA vydala nariadenie na odstránenie rizikových zariadení s ukončenou technickou podporou.
- Útočníci aktívne zneužívajú zraniteľnosti v Solarwinds WHD na kompromitáciu systémov.
- Výskumníci odhalili nový mobilný spyware ZeroDayRAT distribuovaný prostredníctvom Telegramu.
- Holandské OČTK zadržali prevádzkovateľa phishing-as-a-service platformy JokerOTP.
- Holandský telekomunikačný operátor Odido potvrdil rozsiahly únik dát.
- Muž žiadal odmenu za odstránenie citlivých súborov omylom zdieľaných holandskou políciou.
- Nový Android bankový malvér Massiv sa šíri ako falošná aplikácia IPTV.
- Operácia CrescentHarvest cieli na iránskych disidentov prostredníctvom phishingu a malvéru RAT.
- Anthropic predstavuje Claude Code Security na AI-asistované odhaľovanie zraniteľností v zdrojovom kóde.
- Rusky hovoriaci útočník použil generatívne AI služby pri kompromitovaní viac ako 600 firewallov Fortinet FortiGate.

- Iránska APT skupina MuddyWater nasadzuje nové druhy malvéru.
- Reco.ai v rámci promovania svojich služieb zverejnila prehľadový článok o možnostiach, význame a rizikách AI agentového ekosystému OpenClaw.
- Platforma 1Campaign umožňuje tvorbu a správu phishingových kampaní promovaných cez Google Ads.
- Falošné pohovory na pozície vývojára v Next.js ako vektor útoku na vývojárov.
- Skupina UNC2814 prenikla do desiatok telekomunikačných firiem a vládnych agentúr.
- Zariadenia Apple iPhone a iPad sú certifikované na ukladanie utajovaných skutočností NATO.
- Google sprísnila kritériá využívania API kľúčov pre prístup ku Gemini AI.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Microsoft opravil aktívne zneužívanú zero-day zraniteľnosť v balíku Office

Spoločnosť Microsoft vydala bezpečnostné aktualizácie Microsoft Office, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť. CVE-2026-21509 možno zneužiť podvrhnutím súborov na obídenie bezpečnostných mechanizmov pre ochranu pred zneužitím funkcií COM/OLE a získanie kontroly nad systémom. Zraniteľnosť zneužíva skupina APT28 v rámci rozsiahlej kampane. Americká CISA pridala zraniteľnosť na svoj zoznam aktívne zneužívaných zraniteľností KEV (Known Exploited Vulnerabilities).

Kritické zero-day zraniteľnosti v Ivanti Endpoint Manager Mobile

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre Ivanti Endpoint Manager Mobile, ktoré opravujú dve aktívne zneužívané kritické zero-day zraniteľnosti. CVE-2026-1281 a CVE-2026-1340 umožňujú injekciu kódu. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Zraniteľnosť Windows Notepad umožňuje vzdialené vykonanie kódu

Spoločnosť Microsoft v rámci Patch Tuesday vo februári 2026 opravila vysoko závažnú bezpečnostnú zraniteľnosť v textovom editore Windows Notepad. CVE-2026-20841 umožňuje vzdialené vykonanie kódu prostredníctvom dokumentu Markdown.

Kritická zraniteľnosť FortiClientEMS 7.4.4

Fortinet FortiClientEMS verzie 7.4.4 obsahuje zraniteľnosť, ktorá umožňuje vykonávať SQL injekciu prostredníctvom nesanitizovaných HTTP požiadaviek. Vzdialený neautorizovaný útočník môže získať schopnosť vykonávať kód a príkazy.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Microsoft v balíku aktualizácií Patch Tuesday opravil zraniteľnosti

Spoločnosť Microsoft vydala vo februári 2026 balík opráv pre portfólio svojich produktov opravujúci 54 zraniteľností, z ktorých 2 spoločnosť označila ako kritické. Tieto umožňujú získať citlivé informácie a eskalovať oprávnenia. Šesť opravených zraniteľností je aktívne zneužívaných a umožňujú eskalovať oprávnenia útočníka, obchádzať bezpečnostné prvky a zneprístupniť službu.

Apple opravili aktívne zneužívanú zero-day zraniteľnosť operačných systémov

Spoločnosť Apple vydala bezpečnostné aktualizácie svojich operačných systémov iOS, iPadOS, macOS, tvOS, watchOS a visionOS, ktoré opravujú viacero zraniteľností, z čoho jedna je označená ako aktívne zneužívaná zero-day.

Kritická zraniteľnosť modulu WPvivid Backup & Migration pre WordPress umožňuje vykonávať kód

Vývojári modulu WPvivid Backup & Migration pre WordPress opravili kritickú zraniteľnosť, ktorá umožňuje útočníkom zneužiť proces výmeny šifrovacích kľúčov na podvrhnutie ľubovoľného škodlivého súboru a jeho nahratie do ľubovoľného verejne dostupného adresáru.

Kritická zraniteľnosť BeyondTrust Remote Support a Privileged Remote Access umožňuje vykonávať príkazy

Vývojári BeyondTrust Remote Support a Privileged Remote Access opravili kritickú zraniteľnosť, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi vykonávať systémové príkazy na zraniteľnom systéme.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná zraniteľnosť v Google Chrome umožňuje vzdialene vykonávať kód

Vývojári spoločnosti Google opravili vysoko závažnú aktívne zneužívanú zraniteľnosť v prehliadači Chrome, ktorá umožňuje vzdialené vykonanie kódu.

Kritické zraniteľnosti v rozšíreniach Visual Studio Code umožňujú vykonávať kód a exfiltrovať dáta

Výskumníci zo spoločnosti Ox Security identifikovali viaceré závažné zraniteľnosti v populárnych rozšíreniach pre Visual Studio Code (VSCode). Útočníci ich môžu zneužiť na kradnutie lokálnych súborov a vzdialené vykonávanie kódu priamo v prostredí vývojára.

MESAČNÍK ZRANITEĽNOSTÍ FEBRUÁR 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3158.html