CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

# MESAČNÁ SPRÁVA

AUGUST 2025

TLP: CLEAR

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

## 1 Severokórejskí hackeri zneužívajú falošné pracovné ponuky na krádež dát a kryptomien

Severokórejskí hackeri zo skupiny UNC4899 cielene napádajú organizácie prostredníctvom falošných pracovných ponúk na LinkedIn a Telegrame, kde lákajú obete na pozície softvérových vývojárov.

## 2 BreachForums sa vracia na .onion adresu

BreachForums, ktoré v apríli 2025 náhle zmizlo z internetu údajne kvôli kritickej 0-day zraniteľnosti MyBB, sa 25. júla 2025 vrátilo na svoju pôvodnú .onion adresu.

## 3 Phishingová kampaň zameraná na booking.com

Výskumníci zverejnili informácie o sofistikovanej phishingovej kampani cielené na používateľov služby BOOKING.COM, v rámci ktorej útočníci na maskovanie a sťaženie manuálnej inšpekcie URL zobrazovanej v prehliadači zneužívajú japonský homoglyf ん.

## 4 Ruská hackerská skupina secret blizzard využíva útoky aitm na ambasády s malvérom Apoloshadow

Ruská hackerská skupina Secret Blizzard, prepojená s ruskou FSB, od februára 2025 využíva prístup cez domácich poskytovateľov internetu na útoky typu adversary-in-the-middle (AiTM) proti zahraničným ambasádam v Moskve.

## 5 Nový variant clickjackingového útoku kradne dáta zo správcov hesiel

Počas konferencie DEFCON 2025 ukázal bezpečnostný výskumník Marek Tóth nový variant clickjackingu, pri ktorom útočníci prekryjú webové prvky neviditeľnými tlačidlami a prinútia používateľov nevedome spustiť rozšírenie správcu hesiel, čím získajú prístup k prihlasovacím údajom, kreditným kartám, osobným dátam, passkeys aj kódom TOTP.

## 6 Spoločnosť Guardio odhaľuje zraniteľnosti AI prehliadača Comet

Spoločnosť Guardio ukázala, že prehliadač Comet na baze AI agentov od Perplexity je náchylný na známe typy útokov vrátane phishingu, podvodných obchodov a útokov špecifických pre AI systémy ako sú napríklad promt injection.

# RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci august riešil typicky najmä phishingové kampane zasahujúce jeho konštituenciu. Opäť sa objavili prípady podvodných e-mailov, ktoré útočníci posielajú zamestnancom rôznych organizácií v mene ich nadriadených a žiadajú o vykonanie rýchleho prevodu financií. Po potvrdení zamestnanca, že daná transakcia môže byť vykonaná, odosielateľ podvodného e-mailu poskytne inštrukcie k úhrade vrátane zahraničného IBANu, na ktorý má platba prebehnúť. V podobných prípadoch odporúčame overiť si legitimitu požiadavky priamym kontaktovaním oprávneného vedúceho zamestnanca, ideálne osobne alebo telefonicky na legitímny kontakt danej osoby (nie číslo uvedené v podvodnom e-maile). Podobne odporúčame preveriť informáciu o zmene bankových údajov Vášho dodávateľa alebo obchodného partnera, predtým ako odošlete platbu n nový účet.

V auguste prijal CSIRT.SK informáciu o potenciálne kompromitovanom zariadení malvérom. Počas kompromitácie došlo k úniku prihlasovacích údajov pre viaceré účty. Jednotka požiadala zasiahnutú organizáciu o poskytnutie logov. V spolupráci s SK-CERT poskytla organizácii informácie o kompromitovanom zariadení a odporučila vykonať súbor opatrení ako na zasiahnutom zariadení tak aj v internom systéme spoločnosti.

Tento mesiac prebiehala aj kampaň voči zariadeniam Fortinet SSL VPN, ktoré sa stali terčom rozsiahlych útokov typu bruteforce. Bolo do nej zapojených viac než 780 škodlivých IP adries z viacerých krajín. Po prvej vlne útokov na FortiOS nasledovala druhá, zameraná na FortiManager, čo naznačovalo prípravu na zneužitie niektorej zraniteľnosti. CSIRT.SK informoval organizácie, ktoré boli potenciálnymi obeťami, o prijatých informáciách od partnera.

Služba Have I Been Pwned zverejnila v auguste pod názvom "Data Troll Stealer Logs" novú databázu obsahujúcu uniknuté prihlasovacie údaje z rôznych nešpecifikovaných služieb. Vzhľadom na to, že nebolo možné zistiť, odkiaľ konkrétne účty unikli, jednotka odporúčala kontaktovať predmetných používateľov a oboznámiť ich s odporúčaním zmeniť si prihlasovacie heslá všade, kam sa so svojim uniknutým pracovným e-mailom registrovali. V súvislosti s únikom chceme apelovať na všetkých používateľov e-mailových služieb, aby nepoužívali svoje pracovné adresy pri registrácii na súkromne využívané služby. Odporúčame vytvoriť si oddelenú súkromnú e-mailovú adresu určenú iba pre účely registrácie na rôzne webové služby, e-shopy, a podobne.

Ani tento mesiac sa nevyhol pokusom o získanie nelegitímneho prístupu ku chráneným účtom pomocou hrubej sily. CSIRT.SK prijal hlásenia útokov typu brute-force na rozhranie /wp-login.php webových stránok organizácie vo svojej konštituencii. Organizáciu požiadal o preverenie auditných logov, či došlo k úspešnému prihláseniu. Vzhľadom na to, že webová stránka mala dostupnú WordPress administráciu z internetu, boli odporučené opatrenia na obmedzenie prístupu k administračnému rozhraniu stránky. Analýza nepotvrdila prelomenie hesla. Organizácia mala nastavené pravidlo blokovania účtu na 24 hodín po troch neúspešných pokusoch o prihlásenie.

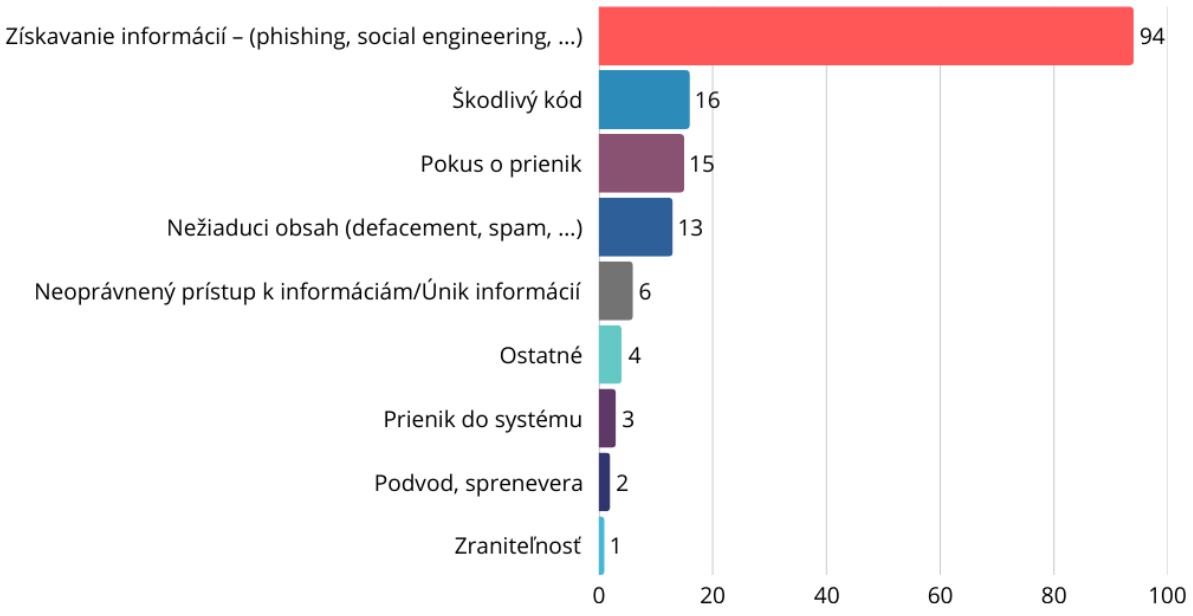
CSIRT.SK prijal v auguste aj informáciu o sťažnosti občana na nedbalý prístup štátneho zamestnanca, ktorý by mohol viesť k potenciálnemu úniku citlivých informácií. V tejto súvislosti odporučil upovedomiť zamestnancov organizácie, aby dbali na bezpečné zaobchádzanie s citlivými dátami a vyvarovali sa

zverejňovaniu fotografií, na ktorých sú viditeľné oficiálne dokumenty, pracovná plocha počítača a podobný obsah.

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 auguste jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre učiteľov Obchodnej akadémie a Strednej zdravotníckej školy v Považskej Bystrici.

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



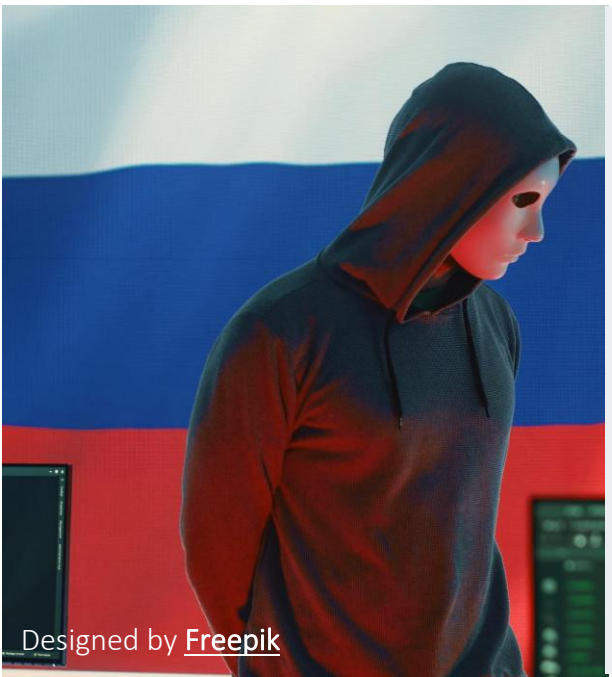
# VÝZNAMNÉ UDALOSTI VO SVETE


## Open-source platforma Thorium pre rýchlu analýzu malvéru a digitálnu forenznú analýzu

CISA spolu so spoločnosťou Sandia National Laboratories vyvinula a formou open-source zverejnila platformu Thorium, ktorá slúži na rýchlu a škálovateľnú analýzu malvéru a digitálnu forenziku. Thorium umožňuje bezpečnostným tímom orchestráciu rôznych analytických nástrojov – od kontajnerov Docker až po VM či bare-metal systémy – a dosahuje výkon viac než 10 miliónov súborov za hodinu a vyše 1 700 analýz za sekundu. Využíva moderné technológie ako Kubernetes, ScyllaDB a REST API, ponúka podrobné filtrovanie výsledkov, značkovanie a riadený prístup podľa tímov.

## Severokórejskí hackeri zneužívajú falošné pracovné ponuky na krádež dát a kryptomien

Severokórejskí hackeri zo skupiny UNC4899 cielene napádajú organizácie prostredníctvom falošných pracovných ponúk na LinkedIn a Telegrame, kde lákajú obete na pozície softvérových vývojárov. Pod zámienkou týchto ponúk ich presvedčia, aby spustili škodlivé kontajnery Docker, ktoré nainštalujú malvér ako PLOTTWIST a MAZEWIRE. Tento malvér im umožňuje získať neoprávnený prístup ku cloudovým službám, napríklad Google Cloud či AWS, kde kradnú citlivé údaje a kryptomeny. Útočníci obchádzajú bezpečnostné opatrenia vrátane viacfaktorovej autentifikácie, manipulujú s prístupovými kľúčmi a využívajú zraniteľnosti v cloudových prostrediach. Táto taktika nadväzuje na predchádzajúce kampane, v ktorých skupina šírila škodlivé balíčky v repozitároch npm s cieľom infikovať vývojárov a ukradnúť finančné prostriedky.


## Ruská hackerská skupina Secret Blizzard využíva útoky AiTM na ambasády s malvérom

Ruská hackerská skupina Secret Blizzard, prepojená s ruskou FSB, od februára 2025 využíva prístup cez domácich poskytovateľov internetu na útoky typu adversary-in-the-middle (AiTM) proti zahraničným ambasádam v Moskve. Útočníci presmerúvajú diplomatov na falošné stránky, ktoré predstierajú bezpečnostné aktualizácie (napr. od Kaspersky), a podstrkujú im vlastné koreňové certifikáty, čím získavajú schopnosť dešifrovať a sledovať ich internetovú komunikáciu. Nasadzujú pritom malvér ApolloShadow a obchádzajú štandardné zabezpečenia bez potreby zneužiť softvérové zraniteľnosti. Microsoft varuje pred používaním nedôveryhodných miestnych ISP a odporúča zapnúť VPN, šifrovanie prenosov a viacfaktorovú autentifikáciu.

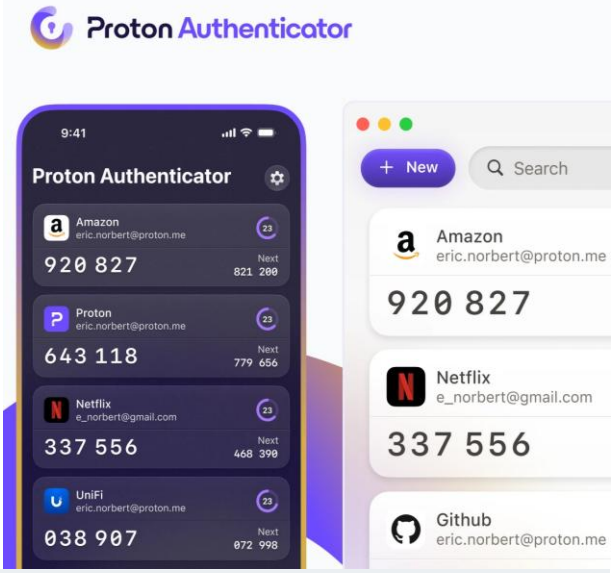
# VÝZNAMNÉ UDALOSTI VO SVETE


## Ransomvérová skupina Akira zintenzívňuje útoky na firewally SonicWall cez zraniteľné VPN prístupy

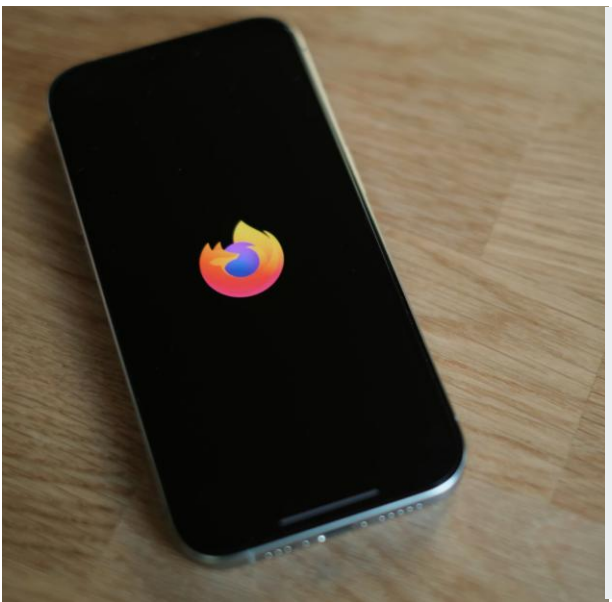
Ransomvérová skupina Akira od 15. júla 2025 výrazne zintenzívnila ransomvérové útoky zamerané na firewally SonicWall, pričom útočníci aktívne zneužívajú zraniteľnosti alebo slabé zabezpečenie VPN prístupov, aby sa dostali do podnikových sietí, kde následne šifrujú dáta a požadujú výkupné. Bezpečnostní výskumníci zaznamenali nárast prípadov a varujú, že útočníci sa zameriavajú najmä na zariadenia bez viacfaktorovej autentifikácie alebo s nezaplátanými softvérovými aktualizáciami. Môže ísť buď o novú zero-day zraniteľnosť, alebo len o zneužitie uniknutých prihlasovacích údajov. Spoločnosť SonicWall zatiaľ nepotvrdila konkrétnu zraniteľnosť, ale odporúča okamžitú aktualizáciu firmvéru a sprísnenie vzdialeného prístupu.

## Proton Authenticator opravuje chybu, ktorá lokálne zobrazovala kódy TOTP

Zdroj: proton.me



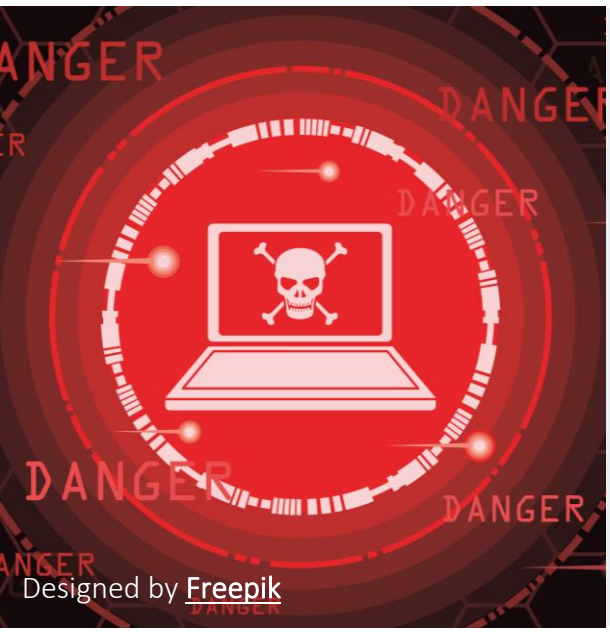

Spoločnosť Proton rýchlo opravila chybu v aplikácii Proton Authenticator pre iOS, ktorá pri zapnutom logovaní zaznamenávala celé TOTP tajomstvá (seedy) v čitateľnej podobe, čo znamenalo, že ktokoľvek s prístupom k zariadeniu alebo k zdieľaným logom mohol tieto kódy zneužiť. Proton zdôraznila, že synchronizácia prebieha cez end to end šifrovanie a dáta sa zo zariadenia neposielajú na servery, takže problém vznikal len lokálne a používateľom odporúča aplikáciu okamžite aktualizovať a dávať pozor na zdieľanie logov.



## Mozilla varuje pred phishingom vývojárov doplnkov pre Firefox s rizikom útokov na dodávateľský reťazec

Mozilla upozornila vývojárov doplnkov pre Firefox na aktívnu phishingovú kampaň, ktorá zasiela falošné e-maily s výzvou na aktualizáciu účtov na addons.mozilla.org s cieľom ukradnúť prihlasovacie údaje. Útočníci po získaní prístupu k účtom vývojárov dokážu realizovať útoky na dodávateľský reťazec. V poslednej dobe možno vidieť rozšírenie phishingových kampaní zameraných na rôzne vývojárske platformy.

# VÝZNAMNÉ UDALOSTI VO SVETE

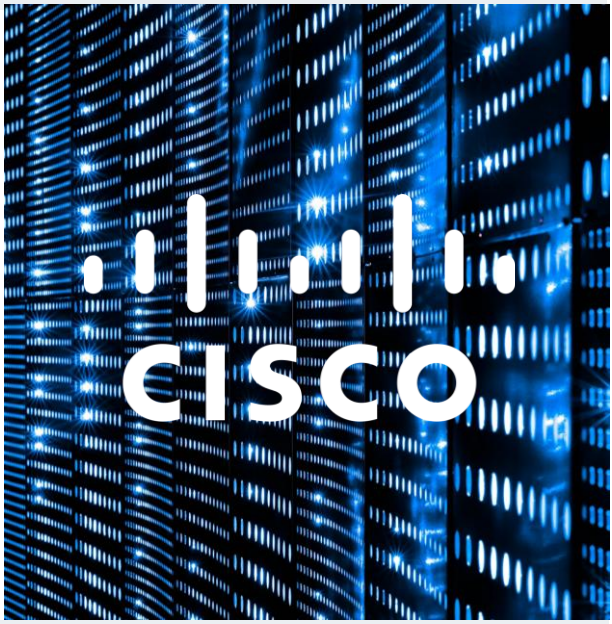



## Nový variant clickjackingového útoku kradne dáta zo správcov hesiel

Počas konferencie DEFCON 2025 ukázal bezpečnostný výskumník Marek Tóth nový variant clickjackingu, pri ktorom útočníci prekryjú webové prvky neviditeľnými tlačidlami a oklamú používateľov, ktorí nevedome spustia rozšírenie správcu hesiel. Tak získajú prístup k prihlasovacím údajom, kreditným kartám, osobným dátam, passkeys aj TOTP kódom. Problém sa týkal 1Password, LastPass, NordPass, Enpass, Dashlane, Keeper, ProtonPass, RoboForm, Bitwarden, iCloud Passwords a LogMeOnce. Niektorí výrobcovia už vydali opravy, iní na nich pracujú. Bezpečnostní experti odporúčajú okamžite aktualizovať rozšírenia a vypnúť automatické vyplňovanie, prípadne nastaviť režim „on click“.

## Cisco potvrdzuje vishingový útok na zamestnanca a únik základných profilových údajov cez cloudové CRM

Spoločnosť Cisco potvrdila, že útočník uskutočnil vishing (hlasový phishing) na jej zamestnanca a získal prístup k jednej inštancii cloudového CRM systému tretej strany. To mu umožnilo extrahovať základné profilové údaje používateľov registrovaných na Cisco.com vrátane mien, e-mailov, telefónnych čísel, adries, priradeného používateľského CISCO ID, názvu organizácie a dátumov vzniku účtov, pričom žiadne heslá, citlivé firemné ani zákaznícke údaje neboli kompromitované. Výskumníci hypotetizujú, že sa môže jednať o súčasť kampane cielenej na Salesforce.

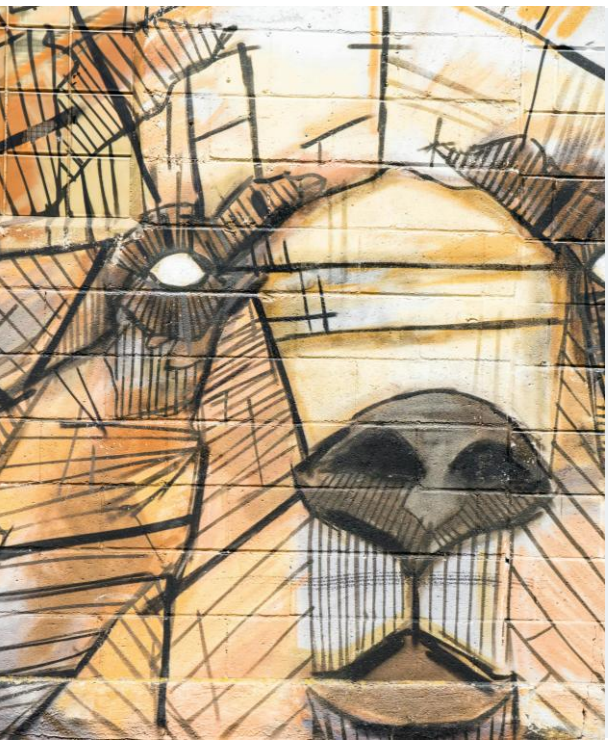




## Nová post-exploitačná metóda využíva Zoom a Microsoft Teams na skrytú C2 komunikáciu

Bezpečnostní výskumníci na konferencii BlackHat USA zverejnili informácie o novej post exploitačnej metóde pri ktorej zneužívajú servery TURN služieb Zoom a Microsoft Teams na budovanie príkazového a riadiaceho (C2) kanála. Namiesto priameho spojenia cez známe C2 servery presmerujú škodlivú komunikáciu cez legitímnu infraštruktúru videokonferenčných nástrojov, čím zakryjú svoje aktivity pred bezpečnostnými riešeniami. Na tento účel nasadia nástroj TURNt, ktorý umožní vytvárať proxy spojenia (napr. cez SOCKS5), tunelovať vzdialené relácie (napr. VNC) a prenášať súbory – všetko cez šifrovanú premávku WebRTC. Útočníci nepotrebujú žiadny exploit, stačí im platný účet v službe a bežný internetový prístup. Vďaka tomu obídu firewally, TLS inšpekciu aj sandboxy, ktoré takéto spojenie vyhodnotia ako bežný videohovor.

# VÝZNAMNÉ UDALOSTI VO SVETE

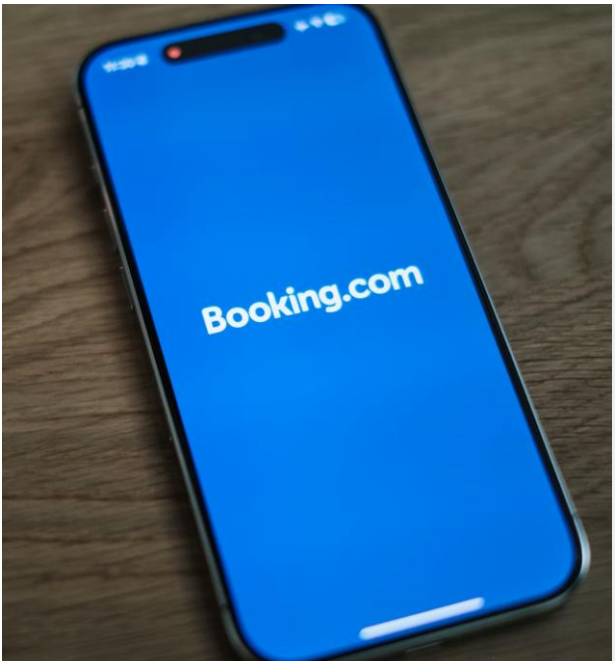


## Kampaň GreedyBear kradne prihlasovacie údaje cez škodlivé rozšírenia pre Firefox maskované ako kryptomenové peňaženky

Spoločnosť Koi Security objavila a zdokumentovala kampaň s názvom GreedyBear, kde útočníci nahrali do oficiálneho Firefox Add-ons Store viac než 150 škodlivých rozšírení, ktoré sa vydávajú za kryptomenové peňaženky ako MetaMask alebo TronLink. Ich cieľom je však kradnutie prihlasovacích údajov a IP adries používateľov. Najskôr získali dôveru pomocou neškodných verzií s pozitívnymi recenziami, potom rozšírenia upravili a vložili do nich malvér, ktorý posiela ukradnuté informácie na ich servery. V rámci kampane už odcudzili približne milión dolárov. Útočníci využívajú AI na rýchle šírenie malvéru a sofistikované vyhýbanie sa detekcii. Vyšetrovanie potvrdilo, že ide o dobre organizovanú skupinu zameranú na kryptomeny.

## Phishingové útoky na Microsoft 365 a šírenie kompromitovaných účtov

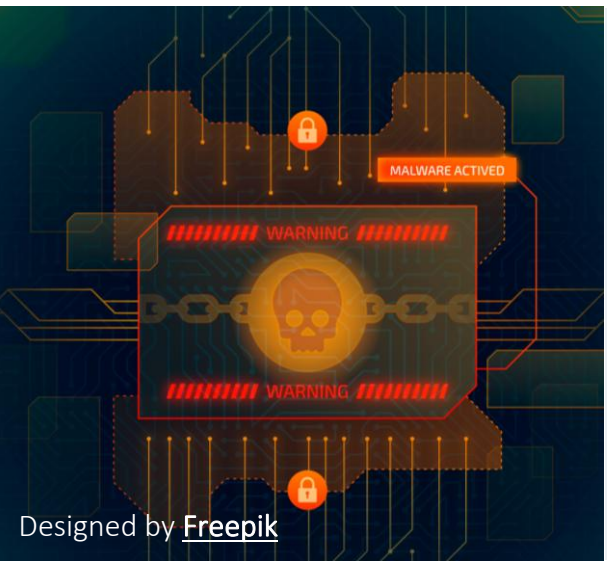
Spoločnosť VARONIS v rámci promovania svojich služieb zverejnila analýzu phishingových útokov na získavanie prihlasovacích údajov do Microsoft 365, ktoré sa ďalej šíria prostredníctvom zdieľania súborov vytvorených kompromitovanými účtami. Analýza poukazuje aj na postupne sa meniaci životný cyklus phishingových kampaní a postupné znižovanie nárokov na technické know-how z dôvodu masívneho rozmachu AI technológií.




## Phishingová kampaň zameraná na Booking.com

Výskumníci zverejnili informácie o sofistikovanej phishingovej kampani cielenej na používateľov služby BOOKING.COM. V rámci nej útočníci na maskovanie a sťaženie manuálnej inšpekcie URL zobrazovanej v prehliadači zneužívajú japonský homoglyf ん. Phishing šíri súbor MSI, ktorý môže slúžiť na ďalšiu distribúciu infostealerov a RAT. Zaznamenali aj kampaň zneužívajúcu identitu INTUIT, v rámci ktorej útočníci vytvárajú typosquattingové domény zamieňajúce písmená i a l a využívajú ich na rozposielanie phishingových e-mailov. Pri priamom prístupe na škodlivú URL obsiahnutú v správe bez prekliku presmerujú návštevníka na legitímne prihlasovanie do služby Intuit.

# VÝZNAMNÉ UDALOSTI VO SVETE




## Ransomvérová skupina Charon cieli na verejnú správu a letecký priemysel na Blízkom východe

Výskumníci zverejnili informácie o novej ransomvérovej skupine CHARON, ktorá sa zameriava na subjekty v sektoroch verejnej správy a leteckého priemyslu na Blízkom východe. Podľa Trend Micro ide o sofistikovanú skupinu, ktorá používa pokročilé techniky ako DLL sideloading, process injection a BYOVD na obídenie a deaktiváciu riešení EDR. Niektoré TTP sa prekrývajú s čínskou skupinou EARTH BAXIA, no môže ísť aj o pokus o falšovanie totožnosti alebo len náhodnú zhodu v modus operandi.

## Nemecko varuje pred zákazom používania adblockerov

Nemecký spolkový najvyšší súd (BGH) zrušil časť rozhodnutia Hamburského odvolacieho súdu a prikázal nové dokazovanie, či rozšírenie Adblock Plus (Eyeo) porušuje autorské práva manipuláciou DOM, CSSOM alebo bytecode. Mozilla upozorňuje, že rozhodnutie by mohlo zakázať nielen adblokery, ale aj rozšírenia zlepšujúce súkromie, prístupnosť či bezpečnosť, čím ohrozí slobodu používateľov, inovácie a otvorenosť webu. Spoločnosť Mozilla sa obáva, že Nemecko bude možno prvá krajina, ktorá zablokuje používanie riešení blokujúcich reklamy.


## GodRAT: nový trojan postavený na Gh0st RAT sa šíri cez Skype

Bezpečnostní výskumníci zo spoločnosti Kaspersky objavili nový trojan GodRAT, ktorý útočníci postavili na kóde Gh0st RAT a šírili cez škodlivé súbory .scr a .pif maskované ako finančné dokumenty posielané cez Skype do krajín ako SAE, Hongkong, Jordánsko a Libanon. Útočníci do obrázkov ukrývali shellkód pomocou steganografie a nasadzovali moduly, najmä FileManager na prieskum systému a kradnutie hesiel z prehliadača, pričom ako záložný implantát používali AsyncRAT. Analýza ukázala, že GodRAT vychádza z malvéru AwesomePuppet RAT, ktorý má prepojenie na APT skupinu Winnti. Ide teda o jeho evolúciu s rovnakými distribučnými trikmi. Napriek tomu, že Gh0st RAT vznikol pred dvadsiatimi rokmi, kyberzločinci tieto techniky stále využívajú a Kaspersky zaznamenal posledné prípady GodRATu ešte 12. augusta 2025.

# VÝZNAMNÉ UDALOSTI VO SVETE

## Spoločnosť Guardio odhaľuje zraniteľnosti AI prehliadača Comet

Spoločnosť Guardio ukázala, že prehliadač Comet na báze AI agentov od Perplexity je náchylný na známe typy útokov vrátane phishingu, podvodných obchodov a útokov špecifických pre AI systémy ako sú napr. promt injection. Počas testov bez váhania kúpil falošné hodinky Apple Watch na neexistujúcom obchode Walmart, otvoril phishingový e-mail vydávajúci sa za Wells Fargo, prihlásil sa na falošnej stránke a splnil inštrukcie ukryté vo falošnej CAPTCHA, čím spustil stiahnutie škodlivého súboru. Guardio tento typ manipulácie označila ako PromptFix a varovala, že AI prehliadače môžu takéto útoky opakovať, čo vedie k novej vlne podvodov nazývanej „Scamlexity“. Odporučila, aby ľudia zatiaľ sami kontrolovali bankovníctvo, nákupy aj e-maily, kým sa bezpečnosť agentických AI výrazne nezlepší.

## Phishingová kampaň ZipLine

Phishingová kampaň označená ako ZipLine mení tradičný prístup phishingových útokov. Obete núti iniciovať prvý kontakt. Útočníci využívajú formuláre „Kontaktujte nás“ na webových stránkach firiem, predstierajú záujem o spoluprácu a čakajú na odpoveď cieľa. Po niekoľkých týždňoch dôveryhodnej komunikácie zasielajú e-mail s neškodným vzhľadom, ktorý obsahuje škodlivý archív .zip. V ňom sa nachádza súbor .lnk, ktorý po otvorení spustí implantát „MixShell“ – pamäťový škodlivý kód s funkciami pre vzdialený prístup a perzistentný prístup do systému. Útočníci často používajú domény a webové stránky zhodné s názvami legitímnych amerických firiem, čo naznačuje starostlivo naplánovanú a koordinovanú kampaň.

# VÝZNAMNÉ UDALOSTI VO SVETE

- Ukrajinský CERT-UA upozornil na kyberútoky skupiny UAC-0099, ktorá cieli na vládne agentúry, obranné sily a firmy v obrannom priemysle na Ukrajine.
- Spoločnosť META predstavila ďalšiu bezpečnostnú funkciu aplikácie WHATSAPP, ktorá má používateľov varovať pred podvodnými kampaňami.
- Bezpečnostní výskumníci zo spoločnosti Hunt.io odhalili uniknutý zdrojový kód bankového trójskeho vírusu ERMAC 3.0, ktorý sa objavil vo verejnom adresári na serveri.
- Bezpečnostní výskumníci odhalili škodlivé balíčky v PyPI a npm, ktoré cez závislosti spúšťajú malvér.
- Severokórejská štátom sponzorovaná skupina KIMSUKI cieli na diplomatické misie ostatných štátov v Severnej Kórei.
- Skupina Storm-0501 prešla od klasického on-prem ransomvéru k útokom v hybridnej cloudovej infraštruktúre.

# ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

## Nové závažné zraniteľnosti Citrix NetScaler môžu byť aktívne zneužívané

Spoločnosť Citrix opravila jednu kritickú a dve vysoko závažné zraniteľnosti zariadení NetScaler ADC a NetScaler Gateway. Kritická zraniteľnosť je pravdepodobne aktívne zneužívaná.

## Kritická aktívne zneužívaná zraniteľnosť vo WordPress doplnku Alone

WordPress webstránky využívajúce tému menom Alone, sú aktívne zneužívané na vzdialené vykonávanie škodlivého kódu cez kritickú zraniteľnosť. Toto zneužitie bolo detegované už vo viac ako 120 tisíc prípadoch.

## Kritická zraniteľnosť v JavaScript balíčku Node-SAML

Vývojári knižnice Node-SAML vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť vo verifikácii kryptografických podpisov, čo môže spôsobiť neautorizovaný prístup k citlivým údajom.

## Google opravil aktívne zneužívané zraniteľnosti operačného systému Android

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj operačný systém Android, ktoré opravujú 6 zraniteľností, z čoho 1 je označená ako kritická a 2 ako aktívne zneužívané. Aktívne zneužívané CVE-2025-21479 a CVE-2025-27038 v komponentoch Qualcomm možno zneužiť na poškodenie obsahu pamäte.

# ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

## Vysoko závažná zraniteľnosť v Cursor AI IDE

Vývojári AI editora kódu Cursor vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-54136 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

## Zero-day zraniteľnosti v produkte Adobe Experience Manager Forms on JEE

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoj produkt Adobe Experience Manager (AEM) Forms on JEE, ktoré opravujú dve kritické zero-day zraniteľnosti. Zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

## Microsoft vydal usmernenie k závažnej zraniteľnosti (CVE-2025-53786) v hybridných nasadeniach MS Exchange

Spoločnosť Microsoft vydala usmernenie pre mitigáciu bezpečnostnej zraniteľnosti CVE-2025-53786 s vysokou závažnosťou pre svoj produkt MS Exchange. Zatiaľ nebolo detegované aktívne zneužívanie zraniteľnosti, avšak Microsoft varuje, že zneužitie je ťažko detekovateľné.

## Kritická zraniteľnosť v kamerách od Axis Communications dovoľuje vzdialené vykonávanie kódu

Bezpečnostní výskumníci z Claroty Team82 zverejnili informácie o zraniteľnostiach produktov spoločnosti Axis Communications z ktorých jedna CVE-2025-30023 je kritická a môže byť použitá na útok na serverovú aj klientskú stranu nasadených produktov.

# ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV



## Aktualizácia nástroja WinRAR opravila aktívne zneužívanú zero-day zraniteľnosť

Vývojári archivačného nástroja WinRAR vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje závažnú bezpečnostnú zraniteľnosť CVE-2025-8088. Táto zraniteľnosť je často zneužívaná vo phishingových kampaniach na distribúciu škodlivého kódu.

## Win-DDoS: Nová technika distribuovaného narušenia dostupnosti služby

Bezpečnostní výskumníci zverejnili na stretnutí DEF CON 33 informácie o zraniteľnosti CVE-2025-32724, ktorá ohrozuje verejne dostupné doménové radiče dosiahnuteľné z internetu. Tie sa vedia efektívne zmeniť na obete, a tiež botov vyvolávajúcich narušenie dostupnosti služby. Zraniteľnosť má povahu zero-click a dovoľuje útočníkovi spôsobiť narušenie služby bez nákladnej alebo špecializovanej sady nástrojov.



## Xerox vydal bezpečnostné záplaty pre vysoko závažné zraniteľnosti CVE-2025-8355 a CVE-2025-8356

Spoločnosť Xerox vydala urgentné bezpečnostné varovanie týkajúce sa dvoch kritických zraniteľností v softvéri FreeFlow Core. Tieto zraniteľnosti umožňujú útočníkom vykonať útoky Server-Side Request Forgery (SSRF) a vzdialene vykonávať kód.

## SAP v augustovom Patch Tuesday opravil viacero kritických a vysoko závažných zraniteľností v produktoch

Spoločnosť SAP vydala 12. augusta 2025 bezpečnostné aktualizácie obsahujúce opravy pre 20 zraniteľností. 3 z nich sú hodnotené ako kritické a umožňujú injektovanie kódu. 2 vysoko závažné dovoľujú získať vyššie oprávnenia, obchádzať autorizáciu a injektovať ABAP kód.

# ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

## Zero-day zraniteľnosť v produktoch Microsoft dostala bezpečnostnú záplatu v augustovom Patch Tuesday

CVE-2025-53779 je chyba relatívnej cesty vo Windows Kerberos, ktorá umožňuje autorizovanému útočníkovi zvýšiť oprávnenia cez sieť ako súčasť útoku nazvaného BadSuccessor. V augustovom Patch Tuesday bolo opravených aj 13 kritických zraniteľností.

## Analytici upozorňujú na bezpečnostné kamery DAHUA – majú 2 závažné zraniteľnosti

Bezpečnostní výskumníci z Bitdefender IoT Research Team zverejnili informácie o zraniteľnostiach CVE-2025-31700 a CVE-2025-31701 vo firmvéri pre bezpečnostné kamery značky Dahua. Ide o závažné zraniteľnosti, ktoré vie útočník zneužiť na vzdialené vykonávanie kódu.

## Závažná zraniteľnosť FortiWeb umožňuje obísť autentifikáciu

Spoločnosť Fortinet opravila vysoko závažnú zraniteľnosť vo svojich zariadeniach FortiWeb, ktorá z dôvodu nevhodnej validácie parametrov v cookies umožňuje vzdialeným útočníkom obísť autentifikáciu a získať administrátorské oprávnenia.

## Kritická zraniteľnosť Cisco Secure Firewall Management Center dovoľuje vykonávať systémové príkazy

Spoločnosť Cisco opravila kritickú zraniteľnosť v Cisco Secure Firewall Management Center, ktorá z dôvodu nevhodnej validácie používateľských vstupov dovoľuje vzdialenému útočníkovi pri prihlasovaní odoslať požiadavku obsahujúcu príkaz Shell. Ten zraniteľné zariadenie vykoná.

# ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

## Aktualizácie Windows 11 24H2 môžu spôsobiť nesprávne fungovanie a poškodenie pevného disku

V aktualizácii programu Defender z augustového balíka Patch Tuesday sa nachádza chyba, ktorá môže spôsobiť chyby na pevných diskoch. Jej najčastejším prejavom je chýbajúci disk v súborovom systéme alebo poškodenie a strata dát. Problém sa podľa viacerých zdrojov prejavuje pri kontinuálnom zápise rádovo desiatok GB.

## Aktívne zneužívaná závažná zraniteľnosť Apple iOS, iPadOS a macOS

Spoločnosť Apple opravila vysoko závažnú aktívne zneužívanú zraniteľnosť v komponente ImageIO systémov macOS, iOS a iPadOS, ktoré umožňuje útočníkom spôsobiť poškodenie pamäte, zneužiteľné na ďalšie fázy útoku. To nastáva pri spracovaní špeciálne upraveného obrázkového súboru.

## Moduly manažérov hesiel pre webové prehliadače sú obeťou clickjackingu

Bezpečnostný výskumník odhalil zraniteľnosť prídavných modulov pre webové prehliadače viacerých manažérov hesiel, ktorá umožňuje vykonávať clickbaitingové útoky a kradnúť z nich citlivé údaje. Útočníci sa môžu dostať ku prihlasovacím údajom, ale aj platobným či osobným údajom.

# MESAČNÍK ZRANITEĽNOSTÍ AUGUST 2025

**VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.**

https://csirt.sk/posts/2756.html