CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JÚN 2025

TLP: CLEAR

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

1 Android malvér CROCODILIS sa stal globálnou hrozbou

Bezpečnostní výskumníci z THREAT FABRIC zverejnili analýzu Android malvéru CROCODILIS, ktorý sa špecializuje na exfiltráciu citlivých údajov a vzdialenú kontrolu infikovaných zariadení

2 FBI varuje pred aktivitami botnetu BADBOX 2.0

Americká FBI vydala varovanie pred aktivitami botnetu BADBOX 2.0, ktorý celosvetovo infikoval už vyše milión smart TV, streaming boxov, projektorov a IOT zariadení.

3 Dánsko nahrádza Microsoft Office a Windows open-source riešeniami pre zvýšenie digitálnej suverenity

Dánsko sa rozhodlo postupne nahradiť Microsoft Office a Windows open-source riešeniami ako LibreOffice a Linux, aby znížilo závislosť od amerických technologických firiem, zvýšilo digitálnu suverenitu a zlepšilo bezpečnosť.

4 Ruská APT29 obchádza dvojfaktorovú autentifikáciu v Gmaile pomocou ASP

Ruská APT29 (známa aj ako Cozy Bear) využila funkciu Application Specific Passwords (ASP) v Gmaile na obídenie dvojfaktorovej autentifikácie a získanie prístupu k e-mailovým účtom prominentných akademikov a kritikov Kremľa.

5 Kybernetická vojna medzi Iránom a Izraelom eskaluje

Hacktivistické skupiny vystupňovali aktivity v súvislosti s napätím medzi Iránom a Izraelom.

6 Výskumníci odhalili novú metódu pre obchádzanie obmedzení modelov AI

NeuralTrust odhalil nový typ útoku na veľké jazykové modely (LLM) s názvom Echo Chamber, ktorý využíva techniku zvanú context poisoning.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

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

Tento mesiac sa objavila netradičná phishingová kampaň zneužívajúca meno spoločnosti Allianz, ktorá sa v úvodnom e-maile snaží zaujať obeť ponukou sady auto-náradia, lekárničky, baterky a štartovacích káblov v cene 100 Eur zdarma za vyplnenie krátkeho dotazníka. Predmet e-mailov je v znení "O exkluzívnom darčeku od Allianzu" a jeho mutáciách. CSIRT.SK prijal hlásenia o prístupoch na podvodné URL obsiahnuté v e-mailoch. Tieto boli preverené.

Ďalšia podvodná kampaň sa zamerala na Sociálnu poisťovňu, ktorej meno zneužila pri zbere osobných údajov a údajov o platobnej karte. Obsah e-mailovej správy hovoril o nedoplatku na poistnom a obsahoval odkaz na phishingovú webstránku.

Tento mesiac sa CSIRT.SK v rámci phishingových hrozieb stretol aj so zneužitím mena Ministerstva vnútra SR. Kampaň šírila odkaz na falošnú webstránku ministerstva. Obete sa snažila presvedčiť, aby na ňu klikli, použitím zámienky o nezaplatenej pokute a hrozbou jej podstatného navýšenia v najbližších dňoch.

Júnovým phishingovým kampaniam sa nevyhla ani spoločnosť Slovnaft. Útočníci zneužili jej meno v e-mailoch s predmetom "Len dnes: 150 € paliva ZADARMO k vašej Slovnaft karte!". Nahlásené boli zaregistrované prístupy na škodlivú doménu z niekoľkých organizácií v konštituencii CSIRT.SK. Vládna jednotka o tom informovala zasiahnuté organizácie a dohliadla na preverenie účtov a zariadení, ktoré pristupovali k podvodnej stránke.

CSIRT.SK upozorňuje, že phishingové e-maily môžu byť nebezpečné aj pre používateľov s účtami s viacfaktorovou autentifikáciou (MFA). To sa stalo zamestnancovi organizácie v konštituencii VJ CSIRT, ktorému útočníci kompromitovali účet vďaka použitiu sady Tycoon 2FA pre vytvorenie svojej podvodnej kampane. Táto sada obsahuje nástroje pre tvorbu vierohodných phishingových stránok, aj na odchytávanie MFA. Po prístupe na podvodnú stránku a zadaní prihlasovacích údajov útočníci tieto okamžite zadávajú do reálnej webovej služby. Obeti tak obratom príde verifikácia MFA, ktorú útočníci odchytia, čím získajú prístup do cieľového účtu.

V júni identifikovala organizácia v konštituencii CSIRT.SK v prostredí svojho file-servera pozostatky po aktivite ransomvéru. Išlo o výsledné súbory šifrovania, ktoré navyše obsahovali tzv. ransomnote. Išlo o malý počet súborov a predpokladá sa, že vznikli v roku 2016. CSIRT.SK ponúkol súčinnosť pri vyšetrovaní predmetného incidentu a forenznej analýze dostupných digitálnych stôp. Organizácia celé prostredie preskenovala a aktuálne neeviduje aktívnu hrozbu, ani ďalšie súvisiace hrozby.

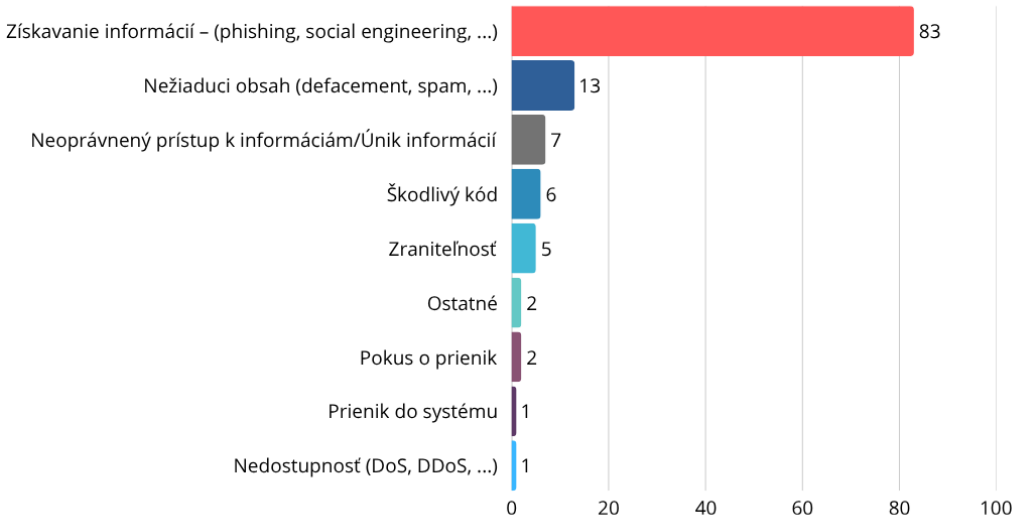
V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles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

V júni CSIRT.SK vydal na svojej webstránke návody ako používať a odhaľovať generatívnu AI. Určené sú najmä pre učiteľov pri práci so žiakmi a študentmi, no praktické rady v nich môže nájsť aj široká verejnosť.

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 máji jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Ministerstva školstva, výskumu, vývoja a mládeže Slovenskej republiky a študentov ZŠ Tupolevova v Bratislave.

Členovia tímu CSIRT.SK sa zúčastnili na konferenciách Poradca Podnikateľa- Školský zákon 2025 v Pribyline a Raabe- Učiteľ nie je Google 9 v Bratislave, na ktorých prezentovali svoje preventívne aktivity, najmä vzdelávanie študentov a učiteľov v oblasti kybernetickej bezpečnosti a svoje skúsenosti z prednášok.

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



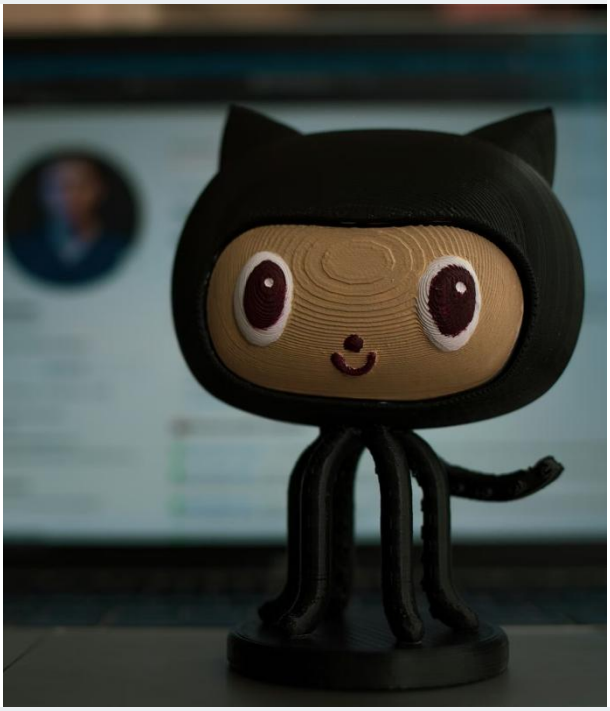
VÝZNAMNÉ UDALOSTI VO SVETE

Malvér CROCODILIS pre Android sa stal globálnou hrozbou

Bezpečnostní výskumníci z THREAT FABRIC zverejnili analýzu malvéru CROCODILIS pre Android, ktorý sa špecializuje na exfiltráciu citlivých údajov a vzdialenú kontrolu infikovaných zariadení. Jednoduchý malvér zachytený v malých kampaniach v Turecku sa vyvinul v celosvetovú hrozbu. Vývojári pridali ďalšie funkcionality pre maskovanie prítomnosti a sťaženie malvérovej analýzy a funkciu pre pridanie falošných kontaktov na zariadení, ktorá zvyšuje úspešnosť vishingových volaní.

Malwaretisementová kampaň na GITHUBe cieli na hráčov, výskumníkov a hackerov

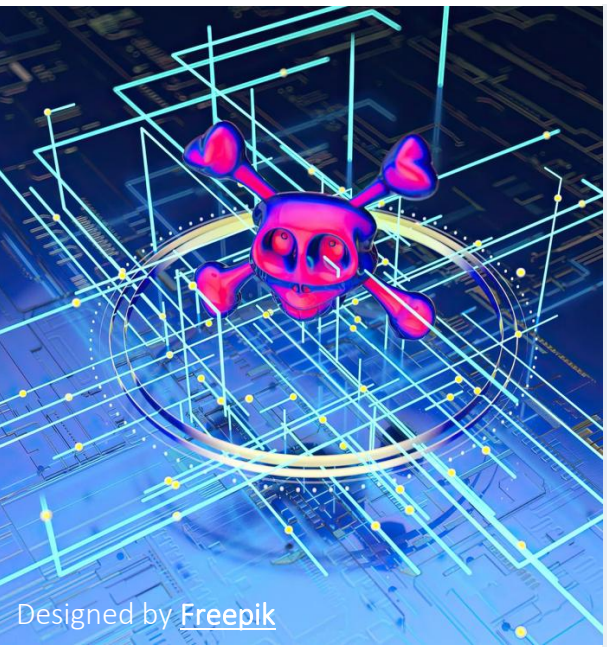
Bezpečnostní výskumníci zo spoločnosti SOPHOS zverejnili informácie o malwaretisementovej kampani cielenej na hráčsku komunitu, výskumníkov a hackerov, ktorá šíri malvér prostredníctvom exploitov, malvéru, botov a cheatov hostovaných na portáli GITHUB. Tieto projekty obsahujú skrytý kód na inštaláciu zadných vrátok umožňujúcich získanie vzdialenej kontroly nad zariadeniami alebo rôzne formy infostealerov. Útočníci na promovanie svojich repozitárov automatizovane zasielajú nové commity, čím zachovávajú dojem aktívne udržiavaného projektu. Samotné zadné vrátka majú rôzne formy, od pythonových skriptov, cez šetriče obrazovky, javascriptové súbory s payloadmi až po Visual Studio PreBuild eventy. Kampaň poukazuje na význam analýzy zdrojového kódu pred jeho prevzatím alebo spustením.



FBI varuje pred kryptopodvodmi na platforme HEDERA

Americká FBI varuje pred podvodmi zneužívajúcimi NFT airdropy HEDERA HASHGRAPH na krádež kryptomien. Útočníci do peňaženky obete zašlú NFT alebo tokeny so správami vyzývajúcimi na návštevu URL, ktoré presmerovávajú na phishingové stránky alebo dApps slúžiace na zber prihlasovacích údajov alebo seedov pre obnovu kryptopeňaženky. Na promovanie phishingového obsahu okrem airdropov zneužívajú aj phishingové e-maily, falošné webové stránky a reklamy na sociálnych sieťach. Vlastníci kryptomien by nikdy nemali zadávať seedy pre obnovu kryptopeňaženiek do webových stránok.

VÝZNAMNÉ UDALOSTI VO SVETE



FBI varuje pred aktivitami botnetu BADBOX 2.0

Americká FBI vydala varovanie pred aktivitami botnetu BADBOX 2.0, ktorý celosvetovo infikoval už vyše milión smart TV, streaming boxov, projektorov a IOT zariadení. Zariadenia sú infikované škodlivými aktualizáciami firmvéru alebo inštaláciou malvéru. Útočníci kompromitované zariadenia zneužívajú ako rezidenčné proxy na maskovanie svojich aktivít a obchádzanie bezpečnostných mechanizmov na báze geolokácie, klikanie na reklamy, získavanie a exfiltráciu citlivých údajov alebo prístupy k zariadeniam predávajú za účelom získania prístupu do korporátnych sietí za účelom realizácie ďalších útokov. BADBOX úspešne pokračuje vo svojich aktivitách napriek opakovaným operáciám zo strany OČTK.

Google ukončuje podporu koreňových certifikátov Chunghwa Telecom a Netlock

Spoločnosť GOOGLE s odvolaním sa na dlhodobé nedodržiavanie súladu oznámila ukončenie podpory koreňových CA certifikátov podpisaných spoločnosťami CHUNGHWA TELECOM a NETLOCK v rámci Chrome Root Store. Rozhodnutie nadobudne platnosť 1. augusta 2025. Jedná sa o prvé kroky vyplývajúce z nedodržania prísnejších kritérií pre spoluprácu s certifikačnými autoritami, ktoré Google oznámila v marci 2025. Chunghwa je najväčším telekomunikačným operátorom na Taiwane a Netlock významným poskytovateľom digitálnych podpisov v Maďarsku a štátoch EÚ. Prípadné obmedzenia možno v prípade nutnosti obísť manuálnym pridaním ich koreňových certifikátov do zoznamu lokálne dôveryhodných certifikátov.

Dánsko nahrádza Microsoft Office a Windows open-source riešeniami pre zvýšenie digitálnej suverenity

Dánsko sa rozhodlo postupne nahradiť Microsoft Office a Windows open-source riešeniami ako LibreOffice a Linux, aby znížilo závislosť od amerických technologických firiem, zvýšilo digitálnu suverenitu a zlepšilo bezpečnosť. Tento krok je motivovaný aj rastúcimi nákladmi na produkty Microsoftu a obavami z politického vplyvu na prístup k digitálnym službám. Hoci prechod bude náročný, chce takto získať väčšiu kontrolu nad digitálnou infraštruktúrou a podporiť európske open-source riešenia.

VÝZNAMNÉ UDALOSTI VO SVETE

Kybernetická vojna medzi Iránom a Izraelom eskaluje

Hacktivistické skupiny vystupňovali aktivity v súvislosti s napätím medzi Iránom a Izraelom. Izrael narušil vysielanie iránskej štátnej televízie a odvysielal výzvu na protesty proti režimu. Útočníci zároveň manipulujú so satelitným vysielaním, Zasiahnuté boli aj iránska banka a kryptoburza Novitex. Iránski hackeri kompromitujú izraelské IP kamery na špionáž a útočia na ciele kybernetickými prostriedkami.

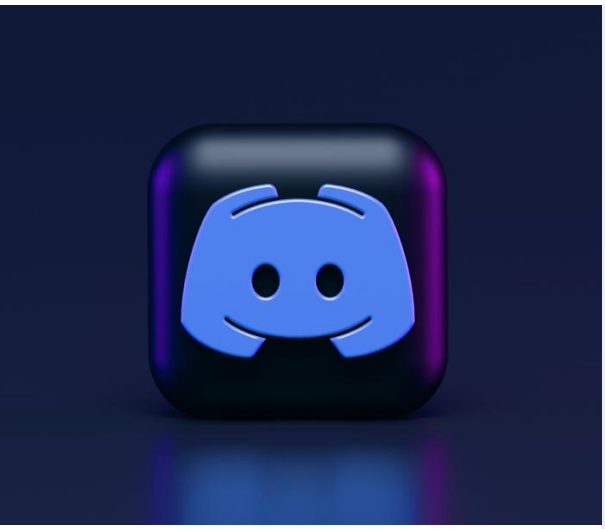
Skupiny vykonávajú najmä DDoS útoky, zmeny vzhľadu a obsahu webstránok a zverejňujú citlivé údaje. Niektoré z nich pohrozili útokmi na USA v prípade ich zapojenia do konfliktu. Až 35 proiránskych skupín cieli na izraelskú kritickú infraštruktúru, zatiaľ čo proizraelských skupín je aktívnych len 12. Proiránski aktéri využívajú sociálne inžinierstvo, dezinformácie, recyklujú staré úniky a vydávajú sa za pôvodcov nesúvisiacich incidentov.

Irán v reakcii na hrozbu kyberútokov obmedzil internetové pripojenie, varoval pred používaním WhatsAppu a podľa RADWARE stúpla aktivita na telegramových kanáloch proiránskych skupín. Izrael sa ocitá pod kybernetickým tlakom, zatiaľ čo USA cez víkend zbombardovali tri iránske zariadenia na obohacovanie. Kyberpriestor tak odráža geopolitické napätie – Irán sa izoluje, hacktivisti si volia strany a kyberútoky sa stávajú súčasťou širšieho konfliktu.

Výskumníci odhalili vyše 46 000 zraniteľných inštancii GRAFANA

Viac než 46 000 verejných inštancií platformy Grafana zostáva nezabezpečených a zraniteľných voči útokom, ktoré umožňujú prevzatie používateľských účtov. Zraniteľnosť CVE-2025-4123, bola opravená v aktualizácii vydanej 21. mája 2025. Napriek tomu viac než tretina všetkých verejne dostupných inštancií Grafana nebola aktualizovaná a stále je vystavená riziku. Útočníci môžu zneužiť túto zraniteľnosť na presmerovanie obetí na webstránky so škodlivými modulmi, ktoré umožňujú prevziať používateľské účty, získať prístup k citlivým údajom a potenciálne spustiť ďalšie škodlivé operácie. Odporúča sa, aby správcovia systémov bezokladne aplikovali dostupné bezpečnostné aktualizácie a zabezpečili svoje inštancie Grafana pred potenciálnymi útokmi.

VÝZNAMNÉ UDALOSTI VO SVETE

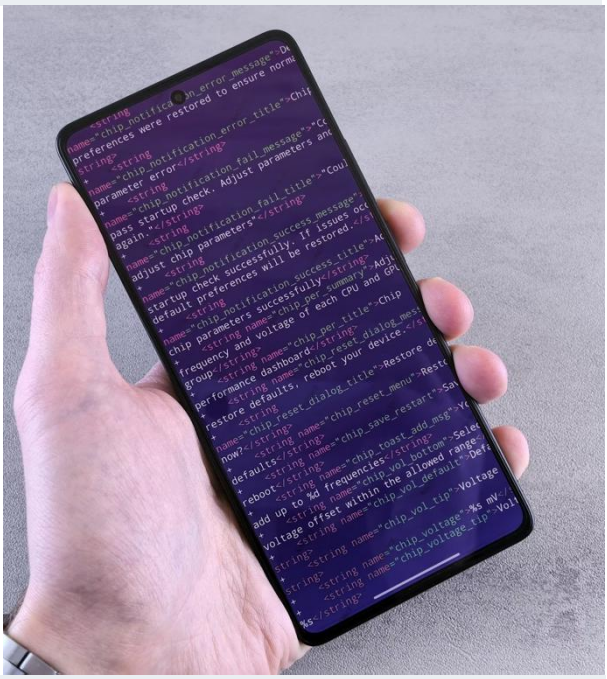


Útočníci šíria malvér cez Discord prostredníctvom recyklovaných pozvánok

Spoločnosť CHECK POINT RESEARCH odhalila sofistikovanú kampaň, kde útočníci zneužívajú chybu v Discordových pozvánkach, ktoré môžu byť znova použité po ich expirácii alebo odstránení. Používatelia sú presmerovaní na podvodné servery, kde falošný bot spúšťa skripty PowerShell na stiahnutie malvéru vrátane AsyncRAT a Skuld Stealer, zameraného na krádež údajov a kryptomenových peňaženiek. Kampaň zasiahla viac než 1 300 používateľov v USA, Európe a Ázii. Článok obsahuje indikátory kompromitácie (IOC).

Nová verzia malvéru Godfather pre Android spúšťa aplikácie vo virtualizovanom prostredí

Bezpečnostní výskumníci zo spoločnosti ZIMPERIUM ZLABS odhalili novú formu sofistikovaného útoku, ktorý predstavuje vážne riziko pre mobilné aplikácie – ide o bankový malvér GodFather, ktorý zneužíva technológiu virtualizácie priamo na zariadení. Zneužíva open-source VirtualApp na tvorbu virtualizovaného prostredia, v ktorom prostredníctvom StubActivity spúšťa záujmové aplikácie. Nástroj Xposed zneužíva na API hooking a získanie samotných dát. Tento prístup umožňuje malvéru obísť bežné bezpečnostné mechanizmy a detekciu, keďže väčšina škodlivého kódu sa presúva do aplikačnej vrstvy, čím sa znižuje pravdepodobnosť jeho odhalenia klasickou analýzou.



CLOUDFLARE mitigoval DDoS útok s rekordnou intenzitou 7,3 Tbps

Spoločnosť Cloudflare tvrdí, že v máji 2025 mitigovala rekordný útok typu distributed denial of service (DDoS, odmietnutie služby), ktorý zasiahol hostingového poskytovateľa a v maxime dosiahol až 7,3 terabitu za sekundu (Tbps). Útok trval iba 45 sekúnd a spôsobil prenos približne 37,4 terabajtov dát – čo zodpovedá približne 7 500 hodinám HD streamovania alebo 12,5 milióna fotografií vo vysokom rozlíšení. Útočníci využili viac ako 122 000 zdrojových IP adries z 161 krajín, prevažne z Brazílie, Vietnamu, Taiwanu, Číny, Indonézie a Ukrajiny. Útok zahŕňal UDP flooding a techniky odrazu a amplifikácie, ktoré rozptýlili prevádzku na viac ako 34 000 portov za sekundu, čím sa predišlo detekcii a efektívne preťažil brány firewall a IDS systémy. Indikátory kompromitácie (IOC) boli zdieľané prostredníctvom IOC BOTNET THREAT FEED.

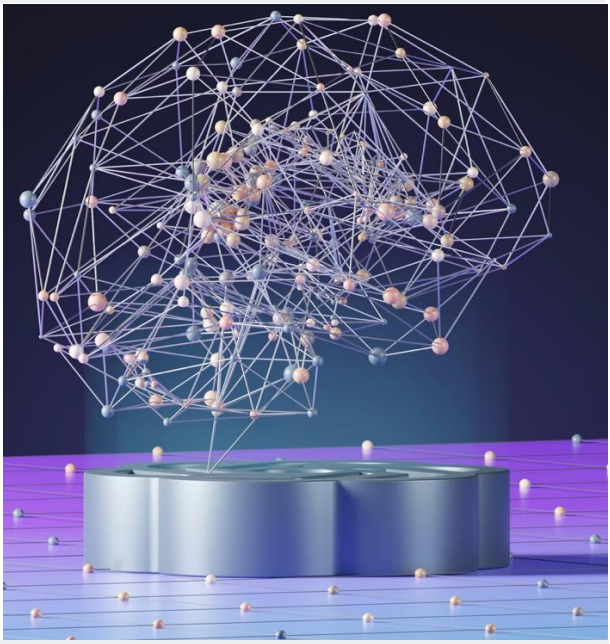
VÝZNAMNÉ UDALOSTI VO SVETE

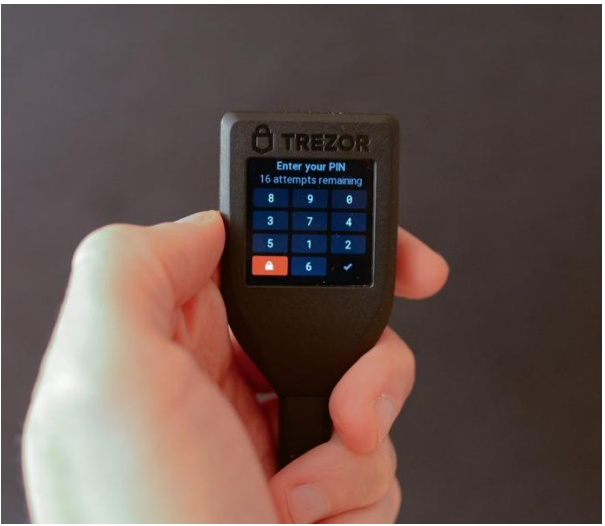
Ruská APT29 obchádza dvojfaktorovú autentifikáciu v Gmaile pomocou ASP

Ruská APT29 (známa aj ako Cozy Bear) využila funkciu Application Specific Passwords (ASP) v Gmaile na obídenie dvojfaktorovej autentifikácie a získanie prístupu k e-mailovým účtom prominentných akademikov a kritikov Kremľa. Útok začal falošnými e-mailovými pozvánkami, ktoré sa tvárili ako oficiálne správy od amerického ministerstva zahraničných vecí. Cieľom bolo presvedčiť obete, aby vytvorili 16 miestne heslo ASP, ktoré následne zdieľali s útočníkmi, čím im umožnili trvalý prístup ku svojim e-mailom. Útok bol starostlivo naplánovaný a prebiehal niekoľko týždňov, pričom útočníci pôsobili ako technická podpora, aby získali dôveru obetí. Google identifikoval túto aktivitu ako UNC6293 a potvrdil, že ide o operáciu spojenú so skupinou APT29. Spoločnosť následne prijala opatrenia na zabezpečenie kompromitovaných účtov a odporučila používateľom, aby využívali program Advanced Protection pre zvýšenú bezpečnosť.

Výskumníci odhalili novú metódu pre obchádzanie obmedzení AI modelov

NeuralTrust odhalil nový typ útoku na veľké jazykové modely (LLM) s názvom Echo Chamber, ktorý využíva techniku zvanú context poisoning. Na rozdiel od tradičných útokov, ktoré sa spoliehajú na priame škodlivé príkazy, tento útok postupne manipuluje interným kontextom modelu cez nepriame narážky a sémantické navádzanie v priebehu viacerých interakcií. Útok dosiahol úspešnosť nad 90 % v kategóriách ako násilie, nenávisť, pornografia a dezinformácie, pričom zistil slabiny v súčasných bezpečnostných mechanizmoch LLM. NeuralTrust odporúča implementovať dynamické skenovanie konverzačného kontextu a detekciu nepriameho navádzania ako prostriedky na ochranu pred takýmito útokmi.





Phishingová kampaň zneužívajúca systém zákazníckej podpory TREZOR

Útočníci zneužívajú systém zákazníckej podpory hardvérovej kryptopeňaženky a manažéra hesiel TREZOR na rozposielanie phishingu. Systém umožňuje vytvoriť tiket pod ľubovoľným e-mailom, na ktorý je zaslaná automatická odpoveď s predmetom zhodným s popisom tiketu. Phishingové stránky slúžia na získavanie seedov pre prístup k peňaženke.

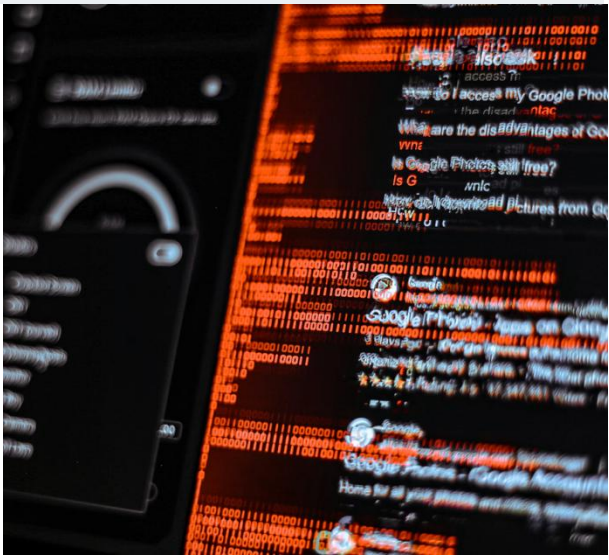
VÝZNAMNÉ UDALOSTI VO SVETE

Phishingová kampaň zneužívajúca funkcionalitu Microsoft 365 Direct Send

Útočníci na rozosielanie phishingového obsahu zneužívajú službu Direct Send, ktorá predstavuje menej známu súčasť Microsoft 365. Táto služba umožňuje lokálnym zariadeniam, aplikáciám a cloudovým službám zapojeným do domény odosielať e-maily cez smart host tenanta company-com.mail.protection.outlook.com. Pri nesprávnej konfigurácii ju môžu útočníci prostredníctvom jednoduchého príkazu PowerShell zneužiť na rozosielanie e-mailov. Spoločnosť Microsoft odporúča používať Direct Send len pokročilým používateľom, ktorí dokážu infraštruktúru dostatočne zabezpečiť a správne nakonfigurovať. Článok v odkaze obsahuje indikátory kompromitácie (IOC).

Nový variant útoku ClickFix zneužíva File Explorer na spustenie škodlivého kódu

Výskumníci vytvorili nový variant útoku ClickFix s označením FILEFIX, ktorý na spustenie škodlivého kódu zneužíva odkazy v lište File Explorera. File Explorer dokáže vykonávať príkazy operačného systému. Obeť je informovaná, že s ňou bol zdieľaný súbor a za účelom prístupu je potrebné skopírovať odkaz do File Explorera. Nakoľko obeť nie je vyzvaná na spustenie CMD, ktoré je samo o sebe podozrivé, zvyšuje sa pravdepodobnosť úspechu útoku.



VÝZNAMNÉ UDALOSTI VO SVETE

- Bezpečnostní výskumníci z RELIAQUEST zverejnili analýzu kyberkriminálneho fóra RUSSIAN MARKET, ktorý je v súčasnosti jedným z najpopulárnejších fór pre obchodovanie s prihlasovacími údajmi z infostealerov.

- Kyberkampaň Phantom Enigma šíri škodlivé skripty cez phishingové e-maily s falošnými faktúrami. Útočníci inštalujú škodlivé rozšírenia do prehliadačov, ktoré kradnú autentifikačné tokeny a obchádzajú dvojfaktorovú autentifikáciu.

- Bezpečnostní výskumníci z AIKIDO SECURITY zverejnili informácie o útoku na dodávateľský reťazec na NPM knižnice GLUESTACK @REACT-NATIVE-ARIA.

- Spoločnosť PROOFPOINT zverejnila informácie o aktivitách hackerskej skupiny UNK_SNEAKYSTRIKE, ktoré súvisia so zneužitím platformy pre penetračné testovanie TEAMFILTRATION na útoky na viac ako 80 000 používateľských účtov Microsoft Entra ID.

- Proizraelská hackerská skupina Gonjeshke Darande (Predatory Sparrow) napadla 18. júna 2025 iránsku kryptozmenáreň Nobitex a previedla z nej približne 90 miliónov USD v kryptomenách.

- Spoločnosť VIASAT sa stala obeťou kyberšpionážnej skupiny Salt Typhoon, ktorá je napojená na čínsku vládu.

- Neznámi útočníci cielili na verejne prístupné servery Microsoft Exchange, aby cez prihlasovacie stránky vkladali škodlivý JavaScriptový kód, ktorý zaznamenával stlačené klávesy používateľov a kradli ich prihlasovacie údaje.

- Ruská skupina APT28 (Fancy Bear) nasadila voči ukrajinským vládnym cieľom novú vlnu malvéru. Cez zabezpečené správy v aplikácii Signal distribuovala infikované dokumenty s makrami (Акт.doc), ktoré inštalovali backdoor Covenant.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívané kritické zraniteľnosti v platforme vBulletin

Bezpečnostní výskumníci zverejnili informácie o aktívne zneužívaných kritických zraniteľnostiach v redakčnom systéme pre tvorbu online fór vBulletin. CVE-2025-48827 a CVE-2025-48828 by vzdialený neautentifikovaný útočník mohol zneužiť na volanie chránených metód a vzdialené vykonanie kódu.

Kritická zraniteľnosť v produkte Hewlett Packard Enterprise StoreOnce

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie svojho riešenia pre deduplikáciu, zálohovanie a obnovu dát StoreOnce, ktoré opravujú 8 zraniteľností. Jedna z nich je označená ako kritická. CVE-2025-37093 možno zneužiť na obídenie mechanizmov autentifikácie a získanie úplnej kontroly nad systémom.

Aktívne zneužívaná zero-day zraniteľnosť v prehliadači Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj webový prehliadač Chrome, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť. CVE-2025-5419 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

Aktívne zneužívaná kritická zraniteľnosť v open-source webmailovom riešení RoundCube

Vývojári populárnej webmailovej platformy Roundcube vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2025-49113 by vzdialený útočník mohol zneužiť na vzdialené vykonanie kódu zaslaním špeciálne vytvorenej požiadavky HTTP GET.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Vysoko závažné zraniteľnosti v produkte Ivanti Workspace Control

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 3 vysoko závažné zraniteľnosti v produkte pre centralizovaný manažment zariadení a aplikácií Ivanti Workspace Control. Zraniteľnosti možno zneužiť na získanie prihlasovacích údajov uložených v aplikácii a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Kritické bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty InCopy, Experience Manager, Commerce, InDesign, Substance 3D Sampler, Acrobat Reader a Substance 3D Painter, ktoré opravujú 252 zraniteľností, z čoho 18 je označených ako kritických. Kritické zraniteľnosti by vzdialený útočník mohol zneužiť na obídenie bezpečnostných prvkov, eskaláciu privilégií a vykonanie kódu.

Kritické zraniteľnosti v Trend Micro Apex Central a Endpoint Encryption PolicyServer

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viaceré kritické bezpečnostné zraniteľnosti. CVE-2025-49219 a CVE-2025-49220 v Apex Central možno zneužiť na vzdialené vykonanie kódu. CVE-2025-49216, CVE-2025-49212, CVE-2025-49213 a CVE-2025-49217 v Endpoint Encryption PolicyServer možno zneužiť na získanie neoprávneného prístupu do systému a vykonanie kódu.

Zraniteľnosti v OS Apple boli zneužité na inštaláciu špionážneho softvéru

Spoločnosť Apple vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zraniteľnosť v operačných systémoch iOS a iPadOS. Zraniteľnosť CVE-2025-24200 by útočník s fyzickým prístupom k uzamknutým zariadeniam mohol zneužiť na deaktiváciu USB Restricted Mode. Spoločnosť doplnila aktualizácie aj o zero-click zraniteľnosť CVE-2025-43200. Zraniteľnosť bola podľa analýzy zneužitá na inštaláciu špionážneho softvéru Graphite. Kompromitované mali byť mobilné zariadenia viacerých novinárov v Európe.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická a stredne závažné zraniteľnosti Cisco ISE a CCP s verejným exploitom

Bezpečnostní Spoločnosť Cisco vydala bezpečnostné aktualizácie na produkty Identity Services Engine a Customer Collaboration Platform, ktoré opravujú viaceré bezpečnostné zraniteľnosti, pre ktoré existuje verejne dostupný kód exploitu. Tieto zraniteľnosti možno zneužiť na získanie neoprávneného prístupu do systému, vykonanie administratívnych zmien, nahrávanie súborov, či získanie citlivých údajov.

Vysoko závažná zraniteľnosť v ASUS Armoury Crate

Spoločnosť ASUS vydala bezpečnostné aktualizácie svojho softvéru pre manažment systému Armoury Crate, ktoré opravujú vysoko závažnú zraniteľnosť. Zraniteľnosť s identifikátorom CVE-2025-3464 možno zneužiť na eskaláciu privilégií a získanie administrátorského prístupu k systému.

Kritická zraniteľnosť v produkte Veeam Backup & Replication

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoj produkt Backup & Replication, ktoré opravujú 2 zraniteľnosti, z ktorých jedna je označená ako kritická. CVE-2025-23121 by vzdialený autentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

Kritické zraniteľnosti v Citrix NetScaler ADC a NetScaler Gateway

Spoločnosť Citrix vydala bezpečnostné aktualizácie na svoje produkty NetScaler ADC a NetScaler Gateway, ktoré opravujú 2 zraniteľnosti, z ktorých 1 je označená ako kritická. CVE-2025-5777 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti v Cisco ISE a ISE-PIC umožňujú vzdialené vykonanie príkazov

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre produkty Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC), ktoré opravujú dve kritické bezpečnostné zraniteľnosti. CVE-2025-20281 a CVE-2025-20282 by útočník mohol zneužiť na vzdialené vykonanie kódu v mene používateľa root a získanie úplnej kontroly nad systémom.

Zraniteľnosť v inštalátore Notepad++ možno zneužiť na eskaláciu privilégií

Vývojári populárneho textového editora Notepad++ vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v inštalátore. CVE-2025-49144 možno lokálne zneužiť na eskaláciu privilégií na úroveň SYSTEM a vykonanie kódu.

Zraniteľnosť vo WinRAR umožňuje vzdialené vykonanie kódu

Spoločnosť RARLAB vydala bezpečnostné aktualizácie svojho komprimačného nástroja WinRAR, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-6218 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

MESAČNÍK ZRANITEĽNOSTÍ JÚN 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://www.csirt.sk/posts/2503.html