CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

MÁJ 2025

TLP: CLEAR

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

1 Skype v máji skončil

Spoločnosť MICROSOFT 5. mája 2025 po 14 rokoch fungovania oficiálne ukončila prevádzku komunikačnej platformy SKYPE, ktorú nahradila aplikácia MS TEAMS.

2 Phishingová kampaň FreeDrain kradne kryptomeny cez tisíce falošných stránok a AI obsah

Bezpečnostní výskumníci odhalili phishingovú kampaň FreeDrain, ktorá od roku 2022 využíva vyše 38 000 subdomén na bezplatných hostingových službách na krádež kryptomien.

3 ENISA spustila databázu bezpečnostných zraniteľností

Európska agentúra pre kybernetickú bezpečnosť (ENISA) oficiálne spustila Európsku databázu zraniteľností (EUVD), ktorá je kľúčovým nástrojom na posilnenie kybernetickej bezpečnosti v rámci EÚ.

4 Trójsky kôň v balíku PyPI

Výskumníci zo spoločnosti SOCKET odhalili škodlivý balík PyPI s názvom discordpydebug, ktorý bol prezentovaný ako nástroj na zaznamenávanie chýb pre vývojárov botov pre Discord.

5 Ransomvérová skupina VANHELSING zverejnila zdrojový kód časti svojich nástrojov

Ransomware-as-a-service skupina VANHELSING zverejnila zdrojový kód affiliate panela, leakpage a buildera pre šifrovače pre Windows.

6 Ruská APT28 zneužívala nedostatočne zabezpečené IP kamery v SR na špionáž

Autority kybernetickej bezpečnosti viacerých štátov zverejnili analýzu aktivít ruskej štátom sponzorovanej skupiny APT28, ktorej cieľom bola špionáž a narušenie činnosti štátov podporujúcich Ukrajinu.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci máj 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 prijal hlásenie podvodnej telefonickej a e-mailovej komunikácie. Nahlasovateľa kontaktovala telefonicky žena s ruským/ukrajinským prízvukom z slovenského čísla a tvrdila mu, že má nárok na vyplatenie 9500€. O niekoľko dní ho kontaktovala iná osoba s podobným prízvukom, a následne aj formou e-mailovej komunikácie z gmailovej adresy (údajne z firmy „Kriptosit“). E-mail obsahoval odkaz na stiahnutie. Gmail správne vyhodnotil túto správu ako phishing a zaradil ju do spamu. Vzorku e-mailu, resp. daný prípad sme po analýze vyhodnotili ako určitý druh ransomwaru, ktorý po stiahnutí nainštaluje nástroj na ovládanie vzdialenej plochy a útočník tak môže prevziať kontrolu nad zariadením obete. Následne môže vyžadovať výkupné za odblokovanie prístupu k zariadeniu. Oznamovateľovi sme poskytli odporúčania aké nevyhnutné kroky je potrebné vykonať v rôznych prípadoch interakcie s takýmto obsahom.

V máji sa odohral tiež medializovaný incident týkajúci sa nedostupnosti služieb ZSSK. Monitorovací systém CSIRT.SK zaregistroval cca 3-hodinový výpadok portálu ZSSK. Poskytovateľ služby v rámci nadviazanej komunikácie informoval CSIRT.SK, že sa jednalo o prevádzkový incident zapríčinený výpadkom technologických zariadení v správe Železničných telekomunikácii a Železničnej spoločnosti Slovensko. Služby boli obnovené cca 4 hodiny po výpadku do plnej funkčnosti.

Výpadok služieb zapríčinený skutočným kybernetickým útokom zaznamenali v máji viaceré štátne organizácie. Rozsiahly DDoS útok mal netradičnú formu veľkého množstva odosielaných e-mailov z botnetu, pričom falšoval identitu cieľových organizácií (e-mail bombing). Tento bol následne zamedzený zo strany organizácií pravidlom kontrolujúcim SPF záznam.

CSIRT.SK sa v máji zaoberal tiež prítomnosťou podozrivých aplikácií na koncových zariadeniach organizácie v jeho konštituencii. Vyžiadali sme si vzorku škodlivého obsahu a poskytli vyžiadané odporúčania, akým spôsobom odobrať vzorku infikovaného súboru „na diaľku“, pokiaľ je daný používateľ na vzdialenej lokalite.

Bezpečnostný monitoring CSIRT.SK zaregistroval prítomnosť modifikovaných registrov na pracovnej stanici tej istej organizácie. Pri každom prihlásení používateľa sa automaticky spúšťal neznámy skript. Tento sa pripájal na podozrivú URL. Organizácia vykonala odporúčané opatrenia a poskytla vzorky. Poskytnuté súbory sme podrobili malvérovej analýze a výsledky poskytli zasiahnutej organizácii s informáciami a odporúčaniami k už dohodnutému procesu reinštalácie. Súčasne sme odporučili preventívne skontrolovať z logov aktivitu daného stroja/konta, či nedošlo k úniku dát, prípadne obdobnej nezvyčajnej aktivite.

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.

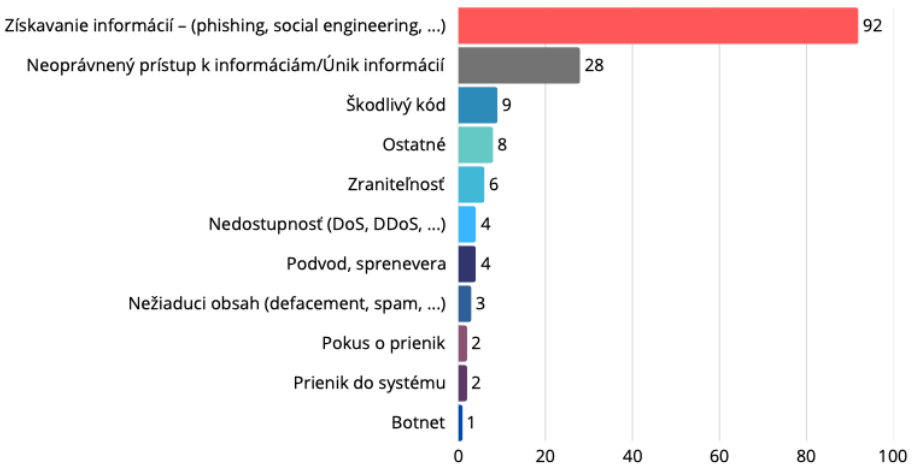
V máji CSIRT.SK plošne varoval svoju konštituenciu ohľadom aktívneho zneužívania slabo zabezpečených IP kamier ruskou štátom sponzorovanou skupinou APT28. Podľa reportu americkej agentúry CISA sa jednalo aj o kamery v kybernetickom priestore Slovenskej republiky. Útok cieli nielen na kamery priamo prístupné na internete, ale aj na kamery nepriamo dostupné prostredníctvom nesprávne nakonfigurovaných routerov, firewallov a média serverov. Útočníci zneužívajú prístup ku kamerám na špionáž a sledovanie verejných priestranstiev, obzvlášť v spojení s prepravou (letiská, železničné stanice, prístavy a pod) alebo pohraničnými oblasťami. Okrem zaslania varovania sme súčasne spustili skenovanie otvorených portov na organizácie v našej konštituencii.

Jednotka CSIRT.SK informovala zasiahnuté organizácie o potenciálne kompromitovaných používateľských kontách. Jednalo sa o uniknuté údaje z databázy HIBP, ktorá bola v máji obohatená o nové dáta. V tejto súvislosti sme organizácie požiadali, aby predmetnú informáciu prešetrili a vykonali opatrenia nevyhnutné pre mitigáciu potenciálnej kompromitácie.

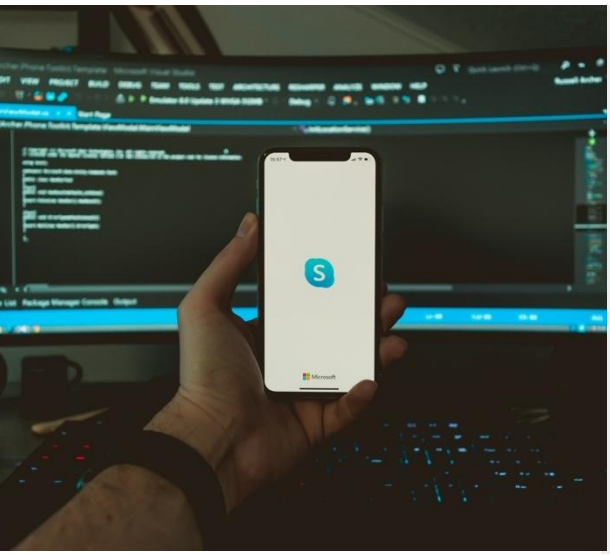
CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných škôl. V máji jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre študentov SOŠ automobilovej, SOŠ Ostrovského a SOŠ beauty služieb v Košiciach, Obchodnej akadémie a Strednej zdravotníckej školy v Považskej Bystrici, Strednej zdravotníckej školy v Nitre, SOŠ obchodu a služieb v Sobranciach a Gymnázia Komenského 32 v Trebišove.

Členovia tímu CSIRT.SK sa zúčastnili na medzinárodnej konferencii 74th TF-CSIRT meeting v Oslo pod záštitou organizácie TF-CSIRT, kde si prevzali dokument k úspešnej medzinárodnej certifikácii VJ CSIRT „SIM3 Trusted introducer – certified“.

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



VÝZNAMNÉ UDALOSTI VO SVETE



Skype v máji skončil

Spoločnosť MICROSOFT 5. mája 2025 po 14 rokoch fungovania oficiálne ukončila prevádzku komunikačnej platformy SKYPE, ktorá bola nahradená aplikáciou MS TEAMS. Používatelia platformy mali od februára 2025 60 dní na migráciu dát do prostredia MS Teams a počas tohto obdobia bolo možné komunikovať medzi platformami navzájom.

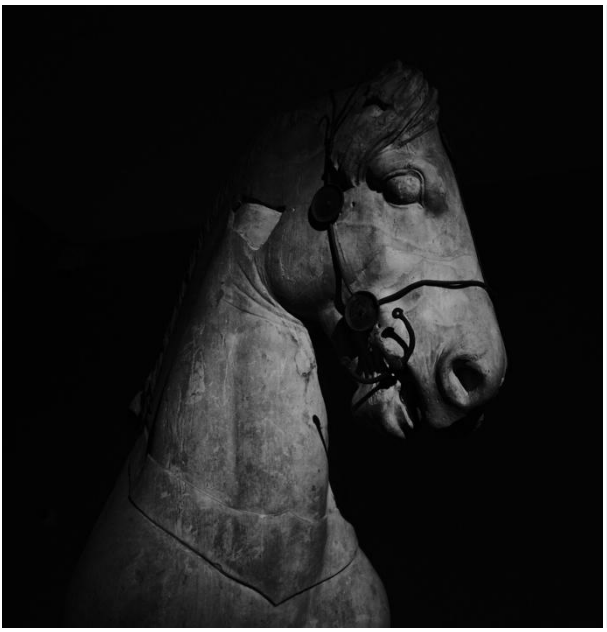
Supply chain útok prostredníctvom kompromitovaných modulov redakčného systému Magento

V apríli 2025 útočníci kompromitovali stovky e-shopov bežiacich na platforme Magento. Aktivovali škodlivý kód vložený do 21 rozšírení od vývojárov Tigren, Ameetanshi a MGS. Tieto backdoory boli do rozšírení implantované už v roku 2019, no aktivované boli až po šiestich rokoch, čo útočníkom umožnilo získať plnú kontrolu nad napadnutými servermi. Ide o formu supply chain útoku. Sansec zároveň identifikoval aj podozrivú verziu rozšírenia Weltpixel GoogleTagManager, hoci nie je jasné, či bola kompromitácia na strane vývojára alebo konkrétneho webu. Prevádzkovatelia online obchodov na báze redakčného systému MAGENTO by mali overiť či nepoužívajú uvedené pluginy. V prípade, že áno, odinštalovať ich, vykonať kontrolu integrity CMS, preventívnu zmenu hesiel a kryptografického materiálu.

Phishingová kampaň FreeDrain kradne kryptomeny cez tisíce falošných stránok a AI obsah

Bezpečnostní výskumníci odhalili phishingovú kampaň FreeDrain, ktorá od roku 2022 využíva vyše 38 000 subdomén na bezplatných hostingových službách na krádež kryptomien. Falošné stránky napodobňujú legitímne peňaženky a cez SEO manipuláciu lákajú obete na zadanie seed frázy, čím útočníci získajú prístup k ich kryptomenám. Kampaň využíva aj generatívnu AI na tvorbu obsahu. Článok obsahuje Indikátory kompromitácie (IOC).

VÝZNAMNÉ UDALOSTI VO SVETE

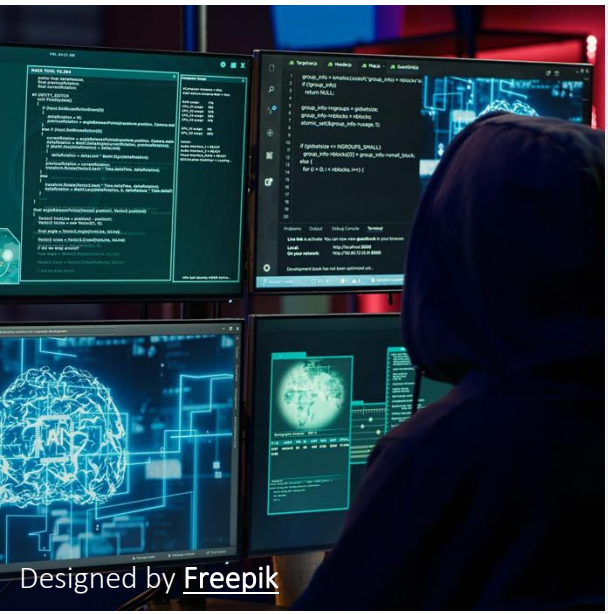


Trójsky kôň v PyPI balíku

Výskumníci zo spoločnosti SOCKET odhalili škodlivý balík PyPI s názvom discordpydebug, ktorý bol prezentovaný ako nástroj na zaznamenávanie chýb pre vývojárov Discord botov. V skutočnosti však obsahoval plne funkčný vzdialený prístupový trójsky kôň (RAT), ktorý umožňoval útočníkom vykonávať príkazy na napadnutých systémoch a exfiltrovať údaje. Balík bol nahraný 21. marca 2022 a dosiahol viac ako 11 000 stiahnutí, čím ohrozil tisíce vývojárskych systémov. Útočníci zneužili dôveru vývojárov v open-source komunite a nedostatočné bezpečnostné kontroly na PyPI, pričom sa vydávali za užitočných členov komunity a propagovali tento balík ako nástroj na ladenie chýb. Článok obsahuje indikátory kompromitácie (IOC) a taktiky, techniky a postupy (TTP).

Čínska skupina CHAYA_004 zneužíva kritickú zero-day zraniteľnosť v SAP NetWeaver

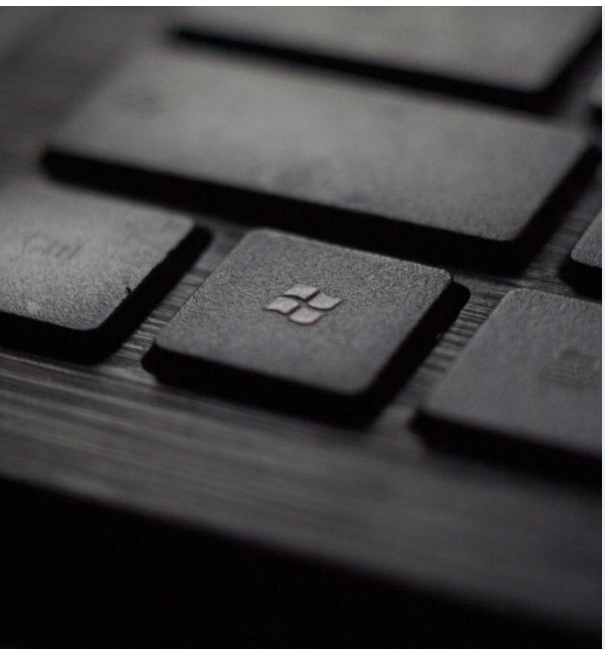
Bezpečnostní výskumníci z FORESCOUT VEDERE LABS pripisujú nedávne útoky zamerané na zneužitie kritickej zraniteľnosti v SAP NETWEAVER čínskej skupine CHAYA_004. Útoky boli vedené z IP adries so self-signed certifikátom napodobňujúcim Cloudflare, ktoré patrili prevažne čínskym poskytovateľom, a v rámci útokov bol použitý reverzný shell SUPERSHELL vyvinutý čínskymi aktérmi. CVE-2025-31324 bolo možné zneužiť na nahratie ľubovoľných súborov a získanie úplnej kontroly nad zariadením. Podľa výskumníkov z MADIANT bola zraniteľnosť zneužívaná ako zero-day minimálne od polovice marca 2025 a honeypot spoločnosti ONAPSIS zachytil prvé pokusy o jej zneužitie už 10. februára 2025. SHADOWSERVER identifikoval viacero kompromitovaných inštancií po celom svete. Články obsahujú Indikátory kompromitácie (IOC).



OČTK rozložili botnet, ktorý bol základom proxy služieb 5SOCKS a ANYPROXY

Orgány činné v trestnom konaní v spolupráci s bezpečnostnými výskumníkmi v rámci medzinárodnej akcie OPERATION MOONLANDER rozložili botnet, ktorý tvoril základ rezidenčných proxy služieb 5SOCKS a ANYPROXY. V rámci operácie Ministerstvo spravodlivosti USA obžalovalo štyroch prevádzkovateľov uvedených platforiem, troch ruskej a jedného kazašskej národnosti. Platformy boli v prevádzke už od roku 2004. Článok od LUMEN obsahuje aj indikátory kompromitácie (IOC).

VÝZNAMNÉ UDALOSTI VO SVETE



Spoločnosť Microsoft ukončí poskytovanie technickej podpory operačného systému WINDOWS 10

14. októbra 2025 MICROSOFT ukončí poskytovanie technickej podpory operačného systému WINDOWS 10. Spoločnosť v tejto súvislosti upustila od zámeru, že súčasne ukončí aj podporu MICROSOFT 365 pre Windows 10 a predĺžila ju o 3 ďalšie roky. Napriek tomuto ústretovému kroku výrobca odporúča migráciu na Windows 11. Podľa globálnych ukazovateľov služby STATCOUNTER má Windows 10 napriek blížiacemu sa dátumu ukončenia podpory stále 52-percentné zastúpenie. **VJ CSIRT na to upozorňuje v rámci pravidelného vydávania** prehľadu kritických zraniteľností.

ENISA spustila európsku databázu bezpečnostných zraniteľnosti

Európska agentúra pre kybernetickú bezpečnosť (ENISA) oficiálne spustila Európsku databázu zraniteľností (EUVD), ktorá je kľúčovým nástrojom na posilnenie kybernetickej bezpečnosti v rámci EÚ. Táto iniciatíva vychádza z požiadaviek smernice NIS2 a poskytuje centralizovaný prístup k spoľahlivým a praktickým informáciám o zraniteľnostiach v oblasti IT, OT a IoT systémov, vrátane údajov o ich zneužívaní a odporúčaných opatreniach na zmiernenie rizík. Databáza ponúka tri hlavné prehľady: kritické zraniteľnosti, zneužívané zraniteľnosti a zraniteľnosti koordinované v rámci EÚ. Cieľom EUVD je zvýšiť transparentnosť a efektivitu v oblasti správy zraniteľností, čím podporuje kybernetickú odolnosť verejného aj súkromného sektora v EÚ.

Ransomvérové a APT skupiny aktívne zneužívajú zraniteľnosti v SAP NetWeaver

Bezpečnostní výskumníci v rámci analýzy útokov zameriavajúcich sa na zneužitie zraniteľnosti v SAP NetWeaver začínajú vykonávať atribúciu útokov. ReliaQuest zachytila zapojenie ransomvérových skupín RansomEXX a BianLian, ktoré webshelly zneužili na šírenie malvéru. RansomEXX šíril backdoor PIPEMAGIC, ktorý zneužíva zraniteľnosť CVE-2025-29824 v komponente Windows CLFS. Forescout zaznamenal útoky asociované s čínskou skupinou CHAYA_004 a EclecticIQ útoky asociuje s aktivitami viacerých čínskych APT skupín. Poukazuje to na závažnosť uvedených zraniteľností a narastajúci záujem rôznych typov útočníkov o zneužitie zraniteľnosti. Články obsahujú indikátory kompromitácie (IOC).

VÝZNAMNÉ UDALOSTI VO SVETE

APT28 zneužíva zraniteľnosti webmailových platforiem na cielenú kyberšpionáž vládnych e-mailových serverov

Ruská štátom sponzorovaná skupina APT28 (známa aj ako Fancy Bear) využila zraniteľnosť typu zero-day v systéme MDaemon na vykonanie kyberšpionážneho útoku proti vládnym webmailovým serverom. Tento útok, označený ako Operation RoundPress, zahŕňal zneužitie zraniteľností typu XSS v rôznych webmailových platformách vrátane MDaemon, Horde, Roundcube a Zimbra. Cieľom útoku bolo získanie citlivých údajov z konkrétnych e-mailových účtov. Útočníci využili zraniteľnosť v MDaemon označenú ako CVE-2024-11182, ktorá bola opravená až v novembri 2024. Úspešné zneužitie tejto zraniteľnosti umožnilo spustenie škodlivého JavaScriptového kódu nazvaného SpyPress, ktorý mal schopnosť kradnúť prihlasovacie údaje a e-maily obetí.

Útočníci šíria malvér prostredníctvom trojanizovanej verzie aplikácie KeePass

Bezpečnostní výskumníci zo spoločnosti WITHSECURE zverejnili informácie o malwaretisement kampani, v rámci ktorej útočníci zneužívali trojanizované verzie manažéra hesiel KEEPASS na inštaláciu Cobalt Strike, exfiltráciu citlivých údajov a nasadenie ransomvéru. Škodlivé inštalátory útočníci promovali prostredníctvom reklám na portáli Bing. Útočníci zmodifikovali open-source kód aplikácie, ktorý doplnili o škodlivé funkcie KeeLoader, pričom bola zachovaná pôvodná funkcionalita produktu. Výskumníci aktivitu atribuujú hackerskej skupine UNC4696, ktorej aktivity sú asociované aj s ransomvérom BLACKAT a ALPHV. Incident poukazuje na mimoriadne nebezpečenstvo zneužitia platených reklám, ktorými možno škodlivé produkty dostať na popredné výsledky internetových vyhľadávačov. Používatelia by produkty mali vždy sťahovať len z oficiálnych webových stránok výrobcov.

Ransomvérová skupina VanHelsing zverejnila zdrojový kód časti svojich nástrojov

Ransomware-as-a-service skupina VanHelsing zverejnila zdrojový kód affiliate panela, leakpage a buildera pre šifrovače pre Windows. Vzhľadom na to, že sa jeden zo starých členov skupiny snažil o ich predaj na hackerskom fóre RAMP, skupina sa rozhodla pre ich zverejnenie. VanHelsing je aktívna od marca 2025 a využíva šifrovače pre platformy Linux, BSD, ARM a ESXi. Bezpečnostní výskumníci sa pustili do analýzy zverejneného kódu, ktorá môže viesť k ďalším zisteniam o infraštruktúre a moduse operandi skupiny.

VÝZNAMNÉ UDALOSTI VO SVETE

Ruská skupina APT28 zneužívala nedostatočne zabezpečené IP kamery v SR na špionáž

Autority kybernetickej bezpečnosti štátov zverejnili analýzu aktivít ruskej štátom sponzorovanej skupiny APT28, ktorých cieľom bola špionáž a narušenie činnosti štátov podporujúcich Ukrajinu. Analýza skúma aktivity od roku 2022, cielené spear-phishingové kampane, zneužívané zraniteľnosti, nástroje a malvér. Špecifikom je časť venovaná špionáži prostredníctvom IP kamier na Ukrajine a pohraničných oblastiach. V tejto súvislosti sú špecificky spomínané kamery na strategických miestach v SR. **VJ CSIRT preverila IP kamery a RTSP servery v rámci svojej konštituencie a rozposlala adresné varovania.**

Zásah proti kyberkriminalite na darknete

Europol, polícia a spoločnosti pôsobiace v oblasti kybernetickej bezpečnosti v rámci medzinárodnej akcie zaistili vyše 2300 domén asociovaných s činnosťou malware-as-a-service služby LUMMA, čím zasiahli podstatnú časť infraštruktúry útočníkov. Zaistenie domén útočníkom znemožňuje prístup do riadiaceho panelu a OČTK môžu na základe monitoringu komunikácie zo sinkholovaných domén identifikovať kompromitované zariadenia. FBI a CISA zverejnili aj analýzu obsahujúcu indikátory kompromitácie (IOC) a techniky, taktiky a procedúry (TTP). **VJ CSIRT preverila koreláciu v rámci platformy MISP (Malware Information Sharing Platform) s evidovanými kybernetickými bezpečnostnými incidentmi.**

VÝZNAMNÉ UDALOSTI VO SVETE

- Skupina LockBit, známa svojimi ransomvérovými útokmi, utrpela bezpečnostný incident, keď jej administrátorské panely na darkwebe boli zneužité a nahradené správou s odkazom na stiahnutie databázy MySQL.

- Výskumníci zo spoločnosti SOCKET identifikovali 3 škodlivé NPM balíčky, ktoré cielia na používateľov AI vývojárskeho editora CURSOR pre zariadenia s Apple macOS.

- Spoločnosť Google zaviedla novú funkcionalitu webových prehliadačov na báze Chromium, ktorá na zariadeniach s operačným systémom Windows minimalizuje riziká vyplývajúce zo spustenia prehliadača s oprávneniami administrátora.

- Vývojári anonymnej siete TOR predstavili experimentálny nástroj ONIUX, ktorý slúži na anonymizáciu sieťovej prevádzky ľubovoľných aplikácií a skriptov na operačných systémoch Linux.

- Vývojári komunikačnej aplikácie SIGNAL vydali aktualizáciu svojho produktu, ktorá aktívne blokuje vytváranie screenshotov aplikácie AI službou Microsoft RECALL.

- Bezpečnostní výskumníci z DATADOG varujú pred útokmi na verejne dostupné REDIS servery, ktoré útočníci infikujú rôznymi formami malvéru, pričom ich primárnym cieľom je ťažba kryptomien.

- YouTuber a bezpečnostní výskumníci z G DATA odhalili, že oficiálny softvér čínskych tlačiarní PROCOLORED už vyše pol roka šíri malvér.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti Frappe Framework

Stručný prehľad pythonovského frameworku Frappe, ktorý vykonali výskumníci CSIRT.SK, odhalil množstvo zraniteľností umožňujúcich útočníkom vykonávať rôzne druhy útokov. V základni kódu sa môže nachádzať množstvo ďalších chýb, ktoré len čakajú na objavenie.

Kód všetkých ukážok zneužitia zraniteľností je k dispozícii v repozitári GitHub.

Aktívne zneužívané zraniteľnosti v produktoch Ivanti EPMM a Neurons for ITSM

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre kritickú zraniteľnosť produktu Neurons for ITSM a dve aktívne zneužívané zraniteľnosti v Endpoint Manager Mobile (EPMM). Zraniteľnosti s identifikátormi CVE-2025-22462, CVE-2025-4427 a CVE-2025-4427 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Kritická zero-day zraniteľnosť v produktoch od Fortinet

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zero-day zraniteľnosť v produktoch FortiVoice, FortiMail, FortiNDR, FortiRecorder a FortiCamera. Zraniteľosť CVE-2023-32756 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Zraniteľnosť je aktívne zneužívaná v rámci útokov na telefónne systémy FortiVoice.

Kritická zraniteľnosť vo vizualizačnej platforme Kibana

Spoločnosť Elastic vydala bezpečnostné aktualizácie svojej vizualizačnej platformy Kibana, ktoré opravujú kritickú zraniteľnosť. CVE-2025-25014 by vzdialený autentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v bezdrôtových kontroléroch Cisco

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre svoje bezdrôtové kontroléry s operačným systémom Cisco IOS XE, ktoré opravujú kritickú zraniteľnosť. CVE-2025-20188 by vzdialený útočník mohol zneužiť na nahratie súborov, vzdialené vykonanie príkazov s oprávneniami používateľa root a získanie úplnej kontroly nad systémom.

Kritická zraniteľnosť v nástroji pre manažment ovládačov ASUS DriverHub

Spoločnosť Spoločnosť ASUS vydala bezpečnostné aktualizácie svojho nástroja pre manažment ovládačov ASUS DriverHub, ktoré opravujú dve zraniteľnosti, z čoho jedna je označená ako kritická. Vzdialený neautentifikovaný útočník by zreťazením zraniteľností s identifikátormi CVE-2025-3462 a CVE-2025-3463 mohol vzdialene vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Zraniteľnosť webového manažmentového nástroja Webmin

Vývojári webového ovládacieho panelu pre vzdialený manažment serverov Webmin vydali aktualizáciu svojho produktu, ktorá opravuje vysoko závažnú zraniteľnosť. CVE-2025-2774 by vzdialený autentifikovaný útočník mohol zneužiť na eskaláciu privilégií, vykonanie ľubovoľného kódu a získanie úplnej kontroly nad systémom.

Kritická zraniteľnosť v IP kamerách Ubiquiti UniFi Protect

Spoločnosť Ubiquiti vydala bezpečnostné aktualizácie pre svoje IP kamery UniFi Protect, ktoré opravujú kritickú zraniteľnosť. Zraniteľnosť s identifikátorom CVE-2025-23123 možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Ďalšia aktívne zneužívaná zraniteľnosť SAP NetWeaver

Spoločnosť SAP vydala bezpečnostné aktualizácie pre opravu ďalšej kritickej zraniteľnosti s identifikátorom CVE-2025-42999, ktorá je aktívne zneužívaná v rámci útokov súvisiacich so zneužitím CVE-2025-31324.

Aktívne zneužívané kritické zraniteľnosti v Craft CMS

Vývojári redakčného systému Craft CMS vydali bezpečnostné aktualizácie, ktoré opravujú dve aktívne zneužívané kritické zraniteľnosti. Kritické zraniteľnosti s označením CVE-2025-32432 a CVE-2024-58136 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Aktívne zneužívaná zraniteľnosť v SAP NetWeaver

Spoločnosť SAP vydala bezpečnostné aktualizácie svojho aplikačného servera SAP NetWeaver, ktoré opravujú kritickú zraniteľnosť. CVE-2025-31324 možno zneužiť na nahratie súborov, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi na prienik do zraniteľných systémov.

MESAČNÍK ZRANITEĽNOSTÍ MÁJ 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2408.html