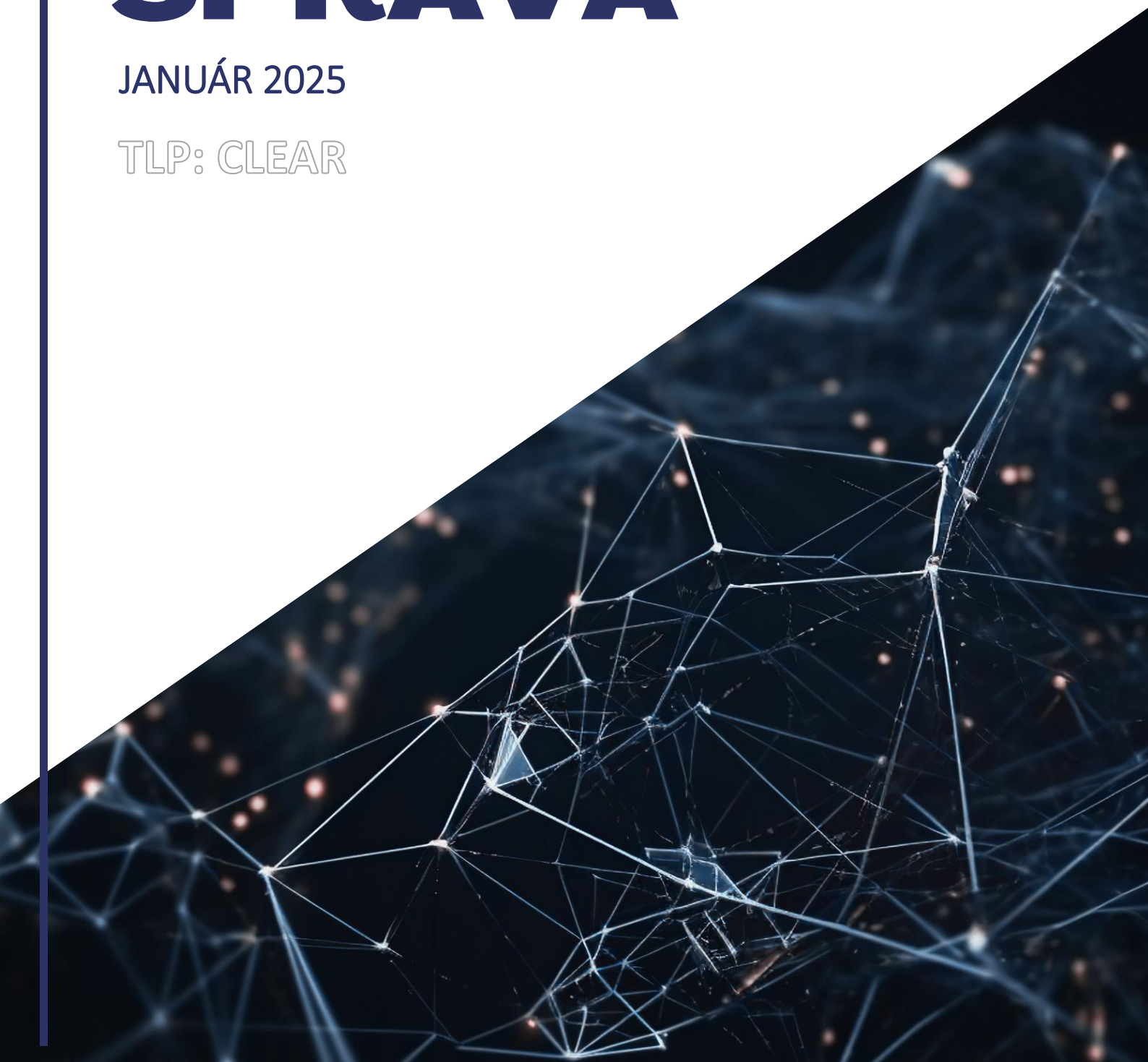
CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JANUÁR 2025

TLP: CLEAR



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

1 Kybernetický útok na Úrad geodézie, kartografie a katastra Slovenskej republiky

Dňa 05.01.2025 bol Vládnej jednotke CSIRT nahlásený incident prostredníctvom oficiálneho e-mailového kanála od Úradu geodézie, kartografie a katastra SR.

2 Phishingová kampaň zneužívajúca identitu spoločnosti Crowdstrike

Spoločnosť CROWDSTRIKE varovala pred phishingovou kampaňou s tematikou pracovných ponúk, v rámci ktorej útočníci zneužívajú identitu ich spoločnosti.

3 Útočníci zneužívajú chybu v peňaženkách Web3 na krádež kryptomeny Ethereum

Bezpečnostní výskumníci zverejnili informácie o novom type útoku, ktorým sa útočníkom zatiaľ podarilo ukradnúť kryptomenu Ethereum v celkovej hodnote 460-tisíc dolárov.

4 Útočníci neznámym spôsobom kompromitovali vyše 5000 stránok WordPress

Bezpečnostní výskumníci zo spoločnosti C/SIDE zverejnili informácie o rozsiahlej kampani, v rámci ktorej došlo ku kompromitácii vyše 5000 webových stránok založených na redakčnom systéme WordPress.

5 TikTok dočasne prerušil poskytovanie služieb na území USA

TIKTOK 17. januára 2025 vo večerných hodinách v nadväznosti na nariadenie Najvyššieho súdu USA zastavil poskytovanie svojich služieb na území Spojených štátov.

6 Cloudflare mitigovala DDoS útok s rekordnou intenzitou

Spoločnosť CLOUDFLARE informovala, že sa jej podarilo mitigovať doteraz najsilnejší DDoS útok, ktorý dosahoval intenzitu 5,6 Tbps.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci január 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. Jednotka zachytila aj útoky hrubou silou na e-mailové kontá.

Zo zaujímavejších prípadov phishingu môžeme spomenúť e-mailové správy s predmetom "Posledná pripomienka na obnovenie domény [doména.sk]", ktoré prijalo viacero organizácií v konštituencii CSIRT.SK. VJ CSIRT získala vzorky podvodných e-mailov, ktoré podrobila analýze.

VJ CSIRT prijala tiež hlásenie e-mailu obsahujúceho malware, ktorý prešiel cez bezpečnostné prvky GOVNET. E-mailové prílohy spúšťali YARA pravidlo pre XWorm_3_0_3_1_Detection. Požiadali sme NASES o preverenie výskytu hrozby v rámci siete GOVNET. VJ CSIRT zaslala varovania na cieľové organizácie s požiadavkou preverenia, či prebehla interakcia s prílohou.

Január priniesol Slovenskej republike jeden z najzávažnejších kybernetických útokov, s akými sa doteraz potýkala. Ransomvérový útok na Úrade geodézie, kartografie a katastra SR (ÚGKK SR) na niekoľko týždňov znepristupnil služby a dáta úradu. Občania nemali okrem iného možnosť získať výpis z katastra, zapísať si nehnuteľnosť, či zaplatiť dohodnutú kúpnu sumu z hypoték, pretože banky si nevedeli uplatniť záložné právo. Zatiaľ neznámy útočník skompromitoval zatiaľ neznámym vektorom útoku infraštruktúru ÚGKK SR, a spustil škodlivý kód typu ransomvér. Znepristupnil prakticky celú produkčnú infraštruktúru. Okamžite po identifikácii bezpečnostného incidentu (5. 1. 2025 o 8:50 hod) spustil ÚGKK SR a dodávatelia proces riešenia bezpečnostného incidentu. Pristúpilo sa k izolácii celej infraštruktúry, vrátane odpojenia všetkých pobočiek, odpojenia od internetu a od siete Govnet. Rovnako prebehlo aj overovanie dostupnosti záloh a snaha o získanie prístupu k znepristupneným zariadeniam. CSIRT.SK spolu s ďalšími zložkami zabezpečujúcimi kybernetickú bezpečnosť SR a zazmluvnenými subjektmi zo súkromnej sféry pracoval na zaisťovaní forenzných stôp a následne ich analyzoval.

Útok na kataster nebol jediným nahláseným januárovým ransomvérovým útokom. CSIRT.SK prijal od partnera hlásenie o ransomvérovom útoku voči systémom jednej slovenskej obce. Jednalo sa o napadnutie jedného PC, ktorý vykazoval známky šifrovania. Bol zabezpečený výjazd zo strany VJ CSIRT na zaistenie zariadenia a preskúmanie dopadov prebiehajúceho incidentu na infraštruktúru obce. Výjazdový tím skontroloval ostatné zariadenia v jej infraštruktúre s negatívnym nálezom a navrhol, aké opatrenia vykonať. Nakoľko je obec súčasťou združenia DEUS, požiadali sme združenie o plošný sken všetkých obcí na prítomnosť tohto ransomvéru a navrhli opatrenia.

Z menej závažných incidentov sa vyskytli prípady zraniteľných webových stránok, patriacich organizáciám v konštituencii CSIRT.SK. Takúto informáciu prijala VJ CSIRT od bezpečnostného výskumníka ohľadom niekoľkých webstránok. Ich podstránky zobrazovali chybovú hlášku

použitej SQL syntaxe, čo potenciálnym útočníkom uľahčovalo vyladenie útoku. Iná webová stránka používala neaktuálnu verziu redakčného systému a prislúchajúcich pluginov WordPress.

Vyskytli sa tiež prípady pokusov o útoky na webové stránky verejných organizácií. V jednom prípade išlo o pokus o vzdialené vykonanie škodlivého kódu. Požiadali sme o blokovanie zdroja útoku v rámci Govnet-u a o preverenie relevantnej sieťovej komunikácie. Na inú webovú stránku smerovali pokusy o útok typu Cross-Site Scripting (XSS).

Pomerne bežne sa vyskytujúci druh útoku na svoje systémy vystavené do internetu zaznamenala v januári aj Všeobecná zdravotná poisťovňa. Jednalo sa o pokusy o uhádnutie prihlasovacieho hesla hrubou silou (bruteforce), kedy útočník v krátkych časových intervaloch opakovane použil emailovú adresu v konvenciách VšZP. Pretože VšZP používa dvojfaktorové overovanie, skončili všetky tieto pokusy neúspešne. Podľa verejne dostupných informácií sa zdroj týchto pokusov historicky vyskytoval pri podobných útokoch na iné organizácie vo svete, o čom sme informovali aj zástupcov VšZP.

CSIRT.SK prijal od partnera informácie o geograficky lokalizovaných IP adresách v našej krajine, ktoré s najväčšou pravdepodobnosťou hosťujú systém infikovaný malvérom SystemBC. Tento malvér sa bežne používa po prieniku do systému krátko pred nasadením rôznych druhov ransomvéru. Kontaktovali sme poskytovateľa predmetného IP adresného rozsahu a požiadali o vyriešenie problému s uvedením odporúčaní pre zasiahnuté/ohrozené subjekty.

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 januári CSIRT.SK plošne rozposlal svojej konštituencii indikátory kompromitácie (IoC) spojené s ransomvérovým útokom na Úrad geodézie, kartografie a katastra SR.

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 januári jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Univerzity Mateja Bela v Banskej Bystrici a študentom a učiteľom SOŠ automobilovej a podnikania v Senci, Spojenej školy Kremnička v Banskej Bystrici, SPŠ stavebnej a geodetickej v Bratislave a SPŠ dopravnej v Trnave.

VÝZNAMNÉ UDALOSTI VO SVETE

Zneužitie obfuskovaného NPM balíčka na nasadenie Quasar RAT

Bezpečnostní výskumníci objavili v registri balíkov npm škodlivý balík "ethereumvulncontracthandler", ktorý sa maskuje ako knižnica na zisťovanie zraniteľností v Ethereum smart zmluvách, avšak v skutočnosti do vývojárskych systémov nahráva open-source trójsky kôň Quasar RAT. Zdrojový kód tohto balíka je obfuskovaný na viacerých vrstvách pomocou techník ako kódovanie Base64 a XOR. Malvér taktiež zahŕňa spúšťanie príkazov PowerShell a vytvára spojenie s C2 serverom cez modifikáciu Windows registrov, čím si zabezpečuje perzistenciu. Tento incident poukazuje na riziká spojené s používaním neoverených balíčkov v open-source softvérových zásobníkoch.

Iránske a ruské entity sankcionované za ovplyvňovanie volieb pomocou AI a kybernetických taktík

Ministerstvo financií USA uvalilo sankcie na dve entity z Iránu a Ruska za ich pokusy ovplyvniť prezidentské voľby v novembri 2024. Tieto organizácie, ktoré sú napojené na Iránske revolučné gardy (IRGC) a ruskú vojenskú rozviedku (GRU), sa snažili ovplyvniť výsledky volieb a rozdeľovať americkú verejnosť prostredníctvom dezinformačných kampaní. Sankcie sa týkajú aj entít, ktoré využívali generatívne AI nástroje na tvorbu a šírenie deepfake videí a falošných správ. Tieto operácie boli podporované finančnými prostriedkami zo strany GRU, ktoré slúžili na financovanie serverov a webových stránok šíriacich dezinformácie.

Kybernetický útok na Úrad geodézie, kartografie a katastra SR

Dňa 05.01.2025 bol Vládnej jednotke CSIRT nahlásený incident prostredníctvom oficiálneho e-mailového kanála od Úradu geodézie, kartografie a katastra SR. V zmysle interných postupov Vládnej jednotky CSIRT a na základe dostupných informácií, bol predmetný incident klasifikovaný ako ransomvér a kybernetický bezpečnostný incident (KBI). Zasiahnutých a zašifrovaných bolo 800 virtuálnych zariadení aj kritických, čo spôsobilo nedostupnosť základných služieb poskytovaných širokej verejnosti v rámci Slovenskej republiky. Orgány sa usilujú minimalizovať škody a obnoviť zasiahnuté systémy. Tento kybernetický útok poukazuje na zraniteľnosť dôležitých verejných systémov a vláda zdôrazňuje potrebu posilnenia kybernetickej bezpečnosti v budúcnosti.

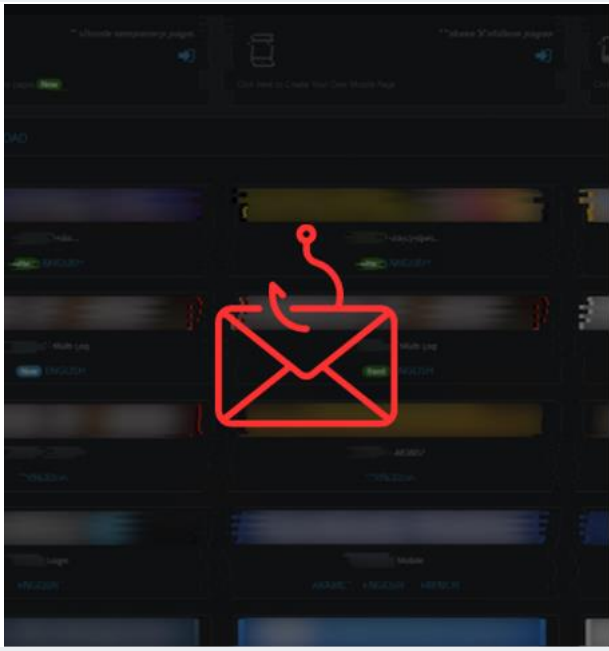
VÝZNAMNÉ UDALOSTI VO SVETE

Platforma telegram pokračuje v zdieľaní údajov s OČTK

Komunikačná služba Telegram zverejnila štatistiky, podľa ktorých od septembra 2024 vyhovela 900 žiadostiam amerických orgánov činných v trestnom konaní a poskytla informácie o telefónnych číslach a IP adresách používateľov. Spolupráca platformy predstavuje významný krok vpred a môže pomôcť pri objasňovaní rôznych druhov kriminality, ktoré páchatelia využívajú na komunikáciu. Telegram Transparency Report pre konkrétne krajiny možno zobraziť prostredníctvom príslušného bota.

Phishingová kampaň zneužívajúca identitu spoločnosti Crowdstrike

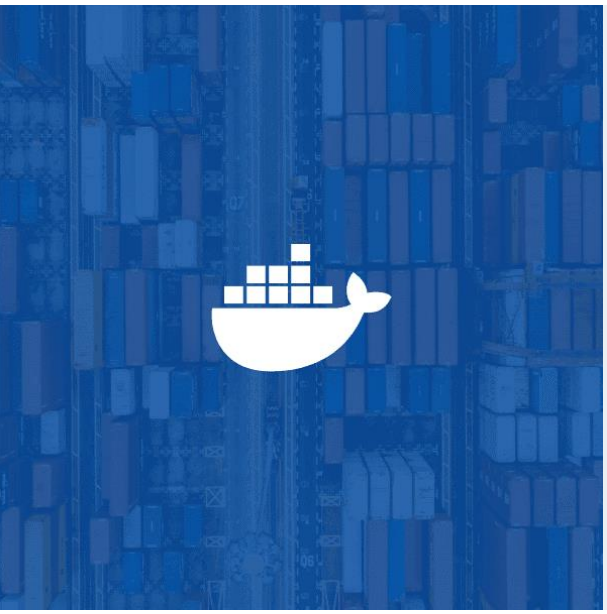
Spoločnosť CROWDSTRIKE varovala pred phishingovou kampaňou s tematikou pracovných ponúk, v rámci ktorej útočníci zneužívajú identitu ich spoločnosti. Hlavným cieľom kampane je infikovať zariadenia obete kryptominerom XMRIG, ktorý používajú na ťažbu kryptomeny Monero. Útok začína phishingovým e-mailom, ktorý sa vydáva za nábor CrowdStrike a nasmeruje príjemcov na škodlivú webovú stránku. Tieto e-maily vyzerajú autenticky, často obsahujú logo CrowdStrike a falošné popisy pracovných pozícií. CrowdStrike radí ľuďom, aby boli opatrní a overovali akúkoľvek podozrivú komunikáciu prostredníctvom oficiálnych kanálov.



Čínska APT skupina Salt Typhon kompromitovala ďalších telekomunikačných operátorov v USA

Bližšie nešpecifikovaný zdroj informoval WALL STREET JOURNAL, že v rámci nedávnych útokov čínskej štátom sponzorovanej skupiny SALT TYPHOON na amerických telekomunikačných operátorov došlo aj ku kompromitácii systémov spoločností Charter Communications, Consolidated Communications a Windstream. Poukazuje to na schopnosti, úspešnosť a závažnosť dopadov útokov zo strany tejto skupiny. Americká vláda a orgány pôsobiace v oblasti kybernetickej bezpečnosti v súvislosti s aktivitami tejto skupiny koncom roka 2024 zverejnili odporúčania pre zabezpečenie systémov.

VÝZNAMNÉ UDALOSTI VO SVETE



Chybný certifikát spôsobil problém so spustením Docker Desktop na macOS

Vývojári kontajnerizačného riešenia Docker varovali pred problémom so spustením aplikácie Docker Desktop na zariadeniach s operačným systémom macOS. Bezpečnostné mechanizmy niektoré verzie označujú ako malvér, nakoľko boli podpísané nesprávnym certifikátom. Vývojári sa snažia o presnú identifikáciu príčiny problému a odporúčajú aktualizáciu zasiahnutých systémov na verziu 4.37.2, ktorá už uvedený problém nemá. Možný je aj downgrade na staršie verzie bez tohto problému alebo použitie skriptov deaktivujúcich bezpečnostné mechanizmy macOS, ale najvhodnejším riešením je aktualizácia na najnovšiu verziu.

Útočníci zneužívajú chybu v peňaženkách Web3 na krádež kryptomeny Ethereum

Bezpečnostní výskumníci zverejnili informácie o novom type útoku, ktorým sa útočníkom zatiaľ podarilo ukradnúť kryptomenu Ethereum v celkovej hodnote 460-tisíc dolárov. Útok zneužíva chybu v mechanizme pre simuláciu transakcií, ktorý sa používa v peňaženkách Web3 na zobrazenie očakávaného stavu blockchainovej transakcie pred jej realizáciou. Útočníci vytvárajú špeciálne webové stránky s tematikou výhry, ktoré po kliknutí na prijatie výhry ukazujú náhľad peňaženky. Časové oneskorenie medzi simulačným mechanizmom a samotným vykonaním transakcie umožňuje ešte pred jej zrealizovaním transakciu zmeniť na prevod a ukradnúť tým kryptomeny. Výskumníci poskytli aj odporúčania.

Nový botnet zneužíva nesprávnu konfiguráciu SPF na rozposielanie phishingových e-mailov

Bezpečnostní výskumníci z INFOBLOX zverejnili informácie o novom botnete pozostávajúcom z kompromitovaných routerov Mikrotik, ktorý zneužíva nesprávne konfigurované SPF záznamy na obchádzanie prvkov e-mailovej ochrany a distribúciu malware. Útočníci špecificky zneužívajú domény s SPF záznamami obsahujúcimi znak +all, ktorý v podstate umožňuje odosielanie e-mailov v mene domény z ľubovoľnej IP. Kampaň je aktívna od konca novembra 2024 a na základe predbežných informácií sa pravdepodobne jedná o aktivitu ruských hackerov. Okrem popísanej funkcionality sú uzly zneužívané aj ako SOCKS4 proxy, na exfiltráciu citlivých údajov a realizáciu útokov DDoS. **VJ CSIRT vykonala kontrolu SPF záznamov subjektov vo svojej konštituencii.**

VÝZNAMNÉ UDALOSTI VO SVETE

Aktívne zneužitie knižnice GO FastHTTP v rámci útokov na služby Microsoft 365

Spoločnosť Seartip zverejnila informácie o rozsiahlych brute-force a MFA fatigue útokoch cielených na službu Microsoft 365, na realizáciu ktorých útočníci zneužívajú knižnicu FastHTTP programovacieho jazyka GO. Útoky sú primárne zamerané na koncové body Azure Active Directory a samotná úspešnosť závisí od prítomnosti MFA, konfigurácie bezpečnostných mechanizmov a samotných používateľov, pričom výskumníci predpokladajú približne 10-percentnú úspešnosť útokov. K dispozícii sú IOC a aj skript PowerShell pre analýzu logov, ktorého cieľom je identifikácia požiadaviek na základe špecifického poľa User-Agent využívaného v rámci FastHTTP.

Útočníci neznámym spôsobom kompromitovali vyše 5000 stránok WordPress

Bezpečnostní výskumníci zo spoločnosti C/SIDE zverejnili informácie o rozsiahlej kampani, v rámci ktorej došlo ku kompromitácii vyše 5000 webových stránok založených na redakčnom systéme WordPress. Útočníci na infekciu a exfiltráciu citlivých údajov zneužívajú doménu wp3[.]xyz. Prvotný vektor prieniku do systémov zatiaľ nie je známy; následne pomocou skriptu stiahnutého z predmetnej domény dochádza k vytvoreniu administrátorského účtu wpx_admin a inštalácii škodlivého pluginu slúžiaceho na získavanie citlivých údajov. Administrátorom odporúčajú implementáciu všetkých best practice postupov pre zabezpečenie CMS, kontrolu jeho integrity a blokovanie komunikácie s uvedenou doménou.

TikTok dočasne prerušil poskytovanie služieb na území USA

TIKTOK 17. januára 2025 vo večerných hodinách v nadväznosti na nariadenie Najvyššieho súdu USA zastavil poskytovanie svojich služieb na území Spojených štátov. Americká vláda platformu obviňuje zo získavania citlivých údajov a ich zdieľania s čínskou vládou. Služba bola opätovne spustená hneď po tom, ako novozvolený prezident Donald Trump ohlásil, že 20. januára 2025 dá spoločnosti TikTok ešte 90 dní na nájdenie amerického kupca. Zároveň navrhol, že by americká vláda kúpila 50 percent systémov, čo by v spolupráci s kupcom zvyšných 50 percent umožnilo pokračovanie služby v USA bez obáv o národnú bezpečnosť. Aplikácia v súčasnosti nie je dostupná na stiahnutie na obchodoch Apple ani Google.

VÝZNAMNÉ UDALOSTI VO SVETE

Rozsiahla malwaretisementová kampaň cielená na používateľov nástroja Homebrew

Bezpečnostní výskumníci upozornili na malwaretisementovú kampaň zameranú na používateľov nástroja Homebrew pre macOS a Linux, ktorej cieľom je infekcia zariadení infostealerom AmosStealer. Phishingová stránka obsahuje príkaz na samotnú inštaláciu, ktorý si má obeť spustiť na svojom zariadení. Na promovanie škodlivého obsahu útočníci zneužívajú platené reklamy na Google zobrazujúce odkaz na legitímnu stránku brew.sh, pričom po kliknutí sú obete presmerované na stránku útočníka brewe.sh. Útočníci v poslednej dobe dokážu pomocou Google Ads vytvárať veľmi dôveryhodne vyzerajúce reklamy.

Chybu v Cloudflare CDN možno zneužiť na cielenú geolokáciu používateľov

Bezpečnostný výskumník identifikoval chybu v službe CDN (Content Delivery Network) od spoločnosti Cloudflare, ktorú možno zaslaním obrázkov cez aplikácie Signal a Discord zneužiť na získanie regionálnej geolokácie príjemcu správy. Metóda vychádza z fungovania služby, ktorá mediálny obsah za účelom urýchlenia prístupu dočasne ukladá v dátových centrách najbližšie k používateľovi. Výskumník smerovaním požiadaviek z Cloudflare Workers alebo Cloudflare Teleport na špecifické dátové centrá analyzuje rýchlosť ich odpovede a dokáže tak identifikovať región, v ktorom sa nachádza analyzovaný subjekt. Cloudflare už údajne zmenil konfiguráciu, no táto zmena lokalizácii používateľa nezabraňuje, iba ju čiastočne komplikuje.

Spoločnosť Cloudflare mitigovala DDoS útok s rekordnou intenzitou

Spoločnosť Cloudflare informovala, že sa jej podarilo mitigovať doteraz najsilnejší DDoS útok, ktorý dosahoval intenzitu 5,6 Tbps. Útok bol realizovaný botnetom na báze MIRAI pozostávajúcim z približne 13 000 uzlov. Po technickej stránke sa jednalo o útoky na báze protokolu UDP. Tzv. hyper-volumetrické útoky sú zaznamenávané pravidelne od 3. kvartálu roka 2024. Článok obsahuje zaujímavé štatistické údaje o DDoS útokoch.

VÝZNAMNÉ UDALOSTI VO SVETE

Malvér J-MAGIC infikujúci VPN brány Juniper využíva inovatívnu metódu maskovania činnosti

Bezpečnostní výskumníci z Black Lotus Labs zverejnili informácie o kampani, v rámci ktorej útočníci infikujú VPN brány Juniper malwarom J-MAGIC. Jedná sa o variant backdooru CD00R a jeho špecifikom je mechanizmus maskovania činnosti, ktorý spustí reverzný shell len po zachytení špeciálneho paketu v rámci sieťovej prevádzky. Útočník musí následne prejsť jednoduchou kontrolou vyžadujúcou zadanie hodnoty, ktorá mu je zaslaná zašifrovaná prostredníctvom zabudovaného verejného RSA kľúča. Jedná sa o zaujímavý mechanizmus maskovania činnosti, ktorý zároveň poskytuje ochranu pred konkurenčnými skupinami a bezpečnostnými výskumníkmi.

VÝZNAMNÉ UDALOSTI VO SVETE

- Ransomvérová skupina Brain Cipher začala zverejňovať údaje ukradnuté počas útoku na platformu RIBridges v štáte Rhode Island.

- Traja rusko-nemeckí občania boli obvinený zo špionáže pre ruskú tajnú službu, pričom ich činnosť zahŕňala špionážne operácie a prípravu sabotážnych útokov proti nemeckým vojenským a priemyselným objektom.

- Bezpečnostní výskumníci zo spoločnosti Watchtowr a The Shadowserver Foundation zaregistrovali 40 expirovaných domén.

- Bezpečnostní výskumníci zo spoločnosti Truffle Security zverejnili informácie o nedostatku vo funkcionalite „Sign in with Google“ OAuth od spoločnosti Google.

- Spoločnosť Microsoft zverejnila informácie o spear phishingovej kampani ruskej skupiny Star Blizzard, ktorej cieľom je kompromitácia účtov WhatsApp.

- CERT-UA varuje pred sofistikovanou kampaňou, v rámci ktorej útočníci na prenik do systémov iniciujú spojenia AnyDesk v mene ukrajinského CSIRT-u.

- Spoločnosť Fortinet sa vyjadrila k uniknutým konfiguračným súborom a prihlasovacím údajom, ktoré minulý týždeň zverejnila hackerská skupina Belsen Group.

- Spoločnosť Halcyon informovala o ransomvérovej kampani skupiny Codefinger, v rámci ktorej útočníci šifrujú Amazon S3 úložiská prostredníctvom natívnej funkcionality AWS SSE-C (Server-Side Encryption with Customer-Provided Keys).

- Spoločnosť Tenable upozornila na chybnú diferenciálnu aktualizáciu skenera zraniteľností Nessus z 31. decembra 2024, ktorá mala za následok znefunkčnenie agentských aplikácií.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť knižnice Python libarchive umožňuje Directory Traversal

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť v Python knižnici libarchive, ktorá umožňuje vykonávať útoky typu directory traversal. Zraniteľnosť sa nachádza v najnovšej verzii knižnice libarchive (4.2.1) a súvisí s absenciou ošetrovania názvov súborov nachádzajúcich sa v poskytnutom súbore ZIP. Táto zraniteľnosť sa nachádza v triede ZipFile v metódach extract a extractall. V prípade, že názvy súborov v nahranom súbore ZIP obsahujú relatívnu cestu (../) alebo aj absolútnu cestu (/tmp/test.txt) je možné danú zraniteľnosť zneužiť nasledovným spôsobom.

Zraniteľnosti routerov a sieťových zariadení Moxa

Spoločnosť Moxa vydala bezpečnostné aktualizácie svojich priemyselných routerov a sieťového príslušenstva, ktoré opravujú dve zraniteľnosti, z ktorých jedna je označená ako kritická. CVE-2024-9140 by vzdialený útočník mohol zneužiť na injekciu príkazov a vzdialené vykonanie škodlivého kódu a CVE-2024-9138 by útočník mohol zneužiť na eskaláciu privilégií na úroveň používateľa root.

Kritické zraniteľnosti vo WordPress plugine Fancy Product Designer

Bezpečnostní výskumníci zverejnili informácie o dvoch kritických zraniteľnostiach vo WordPress plugine Fancy Product Designer. Zraniteľnosti možno zneužiť na upload škodlivých súborov, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Aktívne zneužívaná kritická zraniteľnosť v produkte GFI KerioControl

Spoločnosť GFI vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť v produkte KerioControl. CVE-2024-52875 možno zneužiť na vzdialené vykonanie kódu a následné získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná kritická zraniteľnosť v produktoch Ivanti ICS, IPS a Neurons for ZTA gateways

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 2 bezpečnostné zraniteľnosti v produktoch Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) a Ivanti Neurons for ZTA gateways, z čoho 1 je označená ako kritická. CVE-2025-0282 možno zneužiť na vzdialené vykonanie kódu. Druhú zraniteľnosť možno zneužiť na eskaláciu privilégií.

Vysoko závažné zraniteľnosti vo firewalloch SonicWall s operačným systémom SonicOS

Spoločnosť SonicWall vydala bezpečnostné aktualizácie pre svoje firewally s operačným systémom SonicOS, ktoré opravujú 4 vysoko závažné zraniteľnosti. Najzávažnejšiu zraniteľnosť s označením CVE-2024-53704 možno zneužiť na obídenie mechanizmov autentifikácie a získanie neoprávneného prístupu do systému. Ostatné zraniteľnosti možno zneužiť na obídenie mechanizmov autentifikácie, realizáciu SSRF útokov a eskaláciu privilégií.

Zraniteľnosti Aktívne zneužívaná kritická zraniteľnosť vo firewalloch FortiGate od spoločnosti Fortinet

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zero-day zraniteľnosť v operačnom systéme FortiOS a produkte FortiProxy. CVE-2024-55591 možno zaslaním špeciálne vytvorenej požiadavky zneužiť na získanie administrátorského prístupu k zariadeniu a získanie úplnej kontroly nad systémom.

Bezpečnostné zraniteľnosti v migračnom nástroji Palo Alto Networks Expedition

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú 5 zraniteľností v migračnom nástroji Expedition. Najzávažnejšiu zraniteľnosť CVE-2025-0103 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a vytvorenie alebo odstránenie súborov na systémoch spravovaných prostredníctvom Expedition.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Photoshop, Adobe Substance3D Stager, Adobe Illustrator for iPad, Adobe Animate, Adobe Substance3D Designer, ktoré opravujú 14 kritických zraniteľností. Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu.

Kritické zraniteľnosti v produktoch Ivanti Endpoint Manager, Avalanche, Application Control Engine

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Endpoint Manager (EPM), Avalanche, Application Control Engine, ktoré opravujú 20 zraniteľností, z ktorých 4 sú označené ako kritické. Kritické zraniteľnosti s označením CVE-2024-10811, CVE-2024-13161, CVE-2024-13160 a CVE-2024-13159 sa nachádzajú v produkte EPM a vzdialený neautentifikovaný útočník by ich mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Kritické zraniteľnosti vo webových aplikačných serveroch SAP NetWeaver

Spoločnosť SAP vydala bezpečnostné aktualizácie svojho webového aplikačného servera NetWeaver, ktoré opravujú 8 zraniteľností, z čoho 2 sú označené ako kritické. CVE-2025-0070 a CVE-2025-0066 možno zneužiť na eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom.

Kritické zraniteľnosti v nástroji pre vzdialený prístup SimpleHelp

Vývojári riešenia pre vzdialený prístup SimpleHelp vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú 3 kritické zraniteľnosti. Kombináciou uvedených zraniteľností možno získať úplnú kontrolu nad zraniteľnými systémami.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Microsoft v januárovom Patch Tuesday opravil 12 kritických zraniteľností

Spoločnosť Microsoft vydala v januári 2025 balík opráv pre portfólio svojich produktov opravujúci 161 zraniteľností, z ktorých 58 umožňuje vzdialené vykonanie kódu. Kritické zraniteľnosti sa nachádzajú v Microsoft Digest Authentication, NEGOEX, BranchCache, Windows Remote Desktop Services, Windows OLE, Windows RMCAST, Windows NTLM V1, Azure Marketplace SaaS Resources, Microsoft Purview a Microsoft Excel a možno ich zneužiť vzdialené vykonanie škodlivého kódu, eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Windows Hyper-V NT Kernel Integration VSP obsahuje aktívne zneužívané zraniteľnosti umožňujúce eskaláciu privilégií (CVE-2025-21333, CVE-2025-21334, CVE-2025-21335).

Kritická zraniteľnosť v nástroji pre prenos a synchronizáciu súborov Rsync

Vývojári open source nástroja pre prenos a synchronizáciu súborov RSYNC vydali bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností, z čoho 1 je označená ako kritická. CVE-2024-12084 možno zneužiť na vzdialené vykonanie kódu. Zreťazením zraniteľností CVE-2024-12084 a CVE-2024-12085 možno získať úplnú kontrolu nad zraniteľnými systémami.

Zraniteľnosť v 7-Zip umožňuje obídenie ochrany Mark-of-the-Web a vykonanie škodlivého kódu

Vývojári komprimačného nástroja 7-Zip vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-0411 možno podvrhnutím špeciálne vytvorených súborov zneužiť na obídenie bezpečnostného mechanizmu „Mark of the Web“ a vzdialené vykonanie kódu.

Kritické zraniteľnosti vo WordPress pluginoch RealHomes Theme a Easy Real Estate

Bezpečnostní výskumníci zo spoločnosti Patchstack zverejnili informácie o kritických zraniteľnostiach vo WordPress pluginoch RealHomes Theme a Easy Real Estate, ktoré možno zneužiť na eskaláciu privilégií, získanie administrátorského prístupu a úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti v produktoch Cisco Meeting Management, Secure Endpoint Connector a BroadWorks

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Meeting Management, Secure Endpoint Connector (Linux, Mac a Windows verzie), Secure Endpoint Private Cloud a BroadWorks, ktoré opravujú viaceré zraniteľnosti. Kritickú zraniteľnosť CVE-2025-20156 v Cisco Meeting Management možno zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad systémom. Ostatné zraniteľnosti umožňujú zneprístupnenie služby.

Aktívne zneužívaná kritická zero-day zraniteľnosť v zariadeniach SonicWall Secure Mobile Access 1000

Spoločnosť SonicWall vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zero-day zraniteľnosť v zariadeniach SonicWall Secure Mobile Access série 1000. CVE-2025-23006 možno zneužiť na vzdialené vykonanie systémových príkazov a získanie úplnej kontroly nad systémom.

MESAČNÍK ZRANITEĽNOSTÍ JANUÁR 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2029.html