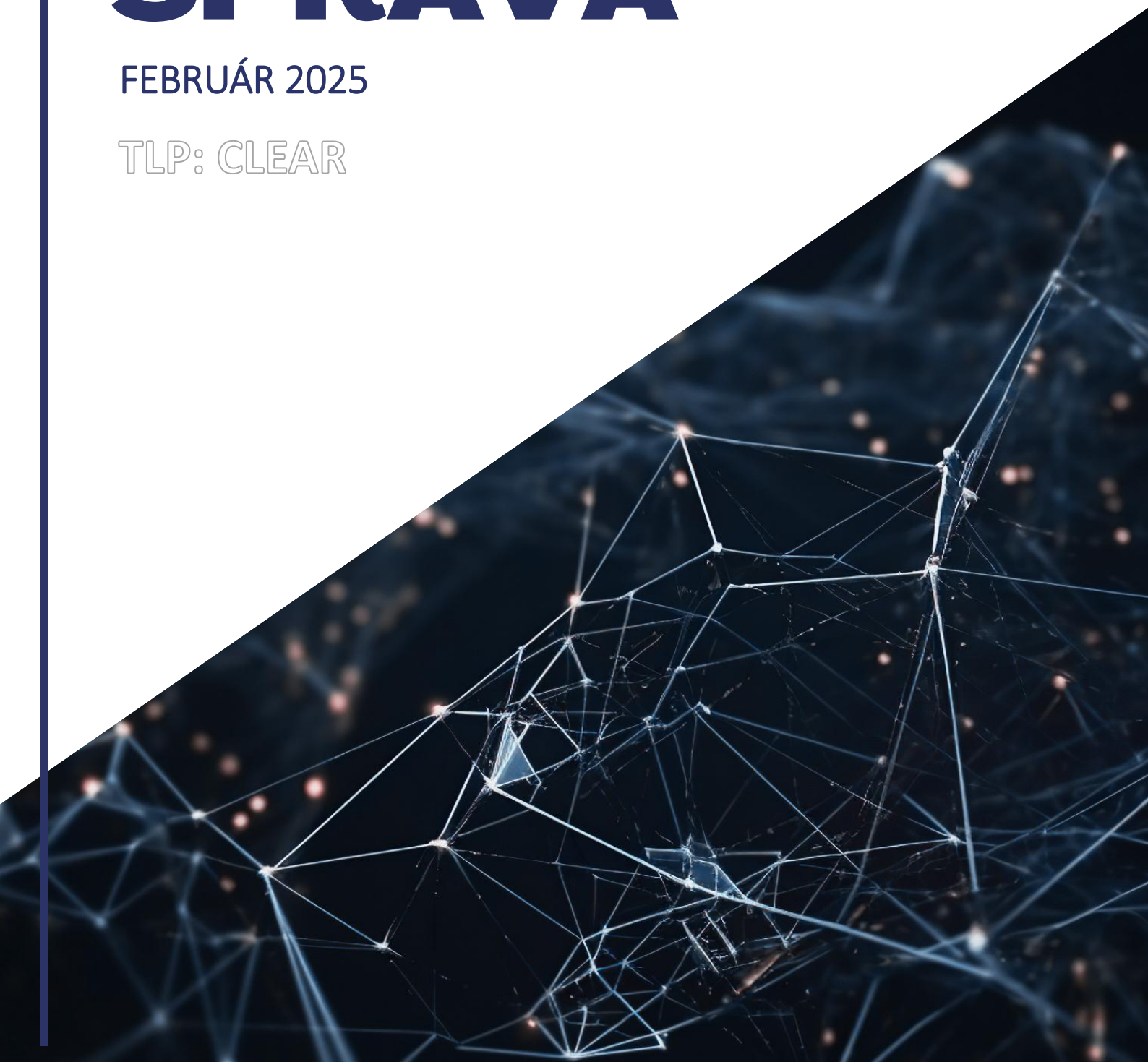
CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

FEBRUÁR 2025

TLP: CLEAR



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

1 Do služby HIBP pribudlo viac než 284 miliónov prihlasovacích údajov z infostealerov

Do služby Have I Been Pwned bolo pridaných vyše 284 miliónov prihlasovacích údajov z infostealerov, ktoré prevádzkovatelia služby našli pri analýze únikov a combolistov kolujúcich po Telegrame.

2 Phishingová kampaň na organizácie používajúce Microsoft ADFS

Kampaň imitujúca zákaznícku podporu, cielila na organizácie používajúce Microsoft Active Directory Federation Services, a to pomocou falošných prihlasovacích stránok.

3 Masívna vlna brute-force útokov cielených na firewally a VPN zariadenia

Organizácia THE SHADOWSERVER FOUNDATION informovala o masívnej vlne brute-force útokov cielených na firewally, VPN a gatewaye od viacerých výrobcov.

4 Spoločnosť Fortinet odhalila nový variant malvéru Snake Keylogger

Spoločnosť FORTINET zverejnila analýzu nového variantu malvéru Snake Keylogger, ktorý je jedným z najznámejších malvérov na zber a exfiltráciu citlivých údajov.

5 ESET zverejnil analýzu útokov severokórejských skupín s tematikou pracovných ponúk

Spoločnosť ESET zverejnila analýzu útokov severokórejských skupín s tematikou pracovných ponúk.

6 Ruské hackerské skupiny zneužívajú QR kódy v rámci útokov na Signal a WhatsApp

Výskumníci z Google Threat Intelligence Group zverejnili informácie o kampani ruských hackerských skupín, zameriavajúcich sa na používateľov aplikácie SIGNAL.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci február riešil typicky najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK. Jednotka zachytila aj útoky hrubou silou na e-mailové kontá.

Najzaujímavejšou februárovou phishingovou kampaňou na Slovensku bola smishingová kampaň zameraná na poistencov Všeobecnej zdravotnej poisťovne. Potenciálnym obetiam prichádzali SMS správy s podvodnými odkazmi smerujúcimi na formulár s požiadavkou informácií o platobnej karte. Zámienkou bolo vyplatenie preplatku poistného na zadanú kartu. Útoky využívali inovatívne techniky a škodlivý kód pre diaľkové zdieľanie signálu NFC. Prebehla aj druhá podobná kampaň s témou daňových preplatkov.

CSIRT.SK prijal hlásenie o zachytenom podvrhnutom e-maile, ktorý útočník odoslal z mailserveru organizácie v konštituencii CSIRT.SK. Prihlasovací portál pre mailserver bol zároveň dostupný z internetu bez šifrovania TLS (cez HTTP). VJ CSIRT požiadala organizáciu o preverenie možnej kompromitácie a odporučila zabezpečiť prihlasovací portál. Ďalšiu kompromitáciu e-mailového účtu v doméne organizácie v konštituencii CSIRT.SK plánoval riešiť správca po zmene hesla zavedením plošnej dvojfaktorovej autentifikácie.

Ďalší prípad sa týkal kompromitácie súkromného zariadenia pracovníka organizácie v konštituencii CSIRT.SK, spojenej s exfiltráciou dát infostealerom. Po analýze boli identifikovaní ďalší zamestnanci, ktorí mohli byť zasiahnutí. Iný prípad kompromitácie pracovného účtu odhalil CSIRT.SK na základe informácií z verejných zdrojov, kde bol publikovaný výpis súborového systému. K nemu mal prístup kompromitovaný administrátorský účet. Je teda možné, že k danému účtu mal prístup aj útočník.

VJ CSIRT sa stretla aj tento mesiac s e-mailovými bombovými hrozbami na organizácie v jej konštituencii. Tento typ bezpečnostného incidentu má potenciál spôsobiť závažné narušenie prevádzky predmetnej organizácie. CSIRT.SK vykonal podrobnú analýzu digitálnych stôp a poskytol zasiahnutej organizácii odporúčania.

Incident s kompromitovaným webovým sídlom organizácie a umiestneným cudzím obsahom riešila VJ CSIRT vyžiadaním a analýzou logov spojených s predmetnou stránkou. Analýza identifikovala údaje poukazujúce na únik prihlasovacích údajov. Po vykonaní opatrení na zabezpečenie sídla sa na predmetnej webovej mape stránky už neukázali škodlivé odkazy.

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

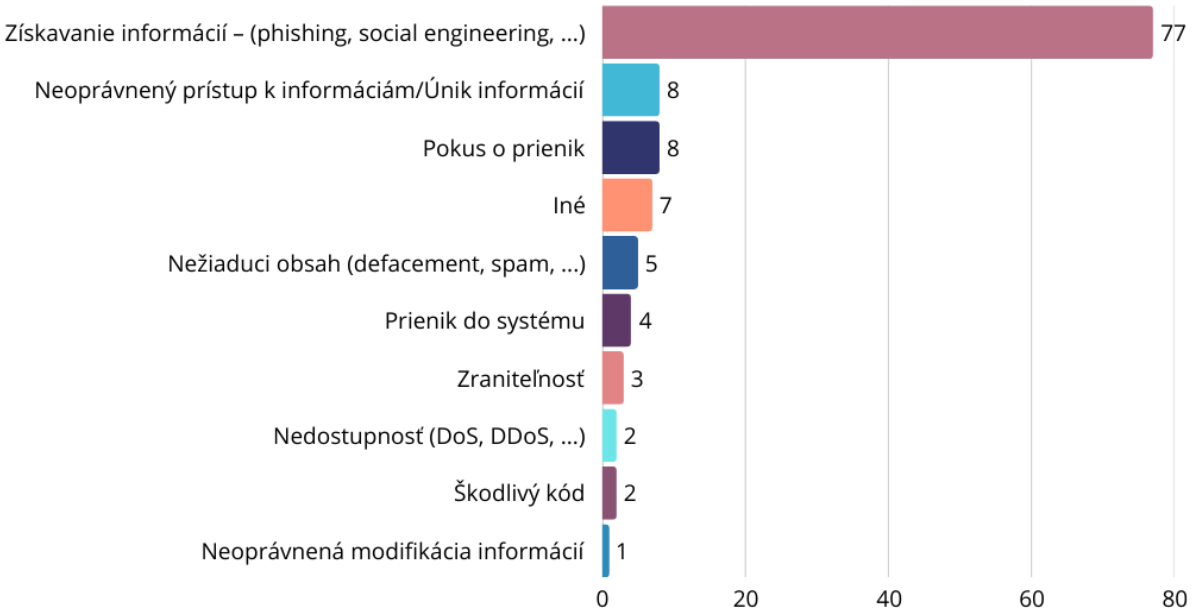
vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén, ktorú monitoruje modul Domino.

Vo februári CSIRT.SK varoval svoju konštituenciu ohľadom úniku a zneužívania strojových kľúčov pre webové aplikácie na platforme ASP.NET. Tieto kľúče sú navrhnuté na ochranu dát v metóde ViewState a možno ich zneužiť na vytvorenie škodlivých payloadov, ktoré majú správny kód MAC (Message Authentication Code). Útočník tak môže poslať požiadavkou POST svoj škodlivý payload, ktorý sa priloží k obsahu ViewState a vykoná po spracovaní ASP.NET Runtime v rámci webového servera IIS. Aj z tohto dôvodu je dôležité pri vývoji dodržiavať pravidlá bezpečného vývoja aplikácií a nepoužívať validationKey a decryptionKey, ktoré je možné nájsť napríklad v dokumentácii a rôznych repozitároch.

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. Jedná sa o cvičenia tabletop alebo hands-on v Kyberaréne MIRRI SR a o prednášky spojená s diskusiou.

Vo februári jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti učiteľom a študentom troch nitrianskych škôl - Strednej zdravotníckej školy, Strednej odbornej školy techniky a služieb a Obchodnej akadémie. V tomto mesiaci navštívila tiež SOŠ technickú v Tlmačoch, SSOŠ podnikateľskú v Senici, SOŠ technickú vo Vrábľoch a Spojenú školu Modrý Kameň.

Nahlásené kybernetické bezpečnostné incidenty za február 2025 (spolu: 117)



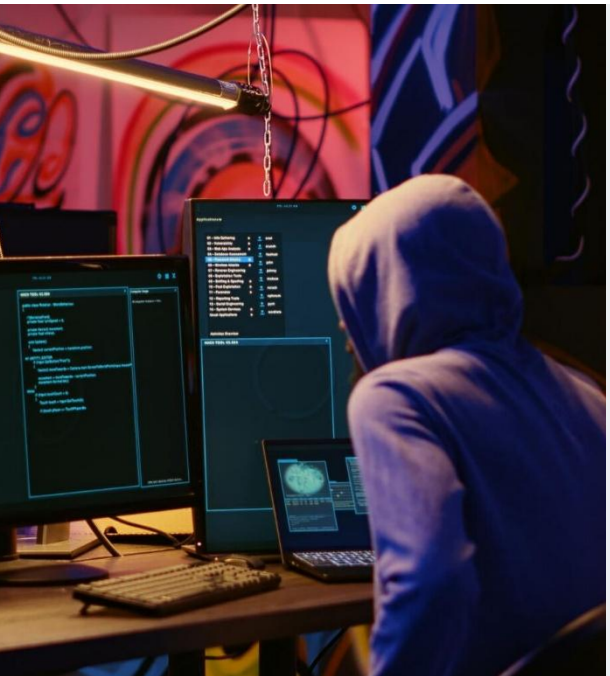
VÝZNAMNÉ UDALOSTI VO SVETE

Do služby HAVE I BEEN PWNED pribudlo viac než 284 miliónov prihlasovacích údajov z infostealerov

Do služby HAVE I BEEN PWNED bolo pridaných vyše 284 miliónov prihlasovacích údajov z infostealerov, ktoré prevádzkovatelia služby našli pri analýze únikov a combolistov kolujúcich po Telegrame. Tieto dáta pochádzajú z 1,5 TB súboru zverejneného na telegramovom kanáli ALIEN TXTBASE. HIBP týmto propaguje aj svoje platené služby pre API prístup. **CSIRT.SK je oficiálnym partnerom HIBP pre vládny sektor v SR**.

Tech support scam kampaň zneužívajúca zabudované funkcie PayPal

Bezpečnostní výskumníci zverejnili informácie o tech support scam kampani zameranej na používateľov PAYPAL. Útočníci zneužívajú funkcionalitu „New Address“ na rozposielanie falošných notifikácií o pridaní novej adresy PayPal a zakúpení produktu, ktoré obsahujú telefónne čísla útočníkov. Útočníci sa počas telefonického rozhovoru obete snažia presvedčiť o hacknutí zariadenia a na inštaláciu nástroja ConnectWise ScreenConnect pre vzdialenú kontrolu.



Útočníci prenikli do systémov rumunskej pobočky Orange

Člen ransomvérovej skupiny HELLCAT vystupujúci pod aliasom REY na hackerskom fóre BREACHFORUMS zverejnil informácie o prieniku do systémov telekomunikačného operátora ORANGE. Spoločnosť Orange potvrdila únik dát a upresnila, že sa jednalo o prienik do nekritických systémov a že v súčasnosti prebieha riešenie incidentu. Rey upresnil, že sa mu podarilo exfiltrovať približne 6,5 GB dát, pričom podstatná časť pochádza od rumunskej pobočky spoločnosti. Na prienik do systémov mal zneužiť uniknuté prihlasovacie údaje a zraniteľnosti v Jira a interných portáloch.

VÝZNAMNÉ UDALOSTI VO SVETE

Palo Alto odhalilo nový modulárny linuxový backdoor AUTO-COLOR

Spoločnosť PALO ALTO zverejnila analýzu nového modulárneho linuxového backdooru AUTO-COLOR, ktorý bol zachytený v rámci útokov na univerzity a vládne organizácie v Severnej Amerike a Ázii. Prvotný vektor prieniku do systémov nie je známy a útok začína spustením súborov s neškodnými názvami, ako napr. door, egg alebo log. Ak je spustený s oprávneniami root, na zabezpečenie perzistencie inštaluje škodlivú knižnicu, skopíruje ju do systémového priečinku a modifikuje /etc/ld.preload. Z hľadiska funkcionality malware umožňuje vytvorenie reverzného shellu, vzdialené vykonanie príkazov, modifikáciu súborov, zapojenie zariadenia do proxy siete útočníka a killswitch na kompletné vymazanie. Článok obsahuje aj indikátory kompromitácie (IoC).

Nárast aktivity botnetu Polaredge kompromitujúceho sieťové zariadenia

Spoločnosť SEKOIA na svojej sieti honeypot-ov zachytila zvýšenú aktivitu botnetu POLAREDGE, ktorý sa šíri zneužívaním zraniteľností v neaktualizovaných, nesprávne konfigurovaných alebo zariadeniach s ukončenou podporou od výrobcov Cisco, ASUS, QNAP a Synology. Zneužitím zraniteľností útočníci šíria nový TLS backdoor, ktorý je sťahovaný prostredníctvom shell skriptov sťahovaných prostredníctvom FTP na IP adrese patriacej službe Huawei Cloud. Malware po infekcii ihneď notifikuje riadiace servery a čaká na ďalšie pokyny. Výskumníci identifikovali vyše 2000 infikovaných IP adries po celom svete. Zatiaľ nie je známy cieľ botnetu, ale predpokladá sa jeho zapojenie do siete ORB (Operational Relay Boxes) zneužívanej na maskovanie činnosti útočníkov.

Phishingová kampaň na organizácie používajúce Microsoft Active Directory Federation Services

Phishingová kampaň, imitujúca zákaznícku podporu, cielila na organizácie používajúce Microsoft Active Directory Federation Services (ADFS), a to pomocou falošných prihlasovacích stránok s cieľom ukradnúť prihlasovacie údaje používateľov a obísť MFA opatrenia. Výskumníci z Abnormal Security zistili, že predmetnými sektormi kampane boli vzdelávací, zdravotnícky a vládny sektor. Snahou bolo získať prístup do služobných účtov.

VÝZNAMNÉ UDALOSTI VO SVETE

Kampaň na LinkedIn severokórejskej APT skupiny Lazarus

Skupina Lazarus (Severná Kórea) vykonáva kampaň falošných pracovných ponúk na platforme LinkedIn, kde ponúka prácu v kryptomenovom a cestovnom sektore. Týmto spôsobom doručuje malvér schopný infikovať operačné systémy Windows, MacOS a Linux. Doručený malvér je písaný v jazyku JavaScript a pôsobí na danom systéme ako stealer na kryptomenu a ako backdoor. Ukradnuté dáta sú následne exfiltrované cez TOR proxy a C2 server.

Útoky na verejne dostupné kľúče ASP.NET vedúce k vykonaniu kódu na serveroch IIS

Spoločnosť Microsoft upozornila na aktívne zneužívanie verejne dostupných kľúčov ASP.NET validationKey a decryptionKey na útoky typu ViewState code injection (injektovanie škodlivého kódu vo frameworku ASP.NET). Použitím týchto kľúčov dokážu útočníci vytvoriť škodlivý ViewState, ktorý server ASP.NET spracuje ako legitímny, čo im umožňuje vzdialené spustenie kódu na IIS serveroch.

Masívna vlna bruteforce útokov cielených na firewally a VPN zariadenia

Organizácia The Shadowserver Foundation informovala o masívnej vlne brute-force útokov cielených na firewally, VPN a gatewaye od viacerých výrobcov. Útoky sú vedené z vyše 2,8 milióna IP adries po celom svete, pričom najviac IP adries je geolokalizovaných v Brazílii, Turecku, Rusku, Argentíne, Maroku a Mexiku. Na základe dostupných informácií sa jedná o kompromitované routery a IoT zariadenia MikroTik, Huawei, Cisco, Boa a ZTE, ktoré sú pravdepodobne zapojené do botnetu alebo proxy siete. Na minimalizáciu tohto typu útoku je potrebná pravidelná aktualizácia zariadení, limitácia dostupnosti manažmentových rozhraní, zmena predvolených hesiel, používanie silných hesiel a implementácia MFA ochrany. Podobný útok prevažne z brazílskych IP zachytil aj NASES.

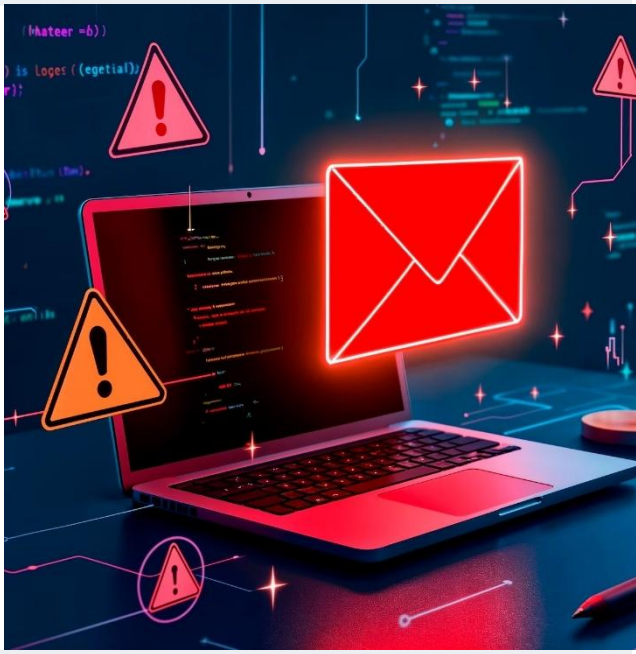
VÝZNAMNÉ UDALOSTI VO SVETE

Zneužitie modifikovaného Google Tag Manager na krádež bankových údajov

Bezpečnostní výskumníci zo spoločnosti SUCURI zverejnili informácie o útokoch na e-shopy na báze redakčného systému MAGENTO, v rámci ktorých útočníci na injekciu kódu na získavanie bankových údajov zneužívajú modifikované GTM (Google Tag Manager). Jedná sa o modifikované verzie GTM a Google Analytics skriptov obsahujúce obfuskovaný kód. Samotné GTM predstavuje kontajner pozostávajúci z viacerých trackingových kódov a pravidiel, ktoré sa spustia len za špecifických podmienok, čo možno zneužiť na cielenie útokov. Útoky zneužívajúce GTM sú pomerne ojedinelé a vzhľadom na to, že sa jedná o bežne používané skripty, v rámci analýzy sú často opomenuté.

Phishingová kampaň zneužívajúca PDF dokumenty hostované na CDN sieti Weblow

Spoločnosť NETKOPE zverejnila informácie o phishingovej kampani na získavanie kartových a bankových údajov, v rámci ktorej útočníci zneužívajú špeciálne vytvorené PDF dokumenty hostované na CDN sieti WEBFLOW. Škodlivý obsah promujú prostredníctvom reklám a SEO optimalizácie výsledkov vyhľadávania veľkých vyhľadávačov. PDF obsahuje obrázok CAPTCHA, ktorý presmerováva na phishingový obsah obsahujúci Cloudflare Turnstile CAPTCHA. Prítomnosť reálnej CAPTCHA zvyšuje dôveryhodnosť scenára a zároveň slúži na maskovanie obsahu pred online skenermi. Po jej absolvovaní sa obeti zobrazí tlačidlo na stiahnutie hľadaného dokumentu, ktoré ale zobrazí popup s výzvou na zadanie bankových údajov.



Hackerská skupina TA2727 infikuje zariadenia Windows, macOS a Android infostealermi

Spoločnosť PROOFPOINT zverejnila informácie o aktivitách hackerskej skupiny TA2727, ktorá sa špecializuje na šírenie infostealerov LUMMA STEALER a DEER STEALER (Windows), MARCHER (Android) a FRIGIDSTEALER (macOS). Skupina na maskovanie svojej činnosti a distribúciu malvéru zneužíva TDS (Traffic Distribution System) od skupiny TA2726 a kompromitované webové stránky injektované kódom JavaScript pre zobrazovanie upozornení na aktualizáciu prehliadača. Upozornenia na základe geolokácie a operačného systému obeti pripravia najvhodnejší payload. FrigidStealer zameraný na macOS je naprogramovaný v jazyku GO a používa knižnicu WailsIO využívanú pre zobrazovanie obsahu priamo vo webovom prehliadači.

VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosť Fortinet odhalila nový variant malvéru Snake Keylogger

Spoločnosť FORTINET zverejnila analýzu nového variantu malvéru SNAKE KEYLOGGER, ktorý je jedným z najznámejších malvérov na zber a exfiltráciu citlivých údajov. Prvotným vektorom prieniku do systémov sú phishingové e-maily obsahujúce škodlivé prílohy alebo URL odkazy na ich stiahnutie. Na doručenie finálneho payloadu útočníci zneužívajú binárne súbory kompilované prostredníctvom skriptovacieho jazyka AUTOIT, čo komplikuje aj ich analýzu. Finálny payload sa prostredníctvom tzv. process hollowing-u injektuje do legitímnych .NET procesov ako napr. regsvcs.exe. Na zabezpečenie perzistencie do priečinka Windows Startup umiestňuje VBS skript, ktorý ho opätovne spustí po reštarte zariadenia. Snake Keylogger podporuje exfiltráciu prostredníctvom SMTP a Telegram Bot API.

Phishing-as-a-service platforma Darcula dokáže klonovať ľubovoľné stránky

Bezpečnostní výskumníci zo spoločnosti NETCRAFT zverejnili informácie o pripravovanej verzii phishing-as-a-service platformy DARCULA s označením DARCULA SUITE, ktorá má umožňovať vytvorenie phishingového obsahu zneužívajúceho identitu ľubovoľného cieľa. Framework po zadaní URL cieľa prostredníctvom nástroja PUPPETEER vytvorí jeho klon a následne umožňuje modifikáciu vstupných polí a formulárov a JavaScript kódu. Nová verzia má znížiť aj požiadavky na technické know-how a zvýšiť používateľskú prívetivosť administratívneho rozhrania pre správu kampane. Výskumníci na telegramových kanáloch zachytili aj predaj jednorazových telefónov s pridanými ukradnutými kartami, čo svedčí o popularite novej verzie Darcula.

Spoločnosť ESET zverejnila analýzu útokov severokórejských skupín s tematikou pracovných ponúk

Spoločnosť ESET zverejnila analýzu útokov severokórejských skupín s tematikou pracovných ponúk. Ide o obľúbenú techniku severokórejských hackerov, kde po nadviazaní komunikácie s obeťou v rámci praktickej časti pracovného pohovoru zašlú súbory alebo odkazy na repozitáre so škodlivým kódom slúžiacim na získavanie a exfiltráciu citlivých údajov. Zaujímavá je heatmapa, podľa ktorej tieto aktivity boli zachytené aj na území SR. Článok obsahuje indikátory kompromitácie (IOC) a taktiky, techniky a procedúry (TTP) skupiny.

VÝZNAMNÉ UDALOSTI VO SVETE

Ruské hackerské skupiny zneužívajú QR kódy v rámci útokov na Signal a WhatsApp

Bezpečnostní výskumníci z Google Threat Intelligence Group zverejnili informácie o rozsiahlej kampani ruských hackerských skupín, ktoré sa zameriavajú na používateľov aplikácie Signal. V rámci útokov zneužívajú funkcionalitu Linked Devices, ktorá umožňuje súčasný beh aplikácie na viacerých zariadeniach. Na prepojenie účtov obetí s inštanciami Signal pod kontrolou útočníka zneužívajú špeciálne vytvorené QR kódy imitujúce pozvánky do skupín, bezpečnostné upozornenia alebo požiadavky na spárovanie zariadení. V rámci útokov na armádne ciele na Ukrajine boli zachytené aj QR kódy umiestnené na phishingových stránkach. Od začiatku roka 2025 boli zachytené obdobné kampane zamerané na používateľov WhatsApp.

VÝZNAMNÉ UDALOSTI VO SVETE

- Austrálska vláda s odvolaním sa na analýzu a ohrozenie národnej bezpečnosti zakázala používanie produktov a webových služieb od spoločnosti KASPERSKY LAB vo vládnych systémoch.

- Bezpečnostní výskumníci z KASPERSKY informovali o malwaretisement kampani s označením GITVENOM.

- Americká FBI pripísala krádež kryptomien z kryptoburzy Bybit z 21. februára 2025 severokórejskej štátom sponzorovanej skupine LAZARUS.

- Ransomvérový útok na nemeckú spoločnosť TELIO mal vážny dopad na väzenské telefónne služby vo viacerých štátoch EÚ, vrátane slovenského ZVJS.

- V rámci medzinárodnej akcie PHOBOS AETOR v Thajsku zadržali 4 členov ransomvérovej skupiny PHOBOS a rozložili darknetové stránky ransomvérovej skupiny 8BASE.

- Bezpečnostní výskumníci z ELASTIC SECURITY LABS zverejnili technickú analýzu útokov hackerskej skupiny REF7707.

- Spojené štáty, Austrália a Spojené kráľovstvo pridali ruského poskytovateľa hostingových služieb ZSERVERS na zoznam sankcionovaných organizácií.

- Spoločnosť MICROSOFT zverejnila informácie o medzinárodnej kampani ruskej štátom sponzorovanej skupiny SEASHELL BLIZZARD s označením BADPILOT, ktorej primárnym cieľom je získavanie neoprávneného prístupu do systémov.

- Spoločnosť MICROSOFT varovala pred aktivitami hackerskej skupiny STORM-2372, ktorá cieli široké spektrum organizácií v Európe, Severnej Amerike, Afrike a Strednom Východe.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Atlassian opravuje kritické zraniteľnosti viacerých produktov

Spoločnosť Atlassian vydala bezpečnostné aktualizácie na svoje produkty Confluence, Bamboo, Bitbucket, Crowd a Jira, ktoré opravujú 7 zraniteľností, z čoho 3 sú označené ako kritické. Kritické zraniteľnosti v Confluence a Crowd je možné zneužiť na vzdialené vykonanie kódu a obídenie mechanizmov autentifikácie. Ostatné zraniteľnosti je možné zneužiť na zneprístupnenie služby. Zraniteľnosti routerov a sieťových zariadení.

Závažné zraniteľnosti OpenSSH

Vývojári OpenSSH vydali bezpečnostné aktualizácie, ktoré opravujú dve zraniteľnosti umožňujúce realizáciu útokov typu man-in-the-middle a zneprístupnenie služby. Úspešným zneužitím zraniteľností môže útočník získať prístup k citlivým informáciám a prevziať kontrolu nad SSH reláciou.

Závažná zraniteľnosť Citrix NetScaler Console a Agent

Spoločnosť Citrix vydala bezpečnostné aktualizácie pre svoje produkty NetScaler Console a NetScaler Agent, ktoré opravujú vysoko závažnú zraniteľnosť. Táto umožňuje autentifikovanému útočníkovi eskalovať svoje privilégiá a vzdialene vykonávať príkazy.

Kritická zraniteľnosť v distribuovanej databáze Apache Ignite

Vývojári distribuovanej databázy Apache Ignite vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2024-52577 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná zraniteľnosť v databázovom systéme PostgreSQL

Vývojári databázového systému PostgreSQL vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť vysokej závažnosti. CVE-2025-1094 vo viacerých funkciách libpq možno zneužiť na vzdialené vykonanie kódu.

Aktívne zneužívaná zraniteľnosť v operačnom systéme Palo Alto PAN-OS

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie pre svoj sieťový operačný systém PAN-OS, ktoré opravujú 4 zraniteľnosti, z ktorých 1 je označená ako aktívne zneužívaná. Zraniteľnosti nachádzajúce sa vo webovom manažmentovom rozhraní a plugine OpenConfig možno zneužiť na injekciu príkazov, získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme. CVE-2025-0108 je podľa spoločnosti GreyNoise v súčasnosti aktívne zneužívaná útočníkmi.

Microsoft v rámci februárového Patch Tuesday opravil 4 kritické zraniteľnosti

Spoločnosť Microsoft vydala vo februári 2025 balík opráv pre portfólio svojich produktov opravujúci 61 zraniteľností, z ktorých 26 umožňuje vzdialené vykonanie kódu. Kritické zraniteľnosti nachádzajúce sa v produktoch Microsoft možno zneužiť na eskaláciu privilégií a vzdialené vykonanie kódu. Zraniteľnosti vo Windows Storage (CVE-2025-21391) a Windows Ancillary Function Driver for WinSock (CVE-2025-21418) sú v súčasnosti aktívne zneužívané útočníkmi.

Kritické zraniteľnosti v produktoch Ivanti ICS, IPS, ISAC a CSA

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Ivanti Secure Access Client (Ivanti Secure Access Client) a Ivanti Cloud Services Application (CSA), ktoré opravujú 10 zraniteľností, z čoho 4 sú označené ako kritické. Kritické zraniteľnosti umožňujú vzdialené vykonanie kódu, získanie neoprávneného prístupu k citlivým údajom a vykonanie zmien v systéme.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické bezpečnostné zraniteľnosti v Cisco Identity Services Engine

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre svoj produkt Cisco Identity Services Engine a Cisco Identity Services Engine – Passive Identity Connector, ktoré opravujú 2 kritické zraniteľnosti. Zraniteľnosti s označením CVE-2025-20124 a CVE-2025-20125 možno zneužiť na vzdialené vykonanie príkazov, eskaláciu privilégií, vykonanie neoprávnených zmien v systéme a zneprístupnenie služby.

Kritické bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty InDesign, Commerce, Substance 3D Stager, InCopy, Illustrator, Substance 3D Designer a Photoshop Elements, ktoré opravujú 45 zraniteľností, z čoho 23 je označených ako kritických. Kritické zraniteľnosti by útočník mohol zneužiť na vykonanie škodlivého kódu, obídenie bezpečnostných prvkov a eskaláciu privilégií.

Kritická zraniteľnosť Wazuh umožňuje vykonávať kód

Vývojári open-source SIEM a XDR platformy Wazuh vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. Táto umožňuje vzdialene vykonávať kód Python. Na uvedenú zraniteľnosť je dostupný proof-of-concept kód demonštrujúci postup jej zneužitia.

Kritické zraniteľnosti Zimbra Collaboration

V produkte Zimbra Collaboration boli opravené dve kritické a jedna stredne závažná zraniteľnosť. Tieto umožňujú útočníkom získať metadáta e-mailov alebo presmerovanie na koncové body v rámci vnútornej siete.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Útočníci aktívne zneužívajú verejne dostupné ASP.NET kľúče na vzdialené vykonanie kódu

Spoločnosť Microsoft varovala pred útokmi na aplikácie ASP.NET, v rámci ktorých útočníci na vzdialené vykonanie kódu a šírenie malvéru zneužívajú verejne dostupné statické strojové kľúče (machine keys) ASP.NET.

Aktívne zneužívaná zraniteľnosť v operačných systémoch iOS a iPadOS

Spoločnosť Apple vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zraniteľnosť v operačných systémoch iOS a iPadOS. Zraniteľnosť s označením CVE-2025-24200 by útočník s fyzickým prístupom k uzamknutým zariadeniam mohol zneužiť na deaktiváciu bezpečnostného mechanizmu USB Restricted Mode.

Aktívne zneužívané zero-day zraniteľnosti v Zyxel zariadeniach série CPE

Bezpečnostní výskumníci z Greynoise a Vulncheck varujú pred aktívnym zneužívaním kritických zero-day zraniteľností v zariadeniach Zyxel CPE. CVE-2024-40891 a CVE-2024-40891 možno zneužiť na vzdialené vykonanie príkazov a získanie úplnej kontroly nad systémom.

Vysoko závažné zraniteľnosti v produktoch VMware AVI Load Balancer, Aria Operations a Cloud Foundation

Spoločnosť Broadcom vydala bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností v produktoch VMware AVI Load Balancer, Aria Operations a Cloud Foundation, z ktorých 4 sú označené ako vysoko závažné. Najzávažnejšie zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k databáze (CVE-2025-22217 – AVI Load Balancer) a k prihlasovacím údajom produktov VMware integrovaných do Aria Operations for Logs (CVE-2025-22218).

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Vysoko závažné zraniteľnosti v PHP balíku Voyager používaného na správu aplikácií Laravel

Bezpečnostní výskumníci zo spoločnosti SonarSource zverejnili informácie o 3 bezpečnostných zraniteľnostiach open-source PHP balíka Voyager používaného na správu Laravel aplikácií. Zreťazením zraniteľností CVE-2024-55417 a CVE-2024-55416 možno dosiahnuť vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Zraniteľnosti v nástrojoch platformy GitHub možno zneužiť na získanie autentifikačných údajov

Vývojári platformy GitHub vydali bezpečnostné aktualizácie svojich produktov GitHub Desktop, Git LFS, GitHub CLI/Codespaces a Git Credential Manager, ktoré opravujú 4 zraniteľnosti, z čoho 2 sú označené ako vysoko závažné. Zraniteľnosti súhrnne označené ako „Clone2Leak“ možno zneužiť na získanie neoprávneného prístupu k prihlasovacím údajom a autentifikačným tokenom.

Kritická zraniteľnosť monitorovacieho a manažmentového frameworku Cacti

Vývojári open-source monitorovacieho a manažmentového frameworku Cacti vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve zraniteľnosti, z čoho jedna je označená ako kritická. Kritickú zraniteľnosť s označením CVE-2025-22604 možno zneužiť na vzdialené vykonanie kódu.

Vysoko závažné zraniteľnosti v DNS systéme BIND možno zneužiť na zneprístupnenie služby

Vývojári DNS systému BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve vysoko závažné zraniteľnosti. CVE-2024-12705 a CVE-2024-11187 možno zneužiť na zahltenie dostupných prostriedkov a zneprístupnenie služby.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické a aktívne zneužívaná zero-day zraniteľnosť v produktoch Apple

Spoločnosť APPLE vydala bezpečnostné aktualizácie, ktoré opravujú 69 bezpečnostných zraniteľností v operačných systémoch iOS, iPadOS, macOS, tvOS, watchOS a visionOS a webovom prehliadači Safari, z čoho 18 je označených ako kritických a 1 ako aktívne zneužívaná zero-day zraniteľnosť. Aktívne zneužívanú zero-day s označením CVE-2025-24085 možno zneužiť na eskaláciu privilégií na zariadeniach s tvOS, watchOS, macOS Sequoia, iOS, iPadOS a visionOS.

Zero-day zraniteľnosti Advantive VeraCore

Advantive VeraCore obsahuje dve aktívne zneužívané zraniteľnosti, z ktorých jedna umožňuje nahrávanie súborov do ľubovoľného priečinku zraniteľnej aplikácie a druhá umožňuje získať kontrolu nad databázou. Útočníci zo skupiny XE Group zreťazujú tieto zraniteľnosti pre nasadenie webshellov.

MESAČNÍK ZRANITEĽNOSTÍ FEBRUÁR 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.