CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

MAREC 2025

TLP: CLEAR

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

1 Smishingová triáda využíva nové techniky pri podvodoch

Smishingové útoky predstavujú stále väčšiu hrozbu pre jednotlivcov ako aj organizácie na celom svete, vrátane Slovenska.

2 Rozloženie kryptoburzy GARANTEX

Ministerstvo spravodlivosti USA oznámilo, že v rámci medzinárodnej operácie OČTK došlo k rozloženiu kryptoburzy GARANTEX a k zaisteniu asociovaných domén.

3 Supply chain útok na GITHUB ACTIONS

Bezpečnostní výskumníci zo STEP SECURITY zverejnili informácie o supply chain útoku prostredníctvom automatizačného nástroja GITHUB ACTIONS, ktorý je využívaný minimálne na 23 000 repozitároch. Skupina Coinbase je spájaná s útokom na dodávateľský reťazec GitHub Actions.

4 CLICKFIX: phishingová kampaň zneužívajúca identitu booking.com

Spoločnosť MICROSOFT upozornila na masívnu phishingovú kampaň zneužívajúcu identitu BOOKING.COM, v rámci ktorej útočníci zneužívajú techniku CLICKFIX na infekciu zariadení obete rôznymi druhmi malvéru.

5 Zneužitie kompromitovaných účtov platformy SIGNAL na šírenie malvéru

Ukrajinský CERT-UA upozornil na malvérovú kampaň cielenú na ukrajinskú armádu a organizácie v obrannom priemysle, v rámci ktorej útočníci na rozposielanie malvéru zneužívajú kompromitované účty na platforme SIGNAL.

6 Hackerská platforma Atlantis AIO automatizuje credential stuffing

Atlantis AIO je nová platforma, ktorá automatizuje útoky credential stuffing na viac ako 140 online službách.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

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

Sofistikovanú formu phishingu nahlásil občan cez kontaktný formulár portálu slovensko.sk. Jednalo sa o podvodnú stránku vladnespravy[.]com, ktorá sa snažila napodobňovať webdizajn slovenských vládnych stránok. Rýchlou analýzou bolo zistené, že skutočným účelom stránky bol phishing, ktorý získaval platobné údaje návštevníkov. Po kontaktovaní poskytovateľa IP adresného rozsahu a požiadavke na odstránenie škodlivého obsahu by už v súčasnosti mali byť odkazy na internet banking nefunkčné.

Marec priniesol aj ďalší prípad výhražných e-mailov doručených na školu. Základná škola v Bratislave nahlásila výhražný e-mail, v ktorom sa útočník vyhrážal vypustením vírusu Ebola v jej priestoroch. Na základe požiadavky bola škole poskytnutá informácia ako vyhodnocovať riziko výhražného e-mailu pomocou oficiálneho dokumentu Ministerstva vnútra SR „Metodika vyhodnocovania rizika bombových hrozieb“, ktorý sa zameriava na proces vyhodnotenia stupňa rizika bombových hrozieb a na prijatie adekvátnych opatrení.

V marci sa jednotka CSIRT.SK stretla s útokmi typu DDoS (cieľom je spôsobiť nedostupnosť služby) na webové služby viacero štátnych organizácií v jej konštituencii. Útoky na dve organizácie zneužívali nástroj Bytespider, crawler spoločnosti Bytedance. V jednom prípade útok zahltil databázu požiadavkami z unikátnych IP adries z celého sveta. Útok bol mitigovaný blokovaním zodpovedných IP adries. Žiaden z týchto útokov neviedol k dlhšie trvajúcemu výpadku služieb, teda nespôsobil väčšie škody.

V rámci ďalších útokov na webové služby prijala VJ CSIRT hlásenie podozrivej aktivity smerujúcej na webové stránky organizácie v jej konštituencii. Aktivitu z konkrétnej zdrojovej IP adresy vyhodnotila ako pokusy o SQL Injection, XSS, ZAP Probe, Directory Traversal, HTTP Parser Attack.

CSIRT.SK prijal tiež hlásenie potenciálnej kompromitácie bližšie neurčeného e-mailového účtu v doméne organizácie pod jej dohľadom. Šetrením sa zistilo, že viacerí používatelia v doméne sa prihlasovali z destinácií, v ktorých sa reálne nepohybujú. Na základe OSINT analýzy sa potvrdil únik prihlasovacích údajov ku predmetného účtu, spôsobený malvérom typu infostealer, ktorý infikuje zariadenia a obetiam kradne prihlasovacie údaje a ďalšie citlivé informácie. VJ CSIRT poskytla zoznam krokov na odstránenie problému. Na základe ďalšej analýzy a prijatých informácií od SK-CERT sa potvrdilo, že jedno zo zariadení v držbe pracovníčky organizácie bolo infikované daným malvérom. Tomuto zariadeniu organizácia zablokovala prístup do infraštruktúry a pracovníčka bola poučená.

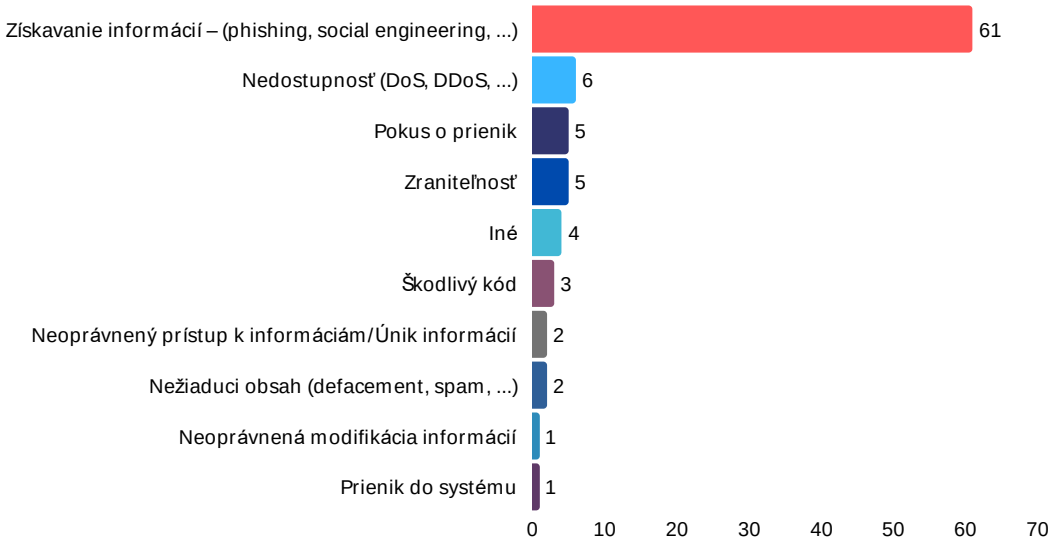
Kurióznym prípadom bol incident, v rámci ktorého útočník zablokoval prístup k zariadeniu starostovi obce a požadoval výkupné. V rámci riešenia incidentu VJ CSIRT odporučila, aby starosta po osobnom zvážení podal trestné oznámenie v súvislosti s vydieraním a potenciálnou krádežou citlivých údajov. Tento prípad predstavuje netypický modus operandi útočníkov, ktorých cieľom je získať finančné prostriedky z výkupného. Útočník nepracoval klasickým spôsobom operátorov ransomvéru. Zariadenie nezašifroval, iba svojej obeti zamedzil prístup k nemu. Je možné, že na to zneužil niektorú aplikáciu pre vzdialený prístup (TeamViewer, ScreenConnect, a pod.).

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

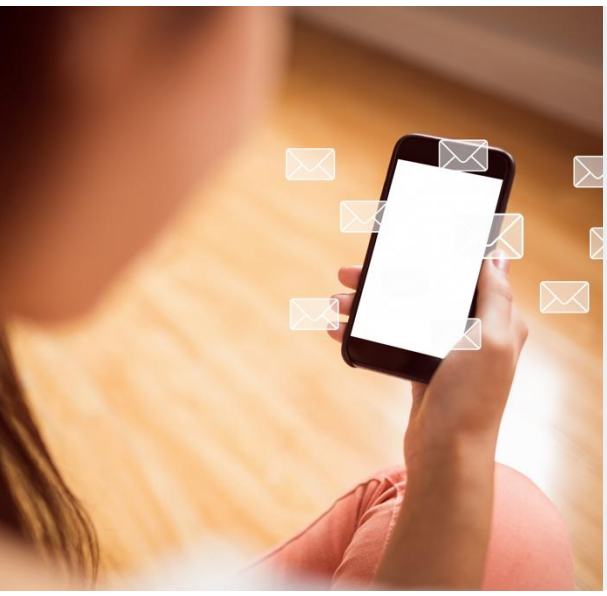
CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných škôl. V marci jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre učiteľov základných, materských a základných umeleckých škôl v okrese Topoľčany a študentom Strednej odbornej školy obchodu a služieb v Piešťanoch, Gymnázia Milana Hodžu v Sučanoch a SOŠ masmediálnych a informačných služieb v Bratislave.

Zamestnanci VJ CSIRT sa zúčastnili konferencie CIO Agenda, ktorá sa konala 4.3.2025 v Prahe. Prezentovali prednášku s témou ransomvérových útokov na štátne organizácie. Túto tému priblížili a rozanalyzovali na reálnom prípade, ktorý jednotka riešila pred niekoľkými rokmi.

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



VÝZNAMNÉ UDALOSTI VO SVETE



„Smishingová triáda“ využíva nové techniky pri podvodoch

Smishingové útoky predstavujú stále väčšiu hrozbu pre jednotlivcov ako aj organizácie na celom svete, vrátane Slovenska. Tieto podvody, pri ktorých útočníci zneužívajú SMS správy alebo moderné komunikačné platformy, ako sú iMessage a RCS (Rich Communication Services), s cieľom získať citlivé údaje, sú čoraz sofistikovanejšie. Na Slovensku bola zaznamenaná kampaň, pri ktorej sa útočníci vydávali za Všeobecnú zdravotnú poisťovňu (VšZP) s cieľom vylákať citlivé informácie. VJ CSIRT uverejnila článok o Smishingovej triáde, ktorý upozorňuje na nové hrozby v oblasti mobilnej bezpečnosti.

Europol rozložil skupinu tvoriacu detskú pornografiu pomocou nástrojov AI

Europol s partnermi v rámci medzinárodnej akcie OPERATION CUMBERLAND rozložili kriminálnu skupinu špecializujúcu sa na tvorbu detskej pornografie (CSAM) zneužitím nástrojov umelej inteligencie. V rámci operácie došlo 26. februára 2025 k zadržaniu 25 osôb a zaisteniu 173 zariadení, ktorých forenzná analýza umožnila identifikáciu ďalších potenciálnych páchateľov. Podľa všetkého sa jednalo o pokračovanie kampane, v rámci ktorej bol v novembri 2024 zatknutý páchateľ dánskej národnosti. Na riziká a aktívne zneužívanie AI na generovanie obsahu CSAM nedávno upozornila aj spoločnosť Microsoft.

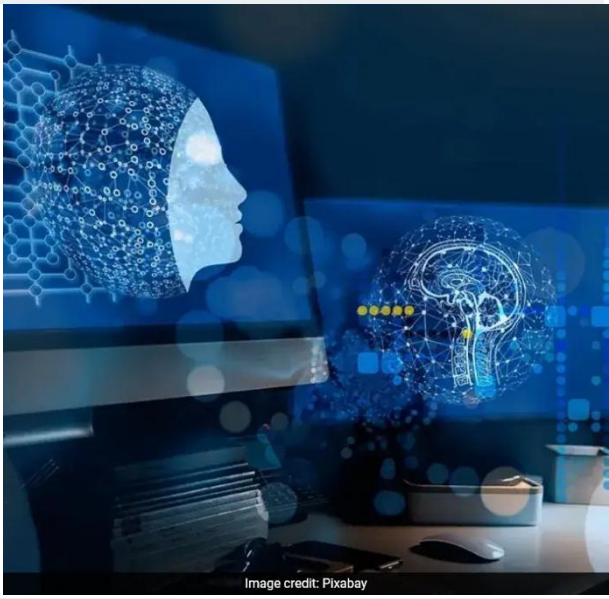
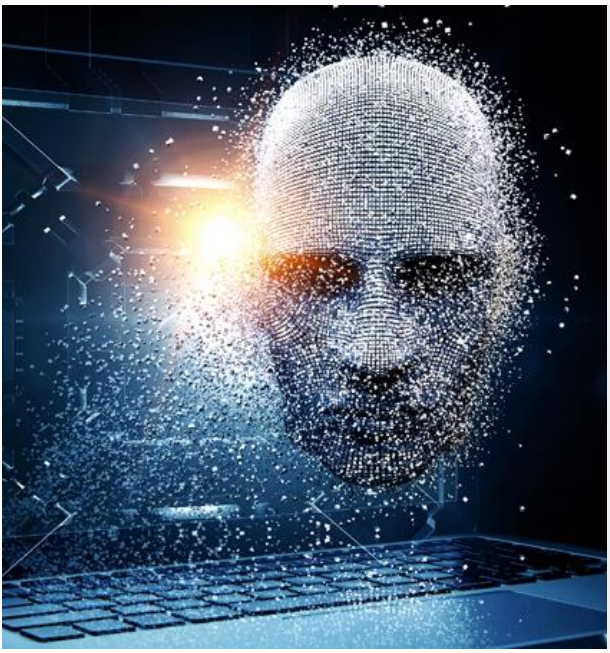


Image credit: Pixabay

Phishingová kampaň šíri škodlivý balík Havoc pod zámienkou nedostupnosti služieb Google a Microsoft

Bezpečnostní výskumníci zo spoločnosti Fortinet zverejnili informácie o masívnej phishingovej kampani na báze CLICKFIX, ktorej cieľom je šírenie modifikovanej verzie open-source post-exploitačného frameworku Havoc. E-maily obsahujú HTML prílohu, ktorá po otvorení zobrazí vyskakovacie okno informujúce o nedostupnosti služieb Google a Microsoft a potrebe manuálnej aktualizácie DNS. Po kliknutí na tlačidlo je do schránky obete skopírovaný kód PowerShell, ktorý po spustení zo SharePoint servera útočníka sťahuje ďalší PowerShell vykonávajúci kontrolu spustenia v sandboxe, kontrolu prítomnosti a prípadnú inštaláciu interpretéra Python. Následne dochádza k stiahnutiu skriptu Python na nasadenie Havoc vo forme injektovaného DLL. Na maskovanie riadiacej komunikácie využívajú Microsoft Graph API.

VÝZNAMNÉ UDALOSTI VO SVETE



Deepfake phishing sa snaží získať prihlasovacie údaje pre Youtube

Spoločnosť Google varovala pred phishingovou kampaňou založenou na deepfake videu s generálnym riaditeľom platformy Youtube, ktorej cieľom je získavanie prihlasovacích údajov tvorcov obsahu. Útočníci vybrané obete kontaktujú e-mailom ohľadom zmien v pravidlách monetizácie obsahu, v ktorom je pripojený odkaz na súkromné video s deepfake obsahom generovaným pomocou AI. Popis videa žiada obete o potvrdenie aktualizovaných podmienok YPP (YouTube Partner Program) na phishingovej stránke slúžiacej na získavanie prihlasovacích údajov. Kampaň má byť aktívna od konca januára 2025, pričom tím YouTube začal jej bližšie skúmanie až v polovici februára 2025.

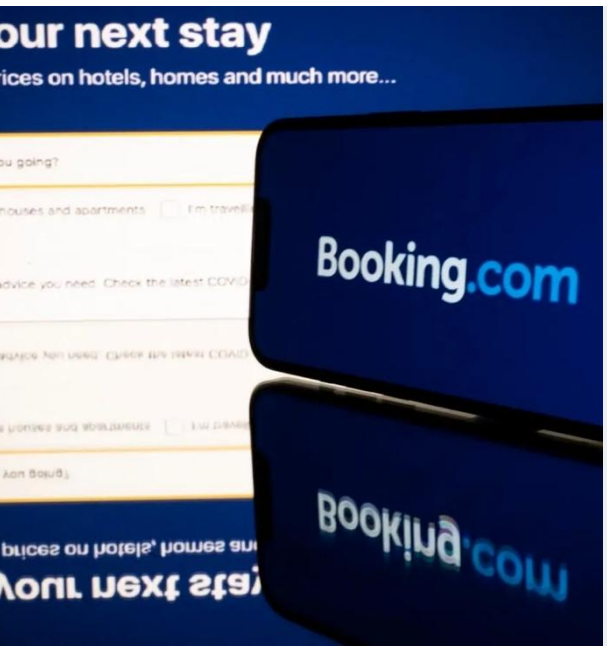
Rozloženie kryptoburzy Garantex

Ministerstvo spravodlivosti USA oznámilo, že v rámci medzinárodnej operácie OČTK došlo k rozloženie kryptoburzy Garantex a k zaisteniu asociovaných domén. Zaisteniu domén predchádzalo postupne zavedenie sankcií, najprv zo strany USA a potom aj zo strany EÚ. Kryptoburzu v minulosti využívali hackerské skupiny Hydra, Conti, LockBit, Black Basta a Ryuk. Tether zablokoval jej kryptopeňaženky v celkovej hodnote 26 miliónov dolárov. Spoločnosť Elliptic údajne vyvinula techniky na sledovanie a označovanie kryptopeňaženiek asociovaných s Garantex.

CISA s partnermi zverejnila detailnú analýzu ransomvérovej skupiny Medusa

Americká CISA s partnermi v rámci iniciatívy #StopRansomware zverejnila analýzu ransomvérovej skupiny Medusa, ktorá od začiatku svojej činnosti v roku 2021 až po súčasnosť kompromitovala vyše 300 organizácií v kritickej infraštruktúre USA a ďalších subjektov po celom svete. Z pohľadu modus operandi skupina na prenik do systému spolupracuje s IAB (Initial Access Broker). Dokument v rámci preventívnych opatrení odporúča pravidelné aktualizácie systémov, segmentáciu siete, minimalizáciu útočnej plochy a blokovanie prístupov z neoverených a nedôveryhodných zdrojov. K dispozícii sú TTP, IOC a aj pravidlá pre host-based detekciu.

VÝZNAMNÉ UDALOSTI VO SVETE

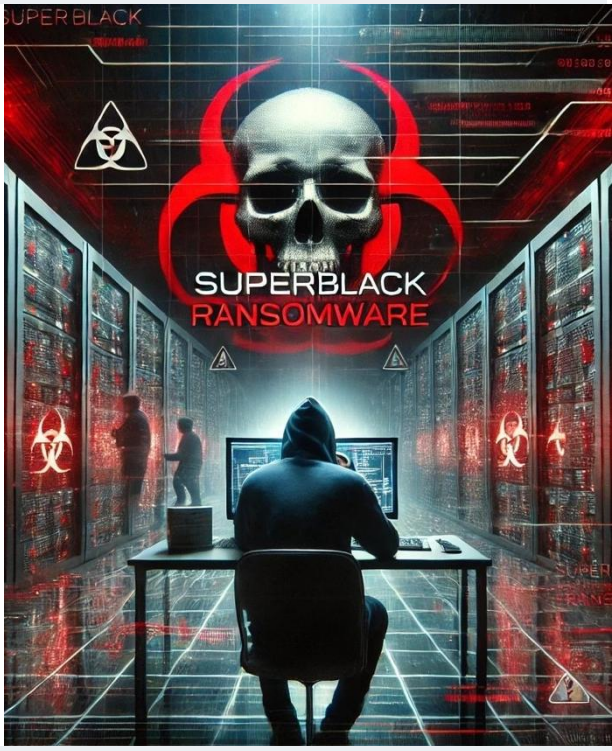


ClickFix: phishingová kampaň zneužívajúca identitu booking.com

Spoločnosť Microsoft upozornila na masívnu phishingovú kampaň zneužívajúcu identitu booking.com, v rámci ktorej útočníci zneužívajú techniku CLICKFIX na infekciu zariadení obete rôznymi druhmi malvéru. Primárnym cieľom útočníkov je kompromitácia zamestnaneckých účtov na platforme, ktoré možno následne zneužiť na získanie citlivých údajov zákazníkov. Microsoft kampaň atribuoval hackerskej skupine STORM-1865. Podobnú kampaň sme tento týždeň zachytili aj v rámci incidentov. Obeti je na phishingovej URL zobrazená falošná CAPTCHA a návod na odstránenie problému spustením PowerShell skriptu, ktorý prostredníctvom mshta.exe vykonáva škodlivý kód obsiahnutý v HTML kóde.

Výskumníci zverejnili analýzu novej ransomvérovej rodiny SuperBlack

Bezpečnostní výskumníci z Forescout zverejnili informácie o novom ransomvérovom aktérovi MORA_001, ktorý zariadenia obete infikuje ransomvérom SuperBlack. Útočník na prenik do systémov zneužíva zraniteľnosti CVE-2025-55591 a CVE-2025-24472 vo firewalloch Fortinet a na zabezpečenie perzistentného prístupu vytvorí nových používateľov a zautomatizuje ich vytváranie v prípade ich odstránenia. Následne v rámci laterálneho pohybu po sieti vykonáva skenovanie siete a snaží sa o získanie prístupu do rôznych systémov. Po exfiltrácii dát sa spustí samotný ransomware a po dokončení šifrovania špeciálny nástroj Wipeblack, ktorý slúži na zahladenie stôp a odstránenie malwaru. Analýza zdrojového kódu odhalila viacero podobností s ransomwarom Lockbit. Fortinet v tejto súvislosti aktualizoval aj popis zraniteľnosti CVE-2025-24472. Článok obsahuje aj indikátory kompromitácie (IOC).



USA po rozhodnutí súdu zrušili sankcie voči kryptomixéru Tornado Cash

USA odstránili sankcie voči kryptomixéru Tornado Cash, pôvodne obvinenému z prania miliárd dolárov vrátane peňazí severokórejských útočníkov. Sankcie boli zavedené v auguste 2022 a zrušené v marci 2025 po súdnom verdikte, ktorý rozhodol, že OFAC prekročil svoje právomoci. Ministerstvo financií USA naďalej varuje pred kybernetickými hrozbami a zneužitím kryptomien. Z veľkého množstva mixérov pridaných na zoznam sankcií ide o prvý prípad, kedy došlo k ich zrušeniu.

VÝZNAMNÉ UDALOSTI VO SVETE

Supply chain útok na GitHub Actions

Bezpečnostní výskumníci zo Step Security zverejnili informácie o supply chain útoku prostredníctvom automatizačného nástroja GitHub Actions, ktorý je využívaný minimálne na 23 000 repozitároch. Útočníkom sa do repozitára nástroja podarilo umiestniť škodlivý kód pre exfiltráciu tajných hodnôt CI/CD z runner worker procesu priamo do repozitárov všetkých projektov využívajúcich uvedenú akciu. V prípade nesprávnej konfigurácie workflow logov boli uvedené údaje verejne dostupné. Podľa vyjadrení vývojárov sa útočníkom bližšie nešpecifikovaným spôsobom podarilo získať GitHub PAT (Personal Access Token) bota @tj-actions-bot, ktorý disponoval privilegovaným prístupom k repozitáru. Vzhľadom na závažnosť incidentu a potenciálne dopady na používateľov zaregistrovali vývojári kvôli transparentnosti CVE-2025-30066. Škodlivý commit bol odstránený a vývojári odporúčajú vykonať bezodkladnú aktualizáciu GitHub Actions a vykonanie reaktívnych opatrení na preverenie úniku dát.

Rozšírenie útoku na GitHub Actions

- Výskumníci odhalili ďalšiu kompromitovanú akciu reviewdog/action-setup, ktorá obsahovala podobný kód na exfiltráciu tajných hodnôt konfigurácie CI/CD a predpokladajú, že údaje bota tj-actions-bot boli získané týmto spôsobom. Spôsob kompromitácie repozitára reviewdog doposiaľ nebol identifikovaný, ale predpokladá sa, že škodlivý kód mohol pridať niekto z prispievateľov projektu, ktorý umožňuje automatické pridávanie vývojárov.

Primárnym cieľom supply chain útoku cez GitHub Actions bol pravdepodobne Coinbase

- Spoločnosť Coinbase bola jednou z prvých obetí útokov na dodávateľský reťazec GitHub Actions, ako uvádza článok od Unit 42 Palo Alto Networks.

Zneužitie kompromitovaných účtov Signal na šírenie malvérov

Ukrajinský CERT-UA upozornil na malvérovú kampaň cielenú na ukrajinskú armádu a organizácie v obrannom priemysle, v rámci ktorej útočníci na rozposielanie malvéru zneužívajú kompromitované účty na platforme Signal. Správy obsahujú archívy vydávajúce sa za reporty zo schôdzí, ktoré obsahujú PDF dokument a spustiteľný EXE súbor. Jedná sa o loader DarkTortilla, ktorého cieľom je stiahnutie Dark Crystal RAT. Správy sú rozposielané z kompromitovaných účtov legitímnych používateľov. Presný spôsob ich kompromitácie nie je známy, ale môže súvisieť s nedávnou kampaňou zneužívajúcou funkciu Signal Linked Devices, o ktorej vo februári 2025 informovala Google Threat Intelligence Group.

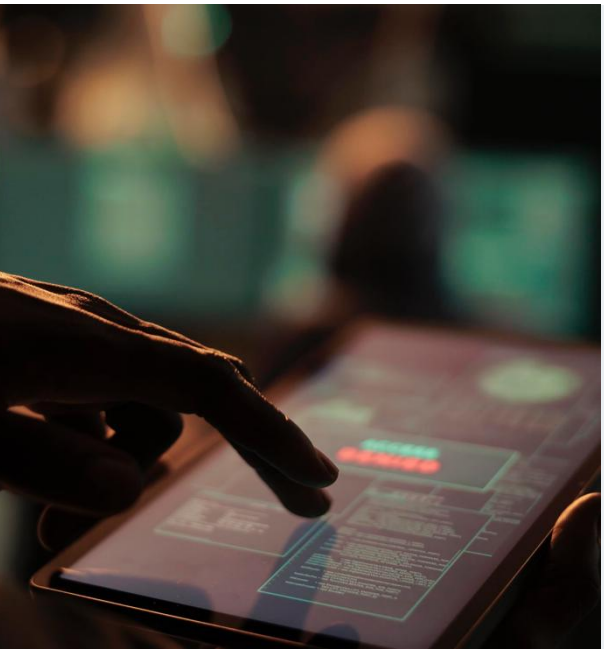
VÝZNAMNÉ UDALOSTI VO SVETE

Tvorca stránky Have I Been Pwned sa stal obeťou phishingového útoku

Zakladateľ služby Troy Hunt a tvorca stránky "**Have I Been Pwned**" sa stal obeťou phishingového útoku, pri ktorom mu bolo kompromitované konto na Mailchimp (online služba, ktorá používateľom umožňuje jednak odosielať newslettery, jednak ich aj navrhnúť). Útočníci získali e-mailový zoznam jeho odberateľov, vrátane 16 000 záznamov. Incident poukázal na zraniteľnosť tradičnej dvojfaktorovej autentifikácie a potrebu odolnejších metód ochrany pred phishingom. Hunt sa ospravedlnil za únik a zdieľal skúsenosti z tejto situácie.

Hackerská platforma Atlantis AIO automatizuje credential stuffing útoky

Atlantis AIO je nová platforma, ktorá automatizuje credential stuffing útoky na viac ako 140 online službách. Credential stuffing je technika, pri ktorej útočníci používajú automatizované nástroje na overovanie ukradnutých prihlasovacích údajov na rôznych webových stránkach s cieľom získať neoprávnený prístup k účtom používateľov. Platforma zjednodušuje a zrýchľuje proces útokov, čím zvyšuje riziko pre online služby a ich používateľov. Na ochranu pred takýmito útokmi je dôležité používať jedinečné a silné heslá pre každú službu a aktivovať viacfaktorovú autentifikáciu, kde je to možné. Prevádzkovatelia online služieb by mali implementovať pokročilé bezpečnostné opatrenia na detekciu a prevenciu týchto typov útokov.



Doména vo vlastníctve Microsoft presmeruje na stránky s hazardným obsahom

Používateľ na komunikačnej platforme Reddit upozornil, že doména microsoftstream.com, ktorá patrí spoločnosti Microsoft bola využívaná v rámci phishingových útokov. V databáze WHOIS vyhľadávanie potvrdilo, že doména je stále vo vlastníctve Microsoftu. Tento incident spôsobil, že všetky stránky SharePoint s vloženými videami z pôvodnej služby Microsoft Stream teraz zobrazujú tento nežiaduci obsah. Bezpečnostná komunita do vyriešenia problému navrhuje pridanie domény do zoznamu škodlivých domén, aby dochádzalo k blokovaniu obsahu zo strany bezpečnostných prvkov.

VÝZNAMNÉ UDALOSTI VO SVETE

- V dátovej sade pre trénovanie AI našli 12 000 prihlasovacích údajov.

- Podvodníci sa vydávajú za členov ransomvérovej skupiny BianLian a odosielajú falošné výhražné správy firmám v Spojených štátoch cez poštovú službu United States Postal Service.

- Spoločnosť Kaspersky zverejnila informácie o malwaretisement kampani zneužívajúcej identitu open-source nástroja na obchádzanie online cenzúry WPD (Windows Packet Divert), v rámci ktorej dochádza k šíreniu kryptominera SilentCryptominer.

- Phishingová kampaň zneužíva falošné OAuth aplikácie na krádež údajov a šírenie malvéru.

- Bezpečnostní výskumníci zo spoločnosti Symantec zverejnili informácie o novom multifunkčnom backdoore BETRUGER.

- Bezpečnostní výskumníci z GoDaddy zverejnili informácie o masívnej kampani s označením Dollyway World Domination.

- Bezpečnostní výskumníci z EclecticIQ zverejnili analýzu automatizovaného frameworku Bruted, ktorý bol vyvinutý ransomvérovou skupinou Black Basta.

- StreamElements, poskytovateľ cloudových nástrojov pre streamerov na platformách ako Twitch a YouTube, oznámil narušenie bezpečnosti údajov u svojho bývalého externého poskytovateľa služieb.

- Spoločnosť Trend Micro odhalila kampaň ruského útočníka Water Gamayuna, ktorý aktívne zneužíva zero-day zraniteľnosť v rámci konzoly Microsoft Management Console.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Broadcom odstránil aktívne zneužívané zraniteľnosti virtualizačnej platformy VMware

Spoločnosť Broadcom vydala bezpečnostné aktualizácie na svoje virtualizačné platformy VMware ESXi, Workstation a Fusion ktoré opravujú 3 aktívne zneužívané zero-day zraniteľnosti, z čoho jedna je označená ako kritická.

Zraniteľnosť knižnice pdfkit pre Python

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť CVE-2025-26240 v knižnici pdfkit v jazyku Python. Spočíva v metóde from_string, ktorá spracúva používateľské vstupy HTML, ktoré však neošetruje. Metóda používa metaznačky, ktorých názvy začínajú na "pdfkit-". Ich hodnoty konvertuje na parametre príkazového riadku pre nástroj wkhtmltopdf. Analýzu vstupov vykonáva metóda _find_options_in_meta, ktorá sa nachádza v súbore pdfkit/pdfkit.py.

Google opravil 2 aktívne zneužívané zero-day zraniteľnosti operačného systému Android

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj operačný systém Android, ktoré opravujú 44 zraniteľností, z čoho 10 je označených ako kritické a 2 ako aktívne zneužívané. CVE-2024-43093 v komponente Framework a CVE-2024-50302 v komponente HID USB možno zneužiť na získanie neoprávneného prístupu k citlivým údajom v systémových priečinkoch a kernel pamäti.

Aktívne zneužívaná kritická zraniteľnosť v IP kamerách Edimax IC-7100

Bezpečnostní výskumníci zverejnili informácie o aktívne zneužívanej kritickej zraniteľnosti v IP kamerách Edimax IC-7100 (produkt s ukončenou podporou). Zraniteľnosť s identifikátorom CVE-2025-1316 možno zneužiť na vzdialené vykonanie kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Čipy Espressif ESP32 obsahujú nezdokumentované funkcie

Bezpečnostní výskumníci zo spoločnosti Tarlogic zverejnili informácie o nezdokumentovaných funkciách v čipoch ESP32, ktoré sú súčasťou veľkého množstva inteligentných a IoT (Internet of Things) zariadení po celom svete. CVE-2025-27840 by útočník s fyzickým prístupom mohol zneužiť na vykonanie neoprávnených zmien v systéme a získanie kontroly nad zariadeniami. Spoločnosť Espressif sa vyjadrila, že sa jedná o príkazy pre účely interného testovania a nie bezpečnostnú zraniteľnosť.

Microsoft v rámci marcového Patch Tuesday opravil 6 kritických zraniteľností

Spoločnosť Microsoft vydala v marci 2025 balík opráv pre portfólio svojich produktov opravujúci 58 zraniteľností, z ktorých 23 umožňuje vzdialené vykonanie kódu. Kritické zraniteľnosti nachádzajúce sa v produktoch Microsoft Office a Microsoft Dataverse a komponentoch Windows Remote Desktop Services, Remote Desktop Client, Windows Domain Name Service a Windows Subsystem for Linux (WSL2) možno zneužiť na eskaláciu privilégií a vzdialené vykonanie kódu.

Aktívne zneužívaná zero-day zraniteľnosť v operačných systémoch Apple

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.

Kritická zraniteľnosť v priemyselných switchoch Moxa

Spoločnosť Moxa vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v priemyselných switchoch série PT a EDS-508A. CVE-2024-12297 by vzdialený útočník mohol zneužiť na realizáciu útokov na báze brute-force a MD5 kolízií, obídenie mechanizmov autentifikácie a získanie neoprávneného prístupu do systému.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná zraniteľnosť v populárnej softvérovej knižnici FreeType

Vývojári populárnej open-source softvérovej knižnice pre vykresľovanie fontov FreeType vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zraniteľnosť vysokej závažnosti. CVE-2025-27363 by vzdialený neautentifikovaný útočník podvrhnutím špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie kódu.

Mozilla v súvislosti s vypršaním koreňového certifikátu vyzýva na aktualizáciu Firefox

Spoločnosť Mozilla upozornila, že 14. marca 2025 vyprší jeden z koreňových certifikátov, ktorý je využívaný aj na overovanie a schvaľovanie doplnkov webového prehliadača Firefox a používateľov vyzvala vykonanie bezodkladnej aktualizácie systémov.

Kritické zraniteľnosti v GitLab možno zneužiť na impersonáciu používateľov a vykonanie kódu

Vývojári platformy GitLab vydali bezpečnostné aktualizácie, ktoré opravujú 9 zraniteľností, z čoho 3 sú označené ako kritické. CVE-2025-25291, CVE-2025-25292 v externej knižnici ruby-saml by vzdialený autentifikovaný útočník mohol zneužiť na impersonáciu používateľov v rámci SAML IdP (Identity Provider) daného prostredia. CVE-2025-27407 v knižnici graphql možno zneužiť na vzdialené vykonanie kódu.

Aktívne zneužívaná zraniteľnosť v operačnom systéme Juniper Junos OS

Spoločnosť Juniper vydala bezpečnostné aktualizácie pre svoj sieťový operačný systém Junos OS, ktoré opravujú aktívne zneužívanú zraniteľnosť. CVE-2025-21590 by lokálny útočník s prístupom k shell-u mohol zneužiť na obídenie bezpečnostného mechanizmu Veriexec, vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť modulu WordPress Ghost

V module WordPress Ghost bola opravená kritická zraniteľnosť, ktorá umožňuje vzdialene vykonávať kód. Chyba spočíva v možnosti vykonávať útoky typu LFI manipuláciou odkazu URL. Kritická zraniteľnosť s označením CVE-2025-26909 umožňuje neautentifikovanému útočníkovi vzdialene vykonávať kód. Chyba spočíva v nedostatočnom overovaní používateľských vstupov vo funkcii showFile(), čo umožňuje útočníkovi prechádzať medzi adresármi a vkladať ľubovoľné súbory servera do upraveného odkazu URL (útok typu Local File Inclusion).

Kritická zraniteľnosť Veeam Backup & Replication

Spoločnosť Veeam opravila kritickú zraniteľnosť v produkte Backup & Replication, ktorá umožňuje útočníkovi s oprávneniami doménového používateľa vzdialene vykonávať kód na serveri Backup Server. Kritická zraniteľnosť s ozačením CVE-2025-23120 umožňuje autentifikovanému používateľovi z lokálnej skupiny, alebo doménovému používateľovi vzdialene vykonávať kód na Backup Server. Chyba spočíva v neošetrenej deserializácii v triedach *Veeam.Backup.Core.BackupSummary* a *xmlFrameworkDs*.

Kritická zraniteľnosť Next.js

Framework Next.js obsahuje kritickú zraniteľnosť, ktorá umožňuje útočníkom obísť kontroly autorizácie pomocou špeciálne vytvorených požiadaviek, ak prebiehajú v Middleware a ďalej už nie. Kritická zraniteľnosť s označením CVE-2025-29927 umožňuje obísť kontroly autorizácie v rámci inštancií Next.js, ak kontroly prebiehajú v Middleware a aplikácie používajú funkciu *next start* s parametrom *output: 'standalone'*.

Kritická aktívne zneužívaná zraniteľnosť Google Chrome

Google opravil kritickú zraniteľnosť vo svojom prehliadači Chrome pre Windows, ktorá umožňuje únik zo sandboxu. Zraniteľnosť je aktívne zneužívaná. Spoločnosť Google opravila kritickú zraniteľnosť s označením CVE-2025-2783 vo verzii svojho prehliadača pre Windows, ktorá kvôli logickej chybe na rozhraní prehliadača a OS umožňuje únik z jeho sandboxu. Nachádza sa v komponente Mojo.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

VMware Tools pre Windows umožňuje obísť autentifikáciu

Vývojári VMware Tools pre Windows opravili vo svojom produkte zraniteľnosť vysokej závažnosti, ktorá umožňuje obídenie autentifikácie a získanie oprávnení administrátora pre isté úkony v rámci kompromitovaného virtuálneho prostredia.

Kritická zraniteľnosť Mozilla Firefox

Spoločnosť Mozilla opravila kritickú chybu vo svojom prehliadači Firefox, ktorá v OS Windows umožňuje vykonať únik zo sandboxu prehliadača. Zraniteľnosť sa podobá na CVE-2025-2783, ktorú v súčasnosti opravila spoločnosť Google vo svojom prehliadači Chrome.

Kritická zraniteľnosť tlačiarní Canon

Spoločnosť Canon opravila kritickú zraniteľnosť s označením CVE-2025-1268 v ovládačoch viacerých svojich zariadení, ktorá umožňuje znefunkčniť tlač, a potenciálne vykonať ľubovoľný kód.

MESAČNÍK ZRANITEĽNOSTÍ MAREC 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2233.html