CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JÚN 2026

TLP: CLEAR

Kybernetickým priestorom v júni 2026 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Nová phishingová kampaň imituje služby Ministerstva vnútra SR

VJ CSIRT získala informácie o nových podvodných webstránkach, ktoré sa snažia napodobniť dizajn a funkcie oficiálnych elektronických služieb a organizácií spadajúcich pod Ministerstvo vnútra SR.

2 FortiBleed: únik prihlasovacích údajov do FortiGate VPN na viac ako 430 000 zariadeniach

VJ CSIRT na základe zistení bezpečnostných výskumníkov zo spoločnosti SOCRadar opakovane upozorňuje na rozsiahlu kampaň označovanú ako FortiBleed, ktorá sa zameriava na zariadenia Fortinet FortiGate.

3 Variant „Miasma“ malvéru Shai-Hulud kompromitoval NPM balíky cez útok na dodávateľský reťazec

Útočníci kompromitovali viac ako 30 npm balíkov z @redhat-cloud-services a vložili do nich novú verziu malvéru Shai-Hulud s názvom Miasma.

4 Europol zaistil servery asociované s botnetom SocGholish a ruskou Evil Corp

Holandská polícia s partnermi v rámci operácie Endgame odstránila malvér SocGholish z takmer 15 000 kompromitovaných webových stránok a odstavila viac ako 100 serverov používaných na jeho distribúciu.

5 Ruské spravodajské služby získavajú kryptografické kľúče na obnovenie zálohy Signalu

FBI a CISA upozorňujú, že ruské spravodajské skupiny rozšírili phishingovú kampaň proti používateľom aplikácie Signal.

6 Mozilla 0DIN demonštrovala kompromitáciu vývojárskeho zariadenia cez repozitár GitHub

Výskumníci z Mozilla 0DIN upozornili na novú techniku útoku, pri ktorej útočníci zneužívajú bezpečné GitHub repozitáre na oklamanie AI nástrojov na programovanie, ako sú Claude Code či podobní agenti.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

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

Aj v júni sa objavili prípady phishingových e-mailov, ktoré šírili malvér Agent Tesla, ktorý slúži ako trójsky kôň pre vytvorenie vzdialeného prístupu ku infikovanému zariadeniu. Napriek svojmu veku (prvýkrát bol pozorovaný v roku 2014) je stále obľúbený.

Kuriózny phishingový prípad predstavovala vzorka spear-phishingového e-mailu, ktorá prišla zamestnancovi organizácie a v ktorom útočník zneužil totožnosť generálneho riaditeľa cieľovej organizácie. Po zamestnancovi požadoval vybavenie nešpecifikovanej záležitosti, ktorú by pravdepodobne komunikoval v ďalšom kroku. Žiadal komunikáciu výhradne e-mailom, čo zdôvodnil tým, že sa nachádza na prebiehajúcej schôdzi. E-mail prišiel z domény ruskej mailovej služby.

CSIRT.SK prijal od partnera hlásenie s predmetom "Podozriva sprava sms s vyzvou na zaplatenie pokuty spojene s prevadzkou OMV". Išlo o phishing šírený formou SMS (tzv. smishing). Po analýze priloženej URL adresy kontaktovala jednotka správcov IP adresného rozsahu a požiadala o odstránenie problémového obsahu. Kampaň postupne narastala a používala pre podvodný obsah ďalšie a ďalšie URL adresy. Jednotka o kampani a hláseniach občanov informovala aj Ministerstvo vnútra SR, ktorého meno kampaň zneužívala. Predmetná kampaň mala vizuálne spracovanie napodobňujúce dizajn legitímnych služieb a organizácií spadajúcich pod Ministerstvo vnútra SR. CSIRT.SK vydal na svojom webe varovanie. Získané indikátory kompromitácie zdieľal s partnermi v rámci ochrany siete Govnet.

V júni zaznamenala organizácia v konštituencii CSIRT.SK opakované neúspešné pokusy o prienik do svojho informačného systému, resp. prihlásenie cez VPN. IP adresy, z ktorých pokusy prebiehali, v rámci vlastného prostredia zablokovala. Jednotka incident analyzovala, zozbierala indikátory kompromitácie, a tieto zdieľala s partnermi s cieľom ochrany siete Govnet.

V medzinárodnom priestore prebehla v júni akcia holandskej polície s partnermi z viacerých krajín, nazvaná Operation Endgame, ktorá viedla ku zneškodneniu botnetu „SocGholish“. SocGholish zneužíval ukradnuté prihlasovacie údaje na prístup do administrátorských rozhraní CMS WordPress, ktoré infikoval škodlivým kódom JavaScript. Infikované stránky WordPress návštevníkov presmerovali na stránky útočníkov, kde im zobrazovali falošné upozornenia na potrebu aktualizácie prehliadača. Ak si obeť stiahla a spustila falošný inštalátor, došlo ku infekcii škodlivým softvérom s rôznou funkcionalitou podľa zámerov útočníkov, napríklad krádež prihlasovacích údajov, alebo nasadenie ransomvéru. Holandské úrady poskytli jednotke zoznam webových stránok relevantných pre jej konštituenciu. CSIRT.SK kontaktovala zástupcov zasiahnutých organizácií a upozornila na bezpečnostnú hrozbu. Poslala tiež podrobný postup, ako skontrolovať a nakonfigurovať WordPress, ako aj čo robiť pri podozrení na zneužitie alebo kompromitáciu.

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.

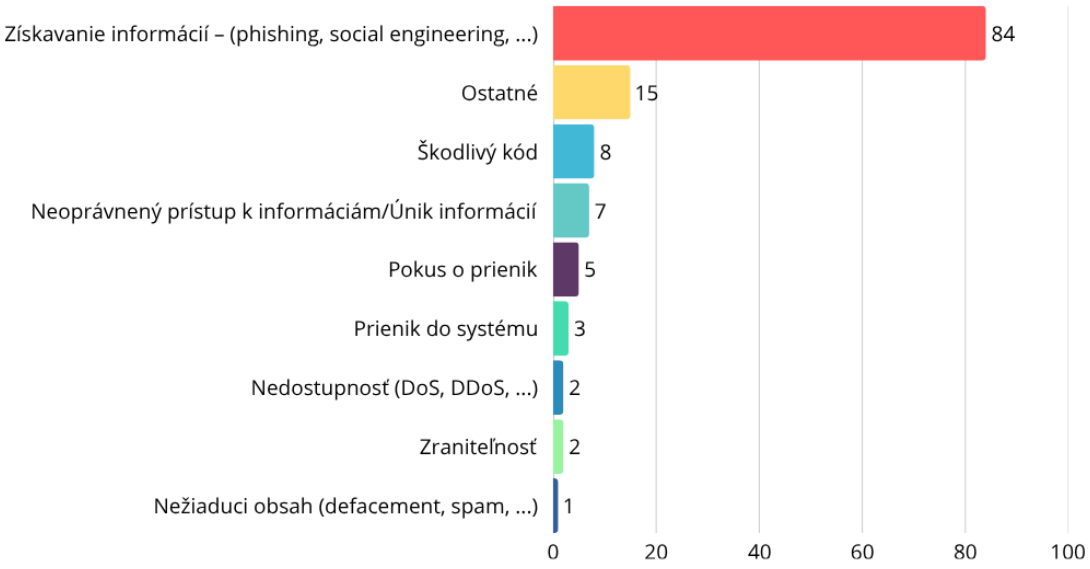
V rámci služby Ares prebiehali penetračné testy piatich webových aplikácií, o ktoré nás požiadali organizácie verejnej správy. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

V júni objavil bezpečnostný výskumník CSIRT.SK dve zraniteľnosti v tiketovacom systéme OTRS Community- kritickú zraniteľnosť CVE-2026-48188, ktorá umožňuje vykonávať útoky typu SQL injection a vysoko-závažnú CVE-2026-48208, ktorá dovoľuje spôsobiť nedostupnosť systému.

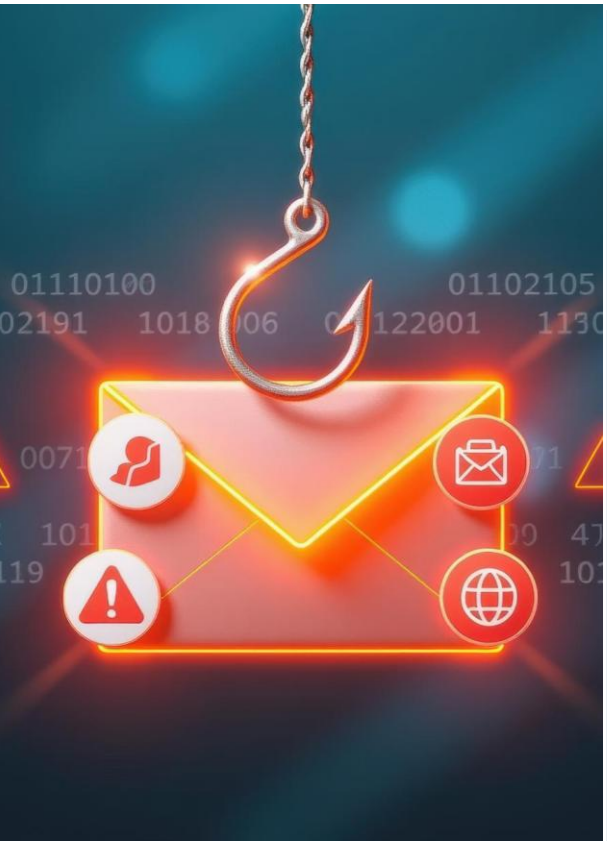
CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných škôl. V júni jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Štatistického úradu SR v Nitre a Bratislave. Študentom prednášala na Základnej škole v Terni, Strednej zdravotníckej škole Moyzesova 17 v Košiciach, Spojenej škole v Sečovciach a študentom a učiteľom na SOŠ polytechnickej DSA v Nitre a Strednej odbornej škole v Snine. Prednášku si vypočuli aj učitelia zo Strednej priemyselnej školy v Považskej Bystrici a SOŠ stavebnej v Nitre.

Členovia tímu CSIRT.SK sa v júni zúčastnili Workshopov kybernetickej bezpečnosti, ktoré usporiadalo MIRRI SR vo všetkých krajských mestách Slovenska. V prednáške sa zamerali na najčastejšie spôsoby prieniku do IT infraštruktúr verejných organizácií, ktoré vo svojej každodennej praxi pozorujú. Účastníkom demonštrovali ukážky takýchto útokov a prezentovali rôzne služby, ktoré im vie bezplatne poskytnúť CSIRT.SK v rámci prevencie, ale aj reakcii na už vzniknutý incident.

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



VÝZNAMNÉ UDALOSTI VO SVETE



Nová phishingová kampaň imituje služby Ministerstva vnútra SR

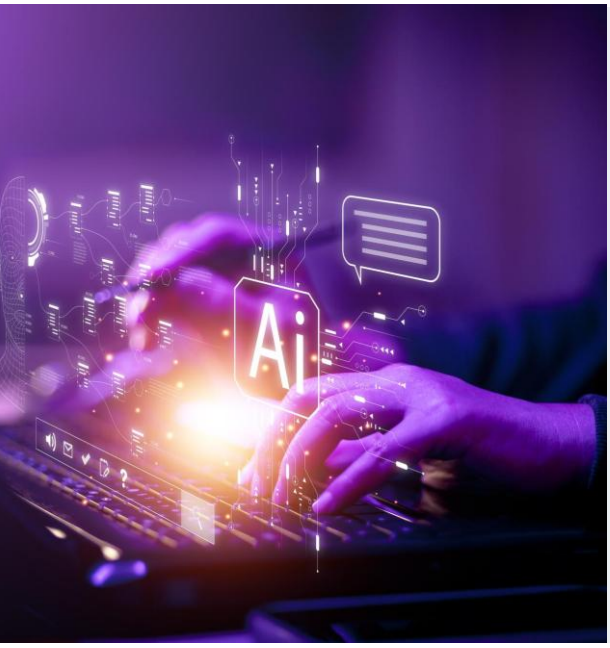
VJ CSIRT získala informácie o nových podvodných webstránkach, ktoré sa snažia napodobniť dizajn a funkcie oficiálnych elektronických služieb a organizácií spadajúcich pod Ministerstvo vnútra SR. Ide o novú phishingovú/smishingovú kampaň, kedy potencionálna obeť príjme SMS správu oznamujúcu uloženie pokuty za dopravný priestupok. Správa obsahuje manipulatívne prvky urgencie a nátlaku. Odosielateľmi nahlásených SMS správ boli telefónne čísla zväčša so zahraničnou predvoľbou (Maroko a Filipíny), z ktorých Ministerstvo vnútra SR nekomunikuje.

Na základe uvedených a ďalších zistení je možné konštatovať, že ide o škodlivú aktivitu s pravdepodobným cieľom získavania citlivých údajov od občanov SR, vrátane údajov finančného charakteru s rizikom finančnej škody. VJ CSIRT na svojom webe vydala varovanie a naďalej sleduje pokračujúcu phishingovú kampaň.

FortiBleed: únik prihlasovacích údajov do FortiGate VPN, vyše 430 000 zariadení po celom svete

VJ CSIRT na základe zistení bezpečnostných výskumníkov zo spoločnosti SOCRadar opakovane upozorňuje na rozsiahlu kampaň označovanú ako FortiBleed, ktorá sa zameriava na zariadenia Fortinet FortiGate. Jedná sa o globálnu vlnu kompromitácií firewallov Fortinet. Úniky obsahujú prihlasovacie údaje k VPN a firewallom FortiGate pre približne 430 000 zariadení po celom svete (report spoločnosti SOCRadar hovorí o 194 krajinách). Databáza zahŕňa používateľské mená, e-mailové adresy a v niektorých prípadoch aj heslá v čitateľnej podobe. Spoločnosť Fortinet uviedla, že nejde o novú zraniteľnosť ani nové úniky. Analýza kampane naznačuje, že útočníci primárne využívajú kompromitované alebo opakovane používané prihlasovacie údaje získané z predchádzajúcich únikov dát a úspešných útokov na heslá hrubou silou. Iné analýzy však hovoria aj o zbere prihlasovacích údajov, ktorý započal v máji 2026. Kampaň proti FortiGate VPN môže byť súčasťou širšieho zberu prihlasovacích údajov pre viaceré technológie.

VÝZNAMNÉ UDALOSTI VO SVETE

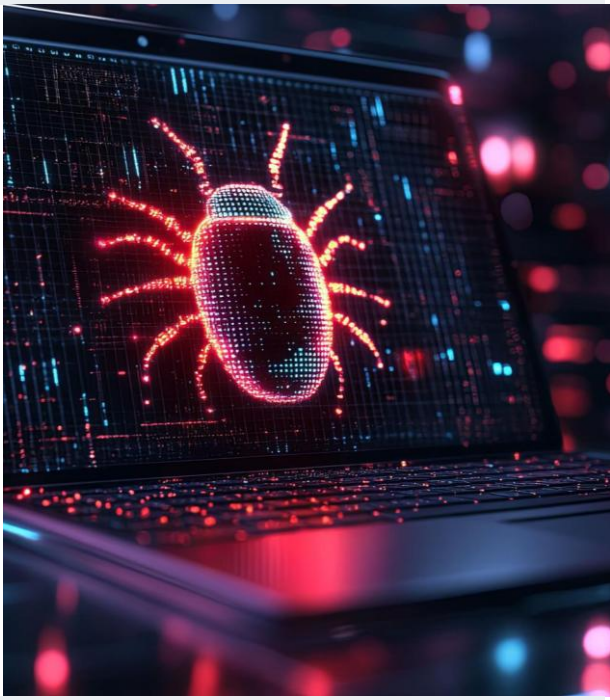


Nová technika ChatGPhish zneužíva dôveru OpenAI a referencovanie URL a obrázkov

Výskumníci z Permiso Security odhalili techniku nazvanú ChatGPhish, ktorá zneužíva spôsob, akým ChatGPT spracováva a zobrazuje obsah webových stránok pri ich sumarizácii. Útočník môže do stránky vložiť skryté inštrukcie, phishingové odkazy, obrázky alebo QR kódy, ktoré sa následne zobrazia v odpovedi ChatGPT ako dôveryhodný obsah. Používateľ tak môže byť presvedčený, že varovanie alebo odkaz pochádza od samotného asistenta, hoci ide o obsah kontrolovaný útočníkom. Výskumníci upozorňujú, že nejde o klasickú kompromitáciu ChatGPT, ale o útoky typu prompt injection, pri ktorých útočníci zneužívajú dôveru používateľov v odpovede generované pomocou AI, čím vzniká nový priestor pre phishing a sociálne inžinierstvo.

Variant „Miasma“ malvéru Shai-Hulud kompromitoval NPM balíky *@redhat-cloud-services* v rámci útoku na dodávateľský reťazec

Útočníci kompromitovali viac ako 30 npm balíkov z @redhat-cloud-services a vložili do nich novú verziu malvéru Shai-Hulud s názvom Miasma. Škodlivý kód počas inštalácie vyhľadával a exfiltroval prihlasovacie údaje, autentifikačné tokeny, SSH kľúče a ďalšie tajomstvá z vývojárskych staníc a prostredí CI/CD. Výskumníci pripisujú útok širšej vlne kampaní na dodavateľské reťazce, ktoré v posledných týždňoch zasiahli aj ďalšie známe projekty s otvoreným zdrojovým kódom. Spoločnosť Red Hat po odhalení incidentu odstránila kompromitované verzie balíkov, začala vyšetrovanie a odporučila používateľom aktualizovať závislosti, preveriť systémy na prítomnosť škodlivého kódu a rotovať všetky potenciálne kompromitované prihlasovacie údaje.



Nová DoS technika HTTP/2 Bomb umožňuje zneprístupnenie služby najpoužívanejších webových serverov

Bezpečnostní výskumníci predstavili novú techniku pre vyvolanie odmietnutia služby s názvom HTTP/2 Bomb. Útok kombinuje zneužitie kompresie hlavičiek HPACK a mechanizmus podobný útoku Slowloris s cieľom prudko zvýšiť spotrebu pamäte webových serverov a udržať ju na vysokej úrovni. Zasahuje predvolené konfigurácie serverov NGINX, Apache HTTP Server, Microsoft IIS, Envoy a Cloudflare Pingora a dokáže ich znefunkčniť. Odborníci preto odporúčajú nasadiť opravy, obmedziť počet hlavičiek v požiadavkách alebo dočasne vypnúť HTTP/2 na zasiahnutých systémoch.

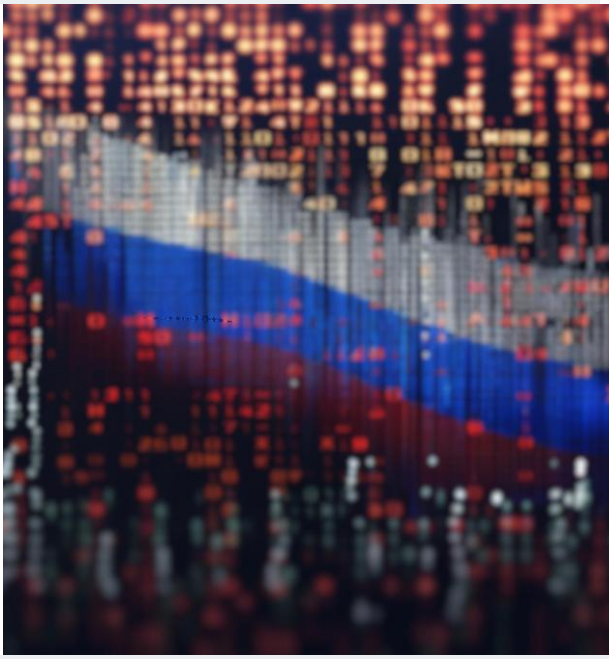
VÝZNAMNÉ UDALOSTI VO SVETE

Čínske skupiny kompromitujú české a taiwanské systémy malvérom Azureveil

Bezpečnostní výskumníci odhalili novú špionážnu kampaň, ktorá dostala názov Operation Dragon Weave. Skupiny spojené s Čínou cielia na vládnych predstaviteľov a občanov v Českej republike a na Taiwane. Útočníci využívajú phishingové správy na doručenie malvéru AdaptixC2 a na skryté riadenie kompromitovaných zariadení nasadzujú infraštruktúru Azureveil postavenú na službách Microsoft Azure. Kampaň sa zameriava na dlhodobý prístup k systémom a zber spravodajských informácií, pričom využíva legitímne cloudové služby na maskovanie škodlivej komunikácie a sťaženie detekcie. Aktivita zapadá do širšieho trendu rastúcej kyberšpionáže zo strany čínskych skupín voči štátnym inštitúciám, kritickej infraštruktúre a strategickým sektorom.

Ruská skupina Gamaredon zneužíva chybu vo WinRAR na šírenie malvéru proti Ukrajine

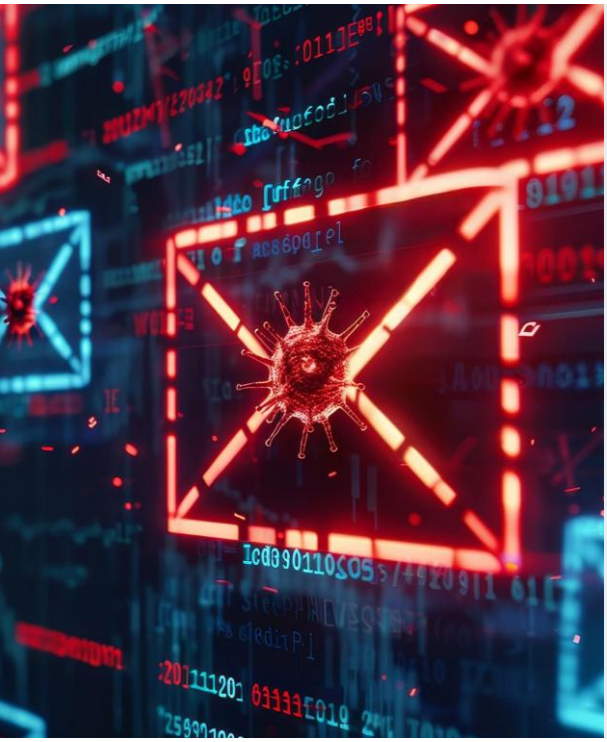
Ruská hackerská skupina Gamaredon zneužíva zraniteľnosť CVE-2025-8088 vo WinRAR na doručovanie škodlivých nástrojov GammaWorm a GammaSteel v rámci špionážnej kampane zameranej na ukrajinské organizácie. Útočníci rozosielajú podvrhnuté RAR archívy, ktoré po otvorení zneužijú chybu na prechádzanie adresármi a umiestnia škodlivý súbor do priečinka Windows Startup. Následne sa spustí viacstupňový reťazec s komponentmi GammaPhish a GammaLoad, ktoré sťahujú ďalší malvér zo serverov útočníkov. GammaWorm zaisťuje perzistenciu a šírenie cez sieťové zdieľania a USB, pričom dokáže spúšťať ďalší kód, zatiaľ čo GammaSteel kradne dáta a zbiera informácie o napadnutom systéme.



Japonské spoločnosti Toshiba a Muji varujú pred phishingovými rozhraniami generovanými prostredníctvom skriptov na polyfill[.]io

Návštevníci webov Toshiba a Muji si začali všímať podozrivé prihlasovacie okná, ktoré nepatrili priamo týmto stránkam, ale vznikali cez externý JavaScript z CDN služby *polyfill[.]io*. Táto služba v niektorých prípadoch vracala HTTP autentifikačné požiadavky, ktoré prehliadač zobrazil ako prihlasovací formulár, čím si od používateľa vyžiadala prihlasovacie údaje. Doména polyfill[.]io je od roku 2024 spájaná so šírením škodlivého kódu, pričom rovnaké správanie zaznamenali aj iné subjekty vrátane ďalších japonských organizácií, a útoky sa objavili aj na platforme Samsung Smart TV. Pôvodný tvorca medzitým migroval službu na domény polyfill.com a polyfill.top.

VÝZNAMNÉ UDALOSTI VO SVETE



Falošné upozornenia od Microsoft šíria malvér cez sociálne inžinierstvo a útoky ClickFix

Výskumníci odhalili kampane, v ktorých útočníci využívajú falošné bezpečnostné upozornenia spoločnosti Microsoft ako návnadu na distribúciu malvéru. Používatelia sa dostanú na stránky, ktoré napodobňujú hlásenia Windows alebo Microsoft 365 a tvrdia, že zariadenie je infikované alebo potrebuje urgentnú opravu. Po kliknutí na „opravu" alebo stiahnutie nástroja sa do systému dostane malvér. Často ide o infostealery alebo trójske kone na krádež hesiel, kryptopeňaženiek a ďalších dát. Niektoré kampane využívajú aj techniky typu ClickFix, kde obeť sama spustí príkazy v systéme podľa inštrukcií z falošného vyskakovacieho okna, čím si nechtiac nainštaluje škodlivý kód. Microsoft a bezpečnostní experti upozorňujú, že tieto útoky stoja skôr na sociálnom inžinierstve, než na softvérových zraniteľnostiach a spoliehajú sa na vyvolanie pocitu strach a urgentnosti.

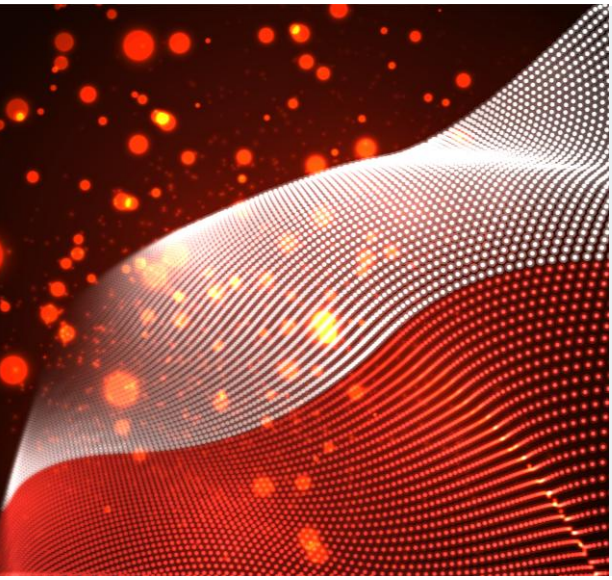
Europol v rámci operácie Endgame zaistil vyše 106 serverov asociovaných s botnetom SocGholish a ruskou Evil Corp

Holandská polícia spolu s partnermi v rámci operácie Endgame odstránila malvér SocGholish z takmer 15 000 kompromitovaných webových stránok a odstavila viac ako 100 serverov používaných na jeho distribúciu. SocGholish sa šíri cez falošné aktualizácie prehliadačov a slúži na získanie počiatočného prístupu do napadnutých systémov, kde často pripravuje pôdu pre ďalší malvér vrátane ransomvéru. Operácia výrazne narušila infraštruktúru jednej z najrozšírenejších malvérových kampaní súčasnosti.

Ransomvérová skupina The Gentlemen vyvíja riešenia na deaktiváciu systémov EDR

Ransomvérová skupina (RaaS) The Gentlemen používa vlastnú platformu GentleKiller, ktorá slúži ako súbor nástrojov na vypínanie EDR/antivírusovej ochrany pred samotným šifrovaním. Systém má minimálne osem variantov, ktoré napodobňujú legitímny bezpečnostný softvér a zneužívajú tzv. techniku BYOVD (Bring Your Own Vulnerable Driver) na získanie oprávnení na úrovni jadra, čo im umožňuje vypnúť ochranné mechanizmy. Nástroje sú poskytované priamo pridruženým partnerom a cielia na viac ako 400 bezpečnostných procesov v približne 48 produktoch. Nástroje kombinujú impersonáciu legitímnych dodávateľov, podpísané či packované binárky a rýchle zneužívanie nových zraniteľností na obídenie bezpečnostných systémov.

VÝZNAMNÉ UDALOSTI VO SVETE

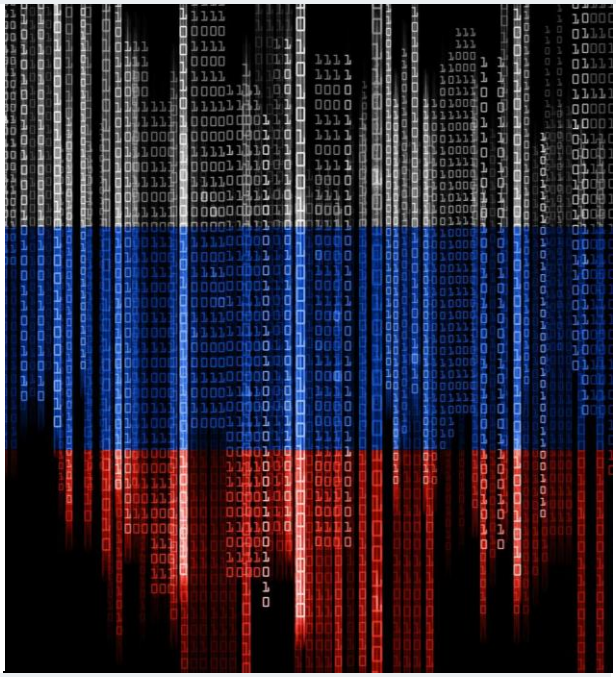


Poľské úrady zatkli 4 členov skupiny špecializujúcej sa na SIM-swappingové útoky

Poľské úrady zadržali štyroch členov organizovanej skupiny podozrivej z rozsiahlych útokov typu SIM-swapping, pri ktorých útočníci prenikali do systémov partnerov telekomunikačných operátorov a kompromitovali e-mailové účty ich zamestnancov. Cieľom bolo získať údaje potrebné na neoprávnené prevzatie telefónnych čísel obetí. Následne zachytávali SMS správy a e-maily, čím získali prístup ku pridruženým kryptomenovým účtom. Zadržaní čelia obvineniam z účasti v organizovanej zločineckej skupine, neoprávneného prístupu k informačným systémom, krádeže a prania špinavých peňazí.

Ruské spravodajské služby získavajú prostredníctvom phishingových kampaní kryptografické kľúče na obnovenie zálohy Signalu

FBI a CISA upozorňujú, že ruské spravodajské skupiny rozšírili phishingovú kampaň proti používateľom aplikácie Signal. Namiesto prihlasovacích kódov a PIN kódov sa teraz snažia vylákať obnovovacie kľúče záloh (*Backup Recovery Keys*), ktoré im umožnia obnoviť zálohu účtu, získať prístup k celej histórii správ a prevziať kontrolu nad účtom. Útočníci sa vydávajú za podporu Signalu a cielia najmä na vládnych predstaviteľov, vojakov, politikov, novinárov a ďalšie osoby s vysokou spravodajskou hodnotou. FBI odporúča používateľom, aby obnovovacie kľúče nikdy nezdieľali, ignorovali podozrivé správy a v prípade podozrenia okamžite vygenerovali nový obnovovací kľúč v nastaveniach aplikácie.



Mozilla 0DIN demonštrovala kompromitáciu vývojárskeho zariadenia prostredníctvom repozitára GitHub spracovaného AI asistentom

Výskumníci z Mozilla 0DIN upozornili na novú techniku, pri ktorej útočníci zneužívajú bezpečné repozitáre GitHub na oklamanie nástrojov AI na programovanie, akým je napríklad Claude Code. Repozitár neobsahuje škodlivý kód, no zámerne vyvolá chybu pri inštalácii, ktorá AI asistenta navedie na spustenie ďalších príkazov. Tie následne stiahnu a vykonajú škodlivý kód uložený mimo repozitára, čím útočník získa vzdialený prístup k zariadeniu vývojára. Technika obchádza bežné bezpečnostné kontroly, pretože samotný repozitár pôsobí dôveryhodne a škodlivý obsah sa objaví až počas automatického riešenia chyby AI agentom. Výskumníci odporúčajú, aby vývojári dôkladne kontrolovali príkazy navrhované nástrojmi AI a obmedzili ich oprávnenia pri práci s neznámymi projektmi.

VÝZNAMNÉ UDALOSTI VO SVETE

Phishingová kampaň cielená na ubytovacie zariadenia šíri škodlivé archívy ZIP obsahujúce malvér v Node.js

Spoločnosť Microsoft upozornila na phishingovú kampaň zameranú na hotely a ďalšie organizácie v sektore pohostinstva v Európe a Ázii. Útočníci rozosielajú e-maily s údajnými sťažnosťami hostí, rezerváciami alebo fotografiami izieb a do správ prikladajú archívy ZIP, ktoré obsahujú škodlivé súbory vydávajúce sa za obrázky. Po otvorení archívu sa spustí viacstupňový reťazec infekcie, ktorý nainštaluje malvér TonRAT písaný v Node.js. Ten zabezpečí útočníkom trvalý prístup k zariadeniu. Umožní im sťahovať ďalší škodlivý kód, zbierať informácie o systéme a komunikovať s riadiacimi servermi. Microsoft odporúča organizáciám monitorovať podozrivé spúšťanie skriptov PowerShellu a Node.js, kontrolovať zmeny v nastaveniach Microsoft Defendera a venovať zvýšenú pozornosť e-mailom s nečakanými prílohami ZIP.

VÝZNAMNÉ UDALOSTI VO SVETE

- Holandské úrady a NCSC rozložili masívny botnet Asocks.
- Vibe coding vytvára novú bezpečnostnú hrozbu - Shadow Builders.
- Anthropic potvrdil plány pre sprístupnenie modelov Mythos.
- Kampaň kompromitujúca stránky WordPress zneužíva neviditeľné znaky Unicode a komentáre cez účty Steam Community v rámci komunikácie C&C.
- Škodlivý nástroj Codexui-android sa zameriava na krádež autentifikačných tokenov pre OpenAI Codex.
- Hackeri zneužili AI podporu od spoločnosti Meta na krádež Instagramových účtov.
- USA varuje pred hackerskými útokmi na verejne dostupné systémy pre monitoring a správu palív a úložísk tekutého materiálu.
- Europol s partnermi v rámci operácie KRATOS 2 rozložil nelegálne streamovacie platformy.
- Francúzske a španielske úrady rozložili online platformu na výrobu falošných dokladov.
- WhatsApp zastavil novú phishingovú kampaň spyvéru Pegasus.
- Útočníci prenikli do francúzskej vládnej komunikačnej platformy Tchap.
- Južná Kórea udelila historicky najvyššiu pokutu za porušenie ochrany osobných údajov.
- Čínska špionážna skupina prenikla do autentifikačnej infraštruktúry a udržala si do nej prístup desať rokov.
- Americká vláda nariadila spoločnosti Anthropic zablokovať prístup cudzincov k pokročilým modelom AI (Fable 5 a Mythos 5) z dôvodu obáv o národnú bezpečnosť.
- FBI upozorňuje na rastúci trend investičných kryptopodvodov.
- Bitdefender varuje pred kampaňou cez WhatsApp s tematikou rezervácií v ubytovacích zariadeniach.
- OxLoader obchádza bezpečnostné kontroly zneužívaním presmerovaní .reloc a šíri malvér CASTLESTEALER cez škodlivé reklamy Google Ads.
- Kanadská spravodajská služba získala historicky prvý súdny príkaz na čistenie infikovaných zariadení.

- Europol s partnermi v rámci operácie Endgame narušil infraštruktúru malware-as-a-service Amadey a StealC.
- Kryptoburza Polymarket odškodní svojich zákazníkov, ktorí sa stali obeťami útoku na dodávateľský reťazec.
- Rusko zneužívalo forenzné nástroje Cellebrite na kompromitáciu zariadení iPhone.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť Palo Alto Networks PAN-OS umožňuje obísť prihlasovanie

Spoločnosť Palo Alto Networks opravila aktívne zneužívanú zraniteľnosť v riešení GlobalProtect v PAN-OS a Prisma Access, ktorá umožňuje neautentifikovaným vzdialeným útočníkom podvrhovať súbory cookies pre prihlásenie prostredníctvom funkcie „Authentication Override“ a vytvárať tak neautorizované spojenia VPN.

Google opravil aktívne zneužívanú zraniteľnosť prehliadača Chrome

Spoločnosť Google Chrome vydala bezpečnostné aktualizácie, ktoré opravujú 74 zraniteľností. Z nich jedna je aktívne zneužívaná zero-day zraniteľnosť. CVE-2026-11645 sa nachádza v nástroji JavaScript V8 a umožňuje útočníkovi čítať a zapisovať mimo vyhradenú pamäť, čo môže viesť k možnosti vykonávať škodlivý kód.

SAP opravil v júni kritické zraniteľnosti v NetWeaveri a Commerce Cloud

Spoločnosť SAP vydala bezpečnostné aktualizácie systémov SAP NetWeaver a SAP Commerce Cloud, ktoré opravujú 15 zraniteľností, z čoho 4 sú označené ako kritické.

Kritická zraniteľnosť Veeam Backup & Replication

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoj produkt Backup & Replication, ktoré opravujú kritickú zraniteľnosť. CVE-2026-44963 umožňuje doménovému používateľovi vzdialené vykonanie kódu na zálohovacom serveri.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti v UniFi OS umožňujú prevzatie kontroly nad serverom

Spoločnosť Ubiquiti opravila kritické zraniteľnosti viacerých zariadení v platforme UniFi OS. Zreťazenie troch z nich umožňuje vzdialenému neautentifikovanému útočníkovi získať v systéme reverzný shell s oprávneniami používateľa root prostredníctvom jedinej špeciálne vytvorenej HTTP požiadavky.

Aktívne zneužívaná kritická zraniteľnosť Check Point Remote Access VPN, Mobile Access SSL/VPN a Spark Firewall

Spoločnosť Check Point opravila aktívne zneužívanú kritickú zraniteľnosť produktov Remote Access VPN, Mobile Access SSL/VPN a Spark Firewall, ktorá umožňuje obísť autentifikáciu a vytvárať VPN relácie. Chyba zabezpečenia vyplýva z logickej chyby pri validácii certifikátov v rámci protokolu IKEv1.

Kritické zraniteľnosti v produkte Ivanti Sentry

Spoločnosť Ivanti vydala bezpečnostné aktualizácie na svoj produkt Ivanti Sentry, ktoré opravujú dve kritické zraniteľnosti. Zraniteľnosti umožňujú získanie administrátorských oprávnení a schopnosti vykonávať vzdialene kód.

Kritická zraniteľnosť Splunk Enterprise umožňuje vzdialene vykonávať kód

Spoločnosť Splunk vydala bezpečnostné aktualizácie pre kritickú zraniteľnosť v Splunk Enterprise, ktorá umožňuje neautentifikovaným útočníkom manipulovať s databázou PostgreSQL, vykonávať operácie so súbormi a zneužitím viacerých koncových bodov dosiahnuť vzdialené vykonanie kódu.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Júnový Microsoft Patch Tuesday opravil šesť zero-day zraniteľností, jedna je aktívne zneužívaná

Spoločnosť Microsoft vydala v júni 2026 balík opráv pre portfólio svojich produktov opravujúci 203 zraniteľností, z ktorých 33 spoločnosť označila ako kritické. Tieto umožňujú vzdialene vykonávať kód, získať citlivé informácie a eskalovať oprávnenia. Šesť opravených zraniteľností je typu zero-day a jedna z nich je aktívne zneužívaná. Tieto umožňujú eskalovať oprávnenia útočníka, obchádzať bezpečnostné prvky, zneprístupniť službu a vykonávať techniky spoofingu.

Aktívne zneužívaná zraniteľnosť Cisco Catalyst SD-WAN Manager

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu produktu Catalyst SD-WAN Manager, ktorá opravuje aktívne zneužívanú zraniteľnosť CVE-2026-20262 vo webovom používateľskom rozhraní. Chyba zabezpečenia umožňuje autentifikovanému útočníkovi vytvárať a prepisovať súbory v systéme a následne získať oprávnenia používateľa root.

Zraniteľnosti v protobufjs ohrozujú dátové a AI systémy

Výskumníci zo spoločnosti Cyera objavili šesť zraniteľností v knižnici protobufjs, ktorá patrí medzi najpoužívanejšie JavaScript implementácie formátu Protocol Buffers a tvorí základ komunikácie v cloudových službách, databázach, AI platformách a distribuovaných aplikáciách.

Kritické zraniteľnosti NGINX umožňujú znefunkčniť službu a vykonávať kód

Spoločnosť F5 vydala bezpečnostné aktualizácie na opravu dvoch kritických zraniteľností v produktoch NGINX, ktoré môžu v niektorých konfiguráciách umožniť vzdialenému útočníkovi vyvolať zlyhanie služby (DoS) alebo spustiť škodlivý kód.

MESAČNÍK ZRANITEĽNOSTÍ JÚN 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3802.html