CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JÚL 2025

TLP: CLEAR

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

1 Upozorňujeme na phishingovú kampaň zneužívajúcu meno VŠZP

VJ CSIRT upozorňuje na pretrvávajúce útoky, ktoré cielia na poistencov Všeobecnej zdravotnej poisťovne. Tieto útoky majú formu phishingových e-mailov s podvodnými odkazmi.

2 VJ CSIRT spolupracuje pri zásahu v Dnipre (Ukrajina) pre bombové hrozby na školách

VJ CSIRT (v gescii SKB MIRRI SR) sa aktívne podieľala na riešení mimoriadne závažného bezpečnostného incidentu v úzkej spolupráci s Národnou centrálou osobitných druhov kriminality (NCODK), Protiteroristickou centrálou, Národnou centrálou proti terorizmu, extrémizmu a kybernetické kriminalite SKPV (ČR), Protizločineckou jednotkou ÚBOK a Kybernetickou políciou Ukrajiny.

3 Česká nemocnica v Nymburgu sa stala obeťou ransomvérového útoku

Česká nemocnica v Nymburku sa stala obeťou ransomvérového útoku, pri ktorom došlo k zašifrovaniu virtuálnych serverov. Útok spôsobil dočasné výpadky služieb vrátane magnetickej rezonancie či babyboxu.

4 Europol s partnermi rozložili hacktivistickú skupinu NONAME057(16)

Europol a Eurojust 15. júla 2025 v rámci operácie Eastwood rozložili proruskú hacktivistickú skupinu NoName057(16), ktorá od marca 2022 vykonávala početné útoky typu DDoS na kritickú infraštruktúru v Európe, Izraeli a na Ukrajine, vrátane útokov počas španielskych volieb a samitu NATO v Holandsku.

5 Ransomvérová skupina interlock aktívne zneužíva techniku FILEFIX

NeuralTrust odhalil nový typ útoku na veľké jazykové modely (LLM) s názvom Echo Chamber, ktorý využíva techniku zvanú context poisoning. Hackeri v rámci útokov vedúcich k nasadeniu ransomvéru INTERLOCK na šírenie svojich malvérov RAT aktívne zneužívajú techniku FILEFIX.

6 Masívna phishingová kampaň zneužívajúca identitu PyPi cieli na vývojárov

Správca Python Package Index upozornil na prebiehajúcu phishingovú kampaň, ktorá cieli na vývojárov a používateľov PyPI.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

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

V júli riešila VJ CSIRT podnet od občianky, ktorej prišiel e-mail od firmy požadujúcej poplatok za digitálnu infraštruktúru. Jednalo sa o formu podvodu, pri ktorej sa jej autori pokúšajú navodiť dojem, že ide o poplatok, ktorý je súčasťou finančných mechanizmov súvisiacich s informatizáciou verejnej správy, so zabezpečením kybernetickej bezpečnosti digitálnych systémov a rozvojom digitálnych služieb v Slovenskej republike. O tomto podvode už informovalo aj Ministerstvo vnútra SR na svojom Facebookovom účte "Hoaxy a podvody".

Spoločnosť Citrix v rámci svojho bezpečnostného bulletinu informovala v júli o novej kritickej zraniteľnosti v produktoch NetScaler ADC a Gateway označovanej ako „CitrixBleed 2“. Umožňuje neautentifikovanému útočníkovi prečítať obsah pamäte zariadenia čo môže viesť k obídeniu viacfaktorovej autentifikácie (MFA) a úniku citlivých údajov. V tejto súvislosti nás kontaktovala partnerská organizácia a poskytla zoznam organizácií, ktoré majú predmetnú službu prístupnú z internetu. CSIRT.SK preveril stav prevádzkovaných zariadení s cieľom vykonania krokov potrebných pre ich zabezpečenie. Poskytol organizáciám presnú identifikáciu zariadení, konfiguračné nastavenia a verzie, ktorých sa táto zraniteľnosť týkala.

CSIRT.SK sa stretol aj s podvodom v rámci internetovej stránky theoneforyoucz.org, ktorá propagovala platformu EURO Income. Táto jednotlivcom na Slovensku sľubuje možnosť získať značný mesačný príjem prostredníctvom programu s fiktívnou podporou Európskeho parlamentu. Z jej obsahu vyplýva, že cieľom podvodnej kampane je umožniť obyvateľom krajiny „zarobiť svoje prvé peniaze“. Kampaň fiktívne podporoval prezident SR Peter Pellegrini. Používateľov stránka vyzývala, aby vyplnili formulár s osobnými údajmi a zapojili sa do tejto „možnosti generovania príjmu“. Na základe poskytnutých informácií jednotka kontaktovala správcu internetového obsahu a nahlásila podvodnú webovú stránku, aby ju správca deaktivoval.

Jednotka prijala tiež informácie o zraniteľnostiach na webstránkach dvoch organizácií v jej konštituencii, kde vstupné polia pre vyhľadávanie nesprávne spracovávali používateľský vstup. To umožňovalo vykonať útok typu DOM-based Cross-site Scripting (XSS) s následnou možnosťou spustenia ľubovoľného javascript kódu, krádeže relácie, alebo zmeny obsahu stránky. Zraniteľnosti jednotka preverila a kontaktovala správcov webových stránok s odporúčaniami krokov na ich odstránenie.

V júli VJ CSIRT prijala aj výpis s logov neúspešných pokusov o prihlásenia cez VPN do infraštruktúry klientskej organizácie zo zahraničných destinácií. Tieto pokusy boli detegované a zablokované bezpečnostnými zariadeniami. Jednalo sa o jednu z mnohých masívnych kampaní zameraných na tento subjekt. To potvrdili korelácie dodaných indikátorov kompromitácie v podobe útočiacich IP adries s ďalšími incidentami v platforme MISP jednotky CSIRT.SK.

V rámci bezpečnostného monitoringu prijala CSIRT.SK informáciu o aktivite z určitej IP adresy, ktorá patrí do sieťového rozsahu klientskej organizácie CSIRT.SK. Aktivita bola vyhodnotená ako 'port scanner', a táto

bola zameraná na IP adresy z rozsahov pridelených rôznym inštitúciám. Predmetná organizácia preverila danú aktivity so zistením úspešného nelegitímneho pokusu o prihlásenie do svojej infraštruktúry cez SSL-VPN. Vykonala nápravné kroky, vrátane zrušenia kompromitovaného účtu. CSIRT.SK si vyžiadala od organizácie logy, ktoré boli predmetom analýzy za účelom kontroly prípadnej ďalšej aktivity kompromitovaného konta v sieti.

V júli sa podobne ako vo februári tohto roka na Slovensku objavila phishingová kampaň zneužívajúca meno Všeobecnej zdravotnej poisťovne. CSIRT.SK prijala z rôznych zdrojov naprieč verejným sektorom hlásenia tejto aktivity. Na základe dodaných podvodných emailových správ po analýze kontaktovala správcov zneužitého IP adresného rozsahu pre odstránenie podvodného obsahu. Všeobecná zdravotná poisťovňa informovala o tejto kampani svojich klientov na svojom webe.

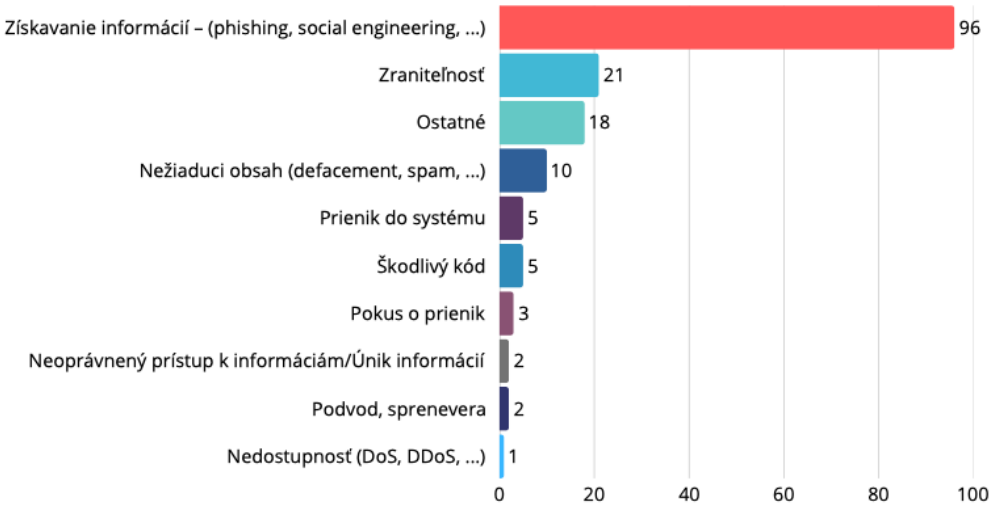
V júli vyvrcholila dlhodobá snaha odhaliť páchateľa masívnej kampane e-mailových bombových hrozieb voči slovenským, českým a litovským školám, fyzickým zásahom medzinárodného slovensko-česko-ukrajinského tímu v ukrajinskom meste Dnipro voči stotožnenému páchateľovi. Jednotka CSIRT.SK počas celej doby poskytovala na požiadanie polícii SR analytickú podporu a významne prispela ku stotožneniu páchateľa.

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 júli sa členovia jednotky zúčastnili Letnej školy kyberkriminality 2025, ktorá sa každoročne koná pod záštitou košickej Univerzity Pavla Jozefa Šafárika.

Členovia tímu CSIRT.SK sa zúčastnili tiež stretnutia so zástupcami českého Národného úradu pre kybernetickú a informačnú bezpečnosť (NÚKIB), organizovaného MIRRI SR, kde si navzájom vymieňali poznatky a skúsenosti z praxe.

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



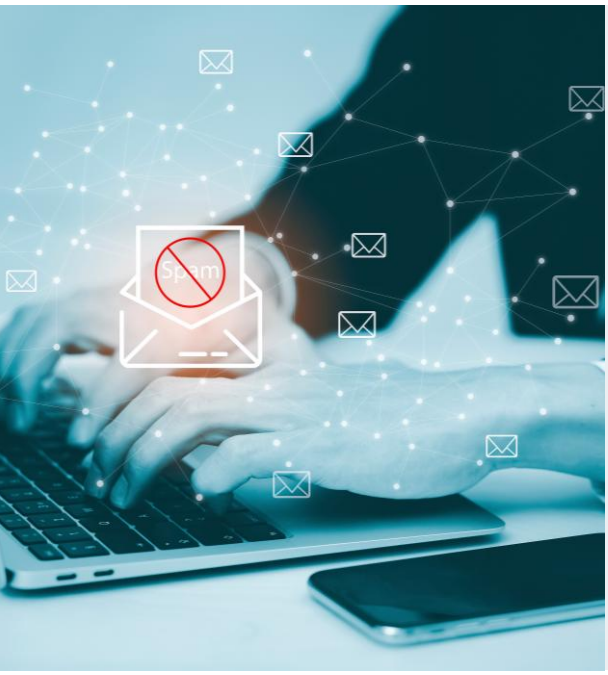
MESAČNÁ SPRÁVA

JÚL 2025

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

VÝZNAMNÉ UDALOSTI VO SVETE



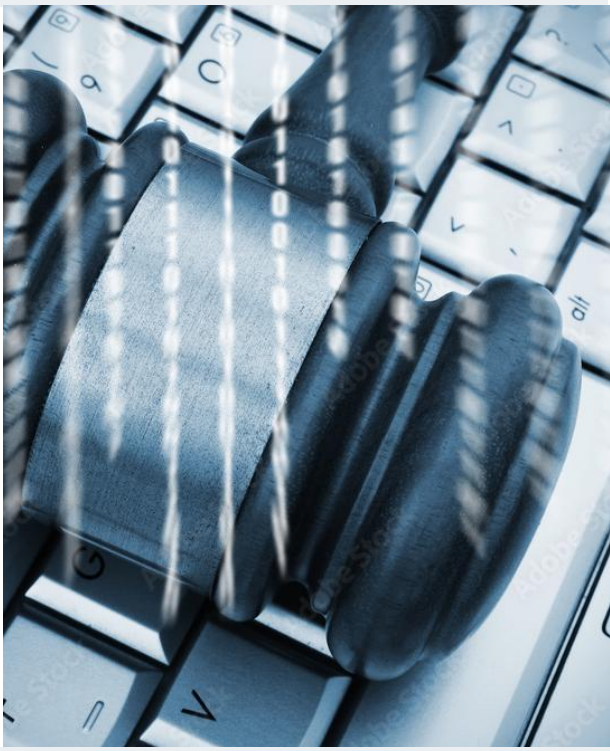
Upozorňujeme na phishingovú kampaň zneužívajúcu meno VŠZP

VJ CSIRT upozorňuje na pretrvávajúce útoky, ktoré sú cielené na poistencov Všeobecnej zdravotnej poisťovne. Tieto útoky majú formu phishingových e-mailov s podvodnými odkazmi.

„Všeobecná zdravotná poisťovňa upozorňuje verejnosť na aktuálnu phishingovú kampaň, v rámci ktorej sa útočníci snažia zneužiť situáciu a dôveru poistencov. Podvodné e-maily informujú o údajnej „novej refundácii“ a obsahujú odkaz na falošnú webovú stránku, ktorá sa na oficiálnu stránku zdravotnej poisťovne podobá. V prípade, ak vám takýto e-mail prišiel, je dôležité neklikať na odkaz v ňom a neposkytovať osobné ani platobné údaje. Odosielateľom týchto e-mailových správ nie je Všeobecná zdravotná poisťovňa.“ – varuje VŠZP na svojom oficiálnom webe.

VJ CSIRT spolupracuje pri zásahu v Dnipre (Ukrajina) pre bombové hrozby na školách

VJ CSIRT (v gescii Sekcie kybernetickej bezpečnosti MIRRI SR) sa aktívne podieľala na riešení mimoriadne závažného bezpečnostného incidentu v úzkej spolupráci s Národnou centrálou osobitných druhov kriminality (NCODK), Protiteroristickou centrálou, Národnou centrálou proti terorizmu, extrémizmu a kybernetické kriminalite SKPV (ČR), Protizločineckou jednotkou ÚBOK a Kybernetickou políciou Ukrajiny. V rámci tejto spolupráce sme poskytli naše odborné kapacity a technické nástroje, ktoré významným spôsobom prispeli k identifikácii a odhaleniu útočníka, ktorý v medzinárodnom meradle šíril bombové hrozby voči viacerým členským štátom Európskej únie. Tento prípad jasne ukázal, aký význam má efektívna koordinácia medzi bezpečnostnými zložkami a technologickými partnermi. Sme hrdí, že sme mohli byť súčasťou tohto medzinárodného tímu, ktorý posilnil bezpečnosť občanov a ochranu verejného poriadku nielen na Slovensku, ale aj v Európe.



New York zavádza povinné hlásenie kybernetických incidentov

New York prijal zákon, ktorý od miestnych vlád a verejných inštitúcií vyžaduje hlásiť kybernetické útoky do 72 hodín a platby výkupného do 24 hodín úradu DHSES. Cieľom je posilniť kybernetickú bezpečnosť, najmä vzhľadom na rastúce hrozby zo strany Iránu, a zlepšiť koordináciu reakcií na útoky. Tento zákon sa týka škôl, nemocníc, dopravných a energetických spoločností a odborníci ho považujú za dôležitý nástroj na prevenciu a rýchlu reakciu na kybernetické incidenty. New York tak vytvára príklad pre ďalšie štáty, ktoré môžu prijať podobné opatrenia.

VÝZNAMNÉ UDALOSTI VO SVETE

Falošné moduly pre Firefox exfiltrujú citlivé údaje a kryptopeňaženky

Viac ako 40 falošných rozšírení v oficiálnom obchode s doplnkami Firefox sa vydáva za populárne kryptomenové peňaženky od dôveryhodných poskytovateľov, s cieľom ukradnúť prihlasovacie údaje k peňaženkám a citlivé informácie. Niektoré z týchto rozšírení predstierajú, že sú peňaženkami od spoločností Coinbase, MetaMask, Trust Wallet, Phantom, Exodus, OKX, Keplr a MyMonero a obsahujú škodlivý kód, ktorý posiela ukradnuté údaje na servery ovládané útočníkmi. Výskumníci zo spoločnosti Koi Security identifikovali tieto rizikové rozšírenia a zistili, že za touto kampaňou stojí rusky hovoriaca skupina. Kampaň je aktívna od apríla 2025. Mozilla podnikla kroky na identifikáciu a odstránenie týchto rozšírení, aby chránila používateľov Firefoxu.

Ransomvérová skupina Hunters International ukončila svoju činnosť

Ransomware-as-a-service Hunters International ukončila svoju činnosť, z leakpage odstránila údaje obetí a obetiam ponúkla sprístupnenie dešifrovacieho kľúča. Podľa výskumníkov z Group-IB sa však môže jednať len o pokus o rebranding skupiny, ktorá nedávno vytvorila skupinu World Leaks, zameriavajúcu sa výhradne na vydieracie operácie. World Leaks využívajú vlastný nástroj na exfiltráciu dát.

Česká nemocnica v Nymburku sa stala obeťou ransomvérového útoku

Česká nemocnica v Nymburku sa stala obeťou ransomvérového útoku, pri ktorom došlo k zašifrovaniu virtuálnych serverov. Útok spôsobil dočasné výpadky služieb vrátane magnetickej rezonancie či babyboxu. Pacientov s potrebou týchto vyšetrení presmerovali do iných zariadení v okolí, pričom zdravotná starostlivosť zostala zabezpečená. Nemocnica prešla do papierového režimu, čo spomalilo administratívu, a dočasne obmedzila prijímanie pacientov. Návrat k plnému digitálnemu fungovaniu potrvá niekoľko dní a nemocnica aktívne spolupracuje s políciou a kybernetickými bezpečnostnými úradmi na vyšetrovaní útoku.

VÝZNAMNÉ UDALOSTI VO SVETE

Nárast phishingového obsahu na doméne .ES

Od štvrtého štvrťroka 2024 do prvého štvrťroka 2025 útočníci výrazne zvýšili zneužívanie španielskej domény najvyššej úrovne .es na phishingové kampane, pričom počet útokov vzrástol až 19-násobne a doména sa zaradila medzi desať najčastejšie zneužívaných. Útočníci používajú druhotné odkazy so subdoménami, ktoré často vyzerajú ako náhodne generované, aby sťažili ich odhalenie. Stránky hostujú na platforme Cloudflare a chránia ich pomocou CAPTCHA Turnstile. Najčastejšie sa zameriavajú na napodobňovanie značky Microsoft, šíria falošné aktualizácie zamestnaneckých príručiek alebo nevyžiadané dokumenty a využívajú tento trend ako bežnú taktiku vo svojich kampaniach. **VJ CSIRT v rámci interných incidentov identifikovala túto kampaň u viacerých organizácií vo svojej konštituencii.**

Hackeri odcudzili 160GB dát telekomunikačného operátora Telefonica

Útočník vystupujúci ako "Rey" zo skupiny Hellcat tvrdí, že 30. mája prenikol do interného systému Jira spoločnosti Telefónica a exfiltroval 106 GB dát vrátane tiketov, objednávok, e-mailov, zákazníckych a zamestnaneckých informácií. Zverejnil 5GB ako ukážku s viac ako 20 000 súbormi a pohrozil zverejnením zvyšku. Telefónica to označila za vydieranie s použitím starších dát, no hacker trvá na tom, že využil aktuálnu chybu v konfigurácii, ktorú spoločnosť nezabezpečila ani po predchádzajúcom útoku. Pravdepodobne ide o staré údaje, no stojí za to to zdôrazniť, pretože skupiny Hellcat a Rey sú dlhodobo aktívne a špecializujú sa na servery JIRA.

Hackeri zneužívajú uniknutý Shellter Elite, nasadzujú infostealery a obchádzajú detekciu

Hackeri začali zneužívať uniknutý nástroj Shellter Elite, ktorý je určený na obchádzanie antivírusov a systémov EDR pri testovaní bezpečnosti, aby nasadili infostealery ako Rhadamanthys, Lumma a Arechclient2. Nástroj sa stal verejne dostupným po tom, ako ho zdieľal zákazník bez oprávnenia, čo umožnilo jeho zneužitie v útokoch od apríla 2025. Elastic Security Labs vyvinul detekčné nástroje pre zneužívané verzie, no Shellter kritizuje Elastic za oneskorené informovanie a zameranie sa na publicitu namiesto bezpečnosti.

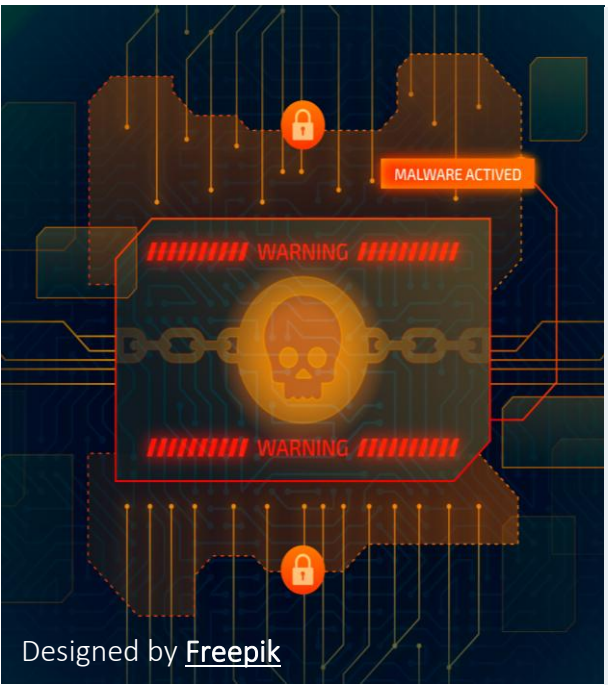
VÝZNAMNÉ UDALOSTI VO SVETE

APT skupina DoNot rozširuje svoj záujem na európske štáty

APT skupina DoNot, známa aj ako APT-C-35, Mint Tempest či Origami Elephant, rozšírila svoje operácie a začala cieliť na ministerstvá zahraničných vecí v Európe. Podľa výskumu Trellix Advanced Research Center sa útoky začínajú phishingovými e-mailami, ktoré obsahujú odkaz na Google Drive. Po kliknutí sa stiahne archív RAR s malvérom LoptikMod, ktorý je schopný zbierať citlivé údaje zo zasiahnutých zariadení. Malvér, ktorý skupina používa od roku 2018, sa vyznačuje technikami na obídenie analýzy, ako je obfuskácia a detekcia virtuálnych prostredí. Cieľom útokov sú vládne inštitúcie, obranné organizácie a mimovládne organizácie, najmä v Južnej Ázii a Európe.

Ransomvérová skupina Pay2Key.I2P obnovila svoju činnosť

Skupina Pay2Key.I2P, spojená s iránskou kybernetickou hrozbou Fox Kitten, obnovila svoju činnosť po zhoršení napätia medzi Izraelom, USA a Iránom. Od februára 2025 uskutočnila viac ako 51 úspešných ransomvérových útokov a získala cez 4 milióny dolárov. Pay2Key.I2P používa pokročilé techniky ako dvojfázové šifrovanie, obchádzanie prostredia sandbox a maskovanie pomocou legitímnych nástrojov. V júni 2025 pridala verziu pre Linux, čím rozšírila svoje možnosti útokov. Skupina spolupracuje s vývojármi ransomvéru Mimic a používa anonymnú sieť I2P na komunikáciu s obeťami. Tieto aktivity ukazujú prepojenie medzi kybernetickými operáciami a geopolitickými záujmami Iránu.



Designed by Freepik

Ransomvérová skupina INTERLOCK aktívne zneužíva techniku FILEFIX

Hackeri v rámci útokov vedúcich k nasadeniu ransomvéru INTERLOCK aktívne zneužívajú techniku FILEFIX na šírenie svojich malvérov RAT. Dlhodobo svoj malvér šírili prostredníctvom kompromitovaných webových stránok a injektora KONGTUKE. Od mája 2025 útočníci zneužívali techniku CLICKFIX, ktorá spočívala v zobrazovaní výziev CAPTCHA a jej cieľom bolo spustenie skriptu PowerShell vedúceho k spusteniu Node.js variantu Interlock RAT. Od júna 2025 distribuovali PHP variant opäť prostredníctvom KONGTUKE. V júli 2025 začali zneužívať FILEFIX, ktorý PHP variant RAT sťahuje z útočníkových serverov chránených prostredníctvom CLOUDFLARE TUNNELS. Ide o prvý verejný prípad zneužitia tejto techniky

VÝZNAMNÉ UDALOSTI VO SVETE

Darknetové fórum pre obchodovanie s drogami ABACUS MARKET náhle ukončilo svoje aktivity

Spoločnosť TRM LABS upozornila na náhle ukončenie darknetového trhu s drogami Abacus Market a výskumníci situáciu vyhodnocujú ako exit scam (podvod, pri ktorom sa prevádzkovatelia stratia aj s finančnými prostriedkami používateľov) alebo tajnej operácie OČTK. Trh fungoval od roku 2021 a rýchlo si získal dominantné postavenie, pričom v roku 2024 zabezpečoval až 70 % všetkých západných darknetových obchodov. Odhadovaný objem transakcií dosiahol až 300 miliónov dolárov v Bitcoinoch a Monere. Toto náhle ukončenie môže súvisieť s nedávnym rozložením obchodu Archetyp zo strany OČTK.

EUROPOL s partnermi rozložil hacktivistickú skupinu NONAME057(16)

Europol a Eurojust 15. júla 2025 v rámci operácie Eastwood, rozložili proruskú hacktivistickú skupinu NoName057(16), ktorá od marca 2022 vykonávala početné útoky typu DDoS na kritickú infraštruktúru v Európe, Izraeli a na Ukrajine, vrátane útokov počas španielskych volieb a samitu NATO v Holandsku. Vykonali 24 domových prehliadok v 7 krajinách, zatkli dvoch podozrivých, vydali sedem medzinárodných zatykačov a vypli viac ako 100 serverov používaných na útoky. Skupina koordinovala svoje akcie cez softvér DDoSia a Telegram, kde verbovala dobrovoľníkov odmenami v kryptomene a hernými stimulmi. Väčšina vedúcich predstaviteľov skupiny sídli v Rusku, no operácia ukázala efektívnu medzinárodnú spoluprácu pri boji proti kybernetickej kriminalite.

Severokórejský malvér Konfety za účelom zmarenia detekcie úmyselne modifikuje inštalačné súbory

Severokórejskí hackeri vytvorili nový variant androidového malvéru Konfety, ktorý využíva úmyselne poškodené súbory APK, aby obišiel antivíry a bezpečnostné analýzy. Namiesto klasickej kompresie používajú neštandardné nastavenia ZIP a šifrované súbory DEX, čo spôsobuje chyby pri rozbaľovaní alebo statickej analýze. Po inštalácii Konfety zhromažďuje údaje o zariadení, načítava škodlivé pluginy a pomocou reklamného SDK CaramelAds zobrazuje falošné reklamy a presmerúva používateľov na nebezpečné stránky. Útočníci často vydávajú malvér za populárne aplikácie, aby oklamali obete mimo Google Play.

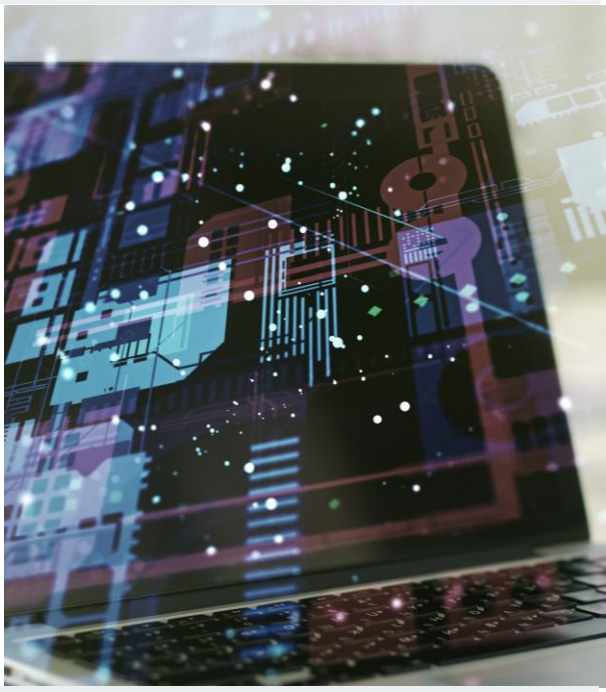
VÝZNAMNÉ UDALOSTI VO SVETE

Japonská polícia vydala nový dešifrovací nástroj pre ransomvér Phobos a 8Base

Japonská polícia vydala nový dešifrovací nástroj pre ransomware Phobos a 8Base, ktorý umožňuje obetiam bezplatne obnoviť zašifrované súbory, najmä tie s príponou .LIZARD. Nástroj podporuje aj ďalšie prípony ako .phobos, .8base, .elbie a .faust a môže fungovať aj pre iné prípony. Používateľ vyberie zašifrované súbory a cieľový priečinok, nástroj ich potom rekurzívne dešifruje a zachová pôvodnú štruktúru priečinkov. Webové prehliadače môžu nástroj označiť za škodlivý, ale je bezpečný a efektívny. Políciu a platformu NoMoreRansom podporujú Europol a FBI. Obete ransomvéru by mali nástroj vyskúšať aj na súboroch bez viditeľnej prípony.

Masívna phishingová kampaň zneužívajúca identitu PyPI cieli na vývojárov

Správca Python Package Index upozornil na prebiehajúcu phishingovú kampaň, ktorá cieli na vývojárov a používateľov PyPI. Útočníci rozosielajú e-maily s predmetom [PyPI] Email verification z adresy noreply@pypj[.]org, ktorá sa podobá oficiálnej doméne pypi[.]org. V e-mailoch používajú odkazy na falošné prihlasovacie stránky, ktoré napodobňujú vzhľad PyPI, aby získali prihlasovacie údaje obetí. Po zadaní údajov na podvodnej stránke útočníci presmerujú obeť na skutočnú stránku PyPI, aby zmiernili podozrenie. Správca PyPI odporúča používateľom kontrolovať URL adresy pred prihlásením, vyhýbať sa klikaniu na odkazy v podozrivých e-mailoch a v prípade kompromitovania okamžite zmeniť heslo a skontrolovať bezpečnostnú históriu účtu.



Skupina UNC2891 cieli na bankové pobočky

Severokórejskí Útočníci zo skupiny UNC2891 (LightBasin) prenikli do bankovej pobočky, pripojili zariadenie Raspberry Pi so 4G modemom k internému sieťovému prepínaču pre bankomaty a cez mobilnú sieť vytvorili skrytý vzdialený prístup do bankovej infraštruktúry. Nasadili nástroj TinyShell, pohybovali sa po sieti a pokúsili sa manipulovať s bankomatovými transakciami, aby uskutočnili neoprávnené výbery. Na riadenie útoku využili dynamic DNS, mobilné pripojenie a pokročilé techniky maskovania, no incident odhalili bezpečnostní výskumníci zo spoločnosti Group-IB ešte predtým, ako útočníci stihli ukradnúť peniaze. Pokus ukazuje, ako kombinácia fyzického prístupu a jednoduchého hardvéru môže obísť tradičné zabezpečenie bánk.

VÝZNAMNÉ UDALOSTI VO SVETE

- Spoločnosť Let's Encrypt oznámila, že prestane posielať e-maily upozorňujúce na vypršanie certifikátov.
- Nemecké úrady žiadajú Apple a Google, aby okamžite stiahli aplikáciu DeepSeek AI z nemeckých obchodov, pretože odosiela osobné údaje používateľov (prompty, nahrané súbory, IP adresy, vzorce písania) na servery v Číne, kde nie je garantovaná úroveň ochrany podľa GDPR.
- Čínska hackerská skupina Salt Typhoon sa od marca do decembra 2024 nepozorovane infiltrovala do siete Národnej gardy USA, kde získala citlivé údaje vrátane konfigurácií sietí, poverení administrátorov a ďalších údajov, ktoré môžu umožniť ďalšie kompromitácie iných vládnych sietí.
- Národné centrum kybernetickej bezpečnosti NCSC UK ohlásilo spustenie novej iniciatívy pre hľadanie bezpečnostných zraniteľností VRI (Vulnerability Research Initiative), ktorá má posilniť spoluprácu a výmenu informácií s bezpečnostnými výskumníkmi.
- Spoločnosť Intruder vyvinula bezplatný open-source nástroj Autoswagger, ktorý pomáha odhaľovať zraniteľnosti v API, najmä chyby v autorizácii.

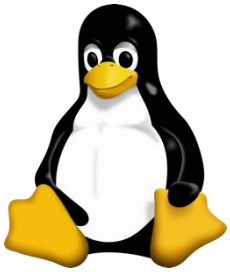
ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná zraniteľnosť Google Chrome

Vývojári spoločnosti Google opravili vysoko závažnú aktívne zneužívanú zraniteľnosť v prehliadači Chrome, ktorá umožňuje spôsobiť pád aplikácie alebo získať schopnosť vykonávať ľubovoľný kód.

Zraniteľnosť Citrix NetScaler ADC and NetScaler Gateway

Spoločnosť Citrix Systems varuje pred kritickou zraniteľnosťou v zariadeniach NetScaler ADC a NetScaler Gateway, ak sú nakonfigurované ako brána – t. j. VPN virtuálny server, ICA Proxy, CVPN, RDP Proxy – alebo ako AAA virtuálny server.



Kritická zraniteľnosť Sudo

Výskumník z Stratascale Cyber Research Unit objavil kritickú zraniteľnosť v softvérovom balíčku sudo, ktorá neoprávnenému používateľovi umožňuje lokálnu eskaláciu privilégií na Unixových a Unixu-podobným operačných systémov.

Kritická zraniteľnosť v Cisco Unified Communications Manager

Zraniteľnosť v produktoch Cisco Unified Communications Manager (Unified CM) a Cisco Unified Communications Manager Session Management Edition (Unified CM SME) môže umožniť neautentifikovanému vzdialenému útočníkovi prihlásiť sa do napadnutého zariadenia ako používateľ root.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť v module Forminator možno zneužiť na kompromitáciu WordPress

Vývojári modulu WordPress The Forminator Forms vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-6463 možno zneužiť na odstránenie súborov redakčného systému a získanie úplnej kontroly nad systémom.

Kritickú zraniteľnosť Anthropic MCP Inspector možno zneužiť na vzdialené vykonanie kódu

Spoločnosť Anthropic vydala bezpečnostné aktualizácie svojho projektu na testovanie a debugovanie MCP (Model Context Protocol) serverov MCP Inspector, ktoré opravujú kritickú zraniteľnosť. CVE-2025-49596 možno zneužiť na vzdialené vykonanie kódu vedúce k úplnému narušeniu dôvernosti, integrity a dostupnosti systému.

Zraniteľnosť v ServiceNow Now Platform možno zneužiť na neoprávnený prístup k údajom

Spoločnosť ServiceNow vydala bezpečnostné aktualizácie svojej cloudovej manažmentovej platformy Now Platform, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2025-3648 by neautentifikovaný alebo autentifikovaný útočník mohol zneužiť na získanie prístupu k citlivým údajom.

Kritické bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty After Effects, Substance 3D Viewer, Audition, InCopy , InDesign, Connect , Dimension, Substance 3D Stager, Illustrator, FrameMaker, AEM Forms , AEM Screens a ColdFusion, ktoré opravujú 60 zraniteľností, z čoho 38 je označených ako kritických. Kritické zraniteľnosti by vzdialený útočník mohol zneužiť na obídenie bezpečnostných prvkov, eskaláciu privilégií a vykonanie kódu.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť webového aplikačného firewallu Fortinet FortiWeb

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť vo webovom aplikačnom firewalle Fortinet FortiWeb. CVE-2025-25257 možno zneužiť na vzdialené vykonanie kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Kritická zraniteľnosť v NPM knižnici mcp-remote umožňuje vzdialené vykonanie príkazov

Vývojári NPM knižnice mcp-remote vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. MCP (Model Context Protocol) protokol predstavuje štandard pre integráciu a výmenu dát medzi LLM modelmi a externými dátovými zdrojmi alebo službami. CVE-2025-6514 možno zneužiť na vzdialené vykonanie príkazov operačného systému.

Aktívne zneužívaná kritická zraniteľnosť vo Wing FTP

Vývojári FTP servera Wing FTP vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2025-47812 možno zneužiť na vzdialené vykonanie systémových príkazov a získanie úplnej kontroly nad systémom.

WordPress plugin Gravity Forms zneužitý na šírenie škodlivého kódu

Útočníci kompromitovali systémy vývojárov populárneho modulu Gravity Forms pre WordPress a modifikáciou inštalačných súborov zrealizovali útok na dodávateľský reťazec, čím ohrozili všetkých jeho používateľov. Jedná sa o celosvetovo rozšírený plugin, ktorý používajú aj spoločnosti ako Airbnb, Nike, Unicef či Google.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti zariadení Hewlett-Packard Enterprise Networking Instant On Access Point

Hewlett-Packard Enterprise (HPE) vydala bezpečnostné aktualizácie pre firmvér zariadení Networking Instant On Access Point, ktoré opravujú jednu kritickú a jednu vysoko závažnú zraniteľnosť. CVE-2025-37103 súvisí s napevno kódovanými prihlasovacími údajmi a CVE-2025-37102 umožňuje vykonávať systémové príkazy.

Zero-day zraniteľnosti Microsoft SharePoint Server

Spoločnosť Microsoft vydala bezpečnostné aktualizácie pre SharePoint Server, ktoré opravujú dve kritické aktívne zneužívané zraniteľnosti. CVE-2025-53770 a CVE-2025-53771 umožňujú vzdialené prevzatie kontroly nad servermi bez nutnosti prihlásenia. Chyby boli zneužité v útokoch proti desiatkam inštitúcií po celom svete.

Kompromitované balíčky NPM šíria malvér

Správca open-source NPM balíčkov pre Node.js uviedol na svojej GitHub stránke varovanie, že sa stal obeťou phishingového útoku. Útočníci vymenili jeho balíčky za škodlivé.

Aktívne zneužívaná zraniteľnosť CrushFTP

Vývojári FTP klienta CrushFTP vydali aktualizáciu pre novú zero-day zraniteľnosť, ktorá je aktívne zneužívaná. Útočníkom umožňuje získať administrátorský prístup ku zraniteľným zariadeniam.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľná aplikácia ExpressVPN smeruje komunikáciu RDP mimo tunel

ExpressVPN vo svojej poslednej aktualizácii opravila chybu, ktorá spôsobuje, že komunikácia vedúca cez Remote Desktop Protocol neprechádza VPN tunelom.

Škodlivý kód ukrytý do WordPress mu-plugins

Útočníci v rámci techník skrývania škodlivého kódu využívajú zložku mu-plugins, ktorú používajú stránky na platforme WordPress pre načítanie automaticky aktivovaných modulov.

MESAČNÍK ZRANITEĽNOSTÍ JÚL 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2685.html