MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

# Mesačná správa CSIRT.SK
## Máj 2024

Vypracoval: CSIRT.SK

TLP: White

Kybernetickým priestorom v máji 2024 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

**I. Spoločnosť CHECK POINT koncom mája 2024 upozornila na rozsiahlu sériu útokov zameraných na jej bezpečnostné brány.** Spočiatku boli pozorované pokusy o prienik prostredníctvom lokálnych používateľských účtov s password-only autentifikáciou a predpokladalo sa, že sa môže jednať o pokračovanie veľkých brute force útokov, ktoré v marci 2024 zachytila spoločnosť CISCO. Detailná analýza však odhalila, že útočníci v skutočnosti zneužívali bezpečnostnú zraniteľnosť, ktorá umožňovala prístup ku všetkým súborom zraniteľných zariadení. Uvedený incident opätovne poukazuje na dôležitosť procesov manažmentu aktív a bezpečnostných zraniteľností v rámci organizácie.

**II. Významným krokom v oblasti kybernetickej diplomacie bola verejná atribúcia série kybernetických útokov ruskej štátom sponzorovanej skupine APT28**, ktorá je známa aj pod aliasom Fancy Bear a jej aktivity sú spájané s ruskou vojenskou spravodajskou službou GRU. Tieto útoky boli zamerané na vládne inštitúcie, súkromné spoločnosti a kritickú infraštruktúru v Nemecku a Českej republike. EÚ a NATO vyjadrili svoju solidaritu a útoky rázne odsúdili**.** Priradenie útoku konkrétnemu aktérovi nielenže zvyšuje povedomie o hrozbe, ale zároveň vytvára medzinárodný tlak a môže viesť až k politickým a diplomatickým opatreniam voči krajinám vykonávajúcim kybernetické útoky.

**III. Z pohľadu významných incidentov je nutné spomenúť aj prienik do systému EUROPOL Platform for Experts**, ktorý slúži na výmenu informácií medzi odborníkmi na bezpečnosť. Útočníci prostredníctvom zneužitia prihlasovacích údajov aktívnych používateľov platformy získali prístup k citlivým údajom, ktoré následne zverejnili na predaj na hackerskom fóre BREACHFORUMS.

**Hackerské fórum BREACHFORUMS bolo následne rozložené v rámci medzinárodnej akcie FBI a Ministerstva spravodlivosti USA.** V rámci operácie orgány zaistili serverovú infraštruktúru, telegramové, TOX a ďalšie komunikačné kanály prevádzkovateľov fóra. Údajne boli zatknutí aj aktuálni administrátori platformy vystupujúci pod používateľskými menami Baphomet a ShinyHunters. Jednalo sa o významný úspech pre orgány činné v trestnom konaní, ktorý dočasne narušil činnosť kyberzločincov a znížil dostupnosť nelegálne získaných informácií.

**Fórum bolo krátko po svojom rozložení opätovne spustené, čo poukazuje na vytrvalosť kyberzločincov.** Momentálne ho prevádzkuje osoba alebo skupina osôb vystupujúcich pod aliasom "ShinyHunters," ktorý bol už v minulosti spájaný s významnými útokmi. Na fóre boli nedávno na predaj zverejnené aj nové úniky dát významných spoločností

ako napr. TICKETMASTER. Existujú však aj teórie, že by súčasná verzia mohla byť vytvorená a prevádzkovaná políciou za cieľom identifikácie ďalších zločincov.

**IV. V mesiaci máj uskutočnili orgány činné v trestnom konaní viacero významných medzinárodných operácií, ktoré viedli k narušeniu činnosti viacerých hackerských skupín.**

EUROPOL s partnermi v rámci akcie OPERATION ENDGAME úspešne **narušil infraštruktúru tzv. malvér dropperov**, ktorých cieľom je infekcia zariadenia obete ďalšími typmi škodlivého kódu, vrátane ransomvéru.

**OČTK identifikovali aj vodcu ransomvérovej skupiny Lockbit**, ktorý vystupoval pod aliasom LockBitSupp. Na základe zverejnených informácií sa jedná o Dmitryho Khorosheva, ktorý je občanom Ruskej federácie. Skupina zareagovala zverejnením rozsiahleho zoznamu ďalších obetí, čím dala najavo svoje odhodlanie pokračovať v nelegálnej činnosti.

**V. Bezpečnostní výskumníci upozornili na nebezpečnú malwaretisement kampaň, v rámci ktorej útočníci malvér šíria prostredníctvom odpovedí na diskusnom fóre STACK OVERFLOW.** Útočníci v rámci navrhovaných riešení odporúčajú inštaláciu škodlivých knižníc programovacieho jazyka PYTHON, ktoré obsahujú malware. Uvedený postup vytvára mimoriadne nebezpečný precedens, nakoľko obsah príspevkov tejto platformy je používaný aj na trénovanie AI modelov od spoločnosti OPENAI, čo vytvára priestor pre vznik nového útočného vektora. Používatelia ľubovoľných diskusných fór a služieb umelej inteligencie musia byť obozretní, aplikovať princípy kritického myslenia a všetky informácie pred použitím dôkladne overiť.

# Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci máj riešil štandardne 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. Časť z nich predávali útočníci na internetových fórach. Opätovne sa objavila phishingová kampaň, v ktorej útočníci predstierajú totožnosť Europolu a vysokopostavených členov Polície SR a posielajú svojim obetiam falošné súdne predvolania spojené s obvineniami z prechovávania detskej pornografie a podobných sexuálnych deliktov.

Objavili sa ďalšie prípady dlhodobo trvajúcej spear-phishingovej kampane, v ktorej sa útočníci vydávajú za nadriadeného obete a požadujú prevod väčšej sumy na zahraničné účty.

Vládna jednotka CSIRT aj v máji monitorovala aktivitu proruských hacktivistických skupín, ktoré zvyknú vykonávať útoky typu DDoS (zneprístupnenie služby) na webové stránky organizácií štátnej a verejnej správy. Skupina Cyber Army of Russia_Reborn sa zamerala na webové stránky niektorých obcí a VÚC, MZVaEZ SR, NR SR, bánk, politických strán a podnikov. Jednotka informovala subjekty, ktoré útočníci spomínali vo svojich správach na sociálnych sieťach.

CSIRT.SK prijal od Fakultnej nemocnice s poliklinikou F. D. Roosevelta v Banskej Bystrici hlásenie o úniku lekárskej správy R. Fica formou fotografie cez mobilnú sieť.

Nahlásená bola aj podozrivá komunikácia z IP adresy organizácie v konštituencii VJ CSIRT na IP adresu spájanú s malvérom Remcos RAT. Situáciu sme preverili, aby sme zabránili potenciálnej škodlivej aktivite.

CSIRT.SK vzhľadom na aktuálne nálezy opätovne upozorňuje na riziká spojené so sprístupnením administrátorských rozhraní z internetu. Či sa jedná o administráciu webstránky, prístup k e-mailovej službe alebo inú webovú aplikáciu, či vzdialený prístup do infraštruktúry, všetky prístupy je potrebné obmedziť na lokálne siete, alebo v nevyhnutných prípadoch zabezpečiť prístup využitím VPN a viacfaktorovou autentifikáciou.

Incidentom mesiaca bola výhražná e-mailová kampaň, šíriaca bombové hrozby na vyše 1000 slovenských škôl a mnohých ďalších organizácií. CSIRT.SK poskytol súčinnosť polícii SR a pracoval na získaní digitálnych stôp, ktorých analýza by mohla viesť k odhaleniu páchateľa. Zatiaľ sa však nepodarilo získať spoluprácu všetkých zainteresovaných subjektov, ktoré relevantné dáta vlastnia.

V rámci svojej proaktívnej činnosti vládna jednotka CSIRT vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii,

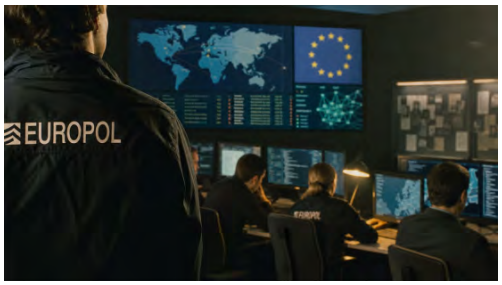
ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén.

# Významné udalosti vo svete

## Smerovače D-Link s ukončenou technickou podporou ako jadro botnet siete Goldoon

Bezpečnostní výskumníci zo spoločnosti Fortinet zverejnili informácie o novom botnete GOLDOON, ktorý infikuje smerovače D-Link DIR-645 s ukončenou technickou podporou. Zariadenia obsahujú zraniteľnosť CVE-2015-2051, ktorú možno prostredníctvom zaslania špeciálne vytvorených HTTP požiadaviek zneužiť na vykonanie škodlivého kódu. V súvislosti s aktívnym zneužívaním tejto zraniteľnosti Vládna jednotka CSIRT zverejnila na svojej webovej stránke varovanie. Uvedená kampaň z pohľadu prevencie výskytu kybernetických incidentov poukazuje na kritický význam manažmentu aktív, manažmentu zraniteľností a riadenia procesu aktualizácie systémov. Vyradenie a náhrada zariadení s ukončenou technickou podporou vyžadujú špecifický prístup a často aj dodatočné finančné náklady.

## EUROPOL s partnermi narušil infraštruktúru a služby slúžiace na šírenie malvéru




EUROPOL a medzinárodné konzorcium partnerov pozostávajúce z OČTK a popredných spoločností pôsobiacich v oblasti kybernetickej bezpečnosti v rámci akcie OPERATION ENDGAME úspešne narušili infraštruktúru a služby kyberkriminálnych skupín a botnetov asociovaných s malvérom ICEDID, PIKABOT, TRICKBOT, BUMBLEBEE, SMOKELOADER a SYSTEMBC. V období medzi 27. a 28 májom 2024 sa podarilo zatknúť 4 hackerov (1 z AM, 3 z UA), zaistiť vyše 100 serverov a 2000 domén a zmraziť časť finančných prostriedkov týchto skupín. Na základe vyjadrenia konzorcia sa jednalo len o prvú fázu operácie a v blízkej budúcnosti plánuje jej pokračovanie.

TLP: White

**Proruské hacktivistické skupiny cielia na subjekty v rámci kritickej infraštruktúry**



Americká Agentúra pre kybernetickú bezpečnosť CISA spolu s medzinárodnými partnermi vydala varovanie pred aktivitami prorusky orientovaných hacktivistických skupín. Bližšie nešpecifikované skupiny sa zameriavajú na kompromitáciu technológií, zariadení a systémov kritickej infraštruktúry krajín Severnej Ameriky a Európy. Útočníci zneužívajú zraniteľnosti alebo nesprávnu konfiguráciu zariadení a systémov, ktoré sú verejne dostupné z internetu. Varovanie obsahuje základné odporúčania pre zabezpečenie systémov. Vládna jednotka CSIRT prostredníctvom systému ACHILLES pravidelne vyhľadáva a adresne varuje potenciálne zraniteľné subjekty vo svojej konštituencii.

**Zneužitie zraniteľnosti v bezpečnostných bránach Check Point na krádež hesiel do VPN**

Spoločnosť CHECK POINT varovala pred masívnou vlnou útokov na svoje portfólio bezpečnostných brán, ktorej cieľom je získanie neoprávneného prístupu do chránených VPN sietí. Zraniteľnosť s označením CVE-2024-24919 možno zneužiť na získanie neoprávneného prístupu k obsahu ľubovoľných súborov na súborovom systéme zariadenia, ktoré obsahujú citlivé údaje ako napr. hashe hesiel lokálnych používateľov, privátne SSH kľúče alebo certifikáty. Exfiltrované údaje útočníci zneužívajú na prienik do systému, laterálny pohyb v rámci siete a ďalšiu škodlivú činnosť. Prvé pokusy o zneužitie tejto zraniteľnosti boli zaznamenané už 7. apríla 2024. Check Point vydala hotfix a zverejnila množinu odporúčaní na zvýšenie zabezpečenia VPN zariadení. Vládna jednotka CSIRT na svojej webovej stránke zverejnila varovanie pred touto kampaňou.

**Severokórejská APT43 zneužíva nesprávnu konfiguráciu záznamov DMARC**




Národná bezpečnostná agentúra NSA, Federálny úrad pre vyšetrovanie FBI a Ministerstvo zahraničných vecí Spojených štátov varovali pred aktivitami severokórejskej štátom sponzorovanej skupiny APT43 (KIMSUKI). Skupina zneužíva nesprávnu konfiguráciu záznamov DMARC na rozposielanie spear-phishingových e-mailov, ktoré sa javia ako legitímne správy od pracovníkov médií, akademickej obce a ďalších expertov na záležitosti krajín východnej Ázie. Varovanie vysvetľuje princíp zneužitia DMARC, obsahuje vzorové príklady a odporúčania na zamedzenie tohto typu útokov. V rámci záznamov DMARC je potrebné nastaviť parameter politiky „p“ na hodnotu „p=quarantine“ alebo „p=reject“.

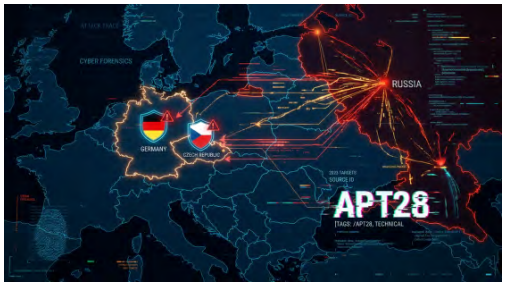
**Koniec bezplatnej podpory pre Windows 10 v roku 2025 ako bezpečnostné riziko**



Štatistické údaje webovej služby StatCounter zachytávajú trend, podľa ktorého mesačný rast aj celkový počet zariadení s operačným systémom Windows 10 výrazne prevyšuje počet zariadení s Windows 11. Spoločnosť Microsoft oznámila, že v priebehu roka 2025 ukončí bezplatnú technickú podporu pre Windows 10. Napriek tomu, že je update na Windows 11 pre držiteľov legálnych verzií bezplatný, migrácia je možná len na zariadeniach spĺňajúcich stanovené prerekvizity. Nedostupnosť aktualizácií a nemožnosť migrácie na verzie s technickou podporou môžu viesť k nárastu počtu systémov s bezpečnostnými zraniteľnosťami. Vzhľadom na významné zastúpenie operačného systému Windows v rámci kybernetického priestoru SR Vládna jednotka CSIRT kontinuálne monitoruje vývoj v tejto oblasti a v rámci mesačných prehľadov kritických zraniteľností na svojej webovej stránke upozorňuje aj na softvér s ukončenou technickou podporou.

TLP: White

**Nemecko a Česká republika atribuovali kybernetické útoky z 2023 ruskej skupine APT28**




Nemecko a Česká republika oficiálne atribuovali kybernetické útoky z roku 2023 ruskej skupine APT28. Verejne dostupné informácie poukazujú aj na ďalšie ciele v Lotyšsku, Poľsku, Švédsku a na Slovensku. Veľvyslanci Ruskej federácie obvinenia z tejto činnosti kategoricky odmietli. Verejná atribúcia spôsobila, že aj ostatné štáty začali postupne zverejňovať informácie o prebiehajúcich útokoch APT28. V rámci tohto kontextu si zaslúži pozornosť aj detailná analýza CERT-PL, ktorá poskytla konkrétne indikátory kompromitácie (IOC) a technické detaily týkajúce sa týchto útokov. Hoci zverejnenie takýchto informácií môže pomôcť iným organizáciám lepšie sa pripraviť a brániť proti podobným hrozbám, zároveň nesie so sebou riziko, že útočníci upravia svoje zaužívané postupy.

**Odhalenie identity vodcu ransomvérovej skupiny Lockbit**




Anglická NCA, americká FBI, EUROPOL a ďalší partneri v rámci medzinárodnej akcie opätovne spustili darknetovú stránku skupiny Lockbit, nad ktorou získali kontrolu vo februári 2024. Na tejto stránke zverejnili správy naznačujúce, že sa im podarilo identifikovať vodcu skupiny a spustili odpočítavanie času do zverejnenia jeho identity. Členovia skupiny Lockbit popreli, že by konzorcium mohlo disponovať uvedenými údajmi a na svojich darknetových stránkach začali zverejňovať zoznam ďalších obetí. Po skončení odpočívania došlo k zverejneniu identity vodcu ransomvérovej skupiny Lockbit, ktorým je občan Ruskej federácie Dmitry Khoroshev.

### Útočníci prenikli do komunikačnej platformy Europolu



EUROPOL potvrdil, že bližšie nešpecifikovaný útočník získal prístup do ich komunikačnej platformy EPE (Europol Platform for Experts). Osoba vystupujúca pod aliasom INTELBROKER exfiltrované dáta ponúkla na predaj na hackerskom fóre BREACHFORUMS. Zverejnený príspevok obsahoval ukážky ukradnutých dát, medzi ktorými boli informácie o členoch EPE, zdrojový kód nástrojov a návody pre rôzne operatívne činnosti. Príspevok analyzovala aj Vládna jednotka CSIRT, nakoľko medzinárodná platforma EPE má aj používateľov z SR.

### Spoločnosť ESET zverejnila technickú analýzu malvéru ruskej APT skupiny TURLA




Spoločnosť ESET zverejnila analýzu backdoor malvéru LUNARWEB a LUNARMAIL, ktorý bol v roku 2023 použitý v rámci útokov na ministerstvo zahraničných vecí bližšie nešpecifikovaného európskeho štátu a diplomatické misie v rámci oblasti stredného východu. Uvedené útoky sú atribuované ruskej štátom sponzorovanej skupine TURLA. Ku kompromitácii systémov došlo pravdepodobne pomocou cielenej spear-phishingovej kampane a zneužitím nesprávnej konfigurácie sieťového monitorovacieho nástroja Zabbix. Analýza popisuje techniky, taktiky a postupy skupiny a známe indikátory kompromitácie. Dve z riadiacich IP adries patrili do kybernetického priestoru SR.

**Čínske APT skupiny maskujú útoky prostredníctvom rozsiahlych proxy služieb ORB**



Podľa analýzy spoločnosti MANDIANT útočníci na maskovanie svojej činnosti čoraz častejšie využívajú rôzne proxy služby, čím značne komplikujú proces detekcie škodlivej činnosti a rovnako aj proces atribúcie. Bezpečnostní výskumníci upozornili, že čínske štátom sponzorované skupiny pri útokoch stále častejšie využívajú rozsiahle proxy siete označované pojmom ORB (Operational Relay Box), ktorých uzly tvoria legitímne VPS servery a kompromitované zariadenia. Služby ORB prevádzkujú kriminálne skupiny a následne ich využívajú v rámci kybernetických útokov ďalšie skupiny, vrátane APT skupín. Analýza od spoločnosti MANDIANT bližšie skúma ORB1/ORBWEAVER, ORB2/FLORAHOX (využívané skupinou APT31) a ORB3/SPACEHOP (využívané skupinami APT5 a APT15). Uvedený trend využitia proxy služieb na maskovanie činnosti výrazne komplikuje detekciu a atribúciu útokov.

**Microsoft postupne ruší podporu skriptovacieho jazyka VBScript**




Spoločnosť MICROSOFT v druhej polovici 2024 začne s postupným rušením podpory skriptovacieho jazyka VBSCRIPT. V prvej fáze sa VBScript stane voliteľnou súčasťou operačného systému Windows, tzv. FoD (Feature on Demand), ktorá bude naďalej predvolene aktivovaná. Následne od roku 2027 už nebude súčasťou predvolenej inštalácie Windows. V poslednej fáze je naplánované úplné ukončenie podpory a odstránenie príslušných DLL súborov z operačného systému. Microsoft tento krok zdôvodnil technologickým pokrokom skriptovacích jazykov PowerShell a JavaScript a zvyšovaním bezpečnosti ekosystému Windows. V súvislosti s týmto krokom možno očakávať aj postupnú adaptáciu útočníkov a príchod nových vektorov slúžiacich na šírenie malvéru.

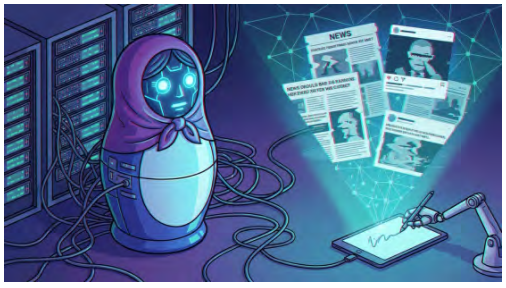
TLP: White

**AI služba Microsoft Recall ako potenciálny zdroj citlivých údajov pri útokoch**




Spoločnosť MICROSOFT v rámci prezentácie novej generácie počítačov COPILOT+ PC orientovanej na využívanie umelej inteligencie predstavila kontroverznú funkciu operačného systému Windows 11. Služba RECALL má slúžiť ako fotografická pamäť počítača, ktorá v pravidelných intervaloch zaznamenáva aktivitu a obsah všetkých povolených aplikácií vo forme sekvencie screenshotov a následne umožňuje vyhľadávanie prostredníctvom textových dopytov. Všetky súvisiace údaje by mali ukladať a spracovávať lokálne jazykové modely priamo na zariadeniach používateľa. Bezpečnostná komunita vzhľadom na rozsah a formu zaznamenaných údajov predpokladá, že údaje služby Recall sa stanú jedným z primárnych cieľov malvéru zameraného na exfiltráciu citlivých údajov.

**Ruská sieť CopyCop využíva AI na generovanie obsahu dezinformačných kampaní**




Bezpečnostní výskumníci zo spoločnosti RECORDED FUTURE odhalili rozsiahlu ruskú sieť s označením COPYCOP, ktorá šíri dezinformácie vo viacerých krajinách NATO. Za pomoci nástrojov umelej inteligencie dokáže skupina rýchlo generovať obsah s rôznymi naratívmi. Pri svojej činnosti útočníci vychádzajú z informácií zverejnených na dôveryhodných spravodajských portáloch, ktoré následne prostredníctvom AI modifikujú podľa potreby. Skupina má spolupracovať aj s ďalšími významnými aktérmi v oblasti šírenia dezinformácií (skupiny DOPPELGANGER a PORTAL KOMBAT). V súvislosti s prudkým rozvojom v oblasti umelej inteligencie možno očakávať nárast dôveryhodnosti obsahu generovaného v rámci hybridných operácií a treba zdôrazniť význam kritického myslenia pri analýze informačného obsahu.

- Neznámy útočník kompromitoval produkčné servery služby Dropbox Sign, ktorá slúži na elektronické podpisovanie dokumentov
- Hackerská skupina „КИБЕРПАРТИЗАНЫ BY“ sa prostredníctvom svojho telegramového kanála prihlásila ku kompromitácii webovej stránky bieloruskej KGB
- Ruská skupina UAC-0149 (Flying Yeti) zneužíva phishingové e-maily a správy na platforme Signal na šírenie malvéru Cookbox
- Európska komisia v rámci obáv z dezinformačnej kampane súvisiacej s voľbami do Európskeho parlamentu kontaktovala spoločnosti META
- Jazykový model GPT-4 je schopný vygenerovať kód pre zneužitie zraniteľnosti len na základe jej popisu v rámci databázy CVE
- Americká CISA a FBI v spolupráci s medzinárodnými partnermi v rámci iniciatívy #STOPRANSOMWARE uverejnila detailnú analýzu služby ransomware-as-a-service Black Basta
- Spoločnosť Microsoft varovala pred zneužívaním nástroja Windows Quick Assist v rámci phishingových kampaní
- Botnet Ebury sa zameriava na kompromitáciu infraštruktúry poskytovateľov hostingových služieb
- V Českej republike bol zaznamenaný masívny nárast mobilných zariadení infikovaných malvérom Cerberus
- Spoločnosť Kia Sales Slovensko sa stala obeťou kybernetického útoku, v rámci ktorého došlo k úniku citlivých údajov
- Spojené kráľovstvo plánuje zavedenie povinného hlásenia ransomvérových incidentov a úplný zákaz platby útočníkom obetiam v rámci kritickej infraštruktúry štátu
- FBI v spolupráci s partnermi rozložila proxy botnet 911 S5, ktorý útočníci aktívne využívali na maskovanie svojej činnosti
- Bezpečnostní výskumníci informovali o novom type DoS útoku s označením DNS BOMB, ktorý dosahuje amplifikačný faktor 20 000
- Nová služba AI Overviews od spoločnosti Google generuje nepravdivé a nezmyselné odpovede

# Závažné zraniteľnosti bežných softvérových produktov

**Aktívne zneužívaná zraniteľnosť bezpečnostných brán Check Point**

Spoločnosť Check Point vydala bezpečnostné aktualizácie pre aktívne zneužívanú zraniteľnosť vedúcu k úniku citlivých informácií, zneužiteľných na prienik do siete a laterálny pohyb v nej. Zraniteľnosť zasahuje bezpečnostné brány Network Security Gateway s povolenými službami Remote Access VPN alebo Mobile Access. Útočníci môžu získať hashe hesiel používateľských účtov a prístup k Active Directory. Zneužitím exfiltrovaných údajov je možné dosiahnuť aj vzdialené vykonanie kódu.

**Zraniteľnosti v produktoch Veeam**

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoje produkty Backup & Replication, Agent for Windows a Service Provider Console, ktoré opravujú viacero zraniteľností umožňujúcich obchádzanie bezpečnostných prvkov, eskaláciu privilégií alebo vzdialené vykonanie kódu.

**Bezpečnostné zraniteľnosti v produktoch Ivanti**

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 16 bezpečnostných zraniteľností v produktoch Avalanche, Neurons for ITSM, Neurons for ITAM, Connect Secure, Policy Secure, Secure Access a Endpoint Manager. Najzávažnejšie sú kritické zraniteľnosti v produkte Endpoint Manager, ktoré možno zneužiť na vykonanie škodlivého kódu.

**Aktívne zneužívané zero-day zraniteľnosti Google Chrome**

Spoločnosť Google vydala bezpečnostné aktualizácie na opravu troch zero-day zraniteľností vo webovom prehliadači Chrome, ktoré možno zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby alebo získanie neoprávneného prístupu k citlivým údajom. Zraniteľnosti sú aktívne zneužívané útočníkmi, odporúčame bezodkladnú aktualizáciu.

TLP: White

**Bezpečnostné zraniteľnosti v produktoch VMware Workstation a Fusion**

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, ktoré opravujú 4 bezpečnostné zraniteľnosti v produktoch VMware Workstation a Fusion, z toho je 1 označená ako kritická. Zraniteľnosti možno zneužiť na vzdialené vykonanie škodlivého kódu, zneprístupnenie služby a neoprávnený prístup k citlivým údajom.

**Bezpečnostné zraniteľnosti v BIG-IP Next Central Manager**

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoj produkt BIG-IP Next Central Manager, ktoré možno zneužiť na vykonanie SQL a OData injekcie a následné získanie úplnej kontroly nad zraniteľnými systémami.

**Kritická zraniteľnosť manažmentového nástroja Veeam Service Provider Console**

Spoločnosť Veeam vydala bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť nástroja Veeam Service Provider Console, slúžiaceho na centralizovaný manažment prostredí využívajúcich technologické riešenia od Veeam. Zraniteľnosť možno zneužiť na vzdialené vykonanie kódu.

**Microsoft v rámci Patch Tuesday opravil aktívne zneužívané zero-day zraniteľnosti**

Spoločnosť Microsoft vydala v máji 2024 balík opráv pre portfólio svojich produktov opravujúci 61 zraniteľností, z ktorých 28 umožňuje vzdialené vykonávanie kódu. Tri zraniteľnosti sú typu zero-day a dve z nich sú aktívne zneužívané.

**Kampaň botnetu „Goldoon“ zneužíva starú kritickú zraniteľnosť smerovačov D-Link**

Bezpečnostní výskumníci z FortiGuard poukázali na novú útočnú kampaň šíriacu malvér/botnet Goldoon, ktorá sa zameriava na routery D-Link. Počas apríla sa dvojnásobne zvýšil nárast útokov na bezpečnostnú chybu s označením CVE-2015-2051. Zaujímavosťou je, že táto zraniteľnosť je už takmer desať rokov stará.

TLP: White

**Mesačník zraniteľností Máj 2024**

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Aktívne zneužívaná zraniteľnosť bezpečnostných brán Check Point
    - Zraniteľnosti v produktoch Veeam
    - Bezpečnostné zraniteľnosti v produktoch Ivanti
    - Aktívne zneužívané zero-day zraniteľnosti Google Chrome
    - Bezpečnostné zraniteľnosti v produktoch VMware Workstation a Fusion
    - Bezpečnostné zraniteľnosti v BIG-IP Next Central Manager
    - Kritická zraniteľnosť manažmentového nástroja Veeam Service Provider Console
    - Microsoft v rámci Patch Tuesday opravil aktívne zneužívané zero-day zraniteľnosti
    - Kampaň botnetu „Goldoon“ zneužíva starú kritickú zraniteľnosť smerovačov D-Link

https://www.csirt.gov.sk/posts/1015.html?csrt=7216744260263986664