CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

AUGUST 2024

TLP: WHITE

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

1 Bankový phishing infikuje mobilné zariadenia malvérom

Výskumníci zachytili rozsiahle phishingové kampane zneužívajúce identitu bánk, ktoré sú cielené na mobilných používateľov a na exfiltráciu citlivých údajov zneužívajú aplikácie pre iOS a Android.

2 Nárast počtu malvérov cielených na platformu macOS

Bezpečnostní výskumníci identifikovali viacero rodín malvéru cielených špeciálne na používateľov zariadení s operačným systémom macOS.

3 USA varovali pred vplyvovými operáciami Iránu

USA v súvislosti s nadchádzajúcimi prezidentskými voľbami varovali pred kybernetickými útokmi zo strany Iránu a vplyvovými operáciami zameranými na širokú verejnosť.

4 OpenAI disponuje technológiou na rozpoznanie textu generovaného ChatGPT

Spoločnosť OPENAI má k dispozícii metódu pre watermaking výstupov z ChatGPT, prostredníctvom ktorej možno dosiahnuť až 99-percentnú úspešnosť detekcie textov generovaných pomocou ich modelov.

5 Francúzske OČTK zadržali a obvinili CEO Telegramu

Francúzske OČTK zadržali zakladateľa Telegramu v súvislosti s nedostatočným moderovaním obsahu na sociálnej sieti, ktorá umožňuje činnosť kyberzločincov a ďalšiu nelegálnu činnosť.

6 Farma notebookov zneužívaná v rámci špionážnych aktivít KĽDR

Ministerstvo spravodlivosti USA a ďalšie OČTK rozložili ďalšiu notebookovú farmu, ktorú severokórejskí hackeri zneužívali na kyberšpionáž.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci august 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. Prihlasovacie údaje k časti takýchto účtov sa vyskytli v predajných ponukách na hackerských fórach.

Najvypuklejšou phishingovou kampaňou v auguste bola banková kampaň zneužívajúca najmä mená bánk ČSOB, Fio a Slovenskej sporiteľne. Útočníci sa pokúšali získať od svojich potenciálnych obetí citlivé platobné údaje pod zámienkou „aktualizácie karty“ alebo „overenia účtu“.

Opäť sme sa stretli s útokmi na prihlasovacie rozhrania webových stránok postavených na platforme Wordpress (.../wp-login.php) a API rozhrania XML-RPC (.../xmlrpc.php), vystavené do internetu. Administratívne a iné citlivé súčasti webstránok dlhodobo odporúčame ponechať dostupné iba lokálne, prípadne cez rozhranie VPN. Tiež odporúčame udržiavať aktualizované samotné CMS, ako aj prídavné moduly, ktoré Vaša webstránka využíva.

CSIRT.SK prijal žiadosť Policajného zboru SR o pomoc pri stotožnení páchateľa, ktorý odoslal výhražný e-mail s bombovou hrozbou na organizáciu v jeho konštituencii. Počas analýzy incidentu získal cenné digitálne stopy, ktoré poskytol polícii.

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.

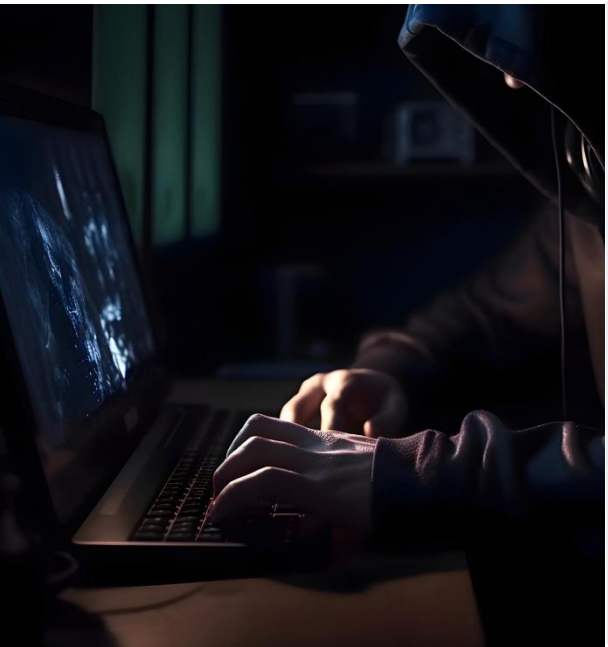
VÝZNAMNÉ UDALOSTI VO SVETE

Nové metódy pre obídenie ochrany Windows SmartScreen a Smart App Control

Bezpečnostní výskumníci zo spoločnosti ELASTIC poukázali na viacero koncepčných nedostatkov a zraniteľností vo Windows Smart App Control a Windows SmartScreen, ktoré možno zneužiť na obídenie bezpečnostných mechanizmov a následné vykonanie škodlivého kódu. Jedna z prezentovaných metód spočíva v podvrhnutí špeciálne vytvorených LNK súborov, ktorú na základe analýzy vzoriek z platformy VirusTotal útočníci zneužívajú už minimálne od roku 2018. Spoločnosť Microsoft predmetné zraniteľnosti opravila v rámci pravidelného balíka aktualizácií.

FBI zverejnila podrobnú analýzu ransomvérovej skupiny Blacksuit

CISA a FBI informovali, že sa ransomvérová skupina ROYAL, aktívna už vyše 2 roky, premenovala na BLACKSUIT. Medzi primárne vektory prieniku do systémov možno zaradiť phishingové kampane šíriace škodlivé PDF dokumenty, kompromitáciu RDP protokolu, zneužitie zraniteľností verejne dostupných služieb a zariadení v infraštruktúre obete alebo zneužitie platných prihlasovacích údajov získaných z rôznych zdrojov. Zverejnená bola aj aktualizovaná verzia analýzy, ktorá do detailov popisuje postupy, taktiky a metódy útočníka (TTP), indikátory kompromitácie (IOC) a YARA pravidlá pre host-based detekciu.



USA rozložili farmu notebookov zneužívaných v rámci špionážnych aktivít KĽDR

Ministerstvo spravodlivosti USA a ďalšie orgány činné v trestnom konaní rozložili ďalšiu notebookovú farmu, ktorú severokórejskí hackeri zneužívali na maskovanie svojej identity a geolokácie a kyberšpionáž. FBI v marci 2024 spustila iniciatívu na vyhľadávanie a rozloženie podobných fariem, ktoré zahraniční štátom sponzorovaní aktéri zneužívajú na kyberšpionážne aktivity. Incident opäť poukazuje na fyzický aspekt špionážnych aktivít.

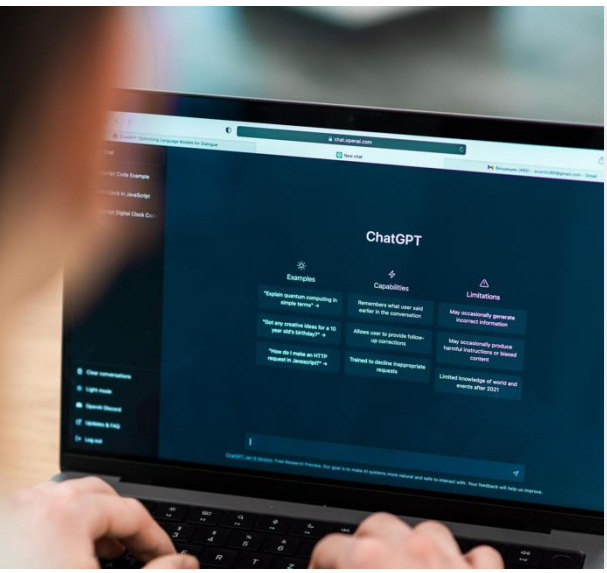
MESAČNÁ SPRÁVA

AUGUST 2024

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

VÝZNAMNÉ UDALOSTI VO SVETE



OpenAI disponuje technológiou na rozpoznanie textu generovaného ChatGPT

Spoločnosť OPENAI má k dispozícii metódu pre watermaking výstupov z CHATGPT, prostredníctvom ktorej možno dosiahnuť až 99-percentnú úspešnosť detekcie textov generovaných prostredníctvom ich modelov, a to aj v prípade parafrázovania výstupu. Mechanizmus by bolo možné obísť len celkovou reformuláciou prostredníctvom iných modelov. Manažment spoločnosti OpenAI je nejednotný ohľadom sprístupnenia technológie, nakoľko na základe prieskumov by to mohlo viesť až k 30 % poklesu používateľov.

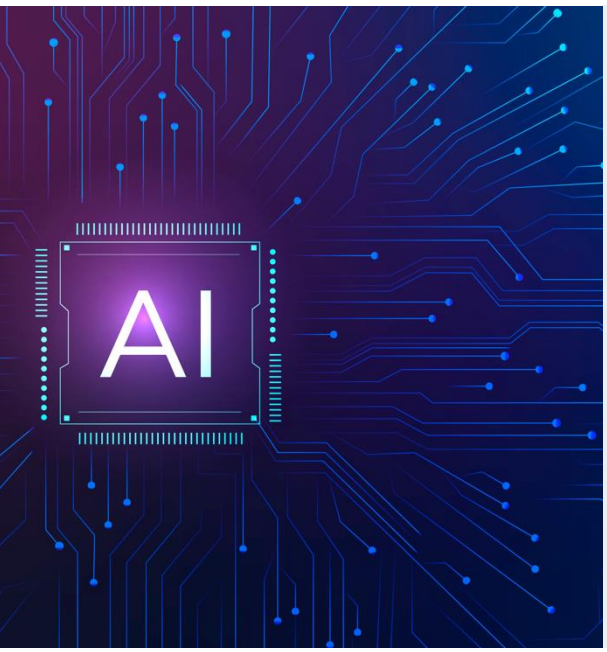
FBI a partneri zverejnili aktualizovanú analýzu skupiny RANSOMHUB

FBI a partneri zverejnili ďalšie informácie o činnosti ransomware-as-a-service skupiny RANSOMHUB, ktorá od februára 2024 úspešne kompromitovala systémy viac ako 200 obetí patriacich do kritickej infraštruktúry USA. S prihliadnutím na TTP skupiny sú z pohľadu prevencie kritické pravidelná aktualizácia verejne dostupných systémov a zariadení a nasadenie MFA ochrany. Analýza obsahuje aktuálne TTP a IOC asociované so skupinou. Nakoľko boli útoky tejto skupiny zaznamenané aj v kybernetickom priestore SR, vládna jednotka CSIRT techniky, postupy, nástroje a indikátory kompromitácie monitoruje.

Nový variant botnetu GAFGYT infikuje zariadenia so slabými SSH heslami

Bezpečnostní výskumníci odhalili nový variant botnetu GAFGYT, ktorý infikuje zariadenia so slabým SSH heslom a následne využíva ich dostupné výpočtové prostriedky na ťažbu kryptomien prostredníctvom nástroja XMRIG. Infikované zariadenia za účelom ďalšieho šírenia botnetu skenujú internet a vykonávajú slovníkové SSH brute force útoky. Z dlhodobého hľadiska prevádzkovatelia botnetu ako primárne vektory prieniku do systému využívajú slabé heslá, továrenské nastavenia zariadení a taktiež známe bezpečnostné zraniteľnosti. Botnet je taktiež schopný vykonávať DDoS útoky. Vzhľadom na celosvetový trend nedostatočného zabezpečenia SSH prístupov botnet predstavuje riziko aj pre zariadenia v kybernetickom priestore SR. CSIRT.SK v rámci preventívnych opatrení na svojej stránke zverejňuje metodiky a návody na zvyšovanie zabezpečenia systémov.

VÝZNAMNÉ UDALOSTI VO SVETE

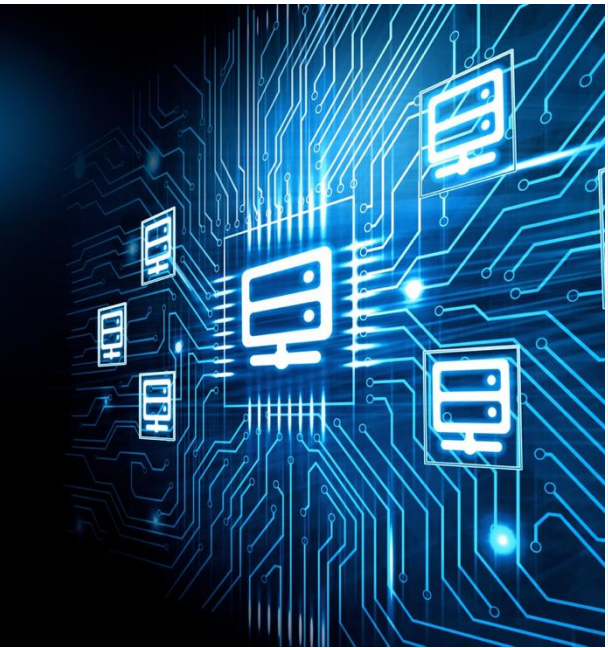


Ďalšie sťažnosti súvisiace s neoprávneným trénovaním AI modelu GROK od X

Európska nezisková organizácia NONE OF YOUR BUSINESS v súvislosti s neoprávneným trénovaním AI modelu GROK na príspevkoch používateľov platformy X podala 9 GDPR sťažností na spoločnosť X. Súvisiace vyšetrovanie zo strany írskeho úradu pre ochranu osobných údajov odhalilo, že k neoprávnenému trénovaniu dochádzalo v období medzi 7. májom a 1. augustom 2024. Samotný model je zatiaľ dostupný len pre prémiových používateľov platformy X a podľa komparatívnych štúdií dosahuje kvality popredných modelov ChatGPT-4o a Claude3.5. Nakoľko prevádzkovatelia veľkých AI modelov čelia problémom s dostupnosťou dát potrebných pre ďalšie trénovanie modelov, viacero bezpečnostných výskumníkov predpokladá nárast počtu podobných prípadov neoprávneného využitia používateľských dát.

Aplikácia Signal bola zablokovaná na území Ruskej federácie

Ruský úrad pre dohľad nad komunikačnými a informačnými technológiami ROSKOMNADZOR s odvolaním sa na porušovanie ruskej legislatívy súvisiacej s bojom proti terorizmu a extrémizmu na území Ruskej federácie zakázal prístup k aplikácii SIGNAL, ktorá umožňuje šifrovanú end-to-end komunikáciu. Vývojári Signal potvrdili, že ich aplikácia je blokovaná vo viacerých štátoch a používateľom odporúčajú aktivovať režim CENSORSHIP CIRCUMVENTION, ktorý čiastočne obchádza pokusy o blokovanie aplikácie maskovaním zasielaných požiadaviek. V Rusku v poslednej dobe možno pozorovať výrazný nárast cenzúry obsahu, v rámci ktorej došlo k zablokovaniu veľkého množstva aplikácií, vrátane VPN riešení.



PostgreSQL databázy so slabými heslami zneužívané na infekciu malvérom

Bezpečnostní výskumníci zverejnili informácie o novom malvéri PG_MEM, ktorý sa špecializuje na ťažbu kryptomeny MONERO na zariadeniach s databázovým systémom POSTGRESQL. Útočníci na počiatočný prienik do systémov využívajú brute-force útoky na databázy s predvolenými alebo slabými heslami a po úspešnom prieniku vytvárajú nový administrátorský účet a odstraňujú administrátorské oprávnenia ostatných používateľov. Následne prostredníctvom špecializovaných príkazov COPY a PROGRAM dochádza k spusteniu shellových príkazov na operačnom systéme napadnutého zariadenia, ktorými je možné vykonávať rôzne škodlivé aktivity, vrátane sťahovania rôznych foriem malvéru.

VÝZNAMNÉ UDALOSTI VO SVETE

Phishingová kampaň zneužívajúca identitu bánk infikuje mobilné zariadenia

Spoločnosť ESET varovala pred phishingovými kampaňami zneužívajúcimi identitu českej ČSOB a ČP, maďarskej OTP a gruzínskej TBC, ktoré sa zameriavajú na mobilných používateľov. Na zber a exfiltráciu citlivých údajov zneužívajú PWA (Progressive Web Application) aplikácie pre iOS a Android. V prípade Android zariadení boli zaznamenané aj WebAPK. Phishingový obsah je šírený prostredníctvom vishingu, smishingu a reklám na sociálnych sieťach. Po získaní prihlasovacích údajov útočníci v druhej fáze obeť navádzajú na inštaláciu Android malvéru NGATE, ktorý využíva open-source komponent NFCGATE. Škodlivý softvér umožňuje zaznamenávať NFC dáta z kariet v blízkosti infikovaného zariadenia a ich exfiltráciu k útočníkovi. Okrem bankových sa môže jednať aj o prístupové karty. Na kampaň upozornila aj Polícia ČR.

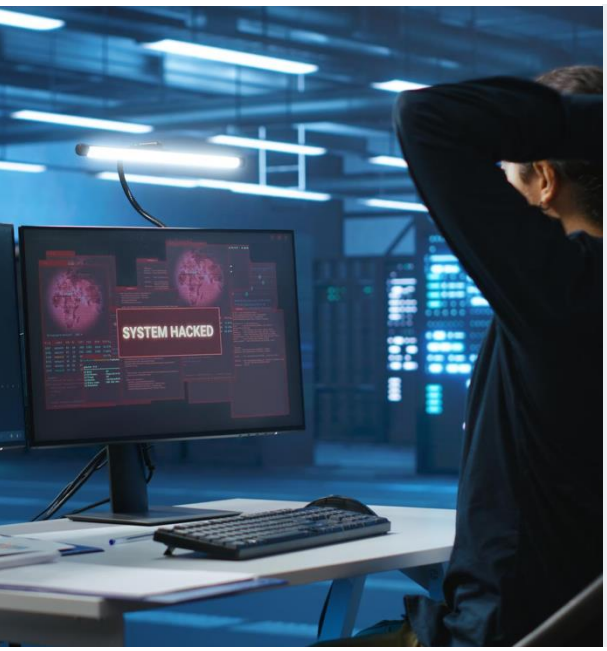
Potenciálne zraniteľnosti mobilných aplikácií pre platbu kartou

Bezpečnostní výskumníci upozornili na potenciálne zraniteľnosti mobilných aplikácií pre platbu kartami, vrátane GOOGLE PAY. Karty po pridaní do aplikácie možno využiť na platby za služby s predplatným a overovanie aj v prípade, že karta už bola zneplatnená používateľom alebo bankou. Samotný problém vyplýva z dôvery bánk a finančných inštitúcií, ktoré pri platbách mobilnými aplikáciami údajne neoverujú stav karty. Uvedené zraniteľnosti zvyšujú riziká vyplývajúce z incidentov súvisiacich s únikom bankových údajov. Bankové inštitúcie a výrobcovia aplikácií prisľúbili detailnú analýzu a nasadenie príslušných protiopatrení.

Francúzske OČTK zadržali a obvinili CEO Telegramu

Francúzske OČTK zadržali zakladateľa TELEGRAMU v súvislosti s nedostatočným moderovaním obsahu na sociálnej sieti, ktorá umožňuje činnosť kyberzločincov a ďalšiu nelegálnu činnosť. Vedenie spoločnosti sa vyjadrilo, že dodržiava všetky normy a nariadenia EÚ a zadržanie jej zakladateľa považuje za bezprecedentné a očakáva jeho skoré prepustenie. Francúzski vyšetrovatelia následne formálne obvinili DUROVA, že platforma Telegram šíri detskú pornografiu a umožňuje kyberkriminálnikom vykonávať nelegálnu činnosť. Ďalšie obvinenia sa týkajú nedostatočnej spolupráce s OČTK pri vyšetrovaní a žiadostiach o informácie o používateľoch platformy. Zároveň boli zverejnené informácie, že francúzske OČTK už dlhšiu dobu Durova vyšetrovali. Durov má aj francúzske občianstvo, po zaplatení kaucie bol prepustený a do súdneho pojednávania nesmie opustiť Francúzsko.

VÝZNAMNÉ UDALOSTI VO SVETE



Vydieračská skupina Mad Liberator cieli na obete používajúce Anydesk

Bezpečnostní výskumníci zverejnili informácie o novej vydieračskej skupine MAD LIBERATOR, ktorá sa zameriava na exfiltráciu a zverejňovanie údajov používateľov nástroja ANYDESK. Útočníci na základe náhodne generovaných „Anydesk Connection ID“ skúšajú zostavovať spojenia, až kým nejaká z obetí spojenie nepovolí. Následne stiahnu a spustia malvér s názvom „Microsoft Windows Update“, ktorý slúži na prekrytie obrazovky oknom informujúcim o prebiehajúcej aktualizácii operačného systému a deaktiváciu klávesnice, čím dochádza k maskovaniu vykonávaných úkonov. Anydesk File Transfer je v rámci útoku využívaný na exfiltráciu dát z OneDrive, sieťových a lokálnych úložísk. Po útoku na zariadeniach obete vytvárajú aj ransomnote.

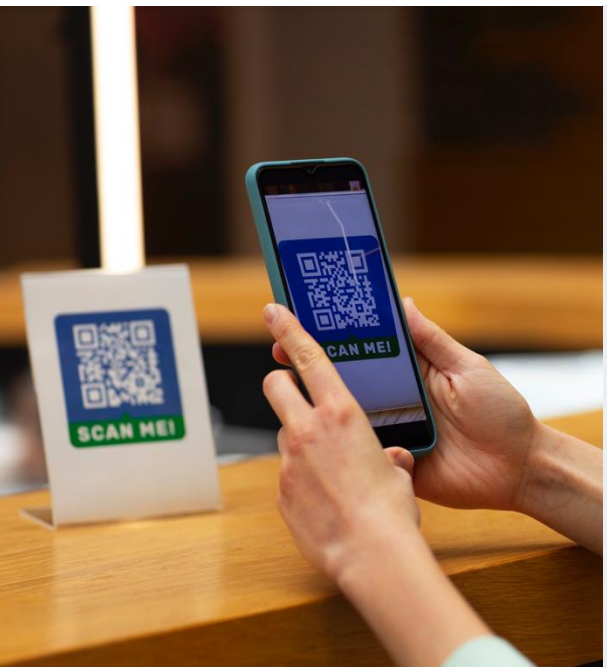
Nárast počtu malvérov cielených na platformu macOS

Malvér BANSHEE STEALER sa zameriava na exfiltráciu citlivých údajov zo zariadení s operačným systémom macOS. Dáta dokáže exfiltrovať zo súborov, webových prehliadačov a ich rozšírení, iCloud Keychain, aplikácie Notes a kryptopeňaženiek. Škodlivý softvér testuje, či nie je spúšťaný vo virtualizovanom prostredí a prostredníctvom CFLocaleCopyPreferredLanguage API sa zameriava na zariadenia, kde primárny jazyk nie je ruština. Bezpečnostní výskumníci objavili aj ďalšiu rodinu malvéru cielenú na macOS, ktorý zneužíva SwiftUI na zobrazenie výzvy na zadanie hesla, Apple Open Directory API na jeho overenie a až následne sťahuje a spúšťa škodlivé skripty z riadiaceho servera útočníka. Vo všeobecnosti možno pozorovať nárast malvérov cielených na platformu macOS.

USA varovali pred vplyvovými operáciami Iránu

FBI, CISA a ODNI v súvislosti s nadchádzajúcimi prezidentskými voľbami varovali pred kybernetickými útokmi zo strany IRÁNU na infraštruktúru prezidentských kandidátov a vplyvovými operáciami zameranými na širokú verejnosť. FBI a CISA potvrdili nedávno avizovaný prienik do Trumpovej kampane a útok pripísali iránskym APT. Spoločnosť OPENAI informovala, že deaktivovala používateľské účty ChatGPT asociované s tvorbou dezinformačného obsahu v rámci iránskych vplyvových operácií skupiny STORM-2035. Spoločnosť MICROSOFT za posledných 6 mesiacov taktiež zaznamenala výrazný nárast vplyvových operácií Iránu a Ruska, cielených primárne na prezidentské voľby v USA. Z dlhodobého pohľadu na vplyvové operácie nejde o nič nové, nakoľko Irán má popredné miesto spolu s Ruskom, Severnou Kóreou a Čínou.

VÝZNAMNÉ UDALOSTI VO SVETE



Rozsiahla quishingová kampaň na získavanie prihlasovacích údajov do MS 365

Útočníci v rámci rozsiahlej quishingovej kampane slúžiacej na zber prihlasovacích údajov do MICROSOFT 365 zneužívajú cloudový nástroj MICROSOFT SWAY. Phishingové e-maily obete presmerovávajú na prezentácie vytvorené prostredníctvom služby Sway, ktoré obsahujú QR kódy slúžiace na presmerovanie na ďalšie stránky so škodlivým obsahom. Na dodatočné maskovanie phishingového obsahu útočník použil službu CLOUDFLARE TURNSTILE. Zneužitie QR kódov umožňuje obísť bezpečnostné prvky, ktoré škodlivý obsah rozpoznávajú len na základe analýzy textového obsahu a začína byť obľúbenou metódou šírenia phishingových URL v kampaniach cielených primárne na mobilných používateľov.

Nové metódy exfiltrácie citlivých údajov z AI systémov vrátane MS 365 Copilot

Bezpečnostný výskumník WUNDERWUZZI zverejnil informácie o zraniteľnosti MICROSOFT 365 COPILOT, ktorú bolo prostredníctvom tzv. ASCII smuggling útoku možné zneužiť na exfiltráciu citlivých údajov. Spoločnosť MICROSOFT zraniteľnosť už opravila, ale zároveň upozornila na bezpečnostné riziká vyplývajúce z využívania nedostatočne zabezpečených Copilot botov, ktoré sú verejne dostupné a bez mechanizmov autentifikácie. Ďalší výskumníci demonštrovali viaceré metódy útokov zameraných na zneužitie AI systémov ako Copilot a s narastajúcou popularitou a prehlbujúcou sa integráciou do systémov to začína vytvárať novú oblasť rizika.

VÝZNAMNÉ UDALOSTI VO SVETE

- Ruská hackerská skupina APT28, známa aj ako Fancy Bear, opäť útočí na diplomatické misie.
- Artefakty vytvorené v rámci GitHub Actions môžu byť potenciálne zneužité na získanie prihlasovacích tokenov, čo môže viesť k neoprávnenému prístupu k citlivým údajom a systémom.
- Skupiny napojené na ruskú Federálnu bezpečnostnú službu (FSB) sa v rámci kyberútokov zameriavajú na ruskú opozíciu, ako aj na rôzne subjekty v Spojených štátoch a Európe.
- Ransomvérová skupina Qilin sa v rámci svojich útokov zameriava na krádež dát z prehliadačov Chrome.
- V Spojených štátoch amerických bol obvinený člen ruskej ransomvérovej skupiny Karakurt.
- Aktér s prezývkou Greasy Opal, ktorý poskytuje nástroje na obídenie CAPTCHA systémov, operuje z územia Českej republiky.
- Bola objavená nová metóda perzistencie na zariadeniach s operačným systémom Linux, ktorá umožňuje útočníkom udržať si prístup k infikovaným systémom aj po reštarte alebo aktualizácii.
- Technika AppDomain Injection umožňuje útočníkom zneužiť ľubovoľnú .NET aplikáciu tým, že injektujú škodlivý kód do aplikačnej domény (AppDomain).
- Ruská hackerská skupina APT29, známa aj ako Cozy Bear, využíva exploity, ktoré sú takmer identické s tými, ktoré sa nachádzajú v komerčných spyware nástrojoch.
- FBI a partneri rozložili ransomvérové skupiny RADAR a DISPOSSESSOR, ktoré boli aktívne od augusta 2023 a svoje aktivity zameriavali na malé a stredne veľké podniky.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná zraniteľnosť v jadre Android

Spoločnosť Google vydala balík opráv pre OS Android, ktorý okrem iného rieši vysoko závažnú zero-day zraniteľnosť jadra, umožňujúcu vzdialené vykonávanie kódu. Zraniteľnosť je pravdepodobne zneužívaná pri cielených útokoch.

Zraniteľnosti v Roundcube umožňujú exfiltráciu citlivých údajov a rozposielanie e-mailov

Populárna webmailová platforma Roundcube obsahuje tri vysoko závažné zraniteľnosti, ktoré by vzdialený neautentifikovaný útočník zaslaním škodlivého e-mailu mohol zneužiť na realizáciu XSS útoku, získanie perzistencie v systéme obete, krádež citlivých údajov a rozposielanie e-mailových správ.

Zero day zraniteľnosti Windows vedú k downgrade systému

Bezpečnostný výskumník spoločnosti SafeBreach Alon Leviev na konferencii Black Hat 2024 odhalil dve zero-day zraniteľnosti. Vysoko závažné zraniteľnosti sa týkajú zvyšovania privilégií v systéme Windows Backup (VBS) vrátane podmnožiny Azure Virtual Machine SKUS.

Kritická bezpečnostná zraniteľnosť v OpenSSH

Vývojári nástroja OpenSSH vydali bezpečnostnú aktualizáciu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť. Zraniteľnosť možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad zraniteľným systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť „Sinkclose“ v procesoroch AMD

Spoločnosť AMD varuje pred vysoko závažnou zraniteľnosťou procesora, známou ako „SinkClose“. Táto chyba ovplyvňuje všetky procesory AMD vyrobené od roku 2006 a umožňuje útočníkom zvyšovanie privilégií a ľubovoľné vykonávanie kódu.

Zraniteľnosť MS Office a 365 umožňujúca získanie NTLM hashov

Spoločnosť Microsoft zverejnila informácie a odporúčania pre mitigáciu zraniteľnosti MS Office a MS 365 Apps, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na exfiltráciu NTLM hashov používaných v rámci autentifikácie.

18 rokov stará zraniteľnosť „0.0.0.0“

Výskumný tím spoločnosti Oligo Security poukázal na zraniteľnosť s názvom “0.0.0.0 Day”, ktorá ovplyvňuje webové prehliadače Google Chrome, Mozilla Firefox, Apple Safari a prehliadače na báze Chromium. Zraniteľnosť umožňuje škodlivým webovým stránkam obchádzať zabezpečenie prehliadača a komunikovať so službami spustenými v lokálnej sieti. Útočníkovi umožňuje získanie neoprávneného prístupu k lokálnym službám a vzdialené vykonanie kódu. Zraniteľnosť je známa od roku 2006.

Zraniteľnosti nástroja pre správu hesiel 1Password pre MacOS

Vývojári nástroja pre správu hesiel 1Password for Mac vydali bezpečnostné aktualizácie, ktoré opravujú dve bezpečnostné zraniteľnosti umožňujúce získanie neoprávneného prístupu k uloženým heslám. CVE-2024-42218 a CVE-2024-42219 možno zneužiť na obídenie bezpečnostných mechanizmov operačného systému macOS a mechanizmov riadenia vzájomnej komunikácie medzi procesmi.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti v Ivanti Virtual Traffic Manager a Ivanti Neurons for ITSM

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Virtual Traffic Manager a Neurons for ITSM, ktoré opravujú 3 bezpečnostné zraniteľnosti, z toho 2 sú označené ako kritické. Zneužitím zraniteľností je možné získať neoprávnený prístup do systému a k citlivým údajom.

Kritické zraniteľnosti v produktoch SAP

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 17 zraniteľností, z toho 2 sú označené ako kritické. Kritické zraniteľnosti sa nachádzajú v produktoch SAP BusinessObjects Business Intelligence Platform a SAP Build Apps a možno ich zneužiť na realizáciu SSRF útokov a získanie neoprávneného prístupu do systému.

Microsoft v rámci augustového Patch Tuesday opravil 9 kritických zraniteľností

Spoločnosť Microsoft vydala v auguste 2024 balík opráv pre portfólio svojich produktov opravujúci 90 zraniteľností, z ktorých 24 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú v produktoch Microsoft Dynamics 365, Microsoft Copilot Studio a Azure Health Bot a v komponentoch grub2, shim, Windows TCP/IP, Windows Reliable Multicast Transport Driver a Windows Network Virtualization. Zraniteľnosti s označením CVE-2024-38189, CVE-2024-38178, CVE-2024-38193, CVE-2024-38106, CVE-2024-38107 a CVE-2024-38213 sú aktívne zneužívané útočníkmi.

Microsoft odhalil bezpečnostné zraniteľnosti v OpenVPN

Bezpečnostní výskumníci zo spoločnosti Microsoft na hackerskej konferencii Black Hat USA 2024 zverejnili informácie o 4 zraniteľnostiach OpenVPN, ktorých zreťazením by vzdialený útočník mohol získať úplnú kontrolu nad systémom. Vývojári OpenVPN zraniteľnosti opravili ešte v marci 2024 vydaním verzie 2.6.10.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v module WordPress GiveWP

Modul WordPress GiveWP, ktorý poskytuje možnosť vytvorenia darcovského rozhrania na webstránkach, obsahuje kritickú zraniteľnosť súvisiacu s nedostatočným overovaním používateľských vstupov. Jej zneužitím dokáže útočník vzdialene vykonávať kód a mazať súbory. Môže získať úplnú kontrolu nad zraniteľnou inštanciou WordPress.

Kritické zraniteľnosti v produkte SolarWinds

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie pre službu Web Help Desk (WHD), ktoré opravujú kritické zraniteľnosti s označením CVE-2024-28986 a CVE-2024-228987. Vzdialený útočník ich môže zneužiť na vzdialené vykonávanie kódu a neoprávnený prístup do systému.

Aktívne zneužívaná zraniteľnosť v Google Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj webový prehliadač Chrome, ktoré opravujú 19 zraniteľností. Najzávažnejšie zraniteľnosti v komponentoch V8, Passwords, Skia, Fonts a Autofill možno zneužiť umožňujú vzdialené vykonanie kódu a zneprístupnenie služby. Zraniteľnosť s označením CVE-2024-7965 je aktívne zneužívaná útočníkmi.

Kritická zraniteľnosť v doplnku WordPress WPML

Vývojári populárneho doplnku WordPress WPML slúžiaceho na vytváranie viacjazyčných stránok vydali bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť. Zraniteľnosť s označením CVE-2024-6386 umožňuje vykonanie škodlivého kódu a získanie úplnej kontroly nad inštanciou redakčného systému WordPress.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť FORTRA FileCatalyst Workflow

Fortra FileCatalyst Workflow obsahuje kritickú zraniteľnosť, ktorá umožňuje vzdialeným útočníkom administrátorský prístup ku prednastavenej databáze softvéru, čím môžu získať úplnú kontrolu nad zraniteľnou webovou aplikáciou.

MESAČNÍK ZRANITEĽNOSTÍ AUGUST 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
   - Operačný systém Android
   - Roundcube
   - OpenSSH
   - Procesory AMD EPYC, Ryzen, AMD Threadripper PRO, AMD Athlon 3000 Mobile, AMD Instinct MI300A
   - Google Chrome, Mozilla Firefox, Apple Safari, webové prehliadače na báze Chromium
   - 1Password 8 for Mac
   - Ivanti Virtual Traffic Manager, Ivanti Neurons for ITSM
   - SAP Build Apps, BusinessObjects Business Intelligence Platform,BEx Web Java Runtime Export Web Service, CRM ABAP, Commerce, Commerce Backoffice, Commerce Cloud, Content Server, Document Builder, NetWeaver Application Server ABAP, Permit to Work, Replication Server, S/4 HANA, Shared Service Framework, Student Life Cycle Management (SLcM), Web Dispatcher
   - Microsoft .NET 8.0, App Installer, Azure Connected Machine Agent, Azure CycleCloud, Azure Health Bot, Azure IoT Hub Device Client SDK, Azure Linux, Azure Stack Hub, C SDK for Azure IoT, CBL Mariner, Dynamics CRM Service Portal Web Resource, Microsoft 365 Apps for Enterprise, Microsoft Copilot Studio, Microsoft Dynamics 365 (on-premises) version 9.1, Microsoft Edge (Chromium-based), Microsoft Office, Microsoft OfficePLUS, Microsoft Outlook, Microsoft PowerPoint, Microsoft Project, Microsoft Teams for iOS, Microsoft Visual Studio, Remote Desktop client for Windows Desktop, Windows, Windows Server
   - OpenVPN
   - WordPress plugin GiveWP
   - SolarWinds WHD

- Google Chrome
- WordPress plugin WPML
- FORTRA FileCatalyst Workflow

csirt.gov.sk/posts/1306.html