MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Marec 2024

TLP: White

Kybernetickým priestorom v marci 2024 rezonovalo hneď niekoľko tém súvisiacich s prudkým rozvojom v oblasti informačných technológií a umelej inteligencie, odhaľovaním kritických bezpečnostných zraniteľností v celosvetovo používaných zariadeniach a produktoch a problematikou stotožňovania kybernetických útokov so štátom sponzorovanými hackerskými skupinami z Čínskej ľudovej republiky a Ruskej federácie.

Prvou témou bolo **využitie umelej inteligencie útočnými skupinami na tvorbu deepfake videí**. **Klamlivé videá** zneužívajúce identitu veľkých spoločností, televíznych staníc, politicky aktívnych a verejne známych osobností, ktorých cieľom bolo **šírenie naratívov nabádajúcich na investovanie do kryptomien**, vládna jednotka **CSIRT.SK zaznamenala aj v rámci Slovenskej republiky**. Umelá inteligencia prináša nové možnosti tvorby klamlivých scenárov s cieľom získať dôveru alebo vyvolať paniku u cieľov phishingových aj propagandistických kampaní. V prípade investičných podvodov do kryptomien útočníci deepfake videá zneužívajú na vytvorenie dôveryhodnej prezentácie falošných produktov a služieb, ktoré sľubujú vysoké zisky za krátky čas. Cieľom útočníkov je získať citlivé informácie od svojich obetí, ako sú prihlasovacie údaje, bankové údaje alebo iné osobné údaje, ktoré priamo alebo s odstupom času zneužívajú na zárobok a páchanie počítačovej kriminality.

Zneužitie deepfake v praxi prináša nové **technologické výzvy spojené s rozpoznávaním obsahu** generovaného umelou inteligenciou a **obavy o celkovú bezpečnosť digitálnych ekosystémov a pred zásahmi do reálneho života v podobe ovplyvňovania verejnej mienky**. Verné napodobnenie výzoru a hlasu verejne známych osobností a inštitúcií možno zneužiť na šírenie falošných odkazov, diskreditáciu alebo dokonca manipuláciu verejnej mienky. V súvislosti s touto problematikou možno sformulovať **základné odporúčania na rozpoznanie deepfake obsahu** generovaného umelou inteligenciou:

- **kritické myslenie:** Najsilnejším nástrojom na odhaľovanie podozrivého obsahu je zdravý rozum. Buďte obzvlášť obozretní pri nezvyčajných vyjadreniach známych osobností.
- **dôkladne overujte zdroj informácií:** Skúmajte dôveryhodnosť zdroja obsahu. Ak sa jedná o videá, overte pôvodný zdroj alebo autorstvo. Nezakladajte si len na jednom zdroji informácií, ale radšej skontrolujte viacero nezávislých zdrojov.
- **všímajte si kvalitu videí:** Deepfake videá môžu mať niekedy nízku kvalitu alebo nekonzistentnú grafiku. Hľadajte znaky ako rozostrenie, nezladené pohyby alebo nesúlad farieb, ktoré by mohli naznačovať, že video je upravené. Vizuálne nedostatky môžete ľahšie spozorovať na obrazovke s vysokým rozlíšením.
- **všímajte si nezvyčajné pohyby a správanie postáv:** Deepfake videá často zobrazujú postavy, ktoré vyzerajú nezvyčajne alebo správajú sa nerealisticky. Pozorne sledujte pohyby pier, očí a iné detaily, ktoré by mohli naznačovať, že video je falošné.
- **všímajte si nedostatky a chyby vo zvuku:** Ak je video doprevádzané zvukom, skontrolujte, či sa zvuk zhoduje s pohybmi pier a hlasovými charakteristikami postavy. Nezrovnalosti medzi zvukom a vizuálnym obsahom môžu naznačovať, že video je deepfake.

TLP: White

Tieto odporúčania Vám môžu pomôcť rozpoznať deepfake obsah a zvýšiť Vašu schopnosť chrániť sa pred súvisiacimi pokusmi o manipuláciu.

O témach kybernetickej bezpečnosti vo svete AI na konferencii **ITAPA AI&ROBOTICS** diskutovali aj zástupcovia Národného centra kybernetickej bezpečnosti SK-CERT a Ministerstva investícií, regionálneho rozvoja a informatizácie SR.

Primárnou **témou hackerskej súťaže Pwn2Own, ktorá sa konala od 20. do 22. marca 2024 v kanadskom meste Vancouver, bolo hľadanie bezpečnostných zraniteľností** v 8 kategóriách zameraných na virtualizačné platformy, webové prehliadače, podnikové systémy a aplikácie, serverové technológie, lokálnu eskalácia privilégií, komunikačné systémy, cloudové a kontajnerizačné technológie a automobily. Na základe sumárnej správy spoločnosti TREND MICRO sa **bezpečnostným výskumníkom podarilo odhaliť 29 zero-day zraniteľností** a veľké množstvo ďalších chýb, za ktoré si **odniesli výhry v celkovej hodnote 1 132 500 dolárov**. Tímu SYNACKTIV sa podarilo zvíťaziť v kategórii automobily, ktorej **cenou bol automobil Tesla Model 3**. Výrobcovia zasiahnutých zariadení a produktov v priebehu marca postupne vydávali bezpečnostné aktualizácie na opravu týchto zraniteľností. Súťaže tohto formátu posúvajú hranice ofenzívnej bezpečnosti, prispievajú k zvyšovaniu kybernetickej bezpečnosti produktov a propagujú problematiku IT bezpečnosti naprieč všetkými generáciami.

Z pohľadu kybernetických útokov **USA a krajiny EÚ zaznamenali aktivity** štátom sponzorovaných **skupín z Ruska** (APT28 – FANCY BEAR, APT29 – COZY BEAR / MIDNIGHT BLIZZARD) **a z Číny** (APT31 – ZIRCONIUM, APT41 – VOLT TYPHOON).

Ministerstvo spravodlivosti USA v marci 2024 **obvinilo 7 členov skupiny APT31**, ktorí mali byť zapojení do kybernetických **útokov na prvky kritickej infraštruktúry** a poslalo tak Čínskej ľudovej republike jasný odkaz, že disponuje dôkazmi mapujúcimi jej činnosť. **Fínska polícia** skupine **formálne pripísala** kybernetický **útok na parlament z roku 2020**. **Národné centrum kybernetickej bezpečnosti Veľkej Británie** **vyhlásilo**, že táto Čínou sponzorovaná skupina bola zodpovedná za **kompromitáciu e-mailového servera parlamentu** v roku 2021.

Vyšetrovanie aktivít skupiny APT31 proti USA, Fínsku a Veľkej Británii poukazuje aj na komplikácie spojené s **atribúciou kybernetických útokov**. Aj keď môže byť identifikácia páchateľov kľúčová pre podniknutie adekvátnych protiopatrení, proces atribúcie môže byť **náročný a rizikový**. Nesprávna identifikácia páchateľov môže viesť k diplomatickému napätiu, eskalácii konfliktov alebo dokonca k nespravodlivým represiám. Pri atribúcii útokov je preto nevyhnutné postupovať opatrne a s dostatočnými dôkazmi, aby bolo minimalizované riziko falošnej identifikácie a následných negatívnych dôsledkov.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci marec 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. Aj tento mesiac sa objavila phishingová kampaň zameraná na občanov Slovenskej republiky, v ktorej útočníci, predstierajúci totožnosť Europolu a vysokopostavených členov Polície SR, posielajú svojim obetiam falošné predvolania kvôli prechovávaniu detskej pornografie a podobným sexuálnym deliktom. Nahlásené boli aj správy z kampane Sextortion, kde sa podvodníci pokúšajú presvedčiť obeť, že si ju cez jej kameru natočili pri sledovaní videí pre dospelých, a vydierať ju.

Objavila sa tiež dlhodobo trvajúca spear-phishingová kampaň, v ktorej sa útočníci vydávajú za vedúceho zamestnanca obete a požadujú prevod väčšej sumy na zahraničné účty.

Vládna jednotka CSIRT prijala v marci hlásenie dvoch ransomvérových incidentov, ktoré vyšetruje. Závažnejší z nich sa stal v Slovenskej národnej knižnici v Martine a bol medializovaný. Knižnica prišla o významnú časť systému pre digitalizáciu písomností v jej majetku. Vďaka kvalitnému manažmentu zálohovania však incident nespôsobil väčšie nezvratné škody. Druhý ransomvérový útok zasiahol webovú stránku organizácie v konštituencii CSIRT.SK na strane webhostingu. Organizácia sa o ňom dozvedela až po kontaktovaní jednotkou s informáciou, že útočníci plánujú zverejniť ukradnuté dáta. Vzhľadom na to, že išlo o verejné dáta, ich zverejnenie útočníkom neprestavuje riziko úniku osobných informácií.

Zaujímavým incidentom bola tiež prítomnosť škodlivého softvéru na ťažbu kryptomien (konkrétne CoinMiner) v evidenčnom systéme jednej organizácie. Systém bol v správe externého dodávateľa. Pri obnove systému bol priamy prístup z internetu zamenený za bezpečnejší prístup cez VPN rozhranie.

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 útoky vo svete

Ruská APT28 upravuje malvér a vyvíja nové metódy jeho šírenia



Ruská štátom sponzorovaná hackerská skupina APT28 (FANCY BEAR) pokračuje vo phishingových kampaniach, ktorých cieľom je infikovať systémy obete malvérom a získať citlivé údaje. Špecifikom týchto kampaní je využívanie imitácií dokumentov od vládnych aj mimovládnych organizácií v Európe, Ázii a Amerike. Analýza spoločnosti IBM vyzdvihuje schopnosť APT28 efektívne a rýchlo modifikovať funkcie používaného malvéru a vyvíjať nové metódy jeho šírenia. Vzhľadom na skutočnosť, že skupina často zneužíva kritické zraniteľnosti v produktoch MICROSOFT EXCHANGE a OUTLOOK, mimoriadny význam z hľadiska prevencie má funkčný proces manažmentu zraniteľností.

Ruská APT29 opäť prenikla do systémov spoločnosti MICROSOFT



Spoločnosť MICROSOFT informovala, že ruská štátom sponzorovaná hackerská skupina APT29 (MIDNIGHT BLIZZARD) získala prístup k jej interným systémom a repozitárom zdrojového kódu. Incidentom neboli zasiahnuté dáta zákazníkov. Na prienik do systémov hackeri zneužili údaje získané útokom v januári 2024, počas ktorého kompromitovali mailový server spoločnosti prostredníctvom tzv. password-spraying útoku. Počas tohto typu útoku sa útočník pokúša o prihlásenie na rôzne používateľské účty pomocou toho istého hesla. Uvedený prípad poukazuje na dôležitosť riadenia a ochrany prístupov pomocou viacfaktorovej autentifikácie, kvalitnej politiky hesiel a jej kontroly a vynútenej zmeny a zneplatnenia akýchkoľvek citlivých údajov, ktoré mohli byť v rámci kybernetických incidentov odcudzené.

TLP: White

Ruská APT29 rozširuje cielenie phishingových kampaní



Ruská štátom sponzorovaná hackerská skupina APT29 (MIDNIGHT BLIZZARD) vykonáva rozsiahle phishingové útoky na politické strany v Nemecku, ktorých cieľom je získať prístup k citlivým údajom nemeckých politikov. Na dosiahnutie tohto cieľa APT29 využíva phishingové správy obsahujúce odkaz na stiahnutie ZIP súboru s dropperom ROOTSAW, ktorý následne sťahuje malvér WINELOADER. WINELOADER zdieľa viacero funkcionalít s predchádzajúcimi rodinami malvéru, ktoré v minulosti skupina APT29 používala. Hlavné riziko predstavuje rozšírenie cielenia z diplomatických misií na politické strany a možno predpokladať rovnaké cielenie aj na ďalšie členské štáty EÚ.

Ministerstvo spravodlivosti USA obvinilo členov čínskej APT31



Ministerstvo spravodlivosti USA obvinilo 7 členov čínskej štátom sponzorovanej hackerskej skupiny APT31 (ZIRCONIUM), ktorí mali vykonávať kybernetické útoky na kritickú infraštruktúru USA. Obvinenie predstavuje jasný odkaz Čínskej ľudovej republike, že aktivity skupiny monitorujú a disponujú dôkazmi mapujúcimi ich činnosť. Po tomto kroku USA aj FÍNSKO a VEĽKÁ BRITÁNIA atribuovali skupine APT31 viaceré kybernetické útoky s kritickými dopadmi. Fínska polícia skupine formálne pripísala kybernetický útok na parlament z roku 2020. Národné centrum kybernetickej bezpečnosti Veľkej Británie vyhlásilo, že táto Čínou sponzorovaná skupina bola zodpovedná za kompromitáciu e-mailového servera parlamentu v roku 2021.

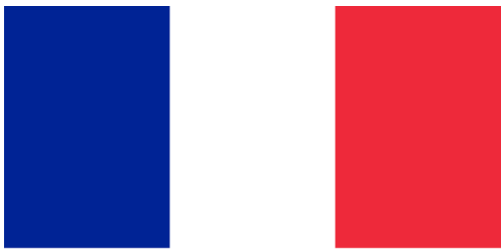
Americká agentúra CISA varovala subjekty kritickej infraštruktúry pred útokmi čínskej APT41

Agentúra CISA v spolupráci s americkou vládou, NSA, FBI a medzinárodnými partnermi varovala subjekty kritickej infraštruktúry USA pred aktivitami čínskej štátom podporovanej hackerskej skupiny APT41 (VOLT TYPHOON). Séria dokumentov obsahuje strategické odporúčania pre vrcholový manažment, praktické rady na zabezpečenie systémov, detailnú analýzu zaužívaných taktík, techník a postupov (tzv. TTP) a zoznam technických indikátorov kompromitácie. Vzhľadom na modus operandi skupiny, ktorý sa zameriava na zneužitie zraniteľností v systémoch voľne dostupných z internetu, je kritické minimalizovať ich počet, vykonávať pravidelnú aktualizáciu systémov, implementovať viacfaktorovú autentifikáciu a centralizovane uchovávať logy zo všetkých zariadení a systémov v infraštruktúre.

Spoločnosť CISCO upozornila na masívnu kampaň cielenú na VPN služby

Spoločnosť CISCO nedávno upozornila na rozsiahlu kampaň zameranú na pokusy o prihlásenie sa jedným heslom do rôznych účtov naprieč zákazníkmi (tzv. password-spraying), ktorí využívajú Cisco VPN. Útoky sa zrejme zameriavajú aj na iné služby VPN a zatiaľ nie je jasné, či sú súčasťou prieskumnej činnosti alebo cieleného útoku. Bezpečnostní výskumníci Aaron Martin a Chris Grube zverejnili informácie, že táto aktivita môže súvisieť s botnetom „Brutus“, ktorý v súčasnosti využíva viac ako 20 000 IP adries po celom svete. Prevádzkovatelia botnetu doposiaľ neboli jednoznačne identifikovaní, ale výskumníkom sa podarilo identifikovať dve IP adresy, ktoré boli v minulosti spojené s aktivitami APT29 (MIDNIGHT BLIZZARD).

Rozsiahly DDoS útok na francúzske vládne weby



Webové stránky vládnych organizácií vo Francúzsku sa stali terčom rozsiahlych DDoS útokov. K útokom sa prostredníctvom sociálnej siete TELEGRAM prihlásili hackerská skupina Anonymous Sudan, ruské komunitné hackerské hnutie NoName057(16) a viacero menších hackerských skupín. Odborníci v oblasti kybernetickej bezpečnosti varujú pred potenciálnymi dôsledkami takýchto útokov a zdôrazňujú potrebu implementácie opatrení na ochranu webových stránok pred DDoS útokmi. Skupina NoName057(16) sa dlhodobo špecializuje na vykonávanie DDoS útokov a využíva softvér DDoSia, ktorý si inštalujú podporovatelia skupiny. Ten po nainštalovaní z riadiaceho servera stiahne zoznam aktuálnych cieľov útoku.

Americká NSA odporúča nasadenie princípov zero-trust

Národná bezpečnostná agentúra NSA odporúča využitie architektúry nulovej dôvery (eng. Zero Trust Architecture), ktorej primárnym cieľom je minimalizácia únikov dát, dopadov ich zneužitia a ďalších rizík v oblasti kybernetickej bezpečnosti. Jedná sa o bezpečnostný koncept, ktorý je postavený na princípe „nedôverovať a vždy overovať“, kedy pred každým poskytnutím prístupu k chráneným aktívam dochádza k overeniu identity používateľa. Kľúčovými mechanizmami zero-trust sú správa identít a prístupov, mikrosegmentácia sietí a služieb, použitie viacfaktorovej autentifikácie, priebežný monitoring a hodnotenie rizík. NSA od aplikovania týchto princípov očakáva zvýšenie odolnosti subjektov pred narastajúcim počtom útokov čínskych a ruských APT skupín.

TLP: White

Nemecký BSI varuje pred zraniteľnými inštanciami Microsoft Exchange v Nemecku

Federal Office for Information Security

Nemecký úrad pre ochranu informačných systémov BSI adresne varoval nemeckých prevádzkovateľov základných služieb pred zraniteľnými inštaláciami Microsoft Exchange a poskytol základné odporúčania pre zabezpečenie tejto technológie. V rámci znižovania počtu zraniteľných zariadení v kybernetickom priestore Nemecká spolková republika čelí rovnakým problémom ako jednotky CSIRT v Slovenskej republike, kedy varované subjekty často ani po opakovanom upozornení zraniteľné zariadenia neaktualizujú a zvyšujú tým riziko kompromitácie svojich systémov.

Deštruktívny malvér ACIDPOUR je variantom malvéru ACIDRAIN použitého v roku 2022



Spoločnosť SENTINELONE zverejnila informácie o novom malvéri ACIDPOUR, ktorý bol vytvorený špeciálne pre IOT a sieťové zariadenia. Na základe telemetrických údajov bola prvá vzorka do online služby VIRUSTOTAL odoslaná z Ukrajiny a ukrajinská jednotka pre riešenie kybernetických bezpečnostných incidentov CERT-UA malvér pripisuje skupine UAC-0165 s prepojením na Rusko. ACIDPOUR zdieľa kusy zdrojového kódu s malvérom ACIDRAIN, ktorý bol v roku 2022 použitý k útoku na satelitné modemy KA-SAT a spôsobil aj výpadky satelitného spojenia v rámci SR. Nový variant rozširuje cielenie na zariadenia s architektúrou Linux x86 a dopĺňa ďalšie funkcie pre efektívnu deštrukciu dát na RAID poliach a veľkých úložiskách.

Účastníci hackerskej súťaže Pwn2Own Vancouver 2024 odhalili kritické zraniteľnosti v celosvetovo používaných produktoch



Účastníkom celosvetovo uznávanej hackerskej súťaže Pwn2Own Vancouver 2024 sa podarilo odhaliť viacero bezpečnostných chýb vo webových prehliadačoch (Microsoft Edge, Google Chrome, Apple Safari, Mozilla Firefox), virtualizačných platformách (Oracle Virtualbox, VMware Workstation a ESXI, Microsoft HYPER-V Client), operačných systémoch a serverových technológiách (Microsoft Windows, Exchange a Sharepoint, Ubuntu, Apple MacOS), kancelárskych balíkoch (Adobe Reader, Microsoft Office 365), komunikačných platformách (Zoom, Microsoft Teams, Slack) a automobiloch značky Tesla. V nadväznosti na odhalené zraniteľnosti výrobcovia postupne začali vydávať bezpečnostné aktualizácie na ich odstránenie.

Phishingový útok umožňoval krádež vozidiel Tesla



Bezpečnostní výskumníci Bakry a Mysk demonštrovali, že pomocou phishingového útoku typu Man-in-the-Middle možno kompromitovať používateľské kontá Tesla a tie následne zneužiť na odomknutie vozidiel. Útok spočíva vo vytvorení falošnej wi-fi siete s názvom „Tesla Guest“, ktorý je bežne používaný v servisných strediskách Tesla. Po pripojení obete k tejto sieti dôjde k presmerovaniu na falošný web spoločnosti Tesla, kde nič netušiaci používateľ zadá svoje prihlasovacie údaje. Po zadaní údajov sofistikovaný phishing zobrazí aj výzvu na zadanie jednorazového kódu potrebného pre obídenie viacfaktorovej ochrany. Kombináciou týchto údajov útočník dokáže získať úplnú kontrolu nad účtom obete, asociovať s ním ďalšie mobilné zariadenia a tie následne zneužiť na odomknutie vozidla alebo monitorovanie jeho polohy v reálnom čase.

Japonská spoločnosť FUJITSU obeťou kybernetického útoku

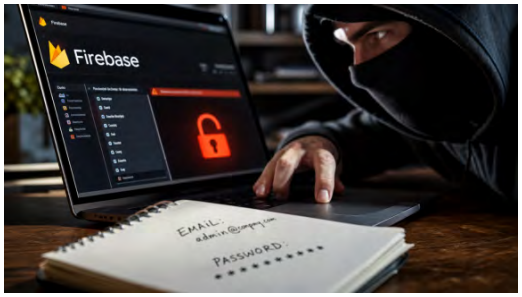
Japonská spoločnosť FUJITSU potvrdila, že sa stala obeťou kybernetického útoku, v rámci ktorého došlo ku kompromitácii viacerých interných systémov spoločnosti. Neznámemu útočníkovi sa pomocou bližšie nešpecifikovanej rodiny malvéru podarilo odcudziť citlivé údaje, vrátane dát klientov. V rámci riešenia incidentu prebieha detailná analýza s cieľom určiť vektor prieniku do systémov a celkový rozsah exfiltrovaných dát. Fujitsu po dokončení analytických úkonov plánuje adresne notifikovať dotknutých klientov. Podobné prípady potvrdzujú, že obeťou kybernetických útokov sa môžu stať aj veľké spoločnosti.

Hackeri zneužívajú kompromitované stránky na platforme WORDPRESS na brute-force útoky



Bezpečnostní výskumníci zaznamenali nový trend zneužívania návštevníkov hacknutých webových stránok s redakčným systémom WORDPRESS na vykonávanie brute-force útokov a inej škodlivej činnosti. Útočník pomocou úprav HTML vzorov redakčného systému do kompromitovaných stránok vkladá kód JavaScript, ktorý z externých zdrojov načítava ďalšie skripty. Tieto skripty z riadiaceho servera útočníka sťahujú súbor JSON obsahujúci URL adresu cieľa, meno používateľa a množinu hesiel, ktoré sa majú otestovať v rámci brute-force útoku. Na základe výsledkov online vyhľadávacej služby PublicHTML bolo infikovaných viac ako 1700 webových stránok. Útočníkom stojacim za touto kampaňou sa dokonca podarilo kompromitovať aj webové stránky asociácie súkromných bánk v Ekvádore.

Nesprávna konfigurácia Google Firebase umožnila prístup k prihlasovacím údajom



Bezpečnostní výskumníci aktívne vyhľadávajú nesprávne nakonfigurované inštancie databáz GOOGLE FIREBASE. V priebehu dvoch týždňov výskumníci identifikovali a upozornili vlastníkov 916 webových stránok, kde konfigurácia umožňovala extrakciu citlivých údajov (osobné údaje a heslá). Je vysoko pravdepodobné, že rovnaký postup aplikujú aj hackeri a získané údaje buď ihneď alebo s odstupom času priamo zneužívajú alebo s nimi obchodujú. Administrátori a vývojári online služieb by pri využívaní cloudových služieb mali dodržiavať odporúčané best practice postupy pre konfiguráciu a zabezpečenie systémov a minimalizovať tak riziko neoprávneného prístupu do infraštruktúry a úniku dát. Vládna jednotka CSIRT.SK s cieľom zvyšovania odolnosti systémov na svojej stránke vydáva návody na hardening systémov.

Phishingová služba DARCULA zneužíva vstavané funkcie Android a iOS



Phishing-as-a-service služba DARCULA na šírenie phishingových URL zneužíva vstavané komunikačné funkcie operačných systémov Android (RCS protokol) a iOS (iMessages). Služba poskytuje predpripravené vzory phishingového obsahu zneužívajúceho primárne identitu poštových doručovateľských služieb po celom svete a na zefektívnenie a automatizáciu svojej činnosti používa populárne technológie Docker a Harbor. S narastajúcim počtom kampaní zneužívajúcich vstavané funkcie mobilných zariadení je potrebné vyvinúť aktivity v súvislosti so zvyšovaním bezpečnostného povedomia a upozorniť potenciálne obete aj na tento typ útoku.

Prehľadová štúdia oblastí zneužitia nástrojov umelej inteligencie



Spoločnosť RECORDED FUTURE zverejnila prehľadovú štúdiu oblastí zneužitia rôznych nástrojov umelej inteligencie v rámci činností hackerských skupín, ktorá identifikuje 4 oblasti. Prvou je tvorba deepfake audio a video obsahu, ktorá môže už v roku 2024 významným spôsobom zvýšiť úspešnosť útokov založených na princípoch sociálneho inžinierstva. Druhú oblasť predstavuje využitie rýchleho generovania textového a obrazového materiálu v rôznych jazykových mutáciách v rámci dezinformačných kampaní. Tretia oblasť spočíva vo využití AI na tvorbu a modifikáciu škodlivých skriptov a malvéru, ktoré efektívne obchádzajú mechanizmy detekcie založené na YARA pravidlách. Poslednou oblasťou je využitie AI na rozpoznávanie identity ľudí alebo identifikáciu výrobcu, typu a konkrétneho modelu zariadení z obrazového a video vstupu.

- **Výpadky IT systémov v McDonald's mali negatívne dôsledky na prevádzky reštaurácií po celom svete**
- **USA obvinili iránskeho hackera, ktorý sa mal podieľať na viacerých kybernetických útokoch na subjekty v USA**
- **Ransomware Phobos pokračuje v cielení na subjekty kritickej infraštruktúry USA**
- **Hackeri zneužívajú QEMU na maskovanie svojej činnosti pomocou tunelovania sieťovej prevádzky**
- **Na platforme Hugging Face bolo identifikovaných viac ako 100 modelov umelej inteligencie so škodlivým obsahom**
- **Belgický výrobca piva Duvel sa stal obeťou ransomvérového útoku, ktorý zastavil výrobu**
- **Brazílski občania sa stali terčom nového bankového trójskeho koňa s názvom CHAVECLOAK**
- **Bezpečnostní výskumníci odhalili nový variant ransomvéru STOPCRYPT s pokročilými mechanizmami maskovania činnosti**

- **Bývalý manažér telekomunikačného operátora v New Jersey vykonával neoprávnené výmeny SIM kariet a umožnil spolupáchateľom hackovať účty zákazníkov spoločnosti**
- **V nadväznosti na zavedenie nových pravidiel pre prístup k erotickému obsahu v štáte Texas spoločnosť PORNHUB začala plošne blokovať prístup na svoje stránky**
- **Viber odmieta tvrdenia palestínskej hacktivistickej skupiny Handala Hack ohľadom prieniku do svojich systémov**

Závažné zraniteľnosti bežných softvérových produktov

Zero-day zraniteľnosti vo webových prehliadačoch Mozilla Firefox



Spoločnosť Mozilla vydala bezpečnostné aktualizácie na opravu dvoch zero-day zraniteľností vo webovom prehliadači Firefox. Zraniteľnosti boli objavené počas hackerskej súťaže Pwn20wn Vancouver 2024. Na obe zraniteľnosti poukázal výskumník Manfred Paul. Úspešné zneužitie zraniteľností umožňuje vykonanie ľubovoľného kódu.

Kritická zraniteľnosť v serveroch Atlassian



Atlassian vydal opravy pre viac ako dve desiatky bezpečnostných chýb vrátane kritickej chyby ovplyvňujúcej Bamboo Data Center a Server. Úspešné zneužitie umožňuje injektovanie škodlivých príkazov bez toho, aby bola potrebná interakcia používateľa.

Ivanti opravila dve kritické zraniteľnosti



Spoločnosť Ivanti vydala opravu dvoch kritických zraniteľností, CVE-2023-46808 a CVE-2023-41724, ktoré sa nachádzajú v nástroji Ivanti Standalone Sentry a Ivanti Neurons for ITSM. Úspešné zneužitie umožňuje útočníkovi ľubovoľné vykonávanie príkazov. Chyby boli predmetom zneužitia troch kyberšpionážnych skupín napojených na Čínu.

Kritické zraniteľnosti v produktoch Fortinet



Spoločnosť Fortinet vydala varovanie pred viacerými kritickými a vysoko závažnými zraniteľnosťami v produktoch FortiClientEMS, FortiOS, FortiProxy a FortiManager. Kritické zraniteľnosti umožňujú útočníkovi vykonávanie kódu alebo príkazov prostredníctvom špeciálne vytvorených paketov alebo HTTP požiadaviek. Vysoko závažné zraniteľnosti sa týkajú obchádzania autorizácie a vykonávania ľubovoľného kódu.

Kritické zraniteľnosti v produktoch VMware



Spoločnosť VMware vydala bezpečnostné aktualizácie na opravu kritických zraniteľností úniku zo sandboxu v produktoch VMware ESXi, Workstation, Fusion a Cloud Foundation. Úspešné zneužitie môže viesť k úniku z virtuálnych počítačov a umožniť útočníkom získať prístup k hostiteľskému operačnému systému.

Zraniteľnosti v produktoch QNAP NAS



Spoločnosť QNAP poukázala na bezpečnostné chyby vo svojich softvérových produktoch NAS vrátane QTS, QuTS hero, QuTScloud a myQNAPcloud, ktoré by mohli autentifikovanému útočníkovi umožniť prístup k zariadeniam. Kritické zraniteľnosti umožňujú obídenie autentifikácie, injektovanie príkazov a injekciu SQL. Zraniteľnosti sa nachádzajú na viac ako 3 miliónoch zariadení, ktoré majú prístup na internet.

Kritické zraniteľnosti v produktoch SAP



Spoločnosť SAP vydala v marci 2024 balík opráv pre svoje produkty opravujúcich 10 zraniteľností v aplikáciách Business Client, Build Apps, NetWeaver AS Java a ďalších. 2 z nich sú označené ako kritické. Úspešné zneužitie umožňuje neautentifikovanému útočníkovi eskaláciu privilégií.

Kritická zraniteľnosť v Ultimate Member doplnku WordPress



Spoločnosť SAP vydala v marci 2024 balík opráv pre svoje produkty opravujúcich 10 zraniteľností v aplikáciách Business Client, Build Apps, NetWeaver AS Java a ďalších. 2 z nich sú označené ako kritické. Úspešné zneužitie umožňuje neautentifikovanému útočníkovi eskaláciu privilégií.

Mesačník zraniteľností Marec 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 tohto mesačné závažné zraniteľnosti
    - Ultimate Member plugin pre WordPress
    - SAP Business Client, Build Apps, NetWeaver AS Java
    - QNAP QTS, QuTS hero, QuTScloud a myQNAPcloud
    - VMware ESXi, Workstation, Fusion a Cloud Foundation
    - Fortinet FortiClientEMS, FortiOS, FortiProxy a FortiManager
    - Ivanti Standalone Sentry a Ivanti Neurons for ITSM
    - Atlassian Bamboo Data Center a Server

https://www.csirt.gov.sk/posts/805.html?csrt=16114082596159579838