UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Centrum informačných a komunikačných technológií

Úsek informačnej a kybernetickej bezpečnosti
Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)
Šrobárova 2, 041 80 Košice
VoIP: +421 (055) 234 2425, IČO: 00397768
csirt@upjs.sk, https://csirt.upjs.sk/

TLP:CLEAR

Týždenná správa csirt.upjs.sk
1.11.2024 – 6.11.2024

TLP:CLEAR

Vypracoval: csirt.upjs.sk

Nová phishingová kampaň sa zameriava na systémy Windows pomocou škodlivých Linuxovými VM

Nedávna phishingová kampaň s názvom 'CRON#TRAP' bola identifikovaná, kde útočníci infikujú systémy Windows pomocou virtuálnych počítačov so zadnými dvierkami Linux (VM), aby získali neoprávnený prístup do podnikových sietí. Táto metóda zahŕňa odosielanie phishingových e-mailov, ktoré vyzývajú k inštalácii linuxového VM obsahujúceho predinštalované zadné vrátka, čo útočníkom umožňuje zachovať si vytrvalosť a vyhnúť sa detekcii. Kampaň využíva virtualizačný softvér QEMU na spustenie Linux VM na napadnutom hostiteľovi Windows. Tento prístup zdôrazňuje vyvíjajúcu sa taktiku aktérov hrozieb pri využívaní multiplatformových nástrojov na infiltráciu a pretrvanie v cieľových prostrediach.

Zero-Click Flaw vystavuje potenciálnemu útoku milióny populárnych úložných zariadení

V sieťových úložných zariadeniach (NAS) spoločnosti Synology, konkrétne v aplikácii SynologyPhotos, bola identifikovaná kritická zraniteľnosť typu zero-click. Táto chyba umožňuje útočníkom získať prístup root bez interakcie používateľa, čo umožňuje krádež údajov, inštaláciu zadných vrátok alebo nasadenie ransomvéru. Zraniteľnosť ovplyvňuje modely BeeStation aj DiskStation. Spoločnosť Synology vydala opravu, v dôsledku nedostatku automatických aktualizácií však mnohé zariadenia môžu zostať nechránené.

Muž zatknutý v Kanade, o ktorom sa predpokladá, že stojí za Snowflake customer breach

Kanadské úrady zatkli 30. októbra 2024 26-ročného Alexandra „Connora“ Moucku z Kitcheneru v Ontáriu na základe žiadosti USA. Moucka je obvinený z krádeže údajov a vydierania viac ako 160 spoločností využívajúcich cloudovú dátovú službu Snowflake. Pôsobiaci pod aliasmi ako „Judische“ a „Waifu“ údajne pristupoval k citlivým údajom o zákazníkoch od veľkých korporácií, vrátane AT&T, TicketMaster, LendingTree, Advance Auto Parts a Neiman Marcus. Porušenia boli uľahčené zneužívaním účtov, ktorým chýbalo viacfaktorové overenie, pomocou poverení získaných z malvéru infostealer. Zatknutie Moucku je súčasťou širšieho vyšetrovania kyberzločineckej skupiny známej ako „UNC5537“, ktorá je spojená s významnými únikmi údajov a pokusmi o vydieranie.

Malware kampaň využíva inteligentné zmluvy Ethereum na kontrolu balíčkov npm Typosquat

Nedávna malvérová kampaň bola zameraná na vývojárov npm prostredníctvom typosquattingu, kde škodlivé balíčky napodobňujú tie legitímne, aby oklamali používateľov. Najmä táto kampaň využíva inteligentné zmluvy Ethereum pre operácie command-and-control (C2), čím sa zvyšuje jej odolnosť voči tradičným snahám o zrušenie. Využitím decentralizovanej povahy blockchainu môžu útočníci dynamicky aktualizovať adresy serverov C2, čo komplikuje detekciu a zmiernenie. Bezpečnostné firmy Checkmarx, Phylum a Socket informovali o tejto vyvíjajúcej sa hrozbe, pričom zdôraznili potrebu zvýšenej ostražitosti pri manipulácii s balíkmi npm.

Google Cloud presadí do roku 2025 viacfaktorové overenie pre všetkých používateľov

Google Cloud oznámil plány zaviesť povinné viacfaktorové overenie (MFA) pre všetkých používateľov do konca roka 2025, aby sa zvýšila bezpečnosť účtu. Uvedenie na trh bude prebiehať v troch fázach:
Fáza 1 (začiatok novembra 2024): Správcovia dostávajú informácie na prípravu na inováciu zabezpečenia.
Fáza 2 (začiatok roka 2025): MFA sa stáva povinným pre všetkých nových a existujúcich používateľov služby Google Cloud, ktorí sa prihlasujú pomocou hesla
Fáza 3 (koniec roka 2025): Ochrana MFA sa rozširuje na federatívnych používateľov s možnosťou povoliť MFA prostredníctvom primárnych poskytovateľov identity alebo priamo cez účty Google.
Cieľom tejto iniciatívy je zmierniť riziká spojené s phishingom a ukradnutými povereniami v súlade s podobnými bezpečnostnými opatreniami implementovanými inými významnými poskytovateľmi cloudových služieb.