Nebezpečná zranitelnost v Chrome umožnila skupině Lazarus krást kryptoměny

24.10.2024 - | PROTEXT

V květnu 2024 odborníci společnosti Kaspersky při analýze incidentů v rámci telemetrie Kaspersky Security Network identifikovali útok pomocí malwaru Manuscrypt, který skupina Lazarus používá od roku 2013 a který byl zdokumentován týmem GReAT ve více než 50 jedinečných kampaních zaměřených na různá odvětví. Další analýza odhalila sofistikovanou škodlivou kampaň, která se ve velké míře spoléhala na techniky sociálního inženýrství a generativní umělou inteligenci a cílila na investory do kryptoměn.

Skupina Lazarus je známá svými vysoce pokročilými útoky na kryptoměnové platformy a v minulosti používala zero-day exploity. Tato nově odhalená kampaň se řídila stejným modelem: Výzkumníci Kaspersky zjistili, že aktér hrozby zneužil dvě zranitelnosti, včetně dosud neznámého typu chyby záměny ve V8, open-source enginu JavaScript a WebAssembly společnosti Google. Tato zranitelnost nultého dne byla opravena jako CVE-2024-4947 poté, co ji společnost Kaspersky nahlásila společnosti Google. Umožňovala útočníkům spustit libovolný kód, obejít bezpečnostní prvky a provádět různé škodlivé činnosti. Další zranitelnost byla použita k překonání ochrany sandboxu V8 prohlížeče Google Chrome.

Útočníci tuto zranitelnost zneužili přes důkladně navrženou falešnou herní webovou stránku, která uživatele vyzývala ke globální soutěži s NFT. Zaměřili se na budování důvěry, aby maximalizovali účinnost kampaně, a navrhli detaily tak, aby propagační aktivity vypadaly co možná nejautentičtěji. To zahrnovalo vytvoření účtů na sociálních sítích X (dříve známé jako Twitter) a LinkedIn, na kterých byla hra propagována po dobu několika měsíců s využitím obrázků vygenerovaných umělou inteligencí. Skupina Lazarus úspěšně integrovala generativní umělou inteligenci do svých operací a odborníci společnosti Kaspersky předpokládají, že útočníci budou vymýšlet další sofistikované útoky s využitím této technologie.

Útočníci se také pokusili zapojit do další propagace kryptoměnové influencery, přičemž využili jejich působení na sociálních sítích nejen k šíření hrozby, ale také k přímému zacílení na jejich kryptoměnové účty.

„Ačkoli jsme již dříve viděli, že aktéři APT usilují o finanční zisk, tato kampaň byla jedinečná. Útočníci šli nad rámec typické taktiky a použili plně funkční hru jako zástěrku pro zneužití zero-day v prohlížeči Google Chrome a infikování cílových systémů. U notoricky známých aktérů, jako je Lazarus, mohou i zdánlivě neškodné akce – například kliknutí na odkaz na sociální síti nebo v e-mailu – vést k úplné kompromitaci osobního počítače nebo celé podnikové sítě. Značné úsilí investované do této kampaně naznačuje, že měli ambiciózní plány, a skutečný dopad by mohl být mnohem širší a potenciálně zasáhnout uživatele a podniky po celém světě,“ komentoval **Boris Larin**, hlavní bezpečnostní expert společnosti Kaspersky GReAT.

Experti společnosti Kaspersky objevili legitimní hru, která se zdála být prototypem verze útočníků. Krátce poté, co útočníci spustili kampaň na propagaci své hry, tvrdili vývojáři skutečné hry, že z jejich peněženky bylo převedeno 20 000 amerických dolarů (přibližně 465 000 Kč) v kryptoměnách. Logo a design falešné hry přesně kopírovaly originál, lišily se pouze umístěním loga a vizuální kvalitou. Vzhledem k těmto podobnostem a shodám v kódu experti společnosti Kaspersky zdůrazňují, že členové skupiny Lazarus vynaložili velké úsilí, aby svému útoku dodali důvěryhodnost. Vytvořili falešnou hru s použitím ukradeného zdrojového kódu, nahradili loga a všechny odkazy na legitimní

hru, aby ve své téměř identické verzi posílili iluzi autenticity.

Podrobnosti o škodlivé kampani byly prezentovány na summitu bezpečnostních analytiků na Bali a nyní je celá zpráva k dispozici na webu Securelist.com.

O týmu globálního výzkumu a analýz

Global Research & Analysis Team (GReAT) byl založen v roce 2008 a působí v samém srdci společnosti Kaspersky, kde odhaluje APT, kyberšpionážní kampaně, závažný malware, ransomware a podvodné trendy kyberzločinu po celém světě. GReAT dnes tvoří více než 40 odborníků, kteří pracují po celém světě – v Evropě, Rusku, Latinské Americe, Asii a na Středním východě. Talentovaní bezpečnostní odborníci zajišťují vedení společnosti v oblasti výzkumu a inovací v oblasti ochrany proti malwaru a přinášejí do odhalování a analýzy kybernetických hrozeb bezkonkurenční odborné znalosti, nadšení a zvídavost.

https://www.ceskenoviny.cz/tiskove/zpravy/nebezpecna-zranitelnost-v-chrome-umoznila-skupine-lazarus-krast-kryptomeny/2586697