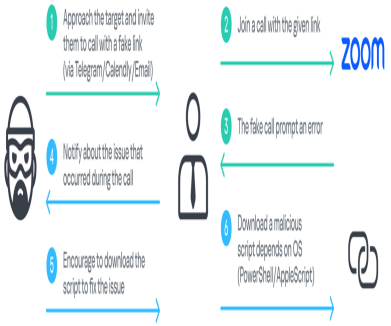

Kaspersky: BlueNoroff colpisce i dirigenti di aziende che usano Windows e macOS con tool basati sullâ??AI

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Milano, 28 ottobre 2025. In occasione del Security Analyst Summit in Thailandia, il Global Research and Analysis Team (GReAT) di Kaspersky ha presentato le piÃ¹ recenti attivitÃ APT attribuite a BlueNoroff, rivelando due campagne malevole denominate â??GhostCallâ?• e â??GhostHireâ?•. Queste operazioni, attive almeno dallâ??aprile 2025, prendono di mira aziende che operano nel settore Web3 e delle criptovalute in India, Turchia, Australia e in diversi altri Paesi, anche in Europa e Asia.

BlueNoroff, una sottodivisione del noto gruppo Lazarus, continua ad ampliare la sua campagna â??SnatchCryptoâ?•, unâ??operazione a scopo di lucro che prende di mira aziende del settore crypto in tutto il mondo. Le recenti campagne â??GhostCallâ?• e â??GhostHireâ?• sfruttano nuove tecniche di infiltrazione e malware personalizzati per compromettere sviluppatori e dirigenti del settore blockchain. Questi attacchi interessano principalmente i sistemi macOS e Windows e sono gestiti attraverso unâ??infrastruttura di comando e controllo unificata.

La campagna GhostCall prende di mira i dispositivi macOS e inizia attraverso un attacco di social engineering estremamente sofisticato e personalizzato. Gli aggressori contattano le vittime tramite Telegram, fingendosi investitori di venture capital e, in alcuni casi, utilizzando account compromessi di veri imprenditori e fondatori di startup per proporre opportunitÃ di investimento o collaborazione. Le vittime vengono quindi invitate a partecipare a falsi incontri di investimento su siti di phishing che imitano le piattaforme Zoom o Microsoft Teams; durante la â??riunioneâ?•, viene richiesto loro di aggiornare il client per risolvere un presunto problema audio. Questa azione porta al download di uno script malevolo che installa il malware sul dispositivo della vittima.

â??Questa campagna si basa su un inganno pianificato con cura e precisione. I cybercriminali riproducono dei video delle vittime precedenti durante incontri organizzati ad hoc per far sembrare le

interazioni delle vere e proprie chiamate e manipolare cosÃ¬ i nuovi utenti. I dati raccolti durante questo processo vengono poi utilizzati non solo contro la vittima iniziale, ma anche per attacchi successivi e di supply-chain, sfruttando le relazioni basate sulla fiducia giÃ esistenti per colpire un numero maggiore di aziende e utentiâ?•,ha commentato Sojun Ryu, Security Researcher del GReAT di Kaspersky.

I cybercriminali impiegano sette catene di esecuzione multistadio, quattro delle quali mai individuate in precedenza, per diffondere una serie di nuovi payload personalizzati, tra cui crypto stealer, browser credential stealer, secrets stealer e Telegram credential stealer.

Nella campagna GhostHire, lâ??APT prende di mira gli sviluppatori di blockchain fingendosi recruiter. Le vittime vengono cosÃ¬ convinte a scaricare ed eseguire un repository GitHub contenente malware, che viene presentato come un test di valutazione delle competenze. GhostHire condivide con la campagna GhostCall lâ??infrastruttura e i tool, ma invece di impiegare videochiamate, si focalizza sul contatto diretto con sviluppatori e ingegneri attraverso false offerte di lavoro. Dopo il primo contatto, le vittime vengono aggiunte su un bot Telegram che invia un file ZIP o un link GitHub, insieme a una breve deadline per completare lâ??attivitÃ . Una volta eseguito, il malware viene installato sul computer della vittima, adattandosi al sistema operativo.

Lâ??uso dellâ??IA generativa ha consentito a BlueNoroff di accelerare il processo di sviluppo del malware e perfezionare le proprie tecniche di attacco. I cybercriminali hanno introdotto nuovi linguaggi di programmazione e aggiunto ulteriori funzionalitÃ , complicando le attivitÃ di rilevamento e analisi. Questa tecnologia consente inoltre agli hacker di gestire ed espandere le proprie operazioni, aumentando sia la complessitÃ che la portata degli attacchi.

â??Rispetto alle campagne precedenti, la strategia di attacco degli hacker si Ã¨ evoluta andando oltre il semplice furto di criptovalute e password dei browser. Lâ??uso dellâ??intelligenza artificiale generativa ha accelerato notevolmente questo processo, facilitando lo sviluppo di malware e riducendo i costi operativi. Lâ??approccio basato sullâ??intelligenza artificiale aiuta a colmare le lacune nelle informazioni disponibili, consentendo attacchi piÃ¹ mirati. Combinando i dati compromessi con le capacitÃ analitiche dellâ??AI, la portata di questi attacchi si Ã¨ ampliata. Ci auguriamo che la nostra ricerca contribuisca a prevenire ulteriori danniâ?•,ha commentato Omar Amin, Senior Security Researcher del GReAT di Kaspersky.

Ulteriori informazioni, compresi gli indicatori di compromissione, sono disponibili nel report su Securelist.com.

Per proteggersi da attacchi come GhostCall e GhostHire, Kaspersky consiglia alle aziende di seguire le seguenti best practice:

Fondato nel 2008, il Global Research & Analysis Team (GReAT) Ã¨ il cuore di Kaspersky e si occupa di scoprire APT, campagne di cyberspionaggio, principali malware, ransomware e strategie criminali clandestine in tutto il mondo. Oggi il GReAT Ã¨ composto da oltre 35 esperti che lavorano a livello globale, in Europa, Russia, America Latina, Asia e Medio Oriente. Professionisti della sicurezza di

grande esperienza che guidano lâ??azienda nella ricerca e nellâ??innovazione anti-malware, mettendo a disposizione expertise, passione e curiositÃ senza precedenti per la ricerca e lâ??analisi delle minacce informatiche.

Seguici su:

Tweets by KasperskyLabIT

http://www.facebook.com/kasperskylabitalia

https://www.linkedin.com/company/kaspersky-lab-italia

https://www.instagram.com/kasperskylabitalia/

https://t.me/KasperskyItalia

Informazioni su Kaspersky

Kaspersky Ã¨ unâ??azienda globale di cybersecurity e privacy digitale fondata nel 1997. Con oltre un miliardo di dispositivi protetti dalle minacce informatiche emergenti e dagli attacchi mirati, la profonda esperienza di Kaspersky in materia di sicurezza e di Threat Intelligence si trasforma costantemente in soluzioni e servizi innovativi per la sicurezza di aziende, infrastrutture critiche, governi e consumatori in tutto il mondo. Il portfolio completo dellâ??azienda comprende una protezione Endpoint leader, prodotti e servizi di sicurezza specializzati e soluzioni Cyber Immune per contrastare le minacce digitali sofisticate e in continua evoluzione. Aiutiamo oltre 200.000 aziende a proteggere ciÃ² che piÃ¹ conta per loro. Per ulteriori informazioni Ã¨ possibile consultare https://www.kaspersky.it/

Contatti:
Immediapress
Contatto di redazione:
NoesisKaspersky Italia

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Immediapress

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Ottobre 28, 2025
Autore
redazione