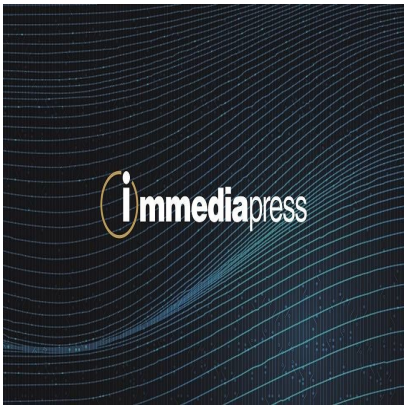

Kaspersky GReAT individua un nuovo spyware HackingTeam attivo dopo anni di inattivitÃ

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Milano, 27ottobre 2025. Il Global Research and Analysis Team (GReAT) di Kaspersky ha scoperto nuove prove che collegano Memento Labs, successore di HackingTeam, a una recente ondata di attacchi di cyberspionaggio. La scoperta Ã¨ il risultato di unâ??indagine condotta nellâ??ambito dellâ??operazione ForumTroll, una campagna APT (Advanced PersistentThreat) che ha sfruttato una vulnerabilitÃ zero-day di Google Chrome. I risultati della ricerca sono stati presentati oggi al Security Analyst Summit 2025 in Thailandia.

Nel marzo 2025, il GReAT di Kaspersky ha scoperto, attraverso lâ??operazione ForumTroll, una sofisticata campagna di spionaggio informatico che sfruttava la vulnerabilitÃ zero-day di Chrome, identificata come CVE-2025-2783. Il gruppo APT responsabile dellâ??attacco aveva inviato e-mail di phishing personalizzate, nascoste sotto forma di inviti al forum â??Primakov Readingsâ?•, indirizzate a media, istituti scolastici e organizzazioni governative in Russia.

Analizzando ForumTroll, i ricercatori hanno scoperto che gli hacker utilizzavano uno spyware denominato LeetAgent, caratterizzato da comandi scritti in leetspeak, una peculiaritÃ rara nei malware APT. Unâ??analisi piÃ¹ approfondita ha rivelato somiglianze tra il suo set di strumenti e uno spyware piÃ¹ avanzato che il GReAT di Kaspersky aveva giÃ osservato in altri attacchi. Dopo aver scoperto che, in alcuni casi, questâ??ultimo veniva lanciato da LeetAgent e che i due condividevano lo stesso framework di caricamento, i ricercatori hanno confermato laconnessione tra i due spyware e tra le relative campagne di attacco.

Sebbene lâ??altro spyware impiegasse tecniche anti-analisi avanzate, tra cui lâ??offuscamento VMProtect, Kaspersky Ã¨ riuscita a recuperare il nome del malware dal codice, identificandolo come Dante. I ricercatori hanno poi scoperto che uno spyware commerciale con lo stesso nome era stato promosso da Memento Labs, il nuovo nome del successore di HackingTeam. Inoltre, i campioni piÃ¹ recenti dello spyware Remote Control System di HackingTeam, analizzati dal GReAT di Kaspersky, presentano forti somiglianze con Dante.

â??Anche sela presenza dei fornitori di spyware sia ben nota nel settore, i loro prodotti restano difficili da individuare, soprattutto nel caso di attacchi mirati. Per risalire allâ??origine di Dante Ã¨ stato necessario rimuovere diversi livelli di codice fortemente offuscato, rintracciare una manciata di impronte digitali rare nel corso di anni di evoluzione del malware e collegarle a una specifica linea aziendale. Forse Ã¨ per questo che lâ??hanno chiamato Dante: chiunque cerchi di scoprirne le origini dovrÃ affrontare un vero e proprio viaggio infernaleâ?•, ha dichiarato Boris Larin, Principal Security Researcher del Kaspersky GReAT.

Per evitare di essere individuato, Dante incorpora un modo unico di analizzare lâ??ambiente circostante prima di determinare se puÃ² svolgere le sue funzioni in modo sicuro.

I ricercatori hanno ricondotto la prima attivitÃ di LeetAgent al 2022 e hanno individuato ulteriori attacchi del gruppo ForumTroll APT, che ha preso di mira aziende e utenti in Russia e Bielorussia. Il gruppo si distingue per la padronanza della lingua russa e la conoscenza delle specificitÃ locali, caratteristiche che Kaspersky ha giÃ osservato in altre campagne attribuite a questa minaccia APT. Tuttavia, alcuni errori occasionali suggeriscono che gli aggressori non fossero madrelingua russi.

Lâ??attacco che sfruttava LeetAgent Ã¨ stato rilevato per la prima volta da Kaspersky Next XDR Expert. Tutti i dettagli completi di questa ricerca, insieme ai futuri aggiornamenti relativi a ForumTroll APT e Dante, sono disponibili per i clienti del servizio di report APT tramite il Kaspersky Threat Intelligence Portal.

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

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.

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/

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

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 27, 2025
Autore
redazione