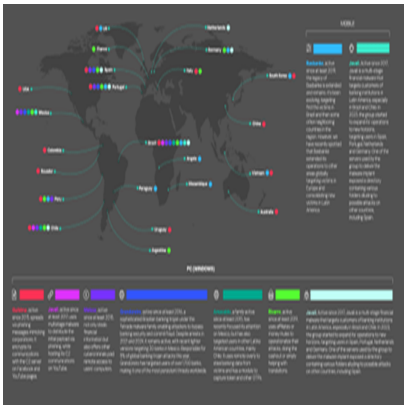

COMUNICATO STAMPA SPONSORIZZATO â?? Kaspersky: attenzione a â??Maverickâ?•, il trojan bancario con codice generato dallâ??AI

Descrizione

(Immediapress) â??
Milano, 21 ottobre 2025 â?? Il Global Research and Analysis Team (GReAT) di Kaspersky ha scoperto nuovi dettagli su Maverick, il trojan bancario recentemente scoperto che colpisce soprattutto gli utenti in Brasile. Il malware si diffonde tramite file LNK dannosi (â??shortcutâ?•) distribuiti tramite WhatsApp e utilizza indirizzi URL scritti in portoghese. Il trojan ha notevoli somiglianze nel codice con â??Coyoteâ?•, un altro trojan bancario brasiliano, e sfrutta la generazione di codice assistita dallâ??intelligenza artificiale, in particolare per la decodifica dei certificati e lo sviluppo del codice in generale.

Recentemente in Brasile Ã¨ stata individuata una grande campagna di diffusione di questi file LNK dannosi tramite WhatsApp. Per aggirare i controlli, il server di comando e controllo (C2) verifica ogni download per assicurarsi che sia originato dal malware, limitando le infezioni alle sole vittime brasiliane.

â??Maverick rappresenta una delle minacce piÃ¹ sofisticate che abbiamo mai incontrato nellâ??ambito dei trojan bancariâ?•, ha commentato Fabio Assolini, Head of Americas & Europe GReAT di Kaspersky. â??Ha giÃ colpito un gran numero di utenti in Brasile e le sue funzioni simili a quelle di un worm gli consentono di diffondersi rapidamente tramite le piattaforme di messaggistica istantanea piÃ¹ diffuse. Lâ??impatto Ã¨ notevole: nei primi 10 giorni di ottobre, le nostre soluzioni hanno bloccato oltre 62.000 tentativi di eseguire il file LNK dannoso in Brasile. Sebbene attualmente il rischio maggiore riguardi gli utenti brasiliani, esiste la reale preoccupazione che, come per altre famiglie di trojan bancari quali Grandoreiro e Guildma, Maverick possa eventualmente espandersi a livello internazionaleâ?•.

Il trojan bancario puÃ² assumere il controllo totale di un computer infetto: acquisire screenshot, monitorare i browser aperti e i siti visitati, installare keylogger, controllare il mouse, bloccare lo schermo quando si accede a un sito bancario, terminare i processi e visualizzare pagine di phishing tramite overlay, il tutto con lo scopo di sottrarre le credenziali bancarie. Una volta attivato, il trojan monitora lâ??attivitÃ delle vittime su 26 siti web di banche brasiliane, sei exchange di criptovalute e una piattaforma per pagamenti. Le infezioni sono modulari e vengono eseguite interamente in memoria con una minima attivitÃ del disco, sfruttando PowerShell e .NET, insieme a shellcode generato e crittografato utilizzando Donut.

Il report completo Ã¨ disponibile su Securelist.com

Per ridurre i rischi causati dai trojan bancari come â??Maverickâ?•, Kaspersky consiglia di:

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 milioni di persone e 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:
ImmediapressNoesisCristina Barelli, Silvia Pasero,Eleonora Bossi

kaspersky@noesis.net

Kaspersky ItaliaAlessandra VenneriHead of Corporate Communications & Public Affairs Italy
alessandra.venneri@kaspersky.com

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Ottobre 21, 2025
Autore
redazione