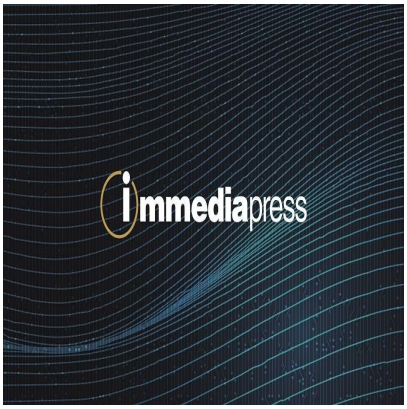

COMUNICATO STAMPA SPONSORIZZATO â?? Kaspersky scopre PassiveNeuron, campagna di cyberspionaggio che colpisce i server Windows

Descrizione

(Immediapress) â??
Milano, 22 ottobre 2025 â?? Il Global Research and Analysis Team (GReAT) di Kaspersky ha scoperto una campagna di cyberspionaggio denominata PassiveNeuron, che prende di mira i server Windows di enti governativi, societÃ finanziarie e industriali in Asia, Africa e America Latina. La campagna Ã¨ stata individuata nel dicembre 2024 ed Ã¨ proseguita fino ad agosto 2025.

Dopo sei mesi di inattivitÃ , PassiveNeuron ha ripreso le operazioni, utilizzando tre strumenti principali, due dei quali precedentemente sconosciuti, per ottenere e mantenere lâ??accesso allâ??interno delle reti prese di mira.

Gli strumenti sono:

â?¢ Neursite, una modular backdoor;

â?¢ NeuralExecutor, un sistema basato su .NET;

â?¢ Cobalt Strike, un framework di penetration testing spesso utilizzato dai cybercriminali.

La backdoor Neursite Ã¨ in grado di raccogliere informazioni di sistema, gestire i processi in esecuzione e indirizzare il traffico di rete attraverso host compromessi, consentendo ai cybercriminali di muoversi lateralmente allâ??interno di una rete. Sono stati rilevati campioni in grado di comunicare sia con server di comando e controllo esterni che con sistemi interni compromessi.

NeuralExecutor Ã¨ stato progettato per distribuire payload aggiuntivi. Lâ??impianto supporta diversi metodi di comunicazione ed Ã¨ in grado di caricare ed eseguire assembly .NET ricevuti dal proprio server di comando e controllo.

â??PassiveNeuron si distingue per la sua abilitÃ nel compromettere i server, che spesso rappresentano la base delle reti aziendaliâ?•, ha affermato Georgy Kucherin, Security Researcher del GReAT.â??I server esposti alla rete Internet sono obiettivi molto ambiti dai gruppi APT (Advanced Persistent Threat), poichÃ© un singolo host compromesso puÃ² fornire lâ??accesso a sistemi critici. Ã? quindi essenziale ridurre al minimo le superfici di attacco correlate e monitorare costantemente le applicazioni server per rilevare e bloccare potenziali attacchiâ?•.

Da alcuni campioni osservati dal GReAT, Ã¨ emerso che i nomi delle funzioni sono stati sostituiti con stringhe contenenti caratteri cirillici, introdotti intenzionalmente dagli aggressori. La presenza di questi elementi richiede unâ??attenta valutazione durante lâ??attribuzione, poichÃ© potrebbero costituire false tracce volte a depistare le analisi. Sulla base delle tattiche, delle tecniche e delle procedure osservate, Kaspersky ritiene che la campagna sia probabilmente associata a gruppi di hacker di madrelingua cinese. Allâ??inizio del 2024, i ricercatori di Kaspersky avevano giÃ rilevato lâ??attivitÃ di PassiveNeuron e descritto la campagna come altamente sofisticata.

Maggiori informazioni relative alla campagna, sono disponibili nel report pubblicato su Securelist.com.

Per evitare questi attacchi mirati da parte di soggetti noti o sconosciuti, i ricercatori di Kaspersky consigliano di:

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
Contatti di redazione:
NoesisCristina Barelli, Silvia Pasero,Eleonora Bossi
Kaspersky ItaliaAlessandra VenneriHead of Corporate Communications & Public Affairs Italy

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Ottobre 22, 2025
Autore
redazione