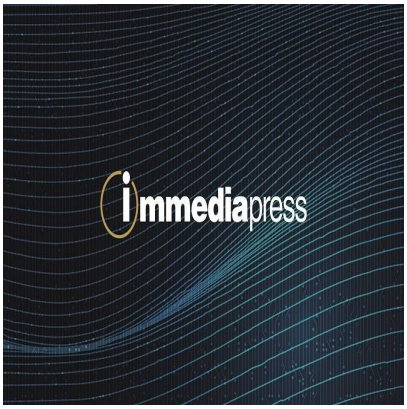

Kaspersky svela la botnet Tsundere che colpisce gli utenti Windows in modo imprevedibile

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Il Global Research and Analysis Team (GReAT) di Kaspersky ha scoperto una nuova botnet creata da un autore di minacce riapparso nel luglio 2025. Per attirare le vittime, lâ??autore dellâ??attacco utilizza un programma di installazione MSI nascosto sotto forma di falso setup per giochi popolari, in particolare sparatutto come â??Valorantâ?•, â??CS2â?? o â??R6xâ?•, nonchÃ© altri software. La botnet Ã¨ attualmente in espansione e rappresenta una minaccia attiva per gli utenti Windows. Ã? giÃ stata rilevata da Kaspersky in Messico, Cile, Russia e Kazakistan.

La botnet Tsundere utilizza un approccio sempre piÃ¹ diffuso che prevede lâ??uso di smart contract Web3 per memorizzare i propri indirizzi di comando e controllo (C2), migliorando in modo significativo la resistenza della propria infrastruttura. Il suo pannello C2 supporta due formati di distribuzione: un programma di installazione MSI e uno script PowerShell con impianti generati automaticamente. Questi impianti installeranno un bot in grado di eseguire in modo persistente il codice JavaScript che riceve dinamicamente, attraverso un canale WebSocket crittografato, dal C2, il che potrebbe portare allâ??esecuzione dannosa del codice inviato dallâ??autore della minaccia.

Per gestire le infezioni e aggiornare le posizioni C2, la botnet Tsundere utilizza riferimenti fissi sulla blockchain di Ethereum, come un wallet e un contratto designati. La modifica del server C2 richiede una sola transazione che aggiorna la variabile di stato del contratto con un nuovo indirizzo. Lâ??ecosistema della botnet include anche un marketplace integrato e un pannello di controllo accessibile attraverso la stessa interfaccia.

Lâ??analisi indica con elevata certezza che lâ??autore della minaccia dietro la botnet Tsundere Ã¨ probabilmente di lingua russa, come dimostra lâ??uso della lingua russa nel codice, in linea con precedenti attacchi collegati allo stesso autore. La ricerca suggerisce anche una connessione tra la botnet Tsundere e il 123 Stealer creato da â??konekoâ?•, offerto su un forum clandestino al prezzo di 120 dollari al mese.

Il codice della botnet Tsundere Ã¨ scritto interamente in lingua russa

â??Tsundere dimostra la rapiditÃ con cui i criminali informatici si adattano: rappresenta un rinnovato sforzo da parte di un attore di minaccia presumibilmente identificato per rinnovare il proprio set di strumenti. Passando ai meccanismi Web3, la sua infrastruttura diventa molto piÃ¹ flessibile e resiliente. Stiamo giÃ assistendo a una distribuzione attiva attraverso falsi programmi di installazione di giochi e collegamenti ad attivitÃ dannose osservate in precedenza, quindi Ã¨ altamente probabile un ulteriore sviluppo di questa botnetâ?•, ha affermato Lisandro Ubiedo, Senior Security Expert del Kasperskyâ??s Global Research and Analysis Team.

Per ulteriori dettagli e indicatori di compromissione, consultare lâ??articolo su Securelist.com.

Per proteggersi da queste minacce, Kaspersky consiglia di:

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Novembre 20, 2025
Autore
redazione