Bitdefender

Cryptominer Bhunt: una nuova pericolosa famiglia di malware per il furto di criptovalute che prende di mira gli utenti privati

La società di sicurezza informatica Bitdefender, che ha scoperto questa nuova minaccia, mette in guardia anche dai pericoli legati alla privacy per via del furto di password

Milano, 19 gennaio 2022 - Bitdefender Labs annuncia la scoperta di BHUNT, una nuova famiglia di malware pensata per rubare criptovalute dai portafogli virtuali degli utenti: Bitcoin, Litecoin, Ethereum, Jaxx, Atomic, Electrum, Exodus sono a rischio furto, insieme alle password memorizzate nel browser e alle passphrase utilizzate per recuperare gli account.

La campagna malware sembra prendere di mira gli utenti privati ed è uniformemente distribuita dal punto di vista geografico.

Mentre BHUNT è responsabile principalmente del furto di criptovalute, esistono tuttavia anche enormi preoccupazioni per la privacy in quanto il malware può esfiltrare le password e i cookie memorizzati nei browser impiegati per navigare sui social media, siti di internet banking e per accedere ad altri account personali.

La famiglia di malware agisce in modo diverso rispetto al solito: i criminali informatici infatti, utilizzano VMProtect e Themida come strumenti per la creazione di pacchetti che usano una macchina virtuale software per emulare parti del codice su una CPU virtuale che ha un set di istruzioni diverso da quello di una CPU convenzionale, rendendo il reverse engineering estremamente difficile.

Altre caratteristiche del nuovo malware:

- BHUNT usa script di configurazione criptati che vengono scaricati da pagine Pastebin pubbliche
- I campioni di BHUNT esaminati sembrano essere stati firmati digitalmente con un certificato digitale rilasciato a una società di software, ma il certificato digitale non corrisponde ai codici binari.
- I server responsabili dell'esfiltrazione utilizzano Hopto.org, un servizio DNS dinamico per mascherare gli indirizzi IP.

Fin dal boom di Bitcoin, le criptovalute sono aumentate notevolmente di valore anno dopo anno. Oltre ad attirare più investimenti, questa possibilità di guadagno ha anche spinto sempre più i criminali informatici a sviluppare malware per rubare le valute digitali specializzandosi nell'accesso ai portafogli di criptovalute. Una volta arrivati a questi portafogli, gli hacker possono trasferire liberamente e irreversibilmente i fondi ai portafogli da loro controllati. I ricercatori di Bitdefender monitorano costantemente i ladri di portafogli di criptovalute per tutelare gli utenti da questa tipologia di crimine informatico.

I dati relativi alla ricerca completa sono disponibili qui.

A proposito di Bitdefender

Bitdefender, leader riconosciuto nel settore della cybersecurity, offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce in tutto il mondo. Responsabile della protezione di milioni di sistemi in ambienti consumer, business e governativi, Bitdefender è l'esperto più affidabile del settore* per eliminare le minacce, proteggere la privacy e i dati per favorire la resilienza informatica. Grazie agli investimenti in ricerca e sviluppo, Bitdefender Labs rileva 400 nuove minacce ogni minuto con 30 miliardi di query giornaliere. L'azienda ha rilasciato innovazioni rivoluzionarie in materia di antimalware, IoT, analisi comportamentale e intelligenza artificiale e la sua tecnologia viene concessa in licenza a oltre 150 brand di cybersecurity, i più conosciuti al mondo. Fondata nel 2001, Bitdefender vanta clienti in 170 paesi e ha uffici in tutto il mondo. Per maggiori informazioni https://www.bitdefender.it.

*Bitdefender si è classificata al primo posto nel 54% di tutti i test di AV-Comparatives 2018-2021 per protezione del mondo reale, prestazioni, protezione dai malware & protezione dalle minacce avanzate.

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it