Bitdefender

Bitdefender scopre un malware con la firma digitale di Microsoft

Milano, 22 ottobre 2021 - Bitdefender Labs pubblica oggi una nuova ricerca che annuncia la scoperta di FiveSys, un nuovo rootkit con una firma digitale emessa da Microsoft. FiveSys si è fatto strada attraverso il processo di certificazione dei driver. La firma digitale valida aiuta il criminale informatico ad aggirare le misure di sicurezza come l'antimalware e le restrizioni del sistema operativo sul caricamento di moduli di terze parti nel kernel. Una volta caricato, FiveSys permette ai criminali informatici di ottenere privilegi potenzialmente illimitati.

Bitdefender ha contattato Microsoft che ha rapidamente revocato i certificati in questione.

Risultati principali:

- FiveSys è utilizzato come proxy del traffico verso indirizzi internet di interesse per gli hacker
- La campagna FiveSys è stata attiva per più di un anno prendendo di mira i giocatori online in Cina - probabilmente per il furto di credenziali e il dirottamento degli acquisti in-game.
- La certificazione per il malware è stata revocata, tuttavia, la probabilità che il gruppo ci riprovi (potenzialmente in altri Paesi) è alta

Bitdefender ha contattato Microsoft Digital Crime Unit (DCU), Europol e FBI e conseguentemente il certificato è stato rapidamente revocato. Nonostante ciò, la società di sicurezza consiglia di applicare gli Indicatori di Compromissione per i sistemi di Endpoint Detection and Response, i servizi di Management Detection Response e altre misure di sicurezza.

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