Cyberattacchi sempre piÃ¹ sofisticati: finte fatture ultra-realistiche in PDF nascondono malware

Descrizione

(Adnkronos) â?? I cybercriminali stanno affinando le loro tecniche di attacco, rendendo sempre piÃ¹ difficile distinguere le minacce digitali dalle attivitÃ legittime. Ã? quanto emerge dall'ultimo Threat Insights Report di HP Wolf Security, che rivela come le tradizionali tecniche di phishing e le strategie "living-off-the-land" (LOTL) stiano evolvendo per aggirare gli strumenti di sicurezza basati sul rilevamento. Le tecniche LOTL, che sfruttano strumenti e funzionalitÃ giÃ presenti nei sistemi operativi, sono ora combinate in modi inediti, rendendo l'individuazione degli attacchi un compito complesso. Il report fornisce un'analisi dettagliata delle campagne di attacco piÃ¹ recenti, basata sui milioni di endpoint monitorati da HP Wolf Security. Tra le scoperte piÃ¹ significative spiccano tre metodi particolarmente ingegnosi.
Il primo metodo Ã¨ il phishing ultra-realistico che sfrutta finte fatture Adobe Reader. Gli aggressori hanno incorporato un "reverse shell" (uno script che garantisce il controllo del dispositivo) in una piccola immagine SVG, mascherata da un file PDF di Adobe Acrobat Reader estremamente verosimile, completo di barra di caricamento fittizia. Per ostacolare ulteriormente l'analisi, il download del file Ã¨ stato limitato alle sole regioni di lingua tedesca. Il report ha inoltre scoperto che gli aggressori stanno nascondendo codici maligni all'interno di file immagine. Utilizzando file Microsoft Compiled HTML Help camuffati da documenti di progetto, i cybercriminali hanno occultato un payload XWorm nei pixel dell'immagine. Questo payload viene successivamente estratto per avviare una catena di infezione in piÃ¹ fasi, che include l'uso di PowerShell per cancellare ogni traccia una volta che i file sono stati scaricati ed eseguiti. "I cybercriminali oggi adottano strategie sempre piÃ¹ sofisticate per mimetizzarsi all'interno delle attivitÃ quotidiane degli utenti, sfruttando strumenti legittimi, file dall'aspetto familiare e tecniche invisibili ai controlli tradizionali. PoichÃ© le minacce sono sempre piÃ¹ difficili da intercettare con i soli strumenti di rilevamento tradizionali, Ã¨ fondamentale adottare un approccio di sicurezza multilivello, capace di isolarle e contenerle prima che possano causare danni reali. In un ambiente digitale sempre piÃ¹ complesso, HP Wolf Security nasce proprio con questo obiettivo: proteggere dispositivi ed endpoint in modo efficace e trasparente, senza interferire con la produttivitÃ , aiutando persone e aziende a muoversi in modo sicuro e garantendo continuitÃ operativa" ha dichiarato Giampiero Savorelli, VP e AD HP Italy. Infine, il report ha rilevato una recrudescenza del Lumma Stealer, un malware molto attivo che viene distribuito tramite archivi IMG. Sfruttando le tecniche LOTL, questi allegati riescono a eludere i filtri di sicurezza e a sfruttare i sistemi fidati. Nonostante un'azione

delle forze dell'ordine nel maggio 2025, il gruppo criminale ha continuato a operare, registrando nuovi domini e ricostruendo la propria infrastruttura. "Gli aggressori non stanno reinventando la ruota, ma stanno perfezionando le loro tecniche," ha commentato Alex Holland, Principal Threat Researcher di HP Security Lab. "Stiamo assistendo a una combinazione sempre maggiore di strumenti 'living-off-the-land' e all'uso di tipi di file meno evidenti, come le immagini, per eludere il rilevamento. Ã? un approccio semplice, veloce e che spesso passa inosservato proprio perchÃ© Ã¨ cosÃ¬ elementare."
Secondo Dr. Ian Pratt, Global Head of Security for Personal Systems di HP Inc., le tecniche LOTL sono particolarmente difficili da contrastare per i team di sicurezza. "Si Ã¨ bloccati tra l'incudine e il martello: o si limita l'attivitÃ , creando attrito per gli utenti, o la si lascia aperta, rischiando che un attaccante si insinui," ha spiegato Pratt. "Anche il miglior sistema di rilevamento puÃ² fallire, per questo Ã¨ essenziale una difesa in profonditÃ che includa il contenimento e l'isolamento delle minacce prima che possano causare danni." I dati del report, che analizza il periodo da aprile a giugno 2025, indicano che almeno il 13% delle minacce identificate da HP Sure Click ha eluso uno o piÃ¹ scanner di email gateway. I file di archivio sono stati il tipo di delivery piÃ¹ diffuso (40%), seguiti da eseguibili e script (35%), con una netta preferenza per i file .rar (26%), suggerendo che gli aggressori sfruttano la fiducia riposta in software comuni come WinRAR per evitare sospetti. â??tecnologiawebinfo@adnkronos.com (Web Info)

Categoria

1. Tecnologia

Tag

1. adnkronos
2. Tecnologia

Data di creazione
Settembre 23, 2025
Autore
andreaperocchi_pdnrf3x8