Primo Piano - *Spionaggio e cybercrime: Proofpoint rileva sovrapposizioni inquietanti tra i due mondi*

Roma - 30 giu 2025 (Prima Notizia 24) **Sorprendente sovrapposizione tra i cluster di due attori di minaccia, TA829 e UNK_GreenSec.**

I ricercatori di Proofpoint, azienda leader nella cybersecurity e compliance, hanno messo in luce una sorprendente sovrapposizione tra i cluster di due attori di minaccia, TA829 e UNK_GreenSec. Questa attività, individuata in una campagna che sfuma i confini tra spionaggio e attività cybercriminale, solleva interrogativi cruciali sulla natura delle minacce odierne. L'analisi di Proofpoint ha rivelato che questa campagna si avvale di infrastrutture, tattiche di distribuzione e componenti malware condivisi, suggerendo una potenziale collaborazione o l'utilizzo di risorse comuni all'interno del panorama criminale sotterraneo. Tra i principali risultati della ricerca: TA829: un attore ibrido. Questo gruppo conduce sia campagne cybercriminali a scopo di lucro sia operazioni di spionaggio allineate agli interessi statali russi. TA829 utilizza strumenti personalizzati come la backdoor RomCom e il malware DustyHammock. UNK_GreenSec: nuovo attore con legami ransomware. È stata osservata l'attività di un nuovo cluster di malware, denominato UNK_GreenSec, che ha dispiegato un nuovo loader e una backdoor chiamata TransferLoader. Questo malware è stato collegato a infezioni ransomware, incluso Morpheus. Sovrapposizione infrastrutturale e tattica. Entrambi gli attori si affidano a router MikroTik compromessi (nodi REM Proxy) per la distribuzione di email, utilizzano catene di reindirizzamento simili e effettuano lo spoofing di pagine di destinazione di OneDrive/Google Drive. Tuttavia, le loro catene di infezione divergono nella fase del payload. "Si tratta di risultati che suggeriscono possibili relazioni tra i gruppi, che vanno dalla condivisione di fornitori di infrastrutture di terze parti, a una collaborazione diretta, o persino all'ipotesi che si tratti di un singolo attore che testa nuovi strumenti", spiegano i ricercatori di Proofpoint. La sottile distinzione tra spionaggio e cybercrime Nella maggior parte dei casi, è possibile distinguere attività riconducibili a cluster differenti e separare spionaggio e cybercrime basandosi su differenze nelle tattiche, tecniche e procedure (TTPs), negli strumenti utilizzati, nel volume/scala delle operazioni e nei target. Tuttavia, nel caso di TA829 e del cluster che Proofpoint ha denominato "UNK_GreenSec", emerge maggiore ambiguità. TA829 è un attore cybercriminale che occasionalmente conduce anche attività di spionaggio allineate agli interessi statali russi, mentre UNK_GreenSec rappresenta un cluster cybercriminale insolito. TA829 presenta sovrapposizioni con attività tracciate da terze parti come RomCom, Void Rabisu, Storm-0978, CIGAR, Nebulous Mantis e Tropical Scorpius. Il cluster cybercriminale UNK_GreenSec, invece, non sembra allinearsi con set di attività pubblicamente riportati. I ricercatori di Proofpoint hanno osservato somiglianze nelle attività descritte in questo report con attività storiche di TA505,

inclusi esche, URL shortener, pattern, registrazione di domini e infrastrutture. Tuttavia, al momento non le stanno attribuendo a TA505, poiché non in grado di affermare con elevata confidenza se TA505 sia definitivamente associato, o se l'attore stia semplicemente utilizzando TTPs sorprendentemente simili. Proofpoint continua a monitorare attentamente queste evoluzioni per fornire informazioni cruciali e proteggere le organizzazioni dalle minacce più sofisticate.

(Prima Notizia 24) Lunedì 30 Giugno 2025