

Pink, l'estortion brand che entra in azienda con una telefonata di vishing



Le aziende investono in *patch management*, *firewall* e rilevamento delle intrusioni, ma il gruppo di estorsione Pink non bussa a nessuna di quelle porte: chiama al telefono. Secondo l'analisi di Unit 42 (Palo Alto Networks), che traccia il cluster come CL-CRI-1147 e lo qualifica come *extortion brand*, l'accesso iniziale ai sistemi aziendali arriva tramite *vishing*, cioè phishing vocale, senza *malware* sofisticati, senza cifratura dei dati e senza vulnerabilità *zero-day*. Una conversazione ben costruita, ed è la vittima stessa a consegnare le chiavi, aggirando di fatto l'intero perimetro tecnologico.

Come funziona la catena di attacco

Lo schema è lineare e per questo efficace. L'aggressore chiama la vittima con false telefonate fingendosi un addetto IT interno e la convince a inserire le proprie credenziali su una pagina di *phishing* controllata. La pagina cattura non solo username e password, ma anche il secondo fattore: con il furto della sessione, Pink supera l'autenticazione a più fattori senza doverla forzare.

Una volta dentro, l'attore individua ed esfiltra rapidamente i dati: tra le piattaforme prese di mira figurano *SharePoint* e *OneDrive*. L'account compromesso viene poi usato per recapitare l'email di estorsione e messaggi minatori direttamente nelle chat interne di *Microsoft Teams*, portando la pressione dentro gli strumenti di lavoro quotidiani.

Nel modello osservato da Unit 42 non compare alcun *payload* di

cifratura: il ricatto si fonda sui dati sottratti, non sul blocco dei sistemi, in linea con lo spostamento di molti attori finanziariamente motivati dal *ransomware* classico all'estorsione mirata. I domini di *phishing* identificati richiamano, non a caso, il lessico della sicurezza moderna: passkeyadd[.]com, passkeydeploy[.]com e deploypasskey[.]com, ospitati tramite l'infrastruttura di DDoS-Guard. Pink riutilizza i domini di secondo livello per colpire più organizzazioni e riserva i domini di terzo livello a bersagli specifici, segno di una pianificazione mirata.

Estorsione a tempo e identità sfuggente

La componente di pressione psicologica è strutturata. In un caso esaminato da Unit 42, dopo trattative rimaste a lungo senza risposta, il 1 giugno 2026 l'aggressore ha ricontattato la vittima da un account di posta gratuito, fornendo un nuovo identificativo qTox e il link al sito Pink Leak, con un ultimatum di 72 ore per rispondere. Il sito di *data leak* del gruppo, secondo quanto riportato dallo stesso, è stato attivato il 31 maggio 2026, e nel giro di pochi giorni sono comparse le prime presunte vittime.

Sull'attribuzione resta cautela. Google Threat Intelligence, che collega l'attività al codice UNC6671, ritiene che Pink possa non essere un gruppo del tutto nuovo, ma il *rebranding* di un team esistente: dopo la chiusura del marchio BlackFile nel maggio 2026 sarebbe nato Redact, poi forse riemerso come Pink. Unit 42 collega inoltre il gruppo alla galassia criminale Com, che ricorre a *social engineering*, furto di account ed estorsione, con tattiche affini a quelle di Bling Libra (noto anche come *ShinyHunters*).

Perché conta per le aziende

Il dato strategico è che Pink non sfrutta una falla tecnica, ma la fiducia organizzativa. Nessun *patch management*, per quanto rapido, intercetta una telefonata che convince un dipendente a digitare la password su una pagina falsa. Per i responsabili della sicurezza la lezione è operativa: verificare con procedure fuori banda ogni contatto che si presenti come supporto IT, in particolare le richieste urgenti di aggiornare l'autenticazione a più fattori o di confermare un accesso; rafforzare la formazione contro il vishing; adottare fattori resistenti al *phishing*, come le *passkey* legate al dispositivo, proprio ciò che i domini malevoli imitano per ingannare; monitorare comportamenti anomali su SharePoint, OneDrive e Teams. La superficie di attacco, ancora una volta, è umana.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/pink-estorsione-vishing-bypass-mfa/>