I ricercatori Check Point svelano l'identità del Linked Cyber Espionage Attackers iraniano pubblicando i dettagli sugli obiettivi della campagna di attacco globale

Check Point Software Technologies Ltd. (NASDAQ: CHKP), la più grande società di sicurezza pure-play a livello globale, ha pubblicato oggi un rapporto di 38 pagine che riportano un'ampia analisi delle attività di cyber-spionaggio condotte dal gruppo 'Kitten Rocket,' con possibili legami con il Corpo di Guarda Rivoluzionario iraniano. Il nuovo rapporto rivela anche i dettagli delle operazioni globali del gruppo e individua più di 1.600 dei loro obiettivi. Guidato da ricercatori della Threat Check Point Intelligence e Reserch Area, i dati emersi dipingono uno scenario di attacchi malware strategici sostenuti da campagne di spear phishing persistenti. I dettagli mostrano specifici individui appartenenti attivamente al gruppo "Kitten Rocket" e organizzazioni situate in Medio Oriente, così come in Europa e negli Stati Uniti, documentando la diversificazione delle loro attività negli ambiti più disparati:

- Settori governativi in tutta l'Arabia Saudita, tra cui agenzie di stampa e giornalisti; istituzioni e studiosi accademici; attivisti per i diritti umani; generali militari; e membri della famiglia reale saudita.
- Ambasciate, diplomatici, addetti militari e persone di spicco in tutto l'Afghanistan, Turchia, Qatar, Emirati Arabi Uniti, Iraq, Kuwait e Yemen, così come la NATO comandi nella regione.
- Decine di ricercatori iraniani, così come alcuni gruppi di ricerca dell'Unione europea, in particolare nei settori della politica estera, la sicurezza nazionale e l'energia nucleare. Obiettivi commerciali e finanziari venezuelani.
- Ex cittadini iraniani di varie influenti posizioni .
- Predicatori e gruppi islamici e anti-islamici; editorialisti e fumettisti famosi; Show televisivi; partiti politici; e funzionari di governo.

I ricercatori Check Point sono stati anche in grado di rintracciare e smascherare la vera identità di un alias attaccante, "Wool3n.H4T", identificato come una delle figure di spicco artefici di questa campagna. Inoltre, in base alla natura degli attacchi e alle ripercussioni associate ad essi, si suggerisce che le motivazioni di Rocket Kitten siano allineate agli interessi di intelligence dello stato, volti a estrarre informazioni sensibili dai loro obiettivi.

"Questa ricerca fornisce un quadro raro della natura e degli obiettivi di un gruppo di spionaggio globale", ha dichiarato Shahar Tal, Reserch Group Manager Check Point, "Mentre i clienti Check Point possono avere la certezza di essere protetti da tutte le varianti conosciute di queste minacce da parte di Rocket Kitten, speriamo che i vendor come noi garantiscano la sicurezza dell'individuo e che i professionisti della ricerca contro i malware prendano le dovute precauzioni e distribuiscano misure di protezione importanti. "

Per leggere il report completo: http://blog.checkpoint.com/ wp-content/uploads/2015/11/rocket-kitten-report.pdf ■

Luisa Pala

20 di passioni
CONSYS.IT
dal 1994 Innovativi per Tradizione
www.consys.it

Check Point
SOFTWARE TECHNOLOGIES LTD.
www.checkpoint.com