30 aprile 2022 18:03

Guerra in Ucraina: come funzionano i devastanti attacchi informatici russi

di Redazione

Secondo il laboratorio di sicurezza informatica di Microsoft, sei gruppi di hacker collegati al Cremlino hanno lanciato più di 237 operazioni contro l'Ucraina, inclusi attacchi che minacciano infrastrutture e servizi critici per le popolazioni. L'intensità degli attacchi tende a seguire quella delle offensive in campo.

Si chiama “guerra ibrida”: per un Paese, e in particolare per la Russia, è un metodo per indebolire gli altri, con mezzi più o meno subdoli. Le leve sono molteplici: disordini popolari, ingerenze elettorali, finanziamento dei partiti, disinformazione, pressioni economiche, attacchi informatici... Nel 2007 è stata l'Estonia ad inaugurare questo metodo subendo un massiccio attacco informatico per più di 20 giorni. Attacchi che avevano paralizzato molti servizi in questo Paese che allora era uno dei più collegati. L'offensiva era stata orchestrata dagli hacker affiliati al Cremlino all'epoca, ma attribuirli era allora difficile e rischioso. Oggi, con l'attuale conflitto in Ucraina, l'uso delle armi informatiche è accettato e non dobbiamo più guardare lontano per poter attribuire attacchi informatici.

Microsoft ha appena pubblicato un rapporto specifico sugli attacchi informatici che la Federazione Russa ha effettuato nell'ambito della sua guerra ibrida contro l'Ucraina. Per Microsoft si tratta di sensibilizzare su questo cyber-branch militarizzato che rimane silenzioso nonostante i danni che può causare. Così, anche prima dell'invasione, i ricercatori Microsoft hanno individuato almeno sei attori legati al Cremlino. Hanno lanciato più di 237 operazioni contro l'Ucraina.

Nella sequenza temporale, già a marzo 2021, gli hacker al servizio di Mosca hanno intensificato gli attacchi alle organizzazioni ucraine e agli alleati dell'Ucraina. Si sono poi infiltrati profondamente e silenziosamente nelle reti. A metà del 2021, questi stessi attori hanno preso di mira i fornitori della catena di approvvigionamento in Ucraina e all'estero per ottenere un accesso aggiuntivo ai sistemi sul territorio e negli Stati membri della NATO. Alla fine, quando le truppe russe hanno iniziato a muoversi verso il confine ucraino, tutti gli obiettivi che fornivano informazioni sui partenariati militari e stranieri dell'Ucraina sono stati attaccati.

L'arma informatica prima del fuoco dell'artiglieria

Nel merito, alcuni attacchi distruttivi non solo hanno degradato i sistemi delle istituzioni in Ucraina, ma hanno anche cercato di interrompere l'accesso della popolazione a informazioni affidabili e servizi essenziali. L'idea è di scuotere la fiducia dei leader del Paese. Oggi, questi attacchi sono sincronizzati con le operazioni militari cinetiche mirando principalmente ai servizi per i civili. Così, il 1 marzo, sono avvenuti attacchi informatici contro un'importante stazione radio in Ucraina. Lo stesso giorno, l'esercito russo ha annunciato che avrebbe distrutto obiettivi di disinformazione ucraini e ha effettuato un attacco missilistico contro la torre della TV a Kiev. Un altro esempio, il 13 marzo, il sequestro di centrali nucleari da parte dell'esercito russo è stato accompagnato poche settimane dopo dalla raccolta di dati presso un'organizzazione di sicurezza nucleare.

Ma ci sono stati anche attacchi che distruggono il sistema. Microsoft ne ha contati quasi 40. Circa il 32% ha preso di mira direttamente le organizzazioni governative ucraine. Peggio ancora, oltre il 40% ha preso di mira organizzazioni in settori critici (militare, economia, reti critiche). In termini di metodi di infiltrazione, è stato utilizzato il phishing e lo sfruttamento di vulnerabilità senza patch. I ricercatori hanno anche notato che gli hacker cercano anche di cancellare le loro tracce con strumenti specializzati.

Poiché gli attacchi informatici seguono o precedono l'ampiezza delle azioni militari, ora ci si aspetta che gli hacker effettuino azioni distruttive di rappresaglia contro i paesi che decidono di fornire maggiore assistenza militare all'Ucraina. Attualmente, Microsoft ha già identificato operazioni negli Stati membri della NATO che forniscono attivamente supporto politico, umanitario o militare all'Ucraina.

(Louis Neveu su Futura-Tech del 29/04/2022)