



YOU DESERVE THE BEST SECURITY

La nuova era dell'hacktivism

L'hacktivism è sempre stato associato a gruppi come Anonymous, gruppi decentralizzati e destrutturati composti da privati cittadini con differenti background. Anonymous ha lanciato diverse campagne contro target variegati, individuati in base alle preferenze e desideri dei suoi membri. Precedentemente, non c'era mai stata alcuna corrispondenza o connessione ideologica fra i membri del gruppo e apparentemente alcuna pianificazione sul lungo periodo. Chiunque, a prescindere dalla fede politica, è sempre stato il benvenuto nei gruppi di hacktivist.

Durante l'anno passato, le cose sono cambiate. Per effetto dei molteplici conflitti nell'Europa dell'est e nel Medio Oriente, alcuni gruppi hacker hanno aumentato le loro attività e la loro attenzione rispetto all'attivismo e al cambiamento voluto. Il fenomeno dell'hacktivism non riguarda più solamente gruppi eterogenei. Ora è meglio organizzato e strutturato oltre ad essere più sofisticato. Nonostante l'attivismo inizi in specifiche regioni geografiche legate a dinamiche di conflittualità, si è ormai esteso.

I colossi aziendali, i governi europei e quello statunitense sono stati bersagliati da questa forma di hacktivism emergente. Nei mesi recenti Stati Uniti, Germania, Lituania, Italia, Estonia, Norvegia, Finlandia, Polonia e Giappone hanno subito pesanti attacchi mossi dai gruppi di attivisti, che in alcuni casi hanno avuto un impatto significativo. Gli attacchi recenti hanno interessato non solo i governi di questi Paesi, ma anche grandi aziende come Lockheed Martin, che opera come contraente della sicurezza globale.

I principali gruppi di hacktivist che hanno agito lo scorso anno condividono diverse caratteristiche proprie delle organizzazioni strutturate: una chiara ideologia politica, una gerarchia dei membri e di leadership ben congegnata, un processo di recruitment formale e anche tool che i gruppi forniscono ai loro membri.

Inoltre, i gruppi sono allineati nella selezione dei bersagli, e in qualche caso, si verifica anche una cooperazione fra di essi. I gruppi svolgono anche consistenti attività di pubbliche relazioni finalizzate a pubblicizzare e promuovere i loro successi anche sui principali canali mediali e siti web. Tutto questo permette ai nuovi gruppi di hacktivist di mobilitarsi rispetto agli eventi governativi, raggiungendo obiettivi strategici e ad ampio spettro con alto tasso di successo, più che mai – e con un maggior impatto sociale.

I gruppi di hacktivist non sono più considerati come un gruppo di alcuni individui selezionati randomicamente che, normalmente, mettono in atto attacchi DDoS o azioni di sabotaggio nei confronti di siti web di bassa classifica, bensì sono organizzazioni coordinate che lanciano DDoS su larga scala e azioni di sabotaggio indirizzate ai bersagli scelti e un sistema di pubbliche relazioni con un alto tasso di reach.

Per questo motivo le agenzie e gli organismi governativi dovrebbero considerarsi avvertiti.

Hacktivism old school

Alcuni esempi di attacchi hacktivist old school includono campagne come l'Operazione KKK contro i membri e sostenitori del Ku Klux Klan, la campagna di rappresaglia contro le Nazioni Unite per non aver garantito un posto a sedere a Taiwan, l'Operazione AntiSec, il cui obiettivo era quello di rubare e pubblicare documenti governativi di natura classificata, e #Opwhales per sostenere la salvaguardia delle balene ed altri. In alcuni casi, ci sono anche state campagne contraddittorie portate avanti da Anonymous nello stesso anno come quella #OpTrump e #OpHilaryClinton.

Il modello hacktivista del 2022

L'evoluzione dell'hacktivismo è iniziata, silenziosamente, 2 anni fa nel Medio Oriente ad opera di diversi gruppi come Hackers of Savior, Black Shadow e Moses Staff. Tali gruppi hanno concentrato gli attacchi esclusivamente su Israele. La maggior parte di questi non nasconde i rapporti con la propaganda anti-israeliana promossa dal regime iraniano.

Parallelamente, altri gruppi del Medio Oriente, fra i quali il più in vista era Predatory Sparrow, si sono concentrati unicamente nell'attacco di bersagli pro-iraniani: il loro unico piano comune era l'opposizione al regime iraniano.

La programmazione geopolitica che ha mobilitato l'hacktivismo non si limita al Medio Oriente, ma è anche parte essenziale della guerra russo-ucraina. Nella prima parte del 2022, il gruppo dei Belarusian Cyber-Partisans, formatosi nel 2020 per contrastare il governo, ha iniziato a lanciare cyber-attacchi devastanti alle truppe russe per ostacolarle. Il cosiddetto IT Army dell'Ucraina è stato fatto mobilitare dal governo ucraino per attaccare la Russia.

Il nuovo fenomeno dell'hacktivismo ha anche coinvolto gruppi schierati dalla parte della narrativa geopolitica russa, con gruppi come Killnet, Xaknet, From Russia with Love (FRwL), NoName057(16) ed altri ancora. Nonostante questo nuovo modello sia cominciato in aree specifiche e circoscritte, le truppe russe mobilitate hanno rapidamente rivolto la propria attenzione, inizialmente verso l'Ucraina, anche a chiunque altro si opponesse ai piani del governo russo come l'Europa, gli Stati Uniti e anche l'Asia.

Questo comportamento ha causato significativi attacchi rivolti a governi e aziende di prima fascia di Stati Uniti, Lituania, Italia, Estonia, Norvegia, Finlandia, Polonia, Giappone, ad esempio. Questi gruppi hanno anche chiaramente dichiarato i propri piani a supporto degli interessi e del conflitto per le informazioni russe, come emerge nel manifesto di Noname057(16). Questo gruppo ha piani evidentemente a favore della Russia e ha indirizzato, con regolarità, gli attacchi verso l'Ucraina con l'intenzione di espandere il proprio raggio d'azione.

Durante gli ultimi mesi, Noname057(16) ha individuato come obiettivi degli attacchi futuri Paesi nell'Unione Europea dichiaratamente impegnati a sostenere l'Ucraina come Polonia, Lituania, Lettonia, Slovacchia e Finlandia. NoName057(16) ha anche attaccato il sito del parlamento finlandese ad agosto, dopo che la Finlandia aveva espresso interesse nell'unirsi alla NATO.

From Russia with Love (FRwL) è un altro gruppo che si è adeguato allo stesso sistema di mobilitazione, ma attirando di meno l'attenzione pubblica. Il gruppo si concentra sulla pubblicazione di informazioni private sui propri canali Telegram e si assume il merito di aver realizzato diversi attacchi contro i nemici russi. Sostengono di aver ottenuto informazioni sensibili accedendo ai canali Telegram connessi al Servizio di Sicurezza ucraino.

FRwL ha partecipato agli attacchi su Lockheed Martin e subappaltatori che producono HIMARS, che sono parte dell'assistenza americana fornita all'Ucraina. Sostiene inoltre di aver fatto breccia nel Gorilla Circuits, un produttore di circuiti informatici, che si inserisce fra i fornitori di Lockheed Martin.

L'altro schieramento è composto da altrettanto numerosi gruppi di hacktivisti che si sono mobilitati per sostenere l'Ucraina. Alcuni, come l'esercito IT ucraino, sono ufficialmente controllati dal governo ucraino. L'IT Army è stato creato qualche giorno dopo l'inizio dell'invasione russa e comprende volontari competenti provenienti da tutto il mondo per sostenere l'Ucraina seguendo le sue direttive.

Basandosi sulla definizione del CCS Zurich, l'IT Army comprende sia una serie di volontari in giro per il mondo che lavorano con l'obiettivo di coordinare attacchi DDoS contro la Russia, sia un ulteriore team che lavora a

un livello più profondo, composto da esperti di difesa e intelligence ucraina, che sono in grado di condurre operazioni tecnicamente più complesse indirizzati a specifici target russi.

Uno dei gruppi più importanti che si è unito alla causa dell'esercito IT dell'Ucraina è il TeamOneFist, il collettivo a favore dell'Ucraina, che, in agosto, aveva preso di mira la città di Khanty-Mansiysk in Russia, danneggiando la centrale elettrica e causando un blackout all'aeroporto.

Nonostante i gruppi pro-Ucraina che si sono mobilitati si siano concentrati esclusivamente sulla Russia, hanno creato dei precedenti per gli hacktivisti affiliati e mobilitati. Negli ultimi mesi abbiamo assistito a una chiara proliferazione degli hacktivisti iraniani mobilitatisi contro Europa e NATO. Il 15 luglio 2022, l'Albania ha subito un grave attacco cyber-terroristico che ha temporaneamente bloccato numerosi servizi digitali e siti web. Il gruppo che si è preso la responsabilità per gli attacchi è un gruppo chiamato Homeland Justice, affiliato al ministro iraniano dell'intelligence e la sicurezza.

In questo caso Homeland Justice è al servizio del governo iraniano contro Mujahedin-e-Khalq (MEK), un gruppo dissidente iraniano supportato dal governo albanese.

Il caso studio Killnet: da est a ovest

Uno dei maggiori attori hacktivisti dell'intero ecosistema è Killnet, che è stato pubblicamente annunciato attorno al febbraio 2022, all'inizio del conflitto russo-ucraino. Il gruppo ha iniziato le sue attività aggressive a marzo, con obiettivi primariamente ucraini. Ad aprile il gruppo ha completamente cambiato l'oggetto della sua attenzione che si è rivolta al supporto degli interessi geopolitici russi in tutto il mondo. Tra fine febbraio e settembre, il gruppo afferma di aver portato a termine più di 550 attacchi. Solo 45 di questi erano indirizzati all'Ucraina: meno del 10% del numero di attacchi totale.

Molti di questi attacchi erano diretti a obiettivi di alto profilo come i principali siti governativi, grosse compagnie finanziarie, aeroporti e molto altro. Mentre in alcuni casi è difficile comprendere l'impatto reale, in altri casi gli attacchi hanno chiaramente avuto successo. Hanno causato inattività ai principali siti web, molti dei quali fornitori di servizi pubblici essenziali.

Ecco alcuni esempi:

1. A marzo, l'aeroporto internazionale di Bradley in Connecticut (US), ha subito un attacco DDoS che ha interessato il proprio sito web. Le autorità statunitensi hanno confermato un tentato attacco DDoS su larga scala sul sito dell'aeroporto.
2. Ad aprile, alcuni siti web che appartengono al governo rumeno, come quello del Ministero della Difesa, quello della Polizia di Confine, quello della Compagnia Nazionale dei Trasporti Ferroviari e una banca commerciale, sono stati resi irraggiungibili per diverse ore. Questi attacchi si sono verificati in risposta ad una affermazione fatta dal leader rumeno del partito Socialdemocratico Marcel Ciolacu, che si è offerto di procurare armi all'Ucraina.
3. A maggio, ingenti attacchi DDoS sono stati portati a termine contro due fra i maggiori Paesi europei:
 - a. Sono stati coinvolti diversi bersagli tedeschi, incluso il governo tedesco e siti web dei politici e fra questi il sito del partito a cui appartiene il cancelliere Olaf Scholz, il sito del Ministero della Difesa tedesco, quello del Parlamento tedesco, quello della Polizia Federale e diverse autorità della polizia statale. Tutto questo è stato una risposta agli sforzi dell'amministrazione Scholz di fornire equipaggio militare all'Ucraina. Il governo ha autorizzato il trasferimento di 50 installazioni di Gepard anti-aircraft, ed ha annunciato la consegna di 7 sistemi di artiglieria semoventi e a fuoco rapido.
 - b. Il Senato italiano, il Ministero della Difesa e l'Istituto superiore di sanità sono stati presi di mira

4. A giugno, due significative onde di attacchi sono state portate a termine contro la Lituania e la Norvegia in risposta ai preoccupanti sviluppi geopolitici che sono avvenuti fra questi Paesi e la Russia:
 - a. Seguendo la decisione del governo lituano di fermare il transito di beni russi verso Kaliningrado, un'onda di consistenti attacchi ha colpito i servizi pubblici lituani e il settore privato. Durante l'attacco Jonas Skardinskas, il capo della cybersecurity presso il Centro di Cyber Sicurezza Nazionale Lituano, ha avvisato che i disagi con i trasporti, i settori finanziari e quello energetico potrebbero continuare per diversi giorni amplificando l'impatto dell'attacco. Ad un certo punto la maggioranza dei siti web lituani non erano accessibili tramite indirizzi IP esterni al paese, più probabilmente come misura preventiva finalizzata a mitigare la portata dell'attacco.
 - b. Lo stesso mese, diverse grosse organizzazioni norvegesi sono state disconnesse. Si pensa che questo attacco sia stato eseguito come risultato di una disputa riguardante il transito attraverso il territorio norvegese verso un estrattore di carbone sotto il controllo russo situato nell'Artico.
5. A luglio, Killnet ha concentrato i propri sforzi sulla Polonia e causato l'indisponibilità di molti siti web. Molti degli attacchi sono stati diretti ai portali governativi, le autorità di tassazione e i siti web della polizia.
6. Agosto è stato un mese piuttosto full per Killnet. È cominciato con un attacco in Lettonia: dopo aver dichiarato la Russia come "un Paese rappresentante del terrorismo", il sito del parlamento lettone ha subito un ingente attacco DDoS. Successivamente (nello stesso mese), l'Estonia ha affrontato l'attacco più esteso da quello del 2007, effettuato in risposta alla rimozione dei monumenti sovietici. L'efficacia di questi attacchi è stata discutibile, in quanto sembra che l'Estonia fosse ben preparata per questo genere di eventualità. Ad agosto, Killnet ha anche iniziato a concentrarsi sugli USA. Il gigante della produzione americana Lockheed Martin è stato pesantemente bersagliato da Killnet come conseguenza del rifornimento al sistema militare dell'esercito ucraino. Parallelamente Killnet ha anche targettizzato la US Electronic Health Monitoring e Tracking System e il senato statunitense, che stava dibattendo rispetto alla possibilità di mandare un aiuto addizionale all'Ucraina.
7. A settembre il gruppo ha bersagliato l'Asia per la prima volta indirizzando i suoi sforzi in particolare al Giappone, a causa del supporto giapponese all'Ucraina. Con l'evolversi del conflitto scaturito dalla contesa delle Isole Kuril, Killnet ha attaccato con successo diversi siti giapponesi, incluso l'e-government, i siti di trasporto pubblico della città di Tokyo e Osaka, i sistemi di pagamento JCB e Mixi, il secondo più grande sito web giapponese.

Leadership, recruitment e strumenti

Struttura organizzativa

I più grandi gruppi di hacktivisti che sono emersi nel corso dell'anno passato sono caratterizzati dalle loro operazioni ben strutturate che li mettono nelle condizioni, non solo di realizzare ondate di attacchi targettizzati, ma anche di attrarre persone con maggiori skills. Queste persone sono solitamente motivate da una chiara ideologia legata allo Stato e i loro obiettivi sono parte di un manifesto che contiene un elenco di regole da seguire.

Per esempio, Killnet ha più di 89.000 iscritti sul suo canale Telegram ed è organizzata secondo una struttura militare con una gerarchia marcatamente top-down. Killnet consiste in un insieme di squadre preparate ad eseguire attacchi che rispondano ad un ordine principale.

Attualmente esistono una dozzina di sotto-gruppi fra i quali il primario è Legion. Tutti questi gruppi sono guidati da un hacker anonimo con nickname KillMilk, che ha annunciato la sua intenzione di distaccarsi dal gruppo a luglio, rimanendo ancora coinvolto nelle attività del gruppo. Legion e le squadre (conosciute come:

“Jacky”, “Mirai”, “Impulse”, “Sakurajima”, “Rayd”, “Zarya”, “Vera”, “Phoenix”, “Kajluk”, “Sparta” and “DDOSGUNG”) sono considerate le forze speciali di Killnet, con Legion identificata come la sua forza di cyber-intelligence.

Tanti piccoli team sono organizzati attorno al maggiore gruppo ed il suo leader principale KillMilk, che assegna ordini d’attacco a ciascun capogruppo, che dà vita a infrastrutture indipendenti, migliorando inevitabilmente le probabilità di sopravvivenza dell’intera organizzazione. Questo metodo si è dimostrato efficace dal momento che la squadra continua a reclutare membri, crescendo numericamente. La pagina Telegram contiene regole, discussioni riguardanti gli obiettivi e le istruzioni rispetto a creare/unirsi a nuove squadre per i membri che cercano autonomia o un avanzamento gerarchico. L’evoluzione di Killnet li ha messi nella situazione in cui gli altri gruppi vogliono collaborare con loro, o ufficialmente unire le forze.

Recruitment

Un nuovo interessante fenomeno riguarda i metodi di reclutamento del gruppo. Diversamente da Anonymous, che è orgoglioso di dare il benvenuto a chiunque, senza imporre alcun prerequisito riguardante skills o piani specifici, la nuova era hacktivista accetta solo membri che rispettano prerequisiti minimi.

Molti gruppi come Killnet e le sue squadre, scelgono di investire in programmi di recruitment congrui, pubblicizzati sui loro canali Telegram. Alcuni gruppi hanno istituito un processo di pre-selezione per assumere solo hacker competenti o esperti di un particolare campo, per ridurre il rischio di fare errori che potrebbero compromettere l’intera operazione.

In ogni caso, Check Point Software ha recentemente osservato che KillNet affida le istruzioni sugli attacchi DDoS alle masse, forse a causa della mancanza di forza-lavoro necessario per portare a termine le azioni pianificate. In molteplici occasioni abbiamo anche visto KillNet offrire ricompense agli individui responsabili di atti di vandalismo fisico e non virtuale in Ucraina.

Il processo di recruitment è simile per molti gruppi russi. Per esempio, XakNet (che si considera come il “Team dei Patrioti Russi”) è un gruppo di utenti russi attivo all’incirca da marzo 2022. Questo minacciava di contrattaccare contro le organizzazioni ucraine per qualunque attacco cyber portato avanti contro la Russia e ha individuato diverse entità interne all’Ucraina che hanno rubato contenuti di un e-mail ufficiale del governo ucraino.

XakNet ha dichiarato che non recluteranno hacker, pentesters (specialisti nell’esecuzione di test di vulnerabilità di siti web), o specialisti OSNIT senza esperienza e capacità dimostrate. Altri gruppi come quello pro-Russia NoName057(16), potrebbe offrire un training tramite diversi mezzi come le piattaforme di e-learning, tutorial, corsi e attività di mentoring.

Strumenti e abilità tecnologica

I gruppi di hacktivisti si sforzano di utilizzare strumenti più avanzati per eseguire i loro attacchi, dal momento che più gli attacchi arrecano danni, più il gruppo guadagna in termini di notorietà ed esposizione. Abbiamo visto globalmente alcuni segni di tattiche avanzate, ma con l’immediata e ripetitiva natura delle campagne hacktivate, la maggior parte dell’attività era concentrata attorno agli attacchi DDoS tramite il ricorso a enormi botnet (rete di computer collegati alla rete telematica che passano sotto il controllo di un’unica entità).

A detta di Avast, NoName057(16) usa un RAT conosciuto come Bobik, che era in circolazione fin dal 2020 assieme a Redline stealer. Report recenti affermano che quei dispositivi infettati da Bobik sono parte di una botnet che esegue attacchi DDoS per conto di NoName057(16). In alcuni casi, il gruppo fa presumibilmente uso di strumenti più sofisticati. Per esempio, TeamOneFist è responsabile alle attività di disturbo contro il sistema russo SCADA, e della breccia nel sistema informatico Belarusian Cyber Partisans delle Ferrovie

Bielorusse, poco prima dell'inizio del conflitto. Ad agosto, From Russia with Love (FRwL), ha affermato di aver scritto il proprio Locker-like ransomware chiamato "Somnia".

Conclusioni

Una delle escalation più significative dei vari conflitti che si sono verificati negli anni, può essere identificata come l'attivismo nell'ecosistema del cyberspazio. Nel corso del decennio precedente, l'hacktivismo era prevalentemente un termine in voga, che non poneva rischi significativi alle organizzazioni globali. Essendo diventato più organizzato, strutturato e sofisticato l'hacktivismo ha inaugurato una nuova era.

Ciò che preoccupa è che molti gruppi di hacktivisti hanno un'agenda di attività legate agli Stati e sono asserviti agli specifici interessi e di specifici governi. Anche se questa dinamica si è manifestata inizialmente in specifiche aree di conflitto, vediamo già la sua diffusione verso occidente ed oltre. Ci aspettiamo inoltre che gli operatori hacktivisti implementino il loro arsenale e scatenino attacchi di disturbo per un Paese. Un'altra crescente preoccupazione è rappresentata dall'ispirazione generata dai gruppi di hacktivisti nei governi, che potrebbe significare l'evoluzione di questa attività in un fenomeno di lungo termine.