Poliziamoderna

Sotto attacco

La guerra che da quattro mesi si sta combattendo alle porte dell'Europa tra Russia e Ucraina è stata più volte paragonata ad un tipo di conflitto *old style*: soldati in trincea, carri armati e truppe che avanzano o si ritirano a seconda degli eventi, postazioni fisse che, di volta in volta, prendono di mira con missili e armi "convenzionali" le posizioni nemiche, bombardamenti a tappeto anche su obiettivi civili, navi che bombardano le città dal mare e navi che, dalle postazioni di terra vengono affondate. Una battaglia che, come si è letto da più parti, che ricorda molto le "guerre di posizione" dei due conflitti mondiali.

Ma c'è una guerra "silente", iniziata molto tempo prima che venisse sparato il primo colpo da parte dell'esercito di Putin verso l'Ucraina; una guerra che, a differenza di quella combattuta sul campo, non ha causato vittime fisiche, ma che, comunque, è riuscita a creare gravi problemi anche nel resto d'Europa e del mondo. Una disputa che si gioca sul terreno virtuale del cyberspazio, dove le armi non vengono impugnate, dove non ci sono grilletti da tirare, bensì mouse da cliccare e tastiere da premere e che sebbene non faccia vittime, è in grado di mettere in ginocchio le strutture importanti di un Paese, creando disservizi e minando il sistema economico e sociale.

Non a caso, ben prima dell'inizio del conflitto in atto, gli esperti hanno intercettato quello che in gergo tecnico viene definito come "rumore di fondo", ossia tutte quelle operazioni in Rete che fanno presagire ad un attacco massiccio da parte dei "pirati" del Web: un "esercito parallelo" a quello che imbraccia armi, non ufficialmente reclutato, me che è sotto gli occhi di tutti a chi risponda, sebbene indossi la "divisa" e porti il nome di una tipica *crew* come Killnet o Legion.

Dimentichiamoci la figura "romantica" dell'hacker in felpa con il cappuccio tirato su che dal garage di casa si diverte a scardinare le difese di un sito importante solo per dimostrarne le vulnerabilità e per poi dire al mondo «Sì, sono stato io!».

Quella che si sta giocando adesso nel cyberspazio è una partita diversa iniziata molto tempo prima e in cui sono stati rilasciati "ordigni silenti", come i *malware*, pronti ad esplodere in un momento preciso per creare più danni possibili; non solo attacchi a siti istituzionali, a strutture economiche o ad organi di informazione, ma una guerra fatta anche di piccoli attacchi ai singoli utenti: non a caso nell'ultimo anno fenomeni come *phishing*, *smishing* e *vishing* hanno fatto registrare un'impennata. E possiamo verificarlo anche da soli, senza guardare i dati statistici, ma dando un'occhiata ai nostri telefonini o alle nostre caselle e-mail, dove è stato un proliferare di messaggi che ci invitavano a cliccare su un determinato link per accedere a un sito inserendo i nostri dati personali.

La dimensione del conflitto in atto è tale da creare ripercussioni su numerosi settori connessi, soprattutto quelli energetico, alimentare, economico-finanziario, dei trasporti e delle telecomunicazioni, poichè in Rete ormai si svolgono gran parte delle loro attività, senza sottovalutare un settore che, soprattutto durante i conflitti, risulta essere fondamentale: la propaganda. Attraverso quest'ultima si può indirizzare e spesso creare un'opinione pubblica che appoggi quasi incondizionatamente un regime… e purtroppo, basta andare indietro di meno di un secolo per ricordarsi di come questo ambito sia così importante per detenere il potere con il consenso.

Una situazione, quella attuale, che non poteva non far innalzare il livello di guardia al massimo da parte di chi è deputato a tenere sotto controllo e fronteggiare gli attacchi nel cyberspazio: «Il Web va ormai considerato come un ecosistema unico – ci dice Ivano Gabrielli, direttore del Servizio polizia postale e delle comunicazioni – come se fosse un lago in cui tutti siamo interconnessi: lanciare un sasso in un lago crea un movimento che è percepibile a tutti i soggetti che si trovano in quell'area; a questo si aggiunge un'attività che viene percepita dalle strutture che si occupano di sicurezza informatica come "rumore di fondo". Non esiste una infrastruttura informatica esposta in Rete che, in qualche modo, non venga interessata da un'attività anonima di studio, alla ricerca di quelle che possono essere le vulnerabilità del sistema attraverso lo studio dei sistemi di sicurezza. Questo rumore di fondo si è enormemente intensificato a ridosso dell'evento bellico e ha generato uno stato di

massima allerta in tutti i Paesi che, anche perché più prossimi a quel “sasso lanciato”, potevano subire conseguenze o essere addirittura interessati direttamente da attacchi informatici».

Anche l’Italia non è rimasta indenne da attacchi alle proprie infrastrutture informatiche, con siti istituzionali oscurati per un certo periodo e siti di servizi, e di informazione, che in conseguenza dell’azione hacker sono stati costretti ad interrompere la propria attività, chiaramente con un conseguente danno verso chi, in quel dato momento, avrebbe avuto bisogno di accedere ad un dato servizio. «L’Italia ha una struttura istituzionale organizzata per prevenire e gestire eventi di questo tipo – prosegue Gabrielli – e ha intrapreso quindi da subito un percorso di massima attenzione e massima allerta in quelle che sono le sedi deputate alla gestione di situazioni di questo tipo. Elemento fondamentale per la difesa da attacchi informatici nelle sedi istituzionali è stato il Nucleo per la cybersicurezza, dove le istituzioni principalmente preposte (ministero dell’Interno, della Difesa, l’intelligence e oggi anche l’Agenzia per la cybersecurity) è stato stabilito che lavorassero in una sorta di coordinamento permanente, in modo da poter avere in anteprima quelle che sono le informazioni che, ciascuno per propria competenza, ricava dall’attività di raccolta informativa e di monitoraggio per gestire una vera e propria prevenzione dinamica che viene fatta in questi casi: ottenere le informazioni su quali sono i comportamenti, le tattiche, le tecniche di attacco, i *malware* che vengono diffusi da soggetti che non hanno un chiaro connotato territoriale. Il coordinamento tra vari settori ci permette di essere il più rapidi possibile nell’elevare la sicurezza informatica, che non è più quella che avevamo concepito qualche tempo fa: ci si metteva sul “perimetro” dell’infrastruttura a guardare oltre il confine, cercando di capire chi stesse sferrando l’attacco. Oggi viene invece prodotto un dinamismo continuo del confine, ossia le mura info-telematiche nelle quali è immersa l’infrastruttura da difendere devono essere continuamente manutenute e rese “intelligenti”: una vera e propria “contraerea” che deve intercettare i missili nemici prima che questi giungano a destinazione, e che deve essere continuamente “educata e istruita”, in modo da poter riconoscere la minaccia anzitempo; nel momento in cui la minaccia fa breccia nel sistema è più difficile riconoscerla e si è già subito un danno, una compromissione».

Quindi, prevenzione e repressione di questi attacchi, poiché di natura “criminale” (secondo l’ultimo report stilato dagli Stati Uniti, l’81% degli attacchi informatici viene ricondotto ad una minaccia criminale), sono compiti deputati alla polizia postale e delle comunicazioni che la fronteggia con la sua struttura, in particolare con le donne e gli uomini del Cnaipic (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche), esperti di criminalità informatica che, giorno e notte, combattono una guerra silenziosa a colpi di mouse e tastiera.

Ma quali sono, in sostanza, gli attacchi subiti attualmente dal nostro Paese? «Principalmente di due tipi: – risponde il direttore del Servizio – il primo orientato a danneggiare e distruggere, e quindi a minare l’operatività di strutture informatiche complesse, con tentativi di attacco che rilasciano *malware* progettati per distruggere e che, una volta superata la struttura di sicurezza perimetrale si portano nel cuore della struttura, si rendono silenti, studiano l’ambiente per poi sferrare l’attacco definitivo, che ha come fine il *wiping* delle macchine collegate, ossia radere letteralmente al suolo l’infrastruttura presa di mira. La seconda tipologia di attacco è quella effettuata con i *ransomware* che, in questo periodo storico, ha colpito infrastrutture importanti (ferrovie, ospedali, importanti aziende e amministrazioni pubbliche); un tipo di attacco, simile al primo, che mira a impedire l’attività dell’infrastruttura colpita, ma che, a differenza dell’altro che viene connotato come bellico o parabellico, è di natura estorsiva e consiste nella richiesta di un riscatto in cambio dei dati rubati. Questi ultimi, in caso di mancato pagamento, vengono resi pubblici o rivenduti al miglior offerente, così come avvenuto in conseguenza dell’attacco al comune di Palermo che si è rifiutato di pagare il “riscatto”».

Un’altra tipologia di attacco alle strutture informatiche, studiato in modo tale da non distruggerle ma di portarle al collasso, bombardandole letteralmente con milioni di richieste d’accesso in contemporanea, è quella di tipo “DoS” (*Denial of Service*): «È una forma meno pericolosa di attacco – spiega Ivano Gabrielli – ma il problema sorge quando sono presi di mira siti che erogano servizi, come banche, autorità portuali, siti di e commerce e che, in questo modo, non risultano raggiungibili, creando un disservizio agli utenti e al business dell’azienda. Ci sono anche attacchi di tipo *Layer 7*, che riguardano essenzialmente gli applicativi e non prevedono richieste di accesso numericamente importanti, ma sono studiate ad hoc per mandare in crash il sistema e non renderlo fruibile, anche se temporaneamente. Da questi tipi di attacchi ci si può difendere *in time*, ossia fronteggiando in tempo reale, attraverso una struttura difensiva, chi sta cercando di intrufolarsi nel sistema: un vero e proprio combattimento “uno contro uno”, tra chi attacca e chi difende. Una sorta di guerra di trincea virtuale».

Ma gli attacchi da parte degli hacker non sempre sono di natura “frontale”, ossia indirizzati direttamente alla struttura da colpire; infatti, sempre più spesso, complice anche l’estensione dello smartworking durante il periodo più duro della pandemia, i pirati del Web sfruttano la principale debolezza principale delle strutture informatiche, ossia il fattore umano. «Un attacco informatico ha

principalmente due chiavi di ingresso – prosegue Gabrielli – la prima è data dalla vulnerabilità di un software, del quale vengono sfruttare le falle dovute a buchi nella programmazione (i cosiddetti “bug”, *ndr*). La seconda modalità di attacco sfrutta invece il fattore umano, infatti più del 50% degli attacchi vengono portati attraverso quella che è la mala gestione, la superficialità o comunque la gestione promiscua di uno strumento informatico, come ad esempio l’uso delle stesse password sia per l’attività lavorativa che per quella personale, oppure l’uso promiscuo dello stesso device per la “doppia attività”, con il computer di casa, magari senza antivirus aggiornato e sul quale si continuano a fare le consuete attività, mentre si è collegati al dominio del posto di lavoro. Così come accaduto qualche mese fa alla Regione Lazio».

Sono tante, purtroppo, le tecniche usate dal mondo della pirateria informatica per accedere ai nostri dati personali, impossessarsi dei nostri dati e, in certi casi, fare da ponte per sferrare l’attacco a strutture ben più importanti, facendo dell’hackerato di turno, il più delle volte inconsapevolmente, il vero e proprio “basista” di una rapina e il proliferare di mail, sms e telefonate sospette negli ultimi anni, ne sono l’esempio: «È una vera e propria “pesca a strascico” quella messa in atto dalla criminalità informatica – prosegue Gabrielli – inizialmente fatta attraverso una mail con un link da cliccare (*phishing*), la cui evoluzione (*smishing*) consiste, invece, nel ricevere un sms sul cellulare da un numero che, grazie ai servizi internazionali di Voip che lo consentono, è in tutto simile o uguale a quello della nostra banca o fornitore di un dato servizio: si clicca sul link proposto e si accede in un’area in cui inserire i nostri dati (spesso anche il numero di carta di credito) ed ecco qui che la nostra vita contenuta nello smartphone (spesso anche quella lavorativa) è alla totale mercè di qualcuno dall’altra parte del mondo». L’ultimo arrivato in questo campo è il cosiddetto *vishing*, in cui si riceve una telefonata da un numero che, come nel caso dello *smishing* è totalmente simile o uguale ad uno da noi conosciuto e memorizzato, in cui un operatore ci invita, a causa di presunti problemi sul nostro conto in banca, a dargli le nostre credenziali di accesso. Dunque, anche qui l’anello debole è costituito dal fattore umano…

Un altro campo su cui si combatte la guerra in corso attualmente è quello delle cosiddette *fake news* e delle *deep fake news*: «È un terreno scivoloso che ha generato e continua a generare un dibattito accesissimo – ci dice Gabrielli – In un mondo come il nostro, in cui la libertà di espressione del pensiero è tutelata ai massimi livelli, è difficile intervenire a priori sulla validazione o meno delle notizie. Il posto occupato fino a poco tempo fa dalla televisione, oggi è stato preso dalla Rete dove l’informazione non vive di momenti di approfondimento ma è dettata principalmente dalla velocità di propagazione delle notizie. Questo è un asset che va in qualche modo tutelato, perché è ovvio che se qualcuno riesce a far filtrare cattiva informazione, il nostro sistema, che si fonda sulla formazione di un’opinione pubblica consapevole, viene ad essere minato. Il miglior argine è comprendere il fenomeno e riconoscerlo; quello in Ucraina non a caso è il primo evento bellico in cui, a livello europeo, è stato imposto con una decisione immediatamente applicabile all’interno degli Stati il *banning* dai nostri sistemi di navigazione “in chiaro” di alcuni di alcuni siti russi come Sputnik e Russia Today. Una presa di posizione molto forte. Come Polizia di Stato, dobbiamo comprendere il fenomeno e monitorarlo continuamente, perché potrebbe portare a problemi nella gestione dell’ordine e della sicurezza pubblica».

Una lotta che passa anche attraverso il supporto dei gestori delle piattaforme social, così come è successo per il terrorismo islamico, terreno sul quale principalmente si gioca questa partita: «I social nascono per essere il luogo in cui anche un singolo può esprimere il proprio parere – prosegue Ivano Gabrielli – Queste piattaforme sono tutte interconnesse e una notizia di un certo tipo, quando è costruita ad arte, può diventare virale, con una facilità e velocità di comunicazione che ovviamente viene sfruttata da chi vuole “viralizzare” il proprio messaggio. Far diventare virale una falsa notizia, significa renderla accattivante, avendo alle spalle anche una struttura importante di sostegno».

Dunque, come da sempre nel campo del contrasto alla crimininalità informatica, c’è sempre un inseguirsi a vicenda tra chi vigila e chi delinque, con la scoperta continua di nuovi tipi di tecniche di attacco che, a loro volta, necessitano di armi sofisticate, strutture all’avanguardia e quel fattore umano che è fondamentale per far sì che la lotta prosegua: «Stiamo producendo, soprattutto dall’inizio della guerra in Ucraina, uno sforzo importante sia a livello centrale che sul territorio – conclude il direttore del Servizio polizia postale – Attualmente possiamo contare su circa 1.800 risorse sul territorio che sembrano tante ma, se confrontate con quelle di altri Paesi in “pima linea” come la Francia (la Gendarmerie schiera quasi 8mila uomini nel campo del cyber) non lo sono. Stiamo vivendo un momento significativo e compiendo uno sforzo davvero incredibile: il trend di questo primo semestre denota ancora un aumento dei casi e ogni giorno registriamo circa quattro/cinque attacchi “importanti”, il che significa oltre 5.000 all’anno; una cifra enorme se paragonata alla situazione precedente la guerra tra Russia e Ucraina in cui se ne contavano al massimo una sessantina all’anno e di “qualità” sicuramente inferiore rispetto a quelli attuali, il che comporta la necessità di intervento di “qualità superiore” da parte di chi è deputato a contrastarli, e di conseguenza un investimento in formazione e

approvvigionamento delle risorse. Un passo importante in vista del futuro, perché non possiamo permetterci di farci cogliere impreparati e non adeguatamente strutturati, perché i fenomeni della criminalità informatica riguardano sì il singolo cittadino, ma da questo, come abbiamo visto, diventano un fenomeno regionale, nazionale e in ultima istanza mondiale».

04/07/2022