CYBER VADEMECUM

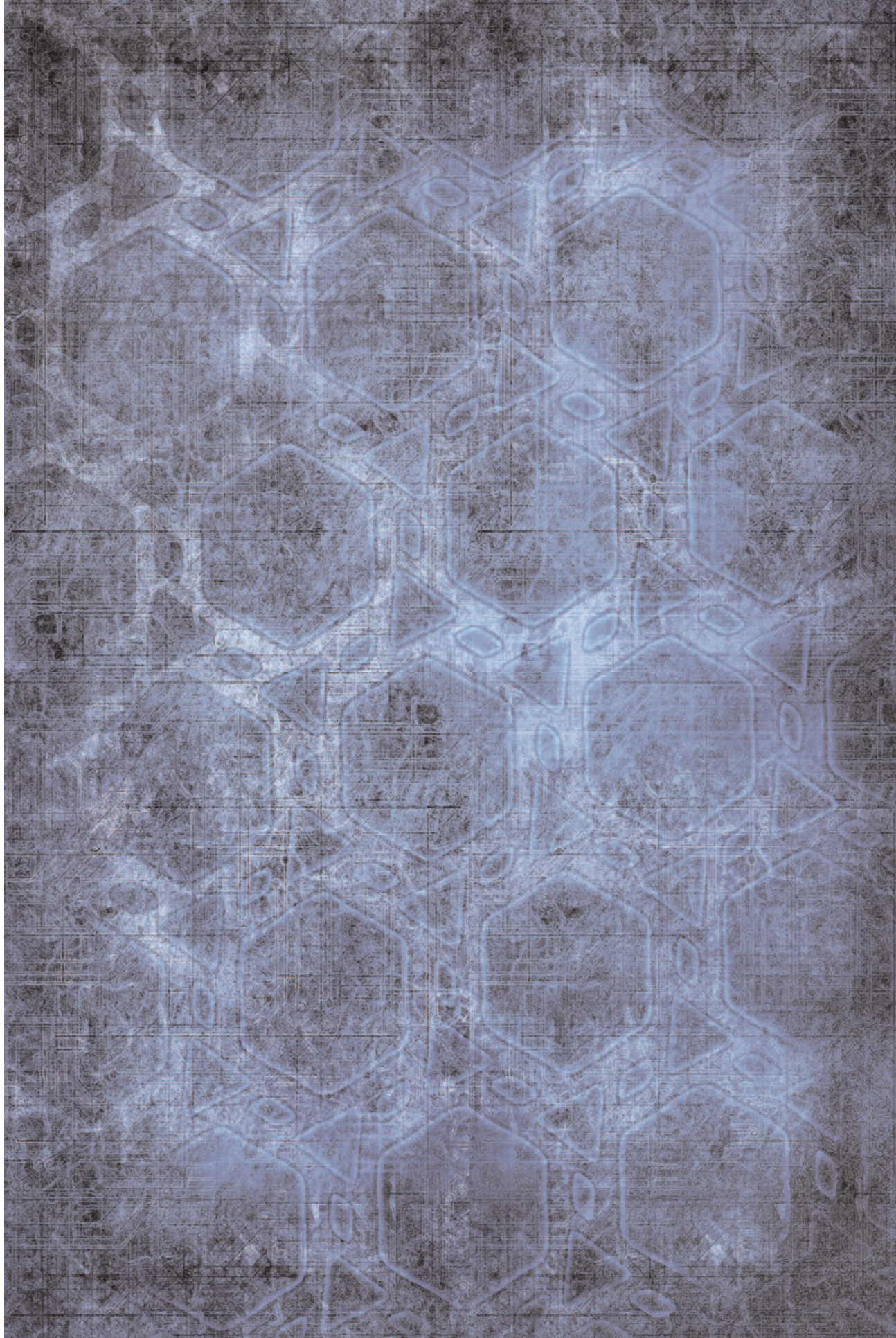
I parte

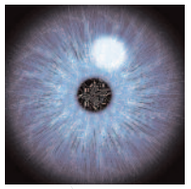
Estesa piattaforma di potenzialità ma anche di rischi, la rete telematica è il segno di una rivoluzione che sta modificando a vari livelli il nostro modo di vivere gli eventi e le attività della vita quotidiana. In pochi anni l'onda d'urto del mutamento continuo degli scenari dischiusi dal web, sempre più articolati e inafferrabili, ha indotto una ristrutturazione del nostro vocabolario, che si è arricchito di una nuova terminologia entrata con estrema velocità nell'uso comune, ancorché soggetta a rapidissima evoluzione. Il vademecum – di cui in questo numero presentiamo il primo capitolo dedicato alle minacce presenti in rete, alle relative modalità e ai potenziali attori nonché alle possibili misure di contrasto – trova fondamento per lo più in notizie tratte da fonti aperte, preliminarmente riscontrate e senza alcuna pretesa di esaustività. Il testo vuole essere una guida per orientare il lettore nella comprensione delle molteplici, complesse dinamiche del Cyber spazio.
Eventuali definizioni diverse reperibili su altre fonti non alterano significativamente i concetti esposti.

DI RAFFAELE AZZARONE

IL CONCETTO DI CYBER SPACE

A partire dagli anni Ottanta si è assistito a un incremento esponenziale della diffusione dei sistemi informatici. Ciò ha portato alla nascita di un nuovo Dominio di comunicazioni, divenuto fondamentale sia per gli aspetti politici, sociali ed economici delle nazioni industrializzate, sia per la vita di tutti i giorni (nel contesto lavorativo e personale) e per il supporto alle infrastrutture nazionali e all'informazione. Tale Dominio è generalmente indicato come Cyber Space, uno spazio che comprende ogni forma di attività digitale che viene svolta in rete.





CYBER SPACE, come la terminologia a esso associata, è definito in diversi modi nella letteratura specialistica:

DOMINIO CARATTERIZZATO dall'utilizzo dell'elettronica e dello spettro elettromagnetico per immagazzinare, modificare e scambiare dati attraverso sistemi interconnessi in rete e associati a infrastrutture fisiche.

DOMINIO COMPOSTO da un consistente numero di computer interconnessi, server, router, switch e fibre ottiche che permettono alle infrastrutture critiche di comunicare e il cui corretto funzionamento è essenziale all'economia e alla sicurezza nazionale.

SPAZIO DI DIFFUSIONE di informazioni attraverso le reti informatiche.

QUINTO DOMINIO della difesa militare (dopo terra, mare, cielo e spazio).

LA MINACCIA

L'espansione nell'uso del cyber space (segnatamente la rete internet) e la dipendenza della civiltà moderna dalla sua infrastruttura, alla quale è richiesta l'assoluta continuità del servizio, ha portato alla crescita esponenziale delle minacce, delle vulnerabilità e dei rischi a cui esso è assoggettato. Il cyber spazio è divenuto pertanto una sorta di 'campo di battaglia' ove, oltre ai sistemi informatici interconnessi, sono presenti dispositivi hardware (HW) e software (SW) capaci di distruggere e/o rendere inefficienti infrastrutture fisiche, tecniche e/o virtuali e, quindi, in grado di danneggiare capacità nazionali in settori critici[1]. Nello scenario internazionale, le Cyber Threat[2] (minacce informatiche) vanno assumendo una crescente valenza strategica, in quanto sempre più incombenti sulle infrastrutture informatizzate deputate a gestire notevoli volumi informativi, sensibili per la funzionalità delle risorse primarie del Paese, oltre che per i singoli individui. Per semplificazione analitica e interpretativa è possibile suddividere la minaccia informatica nelle seguenti principali tipologie.

CYBER CRIME[3]

insieme delle minacce poste in essere da organizzazioni criminali o transnazionali, che sfruttano lo spazio cibernetico per la commissione di reati (truffa, furto di identità, ricatto, sottrazione indebita di informazioni o di creazioni e proprietà intellettuali ecc.).

1. Governativo, economico, energetico, militare, della salute, dei trasporti, sociale ecc.
2. Complesso delle attività controindicate condotte tramite reti e sistemi di Information and Communication Technology (ICT) e/o contro di essi da una gamma diversificata di attori.
3. Tipicamente nel contesto civile.

CYBER ESPIONAGE

insieme delle attività volte a sfruttare le potenzialità della rete per sottrarre segreti industriali a fini di concorrenza sleale o superiorità strategica (sottrazione di progetti militari o dual use).

CYBER TERRORISM

utilizzo della rete da parte di organizzazioni terroristiche a fini di propaganda, denigrazione, affiliazione, coordinamento o per danneggiare infrastrutture critiche o processi che attengono alla sicurezza nazionale, con possibili conseguenze negative sulla società.

CYBER HACKTIVISM

cyber attack da parte di comunità di hacker mosse da ragioni politiche, di rivalsa, ideologiche e di protesta o dal semplice desiderio di deridere le 'vittime' designate aggirando i loro dispositivi di sicurezza. Il cyber hacktivism non si ripromette profitti economici bensì il conseguimento della massima visibilità dell'attacco perpetrato, il più delle volte consistente nell'interrompere il servizio assicurato dall'organizzazione colpita, rendendone inaccessibile il sito o diffondendo dati sensibili sottratti dai loro archivi.

CYBER WAR[4]

scenario relativo a un conflitto tra nazioni, combattuto attraverso l'abbattimento delle barriere di sicurezza delle infrastrutture critiche dell'avversario o attraverso il disturbo o lo spegnimento delle reti di comunicazione strategica e l'eventuale integrazione di queste attività con quelle propriamente belliche.

4. Tipicamente nel contesto militare.

IL CONTRASTO

Per il contrasto alla minaccia si fa riferimento ai concetti che seguono, le cui definizioni non sono tuttavia condivise unanimemente nei fora nazionali e internazionali in cui la materia viene trattata.

CYBER SECURITY

insieme di policy, strumenti, linee guida, risk management, training, tecnologie e attività relative alla prevenzione dell'impiego non autorizzato di risorse informatiche (computer, reti, sistemi di comunicazione, servizi o informazioni archiviate) e del loro eventuale danneggiamento, nonché al ripristino della loro efficienza, disponibilità, integrità e (eventualmente) riservatezza, in caso di

attacco. Dall'analisi dei documenti e provvedimenti adottati dai paesi più industrializzati è possibile enucleare i seguenti punti chiave per le strategie di contrasto:

- rafforzamento della cooperazione internazionale;
- collaborazione e partnership tra settore pubblico e privato;
- attuazione di campagne informative;
- coordinamento tra gli apparati governativi coinvolti.

CYBER DEFENCE

l'insieme della dottrina dell'organizzazione e delle attività/misure di sicurezza volte a proteggere sistemi informatici e di comunicazione da attacchi cyber. Rientrano nella Cyber Defence anche le procedure e capacità per prevenire e scoprire gli attacchi perpetrati ai danni delle informazioni e dei sistemi che le supportano, per reagire a essi, ripristinare le funzionalità dei sistemi coinvolti e analizzare gli eventi allo scopo di incrementare le capacità di difesa sulla base delle esperienze acquisite.

GLI ATTORI

Tra gli attori della minaccia, asimmetrica[5] e multiforme, si ricordano i seguenti:

STATI POTENZIALMENTE OSTILI

rappresentano la minaccia più sofisticata nel dominio cyber, in considerazione delle notevoli risorse umane e finanziarie che possono essere messe in campo per acquisire informazioni nei settori governativi, militari, industriali ed economici o per danneggiare i sistemi erogatori di servizi critici o disinformare.

TERRORISTI

ricercano attacchi distruttivi con elevata risonanza e possono avere connessioni con stati, servizi di intelligence oppure organizzazioni criminali. Sebbene non sia lo strumento principale di un'azione terroristica, l'attacco informatico può costituire un moltiplicatore di forza atto a massimizzare l'impatto di operazioni violente, complicando le risposte di emergenza e le reazioni coordinate agli attacchi fisici.

HACKER

rappresentano una categoria complessa, in quanto spesso agi-

5. Costituita da attività ostili con un numero di obiettivi ridotto e meno facilmente individuati, che usualmente coinvolgono un limitato numero di attori o forze partecipanti, con l'utilizzazione di tattiche non convenzionali che spesso hanno un serio impatto (politico e materiale) rispetto al livello di forze coinvolto.

scono solo per 'gioco' o per acquisire notorietà nel loro ambiente. Solo alcuni di essi sono intenzionati a sfruttare il sistema a loro beneficio e raramente si sono verificate azioni coordinate.

ETHICAL HACKER, noti anche come *white hat*

soggetti con eccellenti competenze di hacking i quali, dopo un passato da bad boy, decidono di aiutare la comunità scovando falle nei sistemi informativi, nei protocolli o nelle applicazioni; oppure soggetti che effettuano penetration test e vulnerability assessment, a fronte di un impegno contrattualmente assunto, per verificare il livello di sicurezza di un sistema informatico.

GRAY HAT

hacker che può ritenersi la combinazione di un black hat con un white hat in quanto capace di inserirsi, in forma non autorizzata, in un sistema informatizzato ma al solo scopo di notificare all'Amministratore che il suo sistema è stato violato, offrendosi per il ripristino della funzionalità dei dispositivi attaccati.

BLUE HAT

esperti di computer security che vengono invitati dalle ditte produttrici a testare i nuovi SW o sistemi informatici prima di lanciarli sul mercato, per la ricerca di eventuali vulnerabilità, in modo da porvi preventivo rimedio.

CRACKER, noti anche come *black hat*

si ripromettono di penetrare nei sistemi altrui per danneggiarli e per questo configurano una categoria più pericolosa degli hacker.

HACTIVIST[6]

categoria di soggetti responsabili del cyber hactivism, consistente nell'impiego di computer e reti informatiche come mezzi di protesta per motivazioni ideali (quali la tutela della libertà di espressione e dei diritti umani), religiose o politiche. Le tecniche utilizzate dagli hactivist comprendono il web defacement, il denial of service, il furto di dati, le parodie di siti web, il cyber squatting[7] ecc. Tra gli hactivist più noti si cita Anonymous (che si batte per la libera circolazione di informazioni sul web), autore di clamorosi attacchi a società e istituzioni a livello internazionale e della frequente pubblicazione di dati sensibili sottratti.

Merita menzione anche il gruppo Lulz Security (LulzSec) responsabile, tra l'altro, della compromissione degli account degli utenti della Sony Pictures nel 2011 e della messa off-line del sito della CIA. Il gruppo compie attacchi informatici per prendersi gioco delle istituzioni violate. Non a caso, il termine Lulz è una variante dello slang LOL, spesso utilizzato in internet, acronimo di Laugh Out Loud (ridere sonoramente), a cui viene associata l'abbreviazione di Security (Sec). Il termine LulzSec può, pertanto, intendersi come 'prendersi gioco della sicurezza'. Il gruppo LulzSec si è alleato con Anonymous per la conduzione delle cosiddette Operazioni AntiSec (spesso precedute dall'hashtag: #OpAntiSec) o Anti Security in quanto volte a colpire FF.PP., organismi d'intelligence e di sicurezza.
Un altro gruppo di hactivist, attivo nell'estate 2012, è quello denominatosi NullCrew che ha attaccato i siti web di Sony Mobile. Tra le sue 'vittime' si ricordano l'Università di Cambridge (in difesa dell'onorabilità del fondatore di Wikileaks, Julian Assange), la Yale University e l'esercito cambogiano. Nullcrew si dichiara contrario a ogni forma di censura sul web e combatte per un'incondizionata libertà di espressione.
Altro gruppo è il GhostShell Team che ha attaccato e sottratto dati da siti cinesi (Project Dragon Fly), da governi e agenzie internazionali di law enforcement (Project Hellfire), da numerose università nel mondo (Project West Wind) e, nel novembre 2012, da enti governativi russi (sottratti 2,5 milioni di account) a fronte dell'operazione Project Black Star. La pericolosità dei movimenti hactivist è notevole in quanto hanno dimostrato il possesso di una competenza tecnica che ne rende particolarmente difficoltoso il contrasto.

Tra gli attori della minaccia sono inoltre da ricordare:

CYBER WARRIOR

soggetti che si sentono o sono coinvolti in una guerra cibernetica, quand'anche per motivi personali o per credo politico o religioso. I cyber warrior possono utilizzare lo strumento informatico per attaccare computer target attraverso tecniche di hacking o difendere le proprie risorse da attacchi provenienti dalla controparte. Il termine cyber warrior può assumere differenti significati a seconda del contesto in cui viene utilizzato. Può riferirsi a malintenzionati o a professionisti (anche reclutati da governi e perciò definiti pure Troop On Line) che si pongono a difesa degli attacchi.

CYBER MERCENARY

lavorano su commissione e dietro compenso per attaccare specifici bersagli. Anche alcune organizzazioni criminali si avvalgono di tale supporto.

INDUSTRIAL SPY HACKER

spie infiltrate nelle società target che fanno fuoriuscire informazioni mediante CD, pen-drive o e-mail.

6. Contrazione dei termini hacker e activist.

7. Accaparramento di nomi di dominio o marchi altrui.

GOVERNMENT AGENT HACKER

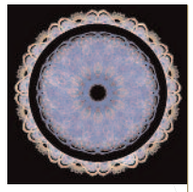
hacker al servizio di Governi per eseguire attacchi altamente sofisticati.

MILITARY HACKER

soggetti ai quali è spesso associato il profilo di State sponsored attack (particolarmente attivi sono Cina, Iran e Corea del Nord).

INSIDER

soggetti in grado di sfruttare le risorse informatiche e le informazioni di cui sono in possesso in ragione del ruolo ricoperto nell'ambiente di lavoro. La recessione che ha colpito l'economia mondiale e che sta comportando la perdita del lavoro per molte persone ha aumentato il livello e l'intensità delle minacce interne che hanno coinvolto e coinvolgeranno le aziende. Ne è esempio il dipendente insoddisfatto che reagisce danneggiando il proprio datore di lavoro o il proprio superiore mediante l'uso improprio dello strumento informatico (danneggiamento dei dati e/o del sistema) o frodando le informazioni industriali disponibili in rete a scopo di lucro.



WANNABE LAMER

spesso teen-ager che impiegano, per emulazione, le tecniche degli hacker, utilizzando i tool facilmente reperibili su internet.

SCRIPT KIDDIE

espressione utilizzata dagli hacker per indicare in senso dispregiativo quei soggetti che utilizzano istruzioni, codici e programmi (script) ideati da altri o scaricati da internet. Gli script kiddie rappresentano la forma meno evoluta di cracker, in quanto carenti in competenze e inventiva, poiché interessati al risultato delle loro azioni e non al perfezionamento delle tecniche informatiche e di hacking.

CYBER BULLI

soggetti che praticano il cosiddetto cyber bullismo o bullismo online, termini che indicano atti di molestia perpetrati tra minorenni facendo uso di e-mail, messaggistica istantanea, blog, sms, tweet, siti web ecc. Quando lo stesso tipo di molestia avvenga tra adulti o tra adulti e minori, il termine più appropriato è quello di cyber harassment (cyber molestia). Anche il cyber bullismo, di solito, prende di mira chi è ritenuto 'diverso' (per aspetto fisico, timidezza, orientamento sessuale, abbigliamento ecc.).

Tra le tipologie di cyber bullismo più ricorrenti si segnalano:

- flaming (da *flame*, infiammare), messaggi violenti e volgari, mirati a suscitare battaglie verbali in forum;
- harassment (molestia): messaggi insultanti mirati a ferire qualcuno;
- impersonation (sostituzione di persona), fingersi un'altra persona in modo da far ricadere su di essa la paternità di messaggi e testi censurabili;
- exposure (rivelazione), pubblicazione di informazioni sensibili o imbarazzanti su un'altra persona a fini denigratori;
- trickery (inganno), conseguimento della fiducia di qualcuno con l'inganno per poi pubblicarne le confidenze;
- exclusion (esclusione), emarginazione deliberata di una persona da un gruppo on-line, per procurargli un sentimento di isolamento;
- stalking (persecuzione), molestie e malignità ripetute e minacciose mirate a incutere paura.

CLASSIFICAZIONE ATTACCHI

La minaccia può concretizzarsi in cyber attack[8] (attacchi cibernetici, altrimenti detti cyber incident) che, in linea di principio, possono avere una o più delle finalità sotto elencate:

– colpire SW e HW dei dispositivi vittima mediante cyber weapon[9];
– impedire il servizio svolto dal sistema target attraverso la saturazione delle risorse da questi possedute (DoS o DDoS);
– acquisire dati in forma non autorizzata, per finalità di spionaggio (industriale, politico, militare ecc.), pubblicazione di informazioni riservate, truffa, furto di identità e di password (con quanto ne consegue in termini di appropriazione indebita di denaro e/o di materiali), sottrazione di dati commerciali (che possono essere venduti alla concorrenza), di rubriche telefoniche da utilizzare per invii di posta indesiderata (spam), sfruttamento delle risorse dei computer vittima, manipolazione delle informazioni, controinformazione ecc.

8. Attacchi cibernetici, cyber incident, definiti come le azioni di disinformazione, lo spionaggio elettronico che indebolisce le capacità competitive di un Paese, la modifica occulta di dati sensibili nei teatri operativi o la disattivazione delle Infrastrutture Critiche di una Nazione, ovvero gli asset commerciali che sono essenziali per il funzionamento della società e dell'economia.
9. Pur non esistendo una condivisa definizione di cyber-arma, questa si può ritenere un'apparecchiatura, un dispositivo ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di Infrastruttura Critica, le sue informazioni, i dati o i programmi in esso contenuti o a esso pertinenti, ovvero di favorirne l'interruzione, totale o parziale, o l'alterazione del funzionamento.

TIPOLOGIE ATTACCHI

Dall'analisi delle tecniche più utilizzate contro i sistemi informatici, emerge il consolidato ricorso alle seguenti tipologie di cyber attack, definite anche malicious activity.

DENIAL OF SERVICE (DoS)

Tra le prime a essere impiegata e ancora tra le più diffuse, ha come obiettivo quello di rendere inutilizzabile un sistema o un servizio (ad esempio inondando un sito target con una moltitudine di richieste simultanee fino a esaurirne le risorse). Le finalità del DoS spaziano da quelle puramente dimostrative a quelle criminali (quali il danneggiamento di attività altrui), causando interruzioni nel business e perdite economiche. Gli attacchi DoS possono essere raffinati e sfruttare vulnerabilità applicative o caratteristiche del sistema attaccato che consentano di sovraccaricarlo con grandi quantità di traffico. Per generare un numero elevato di connessioni o di richieste a un sito occorre, però, un considerevole numero di computer, distribuiti su una vasta area geografica o su più provider. In tal caso l'attacco prende il nome di Distributed Denial of Service (DDoS). Quando un DDoS ha scopi dimostrativi, ad esempio viene eseguito da una moltitudine di attivisti, costoro utilizzano i propri computer connessi in rete e la potenza dell'attacco è tanto maggiore quante più persone vi partecipino. Quando l'azione viene condotta da un singolo o da un piccolo gruppo e/o si intende mantenere l'anonimato, l'attaccante deve poter controllare direttamente un numero adeguato di macchine. Ciò è possibile facendo ricorso a tecniche occulte di controllo remoto, quali le botnet.

Volendo riconoscere un'entità alla minaccia (fonte «Arbor Networks»), la dimensione media degli attacchi rilevati nel 2012 è pari a circa 1.67 Gbps, con una durata media di circa 20 minuti, mentre la dimensione media nel III trimestre 2013 è stata di 2.6 Gbps. Tale portata ha un notevole impatto su organismi e aziende che affidano la loro difesa unicamente a Firewall e Intrusion Prevention System (IPS). Il 37% degli attacchi DDoS rilevati ha, tuttavia, una dimensione che varia dai 2 ai 10 Gbps. Il più massivo attacco nel corso del 2012 ne ha avuta una pari a circa 100 Gbps. Nel marzo 2013 si è assistito al più grande attacco mai registrato (di circa 300 Gbps), che ha stroncato la società britannica Spamhaus (osservatorio antispam) con effetti che si sono ripercossi sull'intera rete.

BOTNET

Derivato dall'unione di R*o*B*ot* e *net*, si riferisce a reti di computer assoggettati, detti zombie o bot, per mezzo di un malware e all'insaputa degli utenti, al comando e controllo di un 'amministratore malevolo' (bot operator o bot herder). Questi utilizza la botnet per lanciare attacchi simultanei e massicci ad altri utenti, finalizzati alla sottrazione di dati, all'invio di spam o all'inibizione delle risorse informatiche di un target. Il fenomeno è sempre più frequente e si registra l'esistenza di 'amministratori' di botnet in grado di 'affittare' queste capacità a elementi criminali. Tra le botnet merita menzione quella denominata Darkness, caratterizzata da elevate capacità di attacco.

SPAM[10] (O SPAMMING)

Consiste nell'invio insistente di posta indesiderata e, oltre a rappresentare il maggiore veicolo per la diffusione dei virus, contribuisce ad accrescere artatamente il traffico sulla rete internet. Lo spam costituisce la modalità più utilizzata per raggiungere milioni di computer con pubblicità indesiderata o per convincere subdolamente gli utenti a connettersi a siti malevoli. Nel 2009 sono stati inviati, su base giornaliera, circa 180 miliardi di messaggi spam, che rappresentano oltre il 90% del traffico di e-mail.

MALWARE

È un SW maligno, progettato per accedere a un sistema informatico, senza il consenso del proprietario, per finalità malevole e/o per danneggiarlo. In questa tipologia rientrano i Virus, i Worm, i Trojan Horse, le Logic Bomb, gli Spyware, gli Adware, i Rootkit e i Bootkit, pur non potendo ritenere tale lista completa né unanimemente condivisa da chi si occupa della materia:

- VIRUS. È un malware composto da un insieme di istruzioni e specializzato per eseguire poche, semplici operazioni e ottimizzato per impiegare il minor numero di risorse in modo tale da rendersi il più possibile invisibile. Di per sé non è un programma eseguibile, in quanto per attivarsi deve infettare un programma ospite ed è in grado, una volta eseguito, di infettare file con compiti dannosi (quali la cancellazione o il danneggiamento di file e la formattazione dell'hard disk), aprire backdoor, far apparire messaggi, modificare l'aspetto del video ecc. L'affermazione dei Social Network ha reso più facile il diffondersi di tali SW malevoli. Le persone coinvolte in queste comunità on-line vengono invogliate, subdolamente, a connettersi a siti malevoli o a scaricare file apparentemente inviati da persone conosciute. Il termine virus, nell'uso comune, viene spesso e impropriamente utilizzato per indicare genericamente i malware.

10. Il termine Spam è l'acronimo di Spiced pork and ham, nome di un tipo di carne in scatola prodotta dalla Hormel Food Corporation e consistente in un agglomerato, in varie versioni, di carne macinata di pollo, maiale, prosciutto ecc. di basso costo. Ossessivamente pubblicizzato nell'immediato dopoguerra in Gran Bretagna, fu oggetto di parodie e sketch comici.

■ WORM. È una categoria di malware in grado di replicarsi all'interno di una risorsa informatica. A differenza dei virus non necessita di legarsi ad altri eseguibili per diffondersi. Il mezzo più comunemente utilizzato per la diffusione è la posta elettronica, ma può essere trasmesso anche tramite memorie di massa come pen drive o hard disk infetti. Un worm semplice, quando non è associato a virus, di per sé non crea gravi danni, al di là dello spreco di risorse computazionali del sistema operativo che rallentano o impediscono il funzionamento normale del computer ospite, fino a giungere alla negazione del servizio. Tra i worm più conosciuti, Confiker ha infettato milioni di piattaforme Microsoft Windows e può essere trasmesso anche come memorie di massa, pen drive o condivisione di rete.

■ TROJAN HORSE, più semplicemente trojan. Si presenta come un programma apparentemente utile ma al suo interno cela funzionalità malevole. I trojan, a differenza dei virus e dei worm, non si diffondono autonomamente bensì richiedono l'intervento diretto dell'aggressore per far giungere l'eseguibile maligno al PC vittima, o mediante accesso fisico a questo o persuadendo il possessore, con tecniche di social engineering, ad aprire un file esca. Un tipo di trojan che costituisce uno degli strumenti più pericolosi attualmente utilizzati dal cyber crime è il Remote Administration Trojan (RAT) o Tool, un malware che nasconde una back-door che installandosi sul computer vittima ne prende il totale controllo. I RAT vengono scaricati in modo invisibile a seguito di tattiche di social engineering o aprendo allegati a e-mail insospettabili. Una volta che un RAT viene installato, l'hacker può utilizzarlo come veicolo per distribuirne di ulteriori a computer vulnerabili (per costituire, ad esempio, una botnet), oppure gestire a distanza il computer infettato, monitorandone l'utilizzo da parte dell'utente ignaro attraverso keylogger, sottraendo dati sensibili, effettuando attività di controllo ambientale tramite l'uso della web-cam e del microfono, prendendo visione di quanto riportato sullo schermo, scaricando nuovi malware, accedendo alle risorse di rete quali file share ed e-mail, cancellare o alterare file, creando altre back-door ecc. Tra i trojan più pericolosi e diffusi si segnala Zeus, balzato alle cronache nel 2007 per la capacità di sottrarre dati personali nei siti di banking on-line[11] e organizzando vere e proprie botnet (Zeus botnet) per controllare i computer infettati e sottraendo loro i dati. Nonostante numerosi arresti effettuati nel 2009, Zeus continua a essere una minaccia nelle sue più moderne varianti mirate a colpire anche i dispositivi mobili, dette Zeus In The Mobile (ZITMO).

11. Tra cui le password, sfruttando tecniche di keystroke logging e diffondendosi con tecniche di phishing su larga scala, ad esempio inviando milioni di messaggi su Facebook.

Un altro trojan degno di nota è Vskimmer, rilevato dalla Società di antivirus McAfee nel corso del monitoraggio di un forum underground russo, che consente di acquisire illecitamente informazioni sulle carte di credito direttamente dai dispostivi di lettura associati a computer che utilizzano Windows per le transazioni finanziarie.
Nel giugno 2013 (fonte IBM) è balzato all'attenzione OBAD, definito come il più sofisticato trojan per piattaforme mobili che utilizzano il diffusissimo sistema operativo Android. Di OBAD si evidenziano la capacità di diffondersi attraverso sms indesiderati (spam), di prendere i privilegi di amministratore del dispositivo non appena infettato e di sfuggire alle analisi, la cifratura del codice malevolo (*code obfuscation*) e la sua diffusione attraverso bluetooth e wi-fi.

■ LOGIC BOMB. È stata la prima ed è la più semplice forma di malware. Consiste in una porzione di codice malevolo inserito in forma occulta in un programma apparentemente innocuo e configurato per produrre i suoi effetti (comparsa di messaggi indesiderati sul display, cancellazione di file, spegnimento del PC ecc.) al verificarsi di specifiche circostanze, come il richiamo di particolari file. Una situazione comune è quella della bomba a tempo (time bomb) che si attiva in un giorno e a un'ora prestabilita. Spesso i virus / worm / trojan contengono bombe logiche.

■ SPYWARE. Si tratta di SW utilizzati per prelevare informazioni sensibili dal sistema in cui vengono occultamente installati, per trasmetterle al destinatario interessato a carpirle fraudolentemente. I dati acquisiti possono spaziare dalle abitudini di navigazione nel web dell'utente, fino alle password o alle chiavi crittografiche utilizzate.

■ ADWARE[12]. Si tratta di una modalità di acquisizione di licenza d'uso di SW, a prezzi ridotti o nulli che, come contropartita, comporta la presentazione all'utente di messaggi pubblicitari durante l'uso dello strumento informatico. Talvolta, però, tali programmi presentano rischi per la stabilità e la sicurezza del computer, in quanto aprono continuamente pop up pubblicitari che ne rallentano le prestazioni o ne modificano artatamente gli indirizzi Web selezionati dall'utente, portandolo su link diversi da quelli voluti oppure comunicando le abitudini di navigazione dell'utente a server remoti, compromettendone la privacy. Per tale ragione, molti antivirus classificano vari adware come riskware (SW rischiosi) e ne bloccano l'installazione.

12. Contrazione di Advertising-Supported Software, ossia SW sovvenzionato dalla pubblicità.

■ ROOTKIT, letteralmente, attrezzatura di amministrazione. Consiste in un SW fondamentale per il funzionamento del Sistema Operativo, prodotto per acquisire il controllo su di un sistema informatico senza aver bisogno dell'autorizzazione dell'utente o di un amministratore. Per tale caratteristica i rootkit vengono spesso utilizzati da hacker e cracker per nascondere le loro intrusioni. Essi agiscono in maniera invisibile, non venendo rilevati né dall'utente né dagli antivirus, permettendo di svolgere una molteplicità di operazioni in modalità stealth (furtiva), quali l'occultamento di backdoor, trojan, virus e malware. La rimozione dei rootkit malevoli è un'operazione molto delicata in quanto si rischia di compromettere l'integrità del sistema operativo su cui si installano come parte integrante di esso.

■ BOOTKIT[13]. È una recente tipologia di virus che viene eseguito nel breve intervallo di tempo in cui, all'accensione del computer, il Basic Input-Output System (BIOS) inizializza i dati di configurazione prima di passare il controllo al sistema operativo. Il virus procede infettando inizialmente il settore dell'hard disk deputato all'avvio del computer in modo da poter poi inoculare, senza essere rilevato, l'agente virale rootkit. Grazie alla possibilità di anticipare l'avvio del sistema, tale virus ottiene il massimo dei privilegi all'interno del sistema vittima, non subendo alcuna restrizione e permanendo invisibile anche grazie alle funzioni da lui stesso inserite affinché non vengano visualizzati né modificati o cancellati i processi malevoli che sono stati attivati

continua

13. Contrazione dei termini boot, processo di avvio di un computer, e Rootkit.