CYBERVADEMECUM

II parte

DI RAFFAELE AZZARONE

Abbiamo dedicato la prima puntata del Vademecum *al concetto di cyber space divenuto, progressivamente, una sorta di vero e proprio 'campo di battaglia'; non è un caso che tra le diverse definizioni elaborate dalla letteratura specialistica troviamo anche quella di 'quinto dominio della difesa militare, dopo terra, mare, cielo e spazio'. Ci siamo soffermati sulle principali tipologie in cui si declina la minaccia informatica, su alcuni attori della medesima, tra cui gli stati potenzialmente ostili, i terroristi e gli hacker, dando spazio agli snodi fondamentali delle strategie di contrasto. Abbiamo iniziato a tratteggiare le diverse forme di* malicious activity, *relative finalità ed effetti. In questo secondo capitolo ne completiamo il quadro, con il focus sulle più recenti versioni di malware, connotate da uno spiccato indice di offensività.*

Le più recenti versioni di malware, particolarmente offensive, si possono presentare in forma cifrata così da evitare l'identificazione dagli antivirus tradizionali, e comprendono anche le seguenti tipologie:

- METAMORPHIC MALWARE, riscrivono i codici malevoli a ogni reiterazione, per cui ogni versione del codice è differente dalla precedente. Ciò rende difficile la loro rivelazione e messa in quarantena da parte degli anti-virus che operano sulla base del riconoscimento della signature del malware, in precedenza memorizzata nel data base;
- POLIMORPHIC MALWARE, in genere suddivisi in due parti, una che muta a ogni interazione e l'altra che rimane costante, il che rende più facile, rispetto al caso precedente, la loro scoperta.

BACKDOOR, letteralmente *porta sul retro*.

Identifica quei programmi che consentono di superare le procedure di sicurezza attivate in un sistema informatico, e di accedervi in forma non autorizzata. Queste porte possono essere intenzionalmente create dai gestori del sistema informatico per rendere più agevole la manutenzione dell'infrastruttura informatica da remoto o per consentire un accesso di emergenza a un sistema (ad esempio qualora non si disponga della password). Le backdoor possono essere installate da alcuni malware e venire utilizzate da cracker per manomettere il sistema in modo da consentire a un utente esterno di prendere il controllo remoto della macchina in forma non autorizzata. Oltre al pericolo per l'integrità delle informazioni presenti sul sistema, le backdoor installate dai virus possono essere utilizzate per condurre attacchi di tipo DDoS.

MAN IN THE MIDDLE (Mitm), letteralmente *uomo interposto*.

Si tratta di una tecnica di attacco con cui l'aggressore si inserisce tra due sistemi interconnessi in rete, spacciandosi per uno di essi e intercettando le comunicazioni che un utente invia al corrispondente, che sono così spedite alla macchina dell'attaccante che può recepirne i contenuti e/o modificarli o distruggerli, prima di rispedirle alla reale destinazione. Gli utenti che risiedono ai due estremi del collegamento non sono in grado di accorgersi della violazione della riservatezza della loro comunicazione. Tale tipo di attacco è reso possibile dalle vulnerabilità dei codici di identificazione delle schede di rete delle macchine interconnesse (Media Access Control-Mac-address) e degli indirizzi IP.

MAN IN THE BROWSER (Mitb o Mib)

Tipologia di attacco simile al Mitm, e consiste nell'infettare un web browser per mezzo di un trojan, in modo da modificare le pagine web, modificare o aggiungere transazioni di on-line banking ecc. senza essere rilevabile né dall'utente né dai server di rete. A titolo di esempio, in caso di transazione bancaria effettuata in rete, all'utente apparirà sul suo schermo l'esatto ammontare della somma trasferita e il destinatario prescelto, mentre la banca riceverà istruzioni alterate per la destinazione dei fondi e/o il loro ammontare. La minaccia Mitb può essere contrastata con tecniche di conferma delle transazioni off line, ad esempio con l'invio di un sms di verifica della banca sulla transazione effettuata, pur se tale procedura può essere a sua volta vanificata qualora anche il telefono mobile dell'utente fosse stato infettato con malware del tipo *man in the mobile* (MitMo).

KEYLOGGER

Strumenti in grado di registrare ciò che un utente digita sulla tastiera del proprio computer o che riproduce con il copia/incolla, e inviarlo via rete a un computer remoto, consentendo il furto di password e/o di dati. I keylogger possono essere di tipo HW o SW. Nel primo caso sono dispositivi (apparentemente filtri di segnale) che vengono collegati al cavo di comunicazione tra tastiera e computer, o al suo interno. Nel secondo caso sono SW malevoli installati nel computer vittima per mezzo di trojan ricevuti tramite internet o inseriti manualmente da persone che hanno accesso fisico alla risorsa informatica. Per evitare di essere monitorati da tali dispositivi si può far ricorso alle tastiere visualizzabili sullo schermo.

FORM GRABBER, letteralmente *accaparratore del modulo*.

Cattura le informazioni private di un utente (quali username e password) direttamente dalle caselle di testo che questo compila in pagine o moduli web, in modo da utilizzare le informazioni per scopi fraudolenti. Tale tecnica è più efficace del keylogger, in quanto i dati acquisiti sono più facilmente leggibili e già strutturati per le finalità degli attaccanti.

DATA BREACH

noto anche come *data leak* o *data spill*. Si riferisce a un incidente informatico, intenzionale (a opera di hacker) o non intenzionale, nel corso del quale dati sensibili, protetti o confidenziali sono copiati o trasmessi o visti o rubati o usati da parte di soggetti non autorizzati. Il data breach può riguardare informazioni finanziarie o dati personali o dettagli delle carte di credito ecc.

ZERO-DAY

Definisce qualsiasi vulnerabilità non nota di un SW o di un processo e, per estensione, indica una tipologia di attacco che inizia nel 'giorno zero', cioè nel momento in cui viene scoperta una falla di sicurezza in un sistema informatico. È notevolmente pericoloso poiché viene lanciato quando non è stata ancora distribuita alcuna *patch* (toppa) relativa al SW preso di mira e i sistemi non sono protetti. Normalmente si parla di zero-day riferendosi a un'attività dolosa compiuta da cracker, ma anche gli ethical hacker sono alla ricerca di tali vulnerabilità allo scopo di segnalarne la presenza.

EXPLOIT

Codice che, sfruttando un *bug* (baco) o una vulnerabilità, porta all'acquisizione di privilegi o al DoS di un computer. Un exploit può sfruttare solo una specifica falla e, quando questa viene riparata, diviene inutile per le nuove versioni del programma attaccato. Per tale motivo alcuni black hat hacker non divulgano gli exploit trovati ma li tengono riservati per loro e per la comunità per poterli utilizzare nel momento più favorevole. Questi codici, quando poi vengono utilizzati, prendono il nome di *zero-day exploit*.

CROSS-SITE SCRIPTING (Xss o Css)

Attacchi contro siti web che visualizzano in modo dinamico le informazioni inserite da un utente senza effettuare i dovuti controlli. Gli attacchi Xss forzano un sito web per aver accesso ai dati immessi dall'utente ignaro e porre in atto azioni malevole (raccolta e manipolazione dati, reindirizzamento delle informazioni riservate, modifica dei dati presenti sul server ecc.). Grazie alle vulnerabilità Xss dei siti, dopo aver infettato il sito target con un codice maligno, un pirata può recuperare i dati scambiati tra l'utente e il sito compromesso o far visualizzare all'utente un modulo in cui inserire dati di autenticazione o reindirizzarlo a una pagina sotto il controllo dell'aggressore che si presenti, in forma ingannevole, con la stessa interfaccia grafica del sito compromesso.

SPAMDEXING

nota anche come *search engine poisoning*. Forma di indicizzazione delle parole chiave normalmente usate per attivare i motori di ricerca. Qualora appositamente alterata, può orientare la ricerca a favore di siti controllati da soggetti ostili. Questa tecnica viene sempre più usata dagli hacker per diffondere SW contraffatti contenenti codici malevoli. Gli utenti della rete, artatamente indirizzati verso i siti ostili, scaricano così, inconsapevolmente, i pacchetti SW manipolati, ritenendoli originali.

SOCIAL ENGINEERING TECHNIQUES

Tecniche finalizzate a carpire, mediante lo studio dei comportamenti dei soggetti nell'uso della rete e l'applicazione di tecniche di persuasione, le informazioni necessarie per accedere alle infrastrutture informatiche dell'obiettivo e dei loro contenuti, ad esempio a scopo di lucro, accedendo ai conti correnti on line del target.

PHISHING, letteralmente *pesca*.

Consiste nel furto digitale dei dati personali registrati negli spazi web per lo svolgimento di attività on line. Quando si tratta di acquisizione di informazioni di rilevante valore o perpetrate ai danni di alti manager di organizzazioni target, in luogo di phishing viene a volte utilizzato il termine *whaling* (da *whale*, balena[1]).

1. Un recente rapporto indica che negli Usa sono rubati, su base annuale, circa nove milioni di dati personali (numeri di carte di credito, indirizzi email, numeri di social security card ecc). Una volta in possesso di tali informazioni, acquisite con tecniche di *social engineering*, i criminali/terroristi sono in grado di acquisire dati finanziari, sensibili o classificati.

TEXT MESSAGE SCAMS, noto anche come S*miShing* (Sms+phiShing).

Forma di *phishing* attuata inviando al telefono cellulare vittima sms fraudolenti. L'evoluzione dei dispositivi di telefonia mobile (Gprs, Umts, Wifi) sta favorendo l'attività di registrazione e monitoraggio di messaggi scambiati via internet, prevalentemente in modalità wireless. La rapida crescita dell'utilizzo di questi prodotti rappresenta la nuova frontiera per le frodi criminali.

SPEAR PHISHING, letteralmente *pesca con l'arpione*.

Attacco con l'inoltro di una *spoofing email* (messaggio ingannevole) che sembra provenire da fonti affidabili (un Ente conosciuto, una persona nota ecc.), che ha per obiettivo una specifica azienda o un'organizzazione e che mira a ottenere l'accesso non autorizzato a dati confidenziali. Come per il *phishing*, lo *spear phishing* ricorre a tecniche di ingegneria sociale per convincere un utente target, in quanto dipendente dell'azienda prescelta, a clickare su un link o aprire email malevole, dai quali il malcapitato scaricherà un malware o altri programmi che faranno del suo computer un bridge verso il sistema core dell'azienda stessa.

ADVANCED PERSISTENT THREAT (Apt)

Identifica sofisticate minacce ai sistemi informatici, che mirano a colpire organizzazioni governative, finanziarie e industriali, per sottrarre informazioni, proprietà intellettuali e dati sensibili per scopi di cyber crime, spionaggio o semplice divulgazione di dati sensibili da parte di movimenti idealisti. L'attacco consiste in azioni coordi-

nate, messe in atto da parte di gruppi altamente specializzati, ben organizzati e spesso ben finanziati (anche da paesi ostili), che si sviluppano in maniera silente nel corso di un lungo periodo (da cui il termine *persistent*), in modo da acquisire i dati voluti con un approccio *low and slow*. Le metodologie comprendono sia le tecniche d'intrusione informatica, sia quelle di social engineering, sia quelle di intelligence tradizionale, per acquisire informazioni sui comportamenti del target. Le Apt rappresentano minacce molto pericolose e non contrastabili con i tradizionali antivirus. Tra le Apt si segnala GhostNet, scoperta nel 2009 e utilizzata per attività di *cyber spying* su vasta scala, a danno di computer appartenenti ad ambasciate, ministeri degli affari esteri, uffici governativi ecc. Il centro di Comando e Controllo di GhostNet è risultato ubicato in Cina. L'infezione è avvenuta attraverso l'inoltro di email contenenti allegati malevoli con i quali veniva inoculato nel PC vittima un trojan grazie al quale ne veniva preso il totale controllo, sia per la sottrazione di dati sia per l'attivazione a distanza della web-camera e del microfono in modo da attivare una sorveglianza ambientale audio-video. Tra gli altri attacchi di tipo Apt si segnala anche l'*Operazione Aurora* – la cui paternità è attribuita a organizzazioni cinesi legate al People's Liberation Army – consistente in un attacco durato tutto il secondo semestre del 2009 e avente come destinatari numerose società (Adobe Systems, Yuniper, Northrop Grumman, Dow Chemical ecc.), con il principale obiettivo di ottenere l'accesso ed eventualmente modificare gli archivi dei codici sorgenti delle citate società, che sviluppano innovative tecnologie nei settori della sicurezza e della difesa. Un altro attacco Apt sofisticato, identificato dalla McAfee sempre nel 2009, è il *Night dragon*, ancor oggi in circolazione con nuove varianti, in quasi tutti i continenti. Night dragon ha come obiettivo società petrolifere e del settore energetico, con lo scopo di sottrarre informazioni su attività, ricerche esplorative e dati finanziari.

CYBER WEAPON

I principali malware rilevati in questi ultimi anni che possono ritenersi cyber armi, nei termini visti in precedenza, pur se tale classificazione non è unanimemente condivisa, sono i seguenti:

- Stuxnet, nome attribuito a un software malevolo, di tipo worm, che include anche una rootkit, progettato e realizzato per colpire una specifica configurazione di impianti industriali controllati informaticamente, denominata *Supervisory Control and Data Acquisition* (Scada). Scoperto nel giugno 2010, ha infettato il sistema prodotto dalla società Siemens per il controllo della centrale nucleare iraniana di Natanz. L'infezione sarebbe avvenuta con una chiavetta Usb (il che fa pensare all'azione consapevole o inconsapevole di un insider), provocando danni alle centrifughe utilizzate per l'arricchimento dell'uranio. Per la complessità e la tipologia del target, la sua creazione è attribuita a paesi di elevate potenzialità nel settore informatico, quali Usa e Israele. Qualora così fosse, stuxnet potrebbe essere ascritto alla cyber warfare in cui un paese mira a recare un grave danno alle infrastrutture critiche di un Paese avversario.
- Du.Qu., malware scoperto nel settembre 2011 e forse derivato dallo *stuxnet*. Ciò porta a ipotizzare, per le complessità e singolarità progettuali, che le due tipologie possano essere state sviluppate dagli stessi autori. Tra i due malware sussistono, tuttavia, notevoli differenze. Mentre stuxnet opera per compromettere sistemi industriali, autoreplicandosi il più velocemente possibile, Du.Qu. è stato progettato per acquisire informazioni nel modo meno invasivo possibile, ottenendo credenziali e documenti per poi condurre un attacco mirato. Stuxnet, in sintesi, è stato realizzato per generare danni nell'immediato, mettendo in crisi i sistemi di controllo delle stazioni industriali, mentre Du.Qu. opera con un trojan finalizzato alla raccolta di informazioni, sostanzialmente silente, di difficile rilevazione e con capacità di autodistruzione a termine esigenza. Du.Qu. viene installato grazie a un exploit di tipo *Zero-day* e una volta operativo installa un *keylogger* per catturare le informazioni digitate sulla tastiera che memorizza, cifra e comprime prima di inoltrarle al controllore. Come altra caratteristica, parte del suo codice è stata scritta con un linguaggio di programmazione non ancora completamente identificato.
- Wiper, nell'aprile 2012 sono stati registrati una serie di incidenti informatici riconducibili a un malware che attaccava i computer di alcuni stabilimenti petroliferi dell'Asia occidentale, in particolar modo iraniani. Tale malware determina la cancellazione dei dati residenti sugli hard disk dei computer infettati e di quelli che possono essere utilizzati per identificarlo. In pratica il file system danneggiato da Wiper impediva il *rebooting*, cosicché in ogni macchina attaccata non rimaneva nulla dopo l'attivazione del malware rendendo impossibile il ripristino del sistema o il recupero dei dati. Wiper è un programma malevolo rimasto per lo più sconosciuto che può aver portato alla creazione di nuove varianti come *Shamoon*.
- Flame, identificato nel maggio 2012, forse derivato da *stuxnet* ma ancor più sofisticato, è stato progettato per lo spionaggio informatico e per sottrarre informazioni dai computer colpiti, dai contenuti presenti sul display, dai file archiviati, dalle registrazioni audio/video e dal traffico inoltrato in internet. Le informazioni ottenute sono inviate a server di comando e controllo dislocati in diverse parti del mondo. Il codice malevolo è costituito da più moduli divenendo così circa 20 volte più grande di *stuxnet*. Flame agirebbe sia sfruttando backdoor sia come trojan che come un worm. Di recente scoperta è la variante di Flame denominata *mini flame* e con-

sistente in un ridotto ma flessibile malware progettato per il furto di dati e il controllo di sistemi infettati nel corso di mirate operazioni di cyber espionage. A differenza di FLAME, progettato per acquisire massive quantità di dati, *mini flame* è uno strumento chirurgico di alta precisione, una cyber weapon che può operare indipendentemente o come componente di flame, da utilizzarsi nella seconda ondata di un attacco.

- GAUSS, rilevato nel giugno 2012, è un malware progettato per sottrarre dati relativi a credenziali bancarie e acquisire il più elevato numero possibile di informazioni sulle macchine infettate. Comprende una parte di codice malevolo (*payload*) criptato, il cui scopo non è ancora noto. GAUSS, basato sulla stessa piattaforma di *flame* e di cui possiede alcune caratteristiche (come le routine per infettare i drive USB), nasce con finalità di spionaggio e ha principalmente attaccato sistemi informatici in Libano, Israele e Palestina.
- MAHDI (il Messia), rilevato nel giugno 2012 dalla società russa di antivirus Kaspersky e da quella israeliana Seculert, è un malware altamente nocivo che sta infettando computer personali, di aziende e istituzioni in Iran, Israele, Afghanistan, Eau e Arabia Saudita. Il programma è di tipo trojan, è scritto quasi interamente in lingua farsi ed è in grado di sottrarre non solo informazioni importanti (tra cui i contenuti visualizzati sul display del computer), ma anche informazioni sui sistemi, file archiviati, contatti e conversazioni audio, oltre che spiare nei Social forum e nelle email, per cui può definirsi anche come spyware. Gli artefici del MAHDI sono ignoti ma non sembrerebbe essere stato progettato, a differenza di *stuxnet*, *du.qu.* e *flame*, da stati o enti governativi.
- SHAMOON, noto anche come *disttrack*. È stato scoperto nell'agosto 2012 e utilizzato per finalità di cyber espionage, in grado di attaccare computer che utilizzano il sistema operativo Microsoft Windows NT. A differenza di altri malware utilizzati per lo stesso scopo, Shamoon è anche dotato di un modulo distruttivo in grado sia di cancellare i file relativi ai dati sottratti sia di sovrascrivere (con l'immagine di una bandiera americana in fiamme) il settore di avvio dell'Hard Disk, rendendo inutilizzabile il computer attaccato. Inoltre può espandersi infettando altri computer connessi in rete, sfruttando le vulnerabilità delle risorse HW condivise. Nell'agosto 2012 SHAMOON è stato utilizzato da un gruppo denominato Cutting Sword of Justice (spada tagliente della giustizia), che ha disabilitato circa 30.000 workstation della Saudi Aramco. Analogo attacco è stato subìto dalla società RasGas del Qatar. Fortunatamente SHAMOON non ha avuto grande diffusione in quanto, a oggi, il numero degli attacchi sarebbe inferiore a 50. Da analisi della Kaspersky è emerso che tale malware, per gli errori riscontrati, è definibile come un'opera *quick and dirty*, ovvero realizzata, a livello amatoriale, da programmatori esperti ma di profilo non elevato.

ADVANCED EVASION TECHNIQUES (Aet)

Categoria di tecniche evasive sofisticate, in grado di eludere i dispositivi di sicurezza posti sulle reti, sfruttando le vulnerabilità dei protocolli di comunicazione. Tali tecniche non sono di per sé dannose ma consentono di veicolare malware attraverso il normale traffico in rete, senza che vengano rilevati. La pericolosità delle Aet risiede nel fatto che sono il prodotto di più tecniche di evasione di base tra loro combinate o combinabili in un pressoché illimitato numero di modi, che agiscono a differenti livelli sulla rete.

SQL INJECTION

tecnica di hacking molto diffusa, mirata a sottrarre informazioni da data base di tipo sql (Società Ibm) accessibili via internet. L'attacco sfrutta le carenze nei controlli e nella validazione degli input generati dall'utente, consentendo all'aggressore di inserire (*injection*) il codice maligno (*sql command*) all'interno della *query* (interrogazione del data-base) che gli consentirà di autenticarsi con ampi privilegi in aree protette del sito, senza essere in possesso delle credenziali di accesso, by-passando il processo di log.in e accedendo così, direttamente, ai dati al fine di visualizzarli, copiarli e/o alterarli.

WEB DEFACEMENT, letteralmente *defacciamento*, ossia modifica o deformazione della faccia

È un attacco a un sito web che ne provoca il cambiamento o la sostituzione dei contenuti di una o più pagine, in genere la home page. Tali attacchi sono tipicamente attuati da system cracker o da hactivist, i quali riescono a entrare in un web server, per lo più con tecniche di sql injection, che permettono loro di acquisire credenziali di amministratore. La pagina sostituita in genere riporta lo pseudonimo del defacer o l'hacking codename, così come spesso è attuato dagli hactivist di A*nonymous*. Il DEFACEMENT non è di per sé dannoso e ha essenzialmente finalità dimostrative della bravura del defacer o di propaganda ideologica o di scherno dell'Amministratore del sistema preso di mira per dimostrare l'inadeguatezza dei dispositivi di sicurezza adottati.

MULTI-VULNERABILITY ATTACK

Nuove strategie, adottate in special modo da hactivist, consistenti nella conduzione in parallelo, da parte di *botnet* o di gruppi di soggetti tra loro coordinati, di differenti tipologie di attacco a vari punti vulnerabili di un'infrastruttura informatica vittima, come i server di rete e i livelli applicativi. Tali campagne risultano particolarmente efficaci in quanto lo scopo viene raggiunto anche se uno solo dei vettori d'attacco riesce a penetrare le difese perimetrali del sistema vittima. L'assunzione degli attaccanti è che nonostante le molteplici tecniche adottate per la protezione dei bersagli, vi saranno comunque uno o più punti vulnerabili.

RANSOMWARE

Tra le minacce cibernetiche emergenti, consiste in un malware progettato per infettare una postazione informatica, bloccandone l'utilizzo, criptando l'hard drive e per il cui ripristino l'attaccante avanza una richiesta di riscatto da versare su conti bancari coperti da anonimato. Nei casi più frequenti l'utente vittima vede apparire sullo schermo un messaggio recante il logo di Ff.Pp., in cui si sostiene che è stata rilevata la frequentazione di siti pedopornografici o l'utilizzo di SW piratati o l'inoltro di messaggi con finalità terroristiche.

SCAREWARE

Vendita di falsi SW antivirus facendo leva, con tecniche di social engineering, sulle paure degli utenti (*scare*, terrore) con messaggi fraudolenti, ad esempio comunicando che il loro computer è infetto e invitandoli ad acquistare subito il falso antivirus. Una volta conseguito il convincimento della vittima, i truffatori potranno impossessarsi del denaro e dei dati della carta di credito.

ROGUE SECURITY SOFTWARE

Frode (*rogue*, furfante) perpetrata con tecniche di social engineering, consistente nel convincere l'utente vittima a rimuovere un fittizio malware presente sul computer unitamente all'antivirus installato, invitandolo ad acquistare e installare l'antivirus suggerito che, spesso, contiene un trojan (tra i metodi volti a persuadere la vittima a comprare i prodotti alternativi vi è anche quello di dichiarare che una quota parte dei proventi verrà devoluta in beneficenza).

PHARMING

Da *phishing*, pescare e *farming*, coltivare; forma di phishing con cui carpire credenziali di accesso, username e password e attuare il furto di identità. Il PHARMING consiste nel reindirizzare il traffico che una vittima è intenzionata a inoltrare a uno specifico web site a un altro dannoso, ma simulato in modo da apparire legittimo. In genere implica la necessità di apportare modifiche alle impostazioni del computer vittima o al D*omain* N*ame* S*ystem* (Dns) che traduce i nominativi, digitati in forma alfanumerica nel browser, in indirizzi IP numerici.

IDENTITY THEFT

furto di identità, acquisizione fraudolenta e utilizzo illecito dei dati identificativi e del reddito di un'altra persona. Le finalità del furto di identità spaziano dall'*identity cloning* (clonazione) al *financial identity theft* (furto dell'identità finanziaria) per ottenere crediti o prestiti o aprire conti correnti, o addirittura al *ghosting* (furto dei dati personali di una persona defunta). I furti d'identità avvengono acquisendo i dati della vittima soprattutto attraverso i social network (ove gli iscritti, spesso senza cautele, inseriscono nomi, foto, numeri di telefono, date e luoghi di nascita ecc.), oppure con tecniche di social engineering (ad esempio rispondendo alle richieste di dati personali provenienti da falsi siti di banche, istituzioni nazionali, aziende fornitrici dei servizi di credit card ecc.). Altre tecniche consistono nell'acquisire i dati a seguito di inoculazione di malware sul PC vittima. Informazioni sugli individui prescelti si possono anche acquisire con metodologie non-cyber, ad esempio rovistando nella spazzatura laddove, incurantemente, sono cestinati ricevute, bollette, estratti conto ecc.

DNS HIJACKING

Il D*omain* N*ame* S*ystem* (Dns) può essere inteso come la rubrica telefonica di internet in quanto consente a un PC di tradurre i nomi dei siti (ad esempio www.ilmeteo.it) nei corrispettivi indirizzi numerici IP (ad esempio 195.24.65.215 in decimale), in modo da permetterne la connessione. Un attacco DNS HIJACKING (dirottamento) consiste nella fraudolenta sostituzione dell'indirizzo del sito desiderato con quello di un altro somigliante a quello voluto, ma in maniera ingannevole e che contiene pubblicità indesiderata o è la pagina di una società concorrente a quella cercata o una pagina contenente malware ecc.

CLICK HIJACKING

Dirottamento del click. Consiste nella cattura fraudolenta del click del mouse di un computer vittima e nel suo reindirizzamento su un oggetto diverso da quello desiderato. Ad esempio, l'utente clicca su un link per accedere a una pagina web ma il suo comando viene reindirizzato, a sua insaputa, su un differente oggetto che potrebbe anche essere un pulsante per attivare una particolare azione. In questo modo l'utente viene costretto, inconsapevolmente, a svolgere attività in rete non desiderate e probabilmente anche poco lecite.

WATERING HOLE ATTACK, letteralmente *attacco all'abbeveratoio*

Il nome di questa strategia trae origine dalla circostanza che il sito compromesso rimane in attesa di essere visitato dalle vittime rispondenti a un certo profilo, in analogia a quanto fa un leone in prossimità di un abbeveratoio in attesa che vi giungano le possibili prede a dissetarsi. La dizione indica una strategia di attacco cyber avente come target un particolare gruppo di individui (ricercatori, un'industria, un'organizzazione particolare ecc.), e l'attacco si articola in più fasi. Innanzitutto l'attaccante deve acquisire informazioni sul profilo delle vittime e sul genere di siti web che normalmente sono da questi visitati (ad esempio dove compaiono articoli scientifici su determinati argomenti o dove giungono aggiornamenti in tempo reale sull'andamento delle borse). Fatto ciò, l'attaccante valuta il grado di vulnerabilità dei siti e dopo averne trovato uno o più che può compromettere, gli inietta un malware in grado di riorientare gli inconsapevoli visitatori verso siti malevoli predisposti per infettarne i PC.

continua