# CYBER VADE MECUM

## III parte

**Raffaele Azzarone**

*Le precedenti puntate del Vademecum sono state dedicate ai molteplici profili di rischio connessi all'utilizzo del cyber space. Attraverso l'approfondimento delle attività che si svolgono in rete è stato possibile delineare il quadro della minaccia che, nel suo complesso, desta grande preoccupazione. Il presente articolo fornisce un cenno sulle tecniche di anonimato che trovano vasto impiego in rete, anche per attività criminali. Vengono quindi proposti alcuni tra i più recenti e clamorosi cyber attacchi e illustrati dispositivi e procedure da attivare su una rete informatica per elevarne il livello di sicurezza. Da ultimo, uno spazio è dedicato ai social network, anch'essi potenziali veicoli di attacco da parte di cyber criminali.*

ANONYMIZER

Le tecniche di anonimizzazione consentono all'utente di navigare in forma privata e non riconducibile all'interno dei siti internet, impedendo ad altri di identificare l'indirizzo IP di provenienza, di tracciare le abitudini di navigazione e di acquisire informazioni sia a carattere personale che sulla localizzazione del soggetto. L'utilizzo di tali tecniche è divenuto sempre più frequente, anche da parte di gruppi di hacktivist e di cyber criminali, e l'espansione del fenomeno è preoccupante all'interno di aziende e organizzazioni in quanto la navigazione anonima effettuata dai dipendenti può esporle a rischi. In linea generale un A*nonymizer* è uno strumento costituito da uno o più Proxy Server che agiscono come una maschera interposta tra il PC dell'utilizzatore e la rete internet. L'accesso a internet avviene occultando sia le informazioni identificative del PC dell'utente sia la destinazione che questi intende raggiungere. Le applicazioni anonymizer si basano tipicamente sulla creazione di un 'tunnel' crittato tra l'utenza e i Proxy Server Http[1] per consentire agli utenti di superare i firewall e le restrizioni legate al filtering dei contenuti.

L'applicazione più diffusa è *Tor* (The Onion Router), basato su una rete distribuita di server utilizzati come relay in rete, gestiti da volontari in tutto il mondo il cui scopo principale è di salvaguardare la privacy della navigazione ricorrendo anche a tecniche di crittografia. Il funzionamento della rete Tor è 'semplice': i dati relativi a una comunicazione o interrogazione su internet non transitano direttamente dal client al web server ma passano attraverso i *Tor relays* che agiscono da router costruendo un circuito virtuale crittografato a strati (*multi-layer encription*[2]). I dati originali vengono cioè criptati e re-criptati molte volte con differenti codici prima del loro invio, in modo che, nell'attraversamento di ogni singolo relay, questo possa decifrare un solo strato, per passarlo poi a quello successivo che agirà analogamente. Il relay finale toglierà l'ultimo strato di cifratura (*exit node*) per poi accedere in chiaro al web server di destinazione che, pertanto, vedrà quest'ultimo nodo come l'originatore della richiesta. Il SW Tor periodicamente negozia un nuovo circuito virtuale attraverso il *Tor Network*, utilizzando la tecnica della descritta crittografia a strati, assicurando la perfetta segretezza nel transito tra i nodi interni alla rete dai quali non è possibile risalire all'origine o alla destinazione della connessione. La notorietà e la diffusione di Tor è anche legata al fatto che, tramite la sua rete, è possibile accedere al Deep web[3].

Una differente modalità per garantire l'anonimato è quella connessa all'utilizzo dei cosiddetti A*nonymous Remail*, server che ricevono messaggi di posta elettronica e li ritrasmettono seguendo istruzioni incluse nei messaggi, senza rivelarne la provenienza originaria. Ne esistono diverse tipologie:

- CYBER PUNK, che sostituisce la testata (*header*) dei messaggi da cui è possibile identificare il mittente e accettare messaggi cifrati con chiave pubblica, e ulteriori funzioni, come il riordino casuale dei messaggi in uscita o il ritardo nella loro trasmissione, in modo da ostacolare attività di analisi del traffico da parte di terzi;
- MIXMASTER, che scompone i messaggi in pacchetti che vengono poi cifrati singolarmente, riordinati in modo apparentemente casuale e inviati separatamente;
- PSEUDONIMOUS REMAILER, che consente l'invio di messaggi utilizzando pseudonimi, avendone in precedenza assegnato uno a ogni utente e depositato, in apposito archivio, le istruzioni su come inoltrare le risposte affinché possano giungere all'utente desiderato.

1. L'*Hyper Text Transfer Protocol* (Http) è usato come principale sistema per la trasmissione di informazioni sul web in una tipica configurazione client-server.
2. Ovvero crittografia a strati, da cui il termine *onion* (cipolla) utilizzato per denominare la rete Tor.
3. Il *Deep web* è l'insieme delle risorse informative inaccessibili agli strumenti standard di ricerca che caratterizzano la tradizionale rete internet (*Surface web*). I contenuti del Deep web comprendono: pagine dinamiche (cioè generate all'occorrenza), pagine non collegate (il cui accesso è impedito per impostazioni di sicurezza), pagine ad accesso ristretto, pagine il cui accesso richiede particolari procedure, archivi ecc. Ma è anche un ambiente in cui si celano malware e attività illegali, quali vendite di documenti falsi, armi e droghe (utilizzando i Bitcoin), siti pedopornografici ecc. La dimensione del Deep web sarebbe 500 volte superiore a quelle del web di superficie.





## PRINCIPALI EVENTI CRIMINOSI CHE HANNO CARATTERIZZATO IL BIENNIO 2013-2014

Gli ultimi anni hanno registrato un incremento esponenziale degli attacchi informatici di grave entità a livello globale, passando dalle poche migliaia del 2001 a centinaia di migliaia. Anche gli attacchi 'mirati' (contro individui, piccole aziende, un particolare settore ecc.), sono stati caratterizzati da un marcatissimo incremento. Nel 2013 il numero di violazioni dei dati personali è aumentato del 62% rispetto all'anno precedente, con oltre 552 milioni di identità violate e con dieci attacchi su vasta scala contro uno solo nel 2012.

L'espansione del fenomeno è attribuibile sia alla diffusione dello strumento informatico sia al crescente orientamento delle organizzazioni criminali a sfruttare le truffe informatiche quali fonti di facili guadagni, nonché all'accentuarsi delle attività di spionaggio on line e alle azioni perpetrate da gruppi di hacktivist. Particolare menzione meritano le azioni malevole che, per l'entità dei danni arrecati, la complessità tecnica e la specificità degli obiettivi lascerebbero intendere la regia di organismi statuali.

L'incremento degli attacchi ha posto in evidenza le seguenti modalità criminose:

- affitto di botnet per l'invio di spam o DDoS per bloccare l'operatività di siti web;
- attacchi di tipo *phishing*, mirati o di massa, al fine di compiere frodi bancarie;
- furto di identità per operazioni di riciclaggio di fondi clandestini;
- furto di dati sensibili, per finalità spionistiche, di segreti industriali o per il loro diretto utilizzo in forma illecita o per renderli pubblici per scopi idealisti;
- penetrazione nei sistemi Scada per acquisire dati o provocare danneggiamenti.

Il 2013 ha anche visto un drammatico aumento di malware sconosciuti utilizzati nei cyber attacchi. Sono stati rilevati, in media, oltre 220.000 nuovi malware al giorno, per circa 80 milioni nel corso dell'anno. Nel primo semestre del 2014, i nuovi codici malevoli ammontano a oltre 60 milioni.

Si tratta di numeri impressionanti se raffrontati a quelli relativi ai nuovi malware rilevati nel 2012 (circa 35 milioni) e nel 2011 (circa 25 milioni).

Significativo è anche il costante aumento di nuovi malware per dispositivi mobili che, nel 2014, sarebbe intorno a 700.000 a trimestre.

L'analisi delle rilevazioni effettuate nel 2013 ha mostrato che la maggior parte dei malware sconosciuti è stata inviata via email. I formati più utilizzati sono Pdf (35%), Exe (33%) e Archive (27%),

mentre solo il 5 % ha riguardato Microsoft Office. L'esplosione di malware sconosciuti e sempre più sofisticati è in parte dovuta all'adozione, da parte degli autori dei SW malevoli, di tecniche di offuscamento, denominate C*rypter*, in grado di eludere gli anti-virus.
Anche le modalità d'attacco sono divenute sempre più ricercate con l'adozione di tecniche volte a sfuggire a B*lack List* e U*rl filtering* poste alla base delle difese tradizionali, adottando *domain name* e indirizzi dinamici, *single-use* e apparentemente generati in modo casuale.
Gli attacchi cyber riguardano dunque l'intera comunità internazionale e, a titolo puramente esemplificativo, si fornisce un cenno su alcuni di quelli eclatanti condotti nel corso degli ultimi 12 mesi

Ottobre 2013

L'Adobe (società produttrice di Photoshop, InDesign e Acrobat) è colpita da un attacco cyber consistente nell'esfiltrazione di dati sensibili di circa tre milioni di utenti, oltre ai codici sorgenti di numerosi prodotti SW dell'azienda.

Novembre 2013

È violato il sistema informatico del Parlamento europeo a Bruxelles da parte di un hacker che è riuscito a prendere possesso delle password delle caselle email di alcuni parlamentari, introducendosi all'interno della loro corrispondenza privata.

Gennaio 2014

Sono attaccati alcuni computer del ministero della Difesa israeliano mediante un messaggio malevolo contenente un trojan (X*treme* RAT) in grado di prendere il controllo dei PC attaccati da cui sottrarre dati sensibili.

Febbraio 2014

– eBay viene violato da hacker che, accedendo al database relativo agli utenti, s'impossessano di dati personali, email crittate e password di accesso. L'azienda assicura che i dati finanziari relativi ai pagamenti non sono stati compromessi, ma esorta alcuni clienti a cambiare password;

– Whatsapp è oggetto di un attacco che comporta l'interruzione del servizio. Si sospetta che l'attacco sia una rivalsa nei confronti di Mark Zuckemberg, a seguito dell'annunciata acquisizione di Whatsapp.

Aprile 2014

Il centro di ricerca dell'European Space Agency a Colonia è vittima di un attacco coordinato teso a esfiltrare dati a scopo di spionaggio. Secondo il «Der Spiegel», l'attacco sarebbe stato sponsorizzato da uno Stato estero.

Maggio 2014

Viene data notizia della scoperta di una campagna di cyber espionage, condotta per oltre un triennio da uno Stato estero, avente come obiettivo personale militare, diplomatici e contractor appartenenti alla Difesa di Usa, Gran Bretagna e Israele. La campagna, perpetrata attraverso falsi social media, ha colpito oltre 2.000 soggetti.

Giugno 2014

Numerosi siti web correlati ai recenti mondiali di calcio in Brasile, vengono offuscati da hactivist con tecniche di DDoS nell'ambito dell'operazione denominata #O*pWorldcup*. Altri siti, del governo brasiliano e di sponsor dell'evento, subiscono massivi furti di dati.





Luglio 2014

Un pirata informatico accede al sito della Banca Centrale Europea a Francoforte ed estrae oltre 20.000 contatti email di partecipanti a eventi e conferenze svoltisi in quella sede. Lo stesso hacker tenta poi un'estorsione, inviando una comunicazione anonima con la quale chiede un riscatto per le informazioni rubate. La Bce sostiene che non è stato sottratto alcun dato sensibile ma invita gli interessati a cambiare password di accesso.

Agosto 2014

Hacker rubano da iCloud (servizio di archiviazione informatica per iPhone e iPad) almeno 200 foto hot di varie celebrità e le pubblicano su un sito internet, da dove altri le diffondono su altri siti e social network. La Apple nega falle nel suo sistema, sostenendo che gli hacker sono riusciti a ottenere le password con tecniche di *phishing* o di *social engineering*.

Settembre 2014

Viene scoperto X*sser m*RAT (mobile Remote Administration Trojan) il primo sofisticato trojan cinese progettato per i dispositivi mobili basati sul sistema operativo iOS (utilizzato negli iPhone, iPad e iPod), forse concepito per identificare i dimostranti di Hong Kong. Il malware si affianca all'analogo *m*RAT sviluppato per prendere il controllo, per fini illeciti, dei dispositivi che utilizzano il sistema operativo Android.

Ottobre 2014

Per la seconda volta in pochi mesi la rete informatica di JP Morgan Chase, la più grande banca statunitense, è violata da hacker. L'attacco consiste nel furto di informazioni (nomi, indirizzi, numeri telefonici e indirizzi email di circa 76 milioni di famiglie e 7 milioni di piccole aziende). La JP Morgan precisa che la breccia non ha riguardato anche dati sensibili, quali il numero dei conti correnti.

## CONTROMISURE APPLICABILI

I provvedimenti che devono essere adottati per fronteggiare le minacce e i cyber attack vanno ricondotti a un insieme di misure di prevenzione, rilevazione, protezione e all'occorrenza di reazione, che coinvolgono diversi componenti dell'architettura del sistema informatico. In termini generali, gli standard di sicurezza da adottare all'interno delle singole organizzazioni devono essere stabiliti in aderenza alle seguenti linee di principio:

Gestione del rischio: da effettuarsi attraverso l'analisi, il monitoraggio, la riduzione e l'accettazione del livello di rischio residuo che si corre connettendosi in rete, prevedendo il ricorso a specifiche procedure dinamiche cui sottoporre i propri sistemi, quali i *penetration test*;

MINIMALITÀ: installando sui sistemi informatici, attraverso interconnessioni sicure, solo i SW, i protocolli, i servizi di rete, le periferiche e i flussi di dati/informazioni strettamente necessari alla loro funzionalità e all'operatività dell'organismo/azienda di appartenenza, ricorrendo a uno stretto e continuo controllo di configurazione, vietando l'accesso a supporti di memoria, provenienti dall'esterno dell'organizzazione, che non siano stati preventivamente validati e registrati;

MINIMI PRIVILEGI: fornendo ai singoli utenti i profili e le autorizzazioni strettamente necessari all'esecuzione dei compiti loro assegnati, stabilendo opportune policy con le quali identificare i soggetti che possono accedere alle reti esterne e quali siti sia possibile visitare (operazioni gestibili dall'amministratore di rete);

AUTOPROTEZIONE DEI NODI: facendo in modo che ogni sistema consideri come *untrusted* gli altri sistemi a cui è connesso, implementando sistematicamente opportune misure di controllo sull'affidabilità dei corrispondenti, sulla tipologia dei flussi scambiati e sui contenuti delle informazioni.

Per fronteggiare la minaccia è necessario adottare, in funzione delle specifiche esigenze e del livello di protezione che si vuol conseguire, i dispositivi e i provvedimenti di seguito illustrati.

**ANTIVIRUS**

Con tale termine s'identificano SW atti a rilevare ed eventualmente eliminare virus informatici e altri malware. La metodologia più utilizzata consiste nel confrontare il file da analizzare con quelli presenti in un archivio in cui sono stati schedati i malware fino a quel momento conosciuti, ovvero la loro signature. Tale metodologia risulta efficace solo aggiornando frequentemente l'antivirus installato. Ovviamente, i malware in grado di attaccare le vulnerabilità zero-day di un sistema non faranno parte di tale archivio e, pertanto, nessun antivirus potrà mai assicurare l'assoluta inviolabilità del sistema.

**FIREWALL (FW)**

Dispositivi HW o SW di difesa perimetrale, a protezione dei punti d'interconnessione tra due differenti reti. La funzione principale è di agire come filtri che controllano il traffico proveniente dall'esterno e che viene generato dall'interno, in modo da consentire l'accettazione o il blocco dei pacchetti-dati in transito, in conformità a un definito set di regole. Tale controllo, che viene effettuato sugli elementi distintivi dei pacchetti, può essere esteso nel caso di dispositivi sofisticati anche all'esame dei contenuti dei pacchetti in transito. I FW costituiscono la prima linea di difesa di un computer collegato a internet o di una rete informatica, ma possono essere resi inefficaci a opera di malware che utilizzano tecniche evasive o di IP *spoofing* o facendo uso di *vulnerability scanner*. Gli hacker comunemente utilizzano i cosiddetti *Port Scanner* da remoto, i quali vanno alla ricerca, su computer target, di 'porte' che risultano essere 'aperte' e quindi accessibili, riuscendo talvolta a identificare il programma in uso su quella porta o il servizio cui questa è destinato.





**IDS**

Intrusion Detection System. Strumento per individuare tentativi d'attacco alla rete o, più in generale, alterazioni delle configurazioni dei sistemi in rete. Il sistema può essere costituito da SW o da *appliance* basate su HW proprietario. L'Ids opera in modo trasparente nella rete in cui viene implementato, in quanto processa il traffico limitandosi a dare l'allarme in caso di ingresso di file che non rispettano le regole e i criteri di sicurezza impostati.

**IPS**

Intrusion Prevention System. Rappresenta l'evoluzione degli Ids nel campo della sicurezza nelle reti, basato su un approccio proattivo. L'Ips dispone di modalità che consentono di intervenire processando il traffico e bloccando le connessioni che non rispettano le regole e i criteri di sicurezza impostati.

**NAC**

Network Access Control. Permette di definire e gestire, in maniera centralizzata, i criteri di sicurezza applicati per consentire gli accessi a una rete. Il Nac verifica sia la legittimità della richiesta di connessione dell'utente sia la conformità del sistema operativo e dei sistemi di protezione del richiedente alle policy di sicurezza adottate. Attraverso i Nac è possibile effettuare servizi di *remediation* (*distribuzione e installazione degli aggiornamenti* SW *nonché delle patch rilasciate dai produttori per risolvere criticità note di sicurezza*) nonché consentire operazioni di verifica degli accessi e analisi delle attività degli utenti.

**NAP**

Network Access Protection. È un insieme di componenti SW dei sistemi Windows che forniscono una piattaforma in grado di garantire la conformità delle postazioni *client* ai requisiti di sicurezza definiti da un'organizzazione.

**SISTEMI URL FILTERING**

Strumenti che analizzano il grado di pericolosità degli URL (*Uniform Resource Locator*: insieme di caratteri e simboli che indicano l'indirizzo univoco di un 'oggetto' in rete) e delle corrispondenti pagine web che s'intendono visitare, negandone l'accesso agli utenti qualora venissero ritenuti potenzialmente dannosi sulla base di una predeterminata black list. Tuttavia, i cyber criminali potrebbero aggirare le black list statiche adottando nomi di domini e indirizzi dinamici, apparentemente generati casualmente e *single use*, con scarse probabilità di essere identificati e registrati come malevoli.

**SISTEMI CONTENT FILTERING**

Strumenti che analizzano il grado di pericolosità dei contenuti dei file scaricati da internet, o degli allegati di posta elettronica, ricorrendo alla loro eliminazione quando ritenuti potenzialmente dannosi.

**NGFW**

New Generation Firewall. Difesa più innovativa e performante per la lotta contro i malware poiché integrano, in un'unica piattaforma HW e SW, i dispositivi per il controllo delle applicazioni e per la prevenzione dalle intrusioni (Ips) e dalle Ad-

vanced Evasion Techniques (Aet), unitamente, a seconda delle soluzioni impiegate, all'adozione di Virtual Private Network (Vpn) e tecniche di crittografia, nonché di tecniche avanzate sia per il controllo del comportamento in rete degli utenti facenti parte di un'organizzazione sia del traffico complessivo in ingresso e uscita, oltre a protezioni anti-malware/anti-spam e filtraggio degli indirizzi.

**TECNICHE STEALTH**

Tecniche per nascondere i nodi di una rete agli aggressori. Il procedimento consiste nel cifrare i dati con chiavi molto robuste, mescolarli bit a bit e sparpagliarli all'interno della rete – con una tecnologia denominata *Information Dispersal Algorithm* – governata da chiavi sicure per cui, per ricostruire il dato originario, è innanzitutto necessario ricostruire le stringhe dei dati nella giusta sequenza, utilizzando una chiave nota solo agli utenti autorizzati.

**SIEM**

Security Information Event Management. Sistema composto di specifici SW e apparati per la raccolta, normalizzazione, correlazione e presentazione di informazioni provenienti da sorgenti eterogenee esterne. La peculiarità dei sistemi Siem risiede nella capacità di effettuare analisi real-time degli allarmi di sicurezza generati dagli apparati HW di rete e dalle applicazioni SW di gestione e monitoraggio e, quindi, di contrarre i tempi di risoluzione degli incidenti.

**STRM**

Security Threat Response Manager. Tipologia di Siem deputata alla gestione centralizzata degli eventi e del contesto potenzialmente presente in un'architettura di rete complessa (*Situational Awareness*) per l'identificazione di attività anomale e di eventuali incidenti informatici.

**DATA LOSS PREVENTION**

Accorgimenti di tipo SW che impediscono la fuoriuscita, da parte di dispositivi informatici connessi in rete, di specifiche tipologie di dati (carte di credito, codici fiscali ecc.), in quanto eseguono le funzioni di controllo entrando nel merito dei contenuti.

**HONEYPOT**

Sistema volontariamente destinato a subire attacchi informatici da parte di soggetti ostili, per raccogliere e studiare il codice malware e ottenere informazioni utili a fronteggiare le azioni poste in essere dai medesimi soggetti, per mezzo della loro analisi.

**EPS**

Evasion Prevention System. Strumento realizzato per la protezione dalla minaccia cibernetica derivante dalle Aet, che consente di analizzare e rilevare le minacce e di attuare contromisure 'multilivello' nell'intero percorso protocollare.

**NEXT GENERATION MALWARE DETECTION**

Nuovi dispositivi in grado di identificare i malware sulla base di analisi semantiche e dei contenuti.





**HARDWARE/ SOFTWARE**

È indispensabile avere la certezza del marchio di fabbrica e della provenienza di HW e SW, in modo da assicurare la maggior sicurezza contro le minacce derivanti dalla navigazione. È bene acquistare il materiale informatico esclusivamente presso rivenditori certificati (verificando la presenza di serial number sul materiale HW) e acquistando il SW originale provvisto delle relative licenze.

**DIGITAL FORENSIC**

Dispositivi di analisi forense, ausilio alle attività di analisi, contenimento e risposta agli incidenti informatici.

**SISTEMI DI CIFRATURA DATI**

Da utilizzare sulle linee di trasmissione in modo da garantire la confidenzialità dei contenuti informativi e, possibilmente, con gestione delle chiavi basata sul *Key Management Infrastructure* che consente la loro distribuzione e il loro caricamento da remoto, direttamente sugli apparati dell'utente, evitando le criticità connesse all'impiego di corrieri e a possibili manipolazioni da parte di personale interno o esterno all'organizzazione.

**PKI**

Public Key Infrastructure. Per le funzioni di firma digitale, garantisce anche l'autenticazione tra corrispondenti e il non ripudio delle comunicazioni inoltrate.

**MAC**

Mandatory Access Control. Consente l'accesso alle reti secondo una politica di verifica dei profili d'utente.

**SAND BOX**

Ambiente di prova, separato dai programmi in sviluppo o in esecuzione, dove eseguire test la cui affidabilità non è stata ancora accertata, alla ricerca automatizzata di possibili malware. Nel 2011 sono stati scoperti malware capaci d'ingannare tali dispositivi, in quanto sono in grado di riconoscere l'attività di analisi svolta (ad esempio, dall'assenza di movimento del mouse e dall'analisi dei segnali video), per cui non si attivano durante tale fase, facendo così credere che il file interessato sia 'pulito'. Altri malware attendono alcuni minuti prima di attivarsi, in quanto l'analisi svolta dalla Sand Box richiede, in genere, solo pochi secondi, così comportandosi come delle 'bombe a tempo'.

**BOC**

Back Up On Cloud. Servizio che consente di effettuare copie dei dati sui server farm remoti costituenti i Cloud, avendo preventivamente fissato sia la frequenza con la quale effettuare i salvataggi sia i file su cui effettuare il back up, se del caso ricorrendo alla loro preventiva cifratura, in modo da garantire l'accesso ai contenuti solo al personale autorizzato.

**PROCESSI PROBABILISTICI**

Approccio innovativo basato sugli aspetti comportamentali dell'utilizzatore all'interno di un'organizzazione che, in termini probabilistici, possono definirsi 'anomali'. Tale procedura è tesa a contrastare le minacce provenienti dai cosid-

detti insider che involontariamente (in quanto vittime di *phishing*) o deliberatamente sono portati a svolgere attività malevole. I processi probabilistici sono caratterizzati da modelli matematici che parametrizzano i comportamenti 'normali' di tutti gli utilizzatori della rete all'interno di un'organizzazione, con capacità di auto-apprendimento e adattamento alla mutevolezza degli scenari, e si basano sulle osservazioni del traffico in ingresso e in uscita delle singole postazioni.

## BEST PRACTICE

Per la difesa dei sistemi informatici è indispensabile che anche da parte degli utenti vengano adottati elementari precauzioni (frequente back up in loco dei dati su hard disk non connessi in rete o su chiavette Usb registrate e di certa provenienza o su cd). Particolare attenzione deve essere posta nell'utilizzo delle password adottando, in particolare, i seguenti accorgimenti:

- utilizzare password alfanumeriche per accedere al sistema, composte da almeno 8 caratteri, tra i quali almeno un numero e un carattere speciale (§, %, ', *, # ecc.);
- evitare di utilizzare, ad esempio, il nome proprio, quello dei familiari e dei propri animali domestici, il numero di targhe di auto proprie e di telefono, date di nascita, nomi di luoghi o di cose preferite o detestate, solo caratteri maiuscoli o minuscoli, il carattere maiuscolo solo all'inizio o alla fine della password, solo caratteri alfabetici o numerici, stringhe di caratteri troppo facili da ricordare ('aaaaa', '123456', 'password' ecc.);
- utilizzare alternanze non ovvie di lettere maiuscole e minuscole, parole con interposizioni di numeri e caratteri speciali (ad es., dIVa5&No), interallacciamenti tra due o più parole (*panino* e *frutta* = pFArnUitNtoa) o tra una parola (*panino*) e numeri (p5A3n9I4n3o), concatenamenti tra due o più parole (vIOlIno^pIAnO), voluti errori ortografici (aSsyKUraZZioNe), acronimi di parole costituenti frasi di senso compiuto (imVsScLdeigDf = *i musei vaticani sono sempre chiusi la domenica e i giorni di festa*), facili da ricordare ma difficili da individuare oltre, ovviamente, alle più disparate combinazioni delle citate metodologie;
- cambiare spesso le password, evitando di derivare le nuove dalle precedenti, e custodirle in luogo sicuro.

È indispensabile che coloro che navigano in internet siano consapevoli dei rischi.
Da un'indagine svolta dall'Ibm, relativa al 2013, è emerso che, per quanto concerne le principali categorie di siti web che contengono *malicious link*:

- l'area più rischiosa è quella dei siti pornografici, dove sono stati rilevati quasi il 23% di tutti i link malevoli scoperti in rete;
- la seconda area, con il 16,5%, è risultata essere quella dei siti dinamici, quali i blog;
- al terzo posto, con l'8%, l'area dei siti web di tipo convenzionale;
- al quarto posto, con il 7,9%, l'area dei giochi (*gambling*) e delle lotterie;
- al quinto posto, con il 5,7%, l'area delle home page personali e i siti che forniscono servizi di comunicazione;
- il restante 39,2% dei link malevoli sono distribuiti sulle rimanenti aree tematiche.





Un ruolo determinante per la prevenzione e la risposta a emergenze informatiche è svolto dai *Computer Emergency Response Team* (Cert) ovvero 'squadre' di specialisti negli ambiti di amministrazione di rete e di sistema e sicurezza informatica, finanziate per lo più da enti governativi, università e organizzazioni varie cui vengono attribuiti, principalmente, compiti di:

- raccogliere le segnalazioni di incidenti informatici e informazioni sulle potenziali vulnerabilità degli HW e SW utilizzati;
- fornire assistenza tecnica agli utenti del comparto di competenza, sia in forma diretta (con piani immediati di *incident response*, in caso di segnalazioni di attacco in corso) sia in forma indiretta (ad esempio, tramite la diffusione di informazioni inerenti ai dispositivi di sicurezza e alle più adeguate contromisure nei confronti delle tipologie di incidente già note e maggiormente diffuse);
- svolgere costante attività di ricerca e sviluppo consistente nel monitorare l'evoluzione tecnologica dei nuovi sistemi informatici, dei relativi programmi operativi e della rete, in modo da valutarne lo stato di sicurezza e il livello di vulnerabilità;
- organizzare corsi di formazione ad amministratori di rete e di sistema e agli operatori/tecnici informatici, in modo da istruirli sulle cyber threat e sulle tecniche di autoprotezione.

Nel mondo esistono numerosi Cert (oltre 140 nella sola Europa), 8 dei quali sono stati costituiti in Italia, pur se alla data in cui si scrive solo 2 risultano essere operanti, mentre è atteso l'avvio sperimentale di quello Nazionale.

## SOCIAL NETWORK

Le piattaforme Social Network (o Social Media) costituiscono una componente rilevante del *Web* 2.0[4] e si sono guadagnate un vastissimo consenso da parte degli utilizzatori di internet in quanto rendono possibile la creazione di reti sociali virtuali che semplificano la nascita e il mantenimento di legami tra persone con interessi affini o di una stessa comunità tematica (studenti, tifoserie, professionisti ecc.) o con le competenze necessarie per risolvere un determinato problema, in modo da poter condividere on line informazioni e opinioni.
Da una recente indagine è emerso che, su scala mondiale, più di due terzi degli utilizzatori della rete visita frequentemente un Social Network e che il 10% del tempo trascorso da un utente medio navigando in internet è speso interagendo in siti di questo genere. Negli ultimi anni hanno anche assunto un rilevante ruolo in paesi soggetti a forme di governo dittatoriali o comunque poco propensi a garantire le libertà individuali.

4. Il web 2.0 rappresenta l'insieme delle applicazioni on line che permettono un significativo livello di interazione sito-utente. Tale accezione evidenzia le differenze rispetto al c.d. web 1.0, composto prevalentemente da siti statici, privi della possibilità di interazione con l'utente, a esclusione della normale navigazione tra le pagine in *hyperlink*.

I Social Network possono costituire una rilevante fonte di informazioni, per finalità lecite o non lecite, potendo da questi rilevare, ad esempio, gli stati d'animo degli utilizzatori, la loro fiducia nelle istituzioni, la presenza di disagi di ordine sociale, la costituzione di movimenti ecc. All'interno di questi ultimi è possibile identificare, attraverso l'esame dei grafi[5], i vari soggetti e i loro ruoli, nonché la dinamica di propagazione di una notizia inserita in rete, i legami di amicizia e inimicizia, le concordanze e le discordanze ecc.

Una volta nota la rete dei collegamenti tra utenti affini e le dinamiche di comunicazione, le informazioni acquisite possono essere utilizzate per operazioni di propaganda, disinformazione o *astroturfing* (consensi artificialmente prodotti) mirati, ad esempio, verso leader politici o a prodotti/esercizi commerciali.

Controllare e modificare l'opinione degli utenti affiliati a un Social Network è un pericolo sempre in agguato. Difatti, tramite tecniche di *social engineering* entità ostili possono penetrare a fondo nel sistema sociale di uno stato fino a minarne, al limite, la stabilità.

Inoltre, le emergenti tecnologie *stealth* delle *Socialbot*[6] comportano il rischio che questi possano essere in grado di assumere posizioni di leadership all'interno di un Social Network, operando un freddo e razionale pre-programmato piano di disinformazione e plagio, con conseguenze immaginabili.

Una prima contromisura consiste nello sviluppo di un adeguato spirito critico da parte dei frequentatori delle reti, in modo da essere estremamente prudenti nel dare credito a false informazioni che vengono ivi immesse.

Dal punto di vista della Cyber Threat, i Social Network possono rappresentare un veicolo attraente per perpetrare attacchi cibernetici. Nel biennio 2013-2014 tali rischi sono stati amplificati dal ruolo crescente dei social media quale strumento essenziale per gli hacker nella pianificazione ed esecuzione di attacchi mirati. Dopo aver preso di mira un'organizzazione e averne identificato gli individui che al suo interno hanno accesso ai dati desiderati, i cyber criminali procedono alla creazione di un profilo dei soggetti monitorati sulla base delle informazioni personali che gli stessi postano sui social media (sport praticato, preferenze culinarie, cantante preferito, conoscenti e amici con cui scambiano messaggi ecc.). Forti di questi elementi, i criminali possono creare mail di *spear-phishing* (ad esempio, facendosi passare per persone note alle vittime) invitando i target ad aprire allegati che, invece dei contenuti promessi, contengono malware con i quali prendere il controllo del PC vittima e, all'occorrenza, esfiltrarne i dati voluti o utilizzarlo come zombie in una botnet.

5. Per l'analisi e la rappresentazione di una rete si fa ricorso ai grafi, ovvero rappresentazioni grafiche costituite da vertici o nodi che rappresentano gli attori, collegati tra loro da archi (o lati) che indicano gli scambi di informazioni tra loro.
6. *Socialbot*, entità virtuali in grado di essere scambiate per esseri umani.