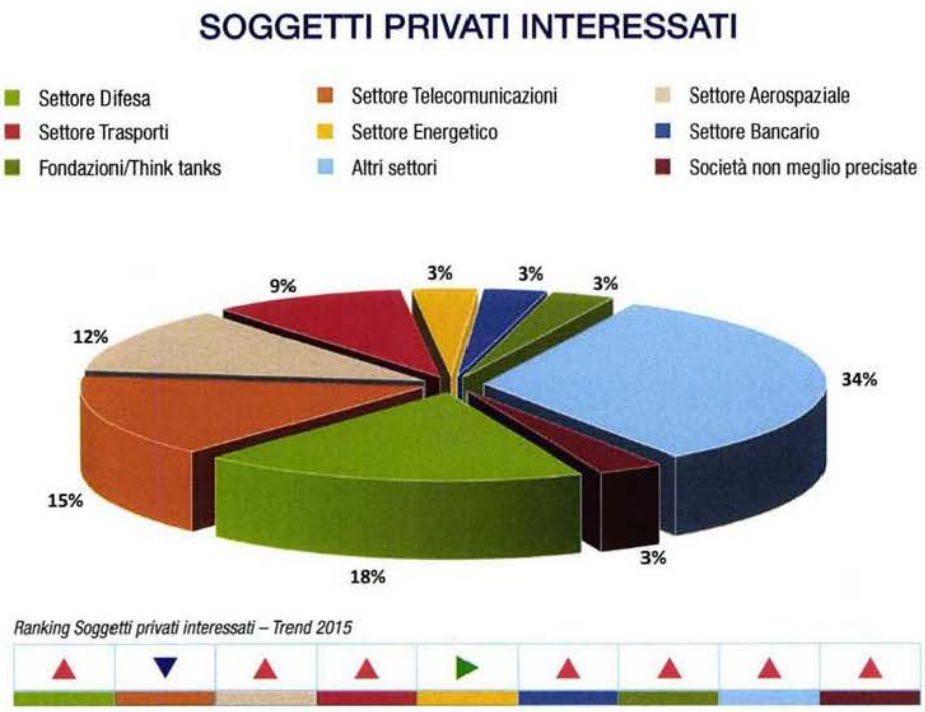

Grafico 4 – Tipologia dei soggetti privati interessati dagli attacchi

Sul fronte dei ***target* privati** (***Grafico 4***), gli obiettivi privilegiati per attacchi di spionaggio digitale sono quelli operanti nei settori della difesa (18%), delle telecomunicazioni (15%), dell'aerospazio (12%) e dell'energia, inclusa quella proveniente da fonti rinnovabili (3%). I restanti soggetti sono stati interessati da azioni di tipo *hacktivist*. Significativo, altresì, il 3% registrato nei confronti del settore bancario, verso cui sono stati impiegati i cd. *banking trojan*.

Sotto la voce "altri settori" (34%) sono state, poi, indicate tutte quelle realtà imprenditoriali – per lo più appartenenti alla categoria delle piccole e medie imprese – afferenti a molteplici classi merceologiche, i cui eventi cibernetici assumono rilevanza statistica solo se analizzati in formato aggregato. La voce "società non meglio precisate" (3%), infine, fa riferimento a quelle attività ostili condotte su larga scala contro le risorse esposte su internet di una moltitudine indiscriminata di *target*.

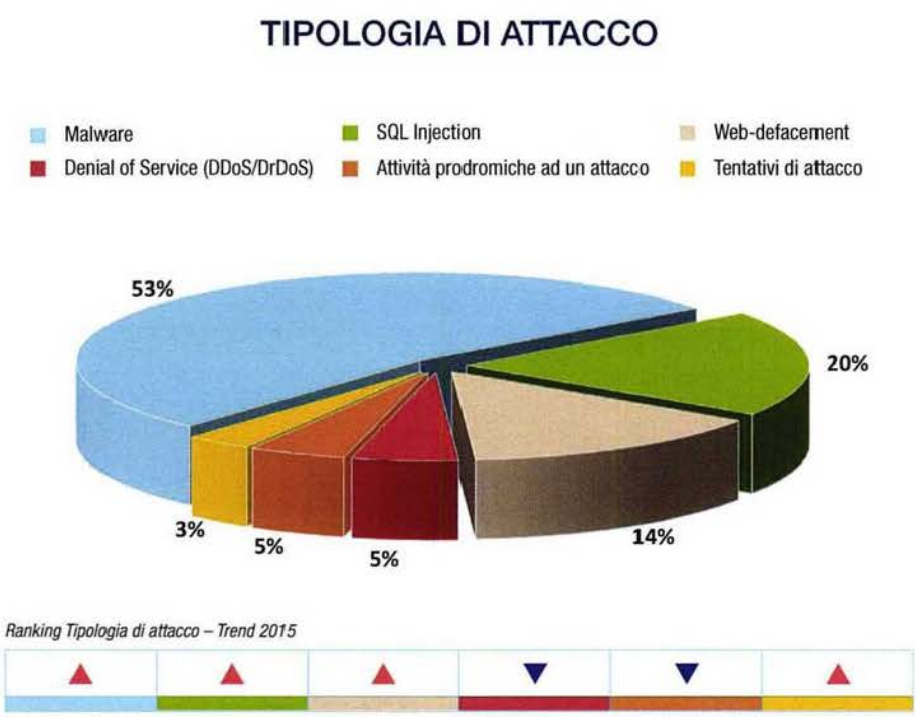

Grafico 5 – Tipologia di attacco impiegata

Con riguardo, infine, alle **tipologie di attacco** (***Grafico 5***), il 53% è costituito da *software* malevolo (*malware*), specie nella forma dell'*Advanced Persistent Threat* (APT), impiegato, come più sopra indicato, non solo per finalità di *cyber*-spionaggio, ma anche nell'ambito di logiche estorsive e di altre attività illecite di natura predatoria. Da rilevare, inoltre, il crescente ricorso a tale strumento da parte anche dei movimenti hacktivisti – oltre alla tecnica *SQL Injection* (20%) – per esfiltrare dati da riversare poi su internet. Altra modalità largamente utilizzata in tale ambito è quella del defacciamento di siti *web* (14%), mentre in calo risultano i *Distributed Denial of Service* (5%).

Valenza residuale hanno assunto le attività prodromiche ad un attacco (5%) quali, ad esempio, quelle di scansione delle vulnerabilità, di mappatura della rete del *target* e di *fingerprinting* dei sistemi, ed i tentativi di attacco (3%).

Trend evolutivi della minaccia cibernetica

Sulla base di quanto rappresentato, le evoluzioni della minaccia *cyber*, in un'ottica di breve-medio termine, continueranno a risentire, in particolare:

- delle vulnerabilità riconducibili al fattore umano, non solo per i profili collegabili alla figura dell'*insider*, ma anche per i *pattern* comportamentali *on-line*, sempre più profilabili attraverso l'impiego di tecniche avanzate di *social engineering*;
- dello sviluppo e della sempre maggiore diffusione di piattaforme per l'effettuazione di transazioni tramite dispositivi *mobile*;
- del continuo incremento della superficie di attacco, anche a seguito di politiche di riduzione del *digital divide*, della maggiore capillarità delle infrastrutture di comunicazione nelle Nazioni in via di sviluppo, nonché della crescente diffusione di dispositivi mobili e di domotica *smart* (*Internet of Things*);
- del potenziamento della digitalizzazione dei documenti e dei processi da parte sia della Pubblica Amministrazione che di società private, in grado di aumentare l'impatto di azioni ostili nel cyberspazio;

- della crescente capacità di offuscamento dei *malware*, idonei ad occultarsi nei livelli più profondi dei sistemi (*Basic Input Output System* e *firmware* di altre componenti dei sistemi informatici, *vds. tavola n. 2*) e delle reti *target*;
- dei *ransomware*, che vedranno evolvere i propri metodi di propagazione, di cifratura e di impiego più mirato;
- del potenziamento dei sistemi di comunicazione delle *botnet*, di cui esempio emblematico è l'utilizzo di connessioni satellitari per ridurre drasticamente la capacità di geo-localizzazione e la riconducibilità dei sistemi di comando e controllo utilizzati.

Appendice

Le parole del *cyber*

Basic Input Output System **(BIOS)**. Programma che risiede sul *chip* della scheda madre e che gestisce l'avvio del sistema operativo. Questo è altresì deputato a verificare che tutte le componenti *hardware* funzionino correttamente.

Distributed Denial of Service **(DDoS)**. Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (*botnet*), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi *server*.

Firmware. Programma integrato in un componente elettronico e che ha la funzione di assicurarne l'avvio e l'interazione con altre componenti *hardware*.

Hacktivist. Termine che deriva dall'unione di due parole, *hacking* e *activism* e indica le pratiche dell'azione diretta digitale in stile *hacker*. Nell'ambito dell'*hacktivism* le forme dell'azione diretta tradizionale sono trasformate nei loro equivalenti elettronici, che si estrinsecano prevalentemente, ma non solo, in attacchi DDoS e *web defacement*.

Hashtag. Nell'ambito dei *social network*, identifica la parola o la frase preceduta dal simbolo cancelletto (#), che consente di indicizzare e classificare i messaggi con una parola chiave, rendendo gli stessi reperibili agli utenti interessati alla tematica.

Internet of Things (IoT). Neologismo riferito all'interconnessione degli oggetti tramite la rete internet, i quali possono così comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri, offrendo un nuovo livello di interazione. I campi di applicabilità sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, fino all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

Malware. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. I *software* malevoli sono divenuti, nel tempo, sempre più sofisticati. Non solo sono adattabili a qualsiasi tipologia di obiettivo, ma sono anche in grado di sfruttare vulnerabilità non ancora note (cd. *0-day*) per infettare le risorse informatiche dei *target*. Ciò consente a tali *software* di non essere rilevati dai sistemi antivirus e di passare praticamente inosservati. Essi, inoltre, sono in grado di celarsi nell'ambito del sistema-obiettivo, di spostarsi al suo interno, così da poterne effettuare una mappatura e propagare l'infezione. Infine, grazie agli stessi, le informazioni di interesse, prima di essere sottratte, vengono compresse e criptate per celarne l'esfiltrazione con il traffico di rete generato dall'ordinaria attività lavorativa del *target*.

Malware reverse engineering. Esame del funzionamento e del comportamento di un *malware* condotta tramite analisi statica o dinamica, al fine di comprendere quali sono le istruzioni eseguite, le finalità del *software* malevolo ed il suo possibile autore.

Ransomware. *Malware* che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I *ransomware* sono, nella maggioranza dei casi, dei *trojan* diffusi tramite siti *web* malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Social engineering. Tecnica di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici.

Spyware. *Malware* usato per raccogliere e trasmettere informazioni da remoto. Le informazioni carpite possono riguardare, a titolo di esempio, abitudini di navigazione in rete, *password* e chiavi crittografiche.

SQL Injection. Tecnica mirata a colpire applicazioni *web* che si appoggiano su *database* programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in *input* e l'inserimento di codice malevolo all'interno delle *query*. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

Trojan. *Malware* che impiega l'ingegneria sociale, presentandosi come un *file* legittimo (ad esempio con estensione .doc o .pdf), facendo credere alla vittima che si tratti di un file innocuo, ma che in realtà cela un programma che consente l'accesso non autorizzato al sistema da parte dell'attaccante. Il *trojan* può avere diverse funzioni: dal furto di dati sensibili al danneggiamento del sistema target. Particolare categoria sono i cd. ***Banking Trojan***, programmati per acquisire le credenziali di accesso degli *account* dei siti di banca *on-line* al fine di effettuare illeciti trasferimenti di fondi verso conti bancari controllati da gruppi di cyber criminali.

Web defacement. Attacco condotto contro un sito *web* e consistente nel modificare i contenuti dello stesso limitatamente alla *home page* ovvero includendo anche le sottopagine del sito.