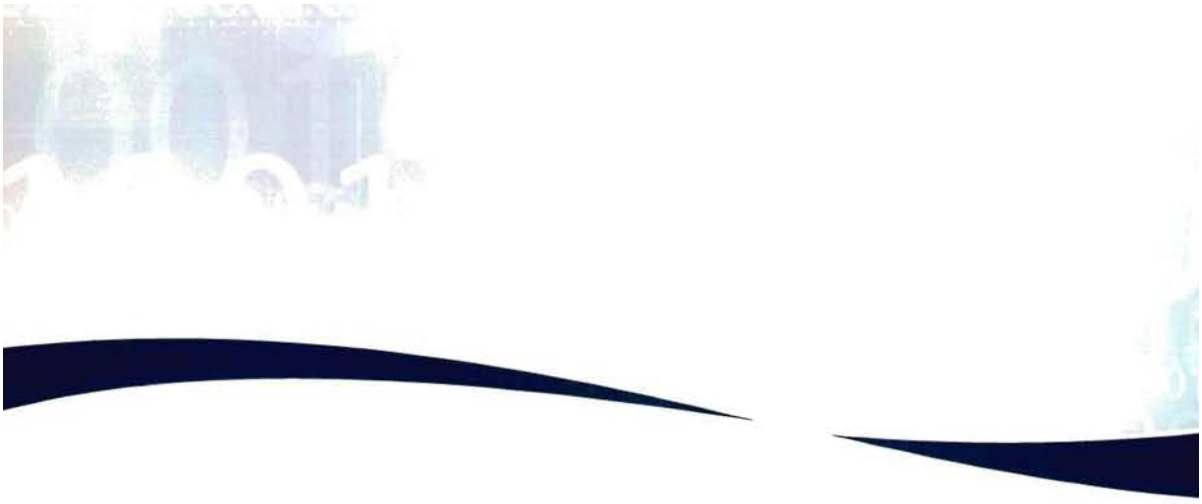

Stato della minaccia cibernetica in Italia e possibili evoluzioni

UNO SGUARDO AL CONTESTO INTERNAZIONALE

Gli attacchi *cyber* verificatisi nel corso del 2016 hanno innovato significativamente il panorama della minaccia, segnando un ulteriore cambio di passo sotto molteplici profili: dal rango dei *target* colpiti, alla sensibilità rivestita dagli stessi nei rispettivi contesti di riferimento; dal forte impatto conseguito, alle gravi vulnerabilità sfruttate sino alla sempre più elevata sofisticazione delle capacità degli attaccanti.

Il riferimento è, in ordine di tempo, agli eventi che hanno interessato, secondo quanto riportato dalle più accreditate fonti aperte internazionali, le istituzioni bancarie di diversi Paesi (Bangladesh, Ecuador, Vietnam e

> AZIONI DI *CYBER* SABOTAGGIO IN DANNO DI INFRASTRUTTURE CRITICHE: UN CASO-STUDIO
>
> Nel dicembre 2015 si è verificata una serie di attacchi cyber condotti contro i sistemi di controllo industriale di tre compagnie di distribuzione elettrica dell'Ucraina (Oblenergo), che hanno causato un *blackout*, protrattosi per diverse ore. Nell'attacco è stato impiegato il *malware BlackEnergy*, rinvenuto nel gennaio 2016, come ampiamente riportato da fonti aperte, anche nelle reti informatiche dell'aeroporto Kiev-Boryspil, della compagnia di bandiera Ukraine International Airlines, di una società di trasporto ferroviario e di una compagnia mineraria ucraine.
>
> Un nuovo *blackout* si è recentemente verificato nel dicembre 2016, interessando sempre l'Ucraina e, in particolare, la capitale Kiev.

Ucraina), provocando trasferimenti illeciti di grandi somme di denaro a causa della penetrazione dei sistemi per la gestione delle transazioni interbancarie ovvero della compromissione dei dispositivi ATM (è il caso di Taiwan). Il dato più preoccupante di tali attacchi è stato ricondotto, dai citati media, all'inedito collegamento tra ambienti *cyber* criminali, sodalizi dediti al riciclaggio ed *insider* nei circuiti finanziari (inclusi i *money transfer*). Alla citata casistica sono stati, poi, aggiunti gli eventi di sabotaggio dei sistemi di controllo industriale impiegati nell'ambito di infrastrutture critiche e quelli ricondotti ad attori supportati da entità statuali, che hanno comportato la sottrazione di informazioni rilevanti sotto il profilo strategico o coperte da proprietà intellettuale, ovvero utili, se opportunamente manipolate, per influenzare le dinamiche politiche di Paesi terzi.

AMBITI E ATTORI DELLA MINACCIA

La minaccia nei confronti delle infrastrutture del dominio cibernetico nazionale è stata caratterizzata da un elevato grado di eterogeneità e dinamismo tecnologico. In linea di continuità con il 2015 e con prevedibile estensione per gli anni a venire, anche nel 2016 il monitoraggio dei fenomeni di minaccia collegati con il *cyberspace* ha evidenziato un costante *trend* di crescita in termini di sofisticazione, pervasività e persistenza a fronte di un livello non sempre adeguato di consapevolezza in merito ai rischi e di potenziamento dei presidi di sicurezza.

Una tendenza, questa, cui si è associata anche la persistente vulnerabilità di piattaforme *web* istituzionali e private, erogatrici in qualche caso di servizi essenziali e/o strategici, che incidono sulla sicurezza nazionale, e la presenza di un sostanziale sbilanciamento del rischio, generalmente contenuto, in capo agli attori della minaccia rispetto a quello dei *target*, derivante dalle perduranti difficoltà di *detection, response* ed *attribution* di un evento.

La crescente dipendenza dei processi produttivi e delle forniture di servizi dal dominio digitale, unitamente alle vulnerabilità che affliggono le *supply chain* degli operatori, siano essi imprese, organizzazioni

ed individui, hanno nel tempo determinato una progressiva estensione della superficie di esposizione alla minaccia.

In tale contesto, il connubio tra un livello di rischio contenuto ed un'elevata redditività dei patrimoni digitali *target* ha contribuito a rafforzare le dinamiche di un insieme di attori operanti nel dominio *cyber*, sempre più collegati, tra l'altro, con filiere e sodalizi criminali tradizionali.

Giova inoltre evidenziare come gli incentivi all'innovazione tecnologica delle istituzioni civili e militari hanno costituito un ambito particolarmente appetibile, catalizzando gli interessi di attori privati, anche stranieri, presenti sul territorio nazionale che hanno cercato di accreditarsi, fra l'altro, attraverso condotte poco ortodosse.

Tenuto conto di quanto sopra, l'azione di tutela e prevenzione si è focalizzata sulla raccolta di informazioni utili alla profilazione degli attori ostili in termini di interessi, obiettivi, capacità e modalità di attacco, al fine di ottimizzare la difesa degli Enti della Pubblica Amministrazione, delle infrastrutture critiche, governative e non, degli operatori privati strategicamente rilevanti e, più in generale, delle reti telematiche nazionali esposte a tali minacce.

Attenzione è stata posta all'individuazione e al monitoraggio delle tecnologie caratterizzanti il dominio cibernetico (*social network*, motori di ricerca, piattaforme di *e-commerce*, *dark net* e sistemi di anonimizzazione) e del panorama tecnologico nazionale e internazionale, che hanno evidenziato un crescente sviluppo di armi digitali e di tecnologie potenzialmente ostili, parte delle quali hanno costituito oggetto di analisi e di *reverse engineering* presso il Polo Tecnologico di Comparto, che opera quale centro di eccellenza nazionale in materia.

Per quel che concerne lo stato della minaccia cibernetica, si è continuato a rilevare una diversificazione dei *target*, delle modalità attuative e delle finalità degli attacchi in base alla matrice della minaccia: da quelle più rilevanti per gli *asset* critici e strategici connesse al *cybercrime*, al *cyber-espionage* ed alla *cyberwarfare*, a quella terroristica ed hacktivista, più stabili nella condotta e negli obiettivi. La minaccia terroristica nell'ambiente digitale permane caratterizzata dalle finalità di proselitismo, re-

clutamento e finanziamento, mentre le attività ostili in danno di infrastrutture IT sono consistite principalmente in attività di *Web-defacement.*

Per quanto riguarda il *cyber-espionage,* è stato pressoché costante l'andamento dei "*data breach*" in danno di Istituzioni pubbliche ed imprese private, incluse le PMI, con finalità di acquisizione di *know-how* ed informazioni di *business* e/o strategiche, anche attraverso manovre di carattere persistente (*Advanced Persistent Threat – APT, vds. Glossario*). Tali manovre sono apparse riconducibili, in via diretta o indiretta, a matrici di natura statuale, rilevandosi in alcuni casi una sovrapposizione, ai danni del medesimo *target,* di campagne promosse da vari attori che, seppure in modo indipendente, hanno sfruttato con tecniche diverse le vulnerabilità dei sistemi informatici attinti.

Il quadro delineato dall'analisi dei dati sulle campagne digitali condotte contro le infrastrutture strategiche nazionali ha evidenziato la presenza di elementi ricorrenti in termini di origine delle minacce e di infrastrutture informatiche utilizzate per sferrare gli attacchi digitali.

Con riguardo a queste ultime, è stato rilevato il ricorso sempre più strutturato a *server* rinvenibili nel mercato nero digitale come ordinari prodotti di *e-commerce,* previamente compromessi dall'offerente mediante *trojan* (*vds. Glossario*) così da garantire all'attaccante l'accesso ad un prodotto utilizzabile per la conduzione di attacchi, preservando l'anonimato. Si tratta, questo, di un fenomeno che, fondato sul paradigma *"APT as a Service"*, ha visto il crescente coinvolgimento di gruppi criminali organizzati, specializzatisi nella conduzione di sofisticate attività delinquenziali con finalità estorsive, attuate perlopiù attraverso campagne *ransomware.*

È stata confermata, inoltre, la progressiva saldatura tra le finalità economiche della *cyber*-criminalità con quelle di comuni *player* di mercato, interessati, questi ultimi, a compromettere la competitività dei rispettivi concorrenti. Tale obiettivo è stato sempre più conseguito mediante la realizzazione di un rilevante danno reputazionale in capo al *target,* specie nel caso di organizzazioni per le quali tale aspetto

è correlato alla capacità di garantire la sicurezza, anche informatica, della struttura e dei dati da essa custoditi. È il caso, ad esempio, delle banche, degli istituti finanziari, dei gestori di piattaforme *cloud*, degli operatori nei settori *e-commerce* ed *e-business*, nonché delle infrastrutture critiche nazionali, la cui *supply chain* è tipicamente soggetta a minori presidi difensivi.

La compromissione delle risorse telematiche si è configurata come un'attività strutturata dell'attore ostile finalizzata, sul **piano strategico**, alla raccolta di informazioni tese a comprendere il posizionamento del Paese *target* su eventi geo-politici di interesse per l'attore statuale ostile (laddove obiettivo dell'attacco *cyber* sia un soggetto pubblico), ovvero ad acquisire informazioni industriali, commerciali o relative al *know-how* (qualora si tratti, invece, di un obiettivo privato). Sul **piano tattico**, l'attaccante è parso interessato a minare la reputazione ed il vantaggio commerciale, sul mercato, dei *target* privati ed a profilare il personale dei *target* pubblici, di cui sono state studiate anche le abitudini digitali alla ricerca di eventuali punti di debolezza sistemica, da sfruttare in vista di un possibile reclutamento convenzionale. In relazione al *modus operandi* impiegato dall'attaccante per il conseguimento dei citati obiettivi, si sono registrati, quali elementi di novità, il ricorso a parole-chiave in lingua italiana per ricercare documenti di interesse da esfiltrare, ad ulteriore conferma dell'elevato grado di profilazione delle attività ostili sui *target* nazionali, e la ricerca di singoli individui ritenuti di particolare interesse in ragione dell'attività professionale svolta, ovvero sulla base dell'incarico e della sede di servizio ricoperti, nonché delle informazioni cui hanno accesso.

Sul fronte del *cyber* terrorismo, si è continuato a rilevare sui *social network*, da parte di gruppi estremisti, attività di comunicazione, proselitismo, radicalizzazione, addestramento, finanziamento e rivendicazione delle azioni ostili. La rete consente infatti di raggiungere sia potenziali nuove reclute presenti nelle sacche di emarginazione sociale, sia esponenti degli ambienti ideologicamente distanti dalle rappresentanze moderate. Sul piano delle capacità *cyber* ostili, è risultato particolarmente

attivo il *Tunisian Fallaga Team* – operativo dal 2013 e noto anche come "*Hacker del Califfato*" – che, sebbene nel 2015 abbia subìto un duro colpo ad opera delle Forze di sicurezza tunisine, negli ultimi mesi del 2016 ha dato mostra di un rinnovato slancio delle proprie azioni digitali eseguite, di massima, con finalità di *defacement* ai danni di siti *web* di enti, aziende e privati cittadini. L'azione digitale di tale gruppo si è caratterizzata, al pari di omologhe formazioni, da un basso livello di sofisticazione delle procedure e degli strumenti d'attacco, dall'individuazione randomica dei *target* (perlopiù cd. *soft target*) e dalla numerosità delle attività *cyber* ostili.

Per quel che concerne le campagne di attivismo digitale, riconducibili soprattutto alla comunità *Anonymous Italia*, esse hanno fatto registrare una generale diminuzione del livello tecnologico delle azioni offensive. Flessione, questa, ascrivibile alla riorganizzazione interna del gruppo successiva allo scompaginamento dei suoi assetti organizzativi posto in essere dalle Forze di polizia. Al di là di ciò, le azioni di *cyber* attivismo hanno continuato a connotarsi per la loro impronta antagonista e antigovernativa – come nella campagna di dissenso alla consultazione referendaria sulla riforma costituzionale – e per la scelta di *target* perlopiù istituzionali, i cui sistemi sono stati oggetto di preliminari operazioni di scansione per la ricerca di vulnerabilità da sfruttare in vista di operazioni di *web defacement* e di esfiltrazione dati. Tale *modus operandi* si è configurato, seppure in minor misura rispetto al passato, come una sorta di "pesca a strascico", nella quale vengono attaccati anche *asset* informatici esposti su internet di obiettivi non direttamente connessi con i motivi della rivendicazione, tra i quali sono emersi quelli di enti locali, sovente affetti da vulnerabilità di agevole sfruttamento.

Elemento di rilievo in tale contesto è stato il riavvicinamento del movimento hacktivista ai temi chiave, non solo della politica italiana, ma anche delle istanze di piazza, come nel caso dell'operazione NoMUOS (*Mobile User Objective System*), oggetto di rilancio contro l'installazione, sul territorio nazionale, di un moderno sistema di telecomunicazione satellitare USA.

SERIE STATISTICHE

Allo scopo di consentire l'immediata ed agevole rilevazione del volume degli eventi *cyber* registrati nel nostro Paese nel corso del 2016, sono state realizzate, anche per questa edizione, le serie statistiche relative agli attacchi, andati a buon fine o tentati, compiuti in danno di obiettivi insistenti sul territorio nazionale, ovvero contro soggetti nazionali, pubblici e privati, presenti con proprie strutture all'estero. L'analisi è stata condotta sulla base degli elementi informativi di AISE ed AISI, degli altri soggetti che compongono l'architettura nazionale e dei Servizi Collegati Esteri.

I valori sono espressi esclusivamente in termini percentuali e non assoluti, così da preservare le inderogabili esigenze di riservatezza circa l'entità numerica delle minacce rilevate.

La serie è corredata, come di consueto, dall'indicazione del *trend*, ricavato dalla comparazione dei dati del 2016 con quelli dell'anno precedente, tracciato, secondo la seguente legenda, in corrispondenza della relativa voce nel grafico.

▲ *Trend* in crescita ▼ *Trend* in diminuzione ► *Trend* stabile

Per quel che concerne la tipologia di **attori ostili** (***Grafico 1***), i **gruppi hacktivisti** (52% delle minacce *cyber*) continuano a costituire la minaccia più rilevante, in termini percentuali, benché la valenza del suo impatto sia inversamente proporzionale, rispetto al livello quantitativo riferito ai **gruppi di *cyber-espionage***, più pericolosi anche se percentualmente meno rappresentativi (19%). Ai **gruppi islamisti** è imputato il 6% degli attacchi *cyber* perpetrati in Italia nel corso del 2016. Da evidenziare come per le tre categorie si sia registrato, rispetto al 2015, un incremento degli attacchi pari al 5% per i gruppi hacktivisti e quelli islamisti e del 2% per quelli di *cyber-espionage*, così come evidenziato nel paragrafo dedicato agli "Ambiti e attori della minaccia". A tale aumento ha corrisposto un decremento, pari al 12%, dei cd. **"attori non meglio identificati"** che si attestano nel complesso al 23% delle incursioni *cyber*.

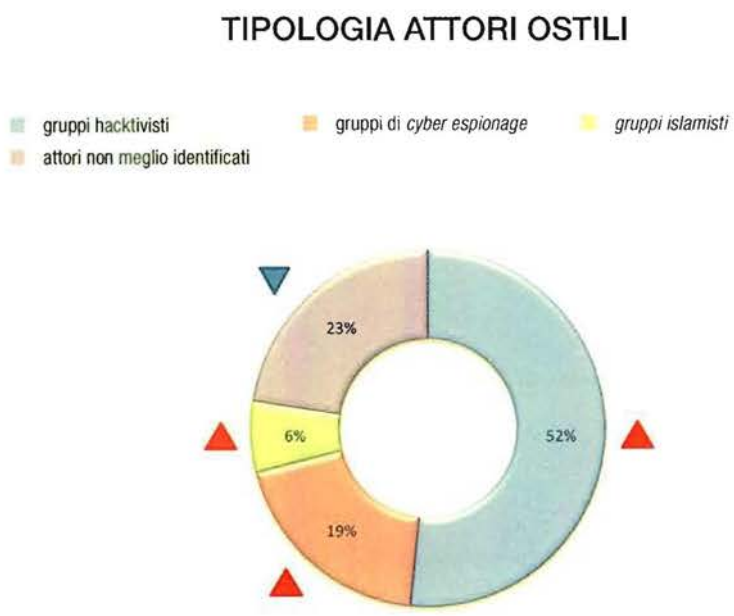

Grafico 1 – Attacchi cyber in Italia in base alla tipologia degli attori ostili (in % sul totale 2016)

Quanto ai dati sugli attacchi *cyber* in base ai **soggetti *target*** (***Grafico 2***) persiste il notevole divario tra le minacce contro i **soggetti pubblici**, che costituiscono la maggioranza con il 71% degli attacchi, e quelli in direzione di **soggetti privati**, che si attestano attorno al 27%, divaricazione, questa, riconducibile verosimilmente alle difficoltà di notifica degli attacchi subiti in ragione del richiamato rischio reputazionale. In entrambi i casi si registra un aumento pari, rispettivamente, al 2% ed al 4%. Un decremento del 6% è stato viceversa osservato nell'ambito dei ***target* non meglio identificati o diffusi** (che costituiscono, complessivamente, il 2%), solitamente oggetto di campagne hacktiviste. Tale dato è esplicativo del fatto che anche queste sono sempre più mirate, privilegiando *target* paganti sotto il profilo simbolico e della relativa rilevanza mediatica rispetto ai cd. *"soft target"*, ossia obiettivi di minore rilievo strategico, accomunati dalla ricorrenza di vulnerabilità comuni e di agevole sfruttamento.

Grafico 2 – Attacchi cyber in Italia in base alla tipologia dei soggetti target (in % sul totale 2016)

Il dettaglio dei dati relativi ai *target* per categoria pubblico/privato consente di rilevare, con riferimento ai **soggetti pubblici** (***Grafico 3***), che pur permanendo una netta predominanza delle Amministrazioni centrali (87% degli attacchi *cyber* verso soggetti pubblici) – dato che ricomprende anche le attività ostili verso movimenti politici – rispetto agli Enti locali (13%), nel 2016 si è assistito ad una inversione di tale *trend*. Gli attacchi contro le Pubbliche Amministrazioni Centrali (PAC) risultano, infatti, in lieve diminuzione (-2%) mentre quelli avverso le Pubbliche Amministrazioni Locali (PAL) sono in aumento (+5%). Vale rammentare come le PAC costituiscano obiettivo privilegiato per azioni di *cyber*-spionaggio, essendo detentrici di informazioni pregiate se non addirittura sensibili, e le PAL siano perlopiù oggetto di campagne di attivismo digitale ovvero condotte per finalità dimostrative da parte di gruppi islamisti.

Rispetto al 2015, non sono stati segnalati eventi cibernetici di particolare rilevanza in danno di organizzazioni internazionali insistenti sul territorio italiano.

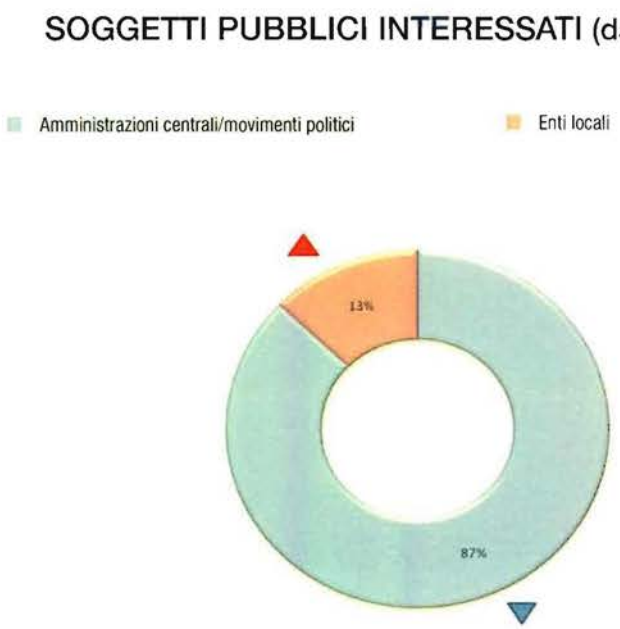

Grafico 3 – Attacchi cyber in Italia in base alla tipologia dei soggetti pubblici target (in % sul totale 2016, dati aggregati)

In relazione ai ***target* privati** (***Grafico 4***), sono emersi elementi di novità. Se nel 2015 *target* principali degli attacchi *cyber* risultavano quelli operanti nei settori della difesa, delle telecomunicazioni, dell'aerospazio e dell'energia, nel 2016 figurano ai primi posti il settore bancario con il 17% delle minacce a soggetti privati (+14% rispetto al 2015), le Agenzie di stampa e le testate giornalistiche che, insieme alle associazioni industriali, si attestano sull'11%. Queste ultime costituiscono una *"new entry"*, insieme al settore farmaceutico che, con il suo 5% degli attacchi verso *target* privati, si posiziona al fianco di settori "tradizionali" come quelli della difesa, dell'aerospazio e dell'energia. Tra questi ultimi, solo quello energetico ha fatto registrare un aumento, pari al 2%, rispetto all'anno precedente, mentre quelli di difesa e dell'aerospazio hanno fatto segnare un decremento, rispettivamente, del 13% e del 7%.

Sotto la voce "altri settori" (41%) sono state ricomprese aziende diversificate che non assumono, qualora singolarmente considerate, rilevanza sotto il profilo strategico.

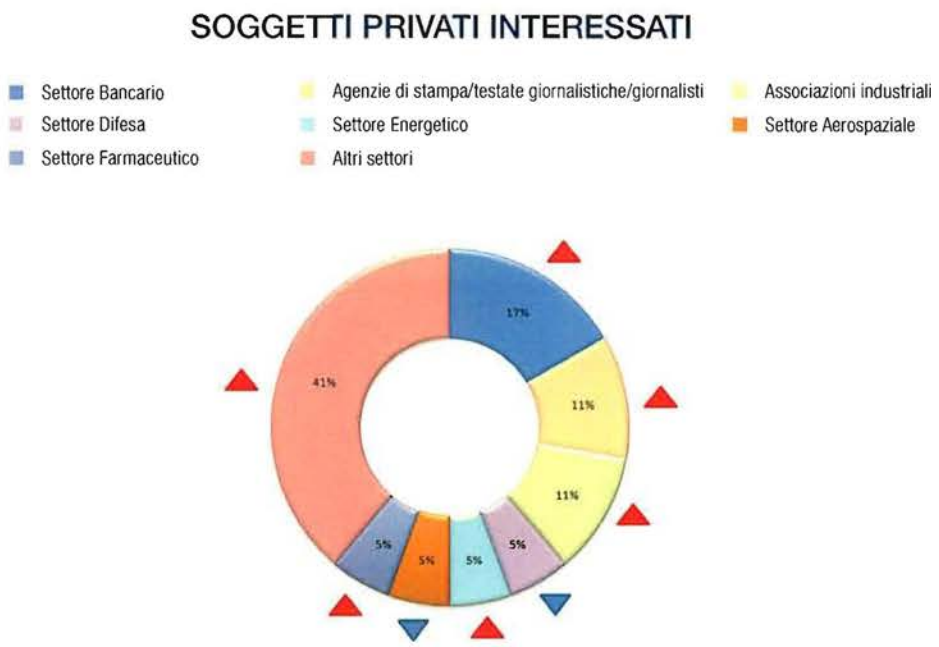

Grafico 4 – Attacchi cyber in Italia in base alla tipologia dei soggetti privati target (in % sul totale 2016)

Con riguardo, infine, alle **tipologie di attacco** (***Grafico 5***), rispetto al 2015, nel 2016 si è registrata un'inversione di tendenza. Se, infatti, nel 2015, poco più della metà delle minacce *cyber* era costituita dalla diffusione di *software* malevolo (*malware, vds. Glossario*), nel 2016 è stata registrata una maggiore presenza di altre tipologie di attività ostili, che ha comportato una contrazione (-42%) del dato relativo ai *malware*, attestatosi intorno all'11%. Tale dato non va letto come una riduzione della pericolosità della minaccia *Advanced Persistent Threat* (APT), bensì come il fatto che gli APT registrati si sono caratterizzati, più che per la consistenza numerica, per la loro estrema persistenza.

Tra le minacce che hanno registrato un maggior numero di ricorrenze vanno annoverate:

l'*SQL Injection* (28% del totale; +8% rispetto al 2015, *vds. Glossario*), i *Distributed Denial of Service* (19%; +14%), i *Web-defacement* (13%; -1%) ed il *DNS poisoning* (2%, *vds. Glossario*), impiegati sia dai gruppi hacktivisti che islamisti.

Le attività prodromiche ad un attacco (23% degli attacchi *cyber*) hanno fatto registrare un aumento del 18% rispetto all'anno precedente. Gli attacchi *cyber* non andati a buon fine e, quindi, "tentati", rimangono sostanzialmente stabili con il 4% (+1% se confrontato col dato 2015).

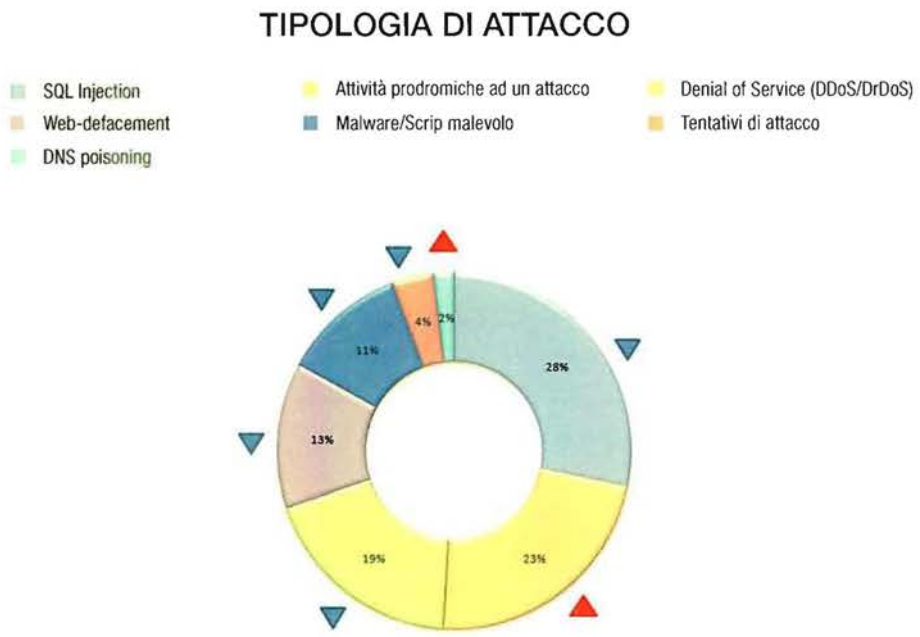

Grafico 5 – Attacchi cyber in Italia in base alla tipologia di attacco impiegata (in % sul totale 2016)

TREND EVOLUTIVI DELLA MINACCIA CIBERNETICA

In prospettiva, alla luce degli elementi considerati e del *trend* in atto, è verosimile nel breve-medio termine, in linea di continuità con il passato, una crescita della minaccia cibernetica ad opera di attori statuali e gruppi connessi alla criminalità organizzata, nonché di potenziali *insider*.

Con riferimento al binomio capacità/intenzionalità degli attori statuali, la consapevolezza dell'entità del rischio ad opera di una moltitudine di attori della minaccia, parallelamente ai massicci investimenti in *cybersecurity* di alcuni Paesi occidentali, potrebbe comportare, a livello internazionale, una allocazione di risorse crescenti finalizzate alla costituzione/consolidamento di *asset* cibernetici a connotazione sia difensiva, sia offensiva, impiegabili nella prosecuzione di campagne di *cyber-espionage*, nonché in innovativi contesti di conflittualità ibrida e asimmetrica (*cyberwarfare*), anche attraverso attività di *disruption* di sistemi critici in combinazione con operazioni di guerra psicologica.

Si prevede una sostanziale stabilità delle attività malevole nel *cyberspace* di matrice attivista (*web defacement*/DDoS, *vds. Glossario*) e terroristica (*defacement*, reclutamento e proselitismo *on-line*), anche se per queste ultime non si può escludere l'acquisizione di capacità operative attraverso il ricorso al cd. *"Cybercrime-as-a-Service"* (*vds. Glossario*). Ciò, a differenza delle attività di natura criminale (sottrazione di dati delle carte di credito, identità personale, frodi *on-line*, commercio illegale di beni e servizi nel *dark web*, ecc.), per le quali permangono le criticità connesse alle crescenti saldature, richiamate in precedenza, con ambienti e sodalizi criminali e non, orbitanti al di fuori del *cyberspace*.

I settori a rischio continueranno ad essere quelli ad alto contenuto tecnologico e di *know how*, con livelli di *time to market* contenuti, quali il segmento farmaceutico e del *software*, ovvero *target* il cui danno reputazionale sia suscettibile di ingenerare significativi impatti economici e di mercato.

I settori bancario e sanitario costituiranno - sempre nel breve-medio periodo - *target* privilegiati, anche per il valore intrinseco dei dati

finanziari e personali posseduti, sfruttabili, attraverso il furto di identità, nell'ambito di attività di frode, nonché, nel caso dell'area finanziaria, per le potenziali ingenti sottrazioni di valuta perseguibili tanto a livello massivo (frodi connesse alle carte di credito/debito), quanto a livello dei circuiti interbancari, nonché attraverso la potenziale manipolazione degli algoritmi di *trading* combinata con attività di speculazione sui mercati. Il gradiente di rischio, per il settore sanitario, potrebbe risultare più significativo in ragione del crescente ricorso al supporto ICT sia nel management dei processi organizzativi (cartelle cliniche, dati sanitari, ecc.), sia nella gestione dei presìdi biomedicali (controllo remoto dei *pacemaker*, robotica sanitaria, sistemi automatici di *monitoring* di parametri critici, ecc.).

L'evoluzione dei sistemi ICS/SCADA (*Industrial Control Systems/Supervisory Control and Data Acquisition, vds. Glossario*) e il progressivo aumento delle possibilità di gestione e controllo in remoto delle attività produttive esporrà, verosimilmente, il settore manifatturiero al rischio di crescenti compromissioni *cyber*, finalizzate ad alterare i dati operativi di processo, con potenziali impatti di ordine non solo economico ma anche cinetico. A questo proposito, una particolare area di criticità è rappresentata dall'evoluzione tecnologica del settore *automotive* e *smart car*, laddove la potenziale interconnessione, già dimostrata da alcuni ricercatori, tra i sistemi deputati all'intrattenimento ed all'ausilio alla guida con quelli dedicati alla gestione elettro-meccanica del veicolo, potrebbe comportare gravi rischi nella condotta dello stesso, in caso di compromissione. Sempre sul piano degli effetti cinetici perseguibili attraverso un attacco *cyber*, l'ampiezza della superficie di attacco delle infrastrutture critiche nazionali (aree del trasporto e dell'energia piuttosto che i sistemi idrici a servizio industriale e/o civile) è direttamente proporzionale al crescente livello di interdipendenza tra le stesse e le rispettive *supply chain*.

Quanto alle metodiche di attacco, l'evoluzione degli APT, oltre a caratterizzarsi per il ricorso ad innovative tecniche di "*spear phishing*" e di "*watering-hole*" (*vds. Glossario*), combinate con sofisticate attività di

ingegneria sociale (*vds. Glossario*), si potrebbe connotare sempre più per l'impiego di *software* nativo, ossia di *Remote Administration Tool* (RAT, *vds. Glossario*), già presente sui sistemi-obiettivo ed utilizzati per lo svolgimento di attività legittime. Ciononostante, lo sviluppo delle manovre intrusive con finalità di *cyber-espionage*, di matrice sia statuale che criminale, continuerà a connotarsi per il ricorso sia ad *exploit* (*vds. Glossario*) e a *malware* "customizzati" sul singolo *target*, sia ad armi digitali *standard*, di larga diffusione nell'ambiente *underground* (*vds. Glossario*). Tale disponibilità, economicità e facilità di accesso a *tool* offensivi è in grado di ampliare il bacino dei potenziali attori ostili, al netto di competenze specialistiche.

PAGINA BIANCA