Novembre 2018, anno XII – N. 11

Cybercrime: la minaccia del nuovo millennio

di Fabio Marzocca[1]

Ndr: in questo articolo Fabio Marzocca propone alcune riflessioni su un tema di interesse generale, che riguarda anche i formatori

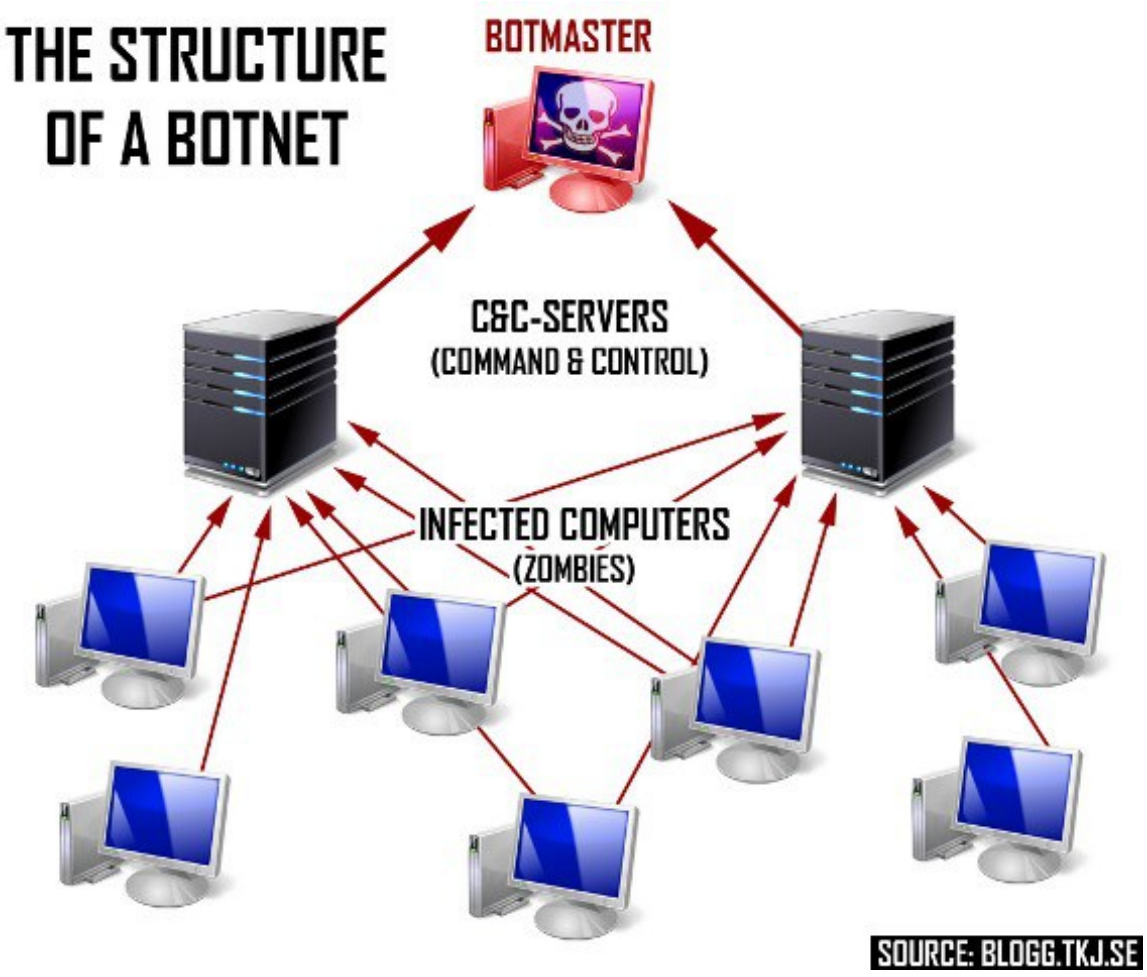
Come sarà ormai piuttosto evidente, la sicurezza informatica è un argomento sempre più importante per le infrastrutture di prossima generazione e sta diventando un argomento fondamentale nel progetto di qualunque nuova infrastruttura. Chiunque utilizzi un sistema informatico, da un computer a uno smartphone, da una Smart-TV a un termostato intelligente, non può fare a meno di scontrarsi con gli aspetti più sconcertanti di questo argomento. La cybersecurity non è più un tema per aziende o per professionisti del settore, ma coinvolge – spesso a sua insaputa – ciascun cittadino del mondo occidentale, direttamente o indirettamente.

L'incessante rapidità di sviluppo delle tecnologie ha aperto la strada a un grande settore della criminalità mai esistito negli anni precedenti, il cyber-criminale. Questa conseguenza rappresenta una delle più evidenti lacune nel processo di ideazione e creazione della tecnologia, laddove i progettisti hanno completamente disatteso la fase di misura dell'impatto diretto delle innovazioni, senza cercare di valutare i loro potenziali riflessi indiretti. Nel creare la tecnologia, si è creato il crimine informatico.
Occorre anzitutto definire il termine "*cybersecurity*": in informatica, la sicurezza è convenzionalmente definita come la protezione della riservatezza, dell'integrità e della disponibilità (CIA, confidentiality, integrity, availability) delle informazioni. Un famoso primo esempio fece notizia nel 2003, quando il "*worm*" (una particolare categoria di malware in grado di autoreplicarsi) Slammer infettò le macchine in una centrale nucleare nello stato

[1] Ingegnere elettronico, scrittore di saggi e romanzi a sfondo psicologico, giornalista informatico. Esperto di aviazione civile, pianificazione strategica, relazioni internazionali e studioso di transdisciplinarità, ha diretto grandi Enti, società private e comunità di supporto e sviluppo di software libero.

dell'Ohio, negli Stati Uniti. L'epidemia di worm rese inefficaci i sistemi di monitoraggio della sicurezza nella centrale nucleare per quasi cinque ore.
Oltre ai cosiddetti "*malware*" vi sono numerosi altri scenari di attacco che interessano i sistemi ICT nelle infrastrutture critiche. Ma quanto sono grandi i rischi derivanti dalla presenza massiccia dei sistemi informatici nelle infrastrutture? Non esiste una risposta chiara a questa domanda. Nessun numero, nessuna quantità di alcun tipo.
Nel web vengono spesso pubblicate stime che pretendono di quantificare il danno economico degli incidenti di sicurezza. Generalmente parlano di miliardi o, a volte, persino di migliaia di miliardi di dollari, tuttavia nessuna di queste fonda le sue basi su una solida ricerca o un'esaustiva valutazione.

La mancanza di una stima chiara per la dimensione del rischio è dovuta a due ragioni principali. Innanzitutto, vi è una mancanza di dati affidabili. Il rischio può esser definito come la combinazione delle probabilità di un evento e delle sue conseguenze, ma ben poco si conosce di queste quantità per gran parte dei rischi che vengono affrontati dai sistemi ICT infrastrutturali. Quindi, nel migliore dei casi, si possono solo effettuare ragionate congetture.



La seconda ragione è che anche se questi dati fossero disponibili, la rapidità di cambiamento e di sviluppo del software li renderebbe ben presto privi di valore. La statistica sui rischi e le probabilità di questi eventi negli anni passati non rappresenta – peraltro – un indicatore per il futuro: non solo la stessa tecnologia è in continua evoluzione, ma l'aggressione è avviata da azioni di esseri umani e non dalle forze della natura (per le quali

una statistica è sempre un valido aiuto per le proiezioni). Gli avversari si adattano alle nuove misure di sicurezza e a volte aggressori completamente nuovi entrano improvvisamente nel campo di gioco.
Quindi non abbiamo una valida risposta quantificabile alla domanda su quanto siano grandi questi rischi. Potrebbe essere utile vedere cosa si conosce circa la natura dei rischi e la loro potenzialità.

Per capire meglio il problema, è utile distinguere tre tipi di incidenti:

- Il primo è costituito da incidenti non intenzionali; in altre parole, inconvenienti. Interruzioni causate da guasti nel software o nell'hardware.
- Il secondo tipo è un attacco mirato intenzionale, che è un incidente durante il quale un aggressore umano cerca intenzionalmente di compromettere la sicurezza di alcuni sistemi o gruppi di sistemi.
- Il terzo tipo è un attacco intenzionale non mirato, in cui l'incidente è causato da un aggressore umano che non sta prendendo di mira specificamente quell'infrastruttura. La differenza tra attacchi mirati e non mirati può essere un po' confusa, ma è importante nel campo della sicurezza informatica, dove gli attacchi non mirati sono numerosi e creano ingenti danni. "Mirato" sta a significare che l'attacco si concentra in particolare su un determinato sistema o organizzazione.

La maggior parte degli attacchi è non-mirato. Ciò potrebbe sembrare strano, tuttavia il risultato è che l'attacco aggredisce in brevissimo tempo un gran numero di vittime, spesso milioni di utenti. Ad esempio, alcuni malware vengono scritti e progettati per trovare e compromettere il maggior numero possibile di macchine-vittima nel minor tempo. L'aggressore spesso non si cura di chi possiede la macchina o in quale azienda si trovi esattamente, vuole solo comprometterne migliaia, combinarle in una rete – una cosiddetta "*botnet*" – e usarle per inviare spam o affittarle ad altri criminali che perseguono attacchi di diversa natura.
In ogni caso, anche se un attacco non è stato progettato per una specifica infrastruttura, la sua rapida diffusione capillare è comunque in grado (statisticamente) di raggiungere siti sensibili e provocare devastazione nei loro dati. Migliaia di attacchi non mirati colpiscono ogni giorno i sistemi degli operatori delle infrastrutture, tanto che le procedure e le azioni di protezione sono ormai diventate routine quotidiana.

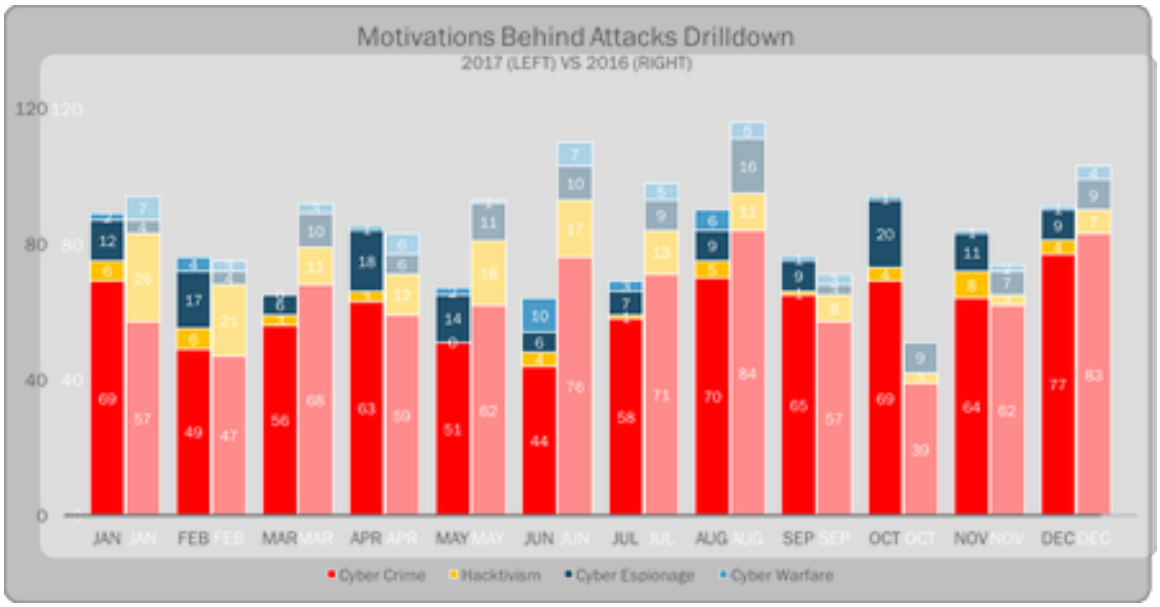
Gli attacchi mirati sono l'immagine speculare dei casi di cui sopra: sono molto più rari, tuttavia sono più difficili da difendere, perché gli aggressori possono sfruttare specifici punti deboli nei sistemi o nelle organizzazioni prese di mira.

In sintesi, si potrebbe dire: il rischio di attacchi non mirati è dato da un'alta probabilità e basse conseguenze (se vengono adottate le procedure standard di difesa), mentre per gli attacchi mirati, il rischio è rappresentato da bassa probabilità ed elevate conseguenze.

I maggiori esperti di sicurezza informatica hanno identificato un ampio insieme di vulnerabilità che non sono ancora state utilizzate negli attacchi, ma che potrebbero essere sfruttate con successo da aggressori più competenti e motivati nell'immediato futuro. La ragione per cui vengono identificate nuove vulnerabilità ancor prima dell'evidenza di

un'aggressione è data dal numero sempre crescente di persone impegnate in questa nuova attività di test e ricerca, quindi la scoperta dei nuovi rischi è proporzionale al numero di persone dedicate a questa attività.

Quali sono le cause strutturali alla base della presenza di tutte queste vulnerabilità e rischi? In primo luogo, ciò è dovuto alla sempre maggiore presenza di sistemi ICT nelle infrastrutture e nella popolazione: più ICT significa una superficie di attacco più grande. Questo fornisce agli aggressori maggiori opportunità, mentre i sistemi di difesa devono distribuire le proprie risorse su più obiettivi potenziali.



In secondo luogo, questi sistemi contengono una riserva praticamente infinita di vulnerabilità. Una delle dolorose lezioni sulla sicurezza informatica è che il software contiene più errori e punti deboli di quanti possano mai essere scoperti e riparati. Ciò dipende essenzialmente dalla quantità e la complessità del codice informatico. Anche un sistema operativo per un singolo componente "*hardened*" (il processo di verifica e messa in sicurezza di un host, mediante l'adozione di specifiche tecniche per ridurre i punti di attacco da parte di un hacker) può facilmente consistere in milioni di righe di codice, spesso decine di milioni. E se scoprire una vulnerabilità è come ricercare un ago nel pagliaio, in questo caso si tratta di enormi pagliai con molto aghi nascosti al loro interno. Solo di recente gli sviluppatori di software stanno ottenendo un supporto migliore nella prevenzione di errori e punti deboli, ma si è ancora molto lontani dal capire come realizzare un software veramente inattaccabile.
Un'ulteriore complicazione è data dal fatto che molti di questi componenti ICT non sono stati progettati pensando alla sicurezza, originariamente sviluppati ben prima che la cybersecurity fosse un problema rilevante. Avrebbero dovuto lavorare in un ambiente "fidato", non nell'odierno mondo ostile di internet, ed era previsto che rimanessero in servizio per decenni: l'eredità di questa progettazione lacunosa che non ha saputo completamente valutare gli impatti diretti ancora affligge questi sistemi a rischio.

E abbiamo parlato solo della complessità di un singolo componente. Ora immaginiamo le

molte, molte migliaia di componenti ICT che sono presenti in un'infrastruttura specifica. Ce ne sono così tanti, infatti, che le aziende che le gestiscono hanno raramente un quadro completo e preciso dei rischi della loro infrastruttura ICT.

Il professor Michel van Eeten, ricercatore nell'area della sicurezza informatica dell'Università di Delft-Olanda, ha coniato una meravigliosa espressione per definire l'analisi dei sistemi complessi: "*la principale manifestazione della complessità è la sorpresa*".
In conclusione: le infrastrutture di nuova generazione contengono un insieme di vulnerabilità molto più ampio di quello finora rilevato. E questo rimarrà il caso per l'immediato futuro. Ogni sistema ICT può essere violato, è solo una questione di quanti sforzi vengono adottati nello specifico.

Cosa può essere messo in atto per attuare un'adeguata difesa dei nostri sistemi? Ovviamente, la migliore difesa sarebbe isolare il componente da internet e da qualunque dispositivo di ingresso che possa introdurre un attacco, ma evidentemente ciò vanificherebbe l'efficienza del componente stesso. Esistono specifiche tecnologie di sicurezza e contromisure (apparecchiature ad-hoc o "*best practices*"), eppure il risultato perfetto non è tuttora raggiungibile né garantito.
Tutto ciò porta a dover fare una valutazione: quali incidenti possono essere tollerati e quali invece occorre prevenire a tutti i costi. Qui ha senso introdurre due punti di vista sulla sicurezza, presi in prestito dal campo dell'affidabilità: sicurezza marginale e sicurezza degli eventi preclusi.

La sicurezza marginale è il paradigma giusto per gli incidenti che possono essere costosi, ma non catastrofici. Gli operatori possono imparare dalle prove e dagli errori e valutare i costi e i benefici della riduzione di determinati rischi caso per caso.

Il secondo paradigma si riferisce a quegli incidenti che devono essere impediti a tutti i costi. Immaginiamo una fusione nucleare. Per tali incidenti, non esistono prove ed errori, la prima prova potrebbe essere l'ultimo errore. L'impatto di tali eventi per la società in generale implica forme di supervisione e di regolamentazione del governo altamente intrusive. Ma in generale, gli operatori di ciascun settore hanno ben chiaro l'aspetto di questi eventi in termini di servizio e tecnologia primaria, perché tutta la loro organizzazione si fonda sull'erogazione di tali servizi (es: il collasso di una rete elettrica o gli incidenti aerei nel controllo del traffico aereo). La chiave è scoprire quali incidenti nei software potrebbero portare a tali eventi.

Si tratta in definitiva di un nuovo nemico, di una minaccia di recente apparizione, alla quale il mondo intero dovrà rendere conto molto spesso nei prossimi anni: uno dei tanti prezzi della tecnologia e una conseguenza della straordinaria velocità con la quale è stata introdotta e con cui si sviluppa. La stessa tecnologia che oggi consente all'uomo di essere collegato con ogni altro luogo del pianeta, che lo abilita all'accesso in tempo reale di informazioni e cultura, che rende possibili processi di produzione altrimenti nemmeno immaginabili, porta al suo interno anche una minaccia che si sviluppa alla stessa velocità e con la stessa competenza della tecnologia che l'ha creata. Una tecnologia che aiuta ad affrontare – e spesso a risolvere – problemi di sicurezza nella vita quotidiana, ha coltivato al suo interno e generato un nuova minaccia globale per le generazioni future: il *cybercrime*.