IL VIRUS VIRTUALE È PIÙ LETALE CHE MAI

di BENIAMINO MUSTO

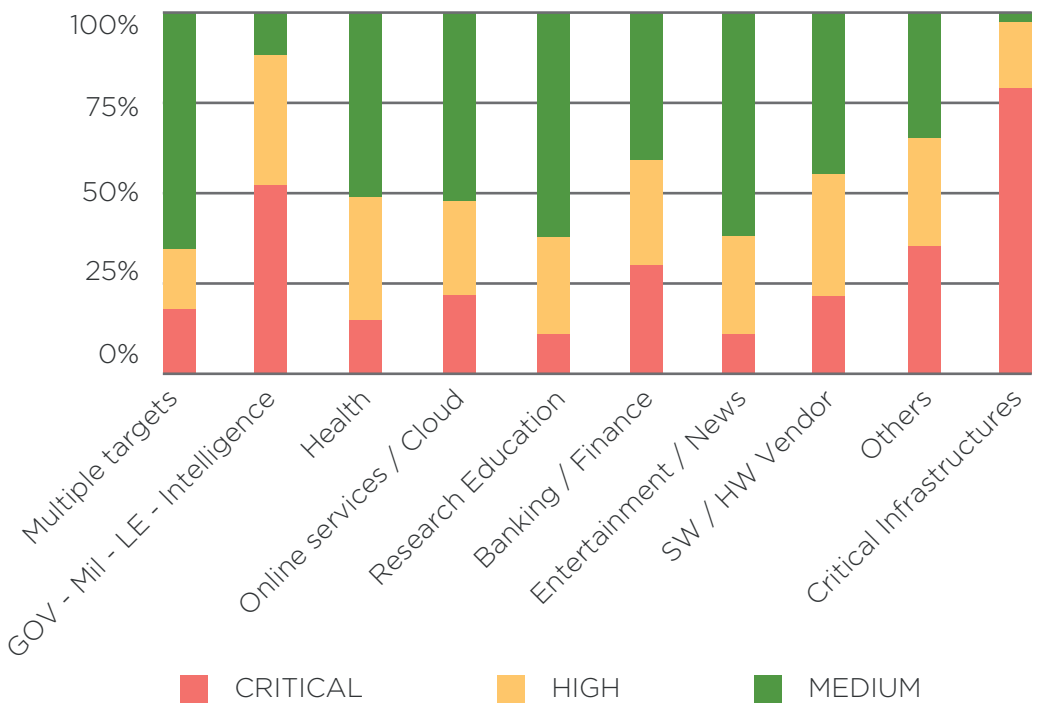
L'ULTIMO RAPPORTO SULLA SICUREZZA INFORMATICA DEL CLUSIT LANCIA UN GRIDO D'ALLARME SULLA PERICOLOSITÀ DEL CYBER CRIME. GLI ATTACCHI GRAVI NEL 2019 SONO STATI 1.670 A LIVELLO MONDIALE, UN QUARTO DEI QUALI HA COLPITO IN PARALLELO BERSAGLI MULTIPLI. RISPETTO ALL'ANNO PRECEDENTE GLI ATTI CRIMINALI A DANNO DEI SERVIZI ONLINE SONO CRESCIUTI DEL 91,5%, E DEL 17% QUELLI AI DANNI DELLA SANITÀ

L'attenzione di tutto il mondo in questo momento è giustamente rivolta nei confronti di un virus fisico. Ma non possiamo e non dobbiamo abbassare la guardia nei confronti di quelli virtuali. Già, perché i cyber criminali stanno affinando sempre di più le loro tecniche di attacco. E i risultati, dati alla mano, sono disastrosi per le vittime. Secondo l'edizione 2020 del rapporto **Clusit**, l'associazione italiana per la sicurezza informatica, nel 2019 gli attacchi gravi, in Italia e nel mondo, sono stati 1.670 con una tendenza in crescita del 7% rispetto al 2018. Questo dato, spiegano gli esperti, "segna un nuovo picco verso l'alto nella rappresentazione della insicurezza cyber". Anche perché, come vedremo, l'ambito sanitario è uno di quelli più colpiti dai criminali informatici.

SOLO LA PUNTA DELL'ICEBERG

Tra gennaio e dicembre 2019 sono stati in media 139 gli attacchi registrati mensilmente a livello mondiale con impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. Si tratta del

Distribuzione Severity per i 10 target più colpiti 2019



Fonte: *Clusit, Rapporto 2020 sulla sicurezza Ict in Italia*

47,8% in più rispetto alla media dei 94 attacchi mensili registrati nel quinquennio 2014-2018. Gli esperti Clusit avvertono, tuttavia, che si tratta solo della punta dell'iceberg: le analisi si riferiscono infatti ad attacchi reali, ovvero effettivamente andati a segno provocando danni importanti. Rimangono quindi esclusi gli attacchi tentati o bloccati. Inoltre, per quanto ormai statisticamente significativo, il campione analizzato nel rapporto Clusit è necessariamente parziale, data la tendenza generale ad evitare di rendere pubbliche le aggressioni cyber. La stessa entrata in vigore del regolamento Gdpr e della direttiva Nis, spiegano gli autori del report, non hanno a oggi portato alla rilevazione di un aumento significativo di attacchi gravi di pubblico dominio verso bersagli europei: questo comporta certamente l'evidenza di uno scenario meno critico rispetto alla situazione sul campo.


© iLexx - iStock

LE TECNICHE D'ATTACCO

I cyber-criminali nel 2019 hanno sferrato attacchi utilizzando malware nel 44% dei casi. Questa tecnica è in crescita del 24,8% rispetto allo scorso anno; nello specifico, i ransomware rappresentano quasi la metà del totale di questa tecnica (46%, in crescita del 21% rispetto al 2018). Gli esperti Clusit confermano la tendenza dei cyber-criminali a utilizzare tecniche di attacco prodotte industrialmente in infinite varianti, a costi decrescenti; allo stesso tempo, tuttavia, appare sempre più elevata la tendenza all'utilizzo di queste tecniche anche da parte di attori statuali e state-sponsored.
Le tecniche di phishing e social engineering segnano invece +81,9% rispetto al 2018, arrivando a rappresentare il 17% del totale. Una quota crescente di questi attacchi si riferisce, evidenziano gli esperti Clusit, a *Bec scams*, ovvero frodi via email che colpiscono in maniera specifica le organizzazioni con l'obiettivo di infliggere danni economici, con impatto spesso notevole.

UN CAMBIAMENTO EPOCALE

A seguito delle loro analisi, gli esperti Clusit evidenziano dinamiche che, in particolare nell'ultimo triennio, hanno spinto sempre più soggetti a entrare nell'arena della cyber war, e questo ha impattato in modo inequivocabile sulla società civile. Secondo **Andrea Zapparoli Manzoni**, membro del comitato direttivo Clusit, "ci troviamo di fronte a un vero e proprio cambiamento epocale nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi". Zapparoli sottolinea che gli attaccanti sono oggi decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari e unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come campo di battaglia, arma e bersaglio le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging, su scala globale, 365 giorni all'anno, 24 ore al giorno. "Viviamo e operiamo in una situazione di inaudita gravità – avverte

l'esperto – in termini di rischi cyber, che mette a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i servizi, online e offline, che su di essa fanno affidamento".

DIVERSI LIVELLI DI IMPATTO

Gli attacchi registrati dagli esperti Clusit sono stati classificati con differenti livelli di impatto, sulla base di variabili di tipo geopolitico, sociale, economico (diretto e indiretto) e di immagine. Nel 2019 gli attacchi andati a buon fine hanno avuto nel 54% dei casi un impatto *alto* e *critico*; il 46% è stato di gravità *media*. Il cyber crime è ancora nel 2019 la principale causa di attacchi gravi: l'83% di essi è infatti stato perpetrato con l'obiettivo di estorcere denaro alle vittime. In particolare, lo scorso anno gli esperti Clusit hanno registrato il numero di attacchi di cyber crime più elevato degli ultimi nove anni, con una crescita del 162% rispetto al 2014 e del 12,3% rispetto al 2018. Rimangono sostanzialmente stabili anno su anno gli attacchi gravi riferibili ad attività di cyber espionage (+0,5% rispetto al 2018, tuttavia gli esperti evidenziano la scarsità di informazioni pubbliche in merito), che rappresentano la causa del 12% degli attacchi gravi nel 2019; diminuiscono quelli appartenenti alla categoria cyber warfare, cioè la guerra delle informazioni (-37,5% rispetto al 2018), che costituisce il 2% del totale degli attacchi. Insieme, cyber espionage e cyber warfare sono però classificabili con una gravità più alta della media, fanno notare gli esperti Clusit.

QUALI SONO I SETTORI PIÙ COLPITI

I cosiddetti *multiple targets* rappresentano il 24% del totale degli attacchi. Si tratta di bersagli multipli che si rivelano obiettivi indifferenziati per un'unica organizzazione criminale che utilizza una logica *industriale* di attacco. Gli attacchi verso questi obiettivi sono in crescita del 29,9% rispetto al 2018. Ma quali sono i settori maggiormente colpiti da attacchi cyber gravi nel 2019? Nel dettaglio, sono stati colpiti il settore pubblico (15% degli attacchi, in discesa del 19,4%), quello sanitario (12% del totale degli attacchi, +17% rispetto al 2018) e i servizi online (11% degli attacchi, +91,5%). Seguono i settori ricerca e formazione scolastica (8% in calo dell'8,3%), bancario e assicurativo (6% in calo del 10,2%) e intrattenimento/informazione (5% in calo del 31,4%), commercio e grande distribuzione organizzata (2% degli attacchi, in crescita del 28,2%), e l'insieme di "altri settori" (3% del totale attacchi, +76,7%), telecomunicazioni (1% del totale, +54,5%) e fornitori di sicurezza informatica (1%; in evidenza qui la crescita a tre cifre: +325%).

La categoria dei multiple targets comprende attacchi verso vittime appartenenti a tutte le altre colpite dallo stesso attacco in parallelo, a dimostrazione del fatto che gli attaccanti sono sempre più aggressivi e conducono operazioni su scala sempre maggiore, con una logica industriale, che prescinde sia da vincoli territoriali, sia dalla tipologia dei bersagli, puntando solo a massimizzare il risultato economico.

A livello qualitativo, i dati del rapporto Clusit 2020 evidenziano che le categorie delle *infrastrutture critiche* e del *settore pubblico*, con il settore bancario e finanziario, hanno subìto nel 2019 il maggior numero di attacchi di impatto classificato come *critico*, mentre le categorie con il maggior numero di attacchi con impatti di livello alto sono la sanità, i fornitori di software e hardware, e ancora il settore pubblico.