# Virus Melissa: 20 anni dopo cosa abbiamo imparato?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*

Il 26 marzo del 1999 iniziò a diffondersi un virus, creato da un tale **David Lee Smith**, che infettò oltre 1 milione di sistemi; provocò danni diretti stimati in oltre 80 milioni di dollari  e bloccò, anche per diversi giorni, l'operatività dei server mail di oltre 300 grandi aziende ed enti governativi.

Il programmatore Smith, ammiratore della bella striptease Melissa, prese possesso di un *account* di AOL e lo utilizzò per pubblicare un file in un gruppo Internet chiamato "alt.sex", promettendo decine di password per accessi gratuiti a siti che forniscono materiale non idoneo per i minori. Una volta aperto il documento Word, il virus si diffondeva nel computer e quindi, utilizzando Outlook, si spediva agli indirizzi email trovati. La email spedita suggeriva al destinatario di aprire il documento allegato che aveva un nome del tipo "sexxxy.jpg" oppure "naked wife".

Già 20 anni fa il phishing sfruttava anche email inviate da persone conosciute!

La velocità di propagazione e i problemi creati misero in allarme l'FBI che sollecitò tutti a porre attenzione alle email ed ai relativi allegati.

Fu questo il primo episodio di una certa gravità? No.

Un grave episodio era già avvenuto 11 anni prima! Infatti, il

2 novembre del 1988 un worm (conosciuto come **Morris worm**) si diffuse su Internet: nelle prime 24 ore aveva già bloccato circa il 10% dei computer connessi in rete. Colpiti furono i sistemi UNIX del Massachusetts Institute of Technology (MIT), e di Harvard, Princeton, Stanford, Johns Hopkins, NASA, ed il Lawrence Livermore National Laboratory.

Oltre a sfruttare una porta ed un problema nel software di identificazione degli utenti in rete, era progettato anche per stare nascosto.

Domanda: gli utilizzatori hanno finalmente compreso la lezione?

Scrive il CLUSIT:«*Tutti gli analisti ed esperti di sicurezza concordano* ***che la maggior parte degli incidenti di sicurezza è legata ad errori umani*** *(si stima che siano circa l'80%-90% degli incidenti) confermando come il fattore umano sia, anche per la sicurezza informatica, l'anello debole del sistema. Solo in Italia si è stimato che circa il 53% degli attacchi sono dovuti a cause endogene (****utilizzo di password deboli e non alfanumeriche, accesso di device aziendali a connessioni pubbliche, navigazione in siti non sicuri e il trasporto di dati sensibili con chiavi USB non cifrate****,…) e a queste si sommano gli attacchi di phishing e spear phishing che provocano impatti significativi sull'azienda sia in termini di frodi e dati rubati che come incremento dei costi operativi per il ripristino dagli incidenti occorsi*.».

Conclusione: 1988, 1999, 2019: nulla è cambiato nell'atteggiamento del cittadino?

Vi è però, a mio parere, una eccezione che fa piacere. Nell'ambito della mia attività presso l'AGID mi è capitato di leggere la esigenza, manifestata dal management di diversi Enti della Pubblica Amministrazione, di far frequentare corsi di sensibilizzazione ad attacchi di Social Engineering a tutto il personale, IT incluso. Ottimo!

Ma ciò a mio parere non basta, in quanto bisogna far sì che l’attenzione alle minacce entri nel DNA delle persone.

Che fare quindi?

La soluzione a mio parere è di iniziare a **diffondere la cultura dell’attenzione ai rischi iniziando dai ragazzi, se non addirittura dai più piccoli.**

Nel prossimo articolo racconterò della mia esperienza con decine di classi medie inferiori in due regioni italiane.

Anthony Cecil Wright

https://www.key4biz.it/virus-melissa-20-anni-dopo-cosa-abbiamo-imparato/251563/