

Le principali minacce di Internet

Venticinque anni fa fece la sua apparizione Brain, il primo virus per PC.

I personal computer erano poco diffusi e molto diversi da come oggi li conosciamo, non esistevano CD o DVD e tantomeno Internet! Brain poteva infatti propagarsi solo se un dischetto floppy contenente il virus veniva spostato da un PC all'altro e questo rendeva piuttosto difficile, nel 1986, fenomeni di propagazione virale a livello mondiale.

Il concetto di virus per computer cominciò a diffondersi quasi immediatamente, scatenando negli anni novanta tra gli appassionati di informatica una vera competizione a chi riusciva in meno tempo o in modo più nascosto ad inserirsi nei sistemi di enti governativi, oppure a creare un virus che si propagasse in tutto il mondo nel più breve tempo possibile.

I virus venivano creati per fama e per notorietà personale e spesso non avevano dei veri effetti dannosi sul PC e potevano essere facilmente rimossi. Fino ai primi anni 2000.

All'inizio di quel decennio, il panorama della sicurezza informatica subì un cambio radicale, quando da un'attività ludica e con il solo scopo di fama e passatempo, i virus divennero una vera attività criminale che aveva come unico scopo quello di rubare soldi ad ignari utenti.

Erano gli anni del forte sviluppo della banda larga e dei computer, in tutte le maggiori città del mondo comparivano milioni di nuovi PC e di nuove connessioni e da allora, la crescita dei virus ha seguito da vicino questa diffusione. L'esplosione della connettività via Internet nei tardi anni '90 ha dato ai virus la possibilità di espandersi e di propagarsi nel mondo in pochi minuti.

L'attività criminale è cresciuta enormemente in questi ultimi anni sino ad arrivare alla cifra record di 40.000.000 di esemplari di virus presenti nei laboratori di ricerca di F-Secure. Ogni giorno arrivano mediamente dai 50.000 ai 70.000 nuovi virus che occorre analizzare e neutralizzare.

Virus che non sono più semplici come negli anni 80, tanto che si è resa necessaria una classificazione dei virus in diverse tipologie o famiglie così da poter distinguere gli attacchi criminali a seconda del metodo che viene utilizzato o dello scopo che si prefiggono.

Abbiamo ad esempio gli **'spyware'**, applicazioni che vengono installate sul computer in modo più o meno inconsapevole, che hanno come scopo quello di raccogliere informazioni sensibili dell'utente quali password, indirizzi mail o credenziali del conto corrente e le inviano a dei server remoti gestiti da veri e propri criminali, che riutilizzano o vendono queste informazioni. Un altro sistema per rubare queste informazioni sono ad esempio i **'keylogger'**, piccoli software che una volta scaricati sul nostro computer registrano tutto quello che digitiamo sulla tastiera, quindi indirizzi web, password, numero di carta di credito e tanto altro. Una volta raccolte le informazioni, come per gli spyware, queste vengono inviate sempre attraverso internet a chi ha scritto il virus, così che possa analizzarle e una volta trovate le informazioni giuste, utilizzarle.

La crescita di internet è stato un notevole progresso dal punto di vista culturale e integrativo della società che ha però portato ad un reale problema legato alla mancanza di un'adeguata protezione durante la fase di navigazione. Una carenza di sicurezza che ha portato i criminali informatici a sviluppare un nuovo tipo di attacco veicolato unicamente attraverso internet: il **'phishing'**.

Utilizzando questa tecnica oramai diffusissima, i criminali creano delle email e delle pagine internet che imitano grafica e testo di siti istituzionali (ad esempio di banche o società di carte di credito) e l'utente, ingannato dall'aspetto molto simile di queste pagine, è portato ad inserire dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.. rivelando così queste informazioni sensibili ai criminali che hanno creato questo inganno.

Ultimi ma solo in ordine di tempo, sono gli attacchi rivolti ai siti di **social network**, L'evoluzione di internet ha portato un numero sempre maggiore di persone ad usare questi sistemi di comunicazione sociale per rimanere in contatto con i propri amici e parenti. I criminali in cerca dei nostri dati personali non sono rimasti a guardare. Attraverso tecniche di phishing e spyware mirano a rubare le nostre credenziali di accesso ai portali per poter controllare i nostri account, rubare le nostre identità e attaccare tutti i nostri contatti.

Internet rimane un posto meraviglioso per passare il tempo, cercare informazioni, condividere esperienze o magari pianificare un viaggio. Purché venga fatto con la medesima accortezza che occorre usare nella vita reale quando si cammina per la strada, si entra in un negozio per fare shopping o ci si ferma a parlare con un amico o uno sconosciuto.

Oltre al buon senso, è ormai necessario dotarsi di un sistema di protezione completo come **Antivirus Security Suite**, sviluppato da 3 in collaborazione con F-Secure, azienda di sicurezza informatica leader nel settore.