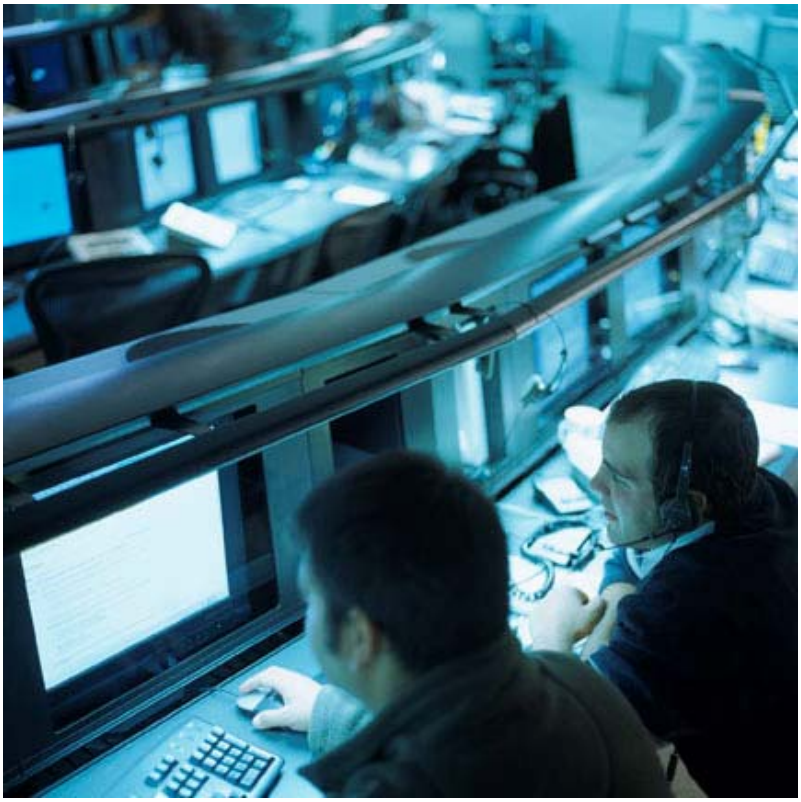
Visita al Security operation center di Symantec in Virginia. Adesso gli hacker si combattono con 40 mila agenti software, infiltrati nella rete.
Nel 2005 oltre 2,5 miliardi di falsi messaggi di phishing hanno tentato di catturate l'identità elettronica degli utenti
(Corriere Economia, settembre 2006)

Il nuovo pericolo di Internet arriva dai furti dell'identità elettronica degli utenti. Ecco perché Symantec ha sguinzagliato dei "web-agenti" molto speciali. Si tratta di oltre 40 mila programmi software che viaggiano silenziosi in rete. Controllano quanto succede e nel caso scoprano nuovi virus o situazioni a rischio, avvisano gli esperti. Ed è questo il motivo per cui Christian controlla con attenzione la serie di monitor installati nella sua zona di lavoro. Un guscio zeppo di apparecchi elettronici, simile alla postazione di comando di una navicella spaziale. Oggi, per 6 ore consecutive, sarà il numero uno della security. Il responsabile del sistema di monitoraggio mondiale che in tempo reale intercetta in 180 paesi gli attacchi dei pirati informatici. In termini tecnici è "l'administrator" dell'intero network del pianeta. E sarà lui a guidare il team dei cyberpoliziotti impegnati a difendere la rete. Ci troviamo nel Soc (Security operation center), il centro di controllo Symantec ad Alexandria, in Virginia. Un bunker superprotetto nei pressi del fiume Potomac, a pochi isolati dal Pentagono, dove si accede dopo una rigida serie di controlli personali.

Perché l'ingresso nella "stanza dei bottoni" avviene dopo il riconoscimento delle impronte digitali e l'esame della retina. Spiega Christian, che per ovvi motivi di sicurezza non rivela il cognome: «quando un Pc è sotto attacco invia un segnale di allerta al Soc. In tempo reale lo rendo disponibile alle postazioni di lavoro dei nostri esperti. In media una trentina ogni turno. Entro una decina di secondi capiamo se l'attacco arriva da un computer domestico, una rete aziendale o enti pubblici». A questo punto il virus informatico viene messo in quarantena in una zona protetta. Si tratta di una rete isolata nella quale valutiamo quali potrebbero essere i danni prodotti. Da questo momento inizia l'analisi e la ricerca dell'antivirus. «Così facendo capiamo la gravità dell'attacco e quali sistemi operativi vengono messi sotto scacco. Può trattarsi di Windows, Apple, Unix o Linux». Nel centro di Washington, che coordina anche quelli di Tokio, Sidney e Monaco in Germania, l'antidoto (altro non è che un programma software con opportune contromisure) viene scoperto in media entro 10-15 minuti. E poi messo su Internet, a disposizione degli utenti.
Ma la battaglia tra hacker e tutori del web negli ultimi mesi si è inasprita. Oltre ai virus e allo spamming indiscriminato, avanza la minaccia del phishing. L'invio di falsi messaggi di posta elettronica studiati dai pirati informatici per catturare informazioni sull'identità degli utenti. Per capire la gravità del fenomeno basta pensare che in un anno sono state spedite 2,5 miliardi di e.mail contenenti phishing. Non solo.



Le strategie messe in atto dai cybercriminali sono ancora più subdole. A spiegarlo è Vincent Weafer, direttore del Soc di Washington: «Adesso gli hacker sfruttano azioni combinate e simultanee. Per esempio un attacco inizia nelle Filippine, poi nel corso di pochi minuti si sposta in Canada ed Europa. Viene spedito un virus che entra nel sistemi informativi, come un "cavallo di Troia", ma l'obiettivo non è il furto diretto di informazioni. Come accadeva fino a oggi. Si insedia invece nel computer per giorni, ma abbiamo avuto il caso di una grande Assicurazione in cui è rimasto un mese». Lo scopo è quello di catturare il maggiore numero di dati sull'identità digitale degli utenti. Queste informazioni su dati personali verranno poi sfruttate nel tempo per mettere in atto frodi, furti e attività illegali.

Non manca però la contromossa. Perché, per difendersi dal nuovo pericolo i poliziotti del web hanno iniziato a distribuire in rete tanti software di simulazione. Agiscono come "agenti infiltrati", con lo scopo di rilevare i computer infetti. «Abbiamo preso spunto dalla vita reale. Sappiamo infatti che i servizi segreti raccolgono parte delle loro informazioni da agenti spediti sotto copertura nelle linee nemiche.
Noi agiamo nello stesso modo. Spediamo dei programmi camuffati che rilevano i possibili virus e le minacce informatiche. E poi riferiscono al centro di controllo». E' interessante osservare che esiste una tipologia di web-agenti che mettono in atto le stesse tecniche usate dagli hacker. Entrano di nascosto nei programmi sospetti e rimangono in attesa che qualche virus si manifesti. Poi informano il "capo".

# # #