ECCO IL CME, ENCICLOPEDIA DEI «WORM»

La guerra ai virus

Alzi la mano chi non ha mai avuto la sfortuna di trovare un virus sul proprio pc.
I virus sono senza dubbio la più concreta minaccia per la sicurezza informatica con la quale ci scontriamo quotidianamente. Ogni tanto l'antivirus fa il suo dovere, avverte con un allarme di averne intercettato uno e che il virus non può essere rimosso. A questo punto sui vostri visi si dipingono espressioni di panico. Superato il primo momento di sgomento, la procedura classica prevede di identificare il nome del "worm" (= verme) e cercare su Internet informazioni dettagliate su come si propaga, quali danni produce sul pc e eventuali soluzioni per la sua rimozione.
E qui viene il bello. Vi collegate al sito del produttore del vostro antivirus, cercate il virus con il nome che è apparso nell'allarme e lo trovate: le informazioni però sono incomplete, in particolare non viene specificato come rimuoverlo. E ora che si fa? Semplice: andate a cercare presso i siti di altre software-house di antivirus, ma purtroppo non trovate nessun virus che corrisponda a quel nome. Siete in un vicolo cieco.
Ma come si possono verificare simili situazioni? Bene, la risposta è che per rilasciare le soluzioni più velocemente possibile, spesso i produttori di antivirus non identificano un virus attraverso un codice universalmente riconosciuto, ma gli assegnano un nome secondo le proprie specifiche. Capita quindi che il malware "w32-pippo" sia chiamato da un altro programma antivirus "worm-32-pluto", rendendo vana qualsiasi ricerca incrociata da parte degli utenti.
Anche per ovviare a queste situazioni lo Us-Cert *(United States Computer Emergency Readiness Team)*, il dipartimento americano per la sicurezza interna che coordina le attività contro gli attacchi informatici, ha sponsorizzato la nascita del *Common Malware Enumeration* (Cme), un progetto che si pone come obiettivo l'identificazione e la classificazione univoca dei nuovi virus. Il sito del Cme, infatti, recita testualmente che l'iniziativa punta a "ridurre la confusione del pubblico durante gli incidenti informatici causati da virus, ad aumentare la comunicazione tra i vari produttori di antivirus e a migliorare lo scambio di informazioni tra i produttori stessi ed il resto della comunità per la sicurezza informatica".
Al "board" del Cme hanno aderito aziende del calibro di Computer Associates, F-Secure, Kaspersky, McAfee, Microsoft, Sophos, Symantec e Trend Micro e questo dovrebbe garantire il successo del programma.
In concreto, i nuovi virus scoperti saranno denominati dal progetto con il codice Cme-N, dove N sarà un indice numerico (ad esempio Cme-243). I produttori di antivirus si impegneranno a inserire questo codice all'interno delle loro "enciclopedie" dei virus, in modo che qualsiasi minaccia virale possa essere univocamente identificata.
Questa soluzione dovrebbe consentire di affrontare il problema dei virus informatici con maggiore serenità. Per maggiori informazioni potete consultare il sito del Cme su ***cme.mitre.org*** .