L'efficacia tecnologia euristica di ESET (NOD32) viene confermata da un test indipendente

Il rapporto di AV-Comparatives dimostra come la combinazione adottata da ESET (NOD32) comprendente un forte motore euristico ed aggiornamenti quotidiani sia il metodo migliore per contrastare il malware

ROMA – Autunno 2006 –ESET, ditta produttrice dell'antivirus **NOD32** e azienda leader nei sistemi di difesa proattiva, ha annunciato che è oggi disponibile una nuova conferma dell'efficacia della sua avanzata tecnologia euristica ThreatSense®, prova che si basa sui risultati di un recente test condotto da AV-Comparatives.

I risultati di laboratorio dimostrano come aggiornamenti ancora più frequenti non aumentino necessariamente la protezione dal malware, e non possono sostituire la difesa proattiva garantita dalla scansione euristica. Il test di AV-Comparatives (disponibile sul sito www.AV-Comparatives.org) ha confrontato la frequenza di aggiornamento degli antivirus e le dimensioni dei file di update attraverso una comparazione di quattro fra le maggiori soluzioni antivirus, dimostrando chiaramente come una forte difesa euristica proattiva combinata assieme ad aggiornamenti perlomeno quotidiani - uno dei punti di forza dell'antivirus NOD32 di ESET - offra agli utenti la migliore protezione contro il software dannoso, presente e futuro.

"NOD32 è il leader dei riconoscimenti Advanced+, avendo ricevuto il massimo titolo in ognuno degli ultimi cinque test. Ciò conferma la più elevata capacità di riconoscimento proattivo di malware rispetto a tutti i prodotti testati negli ultimi 12 mesi," ha affermato Andreas Clementi, project manager di AV-Comparatives ed esecutore del test. "Il test retrospettivo è cruciale, poiché dimostra la capacità del prodotto di bloccare gli attacchi zeroday senza avere il bisogno di aspettare ore per il rilascio degli aggiornamenti."

"Il rapporto di AV-Comparatives sottolinea l'importanza dell'euristica avanzata, uno dei capisaldi dell'antivirus NOD32 di ESET," ha dichiarato Andrew Lee, Chief Research Officer di ESET. "Secondo i risultati del test, Kaspersky rilascia nove volte più aggiornamenti di ESET, tuttavia riconosce solo un terzo del malware che ESET individua in maniera proattiva. Al contrario, ESET (NOD32) rilascia da 2 a 3 volte più aggiornamenti rispetto a Symantec e McAfee, ottenendo un tasso di riconoscimento proattivo da due a tre volte più alto."

"I risultati non sorprendono, poiché le nuove minacce zero-day non possono essere affrontate efficacemente col semplice uso di aggiornamenti di firme antivirus," ha affermato Paolo Monti, direttore tecnico di Future Time S.r.l, il distributore italiano di NOD32. "AV-Comparatives stima che dal 2002 il numero di nuovi virus sia raddoppiato ogni anno, mentre i produttori di antivirus stentano a tenere il passo con la grande varietà di nuovo malware rilasciato ogni giorno. Per quanto si possa esser rapidi nella distribuzione di nuovi aggiornamenti, essi non riusciranno mai a proteggere completamente i sistemi a causa della velocità con cui si evolvono le minacce. Inoltre, è necessario considerare che esiste sempre una finestra temporale tra il rilascio di un aggiornamento sui server del produttore e il suo effettivo impiego sui computer client dove sono installati gli antivirus, un intervallo di tempo che può dilatarsi in una maniera considerevole, a seconda del modo in cui è programmata la ricezione e la distribuzione degli aggiornamenti sui vari computer. Una difesa proattiva di livello superiore, bilanciata con il rilascio di nuove firme digitali, garantisce invece la migliore tutela possibile per il sistema."

Il rapporto di AV-Comparatives, pubblicato nell'Agosto 2006, ha preso in esame i tempi di rilascio e le dimensioni degli aggiornamenti dei quattro maggiori produttori di antivirus che hanno regolarmente ottenuto il riconoscimento ADVANCED+ da AV-Comparatives: ESET, Kaspersky, McAfee e Symantec. Lo studio non è stato eseguito su commissione, e nessuno dei produttori presi in esame era al corrente che nei mesi di Giugno e Luglio 2006 sarebbero state eseguite le rilevazioni per il test.

L'analisi di AV-Comparatives ha preso in esame anche il rapporto fra la frequenza di rilascio degli aggiornamenti e il relativo controllo-qualità. Le aziende che rilasciano aggiornamenti ogni ora soffrono generalmente di un aumento dei falsi positivi a causa del tempo estremamente limitato dedicato alla verifica di errori e bug eventualmente presenti nell'update. La sfida per i produttori di antivirus è riuscire a individuare il corretto bilanciamento fra la protezione euristica proattiva e il flusso continuo di aggiornamenti.