"Flame", allarme super-virus una minaccia senza precedenti

Individuato un malware di potenza mai riscontrata finora. Progettato per lo spionaggio industriale, è in grado di infettare macchine in molteplici modalità, e segue gli attacchi di Duqu e Stuxnet. L'esperto: "Una nuova fase della guerra informatica"

L'ALLARME ARRIVA da Kaspersky Lab, produttori di antivirus, che annunciano la scoperta di un programma nocivo altamente sofisticato, ampiamente utilizzato come arma informatica per compiere attacchi in diversi paesi. Si chiama "Flame" ed è caratterizzato da complessità e funzionalità superiori rispetto a tutte le precedenti minacce informatiche. Un vero e proprio super-virus evoluto, in grado di sottrarre informazioni importanti tra cui i contenuti visualizzati sul display del computer, ma anche informazioni sui sistemi, file archiviati, contatti e conversazioni audio.

Virus evoluto. Il malware è stato scoperto durante un'indagine commissionata dall'International Telecommunication Union (ITU). Il programma nocivo si chiama tecnicamente Worm.Win32.Flame ed è stato progettato per lo spionaggio informatico. Il malware è stato nascosto per oltre due anni, dal marzo 2010. Grazie alla sua estrema complessità e per la natura degli attacchi mirati, nessun software di sicurezza è stato in grado di rilevarlo.

La scoperta è avvenuta in maniera inattesa, mentre gli esperti di sicurezza lavoravano all'identificazione precisa di un ulteriore e ancora sconosciuto programma nocivo, denominato Wiper. Un virus che ha cancellato i dati su un elevato numero di computer nella regione dell'Asia Occidentale. Questo particolare malware era già stato scoperto, ma durante l'analisi degli incidenti, gli esperti si sono imbattuti in Flame.

Spionaggio e furto. L'obiettivo principale di Flame sembra essere lo spionaggio informatico, attraverso il furto di informazioni da macchine infette. Tali informazioni vengono quindi inviate a server di comando e controllo dislocati in diverse parti del mondo. La diversa natura delle informazioni rubate, che può includere documenti, screenshot, registrazioni audio e intercettazioni del traffico di rete, lo rende uno dei più avanzati e completi strumenti di attacco mai scoperti prima d'ora. Il vettore dell'infezione deve ancora essere identificato, ma è chiaro che Flame ha la capacità di riprodursi su una rete locale utilizzando diversi metodi, tra cui la vulnerabilità della stampante e il metodo di infezione tramite la porta USB sfruttata da Stuxnet.

Arma informatica. Anche se le caratteristiche di Flame sono molto diverse da quelle di Duqu e Stuxnet, due potenti malware industriali, la geografia degli attacchi, l'utilizzo di uno specifico software per le vulnerabilità e il fatto che solo i computer selezionati vengano presi di mira, indicano che anche Flame appartiene comunque alla stessa categoria delle armi informatiche più importanti.

Eugene Kaspersky ha dichiarato, a proposito della nuova minaccia: "Stuxnet e Duqu appartenevano ad una sola catena di attacchi, Flame sembra appartenere ad un'altra fase della guerra informatica. E' importante rendersi conto che le armi informatiche possono essere utilizzate per attaccare qualsiasi paese. A differenza di una guerra convenzionale, i paesi più sviluppati sono in realtà i più vulnerabili in questo caso".

28/05/2012