Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di martedì 31 marzo 2015

SOLUZIONI TECNOLOGICHE

I mercenari della Rete

di **Teamsystem.com**

Non hanno volto né nome, mantengono le distanze dalle agenzie governative e agiscono nell'ombra per creare reti di spionaggio informatico attraverso l'uso di virus. A svelare l'esistenza dei nuovi gruppi di **hacker** al soldo dei governi mondiali è stata **Kaspersky**, che in queste ultime settimane ha individuato due gruppi autonomi che operano principalmente in medio oriente. Grazie alle indagini degli analisti di sicurezza ora sappiamo quali strumenti utilizzano e come sono riusciti a creare un sistema di spionaggio che da quasi vent'anni tiene sotto controllo migliaia di computer.

Il gruppo Equation

La scoperta di **Equation**, secondo quanto raccontano gli stessi esperti di sicurezza, è avvenuta quasi per caso. Gli analisti stavano studiando i malware individuati su un computer infettato da **Regin**, un super-virus scoperto qualche mese prima, quando si sono accorti che sul disco fisso del PC erano presenti altri virus. In particolare la loro attenzione si è concentrata su un trojan, un malware che consente al suo autore di spiare le comunicazioni in ingresso e in uscita dal computer, così come di rubare documenti e informazioni sensibili senza che il proprietario se ne accorga. Si tratta di un tipo di virus piuttosto comune, ma quello rintracciato dagli esperti **Kaspersky** aveva caratteristiche molto particolari, che nessuno aveva mai visto prima. Dopo settimane di studio, hanno concluso che il virus viene utilizzato da un team di pirati che hanno battezzato come "Gruppo Equation" e che potrebbe essere attivo addirittura dal lontano 1996.

Un virus indistruttibile

Tutti gli strumenti di hacking usati dal gruppo Equation utilizzano sistemi crittografici per nascondere la loro presenza. Il trojan individuato dagli esperti, però, sfrutta una tecnica di camuffamento che non ha precedenti. È infatti **in grado di modificare il firmware dell'hard disk**, cioè il software che permette il funzionamento del disco stesso. Nascondendosi in questo settore, riesce a sfuggire a qualsiasi controllo antivirus e, cosa ancora più importante, non può essere rimosso nemmeno con una formattazione. Insomma: se anche il computer infettato venisse cancellato e su di esso fosse reinstallato il sistema operativo, il trojan tornerebbe a funzionare come se nulla fosse.

La scelta delle vittime

A convincere gli analisti del fatto che si trattasse di un gruppo di alto livello sono stati anche altri indizi. Per i suoi attacchi, Equation usa un vero arsenale di strumenti software, che vengono scelti a seconda delle esigenze. Il primo attacco, però, avviene sempre con un malware che è stato battezzato **DoubleFantasy**. Questo ha lo scopo di compromettere il computer e analizzarne il contenuto, per capire se il bersaglio possa essere considerato "interessante" per gli scopi del gruppo. Solo in questo caso i pirati di Equation installeranno trojan più complessi per rubare le informazioni che gli servono. La selezione delle vittime non lascia molti dubbi sul tipo di dati che interessano a Equation. I loro malware sono stati rintracciati in computer all'interno di **organizzazioni militari e governative**, centri di ricerca, aziende che agiscono nel settore dell'energia atomica e dell'estrazione del petrolio, società di telecomunicazione e anche in reti televisive e giornali. I Paesi interessati comprendono Iran, Russia, Siria, Nigeria, Somalia e altri stati dell'area mediorientale.

L'ombra degli 007 USA dietro a Equation

Per chi lavorano i pirati di Equation? A indicare la pista statunitense non sono soltanto le tipologie dei bersagli, ma anche alcune caratteristiche tecniche dei software che usano. In particolare, uno dei malware individuati sfrutta per i suoi attacchi una tecnica che è stata usata in seguito per **Stuxnet**, il virus creato nel 2010 da Stati Uniti e Israele per colpire una centrale per l'arricchimento dell'uranio in Iran. Anche se gli analisti di Kaspersky precisano di non essere in grado di affermarlo con certezza, il collegamento tra Equation e i servizi segreti **di Barack Obama** è quindi il più probabile. Come minimo, il gruppo di Equation ha avuto contatti con quello che ha sviluppato Stuxnet, collaborando per fornirgli un metodo che gli consentisse di infettare i computer iraniani.