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

Edizione di martedì 16 dicembre 2014

SOLUZIONI TECNOLOGICHE

Regin, il virus "scongelato"

di **Teamsystem.com**

"Non abbiamo mai visto nulla di simile". È stato il commento degli esperti di sicurezza quando hanno analizzato il codice di **Regin**, un trojan scoperto quasi casualmente due anni fa. Eppure questo software maligno era in circolazione almeno da 6 anni e nessuno se n'era accorto. Regin, che deve il nome all'inversione del termine "in Reg" ovvero "nel registro", usa tecniche di mimetizzazione mai rilevate prima. Ecco di cosa si tratta.

Un virus a pezzi

Gli analisti che lo hanno studiato, hanno scoperto che il codice di Regin è **suddiviso in 5 parti**. L'unica "visibile" è la prima, che appare come un innocuo processo di sistema.

Tutte le altre sono nascoste tramite un complesso sistema di crittografia che impedisce all'antivirus di "leggerne" il codice come avviene di solito. Quando il virus si attiva, ogni parte viene avviata in sequenza, fino ad arrivare alle ultime due (la quarta e la quinta) che contengono le funzioni davvero pericolose. Queste comprendono sistemi di spionaggio in grado di catturare le schermate dal monitor, registrare ciò che viene scritto tramite tastiera e addirittura recuperare dall'hard disk i file che sono stati cancellati dal sistema. Uno degli aspetti più inquietanti riguardo Regin, è che la versione individuata è ormai vecchia. I componenti del virus ritrovati sui computer risalgono infatti a una versione che non dovrebbe essere più attiva dal 2011. Sembra che il virus sia stato "richiamato" in quell'anno attraverso un comando inviato via Internet. Se tutto avesse funzionato a dovere, si sarebbe cancellato da solo e nessuno ne avrebbe mai scoperto l'esistenza. Però qualcosa è andato storto. Probabilmente i computer su cui è stato individuato sono stati scollegati da Internet prima che il comando di autodistruzione fosse inviato, lasciando così delle tracce inaspettate dai suoi creatori.

Un codice multiforme

L'aspetto più sorprendente di Regin è la sua struttura in moduli, proprio come alcuni software commerciali. Questo permette ai suoi creatori di modificarne le caratteristiche, aggiungere nuove funzioni e adattarlo all'ambiente in cui si trova. Tutto ciò usando un sistema di aggiornamento a distanza simile a quello di un qualsiasi altro programma. I dati, però,

vengono inviati attraverso una connessione nascosta che ne impedisce il rilevamento. Tra i moduli analizzati, gli esperti di sicurezza hanno individuato programmi estremamente sofisticati. Uno di questi, utilizzato per infiltrare i sistemi di un'azienda di telecomunicazioni, permetteva ai pirati informatici di prendere il controllo di tutta la rete GSM, ovvero quella che gestisce le comunicazioni dei telefoni cellulari. Attraverso Regin era possibile intercettare le chiamate o addirittura isolare un'intera zona del Paese.

Chi è l'autore di Regin?

Chi lo ha studiato non ha dubbi: Regin è uno dei malware più complessi mai apparsi su Internet. Nei loro commenti, gli analisti lo paragonano spesso a **Stuxnet**, il virus realizzato dai servizi segreti americani e israeliani, utilizzato nel 2010 per sabotare le centrali nucleari iraniane. Anche in questo caso, tutti gli indizi portano a pensare che dietro il virus ci sia un'organizzazione di intelligence di un Paese occidentale. Lo sviluppo di Regin, infatti, avrebbe richiesto grandi investimenti e mesi, se non anni, di lavoro. Qualcosa alla portata solo di un governo. Gli esemplari del virus rintracciati sono poco più di cento, ma tutto fa pensare che la rete di Regin fosse molto più estesa. Bisogna tenere presente che si tratta di semplici "tracce" lasciate dopo il suo smantellamento. Il dubbio, però, è che la rete sia stata sostituita da una nuova, ancora più efficace. Nel corso delle indagini, infatti, è stata individuata una porzione di codice simile alle altre, ma con una differenza fondamentale: ha un'architettura a 64 bit, in grado quindi di funzionare sui sistemi operativi più recenti. Questo elemento porta gli esperti a una conclusione: **a partire dal 2011, la vecchia versione è stata semplicemente sostituita con una nuova, di cui non si sa ancora nulla di preciso.** Ma quali sono i veri pericoli derivanti da un virus come Regin? Per capirlo, possiamo riprendere il caso di Stuxnet, che ha caratteristiche simili. Quando è comparso sul Web, il trojan creato dai **servizi segreti USA** ha causato un grandissimo allarme. Stuxnet, infatti, conteneva funzioni e strumenti che normalmente i pirati informatici non sono in grado di creare. **Una volta in circolazione**, però, **il virus poteva essere copiato e analizzato da chiunque.** La scoperta di Stuxnet ha permesso ai pirati informatici di venire a conoscenza di tecniche che fino a quel momento erano sconosciute. In particolare, il virus permetteva di controllare particolari sistemi che oltre a gestire il funzionamento delle centrali nucleari, sono usati normalmente per gestire i processi industriali in tutte le fabbriche di grandi dimensioni. I cyber-criminali quindi, si sono trovati tra le mani uno strumento che permetteva loro di creare una nuova generazione di malware in grado di sabotare un'intera fabbrica. Con Regin, si corre esattamente lo stesso rischio. Utilizzando la sua architettura, si potrebbero creare dei trojan di "nuova generazione" estremamente efficaci e difficilissimi da individuare anche con un normale antivirus.