Spyware governativi: realtà o leggenda?

Una recente indagine del gruppo CCC (Chaos Computer Club) ha rivelato la presenza delle autorità tedesche nella realizzazione di una backdoor.

Rossano Ferraris

Non è sicuramente il primo caso nella storia della sicurezza informatica e proprio per questo motivo è interessante approfondire il discorso per renderci consapevoli che la presenza di malware governativi a fini anti-terroristici (si spera!) è una pura realtà e non una leggenda da film di fantascienza.

Che cosa sono gli spyware governativi

Gli spyware governativi sono essenzialmente dei piccoli software (trojan) realizzati per essere installati sui computer o reti di computer con lo scopo di catturare informazioni nel corso di importanti investigazioni criminali. Tali operazioni vengono svolte da parte delle forze di polizia e/o servizi.
In linea di principio i trojan realizzati su commissione governativa sono in grado di intercettare email, traffico VoIP, scandire hard disk e registrare conversazioni audio e video.
Questo tipo di software cattura i dati e li invia a un server centrale che si occuperà di analizzarli senza che l'utente 'spiato' se ne accorga: tecnicamente questo trojan viene definito 'spyware'.
I vari governi hanno approcciato questo tipo di strumento in diversi modi: in Svizzera, per esempio, è stato riportato che le agenzie governative, incaricate di condurre indagini digitali, collaborano con i vari ISP (Internet Service Provider) per la registrazione di conversazioni tramite spyware installati sui pc dei criminali.
Come pure in Germania tali agenzie possono impiantare spyware nei pc di sospetti criminali di alto profilo (terrorismo internazionale, mafia, ecc.) attraverso lo strumento delle e-mail mediante tecniche di "social engineering" usate spesso nei noti attacchi di phishing.

Rossano Ferraris, senior research engineer per Total Defense Inc.

Il caso tedesco

La presenza di trojan o spyware governativi può avere un senso quando si tratta di sicurezza nazionale e/o internazionale perché in questo contesto lo spyware da installare ha un target ben preciso e fortemente mirato.
Il discorso cambia notevolmente però quando spyware di questo calibro vengono diffusi 'in the wild', ossia pubblicamente distribuiti su Internet e senza un target specifico (tipicamente quello che viene fatto dai criminali informatici).
Da qui il caso che in Germania ha suscitato un giustificato clamore dopo la

scoperta di un trojan (spyware) che pare abbia origini dalle agenzie governative.
Il CCC (Chaos Computer Club) ha accusato il governo tedesco di aver rilasciato una backdoor (spyware) 'in the wild' .
Inviata al gruppo CCC in modalità anonima questa backdoor è stata studiata con molta attenzione e dell'analisi effettuata si è scoperto che oltre ad avere funzionalità di intercettazione dati essa è anche in grado di controllare in modalità remota il pc infetto, avviare altri programmi e fungere da keylogger (registrazione di ogni tasto premuto dall'utente del pc infetto) per applicazioni come Firefox, Skype, MSN Messenger e altri.
Secondo l'analisi svolta dal gruppo CCC, questo malware proviene da mani autorizzate dal governo tedesco che il gruppo stesso accusa pubblicamente su vari blog locali attirando ovviamente l'attenzione di molti media internazionali.

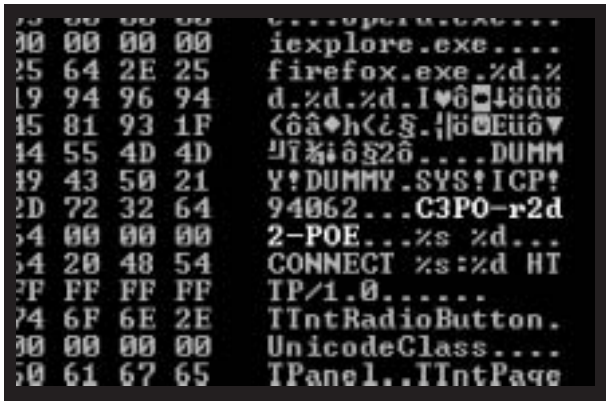

Figura 1 – Porzione di codice usata dal trojan tedesco per iniziare una trasmissione di dati nascosta

Conclusioni

Siamo di fronte a un discorso che sicuramente solleva tanti interrogativi e perplessità da parte del pubblico soprattutto quando veniamo a conoscenza del fatto (che non costituisce alcuna novità) che molti Paesi adottano questi strumenti per combattere il crimine in nome della sicurezza nazionale.
Basti pensare che, solo per restare in Europa, Paesi come la Svizzera, Austria, Romania, Cipro, Spagna (solo per citarne alcuni) hanno già sviluppato e usano strumenti di questo tipo.

Rossano Ferraris

Rossano Ferraris è laureato in Informatica e possiede le certificazioni SANS (GCIH, GCFA, GREM).
Attualmente ricopre il titolo di senior research engineer per Total Defense Inc. (www.totaldefense.com) ex divisione di CA Technologies ISBU.
È membro e co-fondatore del team ISI (Internet Security Intelligence) all'interno del Dipartimento di Ricerca della ISBU (Internet Security Business Unit) con la responsabilità di guidare l'area EMEA nello studio, analisi e tracciamento delle minacce emergenti.
Consulente presso la Procura della Repubblica e le Forze dell'Ordine in materia di analisi forense e tematiche legate ai crimini informatici in Italia.
È inoltre socio AIPSI (capitolo italiano ISSA) e impegnato in attività di sensibilizzazione attraverso interventi pubblici e la scrittura di pubblicazioni sulle insidie provenienti dalla rete.
Rossano Ferraris è co-autore del libro "Qualcuno ci spia: spyware nel tuo pc", edito da Mondadori (2005) e ideatore del blog "SecuritySurfer" (www.securitysurfer.it).

A questo punto qualcuno potrebbe pensare che tali strumenti siano illegali ma attenzione! Qual è il confine tra legalità e illegalità quando subentra la sicurezza nazionale e internazionale?
In questo caso la sfera legale e quella illegale tendono a sovrapporsi e il limite che li contraddistingue può essere non più visibile.
Nasce pertanto un nuovo contesto semantico diretto da regole diverse da quelle con le quali siamo abituati a convivere ma comunque pur sempre realizzato per garantire la sicurezza dei cittadini di un Paese.
Ovviamente si presenta un grave problema quando le regole di questo nuovo contesto non sono rispettate e cioè quando strumenti di questa potenzialità vengono lanciati 'in the wild'.
È possibile giustificare uno spyware lanciato 'in the wild' in nome della sicurezza nazionale?
La risposta è semplice: non è possibile! E il caso tedesco è un esempio di incidente governativo che necessita di risposte chiare perché un cittadino o utente che sia deve essere in grado di capire chi è il vero nemico della sua stessa libertà.