Dalla produzione di componenti tecnologici al Cyber spionaggio

di Mario Avantini

Nuovi allarmi inquietanti: secondo fonti di intelligence USA le l'attuali aziende commerciali cinesi hanno la capacità di accedere in modalità remota alle attrezzature di comunicazione vendute negli Stati Uniti e nei Paesi occidentali. La rivelazione ha determinato allarme circa l'eventuale presenza di backdoor nei dispositivi di comunicazione che potrebbero consentire a un Paese ostile di disabilitare l'infrastrutture di telecomunicazioni e secondo gli analisti del Pentagono, la Cina sarebbe in grado di poter operare in tale direzione. Un altro aspetto inquietante riguarda la capacità di controllo da remoto di dispositivi di trasmissione che possono essere sfruttati per fini di cyber-spionaggio in campo militare e civile, nel furto di tecnologie, segreti commerciali e altre informazioni riservate.

Durante le ultime settimane diverse notizie diffuse su internet riguardavano la presenza di una backdoor in un microchip prodotto in Cina e utilizzato dai militari degli Stati Uniti, l'annuncio non è isolato, infatti, anche la società ZTE e Huawei sono state accusate di introdurre circuiti stealth e software per consentire il controllo remoto dei dispositivi venduti. I sospetti sono motivati anche dal collegamento diretto tra aziende e governo cinese. Huawei (ufficialmente Huawei Technologies Co. Ltd.) è una multinazionale cinese che opera nel networking, telecomunicazioni e società di servizi. È il secondo più grande fornitore di attrezzature mobili e infrastrutture di telecomunicazione nel mondo dopo Ericsson, coprendo settori strategici in molte nazioni occidentali.

Alla Huawei è stato spesso contestata la sua eccessiva “vicinanza” al governo cinese e all’esercito tanto da immaginare che l’azienda sia sotto il totale controllo del governo, sottolineando che Ren Zhengfei, fondatore della società, ha servito come ingegnere dell'Esercito di Liberazione del popolo cinese, nei primi anni 1980. Contestazioni alla Huawei non sono di origine recente, più volte, in passato è stata accusata di operare per conto del governo cinese per la realizzazioni di apparati che consentissero azioni di censura sulla rete, altre per azioni di spionaggio fino agli attacchi informatici come l’operazione GhostNet.

Huawei, sospettata di sfruttare le telecomunicazioni per fini di intelligence con l'introduzione di backdoor nei suoi prodotti, continua a vendere tecnologie di comunicazione negli Stati Uniti, anche se attualmente iniziano a prendere una direzione diversa: infatti la joint venture tra Symantec e Huawei Technologies è finita perché le aziende di sicurezza informatica americane temevano che la collaborazione con il produttore cinese delle telecomunicazioni avrebbe avuto un impatto sensibile sulla sua attività. In particolare, il governo degli Stati Uniti non poteva dare a Symantec accesso alle sue informazioni classificate. Le informazioni potrebbero essere utilizzate da governi ostili per compiere attacchi informatici e attività di cyber-spionaggio in un periodo non lontano . Sul fronte interno il governo degli Stati Uniti, consapevole della sua vulnerabilità, si sta muovendo per la definizione e l'attuazione di strategie informatiche volte a rafforzare i propri sistemi, gli eventi degli ultimi mesi hanno dimostrato che i rapporti con gli appaltatori sono l'anello più debole della catena di sicurezza.

Un altro motivo di preoccupazione deriva dai rapporti che la Huawei ha con l'Iran: la sua infrastruttura informatica e i protocolli di sicurezza si basano appunto sulla tecnologia della società di telecomunicazione cinese Per questo motivo gli analisti statunitensi temono che gli iraniani potrebbe accedere alla stessa backdoor per compromettere la difesa degli Stati Uniti.

Secondo l'agenzia Reuters la ZTE Corp, quarto fornitore al mondo di telefonia portatile, in uno dei suoi modelli di telefoni cellulari venduti negli Stati Uniti contiene una vulnerabilità che potrebbe consentire di essere usato come telecomando di un ricevitore. La backdoor è presente un modello di punta di ZTE basato sul sistema operativo Android, è il primo caso segnalato sulla piattaforma e molti esperti sono convinti che l'evento non sia casuale. La presenza di una backdoor pone di nuovo il problema di hardware certificati, specialmente se lo stesso è parte integrante di strutture critiche come sistemi di comunicazione di un paese. Il Bollettino G2 (accordo informale tra Stati Uniti d'America e Cina) "Minaccia Cinese: Shutdown delle telecomunicazioni", rivela che l'opzione backdoor chip potrebbe essere usata prima di un azione militare contro gli Stati Uniti o paesi occidentali, grazie alla produzione di componenti contraffatti che hanno introdotto in sistemi sensibili d'arma statunitensi. Solo pochi mesi addietro funzionari della sicurezza del Department of Homeland Security, avvisarono in merito alla mancanza di controlli che consentono l'importazione di dispositivi che sono infetti da malware, spyware, backdoor e altri codici maligni che lasciano le unità vulnerabili. Backdoor e malware non sono più un segreto. Le backdoor possono essere facilmente nascoste in dispositivi internet dagli stessi produttori e potrebbero essere utilizzati per i criminali o azioni aggressive di stati.

The White House Cyber Policy Review, pubblicato all'inizio di quest'anno, ha avvertito che :

"L'emergere di nuovi centri per la produzione, il design e la ricerca in tutto il mondo solleva preoccupazioni circa il potenziale per una più facile sovversione dei computer e delle reti tramite manipolazioni dell'hardware o del software. I prodotti contraffatti hanno creato i problemi di approvvigionamento più visibili, ma esistono pochi esempi documentati di non ambigui, sovversioni deliberate. "

Inoltre bisogna sottolineare che le vulnerabilità hardware sono difficilmente individuabili, i dispositivi elettronici possono essere precaricati con spyware o malware; altri potrebbero essere utilizzati per disabilitare o estrarre i dati da sistemi di hosting o utilizzare il dispositivo infetto come punto di lancio per un attacco su tutta la rete a cui è collegato.

"Siamo sicuri circa l'origine hardware? Quali sono i principali problemi che può avere acquisizione hardware senza sapere l'esatta provenienza? " Questa è una domanda fondamentale da porsi.

Infatti, una delle prime conseguenze della crisi economica mondiale ha provocato il taglio dei bilanci nei settori privati, pubblici e militari, incoraggiando il basso costo. Questo ha comportato un drastico calo nell'uso dei rivenditori autorizzati e l'acquisto diretto dal produttore che si trova in Estremo Oriente. Un primo passo per difendersi da utilizzi aggressivi dell'hardware è quello di effettuare un'analisi preventiva del materiale stesso: la sua origine e la sua collocazione operativa. Si è scoperto, infatti, che installatori e/o appaltatori della Difesa degli Stati Uniti, procedevano all'utilizzo di materiale elettronico senza un adeguato controllo sugli apparati stessi. Il problema della contraffazione cinese di componenti elettronici, è molto più diffuso di quanto si pensasse inizialmente. Questi componenti contraffatti sono stati trovati anche in sistemi d'arma degli Stati Uniti, quali i sistemi missilistici, nei dispositivi di visione notturna e in vari aerei militari. Secondo

numerosi rapporti forniti dal Dipartimento della Difesa degli Stati Uniti, la Cina è considerata l'entità più attiva nello spionaggio informatico:

"I tentativi cinesi di raccogliere informazioni tecnologiche ed economiche degli Stati Uniti continuerà ad alto livello e rappresentano una minaccia crescente e persistente per la sicurezza economica degli Stati Uniti."

"La Cina è destinata a rimanere un paese collezionista di informazioni sensibili economiche e tecnologie, in particolare nel cyberspazio"

Pertanto, i rischi sono concreti, in molte occasioni è stato discusso circa i continui attacchi di hacker cinesi contro le reti americane. I funzionari del FBI, il Department of Homeland Security e la divisione sicurezza nazionale del Dipartimento di Giustizia composto un gruppo speciale chiamato "Team Telecom", incaricato di esaminare le richieste da parte di FCC aziende di proprietà estera. Si tratta di una situazione altamente critica: da un lato abbiamo preziosa opportunità di business, d'altra parte vi è la sicurezza della nazione, per questo motivo si è resa necessaria la formazione di questo gruppo di controllo per definire un accordo vero e proprio per preservare entrambe le necessità. In discussione vi è l'instradamento del traffico da parte dei vettori degli Stati Uniti (ad esempio, Verizon Communications Inc. e AT & T Inc) sulle reti la gestione dei quali è concesso in licenza da China Mobile. La preoccupazione per l' hardware che è destinato per un consumo di grandi dimensioni e quindi non può, per ovvie ragioni, essere sottoposto a severi controlli. Sistemi di automazione domestica, unità di controllo per dispositivi antifurto, dispositivi di rete per il business domestico di piccole dimensioni in queste aree, è relativamente facile infiltrare, modificare hardware e venderlo: è sufficiente praticare un prezzo a basso costo. Per i beni di consumo le società non sono attrezzate per la validazione di hardware e si ritiene che dispositivi simili possono anche essere modificati una volta giunti alle distribuzioni. Oggettivamente è una catena difficile da controllare.

Riferimenti:

- The White House Cyber Policy Review
- it.wikipedia.org/wiki/G2_(USA-Cina)
- www.tomshw.it/cont/news/chip...backdoor...dispositivi
- www.endoacustica.com › tecnologia
- www.dday.it/redazione/.../LUnione-Europea-contro-Huawei-e-ZTE
- www.agichina24.it/repository/.../in.../cina...-/usa-cyberspionaggio
- www.blitzquotidiano.it/.../usa-spionaggio-informatico-accuse-a-cina
- www.bitdefender.it/.../la-licenza--di-china-mobile-i--preoccupa