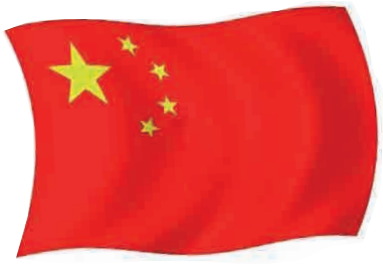

technology review CINA

Iran: attacco informatico all'arricchimento dell'uranio

In un articolo pubblicato nel fascicolo di gennaio-febbraio di "Technology Review" Cina e qui sintetizzato, si ipotizza che, in conseguenza del virus informatico che ha attaccato la centrale nucleare iraniana, la sicurezza dei computer industriali acquisterà un'importanza sempre maggiore.

Natanz, un paese nella provincia di Isfahan, in Iran: qui, l'attenzione della International Atomic Agency è rivolta alla centrale di arricchimento dell'uranio. Nel corso di una ispezione condotta nel gennaio del 2010, un gruppo di investigatori della stessa agenzia aveva scoperto che gli iraniani avevano installato migliaia di centrifughe all'interno della camera di arricchimento della centrale. Questi macchinari in seguito erano stati rimossi per verifiche, oltre che per prevenire il contrabbando di materiali radioattivi.

Si è scoperto, però, che a distanza di pochi mesi l'Iran ne aveva già rimpiazzate 2.000. In circostanze normali, nel caso di difetti nei materiali o altri problemi, la centrale di Natanz avrebbe dovuto sostituire intorno al 10 per cento delle sue 8.700 centrifughe, ovvero circa 800. Le autorità iraniane si erano rifiutate di spiegare la sostituzione delle 2.000 centrifughe.

La International Atomic Agency ha autorità sull'uso dei materiali radioattivi e non sugli equipaggiamenti rimpiazzati. Era però chiaro che qualcosa aveva messo fuori uso le centrifughe. Si apprese in seguito tramite un rapporto privato che un virus molto complesso e distruttivo aveva attaccato i computer della centrale, danneggiando il programma iraniano di arricchimento nucleare con il fine di impedirne la capacità di produrre armi nucleari.

Esistono migliaia di virus informatici, ma questo è stato il primo a venire impiegato come arma da guerra informatica. Il 17 giugno 2010, Sergey Ulasen, direttore del dipartimento antivirus della società di sicurezza VirusBlokAda, con sede a Minks, in Bielorussia, ha dichiarato che, per quanto se ne sapeva, i computer iraniani infetti dal virus informatico erano stati riavviati più volte. Il suo team aveva analizzato campioni del virus e scoperto che ricorreva a un sistema di infezione e contagio definito 0-day (giorno zero).

Il sistema 0-day, l'arma più efficace degli *hackers*, è una minaccia che sfrutta i punti deboli dei computer, ignoti ad altri e persino ai loro programmatori. Quando uno 0-day riesce a penetrare un sistema di sicurezza, le informazioni vengono condivise tra gli *hackers* prima ancora che gli sviluppatori del sistema sotto attacco riescano a intervenire e proteggere gli utenti.

Lo 0-day è un virus molto raro. Le aziende di software antivirus scoprono ogni anno migliaia di nuovi virus, ma appena una manciata è di tale genere. In questo caso, il virus usa un *flash drive* infetto per trasferire i dati da un computer a un altro. Il punto debole sta nei file LNK di Windows Explorer di Microsoft. Una volta connessa la USB al computer, Explorer scansiona automaticamente il suo contenuto. In questo processo il codice malevolo si scarica silenziosamente in un file criptato. In occasione di una comunicazione ufficiale sul Security Forum, VirusBlokAda ha rivelato che il virus era stato rilasciato per la prima volta nel 2009 e da allora era stato migliorato e modificato per un totale di tre versioni, la terza delle quali era stata rilasciata nell'aprile 2010. Una versione di questo virus presentava certificati digitali originali della Realtek Semiconductor di Taiwan e di un'altra azienda di chip, la JMicron Technology.

Nessuno sa come gli *hackers* possano avere rubato i certificati originali delle due aziende. Gli unici indizi rivelano che dev'essersi trattato di qualcuno estremamente abile e munito di grandi risorse. Un gruppo di esperti ha determinato, inoltre, che l'obiettivo dell'attacco era il sistema di controllo Step7 della tedesca Siemens, un sistema con molteplici applicazioni, dall'industria alimentare a quella automobilistica, dalle stazioni petrolifere a quelle per il trattamento dell'acqua. Questo genere di PLC (*Programmable Logic Controller*) viene ampiamente utilizzato per controllare una varietà di motori, valvole e interruttori.

Lo Step7 è un software industriale di controllo che si basa su un modello di Windows. Generalmente, questi sistemi non sono soggetti ad attacchi perché non comportano particolari ritorni economici per gli *hackers*. Tuttavia, i programmi contenenti lo 0-day necessitano di particolari attenzioni perché rappresentano un campo ancora ignoto e in progressiva diffusione. L'analisi della distribuzione nazionale dei computer infetti ha mostrato che in massima parte si trovano in Iraq ed Iran (22 mila e 38 mila macchine infette), seguiti da Indonesia (6.700), India (3.700) e Stati Uniti (meno di 400). È spontaneo associare la sua particolare propagazione a origini militari.