PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4021 di mercoledì 31 maggio 2017

Un insolito caso di criminalità informatica

Quando i quotidiani danno notizie di attacchi per criminalità informatica, i bersagli principali sono per solito le istituzioni finanziarie, gli enti emittenti carte di credito e simili: il caso di un bersaglio insolito. Di Adalberto Biasiotti.

Qualche tempo fa l'ufficio australiano di meteorologia è rimasto vittima di un attacco informatico. I tecnici hanno rilevato una attività insolita su alcuni server e successivamente essi hanno scoperto che degli hacker erano riusciti a superare le barriere di sicurezza del sistema informativo ed erano riusciti a impiantare un RAT - remote access tool- nella rete.

Questo software apre una backdoor in una rete informatica, operando a distanza. L' hacker può quindi accedere alla macchina e può cominciare a sottrarre informazioni.

Questo software criminoso è stato utilizzato per rubare una quantità ancora da determinare di documenti e studi, oltre ad aver compromesso le parole chiave dell'intera rete.

Nello stesso tempo, anche il servizio meteorologico della Nuova Zelanda era stato attaccato da criminali, che, sulla base di tutte le informazioni disponibili, sembrano essere basati in Cina.

La domanda che ci si pone, a questo punto, è perché mai i criminali informatici cinesi abbiano attaccato questi due siti.

Il motivo alle spalle di questo tipo di attacco è il furto di tecnologie proprietarie, che sono state sviluppate da questi servizi meteorologici.

Il responsabile dei programmi di sviluppo ha dichiarato che gli specialisti interni lavorano da sei mesi fino a un anno per sviluppare nuovi modelli di previsione meteorologica. Un gran numero di attività commerciali, come ad esempio la aviazione, i servizi minerari, l'agricoltura e l'industria marittima sono pronti a pagare delle cifre significative per avere a disposizione delle previsioni meteorologiche estremamente accurate. Ecco perché la disponibilità di questi applicativi avanzati può fornire un vantaggio commerciale significativo.

In particolare, un dato, che forse non molti lettori conoscono, è legato al fatto che se l'accuratezza del modello è dall'1% all'1,5% migliore di altri applicativi presenti sul mercato, il valore commerciale cresce in maniera esponenziale.

Un altro aspetto critico nella gestione dei dati, utilizzati per previsioni meteorologiche, fà riferimento la possibilità di modificare i dati stessi.

Certamente molti lettori ricordano l'ormai famoso virus Stuxnet, che sembra sia stato sviluppato dagli americani e dagli israeliani e che è stato iniettato nel sistema informativo che governava le centrifughe, utilizzate per depurare l'uranio, nel 2010, nei laboratori nucleari dell'Iran. Le centrifughe andarono fuori controllo ed esplosero, proprio per l'attività di questo virus.

Ecco la ragione per cui alcuni studiosi hanno messo in evidenza che se un hacker fosse in grado di alterare i dati delle previsioni meteorologiche, le conseguenze potrebbero essere assolutamente devastanti.

Questo scenario da incubo può essere messo sotto controllo, almeno parzialmente, per il fatto che sono numerosi i servizi meteorologici, distribuiti in varie parti del mondo, che incrociano i loro dati.

Per dare un'idea della dimensione dei dati che vengono gestiti, una singola agenzia meteorologica può acquisire quattro terabyte di data ogni giorno, prelevandoli dalle proprie stazioni meteorologiche e da altre stazioni meteorologiche, distribuite nel mondo intero.

A fronte di questa mostruosa quantità di dati, occorre introdurre tecniche avanzate e non facili da realizzare, per proteggere i dati stessi.

Il problema si è posto anche in Europa, dove il compito di tenere sotto controllo eventuali attacchi informatici è stato reso obbligatorio dalla direttiva sulla sicurezza delle informazioni di rete.

Questa direttiva, adottata dal Parlamento europeo il sei luglio 2016, è il primo passo in una ben più vasta attività legislativa sulla sicurezza informatica, su cui l'Europa sta lavorando di lena.

Terremo informati i lettori su ulteriori sviluppi, cogliendo il destro di questo specifico attacco informatico per mettere in evidenza come nessuno possa ritenersi al sicuro da hackers sempre più competenti e quindi sempre più pericolosi.

Adalberto Biasiotti