Lettori: 1.015.000
Il Sole 24 ORE
24-OTT-2011
Diffusione: 291.405
Dir. Resp.: Roberto Napoletano
da pag. 25

CYBER SPIONAGGIO

«Attacchi» via web per 15mila aziende

di **Enrico Netti**

Hacker all'attacco delle aziende italiane, praticamente indifese contro il cyber spionaggio. A fine anno saranno oltre 15mila i server violati, quasi il doppio rispetto al 2009, con una perdita per il sistema Paese stimabile in circa 100 milioni di euro.

Gli obiettivi sensibili? In genere documenti: trattative riservate, informazioni indistriali e commerciali, brevetti, prototipi. Notizie top secret per qualsiasi impresa, il cui valore è quasi impossibile da quantificare. Asset chiave per ogni impresa che però non sono protetti con la stessa cura con cui vengono protetti gli uffici e gli impianti.

Si stima che il 90% delle società quotate sia a rischio di intrusioni informatiche e di cyber spionaggio. Vulnerabilità ancora più elevata per le Pmi. Le poche difese digitali non reggono e non sono in grado di resistere alle offensive che arrivano dai concorrenti o anche da vere e proprie bande organizzate. Forme di spionaggio industriale che spesso vengono scoperte solo a settimane o mesi di distanza.

Servizio ▸ pagina 25

Sicurezza digitale. Nel mirino degli hacker soprattutto brevetti e segreti commerciali **pag. 25**

Sicurezza. Il 90% delle società quotate è a forte rischio di subire intrusioni e spionaggio industriale

Brevetti nel mirino degli hacker

Sferrati attacchi contro 15mila aziende, il doppio rispetto al 2009

Enrico Netti

Offerte e trattative aziendali, brevetti, prototipi, segreti industriali e commerciali, e per finire le informazioni sensibili che le società quotate devono comunicare al mercato. Sono questi i dati più "ricercati" dagli hacker che colpiscono le imprese del nostro Paese secondo gli esperti di Maglan Group, società israeliana specializzata nella consulenza per la difesa delle informazioni digitali.

Un fenomeno in recrudescenza. Quest'anno secondo le stime della società israeliana i server italiani violati dovrebbero essere oltre 15mila, contro gli 8.450 del 2009, con una perdita per il sistema Paese intorno ai 100 milioni di euro. Negli Usa, per esempio, si stimano perdite per centinaia di milioni di dollari l'anno per il solo sistema finanziario.

Altro che caro bolletta, aumento delle materie prime o invasione di prodotti low cost dall'Oriente. Si chiama "cyber spionaggio" la nuova emergenza da cui le imprese italiane devono imparare a difendersi. Una minaccia invisibile che va a caccia di informazioni e documenti archiviati sui computer aziendali, mettendo a serio rischio assett intangibili e opportunità di sviluppo dell'impresa.

«Il livello di sicurezza delle Pmi italiane è estremamente basso - avverte Shai Blitzblau, amministratore delegato di Maglan Group -. Investono in buoni prodotti che troppo spesso non sono implementati in maniera adeguata». Situazione non sembra migliorare tra le grandi aziende. «Oltre il 90% delle società quotate alla Borsa italiana è a forte rischio di attacchi di cyber spionaggio, una reale minaccia alla loro competitività».

Il tema di questa arma usata anche dalla criminalità e dai governi stranieri verrà affrontato durante la conferenza «La sfida della cyber-intelligence al sistema Italia. Strategie e tattiche di information warfare e di network intelligence: dalla sicurezza delle imprese alla sicurezza nazionale» che giovedì si terrà a Roma.

«In futuro le aziende saranno sempre più il bersaglio preferito degli hacker sia sul fronte patrimoniale, per rubare denaro attraverso "operazioni" di Internet banking – conferma Antonio Apruzzese, direttore della Polizia Postale – sia su quello dello spionaggio industriale, che va ad alimentare il mercato "nero" mondiale dei dati. Infomazione in vendita perché «questi dati sono denaro».

Il tallone d'Achille delle nostre Pmi è la relativa indifferenza con cui si affronta il tema sicurezza informatica. «Visti i grandi rischi, invece, deve essere avvertita come una priorità dagli imprenditori» aggiunge Apruzzese. Grandi rischi, le cui conseguenze nel lungo periodo sono impossibili da immaginare, ma sottovalutate. «Troppo spesso non ci si rende conto che la minaccia è sempre più reale - rimarca Corrado Giustozzi, Security evangelist di Capgemini Italia – perché ogni giorno vengono creati virus e trojan specializzati proprio nello spionaggio industriale». Inoltre le spie digitali, una volta "entrate" in una società, ci restano fino a quando sono scoperte, una permanenza di lungo periodo. «La tecnica degli hacker punta a creare un "covert channel", un canale nascosto che permette di ricevere dal bersaglio un flusso costante delle informazioni che circolano al suo interno» spiega l'Ad di Maglan. Un *modus operandi* seguito, tra gli altri, dagli hacker che nel 2010 penetrarono nel Nasdaq. Secondo i nuovi dettagli emersi la scorsa settimana l'attacco sfer-

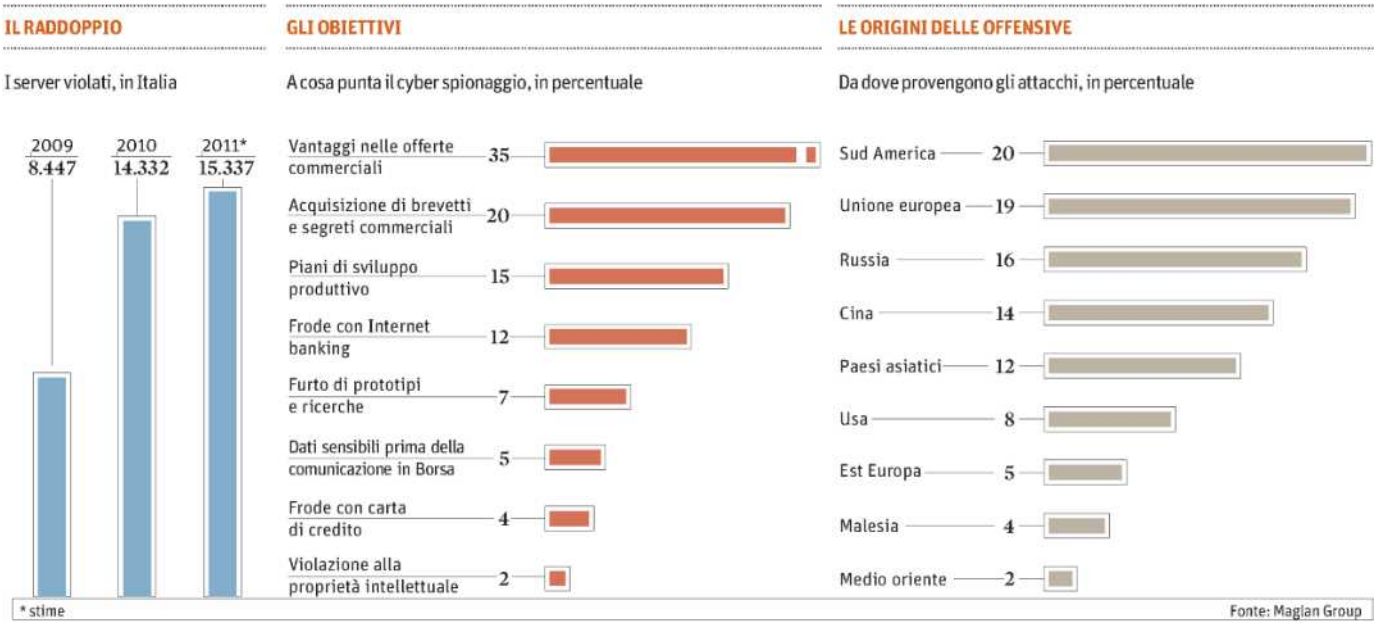
rato fu più grave di quanto si fosse pensato: i pirati furono in grado di accedere a documenti e comunicazioni del Board della borsa tecnologica Usa.

Da dove vengono gli attacchi, chi sono le bande di hacker che agiscono nel lato oscuro del Web? «La frammentazione di Internet permette alle bande criminali di muoversi praticamente indisturbate - sottolinea Andrea Rigoni, direttore generale del Global cyber security center - e per i prossimi anni i service provider dovranno investire di più per la protezione dei loro clienti».

Gli assalitori che si muovono in questo mondo oscuro possono essere bande di mercenari, società concorrenti, gruppi organizzati o singoli individui che vogliono dimostrare le loro capacità. Tra gli attaccanti spiccano i russi e cinesi, «i più evoluti» precisa il capo della Polizia Postale. Dai server basati in questi due Paesi arriva quasi un terzo degli attacchi alle aziende italiane, ma al primo posto spicca il Sudamerica. Non è da meno l'attività che ha come origine il Vecchio Continente: un'incursione su cinque arriva dai nostri vicini. Del resto, come non ricordare la spy story tra Ferrari e Mc Laren, un caso di spionaggio industriale che ha fatto storia.

enrico.netti@ilsole24ore.com

Cyber intrusioni contro l'Italia



Le principali aggressioni

Società ed enti i cui computer sono stati violati: la data indica quando è stato scoperto l'attacco

MASTERCARD, PAYPAL, VISA, POSTFINANCE

- Anonymous lancia una serie di attacchi a supporto di Julian Assange, il fondatore di Wikileaks

DICEMBRE 2010

GOOGLE

- Il sistema di email viene colpito. Si sospetta che l'attacco provenga dalla Cina

1° GIUGNO 2011

RSA

- Vengono rubate le informazioni relative alla piattaforma di sicurezza Rsa

MARZO 2011

SONYBMG, NINTENDO, INFRAGARD-ATLANTA (FBI)

- Intrusioni e sicurezza compromessa dei server

2-3 GIUGNO 2011

SONY PLAYSTATION NETWORK

- Il gruppo LulzSec saccheggia le informazioni personali di milioni di utenti

20 APRILE 2011

SITI DEL GOVERNO TURCO

- Anonymous colpisce diversi siti del governo turco per protestare contro la censura

10 GIUGNO 2011

FOX NETWORKS

- Il gruppo LulzSec ruba le informazioni personali dei partecipanti a X Factor Usa, oltre al database e le password dei dipendenti

22 APRILE 2011

FONDO MONETARIO INTERNAZIONALE

- C'è il sospetto che l'attacco sia stato causato da un "governo straniero"

POLIZIA SPAGNOLA

- Anonymous attacca il sito come reazione per l'arresto di alcuni presunti membri del gruppo

11 GIUGNO 2011

CITIGROUP

- Sottratti i dati di oltre 200mila clienti

MAGGIO 2011

BETHESDA GAME, SENATO USA

- Attaccato la società che sviluppa videogiochi e, per due volte in una settimana, il sito del Senato Usa

13 GIUGNO 2011

LOCKHEED MARTIN

- Attaccato il sito ma fermati prima del furto di dati sensibili

21 MAGGIO 2011

MITSUBISHI HEAVY INDUSTRIES

- Nel mese di agosto potrebbero essere state sottratte le informazioni di un missile anti nave giapponese

11 OTTOBRE 2011

PBS.ORG

- Lulzsec "deturpa" il sito del network tv, posta un falso articolo e ruba il database

30 MAGGIO 2011

Fonte: Lulz security, Reuters, Wall Street Journal