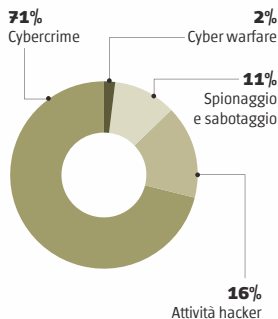


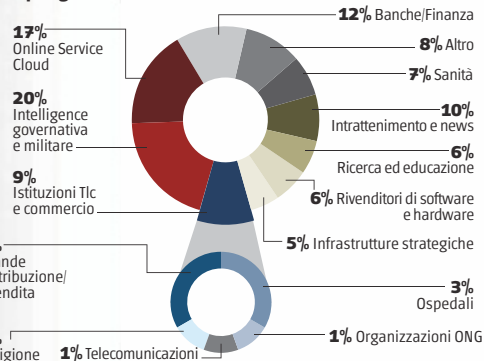
il commento ⇌

## AGGRESSORI E VITTIME

## Tipologia e distribuzione degli attaccanti



## Tipologia e distribuzione delle vittime



## L'ANALISI

di Fausto Biloslavo

## IL CONTAGIO DELLA PAURA

# Italia colpita dagli hacker

## Ora la sanità rischia il caos

*È allarme dopo l'attacco cibernetico mondiale  
Lombardia, per domani si temono ospedali in tilt*

Il cyber attacco mondiale che ha colpito 99 paesi potrebbe minacciare anche l'Italia, in particolare le strutture sanitarie. Si è espanso a macchia d'olio in mezzo mondo dopo aver infettato i computer di 48 ospedali, servizi di ambulanze e centri di igiene mentale inglesi. E da lunedì si teme il caos nelle strutture sanitarie lombarde. A tal punto che è stato lanciato l'allarme dalla società regionale Lombardia informatica. «È fortemente da consigliare a tutte le Aziende socio-sanitarie territoriali e Agenzie di tutela della salute - recita l'avviso - nonché alle postazioni di lavoro dei medici di medicina generale e dei pediatri di base, l'installazione della patch MS17-010 rilasciata da Microsoft». Ovvero l'aggiornamento che sconfigge Wannacry il virus informatico (ransomware), che ha colpito a livello globale e che si diffonde attraverso un allegato infetto della posta elettronica.

«Stimo che i computer attaccati nelle prime 24 ore possano essere 150mila» spiega a il Giornale, Andrea Zapparoli Manzoni, uno degli

autori del rapporto annuale Clusit sulla sicurezza informatica. Già lo scorso anno si era registrata un'impennata del cyber crime. Nel 2016 gli attacchi alla sanità sono aumentati del 102%. I gravi crimini informatici a livello globale sono stati 1050. Europol ha definito l'offensiva cibernetica «di dimensioni senza precedenti». L'obiettivo è ottenere un riscatto in bitcoin (l'equivalente di 500 euro) per sistema bloccato. «Attenzione che attacchi alle banche hanno fatto danni maggiori - spiega l'esperto del Clusit - Solo la banda Carbanak ha sottratto un miliardo di dollari in due anni e qualcosa». E nel 2016 un ospedale di Los Angeles ha pagato 17mila dollari di riscatto per tornare alla normalità.

In Inghilterra oltre alla strutture sanitarie è stata colpita la Nissan. In Francia la Renault ha dovuto bloccare una fabbrica. In Germa-

nia l'attacco si è concentrato sulla compagnia ferroviaria Deutsche Bahn. In Spagna e Portogallo sono rimaste bloccate due società telefoniche. Negli Stati Uniti sembra che solo il corriere Fedex abbia avuto problemi. In Russia un migliaio di computer del ministero dell'Interno sono stati infettati. Anche il più grande istituto bancario, la Sberbank, ha subito l'offensiva cyber criminale, ma l'avrebbe fermata. Le autorità indiane hanno ammesso che sono stati colpiti «il 25% dei computer della polizia». Gran parte dell'Asia, Cina compresa ha subito l'attacco. In Italia sono stati infettati i computer dell'università Bi-

## RICATTI VIA INTERNET

I crimini informatici sono stati 1.050 nel 2016. Alle banche sottratto un miliardo in 2 anni

cocca di Milano, ma l'attacco sarebbe stato «circoscritto». Raptor, l'antivirus, che può sconfiggere la bomba informatica si basa su tecnologia italiana. Negli ultimi due anni sono stati infettati nel nostro paese per ottenere un riscatto, pena la perdita dei dati, almeno il 30% di imprese. Lo scorso anno uno dei dieci attacchi più significativi al mondo è stato compiuto contro la Farnesina probabilmente ispirato dalla Russia, secondo il rapporto Clusit sulla sicurezza informatica.

A livello globale sono in aumento gli attacchi contro la grande distribuzione (+70%), il settore bancario e finanziario (+64%) e le infrastrutture critiche (+15%). La «guerra delle informazioni» è pure esplosa (+117%) ed il banale Phishing, le truffe via internet, si sono impennate del 1166%. Zappatori non ha mezzi termini: «Siamo ad una situazione d'allarme rosso».

## ADESSO SCONTIAMO L'EREDITÀ DI OBAMA

di Gian Micalessin

Altro che Mosca e Pechino. Uno dei mentori del disastro informatico che fa piangere il mondo è quel Barack Obama passato da Milano qualche giorno fa. Un Obama accolto a braccia aperte da Matteo Renzi e da quegli imprenditori che in queste ore si disperano per le possibili conseguenze del virus informatico «Wanna Cry». La responsabilità d'aver trasformato in prassi corrente l'intrusione nei computer e nei telefonini del resto del mondo è, infatti, tutta dell'ex presidente americano. È stato Obama nel 2009 a impiantare in seno alla Nsa (National Security Agency, l'agenzia Usa responsabile dello spionaggio elettronico) quel «Cybercommand» responsabile delle iniziative americane sul fronte della guerra cibernetica. E per quanto tutti cerchino di dimenticarlo è stato Obama ad autorizzare le operazioni, venute alla luce nell'ottobre del 2013, quando l'Nsa venne accusata d'intercettare i telefonini di Angela Merkel e di altri 34 leader internazionali. Per non parlare dei 70 milioni di dati rubati sulla rete telefonica francese, dell'inveterata abitudine d'origliare le comunicazioni dei principali leader dell'Unione Europea e delle indiscrezioni di Wikileaks secondo cui anche il governo Berlusconi finì nel mirino dei segugi elettronici di Obama. Nel caso di «Wanna Cry», il virus informatico che ha mandato in tilt gli ospedali britannici e le ferrovie tedesche esponendo al ricatto aziende pubbliche e private di 99 Paesi, tra cui anche Russia e Cina, le responsabilità