Rassegna stampa

Centro Studi C.N.I. 21 maggio 2017

Waypress
media monitoring

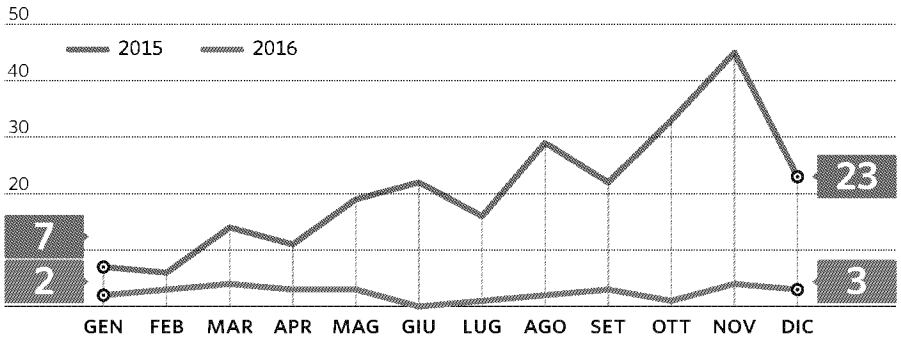
CYBER SICUREZZA

Sicurezza: l'anello debole? L'incoscienza del contesto

Cosa ci hanno insegnato i recentissimi attacchi? Non si sa quando, ma il prossimo obiettivo sarà l'Industria 4.0

di **Alessandro Curioni**

LA BIODIVERSITÀ DEL RANSOMWARE
Il numero di nuove specie di Ransomware che nascono ogni mese



Fonte: Trend Micro

L'attacco WannaCry ha mostrato al mondo che "il re è nudo", ma in ultima analisi i danni sono stati inferiori rispetto alla spettacolarità dell'offensiva, bloccata in tempi abbastanza rapidi grazie all'intuizione di un ricercatore molto fortunato. Possiamo guardare con ottimismo al futuro? Purtroppo no. I governi faticano a tenere sottochiave le nuove armi di distruzione di massa, i criminali si stanno evolvendo e nei prossimi anni si apriranno nuovi lucrosi mercati sui quali delinquere, primo tra tutti quello rappresentato dall'Internet delle Cose. Agosto 2016. Si svolge a Las Vegas il Defcon, incontro di specialisti in materia di sicurezza informatica, e vengono analizzati 23 sistemi IoT, compresi termostati e pannelli fotovoltaici, messi in commercio da 21 differenti produttori per scoprire che presentano 47 vulnerabilità. La notizia arriva dopo che nel dicembre 2015 un gruppo di hacker russi era riuscito a spegnere tre centrali elettriche ucraine grazie a un malware poi chiamato Black Energy, e un report di Aspen Tech in cui il 48 per cento dei gestori di infrastrutture critiche ritiene probabile che nei prossimi tre anni un attacco informatico possa disattivare un servizio essenziale e causare la perdita di vite umane. Tutto questo, combinato a una crescita costante degli incidenti ai sistemi industriali (SCADA e ICS), ha spinto i governi a intervenire. In Europa, in concomitanza con l'entrata il vigore del Regolamento in materia di protezione dei dati personali, è stata varata la Direttiva NIS (Network and Information Security), che ha imposto ai gestori di infrastrutture critiche e agli stati membri dell'Unione l'adozione di misure minime di sicurezza entro il prossimo biennio. Alla fine del 2016, invece, il Dipartimento per la Homeland Security statunitense ha pubblicato gli "Strategic Principles for Securing the Internet of Things". Un'iniziativa forse stimolata dall'attacco del marzo 2016 a un fornitore di servizi idrici che vedeva compromessi i sistemi di trattamento delle acque o quello più spettacolare con cui un ransomware, bloccando i meccanismi di gestione dei biglietti, ha permesso ai cittadini di San Francisco di viaggiare gratuitamente sulle metropolitane cittadine per diverse ore. Torniamo alla stretta attualità e rileviamo che Nissan e Renault, colpite da WannaCry, sono state costrette a interrompere l'attività in alcuni siti produttivi. Cosa sarebbe accaduto se il malware fosse stato realizzato per colpire i sistemi industriali? Oggi forse nulla di drammatico, ma domani, quando i paradigmi dell'Industria 4.0 saranno applicati potrebbe essere un'apocalisse. Essi prevedono l'integrazione orizzontale e verticale, che in combinazione con l'industrial internet porterebbe alla completa interconnessione tra fornitori, produttori e distributori, probabilmente all'interno di ambienti cloud. Una minaccia della virulenza di Wannacry, ma concepita per colpire sistemi ICS e SCADA, potrebbe mettere in ginocchio un comparto economico in poche ore. Un destino non diverso potrebbe toccare alle smart grid, magari con un attacco che parta da uno dei milioni di contatori intelligenti che stanno proliferando in tutto il mondo, sfruttando una qualche, oscura vulnerabilità. Scenari tanto apocalittici sono plausibili quanto più si osserva lo stato dell'arte delle soluzioni informatiche adottate. Il ciclo di vita dei sistemi industriali è molto lungo e ancora oggi sono estremamente diffusi sistemi operativi che risalgono a oltre venti anni orsono, non più supportati dai produttori anche in termini di sicurezza. Nel caso WannaCry la preoccupazione più grande era per Windows XP e Server 2003 per le quali non è stata immediatamente disponibile la correzione, proprio perché "fuori garanzia". Qualcuno potrebbe pensare che i nuovi sistemi saranno più "sicuri": di certo lo sono, ma esiste un problema. In ambito SCADA e ICS un requisito fondamentale è la compatibilità retroattiva, cioè la capacità di un sistema di potere interfacciarsi con tutti i suoi predecessori, questo implica che l'ultimo arrivato effettua il downgrade di se stesso, finendo per ereditare tutte le debolezze presenti nei dispositivi più vetusti. Può andare peggio? Sì, potrebbero pensarci dei terroristi.

– Presidente di Di. Gi. Academy