Wannacry e non solo, le cyber-armi della Nsa sono ancora in giro

- Arturo Di Corinto, 17.05.2018

Hacker's Dictionary. La rubrica settimanale a cura di Arturo Di Corinto

Nel 2017 un gruppo di *hacker* noto come ShadowBrokers informa un tale Jake Williams di essere in possesso di tutte le informazioni che lo riguardano.

Jake non è una persona qualsiasi, fa parte della *hacking unit* della National Security Agency, l'agenzia per lo spionaggio elettronico del governo americano.

Per dimostrargli che dicono la verità pubblicano sul suo stesso blog ogni riga del codice usato da Williams per attaccare i bersagli degli Stati Uniti e poi decidono di divulgare le sue pericolose cyber-armi.

Tra queste ce n'è una alla base del più grande attacco *ransomware* della storia, l'exploit EternalBlue, usato per bloccare i computer di mezzo mondo e farsi pagare un riscatto (*ransom*) per sbloccarli.

Secondo il glossario del Cert Nazionale un «exploit» è un «codice che sfrutta la vulnerabilità di un sistema permettendo l'esecuzione di codice malevolo, generalmente con lo scopo di acquisire i privilegi di amministratore della macchina colpita».

Ecco, questo *exploit* EternalBlue sfrutta una vulnerabilità di sistema delle macchine Windows non aggiornate, senza manutenzione, tipicamente quelle in uso alla Pubblica Amministrazione, mentre a quelle nuove e ben tenute gli fa un baffo. E infatti aveva bloccato ambulanze e pronti soccorso inglesi, ferrovie russe e porti baltici.

Eternal Blue viene utilizzato per installare la *backdoor* «DoublePulsar» e prendere possesso del singolo pc che infetta ma anche di prendere in ostaggio la rete in cui si trova.

È così che nel 2017 circa 300mila computer in 150 paesi sono stati bloccati dal ransomware Wannacry.

Eset, azienda di sicurezza slovacca con sede anche in Italia, oggi ci dice che EternalBlue è tornata a impazzare sulle macchine Windows non protette.

Secondo l'agenzia di stampa *AskaNews*, l'ultimo picco di infezione era coinciso con la campagna ransomware «Satan» ma EternalBlue aveva permesso di continuare molti attacchi informatici di alto profilo nei mesi a seguire.

Oltre a WannaCryptor, Petya, NotPetya ed ExPetya, aveva favorito la diffusione del *ransomware* BadRabbit prima di Natale.

E sempre secondo Eset è stato anche usato dal gruppo di cyberspionaggio Sednit noto anche come Fancy Bear e Sofacy per attaccare le reti Wi-Fi negli hotel europei.

Adesso si scopre che lo stesso *exploit* è stato utilizzato per diffondere crypto miner maligni.

I ricercatori di AlienVault hanno identificato una nuova famiglia di malware per l'estrazione

fraudolenta di cryptovalute, battezzata MassMiner.

A partire da una macchina Windows infetta, MassMiner si diffonde inizialmente sulla rete locale prima di tentare di propagarsi attraverso Internet.

MassMiner include una variante (fork) di MassScan, strumento in grado di eseguire la scansione Internet di server vulnerabili sui quali diffondersi in pochissimo tempo. Anche MassScan usa EternalBlue.

E questo è uno dei motivi per cui le associazioni a difesa della privacy e dei diritti digitali come Access Now hanno chiesto a più riprese al governo americano di non accumulare e di non tenere nascoste queste che sono vere e proprie cyber-armi, ma di avvisare subito chi può renderle innocue, le agenzie pubbliche e le aziende di informatica, per impedirne un uso incontrollato.

Post Scriptum: c'è però una buona notizia per l'italico cyberspazio. Alla Presidenza del Consiglio dei Ministri leggono *il manifesto* e dopo che la scorsa settimana abbiamo denunciato la mancata approvazione del decreto europeo sulla sicurezza cibernetica NIS, l'hanno finalmente fatto. Ieri mattina.