SECURITY NOTES

Petya: cronaca di un nuovo attacco

Da Giuseppe Augiero

Inviato il 05/07/2017

E’ passato poco più di un mese dall’infezione di **Wannacry**, che ha colpito un numero elevato di personal computer, ed ecco arrivare un nuovo allarme per la diffusione di un prevedibile nuovo ransomware: **Petya**.

Per capire cosa stia succedendo occorre fare un passo indietro nel tempo. Alcuni mesi fa un gruppo di hacker chiamato “**Shadow Brokers**” ha pubblicato una serie di exploit e il codice sorgente di alcune routine scritte dall’ NSA per accedere in maniera non autorizzata nei dispositivi elettronici di utenti tenuti sotto controllo.

Uno degli exploit diventato pubblico è **EternalBlue** che permette

l'accesso a un pc con Windows sfruttando alcune vulnerabilità di Samba (condivisione delle risorse). EternalBlue è stato usato da Wannacry come vettore di infezione al fine di permettere una sua veloce propagazione. Nel frattempo Microsoft ha rilasciato alcune patch per i suoi sistemi operativi in modo da evitare il facile contagio di Wannacry.

Come dicevo, a distanza di alcune settimane, ecco apparire Petya.

Da una parte era prevedibile l'arrivo di un nuovo ransomware che sfruttasse le funzionalità di EternalBlue ma dall'altra, con il rilascio degli aggiornamenti di **sicurezza** di Windows, la superficie di attacco e quindi il numero di pc potenzialmente infettabili doveva essere molto ridotto.

COME AGISCE PETYA?

Petya, una volta entrato in funzione, cifra il master file table (MFT) del pc rendendo inaccessibili i file presenti sul disco fisso. Di fatto, terminato il processo di infezione e di cifratura (circa 30/35 minuti), il PC non sarà più avviabile e i dati in esso contenuti non saranno più disponibili.

A differenza di Wannacry, Petya non solo sfrutta le vulnerabilità di Samba per infettare altri pc ma cerca di recuperare, dal pc appena infettato, le credenziali di altri sistemi per poi sfruttarle per accedervi e infettare un nuovo pc.

L'attacco, ancora più critico rispetto ai precedenti, sembra essere

partito dall'Ucraina ed ha coinvolto nomi illustri come la francese Saint Gobain, il sistema di monitoraggio delle radiazioni della centrale di Chernobyl, l'azienda pubblicitaria WPP, l'azienda petrolifera Rosneft, la multinazionale Mondelez, il porto di Rotterdam, una catena di supermercati e alcuni ATM in Ucraina e altri nomi famosi…

Per distribuire il malware inizialmente è stato utilizzato un aggiornamento corrotto di un famoso software di contabilità noto in Ucraina.

Con il passare dei giorni sta diventando certa la supposizione che Petya non sia un vero ransomware ma un **wiper** cioè un malware il cui scopo è cancellare e quindi rendere inaccesibili i dati degli utenti il cui PC è stato infettato. Il nome Petya era stato dato alla nuova minaccia informatica in quanto sembrava che parte del suo codice assomigliasse a un malware già in circolazione chiamato giustappunto Petya che cifrava l'MTF delle partizione NTFS e andava a modificare l'MBR.

Gli analisti dei laboratori di sicurezza di Kaspersky, invece, avevano segnalato che la nuova minaccia fosse ben diversa dal vecchio malware e l'avevano ribattezzata **NotPetya**. Recentemente alcuni esperti di sicurezza hanno scoperto che il nuovo Petya utilizza anche un altro exploit scritto dall'NSA e rilasciato da Shadow Broker il cui nome è **EternalRomance**.

Rimane anomalo il comportamento, in fase di richiesta di riscatto

(300 dollari in bitcoin), del nuovo malware in quanto, invece di generare una email ad hoc per ogni infezione, utilizza un unico indirizzo email (*wowsmith123456@posteo.net*) che è stato prontamente bloccato dal provider tedesco che gestisce il mailserver, quindi pagare il riscatto non serve a nulla.

Il consiglio, in generale, è non pagare mai, in quanto non è garantita la decifratura dei propri dati, foraggereste una attività criminale e compiereste un'azione illegale punita penalmente.

COSA FARE PER EVITARE ATTACCHI COME QUESTO?

- Tenere sempre aggiornato il proprio sistema operativo
- Fare backup e tenere una copia offline
- Usare un buon antivirus
- Fare molta attenzione con gli allegati che si ricevono per email

Giuseppe Augiero
attualmente, si occupa di Network Design e Sicurezza Informatica nel mondo della

Sanita' Pubblica. In passato ha progettato e curato la sicurezza perimetrale di una parte del core business di un Internet Service Provider Italiano e di un Asp Provider. Utilizza Gnu/Linux dai suoi albori, quando la versione del kernel era 0.99, Attualmente Debian-dipendente, è esperto di sicurezza informatica e definito "innovatore digitale"; è sensibile alle tematiche legate all'Open Source e alla Neutralita' della rete. Da oltre quindici anni tiene corsi e seminari in giro per l'Italia su argomenti tecnici e socio-economici relativi al mondo della sicurezza informatica, di Internet e di Gnu/Linux

ARTICOLI CORRELATI: CYBER SECURITY, IN EVIDENZA, PETYA, SICUREZZA

SUGGERITI PER TE:

Incidenti di sicurezza IT: i dipendenti pronti a nasconderli

Crittografia dei servizi web sufficiente a difendersi?

Obiettivo di Petya ExPetr le organizzazioni industriali