Cyber Threat Intelligence Report Petya-based Ransomware

Date : 28 giugno 2017

Il 27 Giugno 2017, sulla rete, si è registrata un'infezione su larga scala, derivante dalla diffusione di un ransomware basato su una variante del codice Petya.

Il malware si propaga sfruttando alcune recenti vulnerabilità di Office/Windows (denominata EternalBlue) ed, in particolare, una versione modificata dello stesso exploit impiegato nel ransomware WannaCry.

I principali target sono aziende localizzate in Ucraina, Russia ed Europa Occidentale e appartenenti a diverse industry. quali ad esempio terminal aeroportuali, aziende energetiche, banche, fabbriche, società di assicurazioni, servizi militari.

Il nuovo attacco ransomware Petya, avvenuto a circa un mese di distanza da quello denominato WannaCry, ha rilanciato l'allerta e la preoccupazione in merito alla sicurezza informatica.

Secondo varie fonti l'attacco avrebbe inizialmente utilizzato per la diffusione un aggiornamento infetto per la suite software MeDoc, un pacchetto software utilizzato da molte organizzazioni ucraine, paese da cui sarebbe appunto partito il virus.

Dopo aver preso il via da Kiev l'infezione si è poi propagata in Russia e in Europa sfruttando la vulnerabilità CVE-2017-0199 (detta EternalBlue), ripetendo in parte lo scenario già visto con WannaCry. La vulnerabilità EternalBlue è legata al protocollo SMB utilizzata sui sistemi Microsoft da Windows XP a Windows 2008 sulla porta TCP 445 o 139 a cui non è stata precedentemente applicata la patch Microsoft MS17-010.

Il ransomware utilizza anche le utility Psexec e WMI (Windows Management Instrumentation) che sono componenti lecitamente presenti nei sistemi Windows. Secondo l'analisi svolta da Group IB, il malware sfrutta anche la vulnerabilità CVE-2017-0144.

Per capire la portata dell'attacco, DeepCyber, azienda italiana specializzata in cyber threat intelligence, ha emesso, il 28 giugno ore 8.00, un primo report in italiano, per l'analisi e le raccomandazioni tecniche.

Per scaricare il report è sufficiente cliccare sul seguente link

DeepCyber_Incident-Report_PETYA-BASED RANSOMWARE