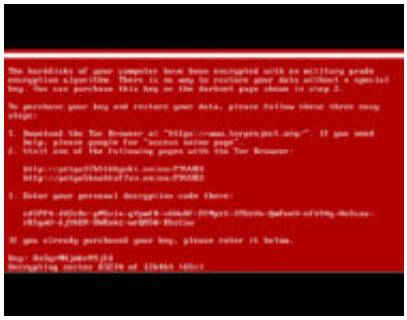
Petya o "NotPetya" - Il nuovo cyberattacco manifesto della guerra ibrida

Date : 28 giugno 2017



Dopo Wannacry è questo il nuovo attacco Ransomware che mette a dura prova la CyberSecurity mondiale

Il virus Petya sembra aver attaccato, in poche ore, più di 2000 utenti, i paesi più colpiti sono statti l'Ucraina: aeroporto di Kiev e Antonov, centrale nucleare di Chernobyl, metropolitana di Kiev, banche e imprese; Copenhagen: trasporti marittimi Moller-Maersk; Olanda: compagnia navale TNT; USA: compagnia farmaceutica Merck e il sistema sanitario Heritage Valley Health System. Nella lista rientrano anche tanti altre grandi aziende come il re degli snack Mondelez e la multinazionale dei servizi legali DLA Piper, l'agenzia pubblicitaria britannica Wpp, l'impresa di materiali edili francesi Saint Gobain, il gigante petrolifero russo Rosneft.

Lo stato più colpito, quello da dove si è propagata l'infezione, è l'Ucraina; gli hacker hanno infatti utilizzato gli aggiornamenti del software finanziario MeDoc utilizzato in larga scala nell'intero paese.

La prima reazione dell'Ucraina è stata quella di colpevolizzare la Russia, indicandola come la più probabile mandante. Ad oggi non si ha certezza di questo ma sembra affermarsi sempre di più l'ipotesi che questa sia una vera propria dimostrazione di potere o un atto intimidatorio, inserendo così il nuovo malware tra le cyber armi e delineando così le caratteristiche della nuova guerra nel cyber spazio.

Le similitudini tra il cyber attacco Petya (NotPetya/SortaPetya/Petna) e Wannacry sono; l'utilizzo dell'exploit EternalBlue, rubato all'Nsa, l'Agenzia nazionale per la sicurezza negli Stati Uniti ndr, e distribuito nel darkweb, progettato per sfruttare un bug nel server SAMBA (SMB) dei sistemi Microsoft, a questo si aggiunge anche l'exploit EternalRomance.

In aggiunta, il ransomworm codifica l'indice dei file nel file system NTFS (MFT) e sostituisce il settore di boot del disco fisso (per le partizioni in standard MBR) con un boot loader custom pensato per stampare a video il testo con la richiesta di riscatto in Bitcoin. Sembra che questo attacco si diffonda anche via e-mail.

Esiste fortunatamente un vaccino, un killswitch. Basta creare un file col nome **perfc** nella cartella **C:\Windows** e renderlo di sola lettura. Per coloro che cercano un modo veloce per eseguire questa procedura, è disponibile un file batch che segue in automatico questi passaggi.

Il file batch, realizzato da Lawrence Abrams, è disponibile al seguente link:

https://download.bleepingcomputer.com/bats/nopetyavac.bat

Altra raccomandazione, assicurati che tutti i sistemi siano aggiornati con la patch "MS17-010", ricordando a tutto il tuo staff “Think before You Click” (pensa prima di cliccare) quando riceve delle email al di fuori di quelle di ordinaria amministrazione.