Polizia di Stato

Polizia Postale e cyberattacco.

In relazione alla notizia dell’attacco hacker a livello globale compiuto attraverso un ransomware noto coi nomi WCry, WannaCry e WanaCrypt0r e rilevato a partire dal febbraio scorso, la Polizia Postale e delle Comunicazioni e in particolar modo il Centro nazionale Anticrimine Informatico per la protezione delle Infrastrutture Critiche - CNAIPIC, sta costantemente analizzando il fenomeno, intensificando le attività di monitoraggio e le procedure atte a garantire la massima sicurezza delle infrastrutture informatiche del Paese.Dalla serata di venerdì 12 maggio la Sala Operativa del CNAIPIC è in costante contatto con i referenti tecnici delle infrastrutture critiche informatizzate e, tramite il Nucleo Sicurezza cibernetica, con i componenti dell’Architettura di difesa Cyber nazionale.Costante il rapporto con gli organismi di cooperazione internazionale ed in particolare con il centro EC3 di Europol.Diramati dal CNAIPIC diversi alert di sicurezza con gli indicatori di compromissione relativi all’attacco hacker, utili per l’innalzamento del livello di sicurezza dei sistemi informatici.Dai primi accertamenti effettuati e dalle risultanze raccolte ad oggi, sebbene l’attacco sia presente in Italia dal primo pomeriggio di venerdì, non si hanno al momento evidenze di gravi danni ai sistemi informatici o alle reti telematiche afferenti le infrastrutture informatiche del Paese.In generale i comportamenti rilevati vedono: le vittime ricevono il malware via rete (non si hanno al momento evidenze di mail vettore dell’infezione). Il malware si installa infatti nella macchina “vittima” sfruttando il noto bug EternalBlue e deposita l’eseguibile *mssecsvc.exe* nella directory di sistema *C:\windows*.Si installa quindi come servizio e procede ad eseguire due attività parallele utilizzando diversi eseguibili. La prima attività consiste nel cifrare determinate tipologie di file come da link; https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168. La seconda provvede a propagare il malware sulla eventuale LAN presente sfruttando la vulnerabilità suddetta del protocollo SMB con le porte TCP 445 e 139. Questa seconda componente inoltre effettua scansioni in rete alla ricerca di nuovi target da infettare via SMB porta 445. Funziona in Ring 0, quindi potenzialmente foriero di maggiori danni di quanti fatti con la sola attività di cifratura. Non è ancora noto se è anche installato la backdoor DoublePulsar o altro.Stranamente, il codice sorgente contiene una richiesta *Open_Internet* (non proxy aware) verso un sito pubblico che, se raggiunto, blocca la seconda attività, quella di diffusione sulla rete.Non si escludono ulteriori problematiche legate alla propagazione di un’ulteriore versione di “WannaCry” 2.0, ovvero al riavvio delle macchine per la giornata di domani, inizio della settimana lavorativa.Pertanto per difendersi dall’attacco, oltre ad eseguire affidabili backup al fine di ripristinare facilmente i sistemi interessati in caso di cifratura da parte di WannaCry, si consiglia quanto prima di:**Lato client/server:- eseguire l’aggiornamento della protezione per sistemi Microsoft Windows pubblicato con bollettino di sicurezza MS17-010 del 14 Marzo 2017;- aggiornare il software antivirus;- disabilitare ove possibile e ritenuto opportuno i servizi: Server Message Block (SMB) e Remote Desktop Protocol (RDP);- il ransomware si propaga anche tramite phishing pertanto non aprire link/allegati provenienti da email sospette;- il ransomware attacca sia share di rete che backup su cloud quindi per chi non l'avesse ancora fatto aggiornare la copia del backup e tenere i dati sensibili isolati.Lato sicurezza perimetrale:- eseguire gli aggiornamenti di sicurezza degli apparati di rete preposti al rilevamento delle intrusioni (IPS/IDS);- ove possibile e ritenuto opportuno bloccare tutto il traffico in entrata su protocolli: Server Message Block (SMB) e Remote Desktop Protocol (RDP)**

14/05/2017