ESERCIZIO M4 D3 – 2

INFEZIONE MALWARE

SISTEMA INFETTATO DA MALWARE WANNACRY

1- BRAINSTORMING

Al momento sappiamo che un solo pc con windows 7 è stato attaccato dal ransomware WANNACRY. Dopo averlo studiato siamo venuti a conoscenza che si tratta più specificatamente di un cryptoworm: cioè un particolare tipo di malware che rende inaccessibili i dati dei nostri computer e, per ripristinarli, chiede un riscatto da pagare in bitcoin. Il malware colpisce chi ha il proprio computer collegato alla Rete e ha un sistema operativo Windows, dato che il software malevolo si propaga grazie all'exploit EternalBlue, uno strumento che sfrutta la vulnerabilità di un protocollo di condivisione di file di rete, SMB (Server Message Block), usato da sistemi Microsoft Windows.
La tesi più accreditata è che il malware si diffonda attraverso computer vulnerabili esposti su internet con le porte 139 e 445. Una volta che un solo computer di una rete locale viene infettato, il malware automaticamente si propaga usando il protocollo SMB; computer non aggiornati e reti esposte via SMB su internet possono essere infettati direttamente senza il bisogno di altri meccanismi, basta che siano accesi e accettino connessioni SMB.
Il contagio potrebbe quindi essere avvenuto tramite phising oppure come accaduto anche in Italia tramite chiavetta USB.
I files sono tutti criptati e tutti con estensione .wncry.

2- PRIMO INTERVENTO

Quindi come primo intervento penserei di tentare di isolare “fisicamente” il pc infetto dalla rete e fare un check su tutte le altre macchine. Creare un nuova regola di firewall sulla rete interna, temporanea, chiudendo qualsiasi comunicazione sulle porte 139 e 445 tentando di bloccare il traffico SMB in entrata e quindi isolare sistemi che potrebbero essere vulnerabili dalla rete.

3- CONTROLLO

Dato che si tratta di un problema superato dagli aggiornamenti, ovvero il ransomware è uscito un paio di mesi dopo il rilascio della patch di aggiornamento distribuita da Microsoft, farei un aggiornamento sia del sistema operativo che dei software antivirus di tutti i dispositivi che non sono stati infettati e che fanno parte della rete.

In più controllerei se sono stati fatti i backup e che non siano stati infettati, quindi una volta aggiornato tutto il sistema rifare una nuova copia di backup.

4- DECRIPTAZIONE

Esistono ormai diversi software in grado di decrittare wannacry; uno dei primi è stato un software, scaricabile da github, che si chiama WANADECRYPT che riesce, appunto, a risalire alla chiave per poter decifrare i files.

5- BEST PRACTICE

- Non cedere alla richiesta di riscatto da parte degli autori del ransomware
- Tenere il sistema SEMPRE aggiornato
- Controllare che esistano i backup e siano fatti regolarmente magari su copie sia fisiche che su cloud
- Fare un controllo sulle regole di firewalling per essere sicuri che il traffico in entrata sia gestito nella maniera corretta
- Istruire, per quanto possibile, chi lavora nell'azienda sulle regole principali della sicurezza informatica per cercare di alzare l'attenzione su possibili comportamenti pericolosi.