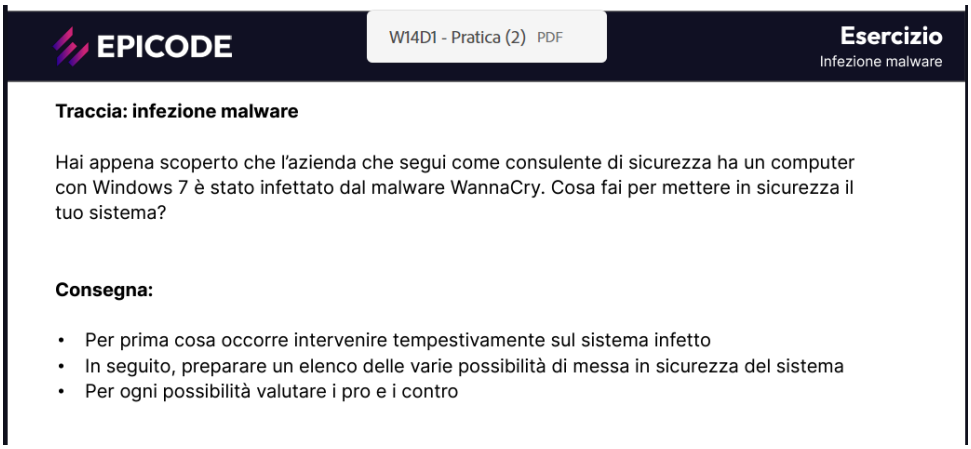
ESERCITAZIONE WEEK 14 DAY 3


EPICODE

W14D1 - Pratica (2) PDF

Esercizio
Infezione malware

Traccia: infezione malware

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema?

Consegna:

- Per prima cosa occorre intervenire tempestivamente sul sistema infetto
- In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
- Per ogni possibilità valutare i pro e i contro

WannaCry è un ransomware che ha fatto notizia nel maggio 2017. Si tratta di un tipo di malware che crittografa i file sul sistema infetto e successivamente richiede un pagamento in bitcoin per fornire la chiave di decrittazione necessaria per ripristinare l'accesso ai file. Si è diffuso rapidamente in tutto il mondo, colpendo principalmente sistemi Windows. Esso ha sfruttato una vulnerabilità di sicurezza di Windows chiamata **EternalBlue**, che era stata precedentemente identificata dalla National Security Agency (NSA) degli Stati Uniti. Tuttavia, il codice sorgente della vulnerabilità è stato successivamente rubato e reso pubblico da un gruppo chiamato Shadow Brokers. WannaCry ha sfruttato questa vulnerabilità per diffondersi rapidamente attraverso reti collegate.

Una volta che i file di un sistema erano stati crittografati, WannaCry visualizzava un messaggio di richiesta di riscatto sullo schermo, chiedendo ai proprietari del sistema di pagare una somma in bitcoin per ottenere la chiave di decrittazione. Ovviamente il pagamento non garantiva sempre il ripristino dei file.

Ha colpito organizzazioni in tutto il mondo, inclusi ospedali, istituti governativi, imprese e utenti individuali. La sua rapida diffusione è stata in parte favorita dal fatto che molte organizzazioni non avevano applicato gli aggiornamenti di sicurezza disponibili per proteggere le loro reti dalla vulnerabilità EternalBlue.

Dopo la diffusione di WannaCry, Microsoft ha rilasciato patch di sicurezza per proteggere i sistemi Windows dalla vulnerabilità EternalBlue. Inoltre, diverse organizzazioni e istituzioni governative hanno collaborato per fermare la diffusione del malware e identificare i responsabili.

Per un tempestivo intervento sul sistema infetto occorre eseguire le seguenti operazioni:

1. **Isolamento della macchina:**
    - Isolare immediatamente il computer infetto dalla rete così da impedire la propagazione del malware ad altri dispositivi della rete, dato che tale ransomware usa propagarsi in tale maniera. Se avviene nel minor tempo possibile, si riduce la probabilità di trovare il ransomware in altri PC collegati alla rete.
2. **Disattivazione della connessione Wi-Fi o del cavo di rete:**
    - Assicurasi che il computer non possa comunicare con altri dispositivi sulla rete, disattivando la connessione Wi-Fi o rimuovendo il cavo di rete.
3. **Disabilitazione dei servizi SMB:**
    - WannaCry sfrutta una vulnerabilità nel protocollo SMB (Server Message Block), quindi il servizio SMB deve essere disabilitato.

Per mettere in sicurezza il sistema:

4. **Applicazione degli aggiornamenti di sicurezza:**
    - Il sistema operativo deve essere completamente aggiornato, installando tutti gli aggiornamenti di sicurezza disponibili per Windows 7.
    - Implementare i patch di sicurezza forniti negli anni per ovviare a tale problematica.

Sicuramente questo rende più sicuro il sistema da possibili attacchi futuri ma non garantisce che il ransomware sia sparito dal sistema se non sono state eseguite correttamente le azioni tempestive.

5. **Utilizzo di un software antivirus/antimalware:**
    - Eseguire una scansione completa del sistema utilizzando un software antivirus o antimalware aggiornato. Rimuovere qualsiasi minaccia rilevata.

Questo permette di scansionare e eventualmente individare file sospetti. Non basta farlo solo sul dispositivo infetto ma anche sui dispositivi della rete, per scongiurare una già avvenuta propagazione.

Se il tipo di malware fosse malauguratamente di tipo 0day (non so se sia questo il caso), la sua firma potrebbe essere sconosciuta e non rilevata e quindi non si risolverebbe il problema.

6. **Ripristino da backup:**
    - Se si ha un backup del sistema precedente all'infezione, si può eseguire il ripristino del sistema da quel punto.

Attenzione a controllare che il backup non contenga il malware!

7. **Monitoraggio dell'attività del sistema:**
    - Monitorare attentamente l'attività del sistema per individuare eventuali comportamenti sospetti, utilizzando strumenti di sicurezza e registri di sistema per individuare anomalie.

Se ben fatto, può portare a individuare processi sospetti, ma non è detto che ciò sia facilmente intuibile.

8. **Segnalazione dell'incidente:**
    - Notifica l'incidente alle autorità di sicurezza informatica e all'organizzazione responsabile della sicurezza IT nella tua azienda o istituzione.
9. **Consulenza di professionisti IT:**
    - In casi gravi, potrebbe essere necessario coinvolgere esperti di sicurezza informatica per analizzare l'infezione e proporre soluzioni specifiche.

È sempre buona norma segnalare e attuare tempestivamente controlli anche su altri sistema dell'azienda. Una volta studiata la problematica, in genere si invia una mail dettagliata ai dipendenti in modo da metterli in guardia e far ein modo che non acccada di nuovo. Vengono consigliati aggiornamenti di sicurezza.