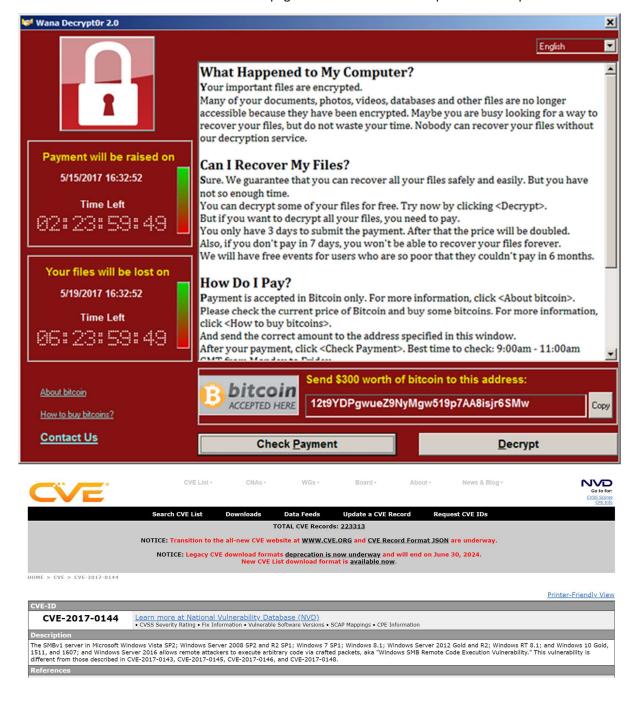
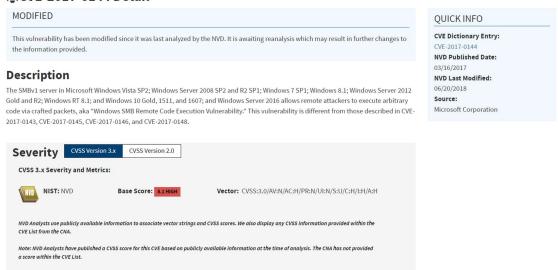
Esercizio WannaCry

WannaCry è un tipo di ransomware che sfrutta una vulnerabilità di Windows nota come EternalBlue per propagarsi all'interno di una rete. Questa vulnerabilità era presente nelle versioni non aggiornate di Windows e permetteva al malware di propagarsi su reti collegate, senza richiedere l'interazione dell'utente. L'exploit EternalBlue era inizialmente una tool di hacking sviluppato dalla National Security Agency (NSA) degli Stati Uniti. Tuttavia, è stato rubato e successivamente utilizzato da gruppi di cybercriminali, incluso il gruppo responsabile di WannaCry. Una volta che WannaCry si è infiltrato in un sistema, ha crittografato i file presenti sulla macchina, rendendoli inaccessibili agli utenti. Successivamente, il malware visualizzava un messaggio di richiesta di riscatto, chiedendo alle vittime di pagare una somma di denaro in bitcoin per ottenere la chiave di decrittazione. Il ransomware cercava di intimidire le vittime con minacce di eliminare definitivamente i file se il riscatto non veniva pagato entro un determinato periodo di tempo.



₩CVE-2017-0144 Detail



Fatte le dovute premesse passiamo ora ad ipotizzare uno scenario in cui abbiamo una rete, nella quale sono connessi 30 host, e uno di questi sia un Win7 infetto da WannaCry. Analizzeremo quindi gli interventi tempestivi sulla macchina infetta e le varie possibilità della messa in sicurezza del sistema, supponendo che non sia disponibile la patch di sicurezza.

Interventi su macchina infetta

- **Isolamento della macchina:** Come prima, è essenziale isolare immediatamente il PC infetto dalla rete per prevenire la propagazione del malware, disconnettendolo fisicamente dalla rete.
- Analisi approfondita: Condurre un'analisi approfondita del sistema infetto per identificare il malware e le sue modalità di esecuzione.

Possibilità di messa in sicurezza degli altri PC

- Isolamento preventivo: Isolare preventivamente gli altri PC disconnettendoli dalla rete finché non è
 possibile garantire la sicurezza.
- Monitoraggio del traffico: Implementare sistemi di monitoraggio del traffico di rete per rilevare eventuali tentativi di propagazione del malware.
- Spegnimento dei sistemi: Spegnere i sistemi non essenziali per ridurre la superficie di attacco e limitare la diffusione del malware.
- Implementare filtri di rete: Configurare filtri di rete per bloccare il traffico sospetto e limitare la comunicazione con indirizzi IP noti associati a WannaCry.
- Formazione degli utenti: Rafforzare la formazione degli utenti sull'importanza di evitare clic su link e apertura di allegati sospetti.
- **Backup offline:** Assicurarsi che i backup siano offline o altrimenti inaccessibili al malware per evitare la cifratura dei dati di backup.

Pro e contro delle misure di sicurezza

Pro dell'isolamento preventivo: Riduce il rischio di diffusione. Tuttavia, può interrompere temporaneamente le operazioni aziendali.

Pro del monitoraggio del traffico: Permette la rilevazione tempestiva di attività sospette. Tuttavia, potrebbe richiedere risorse dedicate.

Pro dell'implementazione di filtri di rete: Riduce la possibilità di comunicazione con server di controllo e diffusione del malware. Tuttavia, può richiedere configurazioni e manutenzione aggiuntive.

Contro dello spegnimento dei sistemi: Potrebbe interrompere le attività aziendali. Tuttavia, riduce la superficie di attacco.

Contro della formazione degli utenti: Ancora difficile eliminare completamente il rischio umano. Tuttavia, la formazione riduce la probabilità di azioni inconsapevoli.

Conclusioni

In assenza di una patch, l'approccio principale è prevenire la diffusione e mitigare il rischio attraverso l'isolamento e la riduzione delle opportunità di propagazione.