REPORT ESERCIZIO

W14-D3

Redatto da Andrea Sciattella

26/05/2024

RANSOMWARE WANNACRY: DETTAGLI

Cos'è WannaCry?

WannaCry è un tipo di ransomware che ha infettato migliaia di computer in tutto il mondo a partire dal 12 maggio 2017. Il ransomware cripta i file del sistema infetto e richiede un riscatto in Bitcoin per decriptarli. WannaCry sfrutta una vulnerabilità nei sistemi operativi Windows per propagarsi.

Vulnerabilità Sfruttata: **CVE-2017-0144**

WannaCry sfrutta la vulnerabilità identificata come **CVE-2017-0144**. Questa vulnerabilità riguarda il protocollo Server Message Block (SMB) di Windows e permette l'esecuzione di codice remoto su sistemi non aggiornati. La vulnerabilità è conosciuta come EternalBlue.

CVE ID: CVE-2017-0144

Descrizione: La vulnerabilità permette a un attaccante remoto di inviare pacchetti appositamente predisposti a un server SMBv1 per eseguire codice arbitrario.

Pubblicazione: La vulnerabilità è stata resa pubblica nel marzo 2017 dopo che il gruppo di hacker Shadow Brokers ha rilasciato gli exploit utilizzati dalla National Security Agency (NSA) degli Stati Uniti.

Metodo di infezione:

Il WannaCry penetra prima in un sistema attraverso *EternalBlue*, sfruttando la vulnerabilità SMB (Server Message Block v1).

Una volta infettato il sistema, WannaCry cifra i file dell'utente, rendendoli inaccessibili senza la chiave di decrittazione.

Il malware poi visualizza un messaggio che richiede il pagamento di un riscatto in Bitcoin per decriptare i file. L'importo richiesto aumenta nel tempo se il pagamento non viene effettuato.

ISOLAMENTO E RIDUZIONE DANNI

Come prima cosa dovremmo intervenire tempestivamente per ridurre i danni in tutta la rete e principalmente nel dispositivo stesso, seguendo l'ordine:

1. **Isolamento del Sistema**:
   - Scollegare immediatamente il computer infetto dalla rete aziendale per evitare la propagazione del malware ad altri dispositivi. Il WannaCry è un worm che si diffonde attraverso le reti quindi isolare il sistema aiuta a contenere l'infezione ai dispositivi.

2. **Disabilitazione dei Servizi Non Essenziali:**
   - Spegnere i servizi di rete non critici e le condivisioni di file per ridurre il vettore di attacco e minimizzare i danni.

3. **Creazione di Backup di Emergenza:**
   - Se possibile, effettuare un backup dei dati critici non ancora cifrati su dispositivi di archiviazione esterni in modo da poter salvaguardare i dati importanti ed evitare perdite irreparabili.

4. **Scansione Anti-Malware:**
   - Effettuando una scansione tramite un software Anti-Malware che può rilevare tramite il database di firme e bloccare il file prima di essere eseguito.

MESSA IN SICUREZZA DEL SISTEMA

Il primo ***metodo*** è la formattazione e reinstallazione del Sistema Operativo, per rimuovere ogni corruzione dei file:

- **PRO**: Garantisce la completa rimozione del malware e ripristina il sistema a uno stato sicuro e funzionante.
- **CONTRO**: Richiede tempo per la reinstallazione e riconfigurazione del sistema e potrebbe risultare in una possibile perdita di dati se non si dispone di backup aggiornati.

Come ***secondo*** metodo abbiamo il ripristino da Backup pulito creato precedentemente:

- **PRO**: Rapida ripresa delle operazioni utilizzando un backup non infetto e ritorno alla configurazione precedente al ransomware del sistema.
- **CONTRO**: Necessità di backup recenti e verificati ed abbiamo il rischio di reinfezione se il backup non è completamente sicuro.

Come ***terzo*** metodo abbiamo l'aggiornamento del Sistema Operativo a Windows 10:

- **PRO**: Accesso a patch di sicurezza e aggiornamenti continui Maggiore protezione contro minacce future.
- **CONTRO**: Costi associati all'acquisto di nuove licenze e potenziali problemi di compatibilità con hardware e software esistenti (che potrebbero non supportare un OS più avanzato).

Invece il ***quarto*** metodo è quello di attivare uno scanner Anti-Malware per rimuovere i file presenti che potrebbero essere nascosti, per sfruttare un'altra infezione.

CONCLUSIONE

Per garantire una sicurezza ottimale, si consiglia quindi di combinare la formattazione e reinstallazione del sistema operativo con un aggiornamento a Windows 10, e continuare ad aggiornare il dispositivo tramite patch e aggiornamenti recenti.

Questo approccio non solo rimuoverà del tutto il malware, ma garantirà che il sistema riceva immediatamente aggiornamenti di sicurezza regolari.

Tuttavia, è cruciale assicurarsi che tutti i dati importanti siano salvaguardati tramite backup regolari e seguendo pratiche di sicurezza.