INFEZIONE MALWARE

Casistica
Computer con Windows 7 infettato dal ransomware WannaCry.

Cos'è WannaCry?
WannaCry è un malware classificato sia di tipo ransomware sia di tipo worm. Queste tipologie significano rispettivamente che quando è in esecuzione cripta i file presenti sul computer e viene chiesto un riscatto per decriptarli e che è in grado di autoreplicarsi diffondendosi nella rete.

Risoluzione
Il primo passaggio da effettuare è quello di isolare le componenti più critiche dalla rete compromessa: macchina infetta, backup dei file, il nodo principale della rete per mantenere la minima operabilità dell'azienda al fine di non causare gravi danni economici sempre se non sia stato compresso anche quest'ultimo.
Diversi aspetti vanno tenuti in considerazione al fine di poter affrontare l'emergenza nel miglior modo possibile.
Una variabile da esaminare è quella dello stato di aggiornamento dei sistemi operativi installati sulle varie macchine connesse. Purtroppo la compromissione di una singola macchina porta alla conclusione che sarà molto probabile che ve ne siano altre vulnerabili all'infezione in quanto è buona prassi avere lo stesso livello di sicurezza su tutta la rete. Tale ragionamento viene fatto in quanto se vi è una macchina sulla quale è stata installata la patch non dovremo preoccuparci dell'infezione da parte del malware e di conseguenza della propagazione in rete del software malevolo.
Una volta aver isolato le macchine dobbiamo procedere con la bonifica di tutti i sistemi. Pertanto i passaggi da effettuare potrebbero essere i seguenti:
- individuare preliminarmente le macchine infette con scansioni antivirus nei casi in cui non vi sia una palese prova che la macchina sia stata compromessa con ad esempio una schermata di richiesta di riscatto
- formattare i dischi in maniera sicura
- collegare i dispositivi a una rete pulita per scaricare, installare e aggiornare il sistema operativo e tutti gli altri software.
- ripristinare i file (Il ripristino da un backup deve essere fatto solo nel caso in cui vi sia la certezza che i dati provenienti da esso siano privi di malware)
- scansione del sistema con software antivirus per verificare che non sia ancora presente il malware
- riconnettersi alla rete
- monitorare il traffico di rete ed eseguire scansioni antivirus per identificare se rimane un'infezione.