INFEZIONE MALWARE

PENETRATION TESTING(2)

TRACCIA

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

COS'E' WANNA CRY

WannaCry è un chiaro esempio di crypto-ransomware apparso nel maggio 2017, un tipo di malware (software dannoso) utilizzato dai cybercriminali per estorcere denaro. Il ransomware compie l'azione dannosa in due modi diversi: crittografando file di particolare rilevanza in modo che risultino illeggibili, oppure impedendo l'accesso al computer, che diviene inutilizzabile. L'exploit va a caccia di una vulnerabilità nel protocollo SMB (Server Message Block) di Windows utilizzato dai dispositivi per comunicare su una rete condivisa. In particolare, ha cercato qualsiasi PC con la porta Samba TCP 445 accessibile.
Al pari di altre tipologie di crypto-ransomware, anche WannaCry tiene in ostaggio i dati dell'utente, promettendone la restituzione e il ripristino solo dopo l'avvenuto pagamento di un riscatto in denaro.
Da parte sua, Microsoft ha rilasciato una patch di sicurezza in grado di proteggere i sistemi informatici degli utenti quasi due mesi prima della comparsa del ransomware WannaCry.

COME SI DIFFONDE

WannaCry incorpora anche elementi di un worm. I worm informatici, a differenza dei virus, non si diffondono infettando i file. Invece, si diffondono attraverso le reti, cercando vulnerabilità in altri computer connessi. Quindi, una volta infettato un computer in una rete, è stato in grado di muoversi per infettarli tutti.

PREVENIRE L'ATTACCO

1. Aggiorna il tuo sistema operativo Windows con le patch di sicurezza più recenti
2. Non cliccare su link sospetti
2. Se non l'hai già fatto, installa un antivirus aggiornato
3. Inizia a fare backup del tuo PC
4. Non aprire allegati e-mail non attendibili
5. Non eseguire download da siti non affidabili
6. Utilizza una VPN quando ti colleghi a un WIFI pubblico
7. Bloccare il traffico SMB in ingresso sulla porta 445

COSA FARE QUANDO SI E' GIA' INFETTI

1. Disconnettere il computer da Internet
2. Ripristino da un backup
3. Se hai eseguito il backup dei file tramite un archivio online, è possibile che i tuoi file locali siano stati crittografati e quindi sincronizzati con i cloud. Quindi la prima cosa è annullare la sincronizzazione del tuo smartphone, tablet o qualsiasi altro dispositivo connesso al cloud il prima possibile.