# W20D1 – IRP e CSIRT.

## Esercizio obbligatorio

L'isolamento prevede la creazione di una rete di quarantena che eviti che l'host infetto possa avere accesso alla rete interna, anche se la macchina resta comunque accessibile tramite internet. L'host infetto è dunque raggiungibile tramite internet da parte dell'attaccante, ma non si trova più nella rete interna, alla quale potrebbe accedere superando l'ostacolo del firewall. La rimozione, invece, prevede la completa eliminazione dell'host infetto dalla rete, isolandolo anche da internet. La rete di quarantena è fuori dalla rete interna e non è nemmeno collegata ad internet, impedendo all'attaccante di accedere sia al sistema infetto, sia alla rete interna. Mentre con l'isolamento il sistema infetto resta accessibile da internet, con la rimozione il sistema in questione è staccato sia dalla rete interna, che dalla rete internet. Per smaltire i dischi compromessi dall'attacco, è possibile ricorrere sia alla soluzione purge, sia alla soluzione destroy. La soluzione purge prevede sia misure logiche sia misure fisiche per l'eliminazione dei dati dal disco, anche se le tecniche fisiche di eliminazione dei dati non sono troppo invasive e non distruggono completamente l'hardware. La soluzione destroy, invece, prevede l'uso di tecniche fisiche molto invasive per rendere inaccessibili i dati e rendere inutilizzabile il disco o il dispositivo di storage. In certi casi è prevista proprio la distruzione completa dell'hardware, ad esempio tramite la trapanazione, che rende il disco non più utilizzabile e le informazioni irrecuperabili. Data l'invasività della distruzione fisica, questa soluzione è adatta per i casi in cui il disco non è riutilizzabile, anche se è la più costosa. La soluzione clear, invece, prevede delle tecniche solamente logiche per la rimozione dei contenuti, per esempio tramite tecniche di read and write, per cui il contenuto viene sovrascritto più volte o tramite un factory reset per resettare a livello industriale.

## Esercizio facoltativo

I due link riportati dai dipendenti dell'azienda possono essere effettivamente la prova di un attacco e riportano degli IOC da tenere sotto controllo. Il primo link riporta ad un possibile codice malevolo per un DNS Changer PowerShell script, in grado di modificare le impostazioni del DNS e di indirizzare il traffico verso domini malevoli ed anche il secondo link sembra contenere dei file sospetti di origine malevola, probabilmente collegati a questo DNS Changer PowerShell script o ad un keylogger. Gli IOC che fanno pensare a questa problematica sono i cambiamenti nelle impostazioni del DNS, il traffico in uscita verso IP sospetti e la presenza di script PowerShell strani come DNS_Changer.ps1 Vi sono anche delle alterazioni nei registri relative al DNS e ai protocolli TCP ed UDP e si notano delle connessioni in uscita verso IP strani tramite DNS. Questo potrebbe essere indice di un attacco del tipo DNS hijacking, che potrebbe servire per indirizzare il traffico verso server malevoli e potrebbe essere il primo passo di un attacco più grande per sottrarre file oppure iniettare malware, ingannando gli utenti per farli accedere a domini falsi. Queste modifiche alle impostazioni DNS e di rete sembrano anche persistenti ed aprono la porta a varie problematiche, ad esempio di phishing o di malware, indirizzando gli utenti verso domini non sicuri o siti malevoli. Questo potrebbe essere proprio il primo passo di un attacco più

esteso con malware o phishing. Alla luce di questi IOC, è importante intervenire subito, isolando i sistemi o usando Wireshark per monitorare più attentamente il traffico DNS, specie quello in uscita. È necessario controllare con attenzione i log, rimuovere eventuali meccanismi di persistenza e soprattutto serve ripristinare le corrette impostazioni DNS, usando anche DNSSEC per una maggiore sicurezza. A seguito di questo attacco, è fondamentale condurre un ulteriore hardening dei sistemi e fare un controllo di eventuali patch di aggiornamento da scaricare e soprattutto implementare maggiori controlli per il DNS, ad esempio prevedendo la possibilità di alert in caso di alterazioni nelle impostazioni DNS o implementando DNSSEC o altri modi per il filtraggio DNS.