Prevenzione dei sistemi da un attacco Ransomware (WannaCry)

Come consulente aziendale è bene promuovere una corretta cultura aziendale per quanto riguarda la prevenzione degli attacchi provenienti dal web.

Una scaletta "tipo" di interventi da svolgere è:

1- L'utilizzo di un software antivirus di acclamata fama ed efficacia;
2- Installare sempre gli aggiornamenti di sicurezza introdotti dal sistema operativo, router, e così via. 15 minuti persi per le installazioni valgono di più di anni di lavoro;
3- Utilizzare password sicure, criptate e non accessibili (es.: il post-it sul pc con la password!) per tutti i servizi a cui si accede;
4- Eventuali PC portatili di lavoro possono essere utilizzati solo e soltanto su reti sicure (come ad esempio quella domestica). Connettersi dall'open Wi-Fi del bar di fiducia non è consentito in quanto possono essere sottratte informazioni preziose;
5- Fare frequenti backup dei dati su Server, PC ed ogni altra macchina in qualche modo riconducibile all'azienda;
6- Utilizzare, se possibile, una VPN;
7- Non aprire file sospetti provenienti da download, email, chiavette USB ecc. Se possibile, scansionare qualsiasi allegato tramite Antivirus o tool online (VirusTotal ad esempio)

Qualora nonostante tutte le accortezze in atto, un PC nella rete aziendale comunque dovesse venir infettato da un Ransomware come WannaCry, possiamo procedere in alcuni modi che possono mitigare o annullare del tutto l'impatto del Malware.

Il primo metodo in assoluto mettere in pratica è quello di mettere in "quarantena" la macchina infetta. Il ransomware si diffonde nella rete aziendale, andando ad infettare le altre macchine (non è detto che non lo siano già). Va quindi scollegato il cavo di rete il prima possibile, disabilitato il WiFi qualora il PC avesse l'antenna, e in caso di estrema necessità andrebbe rimosso anche il cavo di alimentazione in attesa di un intervento tecnico.

L'intervento tecnico può verificarsi in due diverse tipologie:

Reinstallazione dei dati tramite backup.

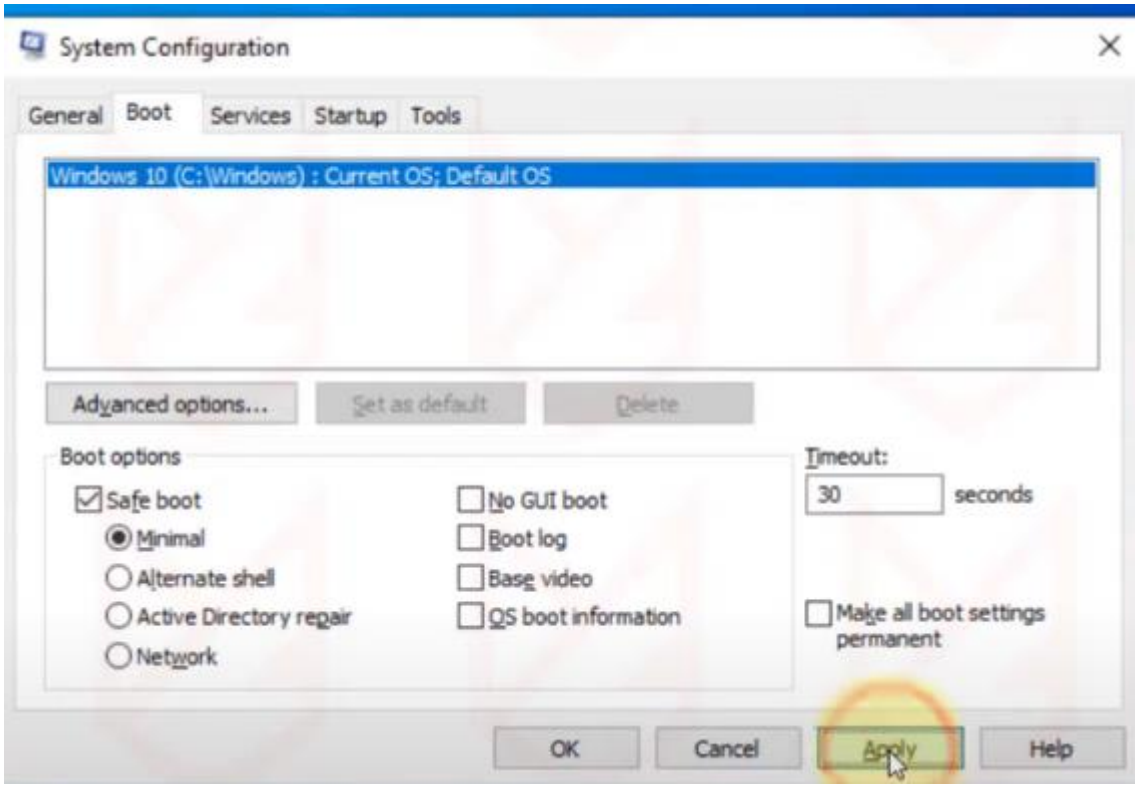
Il sistemista aziendale può formattare il PC e ripristinare i dati da backup qualora l'azienda ne fosse provvista. Il metodo in questione permette alla macchina di essere avviata in safe mode, formattata e riavviata per ricevere nuovamente i dati che sono stati criptati dal malware. Questa tipologia di Malware non blocca tutti i processi del PC, nella stragrande maggioranza dei casi li cripta soltanto, richiedendo un "ransom" in BTC per far si che venga spedita la chiave per permettere la decriptazione. Con un backup esterno possiamo aggirare l'intento dell'Hacker.

Rimozione manuale del Ransomware

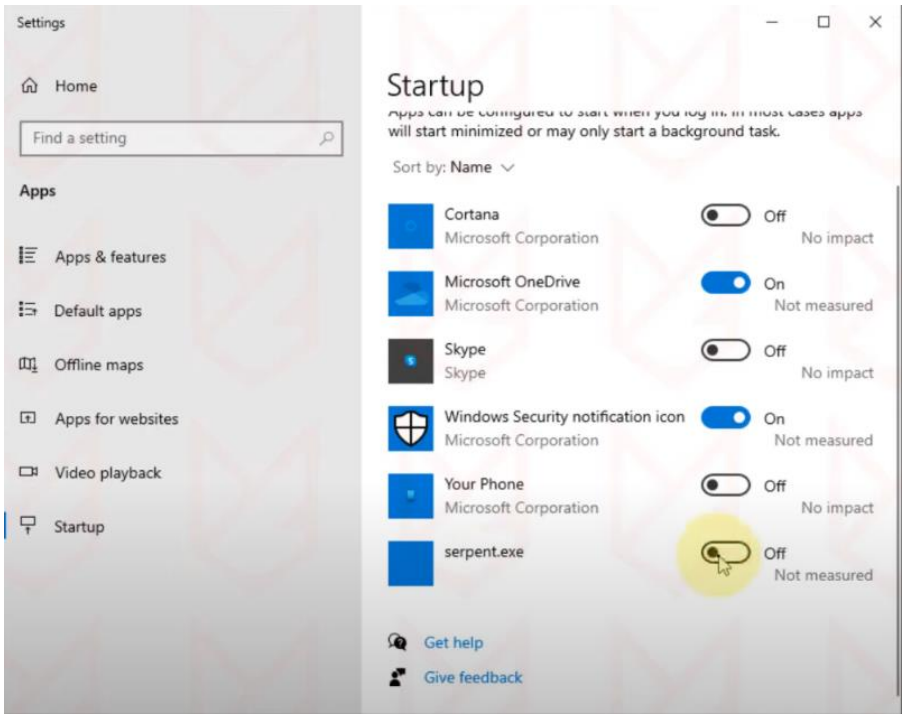
La procedura è piuttosto complicata ma può essere utile ad eliminare il Ransomware dal PC. I file potrebbero comunque rimanere criptati.

È composta dai seguenti step:

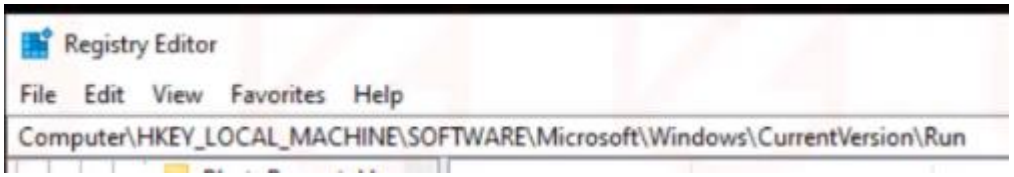
- Boot in safe mode del PC premendo i tasti Win + r e digitare "msconfig", andare su system conf, e poi safe boot. Ciò permetterà al PC di avviarsi solamente con i programmi essenziali, come da immagine seguente (il Ransomware in questione non è WannaCry ma in linea di massima il procedimento è lo stesso.)

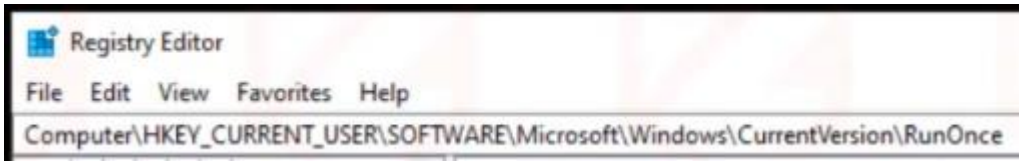


- Disabilitare la riproduzione in avvio del software



- Rimuovere il ransom.exe dalla gestione dei processi
- Disinstallazione dei software sospetti dal pannello di controllo
- Pulire i file temporanei (disk cleanup – temporary internet files, temporary files)
- Rimuovere i resti del Malware (che può replicarsi ad ogni avvio) anche dal Registry editor sia nella cartella Run che RunOnce, come da immagine seguente





- Riaprire msconfig e riavviare il pc in modalità normale
- Eseguire una scansione con software anti-malware.

La procedura descritta ha diversi pro e contro.

Intanto, se portata a termine, permette il riavvio del PC e il ritorno ad una “semi normalità”. I file in linea di massima rimangono criptati ma la macchina può tornare a lavorare. Dovrebbe essere eseguita da un esperto in quanto implica la cancellazione di specifiche directory. Richiede comunque tempo e una certa confidenza.

Bonus: il Ransomware non è WannaCry:

Online vengono messi a disposizione diversi tool come id-ransomware e nomoreransom.org all’interno dei quali è possibile fare un upload di un qualsiasi file criptato o di una richiesta di riscatto. Il tool confronta l’algoritmo e controlla all’interno dell’archivio se corrisponde ad un ransomware noto. Se corrisponde, vi verrà inviata la chiave di decriptazione per riavere nuovamente i files. Se non è presente si sconsiglia comunque il pagamento del riscatto. La macchina andrebbe isolata in attesa di una chiave di decriptazione.