Infezione UEFI

1) In fase di BOOT, il firmware UEFI precedentemente infettato, controlla la variabile fTA in NvRam se fTA==TRUE o non esistente, procedo con i seguenti passi altrimenti se fTA==TRUE procedo col BOOT normalmente senza infettare il sistema.

2) Controllo se vi sono utenti installati nel sistema:
   - NO: Se nel sistema non vi sono utenti significa che il sistema è vergine, per cui non devo fare nessuna operazione.
   - SI: Se nel sistema vi è uno o piu' utenti devo procedere la seguente analisi per ogni utente

3) Per cui se ho utenti nel sistema: Per ogni utente devo controllare se l'Agent è installato e se il file di lock è installato, definisco 4 stati possibile
   - Atrue: Agent installato => Esiste sotto la cartella “startup” il file associato allo scout o all'soldier oppure esiste in %tmp%\..\Microsoft la cartella nascosta associata all'elite
   - Afalse: Agente non installato
   - Ltrue => Esiste un file vuoto in %tmp%\..\ che ha lo stesso nome della cartella elite
   - Lfalse: Lock non esistente

   per cui il processo logico da adottare è implementato seguendo il seguente macrocodice:
   inizializzo le seguenti variabili:
   IsUser = FALSE
   IsFormat=TRUE

   ciclo su tutti gli utenti è testo quanto segue settando in modo opportuno le variabili IsUser e IsFormat:

	A_{true}	A_{false}
L_{true}	IsUser=TRUE IsFormat=FALSE	Remove FILELOCK IsFormat = FALSE
L_{false}	Insert FILELOCK IsUser = TRUE IsFormat = FALSE	

   Usciti dal ciclo:
   - se IsFormat == TRUE => significa che il pc è stato formattato => installo l'Agent e creo il file di Lock su tutti gli utenti del sistema
   - se IsUser == FALSE => significa che sono stati rimossi volutamente tutti gli agenti => disabilita l'UEFI settando la variabile fTA=TRUE