Analisi malware

Il malware in questione è scaricabile tramite questo URL.

https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE

Il malware che stiamo analizzando va a eliminare i processi legittimi di windows come ad esempio microsoft edge,di conseguenza va a nascondersi in alcuni processi del sistema rendendosi difficile da identificare.Disabilita sehop,la quale è una funzionalità di windows che disattivata può rendere il sistema vulnerabile ad attacchi di tipo BOF. Crea/modifica oggetti com ,questo consente al malware di eseguire processi dannosi per la raccolta di informazioni sensibili ad esempio.
Va a leggere:impostazioni di rete,certificati di sistema e impostazioni di sicurezza(forse per eseguire attacchi futuri).
Va a identificarsi come servizio windows (quindi va a inserirsi in un pid basso)in modo tale da avviarsi all'avvio del sistema.

SOLUZIONE

Per prevenire questi tipi di attacchi è consigliabile avere un buon antivirus,effettuare una scansione malware periodica e inoltre non scaricare programmi da fonti non attendibili.

ANALISI 2

Nome malware:PERFORMANCE_BOOSTER_v3.6.exe

Questo tipo di malware viene eseguito dall’utente attraverso il blocco note di windows.
Va a eseguire dei comandi presi da un file.bat e inseriti all’interno del cmd e powershell di windows,raccoglie informazioni sulla rete e sull’installazione di microsoft outlook per pianificare ulteriori attacchi in futuro,esamina le chiavi di registro di microsoft office(forse per identificare delle vulnerabilità).
Infine va a creare una directory dove archivia tutte le informazioni sensibili catturate.

SOLUZIONE

Attraverso un antivirus,rimuovere in maniera tempestiva il malware,tenere sempre aggiornato il sistema,non scaricare file da siti sconosciuti ed effettuare scansioni periodiche con il proprio antivirus.