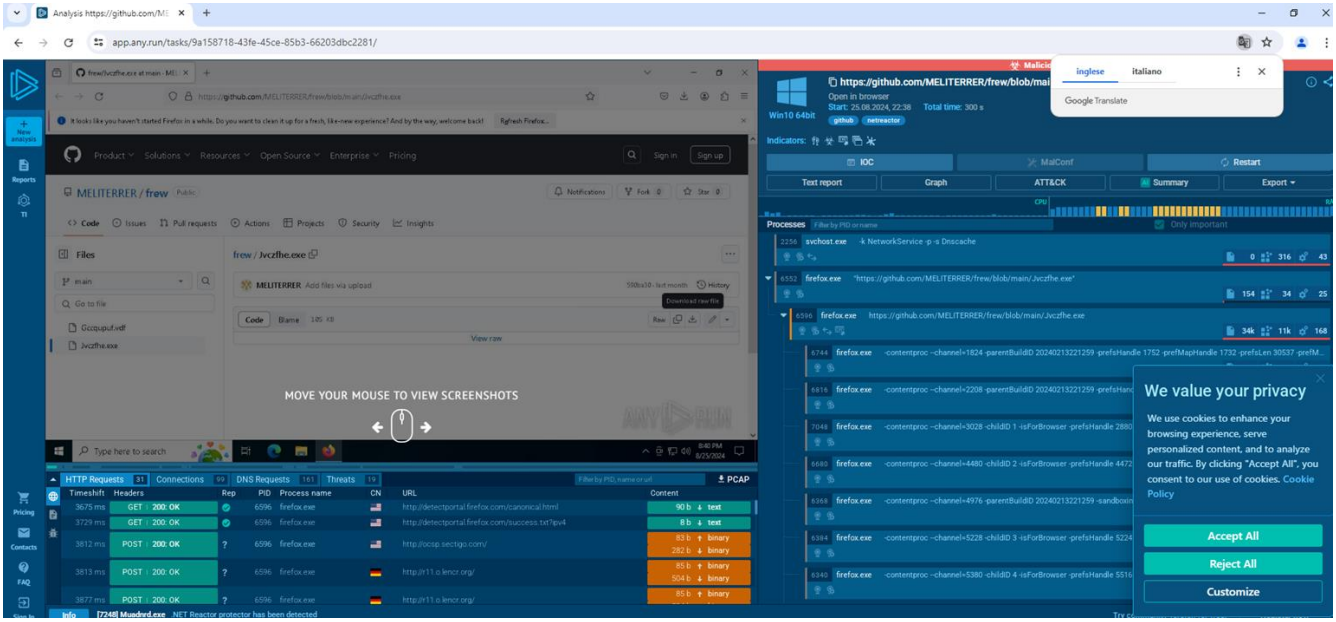
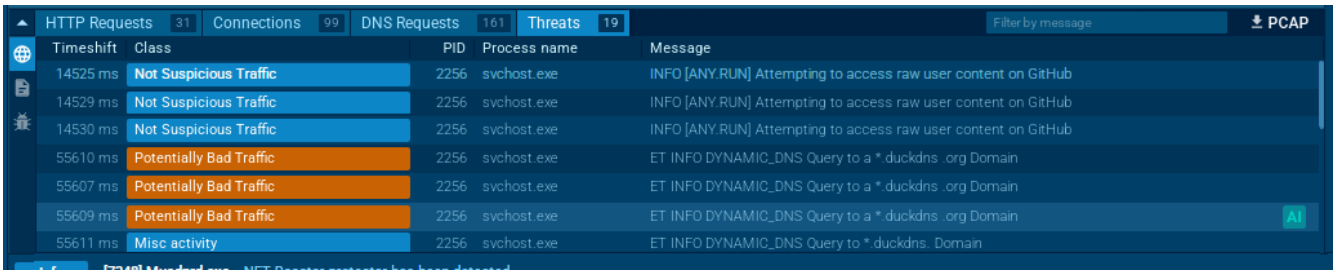
Studio IOC

Relazione sull’analisi di un’attività sospetta tramite ANY.RUN
Durante una simulazione eseguita con il servizio ANY.RUN, ho esaminato il comportamento del file Jvczfhe.exe, un eseguibile scaricato da un repository pubblico su GitHub.



Fin dall’inizio, l’esecuzione del file ha mostrato segnali preoccupanti. ANY.RUN ha rilevato comportamenti malevoli, generando allarmi relativi alle attività di processo e alle comunicazioni di rete.



Il fatto che il file fosse ospitato su GitHub, piattaforma solitamente considerata affidabile, non è un dettaglio trascurabile: spesso gli attaccanti sfruttano ambienti reputati sicuri per aggirare le difese. Nel caso specifico, il file proveniva dal repository MELITERRER/frew, facendo di GitHub un veicolo per la diffusione del malware.

Comportamenti sospetti dopo l’esecuzione
All’avvio, Jvczfhe.exe ha lanciato il browser Firefox, un’attività apparentemente innocua. Tuttavia, l’analisi ha mostrato la presenza di molteplici processi Firefox duplicati, attivi simultaneamente, un comportamento anomalo per una normale sessione di navigazione.

Il malware sfruttava il browser per celare traffico di rete malevolo, eseguendo numerose richieste POST e GET verso diversi server. Sebbene alcune richieste fossero indirizzate a domini apparentemente legittimi (es. firefox.com, sectigo.com), la frequenza e il volume suggeriscono che fossero usati come mascheramento per lo scambio di dati con server remoti.

Un elemento particolarmente critico è stato il coinvolgimento di domini dinamici come quelli di duckdns.org, noti per essere utilizzati da attori malevoli per nascondere gli indirizzi reali dei server di comando e controllo (C2). Le molteplici richieste DNS verso sottodomini di duckdns.org indicano un tentativo del malware di mantenere una connessione stabile con una rete esterna per ricevere comandi o esfiltrare informazioni.

Inoltre, il processo svchost.exe, normalmente legittimo, è stato segnalato da ANY.RUN per attività sospette ("Potentially Bad Traffic" e "Misc activity"), indicando un suo uso anomalo e nascosto per finalità illecite.

Questi segnali — comunicazioni con server sospetti, processi duplicati e uso mascherato di strumenti di sistema — sono tipici di malware backdoor o infostealer, con l'obiettivo di garantire accesso remoto persistente e sottrazione dati.

Conclusione

L'analisi ha evidenziato un malware complesso e subdolo, che si camuffa dietro un'apparenza innocua per operare efficacemente. Presentandosi come un file su GitHub, riesce a essere eseguito senza allarmi immediati, sfruttando processi di sistema e browser per nascondere le proprie attività. La comunicazione tramite domini dinamici consente al malware di mantenere un collegamento costante con i server di comando, difficili da bloccare.

Questo modus operandi suggerisce un intento di ottenere una presenza invisibile e persistente nel sistema, con finalità di spionaggio o controllo remoto.

Raccomandazioni per la prevenzione

Per proteggersi da minacce come questa, è importante adottare un approccio a più livelli. Bloccare i domini sospetti, come quelli di *.duckdns.org, può interrompere le comunicazioni con i server malevoli. È fondamentale evitare di scaricare eseguibili da fonti non verificate, specialmente da repository pubblici come GitHub. Monitorare attentamente i processi di sistema e i browser per individuare comportamenti anomali aiuta a rilevare eventuali infezioni. Infine, utilizzare strumenti avanzati di analisi comportamentale, oltre agli antivirus tradizionali, permette di identificare minacce più sofisticate. Solo con queste azioni integrate si può ridurre il rischio di infezioni silenti e pericolose.