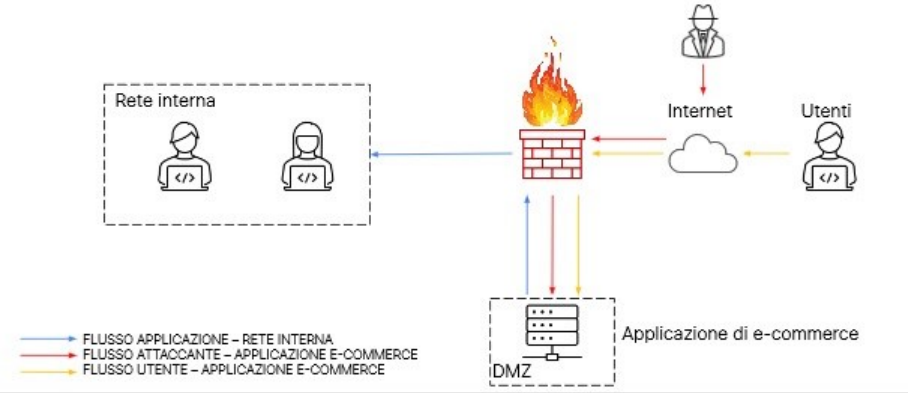
Security Operation

1. Come azione preventiva per difendere l'applicazione web da attacchi di tipo SQLi o XSS si può usare un Web Application Firewall (WAP) in quanto è una soluzione di sicurezza che analizza il traffico HTTP/HTTPS in entrata verso un'applicazione web, bloccando le richieste sospette o dannose. Può essere implementato come hardware, software o servizio cloud, nello schema è rappresentato da una fiamma.

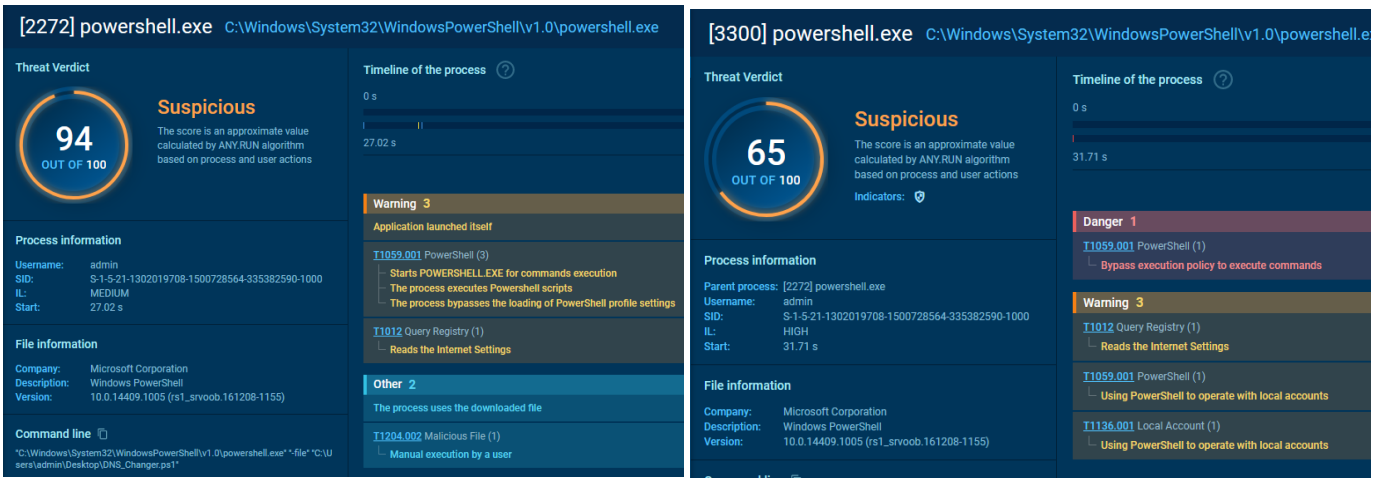


2. Report di due short link collegati ad any.run che, tramite una sandbox, ci consente l'esecuzione e l'analisi di file o URL di siti potenzialmente dannosi, andremo ad aprire "More info" in Process details e il Text report prodotto da any.run per vedere più informazioni a riguardo.

- Del primo shortlink si va analizzare "https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1"

L'utente salva un codice da github con estensione .psl (cioè un file di testo con comandi powershell) e una volta eseguito possiamo osservare, tramite any.run, che avvia il processo powershell.exe, esegue comandi nel contesto di PowerShell bypassando le restrizioni della "Execution Policy" impostata nel sistema.

Scaricare e eseguire file da origini sconosciute o non attendibili comporta rischi per la sicurezza. Un file .psl malevolo potrebbe contenere comandi che eseguono attività dannose come l'iniezione di malware, il furto di dati, la manipolazione del sistema o altre azioni malevole.
Inoltre, PowerShell è uno strumento potente che consente l'esecuzione di comandi di sistema e la gestione delle autorizzazioni degli account utente. Questo significa che gli script PowerShell possono influire sul funzionamento del sistema operativo, creare, modificare o eliminare file, accedere a risorse di rete e molto altro ancora.



- Nel secondo shortlink troviamo any.run che analizza il link: *"https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgtAG_apwtYT6OYs":*

È possibile osservare una sequenza di eventi sospetti che indicano un possibile tentativo di ottenere privilegi elevati o bypassare le misure di sicurezza nel sistema.

Viene scaricato un file .zip che ha un nome simile a un file di sistema. L'uso di un nome simile a un file di sistema legittimo potrebbe essere un tentativo di mascherare il file malevolo e ingannare l'utente.

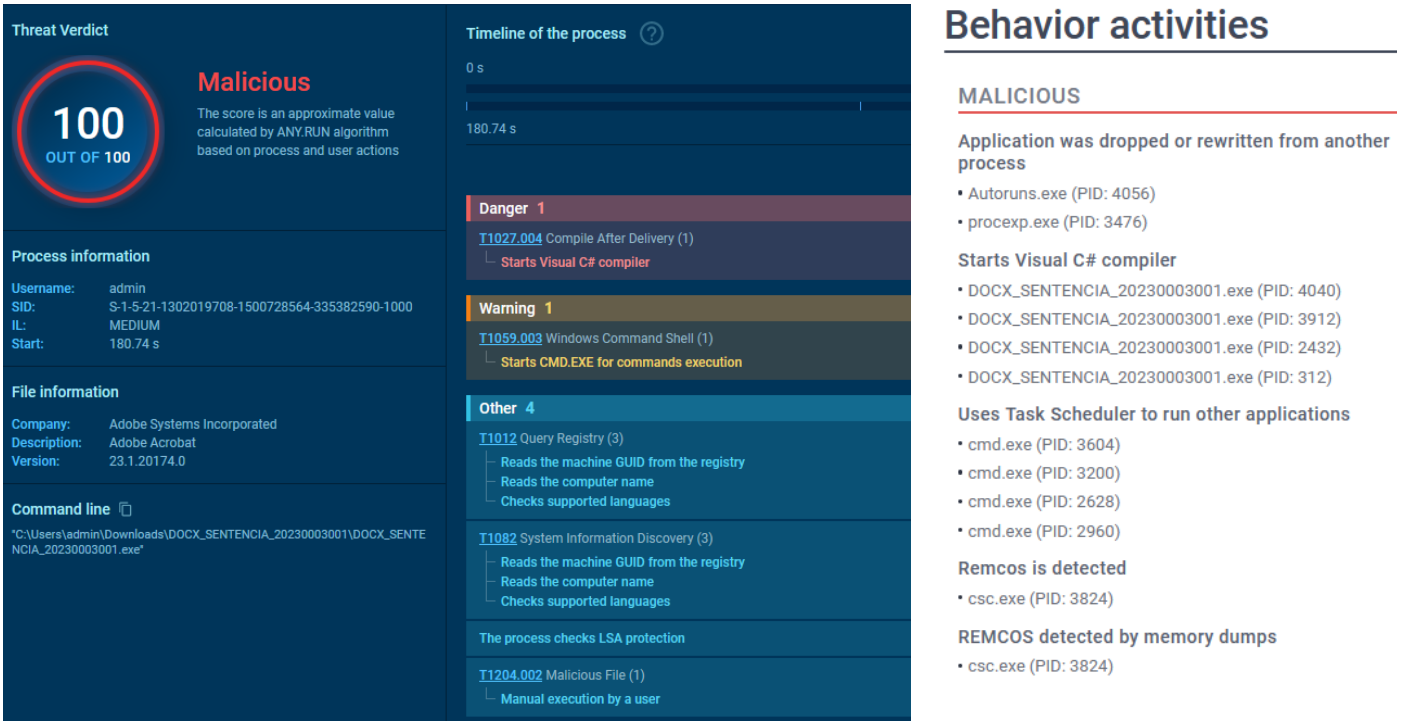
Successivamente, viene rilasciato un driver di sistema. L'installazione di un driver può essere un metodo utilizzato dagli attaccanti per ottenere privilegi elevati nel sistema o per bypassare le misure di sicurezza implementate.

L'applicazione si avvia in modo automatico con l'autorun e apre il prompt dei comandi (cmd). Questo potrebbe indicare un'azione automatizzata che cerca di eseguire comandi o script senza interazione dell'utente.

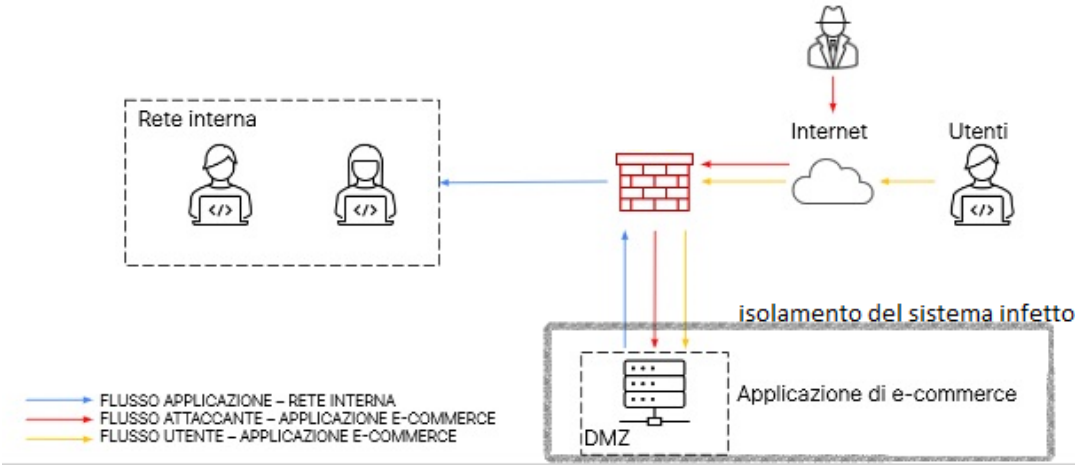
All'interno del prompt dei comandi, vengono lette una serie di informazioni sulla macchina. Questo potrebbe essere un passaggio per raccogliere dati sul sistema o verificare la presenza di determinate configurazioni o software.

Secondo il report automatico di Any.Run, viene rilevato che si tratta di un malware di tipo RAT (Remote Access Trojan) chiamato Remcos. I malware RAT consentono agli attaccanti di eseguire azioni su macchine infette in remoto. La menzione che il malware è attivamente aggiornato suggerisce che gli sviluppatori stiano continuamente apportando modifiche per eludere le difese di sicurezza.

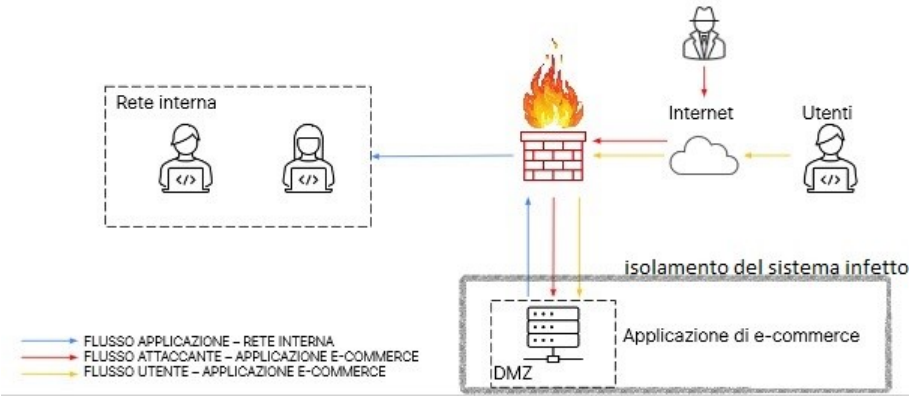
Il contesto suggerisce che il file .zip potrebbe essere stato inviato tramite una e-mail di phishing, e l'utente ha scaricato il file incautamente, aprendo la porta a un'eventuale infezione.



3. Nel caso in cui un malware infetti l'applicazione web per evitare che si propaghi bisogna isolare il sistema infetto dalla rete interna, ma per evitare che si propaghino informazioni sensibili verso l'esterno dobbiamo rimuoverlo anche dalla rete internet in modo che l'attaccante non abbia più accesso dall'esterno.



4. Unione degli schemi 1 e 3



5. Modifiche più aggressive all'infrastruttura:

- Implementare un firewall con WAF Web Application Firewall: Un firewall con WAF può proteggere dalle vulnerabilità comuni come gli attacchi di tipo SQLi (Injection SQL) e XSS (Cross-Site Scripting) monitorando e filtrando il traffico web in entrata ed uscita. Assicurarsi di configurare correttamente il WAF per adattarsi alle esigenze specifiche dell'applicazione web e aggiornarlo regolarmente per tenere conto delle nuove minacce.
- Implementare un IDS Intrusion Detection System: Un IDS monitora il traffico di rete e identifica gli attacchi sospetti o le anomalie nel comportamento del sistema. Ciò consente una rilevazione tempestiva e una risposta appropriata agli attacchi. È importante configurare l'IDS per generare avvisi e notifiche in caso di attività sospette e pianificare l'analisi dei log per identificare eventuali violazioni di sicurezza.
- Implementare un NAC Network Access Control: Il NAC permette di controllare e regolare l'accesso alla rete da parte dei dispositivi connessi, garantendo che solo dispositivi autorizzati e conformi alle politiche di sicurezza possano accedere alla rete. Ciò contribuisce a prevenire l'accesso non autorizzato alla rete e proteggere le risorse.
- Implementare una segmentazione della rete interna: Utilizzare router e switch per creare segmenti separati all'interno della rete aziendale, ad esempio per i diversi uffici come direzione, vendite, HR, ecc. Ciò limita l'accesso tra i segmenti e protegge le risorse aziendali in caso di compromissione di una parte della rete.
- Eseguire controlli e patch di sistema regolari: Monitorare e applicare regolarmente le patch di sicurezza per tutti i sistemi e le applicazioni aziendali. L'automazione di questi controlli può aiutare ad assicurarsi che le patch vengano installate tempestivamente, riducendo così le vulnerabilità esposte.
- Condurre un Penetration Testing: effettuare un test di penetrazione annuale per identificare eventuali vulnerabilità o falle nella sicurezza dei sistemi e delle applicazioni. Questo aiuta a rilevare i punti deboli e a prendere misure correttive per mitigare i rischi.
- Eseguire backup regolari: Effettuare backup regolari dei dati importanti su dispositivi esterni alla rete o sul cloud. In caso di incidente o compromissione dei dati, un backup aggiornato consente il ripristino dei dati senza subire perdite significative.
- Formazione del personale: Assicurarsi che tutto il personale sia formato e informato sulle misure di sicurezza informatica. Ciò include l'educazione su come riconoscere email sospette, evitare l'apertura di allegati o link non attendibili e non utilizzare dispositivi esterni non autorizzati.