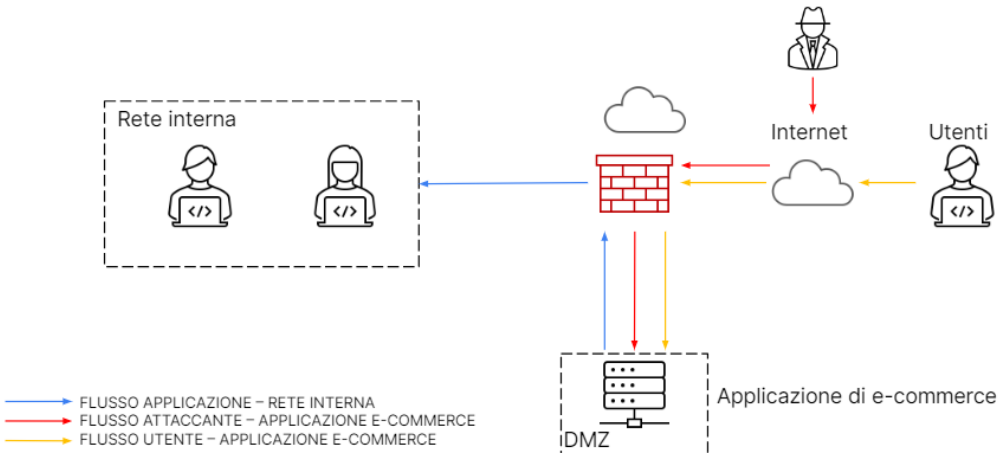
# Analisi rete di e-commerce

**Architettura di rete:**
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

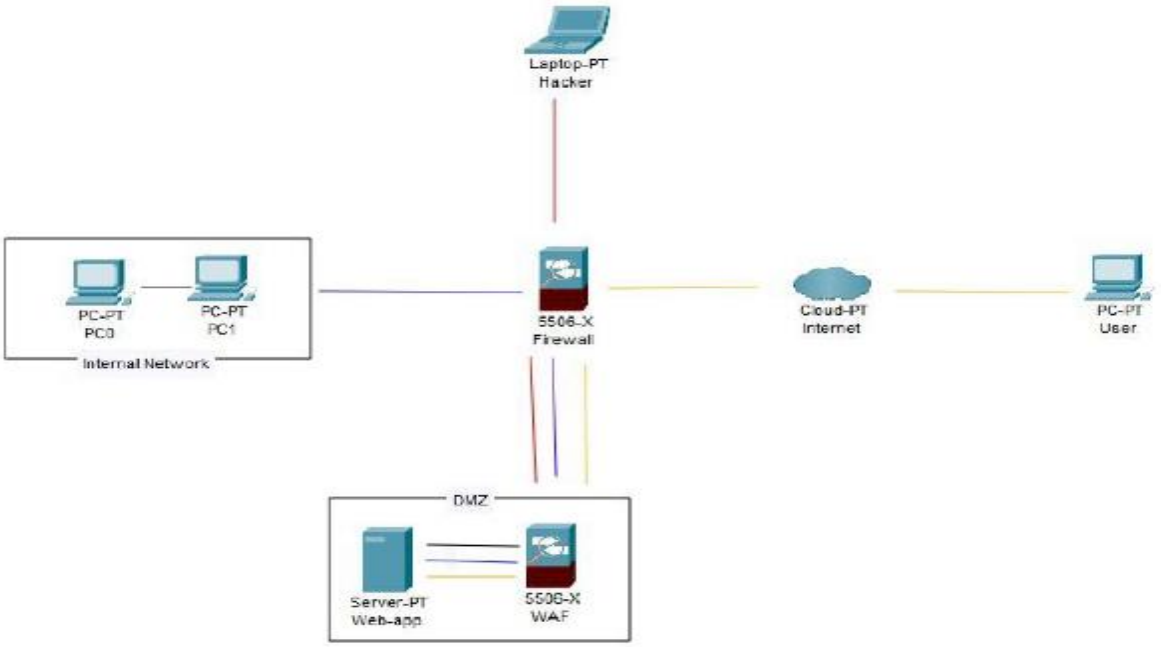
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.




**1.**

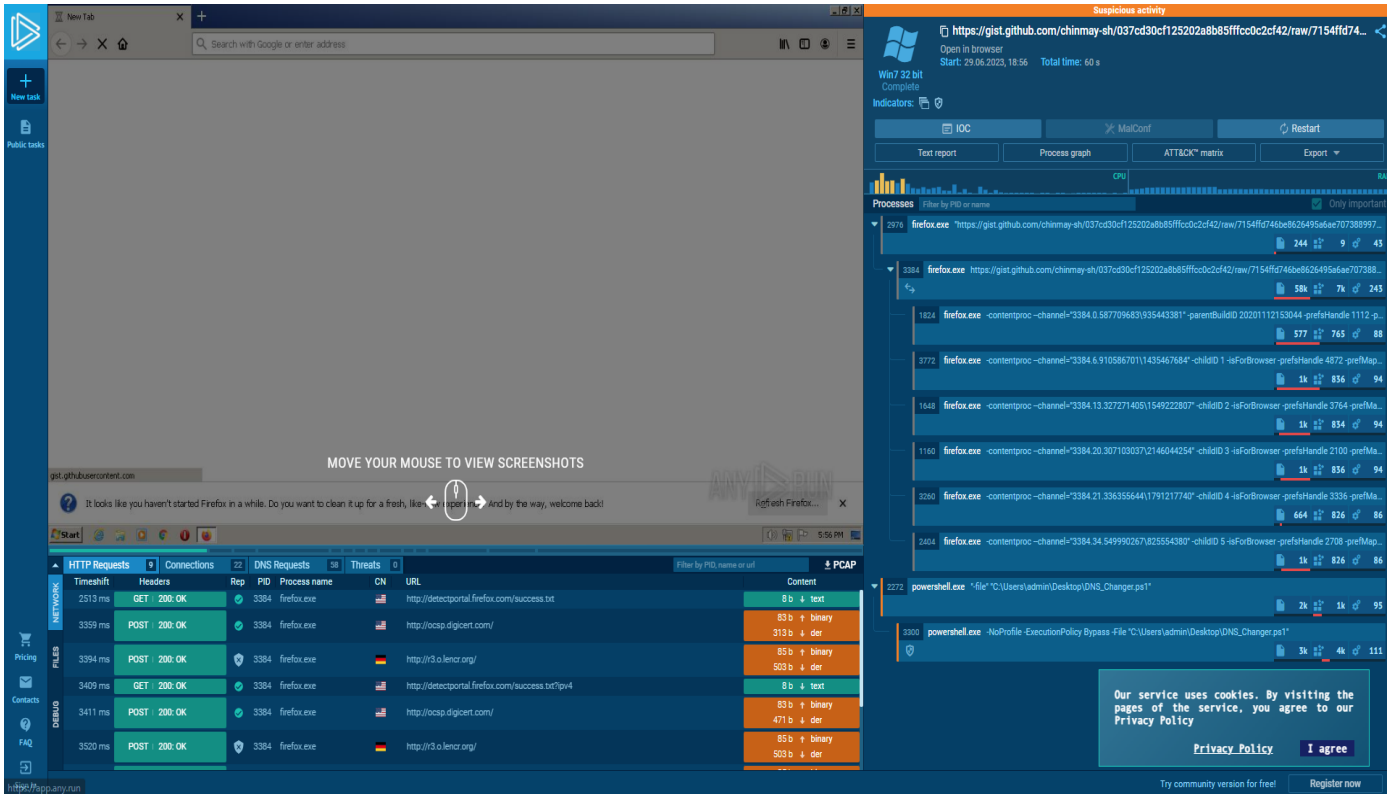
Difesa da attacchi SQLi e XSS.

Per prevenire attacchi SQLi e XSS è possibile aggiungere un WAF (Web Application Firewall) e dei controlli dell'input utente sulla web-app. Il waf è un firewall per applicazioni Web è una forma specifica di firewall per applicazioni che filtra, monitora e blocca il traffico HTTP da e verso un servizio Web.

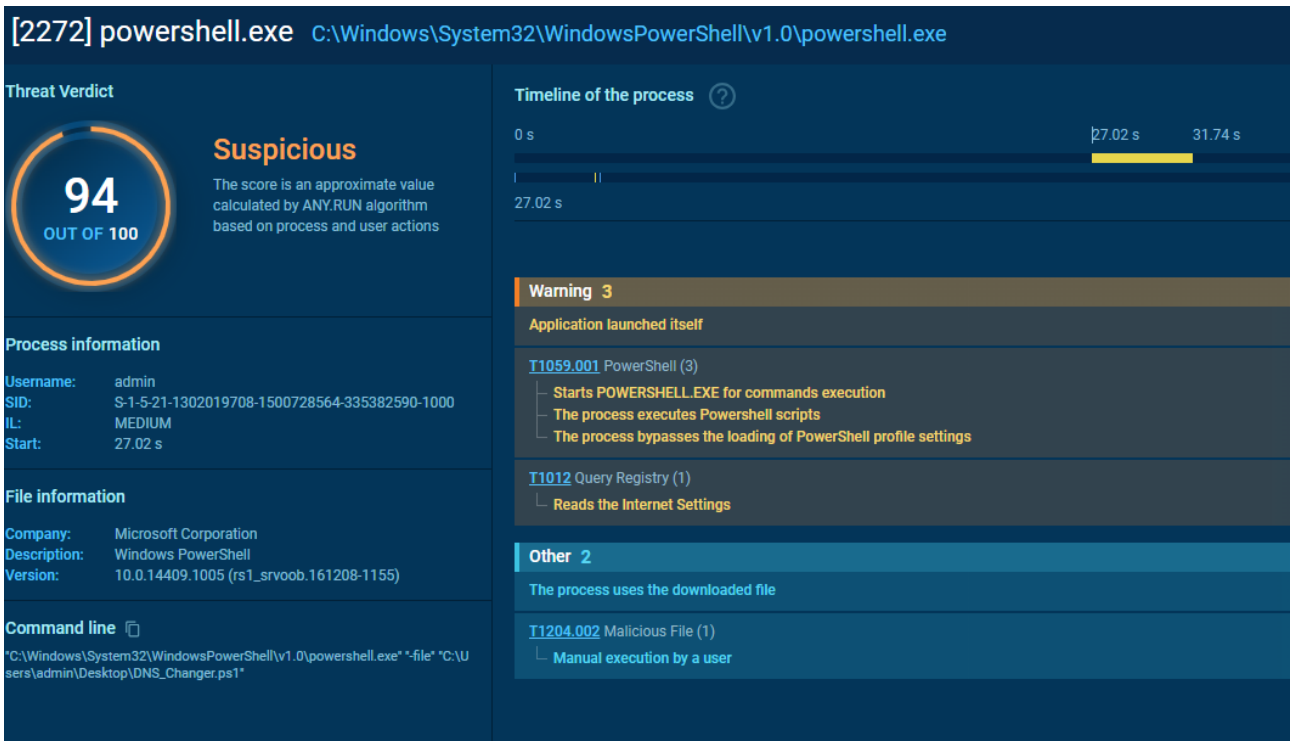


**2.**

Analisi attacco



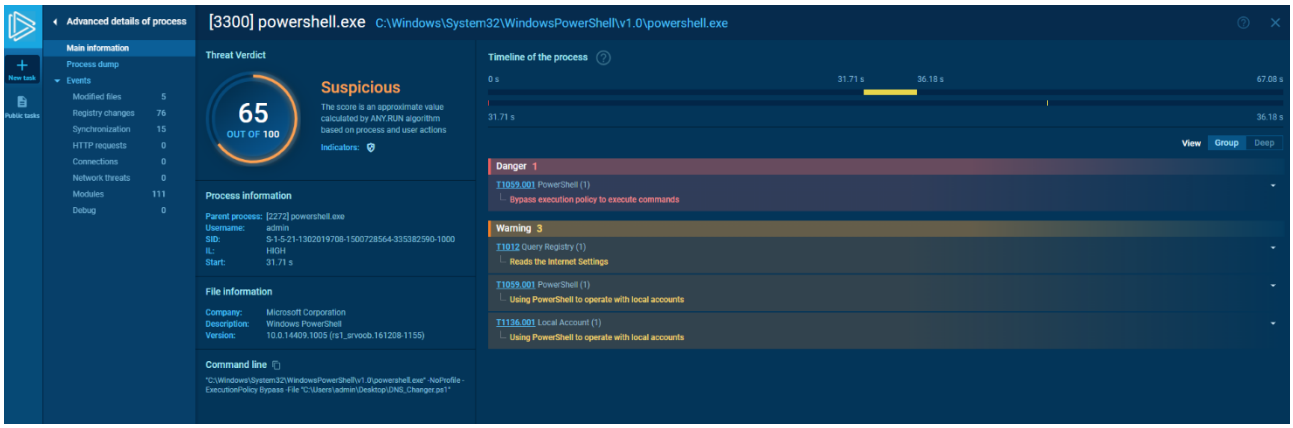

L'utente utilizza Firefox per navigare scarica il file




Il virus Powershell.exe è una forma potenzialmente pericolosa di Trojan progettata per rubare dati e informazioni. Può anche interrompere le attività sul tuo PC come la navigazione web.

Potenzialmente molto distruttivo, apre il tuo computer a molti rischi e pericoli, nascondendosi discretamente dietro un nome apparentemente innocente.

Powershell.exe è anche il nome di un software installato su tutti i computer Windows. È importante essere in grado di capire la differenza tra i due tipi.




Il modo più efficace per sbarazzarsi del virus Trojan Powershell.exe è utilizzare un software antivirus e un'app di rimozione malware.

Il software antivirus può richiedere diverse ore per completare il processo, a seconda della velocità del computer, ma offre anche i metodi migliori per rimuovere i file dannosi.

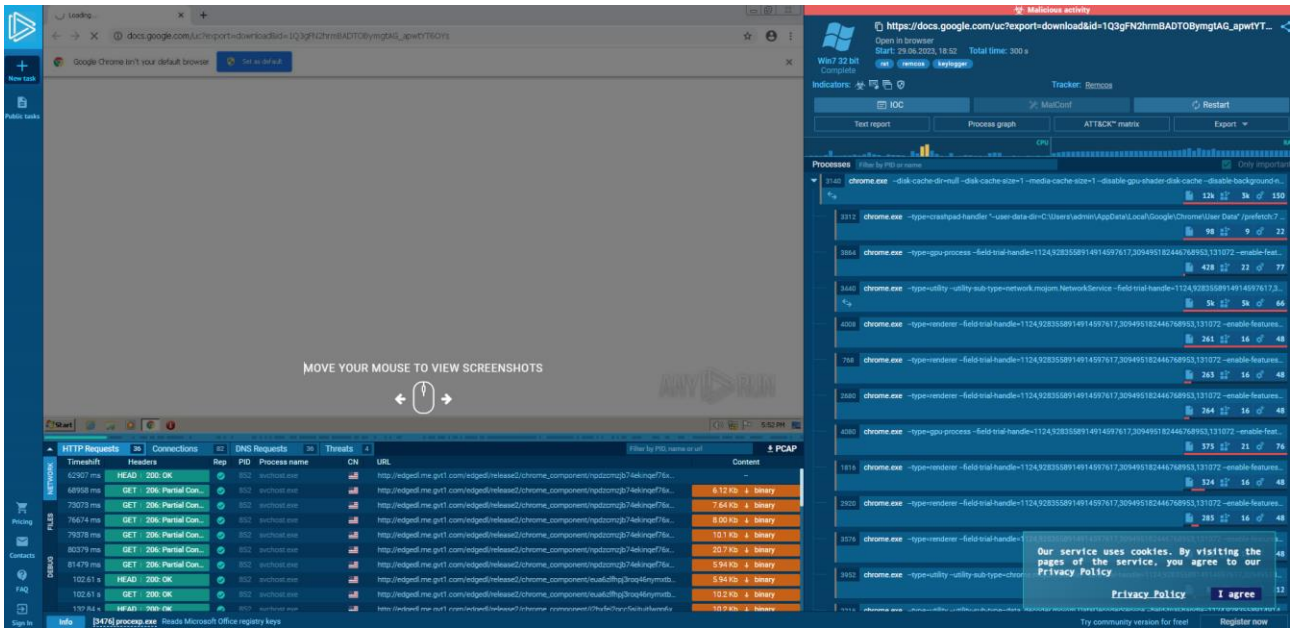
Vale anche la pena installare uno strumento di rimozione malware che aiuti a rilevare malware che Powershell.exe potrebbe aver scaricato sul tuo computer prima che causi problemi.

Come il software antivirus, la scansione del malware può richiedere molte ore a seconda delle dimensioni del disco rigido del computer e della sua velocità.

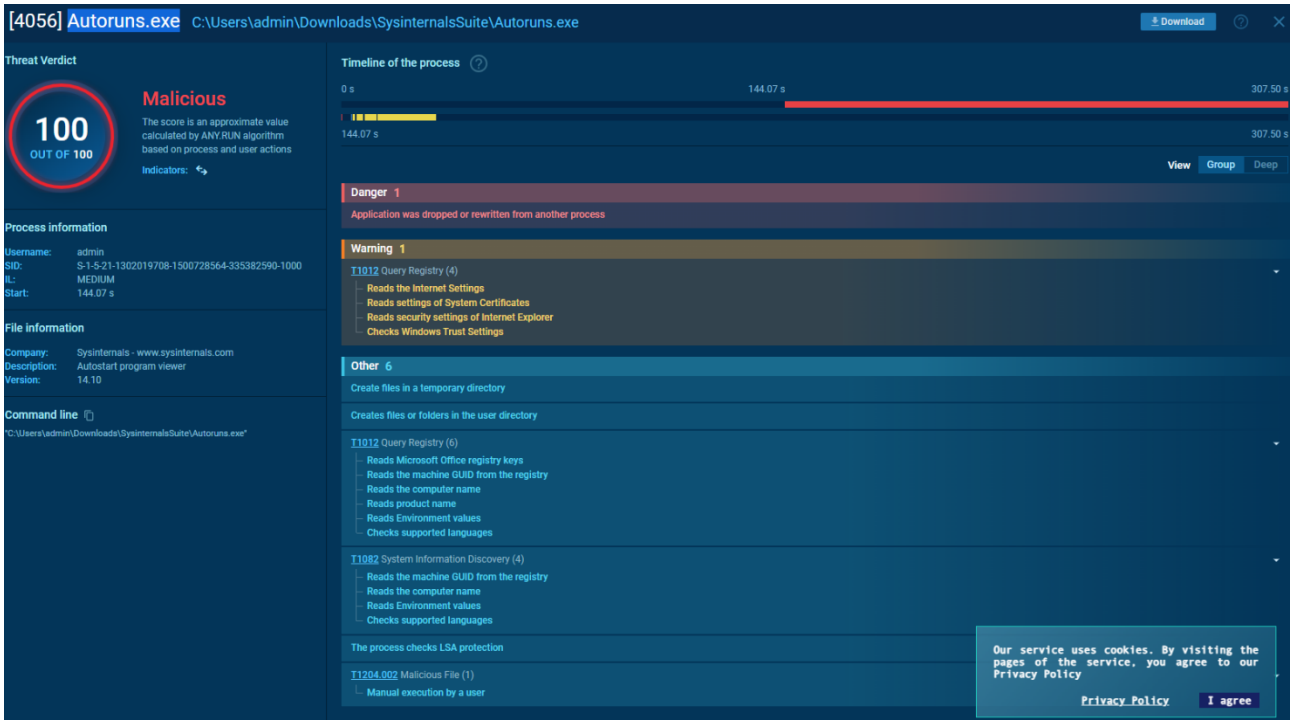
Puoi anche utilizzare Ripristino configurazione di sistema per tornare a un punto precedente sul tuo computer prima di rilevare il virus Powershell.exe. Assicurati di scegliere un periodo di tempo in cui hai la sicurezza che il virus non si trovasse gia' sul tuo computer.

A causa della pericolosità di Powershell.exe, potrebbe essere utile riformattare e reinstallare il sistema operativo. È la migliore garanzia di aver completamente eliminato il virus Powershell.exe dal tuo sistema.

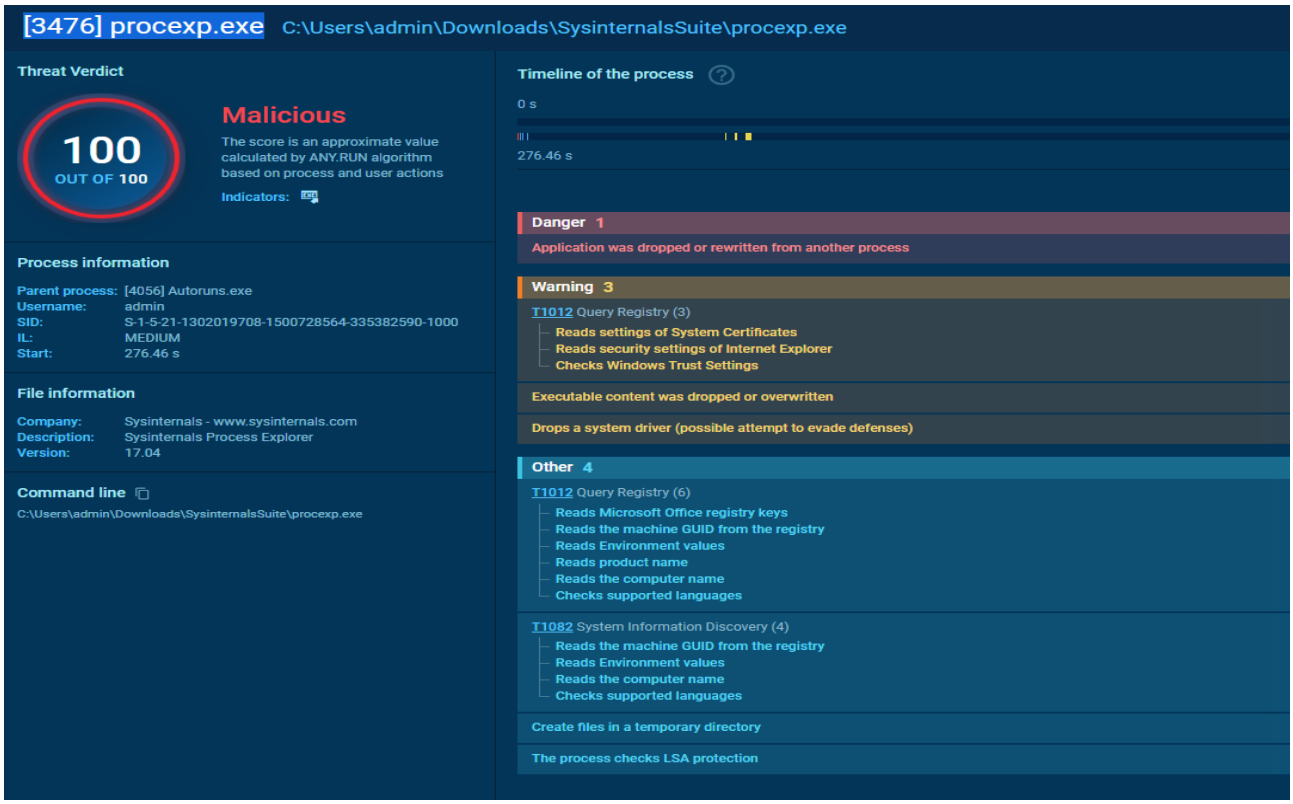
Può richiedere molto tempo e richiede una certa quantità di conoscenza quando si tratta di configurare il computer. Non affrettarti nella decisione e prova prima tutti gli altri metodi.



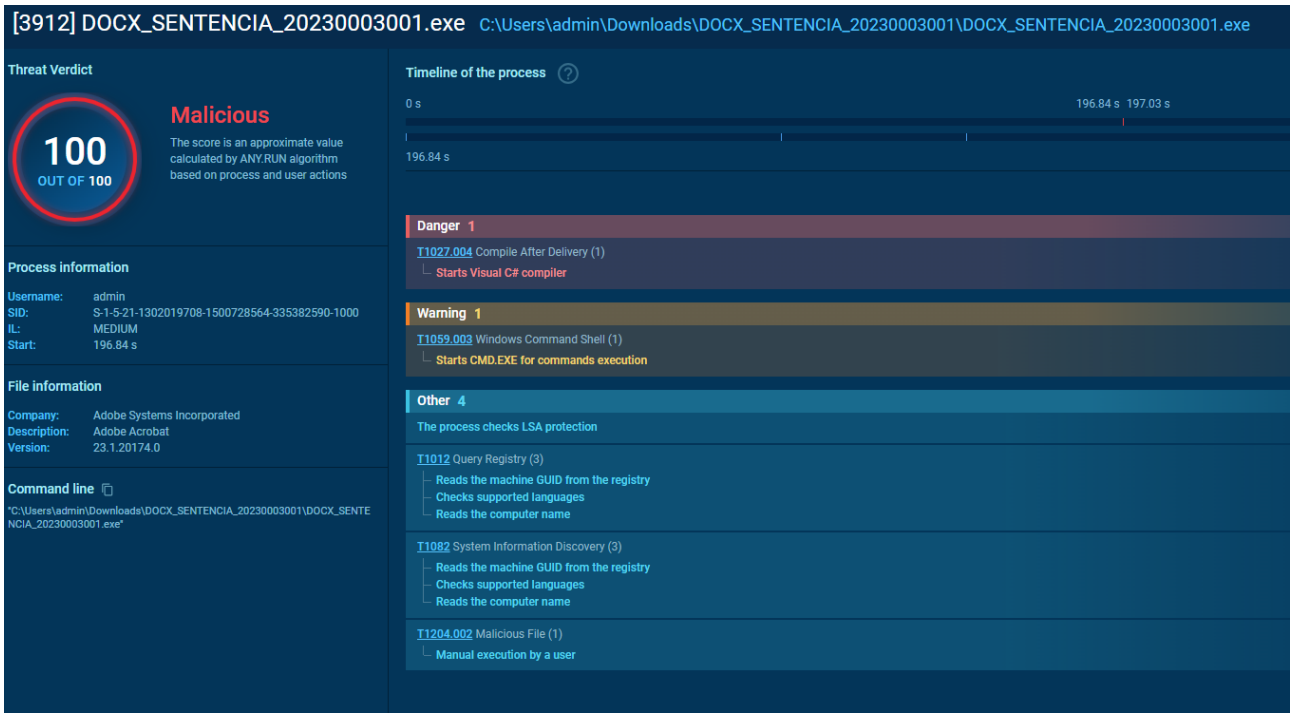

L’utente usa crome per navigare




È una procedura per la ‘avvio automatico di windows (persistenza).




Procexp.exe è un file eseguibile (un programma) per Windows. L'estensione file .exe è l'abbreviazione per *executable* (eseguibile). Avviare solamente file eseguibili da publisher fidati, poiché i file eseguibili potrebbero in teoria alterare le impostazioni del vostro computer o danneggiarlo. Il forum gratuito d'informazioni sui file può essere d'aiuto per scoprire se procexp.exe è un virus, un trojan, spyware, adware che si può rimuovere, oppure un file di sistema appartenente a Windows o un'applicazione di cui ci si può fidare.

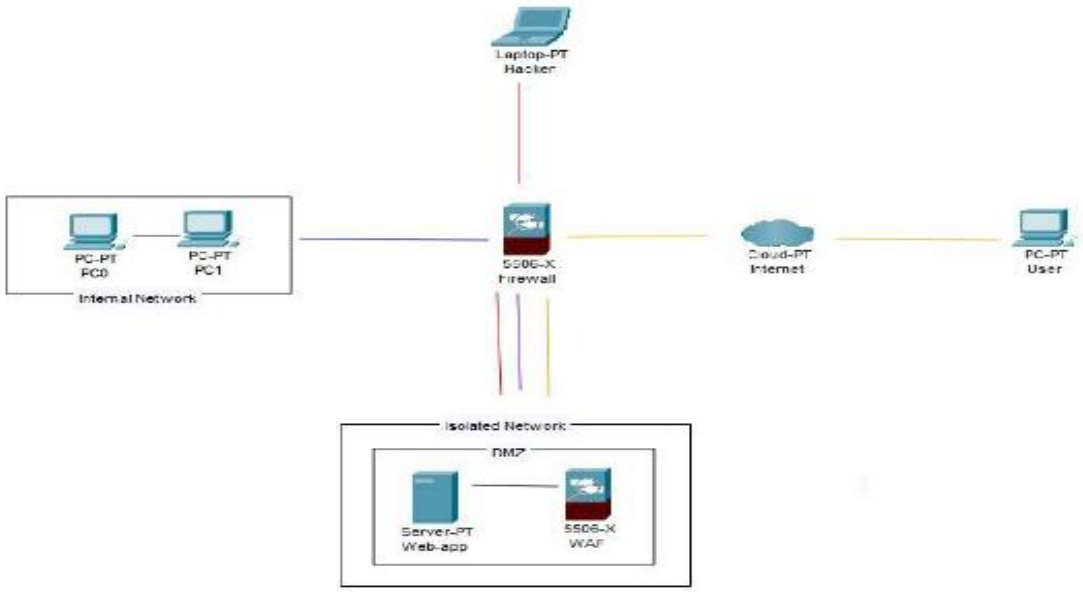


Core.exe è un file eseguibile (un programma) per Windows. L'estensione file .exe è l'abbreviazione per *executable* (eseguibile). Avviare solamente file eseguibili da publisher fidati, poiché i file eseguibili potrebbero in teoria alterare le impostazioni del vostro computer o danneggiarlo. Il forum gratuito d'informazioni sui file può essere d'aiuto per scoprire se core.exe è un virus, un trojan, spyware, adware che si può rimuovere, oppure un file di sistema appartenente a Windows o un'applicazione di cui ci si può fidare.

**3.**

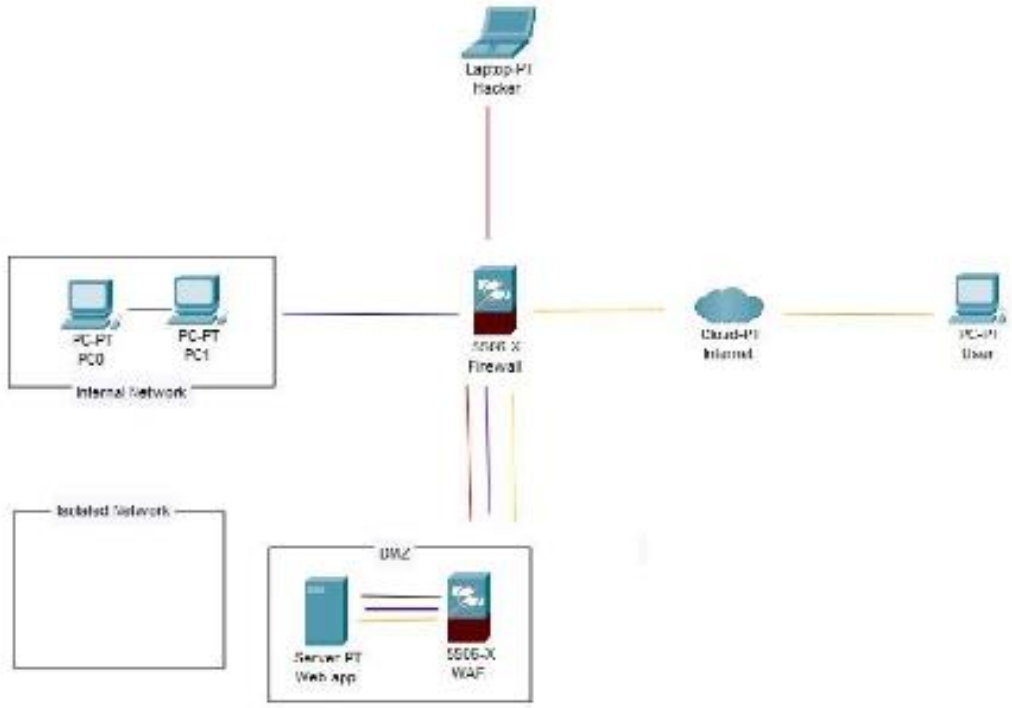
L'applicazione Web è stata infettata da un malware.

Tuttavia il nostro intento, nonostante sia di evitare che si propaghi, è di non rimuovere l'accesso da parte dell'attaccante alla macchina infettata; questo perché la nostra intenzione è quella di osservare le attività e gli obiettivi dell'attaccante. Per far ciò utilizziamo la tecnica dell'isolamento, che consiste la completa disconnessione del sistema infetto dalla rete interna, con tuttavia la possibilità da parte dell'attaccante di accedere ancora con la macchina infettata su internet.




**4.**

1+3




**5.**

Modifiche infrastruttura aggressiva

**IDS** (Intrusion detection system), Si tratta di un strumento che esegue un monitoraggio continuo della sicurezza, allo scopo di identificare in anticipo tutti gli attacchi alle reti informatiche e ai computer.

**NAS** (Network Attached Storage) sono server centrali che forniscono un'archiviazione condivisa per tutti gli utenti appartenenti alla rispettiva rete di computer.

**Server di backup** per la Web-App in caso di disservizio in modo tale da causare un disservizio minimo in caso di problemi.

**UPS** è un dispositivo in grado di fornire temporaneamente alimentazione agli apparecchi elettrici quando sopraggiungono cali di tensione, disturbi oppure vere e proprie interruzioni della corrente.

**Piú reti** per la diversificazione in piú per la NAS è possibile accedere nella rete locale ed a determinati IP in modo tale da avere + layer di sicurezza.

**DOCKER** un popolare software libero progettato per eseguire processi informatici in ambienti isolabili, minimali e facilmente distribuibili chiamati container, con l'obiettivo di semplificare i processi di deployment di applicazioni software.

Quindi in caso di disservizio sarà possibile spostare la web-app infetta in una rete isolata e avviare all'istante il server di scorta con il backup di docker della web-app.