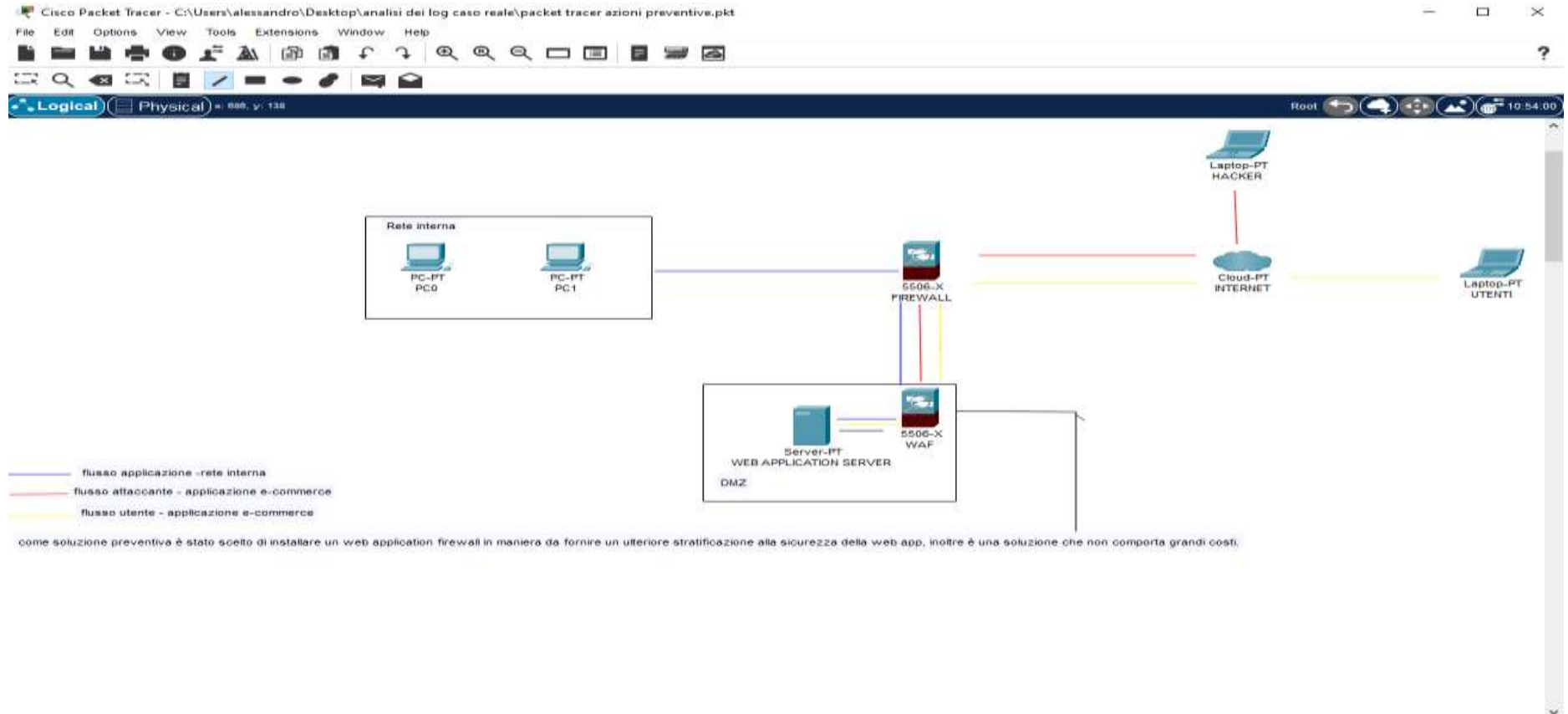
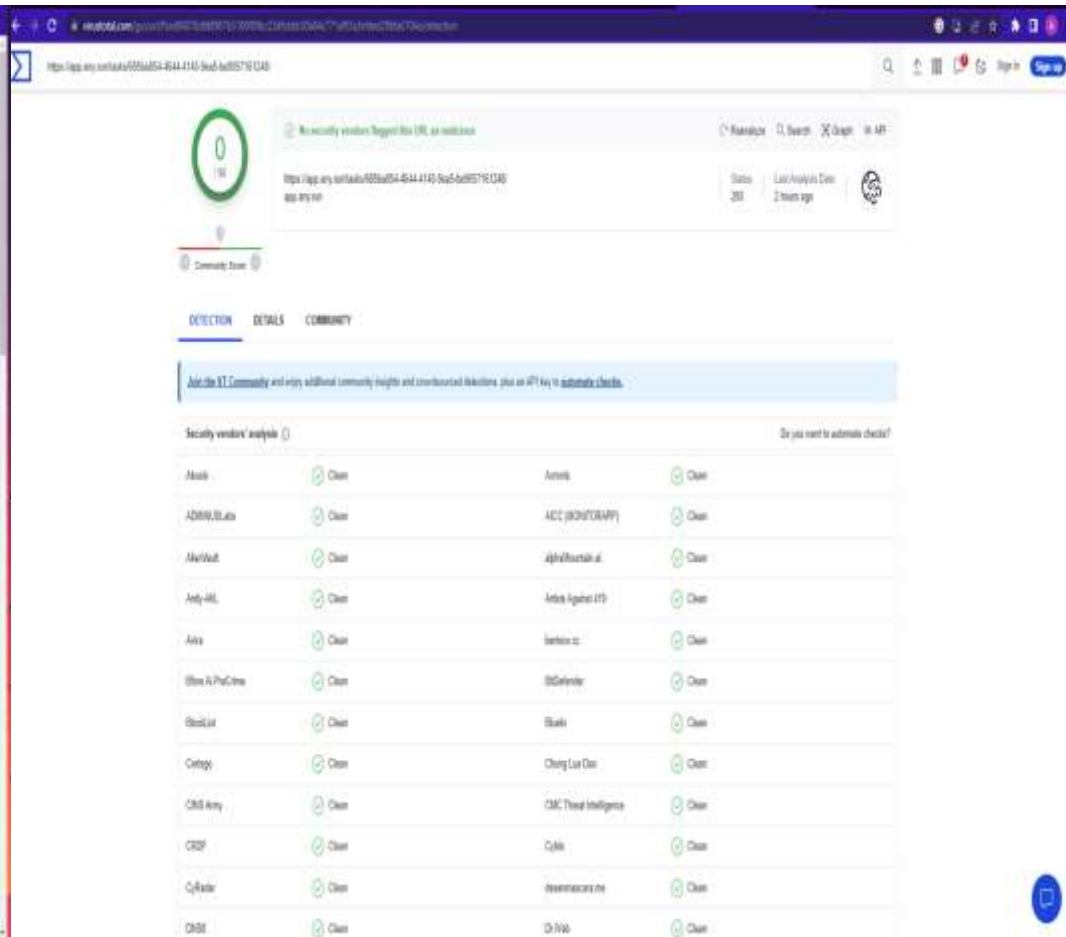
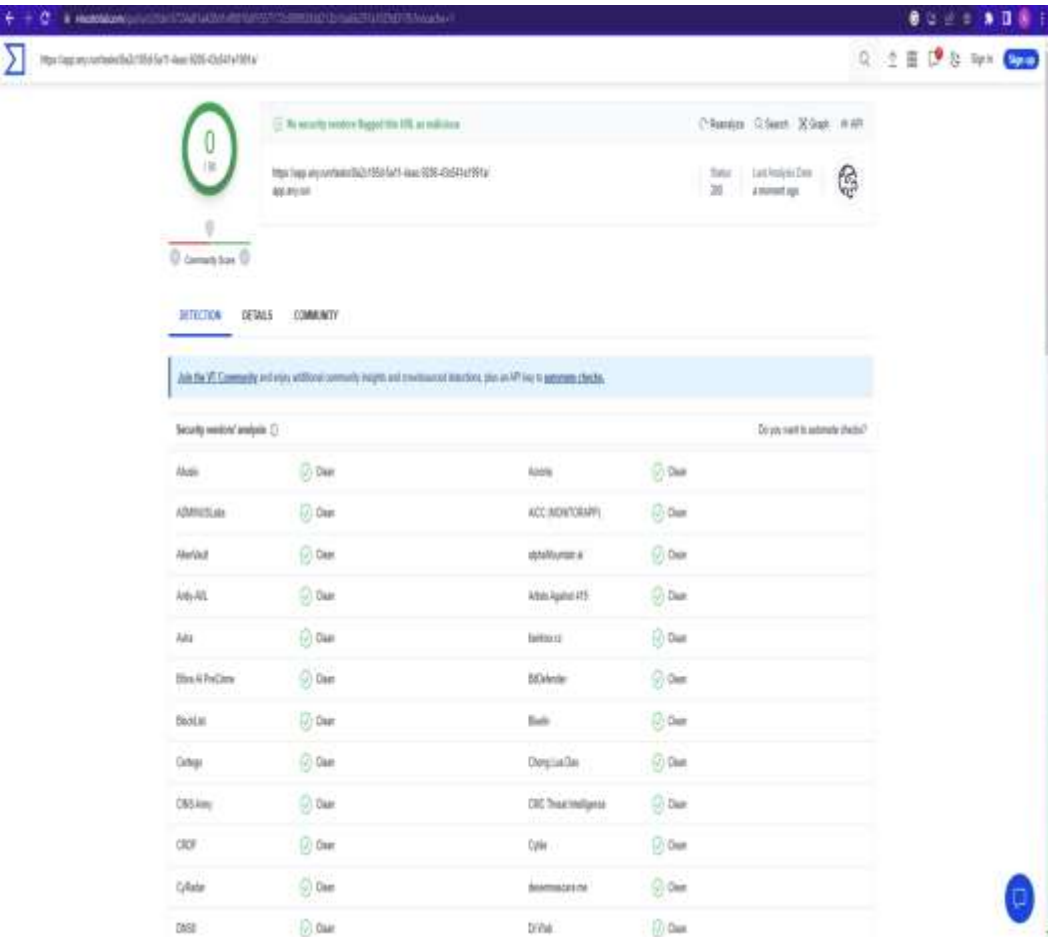


Traccia 1 Bossi Alessandro



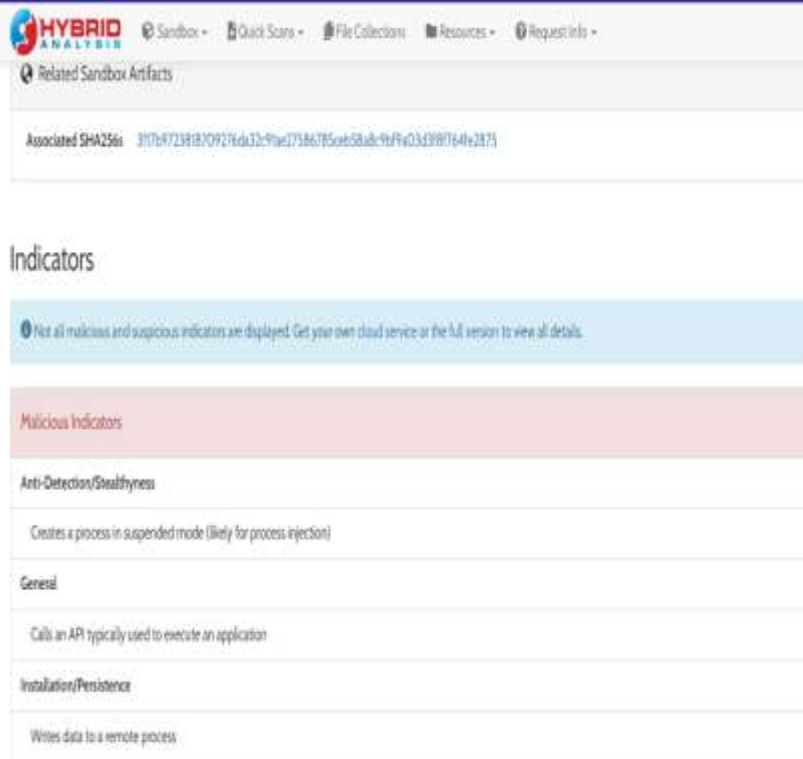
La soluzione preventiva che ho adottato è stato l'inserimento di un WAF per la protezione della web app. Oltre a questo potrebbe essere migliorata lato backend la pagina di log-in in maniera da inserire controlli che evitino attacchi XSS e SQLI

Traccia 2



Per analizzare i link proposti nel secondo punto della traccia ho utilizzato “VirusTotal” per verificare che non fossero malevoli, non trovando nessuna evidenza di virus o malware.

Traccia 2



HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

Related Sandbox Artifacts

Associated SHA256: 317b9723818709276d32c9fac27586785c6b58abc9f9c3d3980764e2875

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators

Anti-Detection/Stealthiness

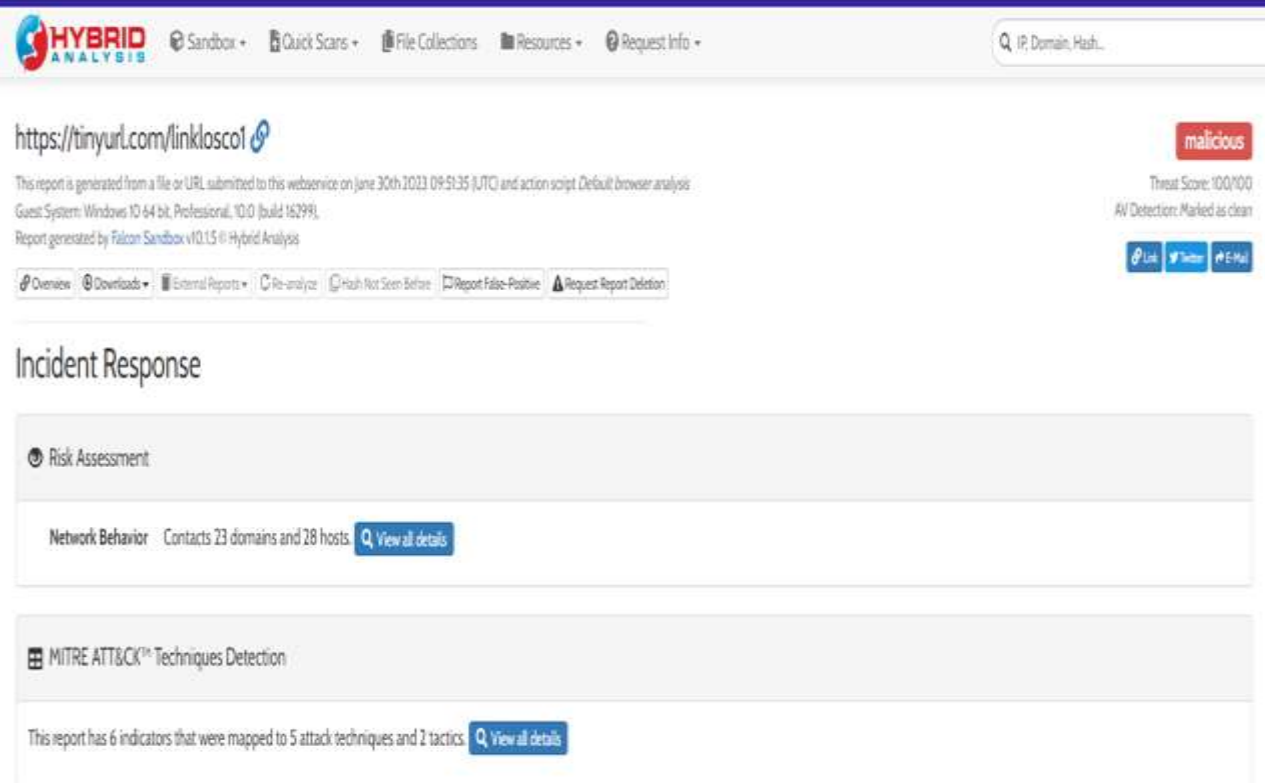
Creates a process in suspended mode (likely for process injection)

General

Calls an API typically used to execute an application

Installation/Persistence

Writes data to a remote process



HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

IP, Domain, Hash...

malicious

Threat Score: 100/100
AV Detection: Marked as clean

[Link](#) [Twitter](#) [E-Mail](#)

[Overview](#) [Downloads](#) [External Reports](#) [Re-analyze](#) [Hash Not Seen Before](#) [Report False-Positive](#) [Request Report Deletion](#)

Incident Response

Risk Assessment

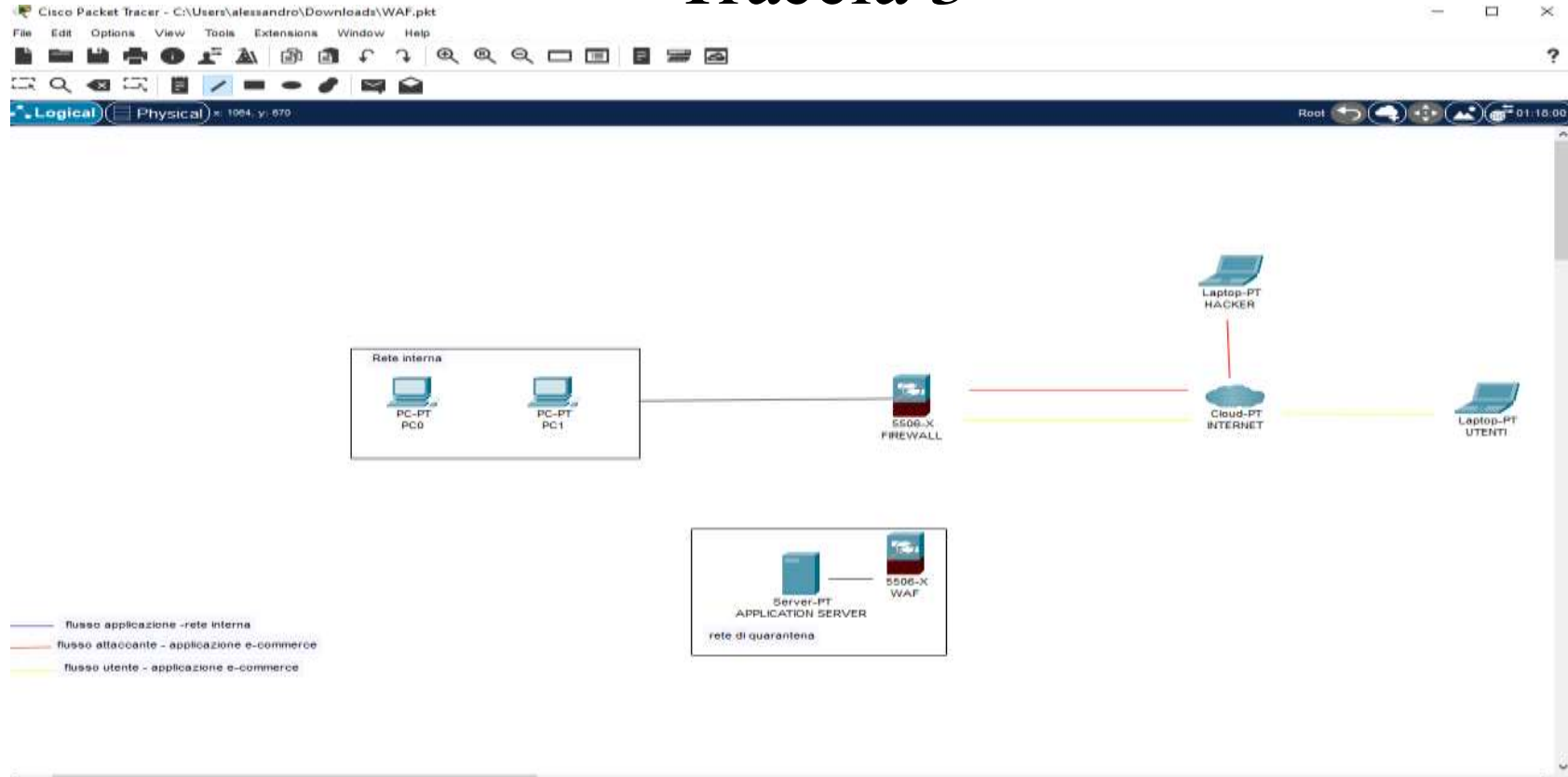
Network Behavior Contacts 23 domains and 28 hosts [View all details](#)

MITRE ATT&CK™ Techniques Detection

This report has 6 indicators that were mapped to 5 attack techniques and 2 tactics [View all details](#)

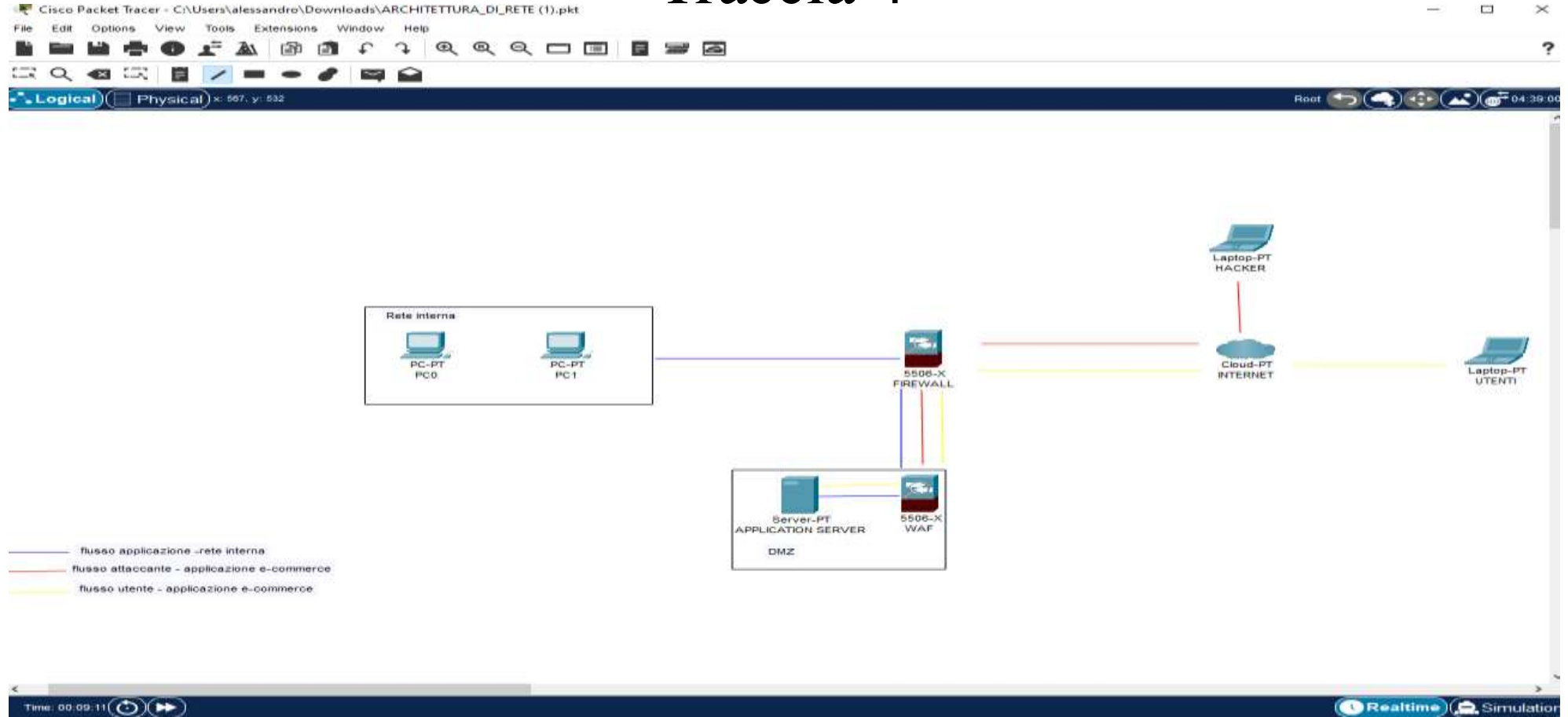
Decido di utilizzare un altro tool per la scansione, Hybrid Analysis e con questo riesco a rilevare la presenza di codice malevolo all'interno del link. In particolare come si vede nello screen di sinistra ci sono degli indicatori che spiegano come crei un processo non individuabile poiché in modalità sospesa, come richiami un API per l'esecuzione di

Traccia 3



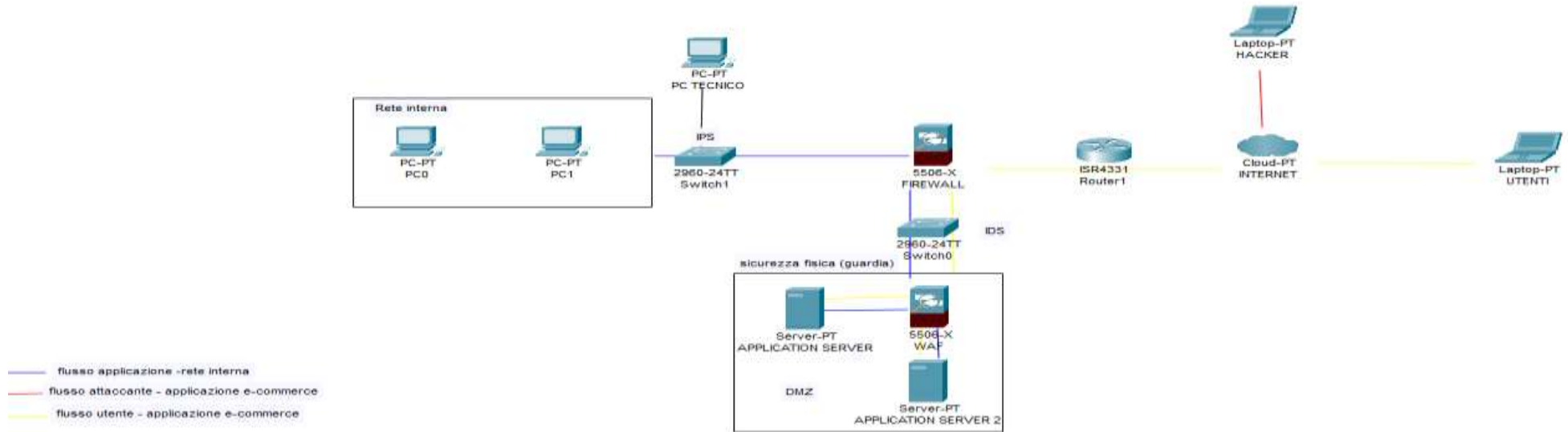
Avendo stabilito e verificato che l'app web è stata infettata, procedo con la rimozione dalla rete sia internet che interna, in questa maniera posso avviare le procedure di rimozione incidente eliminando quindi tutte le tracce rimaste dell'attacco all'interno del server senza correre il rischio di divulgazioni di informazioni sensibili o di infettare la

Traccia 4



Una volta che la minaccia è stata eliminata definitivamente possiamo ripristinare la normale operatività del web server recuperando i dati tramite backup, applicando patch e revisionando eventuali politiche del firewall in maniera tale che l'attacco non possa

Traccia 5



L'ultima struttura di rete prevede l'implementazione di altri sistemi di sicurezza aggiuntivi, quali IPS e IDS, la creazione di un secondo application server, l'installazione di switch e router aggiuntivi, la creazione di un ufficio per il tecnico che monitora gli eventi in tempo reale, una guardia di sicurezza che provveda a fornire l'accesso ai server