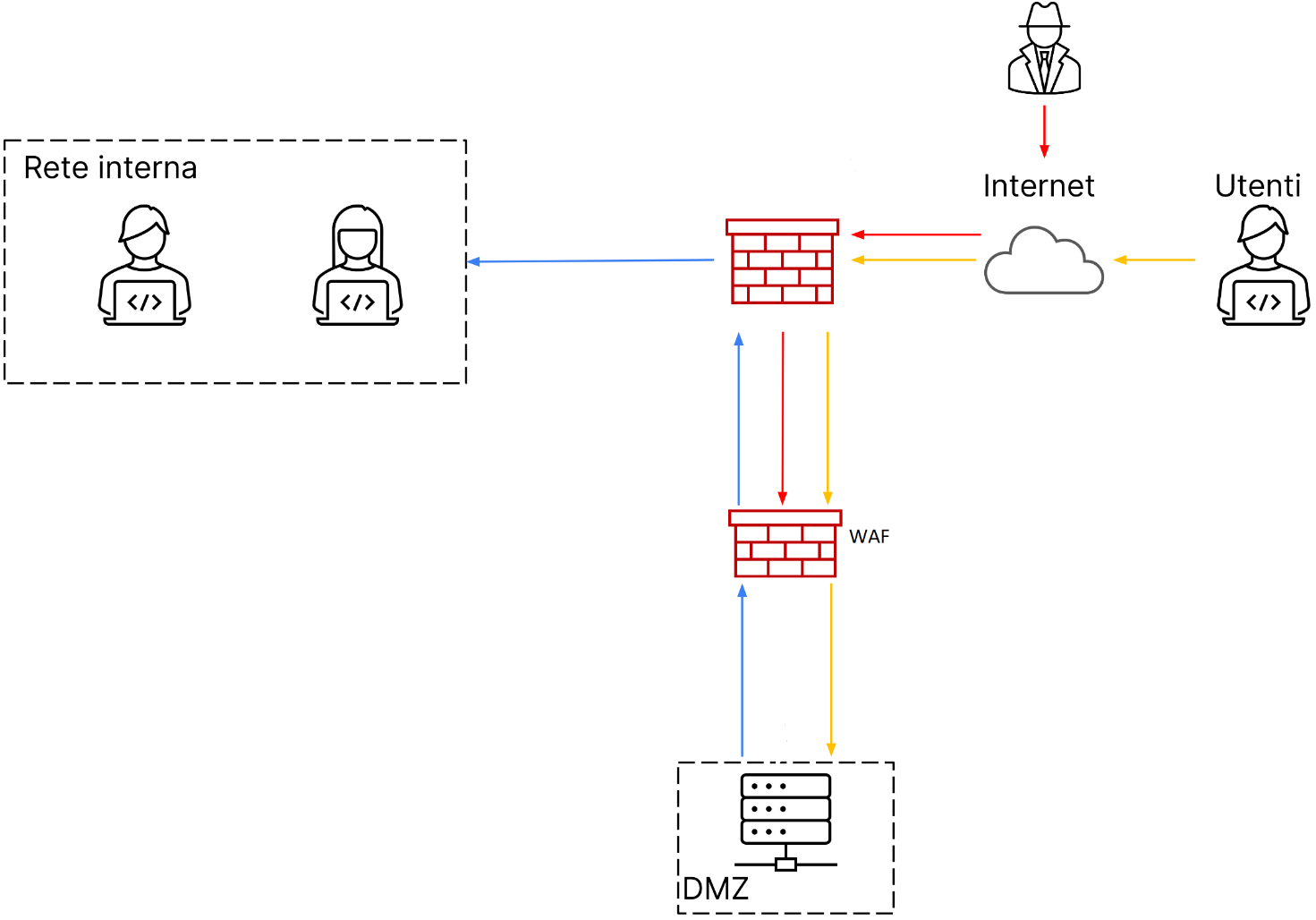
**PROGETTO**

1. **Azione preventiva**

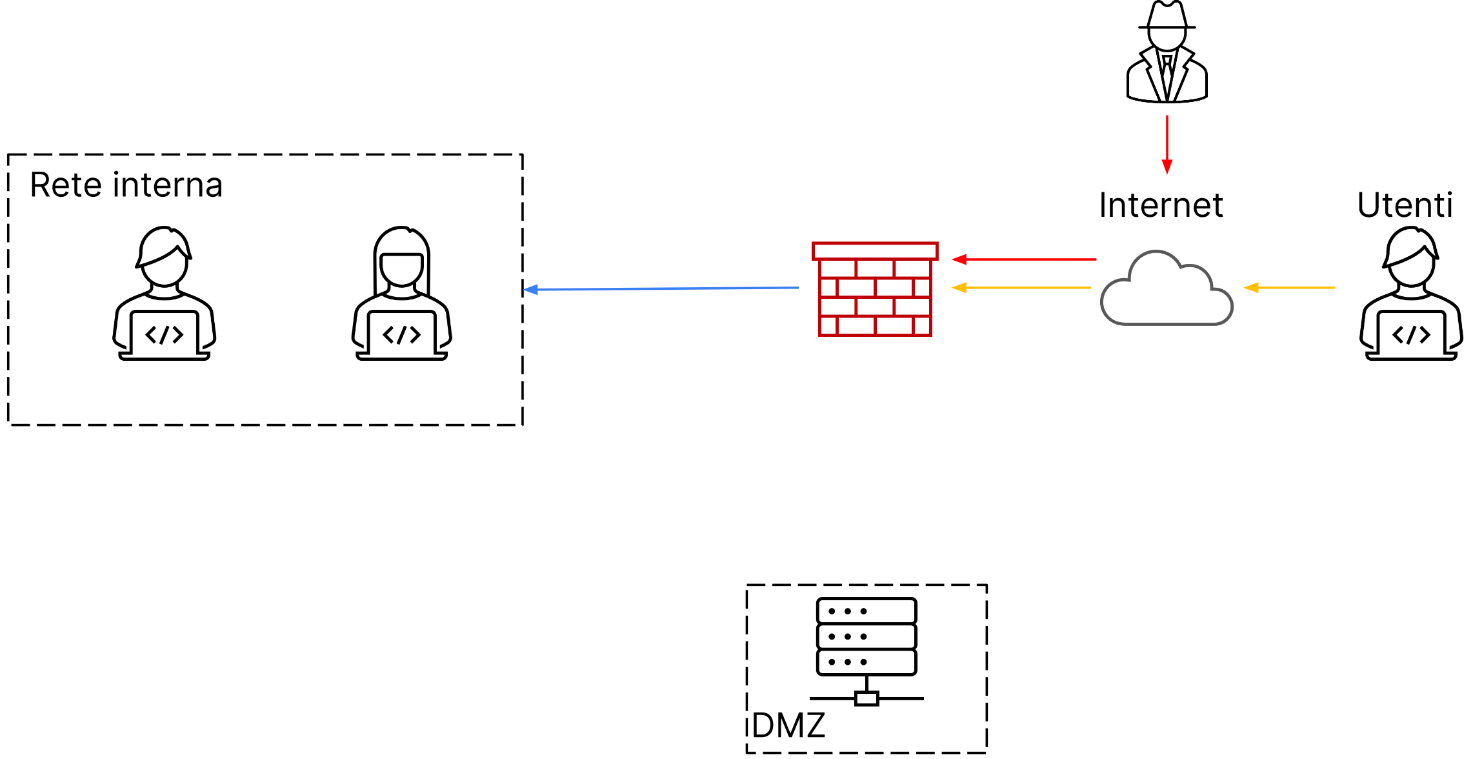
Nel primo punto ci viene richiesto di adottare misure di sicurezza preventive al fine di implementare la difesa di un’applicazione web da attacchi di tipo SQL injection e XSS che ricordiamo essere molto pericolosi in quanto un utente malintenzionato potrebbe cosi facendo rubare dati sensibili degli utenti del sito (nel primo attacco agendo back-end quindi direttamente sul database mentre il secondo front-end)



Come si vede nello schema riportato sopra aggiungendo un WAF (Web Application Firewall) potremmo impedire all’attaccante di eseguire tali operazioni malevole sul server di una web app in quanto nello specifico è configurato proprio per questo tipo di vulnerabilità.

**3. Response**

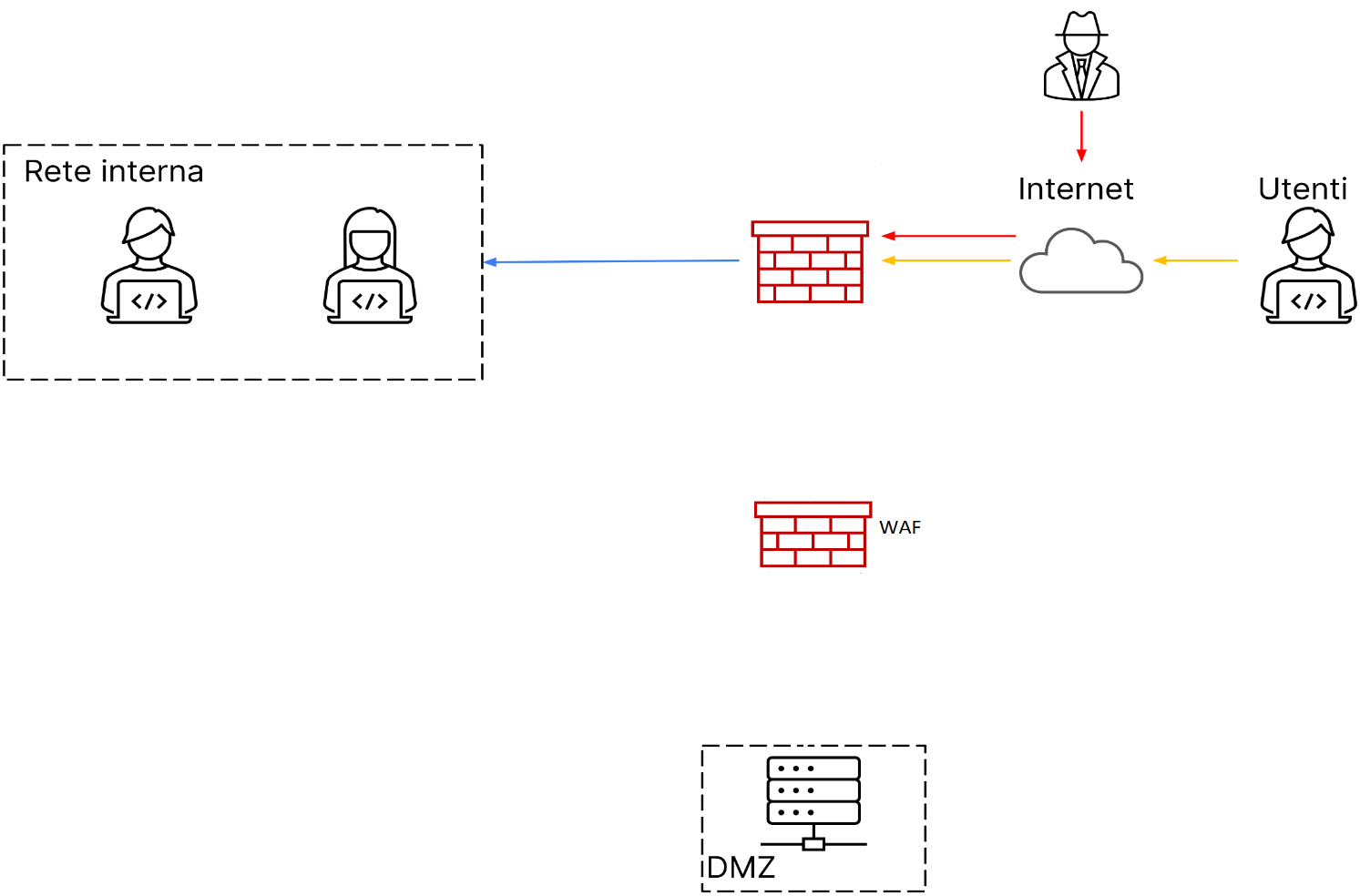
Nel terzo punto invece viene chiesto di agire nel momento in cui l’applicazione web è stata infettata da un malware. La priorità nello specifico è che il virus non si propaghi sulla rete interna aziendale e non divulgando informazioni sensibili verso Internet.



Si procede cosi rimuovendo completamente la DMZ con il server dell’app e-commerce sia dalla rete interna che da Internet in modo tale che l’attaccante non possa avere accesso ne al sito e ne alla rete interna.

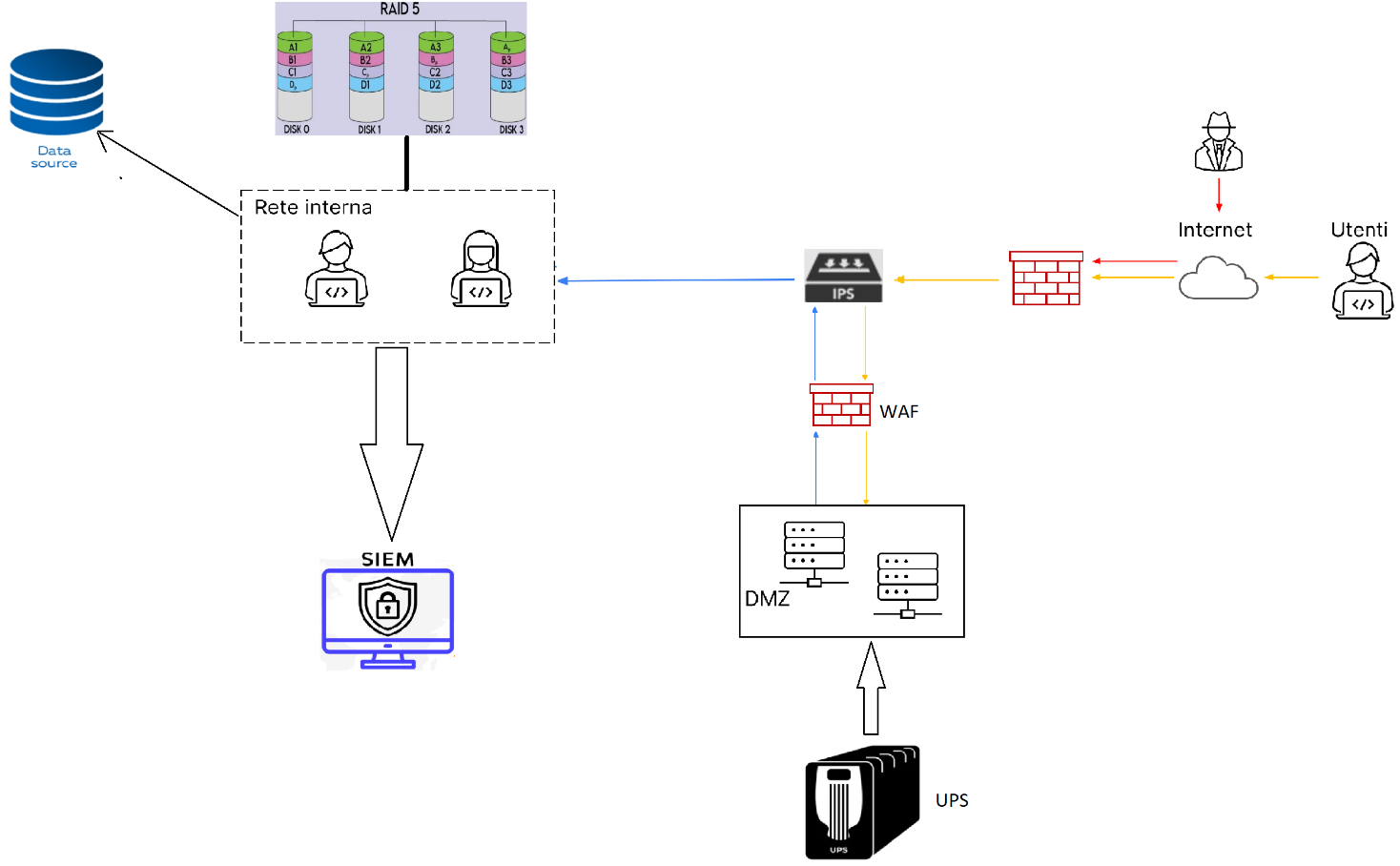
**4. Soluzione completa**

Nella figura che segue è presentata la soluzione completa in cui è raffigurata sia l’operazione di prevenzione sia di response quando l’incidente è avvenuto (quest’ultima messa appunto in pratica attraverso la terza fase dell’Incident Response Plan eseguito dal CSIRT).



**5. Modifica “più aggressiva” dell’infrastruttura**

E’ possibile implementare la difesa modificando l’infrastruttura di un’azienda attraverso ulteriori misure di sicurezza ovviamente anche in base alla disponibilità di capitale dell’azienda stessa.



Nell’esempio riportato nello schema sopra abbiamo aggiunto:

* IPS/IDS come misura aggiuntiva ad un firewall che blocca eventuali intrusioni. Se l’azienda puo permettersi di investire molto capitale sulla sicurezza della propria infrastruttura si sarebbe potuto installare direttamente un firewall next gen che risulta molto più efficace e che effettua un’analisi molto approfondita su tutti e 7 i livelli della pila ISO/OSI
* WAF (Web Application Firewall) per prevenire attacchi di tipo SQLi e XSS
* Un secondo web server sincronizzato nella DMZ nel caso in cui si verifichi un errore in quello principale e smetta di funzionare (Failover Cluster)
* UPS (generatore di corrente) sui server web nell’eventualità di una temporanea mancanza di corrente elettrica
* SIEM (Security information and event management) ovvero un sistema centralizzato che riceve file di log dai dispositivi nella rete interna attraverso l’installazione di agent sugli stessi in modo tale da poter tracciare tutte le attività dei dipendenti ed avvisare il management di eventuali anomalie tramite alert. (Gli orari devono essere sincornizzati)
* RAID -5 per la protezione dei dischi. In questo modo se uno si dovesse rompere le operazione continueranno con il funzionamento di un altro disco. In questa configurazione si utilizzano 3 o più unità.
* Full backup di tutti i dati supponendo che ci sia grossa disponibilità di spazio
* Antivirus che anche se non schematizzato in figura rappresenta sempre una delle migliori misure di sicurezza per la triade CIA

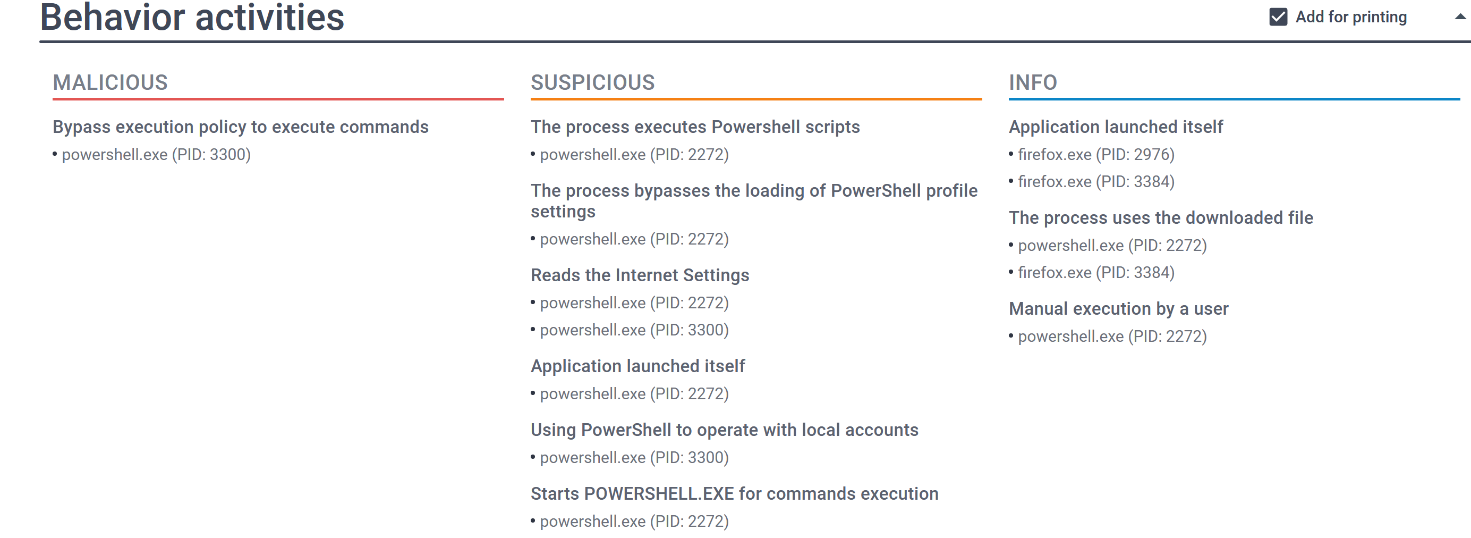
1. **Analisi attacco**

<https://tinyurl.com/linklosco1>

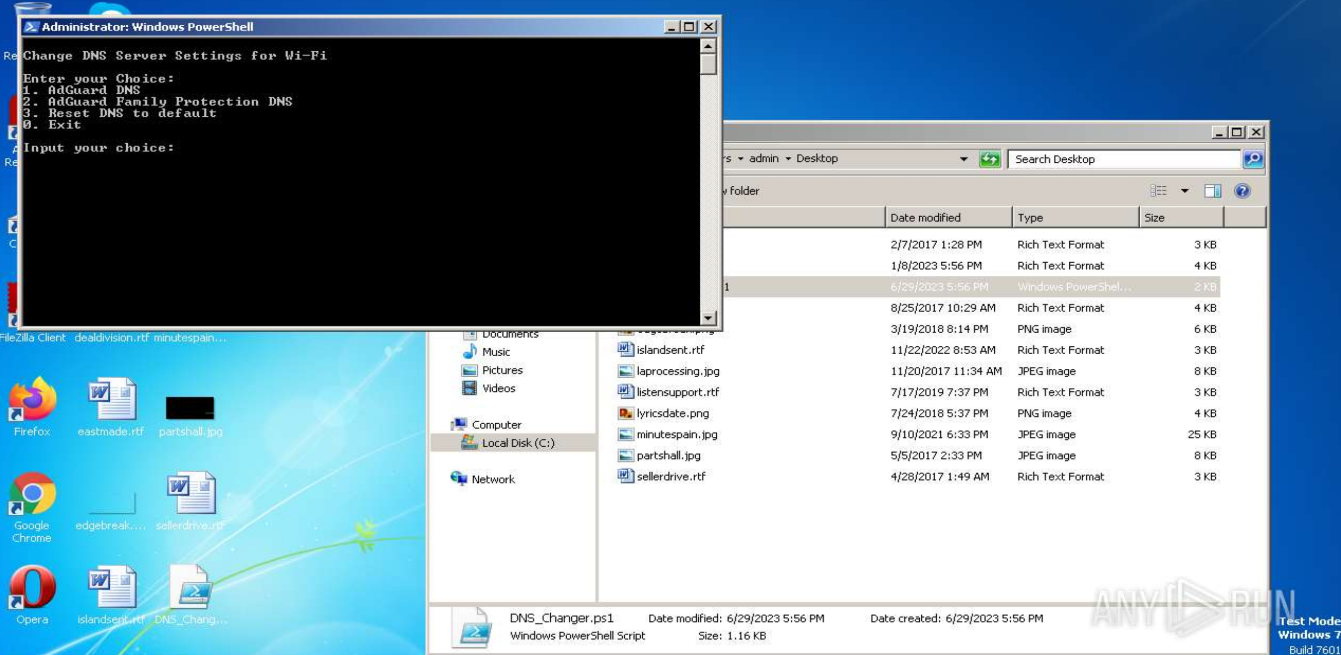


Any run è uno strumento importantissimo per il monitoraggio e l’analisi di minacce informatiche in tempo reale.

Cliccando sulla sezione *text report* si nota che il primo link fa riferimento ad un url malevolo come indicato nell’immagine sopra (attività sospetta) con relative ulteriori info (OS, data e ora…)



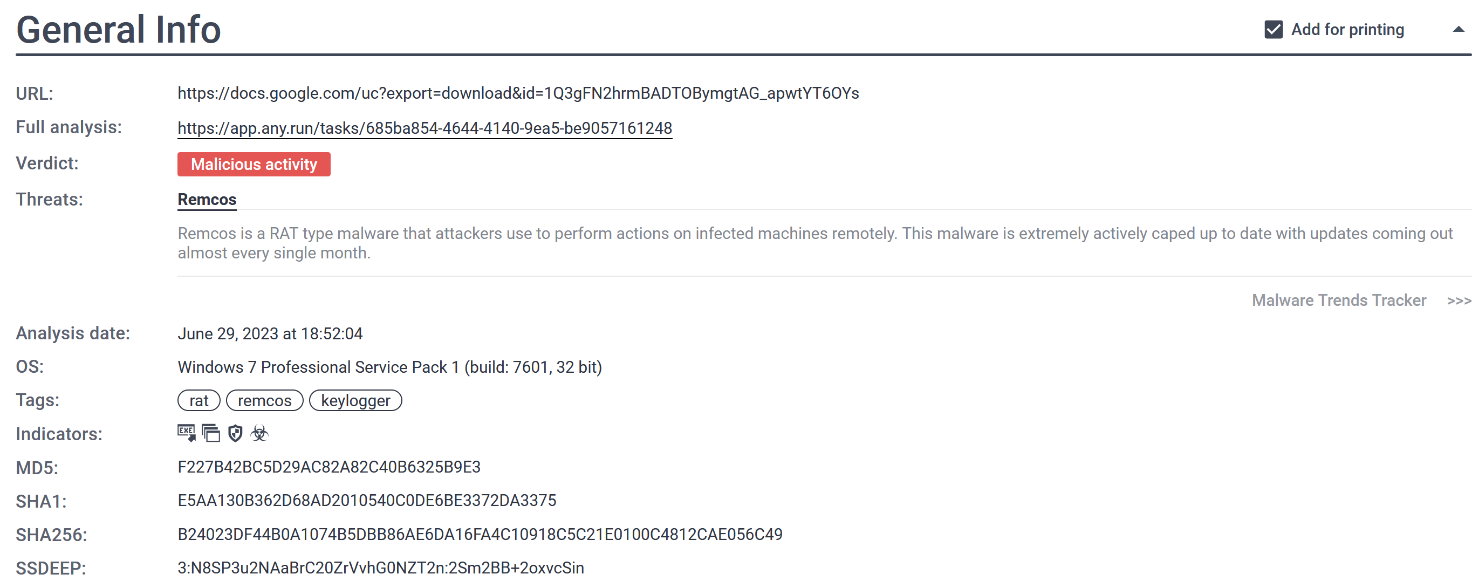
Nello specifico risulta uno script che esegue una shell di windows bypassando le policy di esecuzione per eseguire comandi.



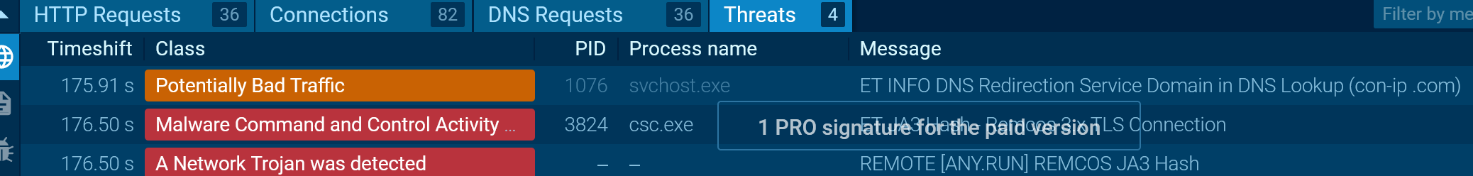
In questo caso permette la modifica da amministratore delle impostazioni DNS.

E’ possibile vedere il codice malevolo dalle instantanee riportate.

<https://tinyurl.com/linklosco2>



Nell’analisi del secondo link invece si evince la presenza di un’attività malevola e tra i tag riportati si puo capire che si tratta di un remcos trojan che consente una serie di operazioni tra cui l’installazione di eseguibili malevoli con nomi di file innocui. Permette la lettura delle impostazioni di internet e puo installare una backdoor usando porte inusuali. Inoltre installa keylogger per rubare dati sensibili attraverso gli input che la vittima digita sulla tastiera.



Sempre nella sezione *text report* è possibile leggere ulteriori info.

