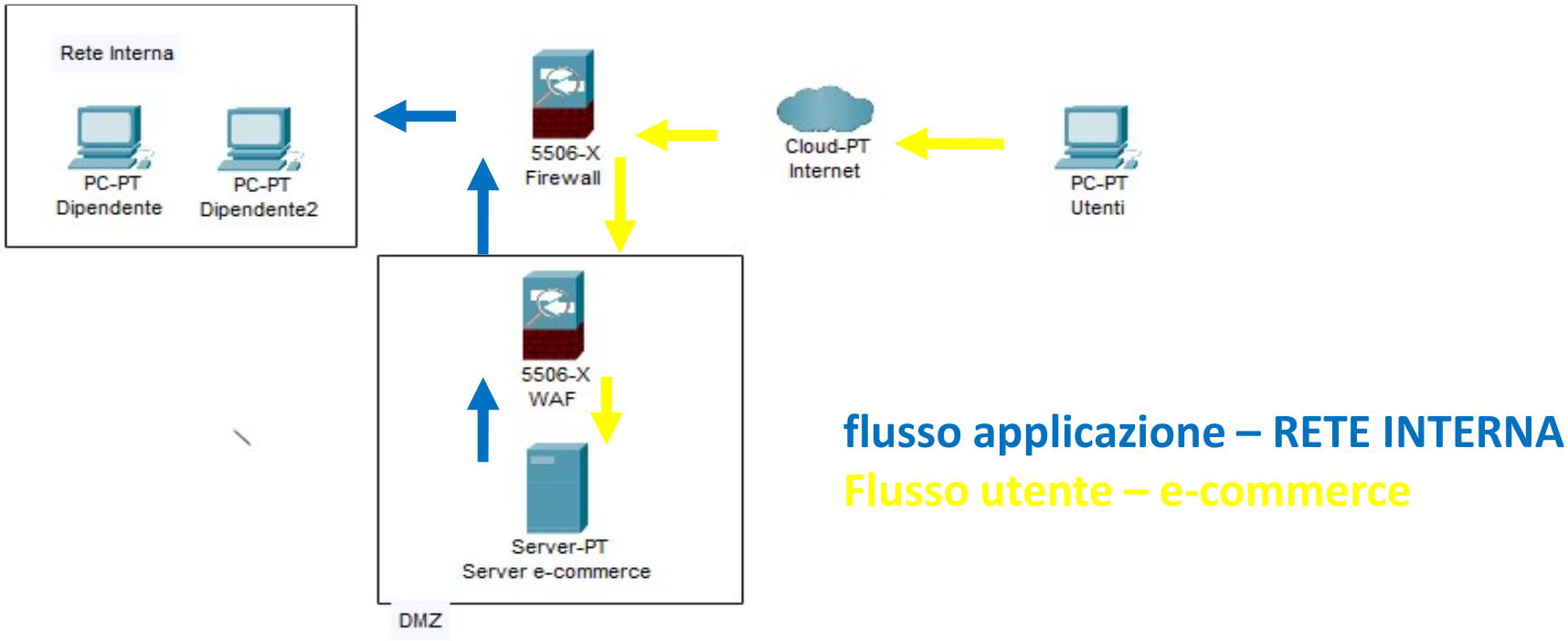
PROGETTO MODULO 7

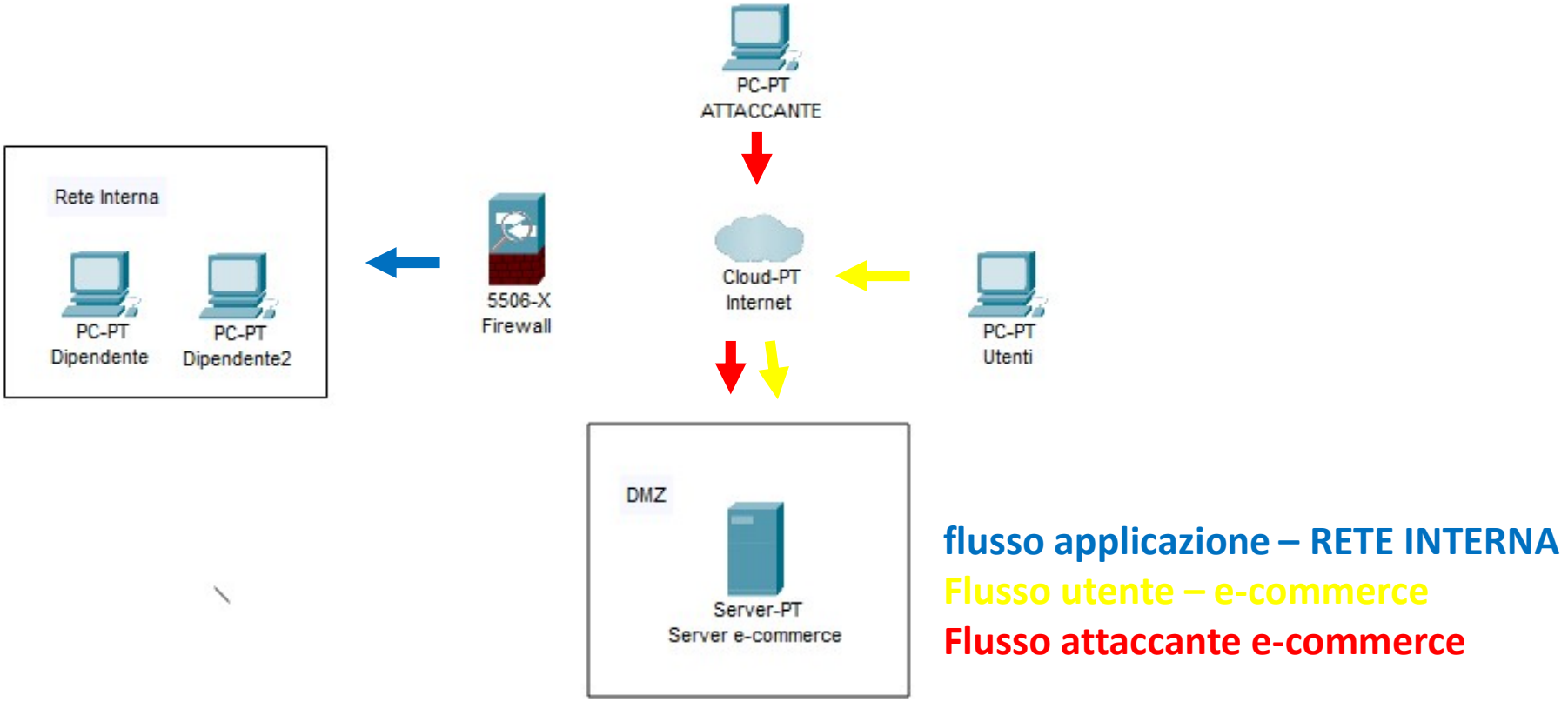
Per la realizzazione di questo progetto, bisognava occuparsi di vari casi e trovare la soluzione migliore.

1. AZIONE PREVENTIVA: il primo punto ci chiedeva di trovare un'azione preventiva per difendere l'applicazione web da attacchi SQLi e XSS. La soluzione che ho attuato per evitare questi tipi di attacchi è stata mettere una WAF(Web Application Firewall) che offre una protezione specifica per le applicazioni web.

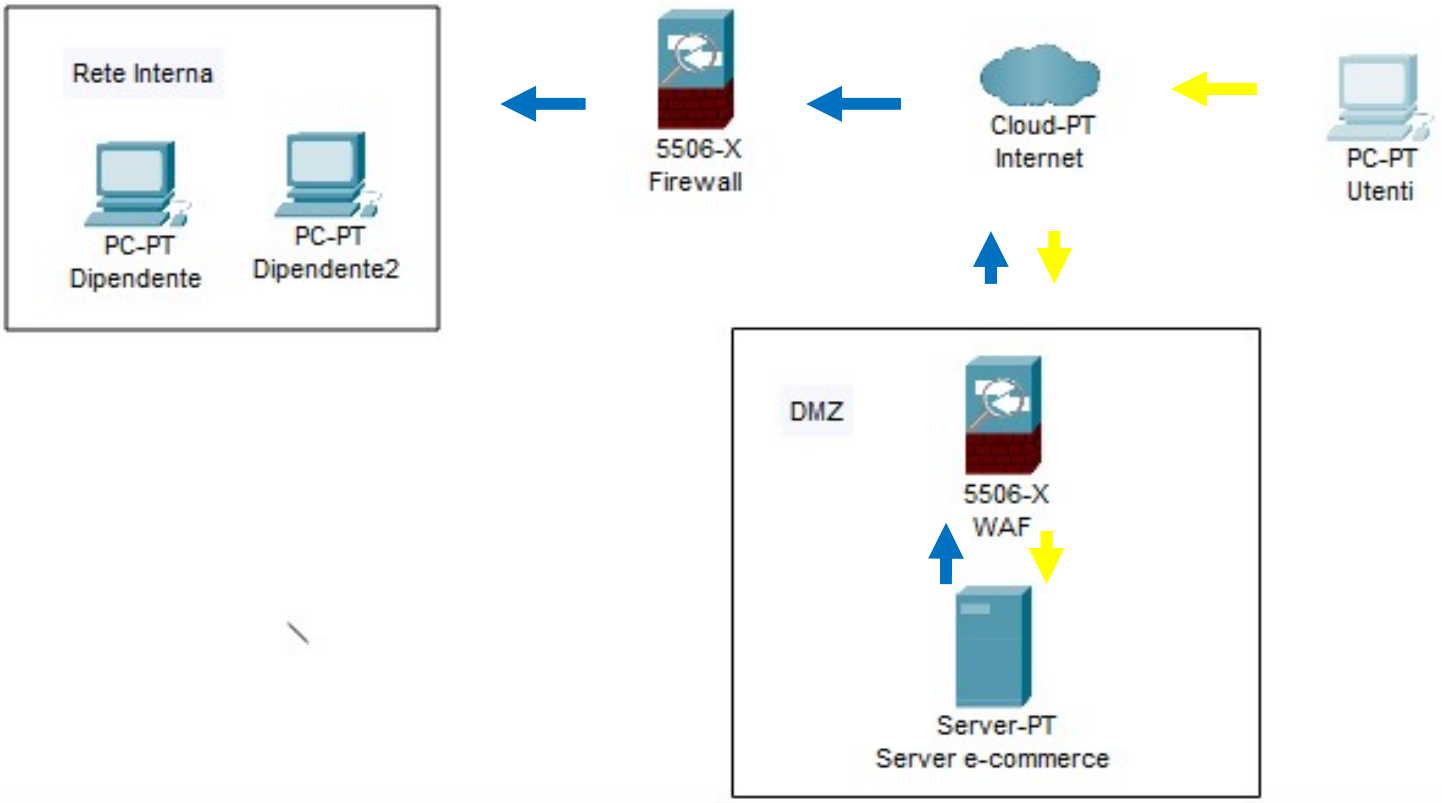


3. RESPONSE: il terzo punto ci informa che l'applicazione web è stata infettata da un malware. La priorità è quella di non far propagare il malware sulla rete, ma al tempo stesso non bisogna divulgare informazioni sensibili verso internet.

Per non far propagare il malware, ho isolato il server e-commerce facendolo comunicare solo con internet, così la rete interna e al sicuro; ma l'attaccante ha comunque accesso verso l'applicazione web.



4. SOLUZIONE COMPLETA: questo punto richiedeva di unire il punto 1 **(L'AZIONE PREVENTIVA)** con il punto 3 (**RESPONSE**)

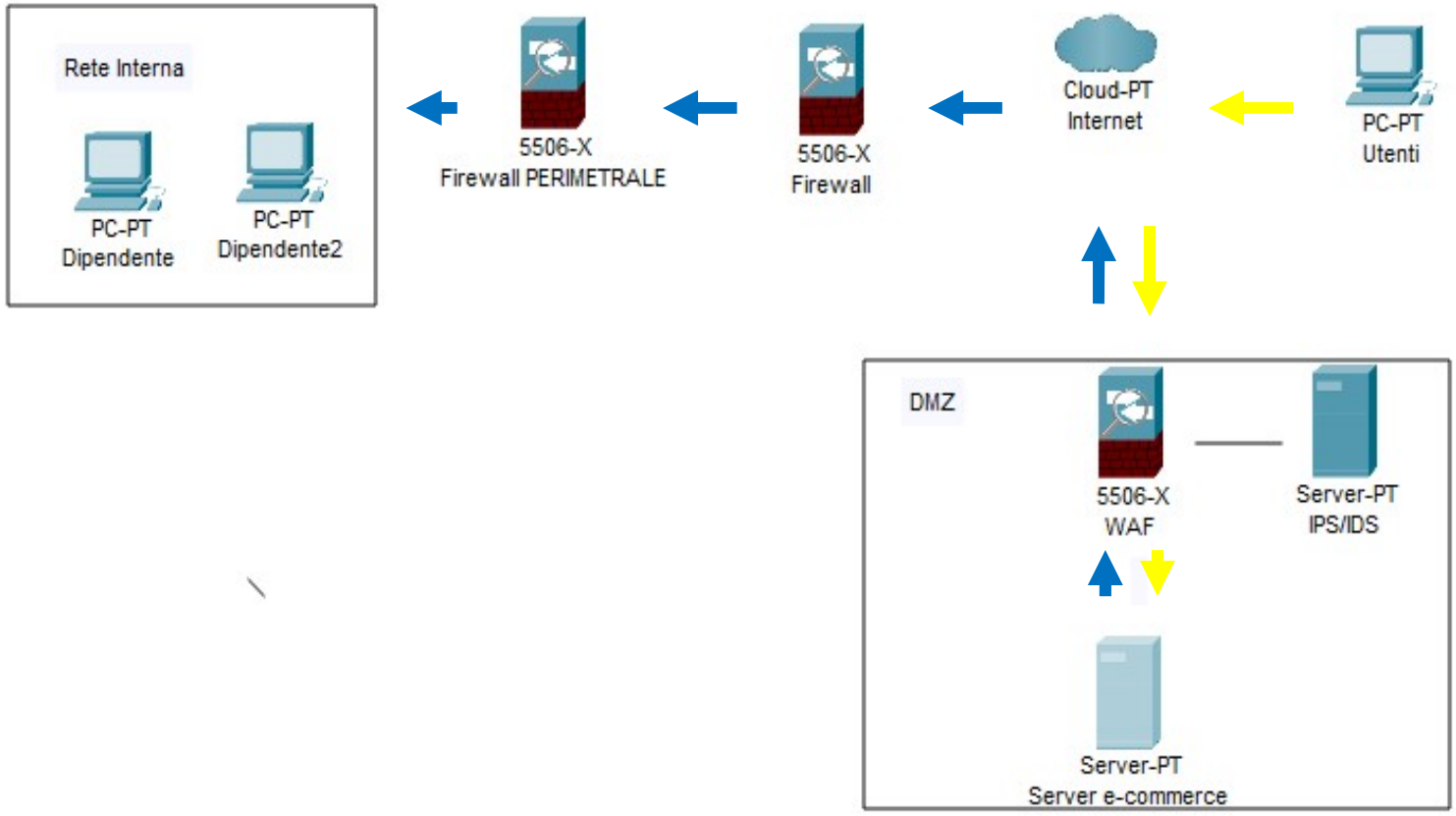


flusso applicazione – RETE INTERNA

Flusso utente – e-commerce

5. MODIFICA << più aggressiva>> DELL'INFRASTRUTTURA: in questo punto si dovevano aggiungere altri elementi di sicurezza.

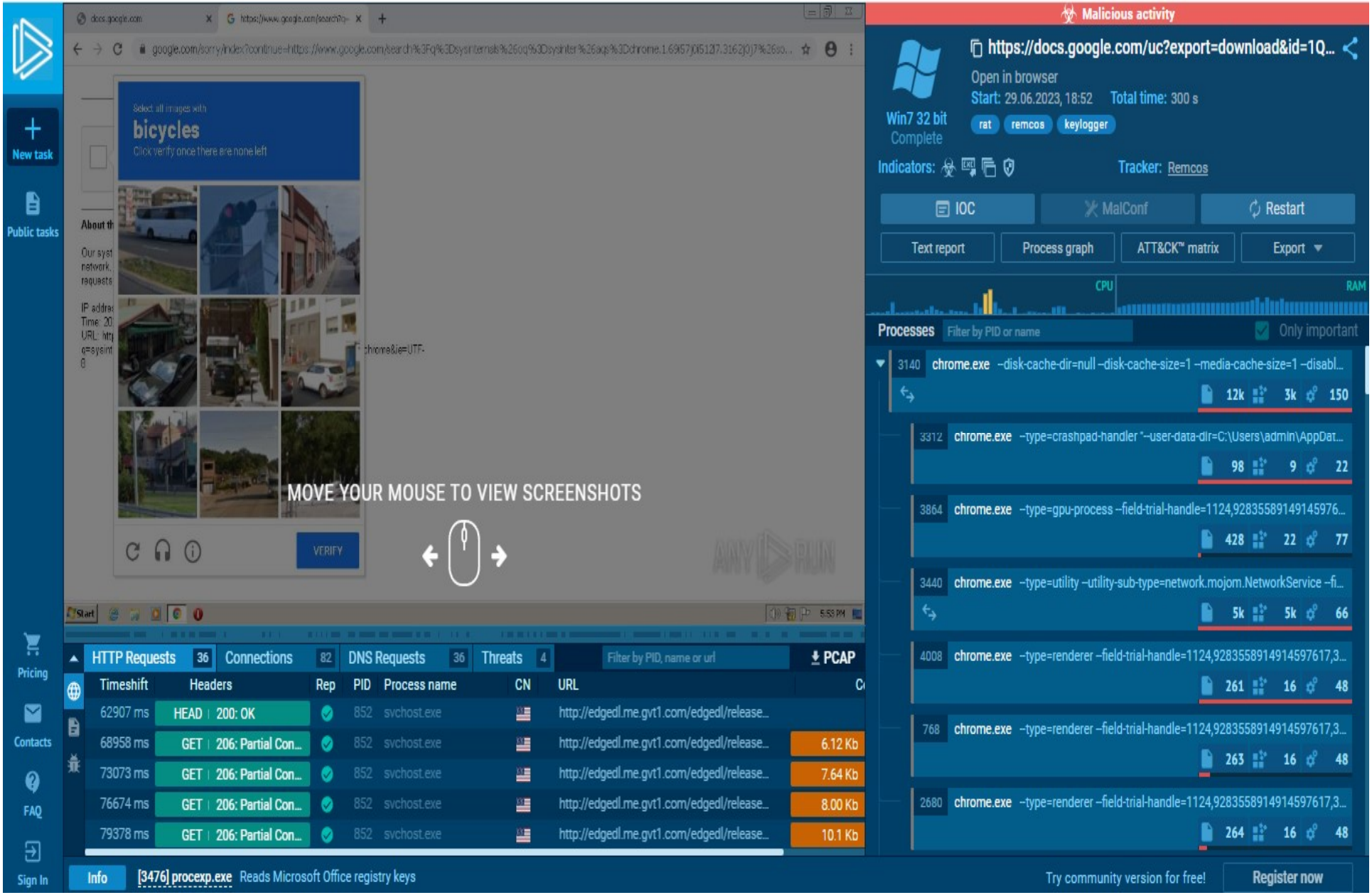
Per rendere più sicura l'azienda ho inserito al fianco della WAF un IPS/IDS per avere più controllo del traffico all'interno della DMZ, infine ho aggiunto un Firewall perimetrale per rendere più sicura la rete interna.



2. ANALISI ATTACCO: questo punto chiedeva di analizzare due link che segnavano un eventuale attacco.

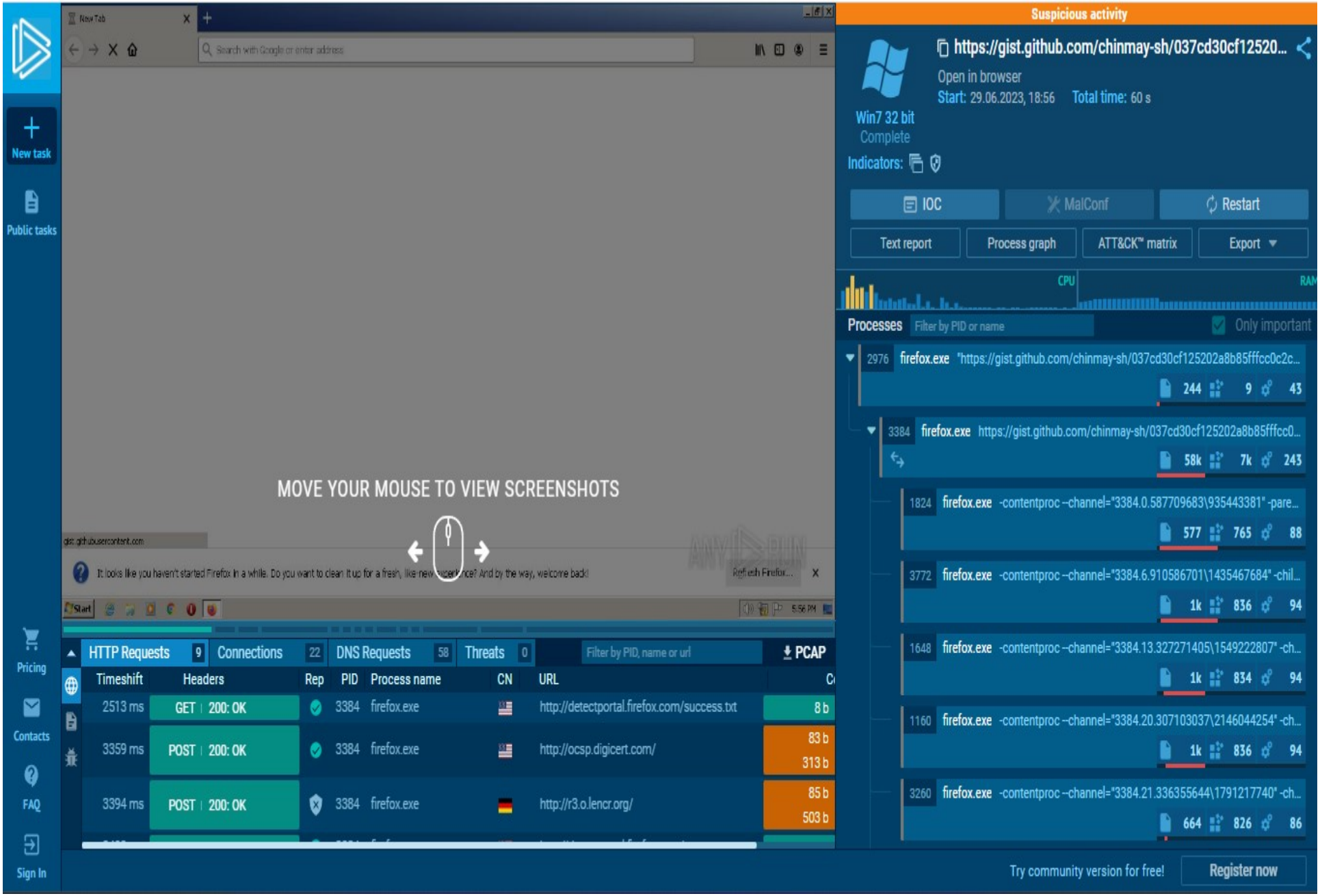
Analizzando questo link: https://tinyurl.comm/linklosco2 ho visto che è un malware di tipo RAT (Remote Access Trojan) che gli aggressori utilizzano per eseguire azioni su macchine infette da remoto. Questo malware è aggiornato in modo estremamente attivo con aggiornamenti in uscita quasi ogni mese.

Cercando su internet ho visto come viene utilizzato questo RAT: consente agli hacker di monitorare e controllare il computer o la rete. Il malware crea una backdoor virtuale sul PC della vittima che fornisce agli hacker l'accesso remoto al sistema.


New task
Public tasks
Pricing
Contacts
FAQ
Sign In
Select all images with
bicycles
Click verify once there are none left
VERIFY
MOVE YOUR MOUSE TO VIEW SCREENSHOTS
HTTP Requests 36
Connections 82
DNS Requests 36
Threats 4
Filter by PID, name or url
PCAP
Timeshift Headers Rep PID Process name CN URL
62907 ms HEAD | 200: OK 852 svchost.exe http://edgedl.me.gvt1.com/edgedl/release...
68958 ms GET | 206: Partial Con... 852 svchost.exe http://edgedl.me.gvt1.com/edgedl/release... 6.12 Kb
73073 ms GET | 206: Partial Con... 852 svchost.exe http://edgedl.me.gvt1.com/edgedl/release... 7.64 Kb
76674 ms GET | 206: Partial Con... 852 svchost.exe http://edgedl.me.gvt1.com/edgedl/release... 8.00 Kb
79378 ms GET | 206: Partial Con... 852 svchost.exe http://edgedl.me.gvt1.com/edgedl/release... 10.1 Kb
Malicious activity
https://docs.google.com/uc?export=download&id=1Q...
Open in browser
Start: 29.06.2023, 18:52 Total time: 300 s
Win7 32 bit
Complete
rat remcos keylogger
Indicators:
Tracker: Remcos
IOC
MalConf
Restart
Text report
Process graph
ATT&CK™ matrix
Export
CPU
RAM
Processes
Filter by PID or name
Only important
3140 chrome.exe --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disabl... 12k 3k 150
3372 chrome.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppDat... 98 9 22
3864 chrome.exe --type=gpu-process --field-trial-handle=1124,9283558914914597 6... 428 22 77
3440 chrome.exe --type=utility --utility-sub-type=network.mojom.NetworkService --fi... 5k 5k 66
4008 chrome.exe --type=renderer --field-trial-handle=1124,9283558914914597617,3... 261 16 48
768 chrome.exe --type=renderer --field-trial-handle=1124,9283558914914597617,3... 263 16 48
2680 chrome.exe --type=renderer --field-trial-handle=1124,9283558914914597617,3... 264 16 48
Info
[3476] procexp.exe Reads Microsoft Office registry keys
Try community version for free!
Register now

Invece analizzando quest’altro link:

https://tinyurl.com/linklosco1 ho visto che è uno script per PowerShell: è sospetto perché Il processo ignora il caricamento delle impostazioni del profilo di PowerShell, praticamente viene eseguito senza richiedere autorizzazioni amministrative.


New task
Public tasks
Pricing
Contacts
FAQ
Sign In
MOVE YOUR MOUSE TO VIEW SCREENSHOTS
HTTP Requests 9
Connections 22
DNS Requests 58
Threats 0
PCAP
Timeshift
Headers
Rep
PID
Process name
CN
URL
2513 ms GET | 200: OK 3384 firefox.exe http://detectportal.firefox.com/success.txt 8 b
3359 ms POST | 200: OK 3384 firefox.exe http://ocsp.digicert.com/ 83 b 313 b
3394 ms POST | 200: OK 3384 firefox.exe http://r3.o.lencr.org/ 85 b 503 b
Suspicious activity
https://gist.github.com/chinmay-sh/037cd30cf12520...
Open in browser
Start: 29.06.2023, 18:56 Total time: 60 s
Win7 32 bit
Complete
Indicators:
IOC
MalConf
Restart
Text report
Process graph
ATT&CK™ matrix
Export
CPU
RAM
Processes
Filter by PID or name
Only important
2976 firefox.exe "https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2c... 244 9 43
3384 firefox.exe https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0... 58k 7k 243
1824 firefox.exe -contentproc --channel="3384.0.587709683\935443381" -pare... 577 765 88
3772 firefox.exe -contentproc --channel="3384.6.910586701\1435467684" -chil... 1k 836 94
1648 firefox.exe -contentproc --channel="3384.13.327271405\1549222807" -ch... 1k 834 94
1160 firefox.exe -contentproc --channel="3384.20.307103037\2146044254" -ch... 1k 836 94
3260 firefox.exe -contentproc --channel="3384.21.336355644\1791217740" -ch... 664 826 86
Try community version for free!
Register now