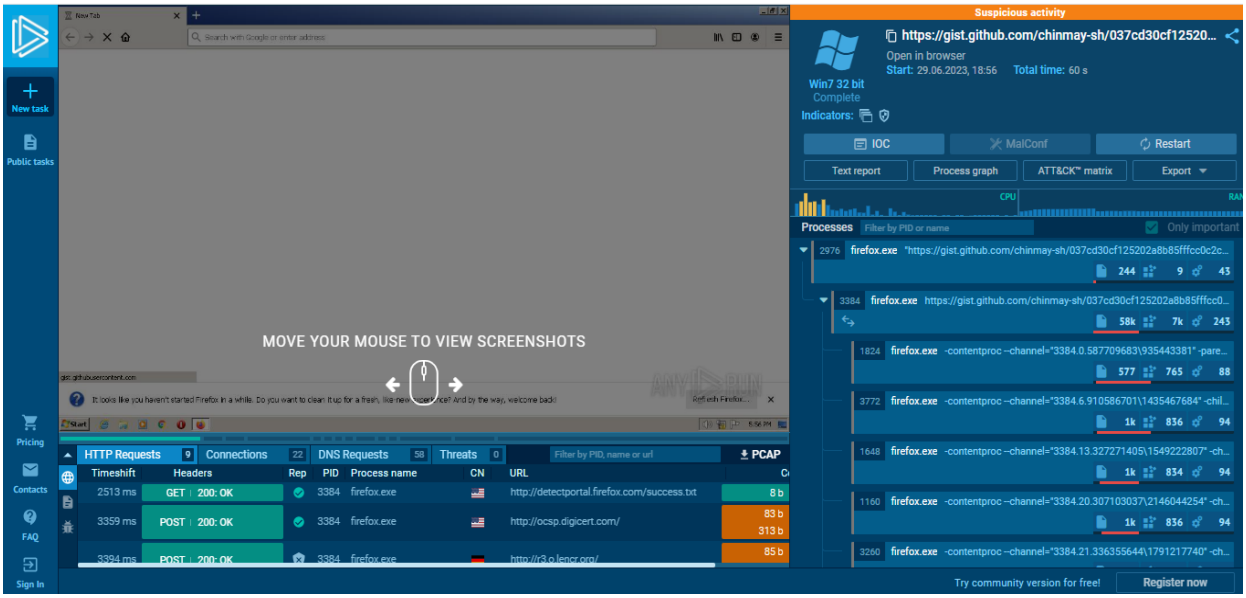
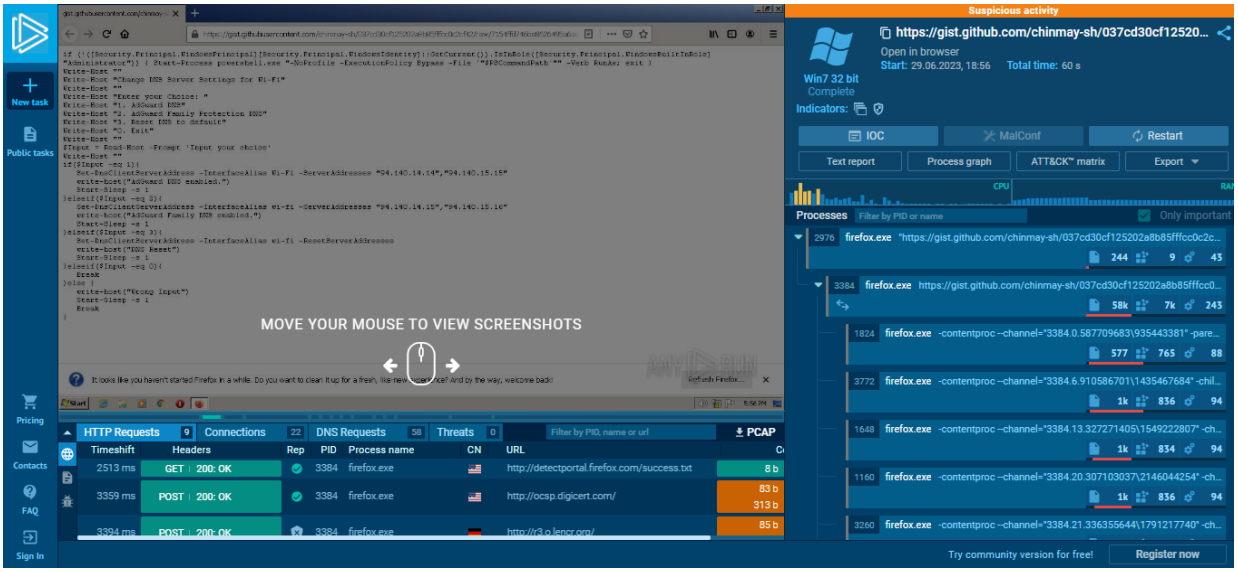
M5 D7

ESERCIZIO 2

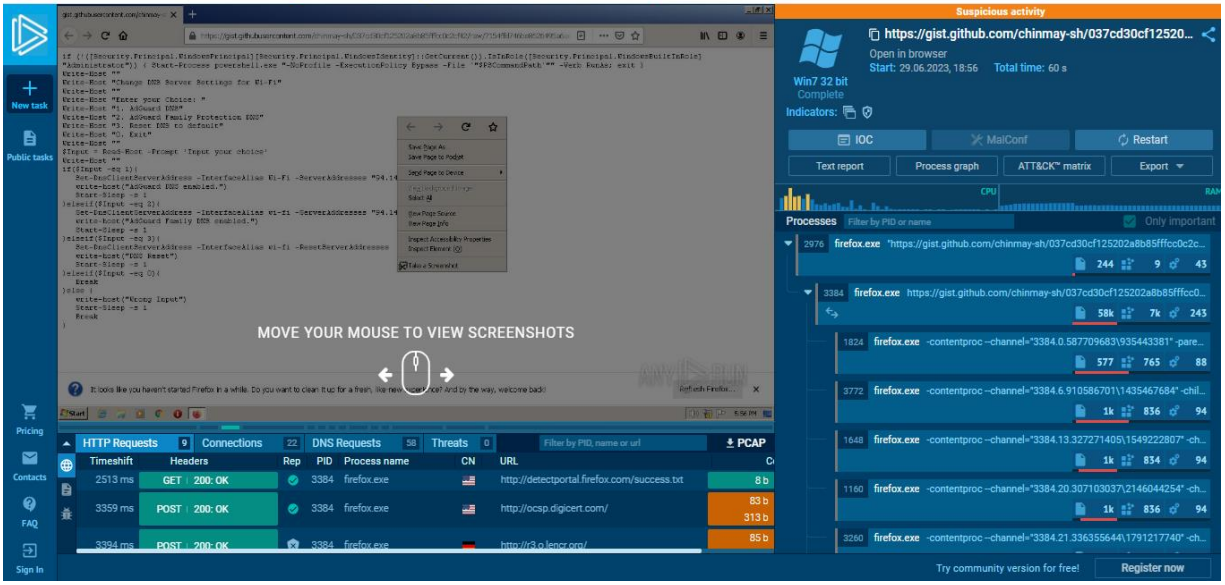
Analisi dei vari link:

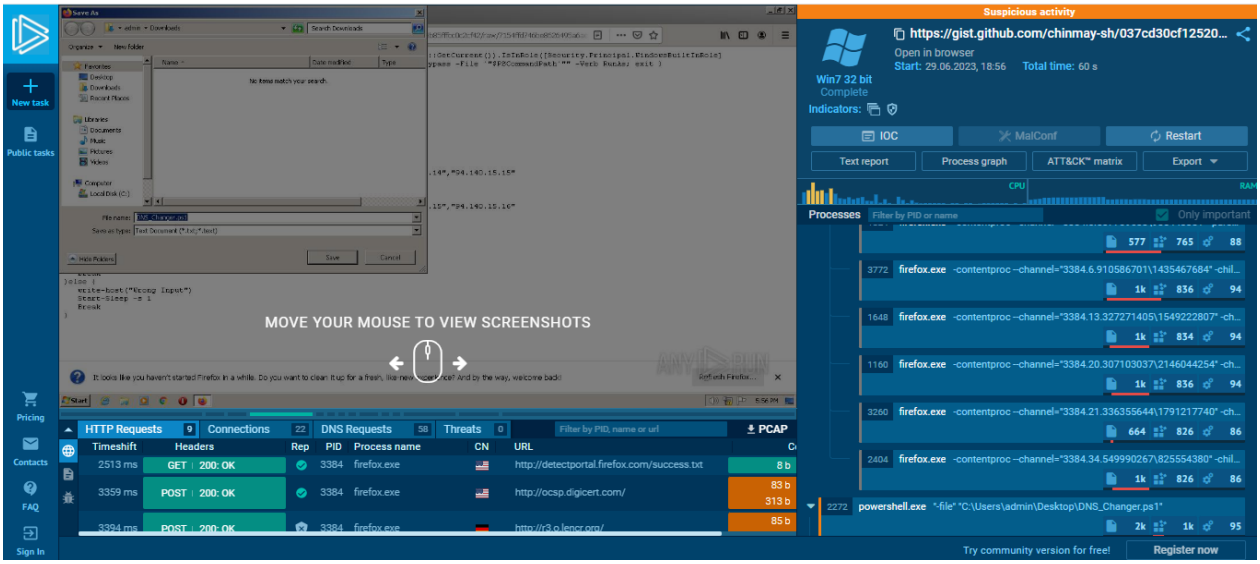
Sia nel primo che secondo link l'analisi è avvenuta con Anyrun.

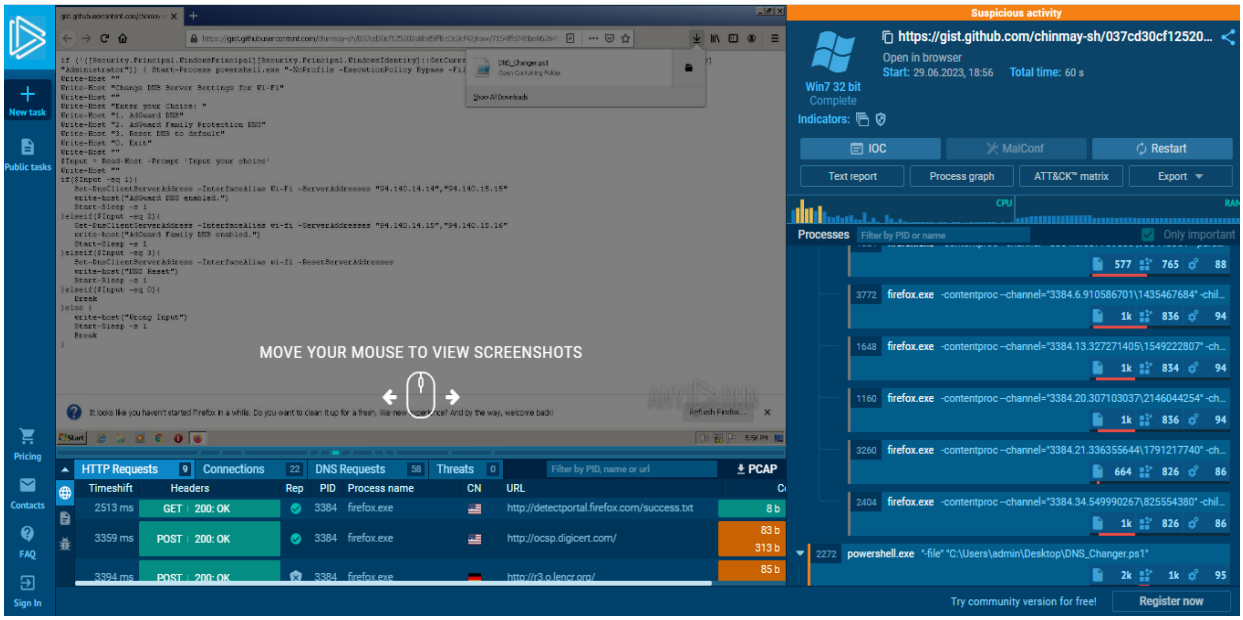




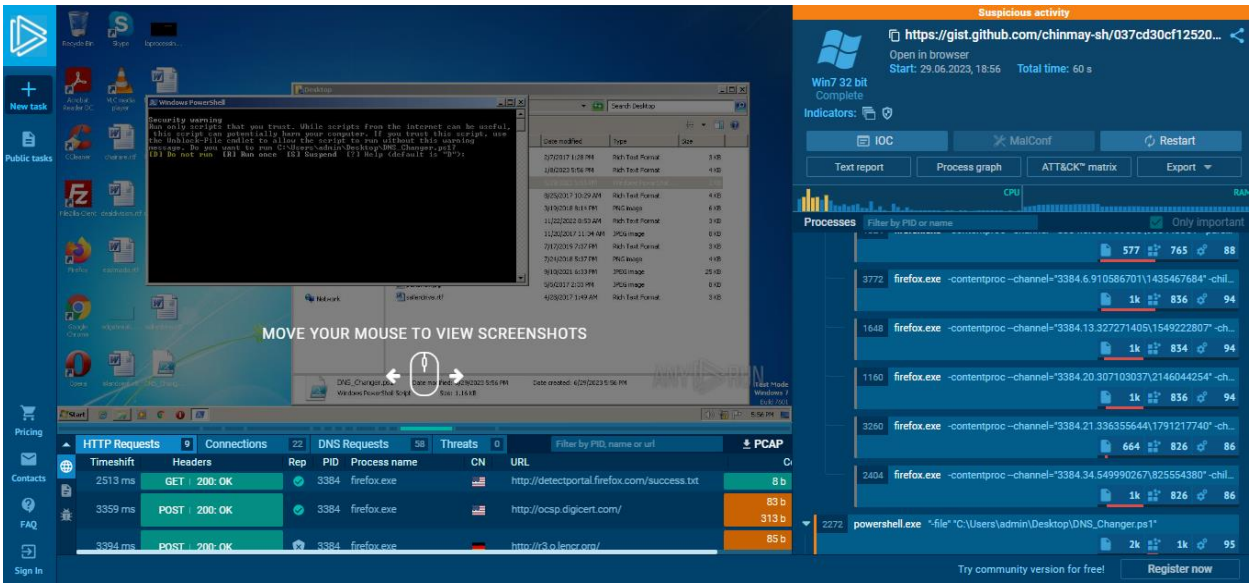
Nel primo caso si tratta di attività sospetta (arancione) mentre il secondo link parla di un rischio più alto con malware (rosso).

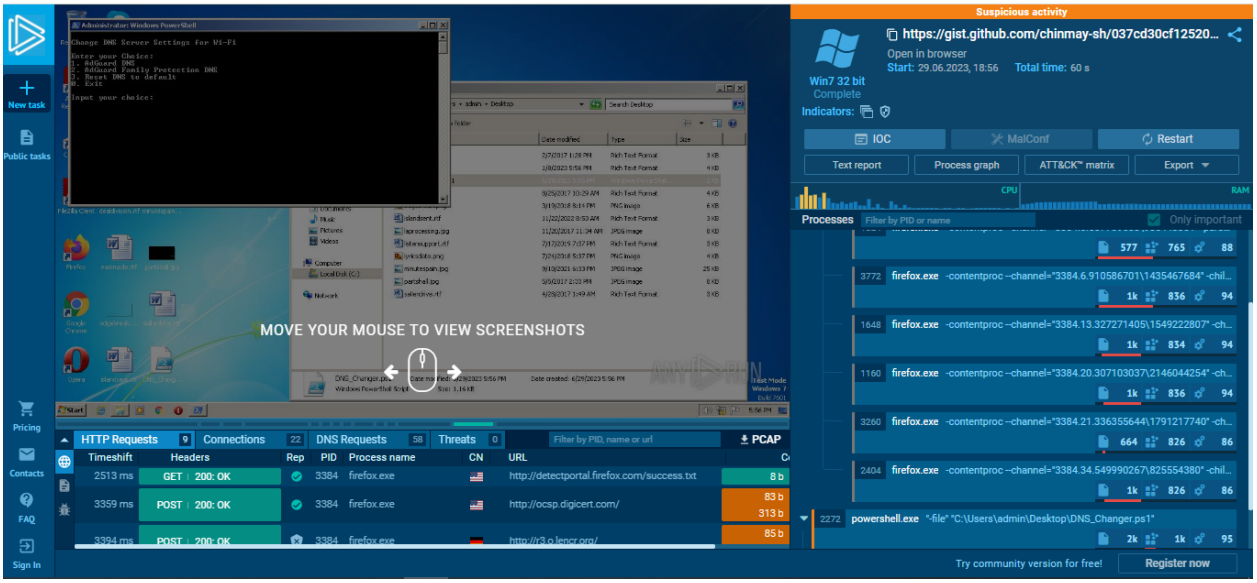

Suspicious activity
https://gist.github.com/chinmay-sh/037cd30cf12520...
Open in browser
Start: 29.06.2023, 18:56 Total time: 60 s
Win7 32 bit
Complete
Indicators:
IOC
MalConf
Restart
Text report
Process graph
ATT&CK™ matrix
Export
Processes
Filter by PID or name
Only important
MOVE YOUR MOUSE TO VIEW 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
85 b
Try community version for free!
Register now

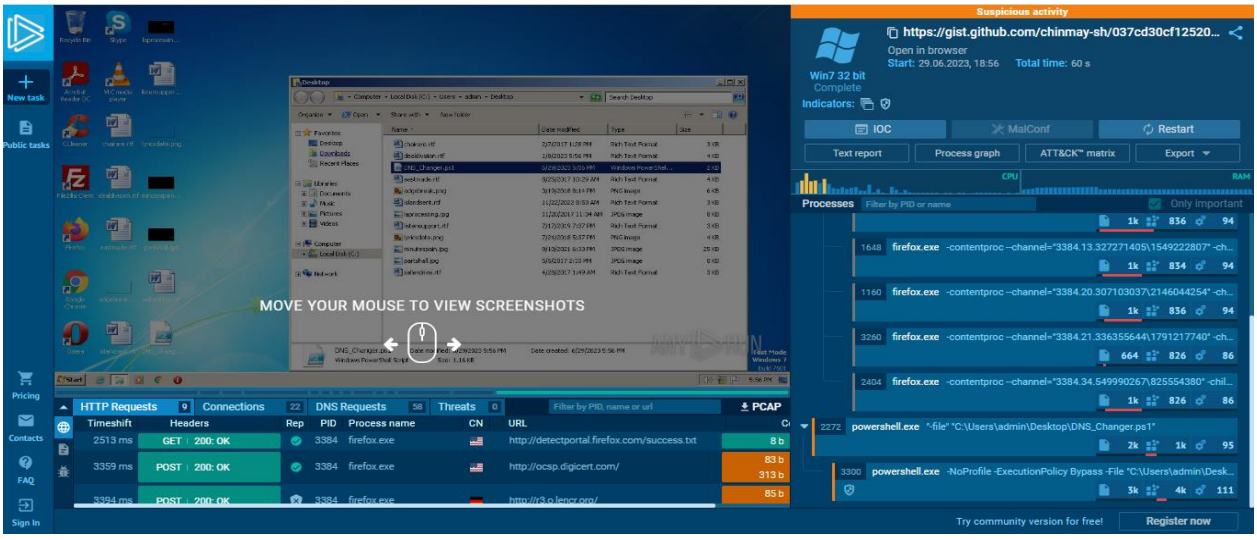

Suspicious activity
https://gist.github.com/chinmay-sh/037cd30cf12520...
Open in browser
Start: 29.06.2023, 18:56 Total time: 60 s
Win7 32 bit
Complete
Indicators:
IOC
MalConf
Restart
Text report
Process graph
ATT&CK™ matrix
Export
Processes
Filter by PID or name
Only important
MOVE YOUR MOUSE TO VIEW 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
85 b
Try community version for free!
Register now


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
Processes
Filter by PID or name
Only important
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
85 b
Try community version for free!
Register now

In dettaglio ci sono i vari processi in ordine cronologico, si tratta di uno script con powershell (primo caso), non si tratta di un vero e proprio malware.







Se si fosse attivato in automatico il malware si poteva trattare di un DNS Poisoning.