

M5 D7

ESERCIZIO 2

Analisi dei vari link:

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

The screenshot displays the Anyrun web interface. On the left, a sidebar contains navigation links: New task, Public tasks, Pricing, Contacts, FAQ, and Sign in. The main window is divided into two panes. The top pane shows a message: "MOVE YOUR MOUSE TO VIEW SCREENSHOTS" with a mouse cursor icon. Below this, a table lists HTTP requests. The bottom pane shows a list of processes, with the first one highlighted: "firefox.exe" with PID 2976. The right pane shows a "Suspicious activity" panel with a list of processes and their associated URLs. The first process is "firefox.exe" with PID 2976, and the URL is "https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc02c...".

HTTP Requests	Connections	DNS Requests	Threats
2513 ms GET 200 OK	3384	firefox.exe	http://detectportal.firefox.com/success.txt
3359 ms POST 200 OK	3384	firefox.exe	http://ocsp.digicert.com/
3394 ms POST 200 OK	3384	firefox.exe	http://i3.o.limg.net/

Processes	Filter by PID or name	Only important
2976	firefox.exe	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc02c...
3384	firefox.exe	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc02c...
1824	firefox.exe	-contentproc--channel="3384.0.587709683\935443381"-pare...
3772	firefox.exe	-contentproc--channel="3384.6.910586701\1435467684"-chil...
1648	firefox.exe	-contentproc--channel="3384.13.327271405\1549222807"-ch...
1160	firefox.exe	-contentproc--channel="3384.20.307103037\2146044254"-ch...
3260	firefox.exe	-contentproc--channel="3384.21.336355644\1791217740"-ch...

The screenshot displays the Anyrun web interface. On the left, a sidebar contains navigation links: New task, Public tasks, Pricing, Contacts, FAQ, and Sign in. The main window is divided into two panes. The top pane shows a message: "MOVE YOUR MOUSE TO VIEW SCREENSHOTS" with a mouse cursor icon. Below this, a table lists HTTP requests. The bottom pane shows a list of processes, with the first one highlighted: "firefox.exe" with PID 2976. The right pane shows a "Suspicious activity" panel with a list of processes and their associated URLs. The first process is "firefox.exe" with PID 2976, and the URL is "https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc02c...".

HTTP Requests	Connections	DNS Requests	Threats
2513 ms GET 200 OK	3384	firefox.exe	http://detectportal.firefox.com/success.txt
3359 ms POST 200 OK	3384	firefox.exe	http://ocsp.digicert.com/
3394 ms POST 200 OK	3384	firefox.exe	http://i3.o.limg.net/

Processes	Filter by PID or name	Only important
2976	firefox.exe	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc02c...
3384	firefox.exe	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc02c...
1824	firefox.exe	-contentproc--channel="3384.0.587709683\935443381"-pare...
3772	firefox.exe	-contentproc--channel="3384.6.910586701\1435467684"-chil...
1648	firefox.exe	-contentproc--channel="3384.13.327271405\1549222807"-ch...
1160	firefox.exe	-contentproc--channel="3384.20.307103037\2146044254"-ch...
3260	firefox.exe	-contentproc--channel="3384.21.336355644\1791217740"-ch...

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

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.

The screenshot displays a Windows 7 desktop environment. On the right side, a 'Suspicious activity' monitor is active, showing a list of processes. The processes listed include:

- firefox.exe (PID 3384) - contentproc -channel="3384.6.910586701\1435467684"-chil...
- firefox.exe (PID 1648) - contentproc -channel="3384.13.327271405\1549222807"-ch...
- firefox.exe (PID 1160) - contentproc -channel="3384.20.307103037\2146044254"-ch...
- firefox.exe (PID 3260) - contentproc -channel="3384.21.336355644\1791217740"-ch...
- firefox.exe (PID 2404) - contentproc -channel="3384.34.549990267\825554380"-chil...
- powershell.exe (PID 2272) - "file" "C:\Users\admin\Desktop\DNS_Changer.ps1"

The desktop background features a watermark that reads 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS'. The taskbar shows various icons, including the Start button, taskbar search, and several application icons.

This screenshot is similar to the one above, showing the same Windows 7 desktop environment. The 'Suspicious activity' monitor on the right displays the same list of processes, including firefox.exe and powershell.exe. The desktop background still features the 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS' watermark.

This screenshot shows the same Windows 7 desktop environment. The 'Suspicious activity' monitor on the right displays the same list of processes, including firefox.exe and powershell.exe. The desktop background still features the 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS' watermark.

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