

## Curso de triage informático

El triage informático se define como un proceso para analizar y priorizar las respuestas ante incidentes de seguridad informática, en base a la gravedad de su condición; escogiendo, separando y analizando evidencias, de una forma rápida, para identificar, contener y erradicar el daño, e iniciar la pertinente investigación y análisis forense del Sistema.

En este curso he aprendido a analizar los procesos activos en nuestro ordenador aplicando la heurística para detectar posibles casos de malware.



En izquierda se puede ver como la ejecución de Chrome tiene una descripción y una firma fiables mientras que el de la derecha no tiene ninguno de los dos. Además el proceso de la derecha se está ejecutando en TEMP lo cual no es común, todo esto nos hace sospechar que se pueda tratar de un proceso malicioso.

Processes								
Services								
Disk								
Name	PID	CPU	I/O Total r...	Private byt...	User name	Description	Verified Signer	
utorrent.exe	2676			152.3 KB	WIN-6S8...	WebHelper	BitTorrent Inc	
utorrent.exe	2812			149.2 KB	WIN-6S8...	WebHelper	BitTorrent Inc	
icq.exe	1976	0.04	489.7 KB/s	2.4 MB	WIN-6S8...	ICQ	I C Q Ltd	
setup.exe	2028			1.2 MB	WIN-6S8...	Microsoft Setup Bootstrapper	Microsoft Corporation	
WinRAR.exe	312			278.2 KB	WIN-6S8...	WinRAR archiver	win.rar GmbH	
notepad.exe	3084			12.8 KB	WIN-6S8...	Notepad	Microsoft Windows	
firefox.exe	2204	0.57	55.9 KB/s	4.4 MB	WIN-6S8...	Firefox	Mozilla Corporation	
firefox.exe	1664	2.64	29.5 KB/s	1.4 MB	WIN-6S8...	Firefox	Mozilla Corporation	
chrome.exe	2732	18.40	3.6 MB/s	960.7 KB	WIN-6S8...	Google Chrome	Google Inc	
chrome.exe	2884		218.0 KB/s	1.7 MB	WIN-6S8...	Google Chrome	Google Inc	
chrome.exe	3684		71.6 KB/s	1.5 MB	WIN-6S8...	Google Chrome	Google Inc	
wordpad.exe	2368	0.02		394.4 KB	WIN-6S8...	Windows Wordpad Applicati...	Microsoft Windows	
wordpad.exe	2296			417.3 KB	WIN-6S8...	Windows Wordpad Applicati...	Microsoft Windows	
AcroRd32.exe	2508	1.59	58.5 KB/s	372.4 KB	WIN-6S8...	Adobe Reader	Adobe Systems, Incorporated	
AcroRd32.exe	3412			384.5 KB	WIN-6S8...	Adobe Reader	Adobe Systems, Incorporated	
AcroRd32.exe	2664			3.3 MB	WIN-6S8...	Adobe Reader	Adobe Systems, Incorporated	
explorer.exe	1180	0.25	11.1 MB/s	958.6 KB	WIN-6S8...			

Viendo los procesos activos podemos ver como el proceso explorer.exe resaltado en morado a establecido una conexión y no tiene una descripción ni una firma por lo cual debemos analizar ese proceso más detenidamente.

chrome.exe(2732)	WIN-6S8C3R5L7TN	60092	github.com	80	TCP	Established
chrome.exe(2732)	WIN-6S8C3R5L7TN	58200	google.com	80	TCP	Established
explorer.exe(1180)	127.0.0.1	60092	67.57.196.2	8080	TCP	Established
explorer.exe(1180)	127.0.0.1	60092	67.57.196.2	8080	TCP	Established

Analizando más detenidamente vemos que ha establecido una conexión a una dirección ip y no a un dominio como lo han hecho los procesos de Chrome. Esto nos indica que se trata de un proceso malicioso.

Además, en este curso se enseña como de detectar posibles emails falsos viendo si el dominio de la dirección de email no coincide con el de la empresa, si hay faltas de ortografía o de

concordancia, si el correo solicita información personal, si el asunto del correo es de máxima alerta. También suelen contener archivos adjuntos. Viendo todo esto podremos hacernos una idea de si un correo puede ser malicioso.