Registri ed Eventi di windows

Guida approfondita sui registri, gli eventi e il loro utilizzo nei controlli

Abbiamo visto come analizzare i processi, il disco fisso, il prefetch e tanto altro nel dettaglio, ma ancora una o meglio due cose fondamentali mancano all'appello. I registri e gli eventi di windows. Sono entrambi degli artefatti che sono implementati dentro windows, e in questo capitolo vedremo cosa sono, come utilizzarli e alcune peculiarità.

Registri

I registri di windows sono stati introdotti nella versione 3.1, ed è essenzialmente un database interno al sistema e condiviso. Gli sviluppatori possono sfruttare questa risorsa per immagazzinare valori, sotto forma di "CHIAVI". Questa funzione viene usata sia da applicazioni di terze parti, sia applicazioni, programmi e servizi di windows. Questo significa e appunto ci indica che delle informazioni importanti di vari servizi, sono immagazzinate nei registri e noi nel capitolo "Metodi bypass e come trovarli" avremmo tutte le reference alle varie chiavi di registro specifiche per alcune informazioni. I registri possono essere visualizzati dalla applicazione di prima parte di windows. Per farlo semplicemente richiamare "regedit" dal pannello run (tasto win + R). Altre opzioni possono essere Registry Explorer di Eric Zimmerman, RegScanner, Advanced Regedit e così via. Un artefatto molto semplice nel suo cuore ma forse la parte veramente complicata che viene tralasciata dai vari staffer è quella di sapere le singole chiavi di registro a cosa fanno riferimento, oltre a da dove provengono e cosa significano per noi che dobbiamo ultimamente provare se un player sta usando i cheats o meno. Senza ombra di dubbio un argomento interessante.

Eventi

Gli eventi di windows sono sempre parte del sistema operativo, e come tante altre cose, ultimamente gli eventi sono stati pensati per registrare vari tipi di attività. Vari davvero, perché di eventi ce ne sono di tutti i tipi, ma piuttosto di vedere gli eventi nel singolo, cosa che accadrà nella parte più orientata alla pratica, in questo capitolo ci limitiamo a fondare delle buone idee su come questi eventi funzionano e vengono usati. Gli eventi vengono tutti salvati in file peculiari, con estensione .evtx. Questi file, sono dei database specifici per essere letti in un particolare modo, e per immagazzinare quindi i log dei vari eventi. Gli eventi più superficiali li possiamo visualizzare sul visualizzatore di eventi di windows, che viene evocato con la keyword "eventvwr" nel menù di run (tasto win + R). Questa applicazione ci permette di esplorare tutti gli eventi salvati nella cartella "%SystemRoot%\System32\Winevt\Logs*". I file .evtx è un formato si usato da servizi di windows, ma può essere utilizzato anche da applicazioni di terze parti, per tenere traccia di eventi importanti per il loro utilizzo. Noi usiamo questo artefatto per provare la occorenza di un qualche metodo bypass specifico o l'esecuzione di file etc. Tutti argomenti che riguardano comunque la sezione pratica ma come per i registri sopra spiegati, è un artefatto molto semplice e generico, che però nello specifico a tanto potenziale, ma viene spesso tralasciata tutta la teoria, quindi le persone usano a caso il visualizzatore eventi senza neanche sapere probabilmente cosa stanno cercando o cosa hanno trovato, quello che significa per loro e per il player stesso.

Conclusioni

Alla fine questi due argomenti hanno in comune una cosa, ovvero il fatto che sono degli artefatti che di un utilizzo generale ce ne si fa ben poco. Sono principalmente usati per cercare evidenze

specifiche a determinate conclusioni e quindi non molto importanti a livello di teoria, il che le lascia inesplorate da questo punto di vista. Questo capitolo ci è servito invece ad esplorare la teoria dietro questi artefatti e vi invita a seguire il prossimo capitolo, che entra nello specifico e analizza ogni singolo metodo bypass e/o detect mai trovata. Come sempre questa guida mira ad essere perfetta, ma come tutte le cose ultimamente non lo sarà mai e nemmeno voi, quindi informatevi, esercitatevi ed ultimamente miglioratevi. Grazie della lettura.