Contribution ID: **325** Type: **Presentazione orale**

Analisi di un attacco Malware su WordPress

Wednesday, 28 May 2025 12:30 (25 minutes)

Il presente lavoro analizza un attacco malware riuscito ai danni di un sito WordPress, con un focus specifico sul reverse engineering di plugin malevoli scritti in PHP. Il codice dannoso sfrutta PHP e JavaScript esterno per eseguire azioni illecite e implementa tecniche di offuscamento, tra cui encoding ASCII/Hex e manipolazione dinamica delle variabili.
Uno degli aspetti chiave del codice offuscato riguarda la sostituzione ricorsiva delle variabili e l'uso dell'istruzione <goto>, impiegate per confondere il flusso di esecuzione ed eludere i meccanismi di analisi statica. Attraverso un approccio combinato di analisi statica, è stato possibile deoffuscare il codice, ripristinare la logica esecutiva originale e individuare i meccanismi di comunicazione con server remoti. L'analisi è stata condotta in un ambiente isolato e controllato, garantendo la sicurezza dell'infrastruttura di test.
I risultati dello studio hanno permesso di valutare la reale pericolosità del malware, evidenziando le sue capacità di evasione, persistenza, tecniche e portata dell'attacco.

Primary authors: AMORI, Francesco (Istituto Nazionale di Fisica Nucleare); ZOTTI, Stefano Enrico (Istituto Nazionale di Fisica Nucleare); CIASCHINI, Vincenzo (Istituto Nazionale di Fisica Nucleare)

Presenter: AMORI, Francesco (Istituto Nazionale di Fisica Nucleare)

Session Classification: Security e compliance

Track Classification: Servizi ICT