# Scoperto un malware “invisibile” che colpisce Apache

Ott 18, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

---

**È stato battezzato p0sT5n1F3r= e consente di rubare tutti i dati che vengono inseriti dai visitatori senza lasciare alcuna traccia.**

Un modulo persistente nascosto nella piattaforma Apache e in grado di memorizzare ed esfiltrare le informazioni sensibili inviate dai visitatori in un sito Web. È questa la sintesi del report con cui **Yarix** ha rivelato al mondo l’esistenza di **p0sT5n1F3r=**.

Il malware, che la società di sicurezza definisce un **APT** ma che sembra agire più che altro come uno **skimmer**, ha caratteristiche estremamente particolari che lo rendono difficilissimo da individuare.

Come spiegano i ricercatori, p0sT5n1F3r= è inserito in un modulo per **Apache** e agisce a livello server per sniffare le informazioni una volta che queste sono state decodificate dal Web Server. Le informazioni vengono memorizzate e poi trasmesse in modo da non destare sospetti negli amministratori.

La trasmissione, infatti, non avviene in maniera autonoma, ma in seguito a un collegamento avviato dall’esterno dai pirati informatici che, agli occhi di qualsiasi strumento di controllo, sembra del tutto legittimo.

Allo stesso modo, l’attività di sniffing non lascia alcuna traccia nei log di sistema e lo stesso codice del malware, che i ricercatori hanno sottoposto a scansione su **VirusTotal**, sfugge ai motori antivirus in commercio.




Insomma: p0sT5n1F3r= è in pratica uno sniffer quasi invisibile, che dale parti di Yarix hanno individuate dopo una complessa analisi che ha richiesto il superamento di **numerosi livelli di offuscamento** utilizzati dai pirati per nascondere la presenza del modulo.

Nel caso specifico, il malware è stato utilizzato per rubare informazioni sulle credenziali di pagamento inserite dai visitatori, ma la stessa tecnica potrebbe essere utilizzata per intercettare anche altri tipi di informazioni.

“È un testa a testa senza esclusione di colpi, quello tra hacker ed esperti di cyber security: ad ogni passo avanti nello sviluppo dei sistemi di protezione si contrappone una minaccia nuova. In questa logica si inserisce l’individuazione di un APT mai rilevato in precedenza a livello internazionale” commenta **Mirko Gatto**, CEO di **Yarix**.

“Averne identificato la comparsa ci dice molto sulla capacità offensiva ed organizzativa del cyber crime, ma al tempo stesso ci conforta rispetto alla possibilità di aver spuntato alcune delle armi degli hacker, per quanto riguarda questo inedito e pericoloso strumento di attacco”.

Condividi l’articolo

Il worm Graboid fa strage di Docker vulnerabili

## Articoli correlati

## Altro in questa categoria

https://www.securityinfo.it/2019/10/18/scoperto-un-malware-invisibile-che-colpisce-apache/