Var Group ha scoperto un APT mai rilevato in precedenza

Di **Redazione LineaEDP** - 18/10/2019

Il nuovo strumento di attacco hacker scoperto da Var Group rappresenta una minaccia evoluta per tutte le aziende che gestiscono pagamenti o dati personali

Var Group, player attivo nei servizi e nelle soluzioni ICT per le imprese e parte del gruppo SeSa S.p.A., ha scoperto un nuovo APT che non era mai stato rilevato a livello globale.

La scoperta è stata possibile grazie alle attività di incident response, assessment e digital forensics condotte da Yarix, la Divisione Digital Security di Var Group, in questi giorni per ricostruire la dinamica di un incidente di cyber security all'interno del sistema digitale di un operatore di primo piano nel comparto dei trasporti.

Un incidente a cui l'azienda ha reagito prontamente ma che purtroppo, data la sua complessità, è risultato non individuabile proprio a causa delle sofisticate tecniche utilizzate, in grado di eludere tutti i sistemi di sicurezza in dotazione all'Azienda.

L'analisi tecnica di Yarix è stata suddivisa in più parti, la prima già consultabile a questo link; le successive, contenenti ulteriori dettagli sul funzionamento interno, sono ancora in corso e verranno pubblicate nei prossimi giorni.

È già tuttavia possibile affermare che ci troviamo di fronte a una serie di evidenze molto interessanti:

L'incidente non era rilevabile dai log: l'APT individuato è progettato per nascondere le tracce del proprio funzionamento.

L'APT è in grado di captare – in gergo sniffare – le informazioni sensibili di utenti di piattaforme online di pagamento, inserendosi all'interno del processo quando i dati, trasmessi in modo cifrato, vengono lecitamente decifrati dal web-server.

Alterando un modulo di Apache – web-server open largamente utilizzato – l'APT intercetta ed archivia in memoria dati sensibili, a cui l'hacker può in seguito accedere collegandosi direttamente dall'esterno simulando traffico del tutto lecito; non essendoci alcun invio autonomo di dati verso l'esterno del sistema, né tantomeno nessuna registrazione delle attività, la violazione risulta molto difficile da rilevare.

È la prima volta in cui abbiamo evidenza che la compromissione di moduli di Apache venga utilizzata in questo modo; in precedenza questa tecnica è stata utilizzata per impiantare backdoor (ad esempio il malware Linux/Cdorked.A) al fine di ridirezionare il traffico verso siti compromessi.

Dalle banche alle aziende di e-commerce alle aziende sanitarie

Sono trasversali i potenziali bersagli esposti a questa nuova minaccia che impatta un'ampia fetta del sistema economico e produttivo. Tutte le organizzazioni dotate di tali piattaforme sono potenzialmente vulnerabili a questo tipo di minaccia appena scoperta nel nostro Paese da Yarix.

Nello specifico, tutti i dati in transito da e verso un web-server in cui sia stato impiantato un modulo compromesso possono essere intercettati ed archiviati in memoria senza lasciare tracce in caso di indagine forense post-mortem e resi disponibili all'attaccante: dati personali, dati bancari e informazioni sensibili risultano infatti intercettati post decodifica operata legittimamente dal web-server.

Per l'individuazione di questa minaccia, Yarix ha messo in campo risorse appartenenti a team differenti, che hanno permesso di definire una strategia di indagine basata su:

- attività di incident response, che ha comportato attività di analisi dinamica del comportamento del sistema, consentendo di individuare le richieste illecite operate dall'attaccante; richieste che non venivano in alcun modo registrate dai sistemi di logging. Sulla base di queste evidenze, ricostruendo il flusso dei dati in transito nel sistema, è stato poi possibile riconoscere la compromissione di un modulo di Apache e, di conseguenza, la dinamica di funzionamento del malware;
- attività di assessment, che hanno consentito di identificare la possibile kill-chain seguita dall'attaccante;
- attività di malware analysis, che, grazie a tecniche di analisi statica e dinamica, hanno permesso di "sezionare" il modulo compromesso, identificarne gli algoritmi di cifratura utilizzati e comprendere quindi nel dettaglio ogni sua caratteristica e funzionalità.

Un insieme quindi sinergico di attività, svolte da personale con elevate competenze, al fine di ricostruire lo scenario operato dall'attaccante e poterne interrompere l'operatività.

TAGS Apt VAR Group Yarix

VAR GROUP HA SCOPERTO UN APT MAI RILEVATO IN PRECEDENZA

Redazione LineaEDP

LineaEDP è parte di BitMAT Edizioni, una casa editrice che ha sede a Milano con copertura a 360° per quanto riguarda la comunicazione rivolta agli specialisti dell'Information & Communication Technology.