I pirati adesso vanno a caccia dei file ENV

Nov 23, 2020 Marco Schiaffino Attacchi, In evidenza, Intrusione, News, RSS, Scenario 0

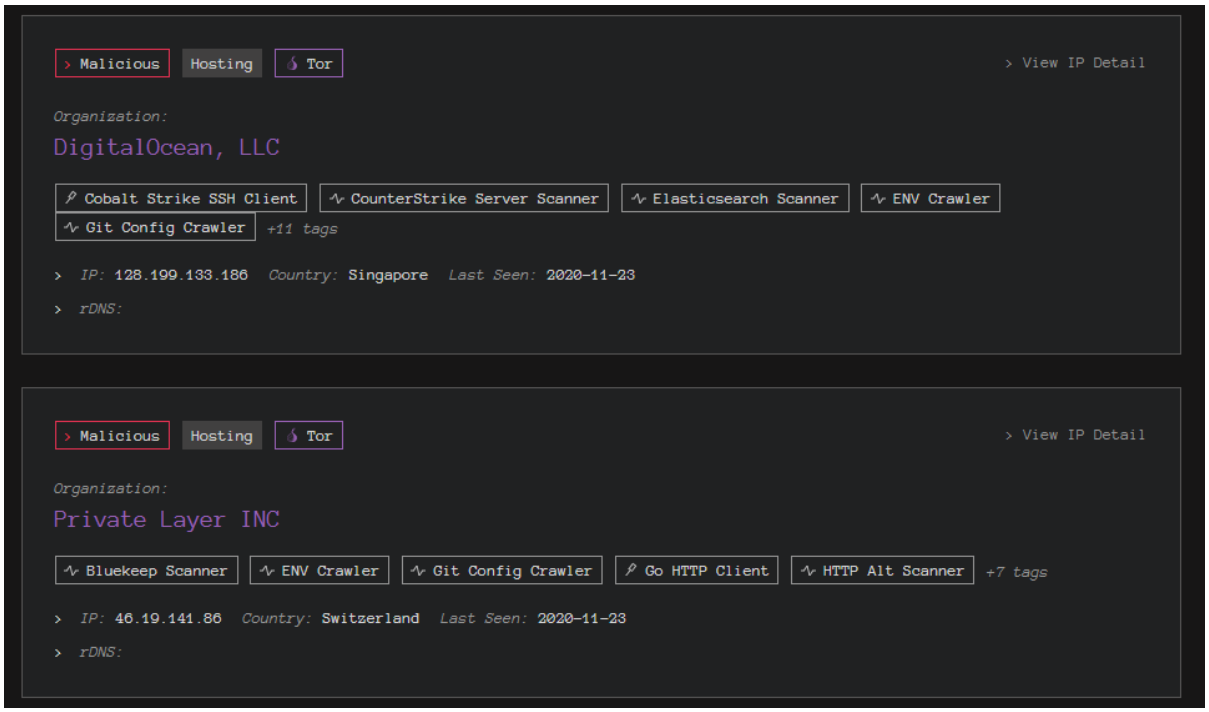
Gli esperti hanno individuato botnet dedicate che eseguono una scansione continua per rilevare i file. Obiettivo: rubare le impostazioni dei server.

Si apre un nuovo fronte nella partita sulla cyber security, che questa volta coinvolge piattaforme come **Docker**, **Node.js**, **Symfony**, e **Django**. I cyber criminali, infatti, sembrano averle prese di mira attraverso un'attività continua di scansione online.

A lanciare l'allarme sono numerose società di sicurezza, tra cui **Bad Packets** e **Greynoise**. Entrambe, infatti, hanno individuato attività di scansione che punta specificatamente a individuare la presenza di **file ENV** accessibili online.

Si tratta di particolari file che vengono utilizzati dagli sviluppatori per memorizzare informazioni "sensibili" come **token di accesso alle API, credenziali dei database e simili**. File che, normalmente, dovrebbero essere conservati in cartelle protette ma che spesso (troppo spesso) rimangono esposti. Questo tipo di attività, in realtà, va avanti da tempo.

Negli ultimi mesi, però, ha subito un'accelerazione. Negli ultimi tre anni sarebbero stati individuati più di 2.800 indirizzi IP unici utilizzati per questo tipo di scansione.



Secondo gli esperti, l'obiettivo dei pirati informatici è quello di individuare i file ENV accessibili, scaricarli ed estrarre le informazioni che contengono per utilizzarle poi in vari tipi di attacchi.

L'accesso ai servizi cloud tramite API, per esempio, permetterebbe loro di abusare del software in questione, ma anche le altre informazioni (in molti casi credenziali di accesso) consentirebbero loro di **infiltrare le reti aziendali con estrema facilità**.

L'appello, rivolto agli sviluppatori e agli amministratori IT, è naturalmente quello di avviare procedure e policy per la verifica del livello di sicurezza nella gestione di questi file, che ormai rappresentano un obiettivo privilegiato per i cyber criminali.

Condividi l'articolo

Falla in Facebook Messenger consentiva di spiare a distanza un utente

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/23/i-pirati-adesso-vanno-a-caccia-dei-file-env/?utm_source=rss&utm_medium=rss&utm_campaign=i-pirati-adesso-vanno-a-caccia-dei-file-env