Database ElasticSearch (ancora) nel mirino dei pirati

Giu 15, 2020 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Malware, News, RSS, Scenario 0

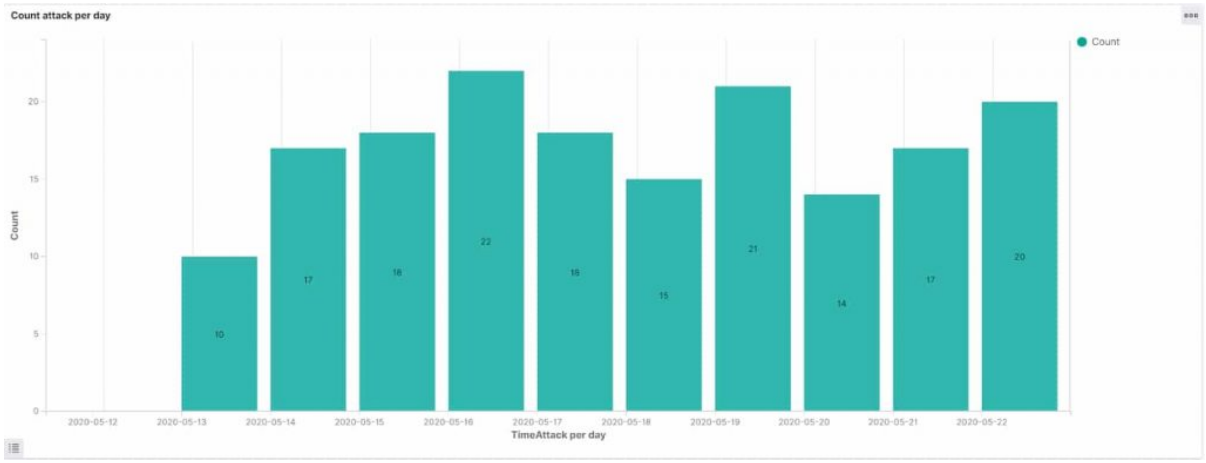
I cyber criminali utilizzano strumenti di scansione che permettono di rilevare in tempi record i server esposti e colpiscono immediatamente.

Non si arrestano gli attacchi ai server **ElasticSearch** esposti su Internet a causa di configurazioni errate. Anzi: secondo quanto riportano i ricercatori di **Comparitech**, che hanno provato a fare un piccolo esperimento per testare la capacità di reazione dei pirati informatici.

La società di sicurezza ha messo online un honeypot, cioè un server ElasticSearch utilizzato come "esca" per registrare gli attacchi portati dai cyber-criminali. Il risultato dell'esperimento è sconcertante: il server in questione ha infatti subito **una media di 18 attacchi al giorno**.

L'elemento ancora più curioso riguarda il fatto che i pirati informatici sono istati in grado di individuare il server molto più rapidamente di qualsiasi motore di ricerca.

Gli analisti di Comparitech lo hanno messo online l'11 maggio. Mentre **Shodan** ha impiegato cinque giorni per individuarlo, **il primo attacco dei pirati è arrivato dopo solo 8 ore e 35 minuti**.



La maggior parte degli attacchi, si spiega nel report, avevano l'obiettivo di sfruttare una falla di sicurezza risalente al 2015 per installare sui server dei miner per la generazione di cripto-valuta. Altri, invece, puntavano a sfruttare la stessa vulnerabilità (CVE-2015-1427) per rubare le credenziali di accesso.

La tipologia di attacchi, in ogni caso, è stata estremamente varia e il "colpo di grazia" è arrivato il 29 maggio, quando **un bot ha individuato il server e ha cancellato tutti i file** lasciando al loro posto un messaggio con una richiesta di riscatto.

Una strategia cui abbiamo già assistito in passato (ne abbiamo parlato in questo articolo) e che, a quanto pare, non è affatto passata di moda.

Insomma: chiunque gestisca un server ElasticSearch farà meglio a predisporre tutte le misure di sicurezza possibili e immaginabili. Dopo questo esperimento, infatti, una sola cosa è certa: sarà sottoposto a un vero e proprio bombardamento di attacchi.

Condividi l'articolo

EKANS: come funziona il ransomware che ha colpito Enel e Honda

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/06/15/database-elasticsearch-ancora-nel-mirino-dei-pirati/?utm_source=rss&utm_medium=rss&utm_campaign=database-elasticsearch-ancora-nel-mirino-dei-pirati