Written by Marco Attard
25 July 2019

Elasticsearch is yet again under cybercriminal attack, as Trend Micro describes a vicious breed of malware able to turn the enterprise search engine into a cryptocurrency mining botnet able to deliver denial of service (DDoS) attacks.


As the security vendor puts it, the treats transform targets into "botnet zombies." It targets exposed or publicly accessible out-of-date Elasticsearch databases/servers, and forces them to download a series of malicious Java commands from an expendable or easy-to-replace domain. The first script shuts down the firewall and competing cryptocurrency mining activities, before a second script prepares the host by removing configuration files and any traces of the initial infection.

Once the two scripts are in place, the attackers load the machine with the BillGates/Setag malware able to hijack systems, initiate DDoS attacks and even link with other infected machines to create botnets. Trend Micro describes such multistage execution techniques as a red flag, and it could mean the cybercriminals are simply testing tools or readying infrastructure before making actual attacks.

Elastic has already issued a patch for the vulnerability, but customers have to keep in mind the real-life repercussions of keeping an unsecure Elasticsearch server. Additional mechanisms such as data categorisation, network segmentation and intrusion prevention should also help reduce exposure to malware and breaches, not to mention security solutions able to defend against such threats.

Go [Multistage Attack Delivers BillGates/Setag Backdoor, Can Turn Elasticsearch Databases into DDoS Botnet 'Zombies'](#)