Attacks on Elasticsearch databases

Threat Memo - TM 20-038 Date: 06/04/2020 - Version: 1.0

TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Hacktivism	Wiping, disruption, vandalism	World	IT services	A1

Key Points

- The widely used Elasticsearch data aggregation and analysis service is being targeted by an automated campaign.
- The campaign identifies and wipes internet exposed databases.
- Elasticsearch services have in the past been repeatedly found accessible due to misconfigurations and bad management, exposing troves of data they were supposed to safekeep.

Summary

Since March 24, a destructive campaign has been targeting exposed Elasticsearch databases worldwide. According to news sources[1] and a security researcher, these attacks are currently automated, searching for insecure servers and deploying scripts that wipe their content.

Specifically:

- The attacks target databases that have been left accessible on the internet, without password, thus easily compromised.
- They attempt (but don't always succeed) to wipe the exposed contents.
- The attackers further plant a "false flag", the name of the cyber security company, Night Lion Security. The company has denied any connection with the destructive attacks. The presence of this false flag has however helped identify database cases where even though there had been unauthorised access, the malicious script was not successful in wiping contents.
- According to the site BinaryEdge that performs intelligence gathering over internet resources, there have been at least 15.000 cases where the Night Lion flag has been discovered out of the total of 34.500 estimated exposed Elasticsearch servers.
- In parallel, there appears to be a second threat actor who is also accessing exposed Elasticsearch databases and leaving hacking notices to victims. This wave is significantly smaller in scale with about 40 cases discovered so far.

In general, discovery of exposed Elasticsearch databases online is a common phenomenon and in numerous cases in the past, security researchers have informed owners or benevolently identified cases of exposure of personal data, sensitive business information, etc. The annex gives an overview of some recently publicised cases.

The current wiper activity is escalating the seriousness of events that in the past could be dismissed as system administrator oversight (nevertheless with potentially serious economic and privacy repercussions) to destructive incidents. Furthermore, the apparent success of the destructive script to identify and wipe the databases could incentivise cybercriminals to also run automated data stealing campaigns.

Comments

Even if not running the risk of destructive action, databases as well as other enterprise assets are in constant threat of exposing critical internal information. System administrators should follow a cautionary enterprise security policy regarding the exposure surface to the internet and additionally audit their systems for possible misconfiguration errors.

As has happened in the past (2017) this threat activity could also move in the direction of cyber-criminals taking control of data repositories and extorting payment from the victims either by threatening their destruction with commanded wipers or by encrypting them with ransomware.

CERT-EU continues to monitor developing threats to information assets and will alert its constituency on new threat vectors.

[1] https://www.zdnet.com/article/a-hacker-has-wiped-defaced-more-than-15000-elasticsearch-servers/#ftag=RSSbaffb68

Annex I – Recent data exposure incidents associated with Elasticsearch databases

Date	Country	Affected organisation	Details/ Impact
March 2020	Israel	Straffic Marketing	49 million unique email addresses stored in an Elasticsearch database, exposed.
January 2020	US	Technology company	Five unprotected Elasticsearch servers associated with a US technology company had exposed approximately 250 million customer records to the public internet from 2015 to December 2019
December 2019	US	Microsoft	250.000 customer records had been exposed online until Dec.31, 2019, due to a misconfigured Elasticsearch database. Customer data, although redacted to some extent, included email addresses, IPss, locations, support claims and cases, support agent emails, case numbers, resolutions, as well as internal notes marked as "confidential".
December 2019	Estonia	Browser vendor Blisk	3.4GB Elasticsearch server found accessible online without a password, containing 2,9 million records including personal data of thousands of web developers.
November 2019	US	Two data enrichment companies	4 billion user accounts spanning more than 4 terabytes of data. Unsecured Elasticsearch server where all the information was unprotected and accessible via a web interface.
October 2019	Russia	Unknown	Due to a publicly accessible Amazon Web Services (AWS) Elasticsearch cluster tax and personal data files of at least 20 million Russian citizen were exposed online.
October 2019	China	Sichuan Lianhao Technologies, a provider of internet of things medical solutions	ElasticSearch services build upon an unsecured database exposed 24 million patient records.
October 2019	China	The medical department of Tsinghua University	Personal data of 60.00 patients exposed. Accessibility probably as above.
September 2019	Equador	Probably government sources	More than 20,8 million citizen records (including children) containing personal data where exposed on an Elasticsearch server.
August 2019	Georgia	Credit agency Credia.ge	Misconfigured Elasticsearch database resulting in the exposure of 140.000 customer records, including personal data (names, addresses, dates of birth, passport numbers, email addresses, loan amounts, tax ID codes, IBAN bank numbers, unicard IDs, and loan status). Second exposed database was also discovered in adjacent IP, also with credit information, containing a ransom note.