Meow Attack is Wiping Internet-Exposed Databases

Executive Summary
On 20 July, 2020, the first of what would become almost 4,000 unsecured and public-facing databases were completely destroyed. No explanation or ransom note was provided in what has been dubbed the ‘meow’ attacks. A number of recommendations on mitigating Meow attacks are available in the full report. HC3 analysts assess with high confidence that this attack poses a risk to Healthcare and Public Health (HPH) sector organizations as many HPH databases are currently exposed to the Internet.

Report
On 20 July, 2020, security researcher Bob Diachenko tweeted that an Elasticsearch database was destroyed by what he termed a ‘meow’ bot attack. The database, which belonged to the company UFO VPN, was public-facing and unsecured. Diachenko noted that the “new Elasticsearch bot attack does not contain any ransom or threats, just ‘meow’ with a random set of numbers. It is quite fast and search&destroy clusters pretty effectively.” He told Bleeping Computer that “the attack appears to be an automated script that overwrites or destroys the data completely” and provided the following screenshot indicating the results of the attack. Note the index names are suffixed with ‘meow’ and the size of the indexes are all 283 bits. It is unknown as to why the attackers are deleting the exposed, unsecured databases, but security researcher Anthr@x was able to determine that the attacks are being carried out via Proton VPN IP addresses.

The attacks were initially observed targeting unsecured Elasticsearch and MongoDB databases, but additional attacks have since been noted on Redis and Apache ZooKeeper servers. Security researcher Victor Gevers also indicated that Cassandra, CouchDB, Hadoop, and Jenkins databases, along with network-attached storage (NAS) devices, had been affected. As of 25 July, 2020, Bleeping Computer reported that almost 4,000 databases in total had been deleted. The HPH sector is particularly vulnerable to this kind of attack as research conducted in September 2019 by IntSights showed that almost one-third of 50 evaluated HPH databases were exposed to the Internet.

The National Capital Region Threat Intelligence Consortium (NTIC) Cyber Center recommends database administrators audit all internet-facing database instances, ensuring that all unneeded ports are closed, especially TCP ports 22 (SSH), 23 (Telnet), 3389 (RDP), and 9200 (Elasticsearch). For databases that require remote access, NTIC recommends requiring the use of a VPN for access, enabling multifactor authentication on user accounts, and regularly monitoring access for unauthorized or suspicious activity. NTIC also highly recommends regularly backing up data and storing these backups securely off the network.
Analyst Comment
HC3 analysts assess with high confidence that this attack poses a risk to HPH sector organizations with databases accessible via the Internet. Storing data in unsecured databases not only puts the data at risk of being stolen but, in the case of the Meow attacks, could potentially lead to permanent data destruction and loss.

References
https://arstechnica.com/information-technology/2020/07/more-than-1000-databases-have-been-nuked-by-mystery-meow-attack/
https://www.searchenginejournal.com/meow-attack/375764/#close
https://twitter.com/MayhemDayOne
https://us7.campaign-archive.com/?u=deea5254cca2a43f7e9f467c2&id=421e59538f (NTIC Alert)