Health Sector Cybersecurity Coordination Center (HC3)

Analyst Note

July 28, 2020 **TLP: GREEN** **Report: 202007300900**

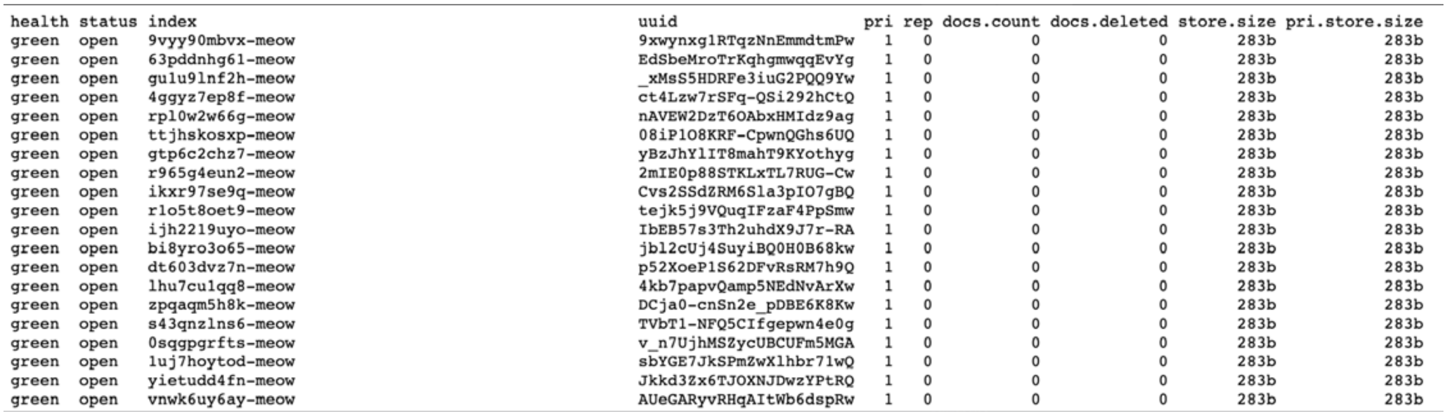
Meow Attack is Wiping Internet-Exposed Databases

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.



```
health status index                                         uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   9vyy90mbvx-meow                               9xwynxglRTqzNnEmmdtmPw   1   0          0            0       283b           283b
green  open   63pddnhg61-meow                               EdSbeMroTrKqhgmwqqEvYg   1   0          0            0       283b           283b
green  open   gulu9lnf2h-meow                               _xMsS5HDRFe3iuG2PQQ9Yw   1   0          0            0       283b           283b
green  open   4ggyz7ep8f-meow                               ct4Lzw7rSFq-QSi292hCtQ   1   0          0            0       283b           283b
green  open   rpl0w2w66g-meow                               nAVEW2DzT6OAbxHMIdz9ag   1   0          0            0       283b           283b
green  open   ttjhskosxp-meow                               08iP1O8KRF-CpwnQGhs6UQ   1   0          0            0       283b           283b
green  open   gtp6c2chz7-meow                               yBzJhYlIT8mahT9KYothyg   1   0          0            0       283b           283b
green  open   r965g4eun2-meow                               2mIE0p88STKLxTL7RUG-Cw   1   0          0            0       283b           283b
green  open   ikxr97se9q-meow                               Cvs2SSdZRM6Sla3pIO7gBQ   1   0          0            0       283b           283b
green  open   rlo5t8oet9-meow                               tejk5j9VQuqIFzaF4PpSmw   1   0          0            0       283b           283b
green  open   ijh2219uyo-meow                               IbEB57s3Th2uhdX9J7r-RA   1   0          0            0       283b           283b
green  open   bi8yro3o65-meow                               jbl2cUj4SuyiBQ0H0B68kw   1   0          0            0       283b           283b
green  open   dt603dvz7n-meow                               p52XoeP1S62DFvRsRM7h9Q   1   0          0            0       283b           283b
green  open   lhu7culqq8-meow                               4kb7papvQamp5NEdNvArXw   1   0          0            0       283b           283b
green  open   zpqaqm5h8k-meow                               DCja0-cnSn2e_pDBE6K8Kw   1   0          0            0       283b           283b
green  open   s43qnzlns6-meow                               TVbT1-NFQ5CIfgepwn4e0g   1   0          0            0       283b           283b
green  open   0sqgpgrfts-meow                               v_n7UjhMSZycUBCUFm5MGA   1   0          0            0       283b           283b
green  open   luj7hoytod-meow                               sbYGE7JkSPmZwXlhbr7lwQ   1   0          0            0       283b           283b
green  open   yietudd4fn-meow                               Jkkd3Zx6TJOXNJDwzYPtRQ   1   0          0            0       283b           283b
green  open   vnwk6uy6ay-meow                               AUeGARyvRHqAItWb6dspRw   1   0          0            0       283b           283b
```

Figure 1 Screenshot of Elasticsearch database after Meow attack

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://www.bleepingcomputer.com/news/security/new-meow-attack-has-deleted-almost-4-000-unsecured-databases/
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://www.comparitech.com/blog/vpn-privacy/ufo-vpn-data-exposure/
https://healthitsecurity.com/news/exposed-misconfigured-databases-put-patient-data-at-risk
https://us7.campaign-archive.com/?u=deea5254cca2a43f7e9f467c2&id=421e59538f (NTIC Alert)