MongoDB malicious code attacks more than 26,000 victims in a week

Malware that attacks the MongoDB database has rekindled last week and after the weekend with the arrival of three new groups hijack more than 26,000 servers, of which one group attacked 22,000 machines.

Malware that attacks the MongoDB database has rekindled last week and after the weekend with the arrival of three new groups hijack more than 26,000 servers, of which one group attacked 22,000 machines.

The attacks were discovered by security researchers Dylan Katz and Victor Gevers, following the MongoDB Apocalypse case beginning in late December 2016 and lasting until the first months of 2017.

In these attacks, many hacking groups search for MongoDB databases that are still open to external connections, wiping content and replacing blackmail content.

Most of these (DB) databases are test systems but some still contain data. There are companies that have paid and realize that they have been cheated and attackers who have never had their data.

Discover the new hijack MongoDB case

Some researchers tracked attacks with the help of Google Docs. The attacker has destroyed more than 45,000 databases, probably more.

From MongoDB, these extortion attacks have spread to other server technologies such as ElasticSearch, Hadoop, CouchDB, Cassandra and MySQL. Over the fall and summer, hacking groups related to the incident stopped and many hacked servers were unable to function.

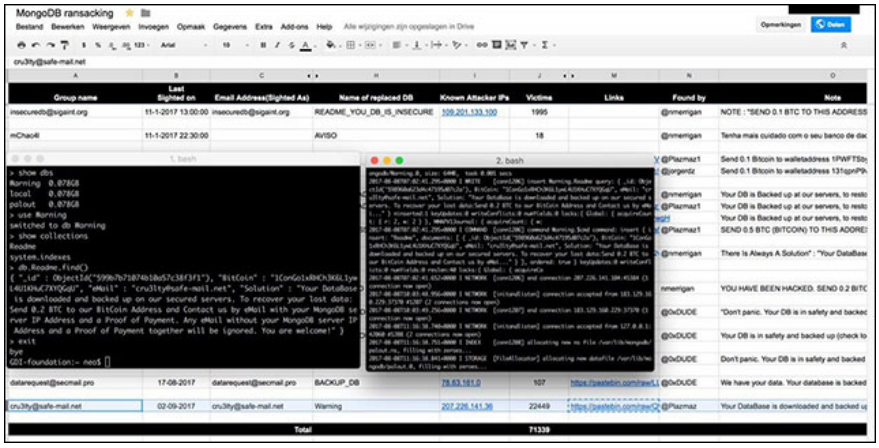
Last week appeared 3 new groups, discovered based on the email address they used in the extortion notice.

Email addressAuthentic numberNumber of requests Address Bitcoincru3lty@safe-mail.net 22,449 0.2 BTC Bitcoin address wolsec@secmail.pro 3,516 0.05 BTC Bitcoin address mongodb@tfwno.gf 839 0.15 BTC Bitcoin address

Fewer attacks but a wider effect

"Compared to the beginning of the year, the number of attacks has decreased but the level of influence (in terms of number of victims) per attack has increased," Gevers said. The first attackers need almost 1 month to hijack 45,000 DB, the Cru3lty group has halved it in just one week.

Gevers said he witnessed the hacker group hijack DB of the user, who restored the backup copy and then the server was attacked again on the same day because the victim did not secure DB Its right.



The number of attacks is less but the effect is greater

'Now we need to find out exactly what is going on. Is it due to a lack of knowledge, related to [MongoDB] security settings or are they running the old version that still has vulnerabilities and no default protection methods? '

Busy years for both attackers and researchers

Gevers said he had to invite some outside experts to analyze MongoDB attacks. Not because he and his colleagues could not investigate, but they were busy with holes in networked devices such as virtual money digging tools, modis of the Arris or IoT devices.

Gevers is the president of GDI Foundation, a non-profit organization working to ensure the safety of network devices. He has been busy for years to protect many types of devices, from AWS S3 to EternalBlue vulnerabilities .