Amazon AWS server will soon get extortion code, similar to MongoDB

Amazon AWS S3 cloud storage server may soon become a victim of malicious code, similar to the way hackers have kept many MongoDB databases to extort money in 2017.

Amazon AWS S3 cloud storage server may soon become a victim of malicious code, similar to the way hackers have kept many MongoDB databases to extort money in 2017.

Identified by information security expert Kevin Beaumont, this is not an unfounded prophecy that is shared by many other security experts.

Amazon AWS S3 has also leaked data

Data on Amazon AWS S3 leaked throughout the year, although other cases became a bit fuzzy. The reason is that companies leave data on 'buckets' (a term used to describe an S3 storage unit) S3 everyone reads and downloads data. Usually this data is secured by security researchers for the access system, but hackers can also get it.

There are bucket S3 more dangerous is that the bucket who can write, allowing anyone to write, delete data without having an Amazon S3 account. Report from Skyhigh Network in 9/2017 that 7% bucket on Amazon AWS S3 is the type that everyone can write.

AWS S3 will follow the path of 'MongoDB and friends'

Experts say hackers holding MongoDB, ElasticSearch, Hadoop, CouchDB, Cassandra and MySQL servers to extort money in 2017 will soon be eyeing the bucket who can write S3.

The extortion attacks in 2017 follow a similar formula. Hacker found a server with a vulnerability, scanned the data, leaving a note asking for money. There are victims who pay for ransom, but most have to give up because hackers do not have a backup place to back up all servers, so they cannot return the data.

The same story may happen to the owners of Amazon S3 servers. Researcher Dylan Katz said that data on S3 will be wiped out, not retained because the bucket S3 contains a lot of data that an attacker cannot hold.

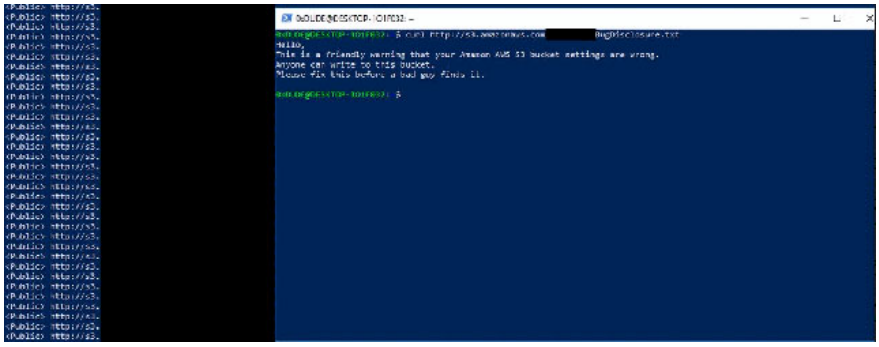
Technically, AWS S3 extortion attack is possible

The problem is that many AWS S3 account owners mistakenly configure the server so everyone can write. 'S3 as well as C language. There are many ways for a bad thing to happen'. Researcher Mike Gualtieri said. Mike also created a PoC script that proved to be able to use the server to make the victim believe that their data was

encrypted.

Researchers have warned every month

The above scenario made many security researchers fear. One of them was Robbit Wiggins when he searched for S3 buckets that everyone could write and left a warning file for the owner of that server for months.



Alert the owner of S3 server

But Wiggins found thousands of such servers. On a tweet, he said he warned 5260 bucket Amazon AWS S3. Wiggins is also not the only one doing this, there are also anonymous people who leave such warnings.

Finding AWS S3 is also not easy

Compared to tens of thousands of MongoDB servers, the number of buckets everyone can write of S3 is much less.

Technically it is more difficult to find servers of MongoDB, Hadoop or ElasticSearch, just scan IPv4 addresses on some ports. But the bucket of S3 uses a long name so the scanning rate when querying is also lower.

These restrictions prevent hackers from reaching S3, but it is not impossible to deal with dictionary attacks.

AWS S3 server contains a lot of sensitive data

According to Victor Gevers, researcher and GDI Foundation president, S3 buckets contain a lot of sensitive data that attackers will be very interested in such as intellectual property, design, backup files, keys, wallets. Bitcoin electronics .

Like Wiggins, Gevers also finds servers that have been misconfigured but not written buckets, but only readable buckets. Accordingly Gevers found and reported 529 servers, of which only 109 were quick fixes.

New malicious variants are appearing

According to Gevers, the AWS S3 server also doesn't need to be able to write to extort money. Gevers said that there will be another type of malicious code that attacks from May 25 this year, the EU GDPR effective date (the data protection standard whereby businesses store personal data must be approved by individuals. there).

The attacker only needs to capture the server, contact the company after May 25 and demand a ransom, otherwise he will notify the authorities and the company will be fined.

'Searching on Shodan or bucket S3 search engine will result quickly, you only need keywords,' Gevers said. Tools available as Public CLoud Storage Search or BuckHacker will make this as easy as childish.

Amazon also warned customers

Amaxon is not unaware of these things. They sent a message to all customers who accessed the bucket S3 last year and also warned on the AWS backend control panel. Since then, the number of S3 bucket vulnerable to attack has also decreased significantly.

However, the bucket on Amazon AWS S3 also does not have much time to secure anymore. Who owns the server should act quickly before their data is stolen or lost forever.

Amazon has given free access to all AWS customers to AWS Trusted Advisor S3 Bucket Permissions Check. This is a tool to check if the S3 bucket is running correctly. There is also S3 Inspector. https://github.com/kromtech/s3-inspector

See more:

1. AWS and Azure dominate the cloud world, above all, no one wins
2. MongoDB malicious code attacks more than 26,000 victims in a week
3. Microsoft shook hands with Amazon to beat Google rival cloud computing