AIG Alert:
Open Source Databases Are a Target for Recent Ransomware Attacks

AIG is monitoring the impacts of a current issue in which companies who utilize open source database software, like MongoDB or CouchDB, to establish a database may be at risk of losing their data and falling victim to a ransom based attack. Open source databases are enticing to use because they are cheap, flexible, and allow for quick setup of a database for a business. The problem is that these databases do not provide any default security protection, meaning that often the default database configuration is used without taking the time to implement security controls. This leaves the newly established database vulnerable to an attack.

No matter the open source software, the instances that are exposed to the internet are predominantly through cloud-based services, which are not responsible for protecting the database. It is anticipated that this type of attack will increase as databases remain exposed.

For example, the default configuration of the open source software MongoDB utilizes port 27017 for communications with the database. Hackers are utilizing a tool called Shodan to scan the internet for this port and to identify instances of MongoDB to target and attack. Once the attacker identifies a MongoDB database, they will access and download the data, delete it, and leave behind a ransom note requiring bitcoin payment to recover the data.[1]

Estimates suggest of the 50,000+ instances of MongoDB that are exposed to the Internet, more than 20,000 are compromised by this attack.[1] Other open source database platforms are also falling victim to these attacks. Estimates are that more than 4,500 instances of Elastic have been compromised in the same manner.[2] Hadoop and CouchDB, two other open source database platforms, are also experiencing the same type of attack.

Why are these attacks happening at such an alarming pace? The issue is that organizations are using open source database software to establish their database and store critical data without utilizing best practices to secure the database and their data. For example, the default configuration of MongoDB allows anyone to access the database without authentication and have read, write, delete capability. Companies that implement proper database security controls are not at risk from recent attacks.

What Can Organizations Do?

Business should identify any instances of open source database software in their environment by scanning for traffic on the default port, such as port 27017 for MongoDB, or looking for instances of the database running in their environment, such as mongod or mongos for MongoDB. Once all instances have been identified, business should consider the following recommended best practices to better protect their data:

- Ensure the database has been updated to the latest supported version of the software and any patches applied.
- Implement role-based access control with separate administrator and user accounts and enforce authentication to the database instance.
- Place the database behind a firewall with strict rules to deny all traffic except for specific application access.
- Implement strong encryption on all data queries and communications with the database.
- Consider implementing additional database encryption while following the NIST organization's[3] recommended best practices for key management.
- Maintain regular backups of data stored within the database.
- Review any further database security hardening practices recommended by the software provider.

When an organization or its employees suffer a cyber-attack, there's more than data at stake. In a rapidly changing landscape, a cyber breach or attack may cause property damage, broad business interruption, or harm to customers. That's why AIG provides clients with proactive risk services, comprehensive insurance coverage, and long-standing breach response and claims teams to help them stay ahead of cyber-related exposures. To learn more, visit www.aig.com/cyberedge.

[1] Krebs (January 2017) Extortionists Wipe Thousands of Databases, Victims Who Pay Up Get Stiffed; https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/#more-37597
[2] ZDNet(January 2017) Elasticsearch Ransomware Attacks Now Number in the Thousands; http://www.zdnet.com/article/elasticsearch-ransomware-attacks-now-number-in-the-thousands/
[3] NIST (January 2017) Nist Publication 800-57 part 1; http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

11/16 2815D