CRYPSIS™

CASE STUDY

Database Exposure Investigation: **POPULAR SOCIAL MEDIA SITE**

AT A GLANCE

A popular social media site discovered they had an exposed database — the question remained: Was it breached? The Crypsis team of experts went the extra mile to use client-side tools to investigate, assuring the client.

CLIENT CHALLENGE

A popular online social media site had reason to believe they had inadvertently exposed a significant amount of consumer data. They needed to bring in a third-party investigation firm to determine what happened, the scope of exposure, and how to properly secure their servers.

CRYPSIS SOLUTION

A team of experts was brought in from The Crypsis Group to investigate. They validated that a database was indeed exposed: Anyone who found the port could query the data, which contained personally identifiable information (PII); the port was exposed following a database configuration change. The database was configured to only log errors — not successful queries. Additionally, there were no firewalls, load balancers, or other network infrastructure in place that could have logged accesses to the database. This absence of database and network logs presented some challenges for the investigation.

By using a method known as "living off the land," (or, finding tools that already exist in the client environment), Crypsis identified a third-party utility used to track server metrics: DataDog. DataDog tracks processor usage, memory usage, disk errors, and daily network bandwidth (bytes transmitted and received). Logs are retained, at least for this client, for over a year. Not only did that cover the window of exposure, it gave the team a baseline of what "normal" looks like for six months prior to the exposure.

Analysis of the DataDog logs showed that the network usage remained consistent during the window of exposure. Additionally, there was a large "spike" at the end, representing Crypsis' queries into the database as they were identifying the data it contained. It is not uncommon for an attacker to do this type of identification when they gain access to a database. Crypsis did not identify any other spikes during the period covered by DataDog. Crypsis was able to validate this finding using the atop utility included in many Linux distributions. Atop monitors processes from the time they are started and tracks metrics such as disk I/O and network utilization. As Elasticsearch runs under the Java process (and was started at the same time the server rebooted, causing the exposure), the statistics tracked covered the entire window of exposure. Atop showed high levels of disk "write" activity for Java, but low levels of "read," as well as a consistent network utilization seen in DataDog. Together, these findings helped the client and their legal counsel draw conclusions regarding their data breach notification obligations. Ultimately, these findings were central to avoiding a substantial data notification effort.

RESULTS

Because of Crypsis' "extra mile" efforts, the team was able to not only provide insight into the likelihood of a breach, but also saved a company from significant disclosure and scrutiny by regulators. It provided the client much-needed peace of mind that their customer data was secure and helped them to become more secure in the future.