MITIGA

Case Study

Mitiga Investigates, Remediates Breach through Third-Party Plugin

THE CHALLENGE:

third-party marketplace breach creates network effect of breaches for plugin users

One of Mitiga's customers, a global company in the eCommerce industry, identified a breach in their environment. A developer at the company had installed a code analytics plugin from GitHub marketplace to try it out, then forgot to remove access. The third-party plugin was later hacked, but ten months elapsed between detection of that breach and notification to users of the plugin. It took a further ten days to notify affected customers of the compromise. This allowed attackers considerable time to access our customer's code. It was essential to quickly evaluate the potential impact.

THE SOLUTION: rapid evaluation of breach impact

To evaluate the potential abuse of the attackers, Mitiga's cloud incident readiness and response platform and services enabled the researchers to scan the logs within minutes to determine the impacts of the compromise.

Their data, including sensitive artificial intelligence algorithms, a critical element of their intellectual property, was stolen and leaked on the Darknet.

The incident response team used Mitiga's platform to accelerate containment of the threat and to conduct root cause analysis. They researched whether there were additional secrets leaked that could have compromised their entire cloud infrastructure (AWS/GCP). The investigation assessed whether there were hard-coded credentials stored within GitHub and conducted threat hunting based on Amazon Web Services (AWS) and Google Cloud Platform (GCP) anomalies that would have suggested compromise.

The anomalies detected included:

- **Change in permissions**
- **Irregular geographic logins**
- **Modifications in permissions and security groups**

Because the third-party plugin allowed the attackers to compromise the source code, they were able to view the entire history of that code, including clear-text cloud secrets stored in older versions. Those cloud secrets allowed the attackers to compromise their entire cloud environment. While they rotated and secured their secrets upon notification of the breach, the security team had not considered the possibility of stored secrets in older versions of code available on GitHub. Due to the lag between the third-party plugin breach and notification, attackers were able to discover and use the stored secrets for a considerable period. Their data, including sensitive artificial intelligence algorithms, a critical element of their intellectual property, was stolen and leaked on the Darknet.

THE BENEFITS: rapid insight into breach and improved security

Mitiga's rapid investigation provided the customer with information that clarified that, while their code was leaked, the infrastructure had not been compromised.

This information reassured the customer, providing assurance that threat actors were not able to further attack their infrastructure. Mitiga aided in all aspects of the incident response, including communicating with legal, insurance, and public relations teams to manage prompt and informative customer notifications.

Mitiga aided in all aspects of the incident response to manage prompt and informative customer notifications.

Mitiga also supported the security team in their efforts to return to business as usual rapidly. This included security recommendations to help the internal security team to prevent this type of attack in the future, including guidance about specific userIDs, roles, and permissions to change to increase security. Mitiga also supplied guidance on the potential effect of installing third-party plugins, managing the permissions of those plugins, and tracking plugin use to ensure that unused plugins are removed to reduce potential risks.

Mitiga's technology and services optimize readiness for cloud and hybrid incidents and accelerate both response and recovery times when incidents occur. Importantly, Mitiga's readiness prioritization also increases resiliency for future incidents. Mitiga's shared-responsibility model is unique. Unlike others, who charge additional fees for incident response and recovery, Mitiga subscribers face no add-on fees.

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | **UK** +44 (20) 3974 1616 | **IL** + 972-3-978-6654 | **SG** +65-3138-3094

MITIGA aws partner network