CUSTOMER CASE STUDY

Mid-size Bank Customer Case Study

How Security On-Demand identified suspicious connections to cloud services

The Breach

Security On-Demand's cloud security monitoring service as a part of the ThreatWatch behavioral analytics service detected abnormal network traffic patterns and URL access requests in the client's logs. The event was sent to the Threat Reconnaissance Unit to be further evaluated by a SOC analyst. After further analysis, the Threat Reconnaissance Unit determined that unknown users connected to a file sharing application and shared files without authorization. The users also exploited vulnerabilities in the remote control service.

The Result

The Threat Reconnaissance unit within SOD recognized that not all unauthorized file sharing indicates a breach, so they notified the client with a % level of confidence that the activity came from outside threat actors. Ultimately, the activity was considered suspicious enough to explain the potential risks and recommend a plan to validate the threat.

The client shut down the suspicious user accounts associated with the activity, and further investigation revealed custom malware, designed to exploit customer banking and account information. During the following days and weeks after the detection, the company remained on high alert, and we continued to monitoring their traffic to ensure indicators were no longer in their network.