Identification of Suspicious Connections to Cloud Services

Customer:

Mid-Size Bank

Issue

Unauthorized sharing of documents involving users connecting to file sharing and exploiting vulnerabilities in remote control service.

How We Detected

Through integration of our cloud security monitoring service, we detected the behavior by observing abnormal network traffic patterns and URL access requests.

How We Responded

When we detect activity that isn't inherently indicative of a compromise, but is nonetheless suspicious, our notification detail rates the level of confidence we have about the issue, an explanation of potential risk and recommendations for validation of the threat.

Customer Response & Follow-Up

Customer was able to disable specific user accounts associated with the activity. Further investigation revealed a confirmed instance of custom malware designed to exploit customer banking and account information.

Vulnerability