Vandalay SIEMs Report

[SidneyRobinson@vandalay.com](mailto:SidneyRobinson@vandalay.com)

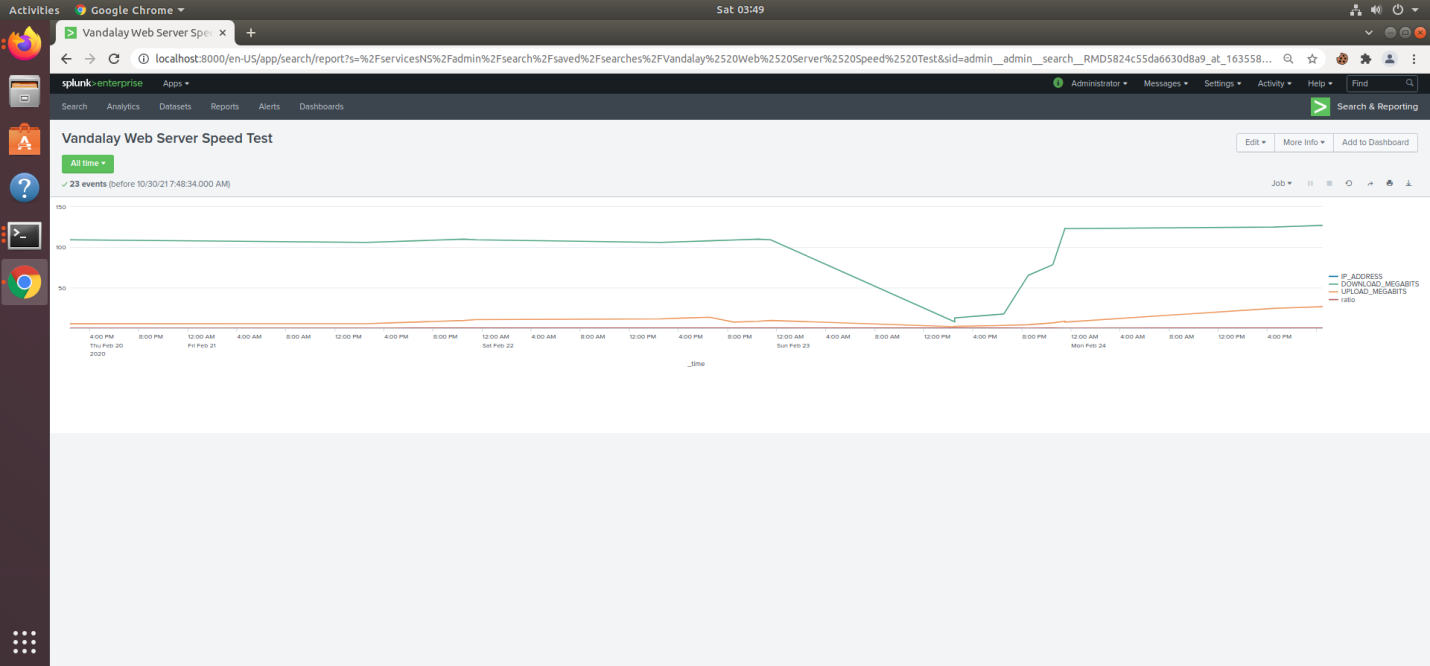
10/31/2021

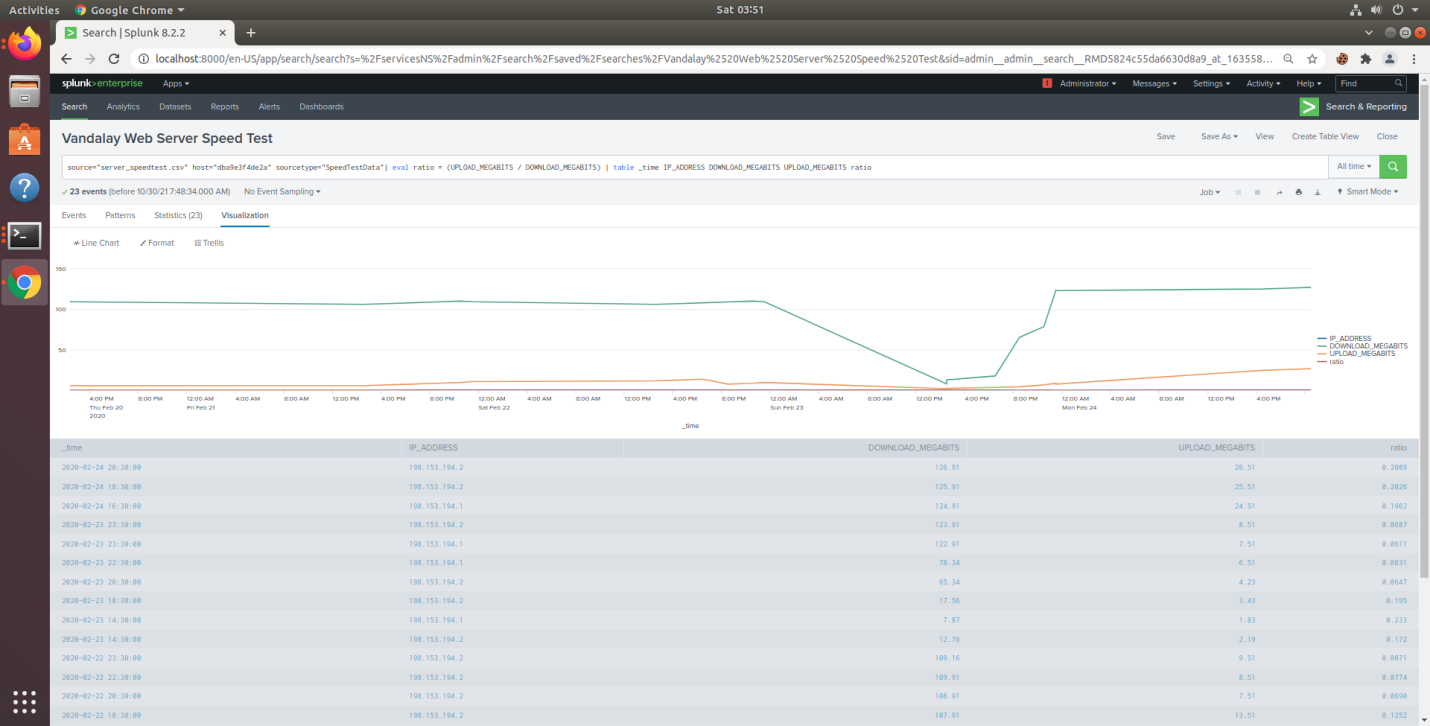
# High-Level Summary

Vandalay Industries, is a worldwide Leader of imports and exports, and as such, Vandalay has attracted the attention of bad actors in cyberspace. Recently, Vandalay Industries has been the target of an adversary attempting to disrupt our online business with DDOS attacks against our web servers. During the attack, a Vandalay web server where taken offline by a DDOS attack and our upload and download data speeds were greatly impacted. We have also discovered that a brute force attack was directed against administrator login accounts.

# DDOS Attack Impact on Upload and Download Speed

We have created the Vandalay Web Server Speed Test report. This report summarizes the network speed results along with upload/download speed ratios. This report will allows us to analyze further network speed data runs as provided by the Networking Team going forward. Here are current results;

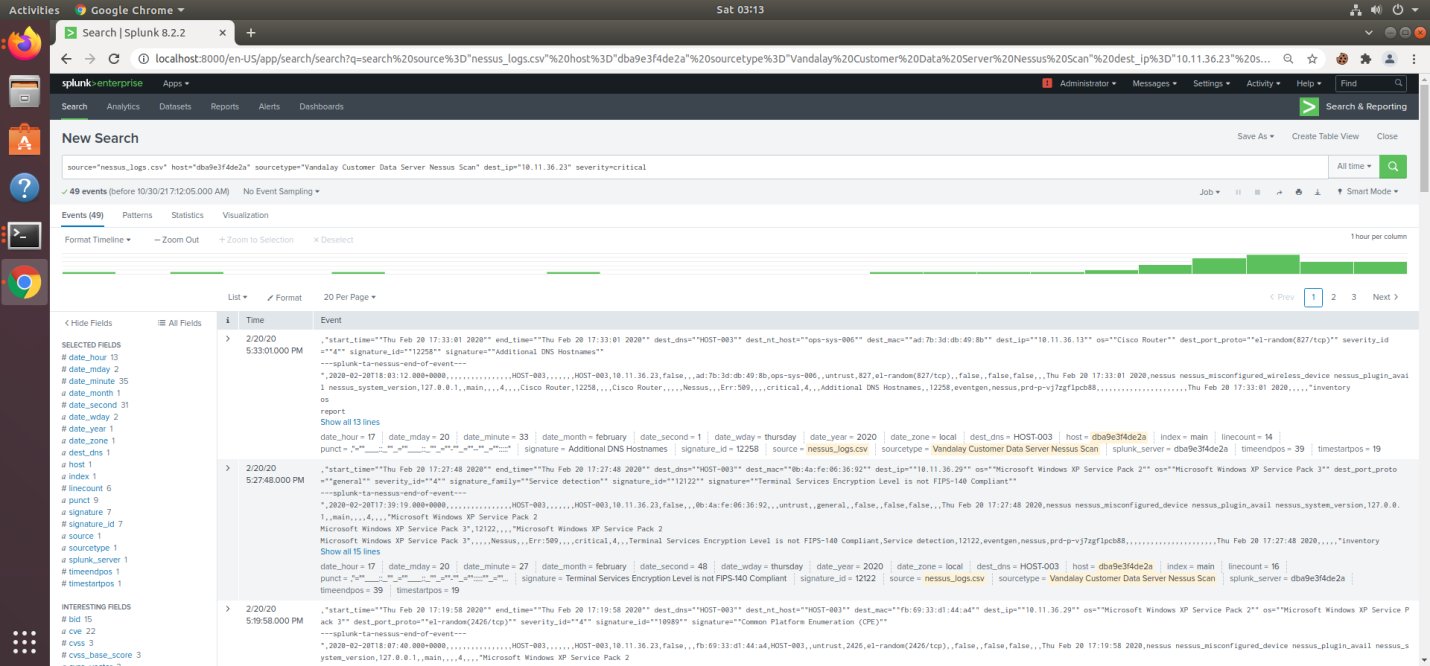


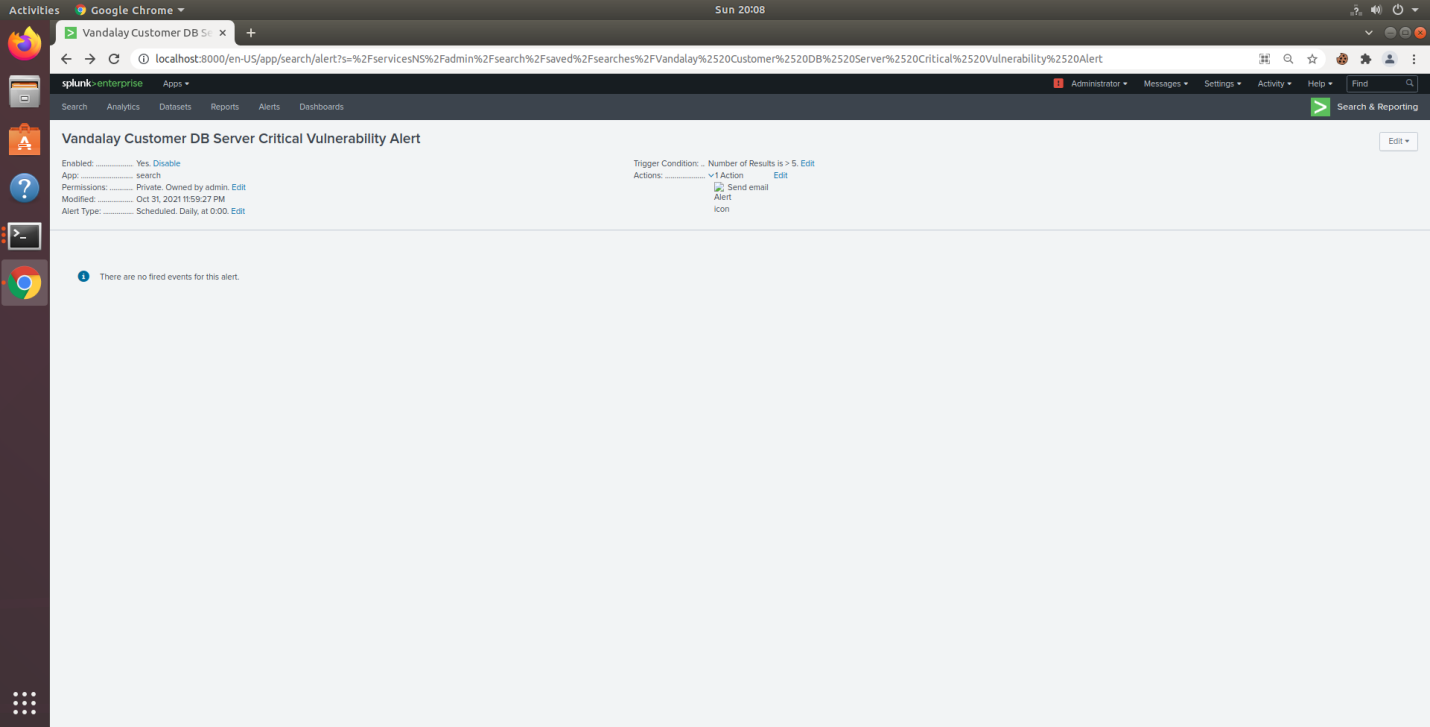


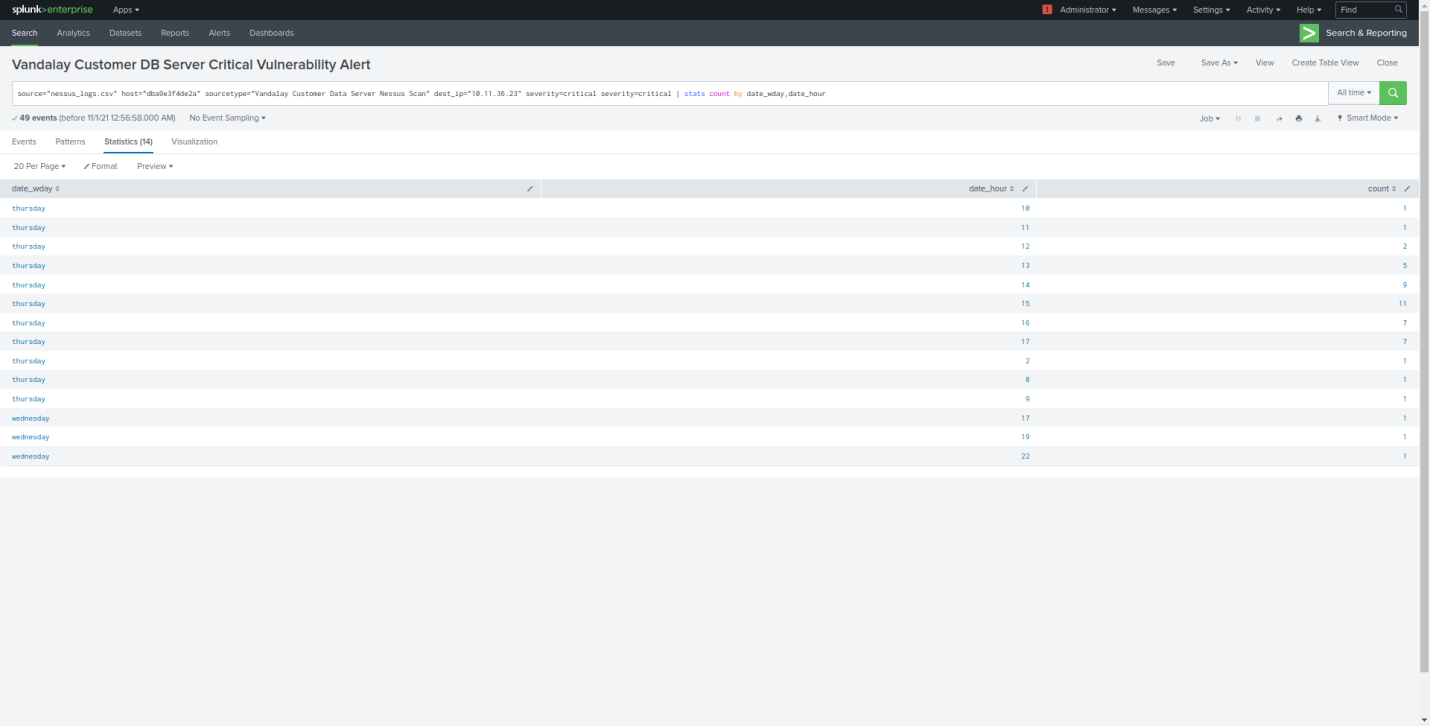
As illustrated in the reports above, the denial of services attack began on 02/23/2020 around 2:30pm(14:30) and affected the Vandalay web server’s (ip 198.153.194.2) ability to properly upload and download data until 10:30pm(22:30).

# Vulnerability of sensitive customer data

We have also created the Vandalay Customer DB Server Critical Vulnerability Report and Alert. This report uses Nessus vulnerability scan data logs to displays all “Critical” vulnerabilities logged and identified by the Nessus Scan logs. A high level email alert is sent to the SOC at [soc@vandalay.com](mailto:soc@vandalay.com) when critical vulnerabilities exceed 5 critical alerts in one hour. Please see the current results below;



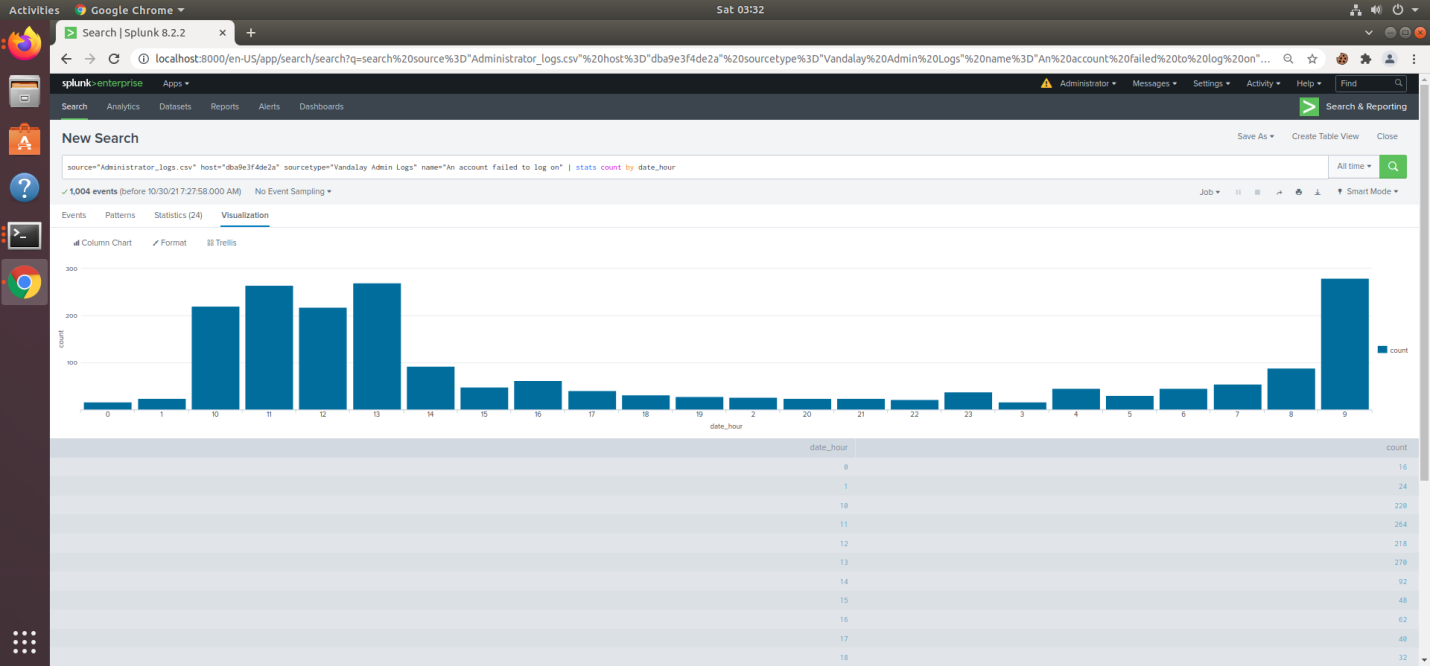


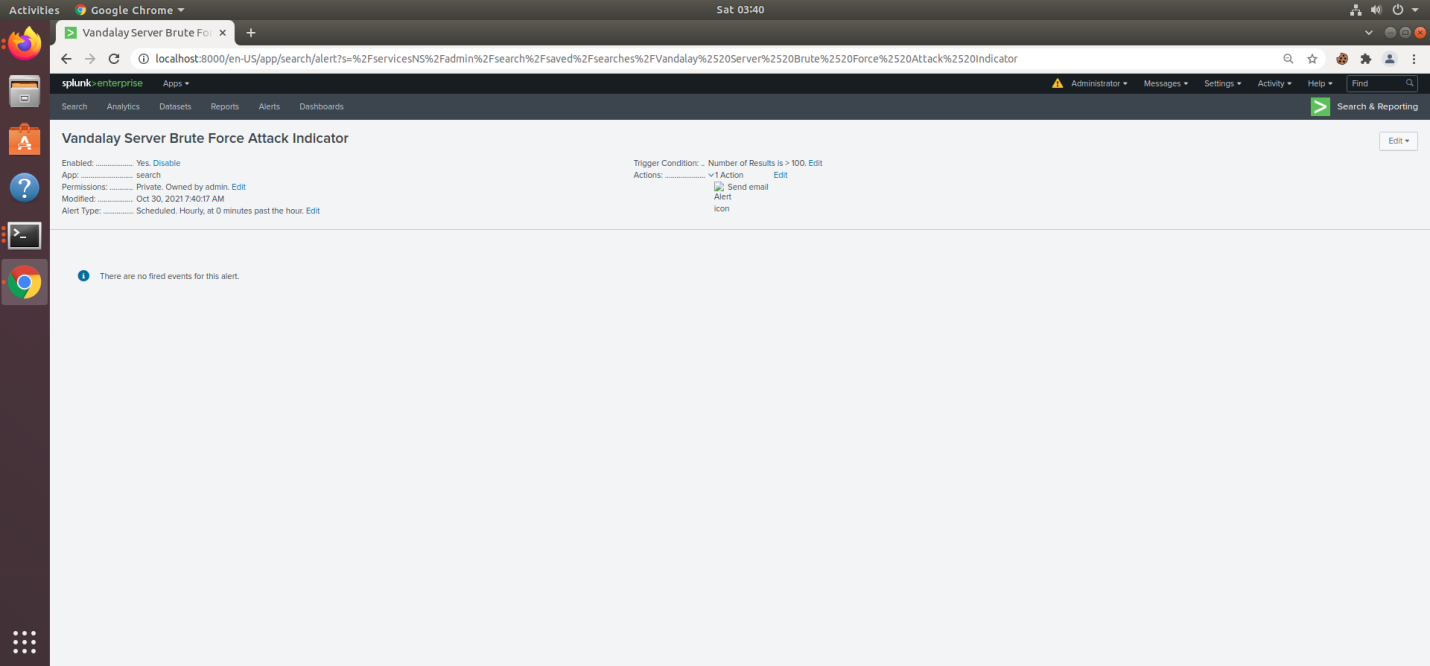


The Nessus vulnerability scan data was also measured by day and day hour to determine a starting base line. The data showed that a maximum of 11 and a minimum of 1 critical vulnerability event(s) are experienced per hour (ip 10.11.36.23). We have currently set the baseline at 5 or less event(s) per hour. This alert baseline can be adjusted as necessary, and as required by the SOC Team to pre-empt customer data vulnerability.

# Brute Force Attack Detection

We have created the Vandalay Server Brute Force Attack Indicator Report. This report warns and helps to mitigate brute force attacks against administrator accounts. This report monitors the volume of failed admin login attempts per hour, and sends an alert to the SOC at [soc@vandalay.com](mailto:soc@vandalay.com) when the number of failed attempts exceed 100 events in one hour.





Based on the above Vandalay Server Brute Force Attack Indicator Report, normal failed admin logins should not exceed 90 to 100 per hour. We have set the report’s initial alert threshold to no greater than 100 failed admin login attempts per hour. This alert baseline can be adjusted as necessary, and as required, by the SOC Team to pre-empt admin account - brute force attacks.

# Findings

The recent cyber DDOS attack on Vandalay Industries affected the company server’s ability to upload and download data for approximately 9 hours. No doubt that the outage will have a financial impact. Further investigation by SOC will be necessary concerning the level of success and escalation to mitigate the brute force attack against the administrator logins. We have responded to these events by analyzing the data and creating reports to monitor and alert for DDOS and administrator account brute force attacks. We have also created additional reports to issue critical vulnerability warnings in order to protect customer data servers. Further efforts will be necessary to detect, respond to, and harden Vandalay systems against cyber attack.