Detecting ATM fraud

Applicability

- Product: Splunk Enterprise or Splunk Cloud Platform
- Function: Monitoring, alerting, reporting
- Data: Business service data for ATM transactions
- A CSV or KV lookup file of ATM user risk scores, already loaded into your deployment

Scenario

You work for a large bank with hundreds of ATMs, each with thousands of users. For government compliance reasons and to protect your customers, you need to monitor these ATMs for signs of suspicious activity. You want to evaluate potential risk of ATM fraud by performing analyses that help to indicate outliers and anomalies of fraudulent behaviors or transactions. You also need to make recommendations to the rest of the security team about which users should be investigated for potentially fraudulent activity.

Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

Splunk recommends that customers look into using data models, report acceleration, or summary indexing when searching across hundreds of GBs of events in a single search. The searches provided here are a good starting point, but depending on your data, search time range, and other factors, more can be done to ensure that they scale appropriately.

Report on most frequent ATM users

Users that use the ATM more than most average users may have questionable motives or have their credentials stolen. You want to see who those users are so you can set up alerts to watch their accounts for any suspicious activity.

```
|source-type=<ATM transaction data source>
|lookup <name of lookup file for ATM user risk scores> user OUTPUT score
|stats sum(score) AS Risk_Score count BY user
|eventstats avg(count) AS avg stdev(count) AS stdev
|where count>(avg+stdev*3.5)
|sort - count
```

Need more help with this search? Click here.
Alert on ATM withdrawal testing

As a financial institution employee, you know that suspicious users sometimes "test" ATM cards by making a small withdrawal first to see if they work and then, if that transaction is successful, they make a large withdrawal. Rarely do legitimate users withdraw very small amounts and very large amounts in a short one minute window. You want to create an alert to trigger on this suspicious activity.

|sourcetype=<ATM transaction data source> |search action=withdrawal |streamstats count time_window=1m min(amount) AS min max(amount) AS max BY user,location |where count>1 and min<20 and max>9000 |table _time user action min max location |dedup user, location |eval min=tostring(round(min, 2),"commas") |eval max=tostring(round(max, 2),"commas")

Need more help with this search? Click here.

Determine riskiest ATM users

Finding out who are riskiest users can help determine whether their questionable transaction activity may be involved in fraud. For each ATM your company manages, you need to calculate a risk score for each user so you can create a watchlist of users to monitor.

|sourcetype=<ATM transaction data source> |lookup <name of lookup file for ATM user risk scores> user OUTPUT score |stats sum(score) AS Risk_Score count BY user |sort - Risk_Score |head 5

Need more help with this search? Click here.

Detect users accessing multiple ATMs simultaneously

Users who withdraw from multiple ATMs at almost the same time are most likely committing fraud. You want to create an alert that will trigger when a unique user makes a transaction at two ATMs in different locations within a very short time period.

|sourcetype=<ATM transaction data source> |search action=withdrawal |eval amount=tostring(round(amount, 2),"commas") |streamstats time_window=1m dc(location) AS dc list(amount) AS amount list(location) AS location earliest(epoch) AS epoch latest(epoch) AS latest_epoch BY user |where dc>1 |dedup user |eval first_time=strftime(epoch,"%m/%d/%y %H:%M:%S"), last_time=strftime(latest_epoch,"%m/%d/%y %H:%M:%S") |table user amount action location first_time last_time

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Detect ATM withdrawals near threshold

In many countries, if a transaction is over a specified limit, it must be reported to the government. To slip under the radar, suspicious users may keep their transactions just under the limit. Users who consistently make ATM transactions just below the government threshold might be trying to hide their activity. You want to report on these transactions to decide if certain users require further investigation.

|sourcetype=<ATM transaction data source>
|where amount>9800 AND amount<10000
|table _time user action amount
|eval amount=tostring(round(amount, 2), "commas")

Results

Use the results of these searches to make recommendations to the rest of the security team about which users should be investigated for potentially fraudulent activity. Further actions might include:

- Running these search on a regular schedule to evaluate activity and track suspicious users over time.
- Creating searches and alerts to watch the transactions that your risky users make.
- Using the Splunk Enterprise Security land speed violation use case for additional information relevant to fraud related to multiple locations.
- Compare users' risk scores to other data points to determine whether users need to be put on a watchlist.

Be sure to follow any industry policies and regulations that are required for compliance.

Additional resources

The Splunk Essentials for the Financial Services Industry app helps you automate the searches provided in this article. The app also provides more insight on how they can be applied in your environment, how they work, the difficulty level, and what data can be valuable to run them successfully. In addition, the Splunk Essentials for the Financial Services Industry app provides a number of other fraud detection solutions for financial services:

- Banking fraud
- Credit card fraud
- Wire transfer fraud

You might also be interested in monitoring ATM usage for business service insights.

Finally, these additional Splunk resources might help you understand and implement this use case:

- .Conf Talk: 40 ways to use Splunk in financial services
• Case Study Video: ATM Fraud