THREAT HUNTER TEMPLATE

Playbook Title:
Detecting Enterprise Macro Activity from Emails

Mitre Tactic:
T1566, Phishing

Mitre Sub Technique:
T1566.001, Spearphishing Attachment

Hypothesis:
Employees are targeted with malicious documents with VBA Macro Code and some employees will open the documents and detonate the payload

Proposed Detection Query:

> Leverage Zeek and Sysmon telemetry logs to detect TrustRecords in Microsoft Document Formats

```
index IN (zeek,sysmon) (.doc OR .xls OR .docx OR .xlsx) (TrustRecords)
AND NOT (files.magnumtempusfinancial.com)
```

Simulation Details: NONE

Hunter Limitations/Observation Notes:
During several portions of the hunt, we discovered that there were log sources (sysmon) that were not properly parsed, which made finding details difficult. If we had these parsed properly, we may have found it easier to get some of the data.

Hunt Findings:
Three users downloaded the malicious document, two users appear to have been affected by the payload.