Enriching suspicious email domains

Phishing remains the single most popular technique for attackers. The open nature of email and your reliance on it for communication make it difficult for defenders to classify messages, so suspicious email investigation is one of your top use cases for automation. You would like to use Cisco Umbrella Investigate to look at a domain name, add the risk score, risk status, and domain category to the event in Splunk SOAR. That way, when analysts are assigned events, they will be able to more quickly recognize the purpose of the email, and the domain enrichment will also provide a connection point to take further action on the output.

Required data

Cisco Umbrella Investigate

How to use Splunk software for this use case

The playbook starts off by fetching the whole text of the event and all of its artifacts, then running a regular expression against that text to extract any email addresses it contained within. From there, two separate domain reputation queries are run on the domains from the extracted email addresses, as well as any domains that were extracted upon email ingestion. Taken together, these should analyze any domains from the email headers and body. The next step is a query against Cisco Umbrella Investigate to determine the risk scores, risk status and categorizations of those domains. Umbrella provides a wealth of threat intelligence about domain names backed by Cisco’s threat research and broad visibility into internet traffic, so this often produces valuable insights into the purpose of a domain and the potential for harm. The remainder of the playbook formats key fields from the domain reputation result and presents them in a note to the analyst. To use the playbook:

1. Configure the Cisco Umbrella Investigate app on Splunk SOAR:
   1. Navigate to Home>Apps>Unconfigured Apps>Search for Cisco Umbrella Investigate>Configure New Asset
   2. Give the asset a name such as “umbrella_investigate”.
   3. On the Asset Settings page, provide the API key from the Umbrella web application.
2. If you haven’t previously used the Suspicious email domain enrichment playbook, configure and activate it.
   1. Navigate to Home>Playbooks and search for suspicious_email_domain_enrichment. If it’s not there, click Update from Source Control and select Community to download new community playbooks.
   2. Click the playbook name to open it.
   3. Resolve the playbook import wizard by selecting the newly created app.
   4. Set the label to email (or whichever name was chosen above in the email configuration).
   5. Set the playbook to Active.
   6. Save the playbook and then run it.
Next steps

This playbook starts the enrichment process for a suspicious email, but there are many possibilities for additional response. For instance, domain names with risk scores higher than a certain threshold could be used to initiate a “block domain” or “delete email” action to prevent the user from following a link in a phishing email. Similarly, endpoint protection tools could be used to track activity on a potentially infected endpoint to monitor for users that may have followed a phishing link and been exposed to credential theft or client-side malware.

The content in this article comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. In addition, these resources might help you understand and implement this guidance:

- Tech Talk: Suspicious email domain enrichment