Monitoring a network for DNS exfiltration

Scenario: A long-standing customer reported to your organization that they found a large number of your company’s marketing plans and product roadmaps on a competitive intelligence website. You believed that your wonderful and loyal coworkers would never betray the organization like that, and your investigation showed you were right. It turns out that hackers used DNS to control compromised hosts and exfiltrate the data. You now need to set up monitoring so that this doesn’t happen again. You can use Splunk software to monitor for changes that are indicators of data exfiltration. These include spikes in client volume, changes in resource type behavior, changes in packet size, hosts repeatedly checking in with the command infrastructure, and domains that have many subdomains.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- **People:** Security analyst, threat hunter
- **Technologies:**
  - Splunk Enterprise or Splunk Cloud Platform
  - [Splunk App for Stream](#)
- **Data:** DNS data

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor DNS logs for signs of data exfiltration. Depending on what information you have available, you might find it useful to monitor for some or all of the following:

- Change in requests for specific resource record types
- Increases in packet size or volume distribution
- Signs of beaconing activity
- Excessive subdomains
- DNS tunneling through randomized subdomains
- DNS queries to randomized subdomains
- HTTP GET requests

Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

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.
• Developing access policies and conducting audits for compliance
• Identifying and classifying sensitive data
• Installing network perimeter and endpoint protection

Measuring impact and benefit is critical to assessing the value of security operations. The following are example metrics that can be useful to monitor when implementing this use case:

• Number of positive exfiltration attempts identified: The number of investigations you initiated from your monitored data that were positive attempts are data exfiltration.

Additional resources

The content in this use case comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this specific use case:

• Blog: Detecting dynamic DNS domains in Splunk
• Conf Talk: Using Splunk and DNS to detect that your domains are being abused for phishing