Detecting SNICat SNI data exfiltration

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Monitoring
- Technology: Splunk Add-on for Google Cloud Platform
- Data: Google Cloud Platform

Scenario

Like many organizations, your organization needs to prevent the stealing of its data by an adversary through data exfiltration. Exfiltration can happen in a range of different ways.

- Adversaries can collect data over encrypted or non-encrypted channels.
- They can utilize command and control channels that are already in place to exfiltrate data.
- They can use standard data transfer protocols such as FTP, SCP, etc to exfiltrate data.
- They can also use non-standard protocols such as DNS, ICMP, etc with specially crafted fields to try and circumvent security technologies in place.

Finally, a TLS server name indication (SNI) extension can be used to exfiltrate data. The SNI exfiltration method is successful in bypassing many security controls. However, you can use this search to identify commands that the SNICat tool uses in the TLS SNI field.

- To run this search you must ingest Zeek SSL data into your Splunk deployment. Zeek data must be ingested in JSON format.
- 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.

Detect SNICat SNI exfiltration

This search detects when any of the predefined SNICat commands are found within the server_name (SNI) field. These commands are LIST, LS, SIZE, LD, CB, EX, ALIVE, EXIT, WHERE, and finito.

You can go further after a command has been detected and run other searches to decode the SNI data to prove or disprove if any data exfiltration has taken place.
search (index=zeek sourcetype=“zeek:ssl:json”) | rex field=server_name “(?<snicat>(LIST|LS|SIZE|LD|CB|CD|EX|ALIVE|EXIT|WHERE|finito)-[A-Za-z0-9](16)\.)” | stats count BY src_ip dest_ip server_name snicat | where (count > 0) | table src_ip, dest_ip, server_name, snicat

Additional resources

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help you detect abuse attempts within your environment, including:

- Detecting host redirection attacks
- Detecting Netsh attacks
- Detecting web fraud

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.