Detecting software supply chain attacks

Scenario: Your organization develops software and you are responsible for threat hunting within it. You have become aware of the increasing frequency of software supply chain attacks which threaten your source codes, build processes, and update mechanisms by infecting legitimate apps to distribute malware. Detecting these attacks, however, is not easy - your organization uses a wide range of software, services, infrastructure and people within the development of your software, making it difficult to apply detection techniques across them. You are aware of the JA3 open-source methodology that allows for creating an MD5 hash of specific values found in the SSL/TLS handshake process. You also know that both JA3 and JA3s are easily obtained from network traffic using various tools. You want to leverage JA3/s hashes as a high fidelity data point to bring anomalous activity close to the forefront.

Prerequisites

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

- People: Security analyst, threat hunter
- Data:
  - Microsoft: Sysmon
  - Deep packet inspection data
- Technologies: Splunk Cloud Platform or Splunk Enterprise

How to use Splunk software for this use case

Depending on your environment, you might find it useful to identify some or all of the following:

- JA3/JA3s hash overview
- First time seen JA3/JA3s hashes
- Rarest JA3s hash and server combinations
- Anomaly probability calculation with JA3/JA3s hashes
- Lookup table creation for scalable anomaly detection with JA3/JA3s hashes
- Windows process and JA3s hash correlation

Results

It is highly probable that by using these searches, anomalous activity can be detected via abnormal JA3/s hashes. However, a number of factors that could affect the success. Therefore, these searches are most effectively run in the following circumstances:

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.
• with an allow list that limits the number of perceived false positives.
• against network connectivity that is not encrypted over SSL/TLS.
• with internal hosts or netblocks that have limited outbound connectivity as a client. None of the searches will work effectively against internal source hosts used for general web browsing or hosts that routinely reach out to a multitude of external services via SSL/TLS sessions.
• in networks without SSL/TLS interceptions or inspection. This is because SSL/TLS interceptions show different characteristics than the actual external server to the client making the request.

Additional resources

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

• .Conf Talk: Hunting the known unknown - Software supply chain attacks
• Whitepaper: Detecting supply chain attacks
• GitHub: Hunting the known unknown -- Software supply chain attack