Severity

Medium

Analysis Summary

Smoke Loader — a malicious bot application — can be used to load additional malware. Smoke Loader has been spotted in the wild since 2011, carrying a variety of payloads. This malware is mostly used to load additional malicious software, which is often obtained from a third-party source. Smoke Loader can load its modules allowing it to do several activities without the use of additional components. To date, the supplier of Smokeloader, who goes by the alias SmokeLdr, is still active in delivering this malware as a service. It is well-known for using deception and self-defense. This malware can be spread in several ways and is widely linked to criminal activity. To hide its C2 activity, this malware sends queries to popular websites like microsoft.com, bing.com, adobe.com, and others.

Impact

- Information Theft
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- 5ec354f88ee7e7ed8871cf64daae490a
- 7203711617b94fe6724676538babef6e
- 2efff80f0710c410bb7aa21b77ced964
- cda548aedabf744baf41925582ab3e50

SHA-256

- 008830c5e7ae84eb28836568dbca222d29b4442e3134bf4f49c02686b48e09bf
- 0314024e779261c0d070d755ee6e87bca22c4887a94c0223f7b072834652d12a
- 0492e7197c5c9a58148b7e8f1115bfc939421c32af3e06db5ee7cf89e5768c69
- 6a15e2734d22e9b1fce00ad3febe41c16582174e2dc029e24c7d5ec73eb28954

SHA-1

- cea09964aed666bbd19d01d21dfb7bbc7a3f1521
- 8c9a7bf11c9f4e27188e2ca5fd465ff2bca436c3
- d70132c7526ef315ca14d3b34e51341eabe2ad52
- fe535c259fb413621684795116a189e34ef0a113

Remediation

- Exercise caution when receiving messages from unknown senders.
- Block all threat indicators at your respective controls.
- Keep your software updated to the latest patches.
- Search for IOCs in your environment.