Mphasis
The Next Applied

Cybercriminals Employ PhantomLoader to Distribute SSLoad Malware

Date: 13th June 2024 | Severity: High

Summary

The nascent malware known as SSLoad is being delivered by means of a previously undocumented loader called PhantomLoader, according to findings from cybersecurity firm Intezer. Researchers at Intezer have provided an in-depth analysis of SSLoad, a stealthy malware targeting victims since April 2024. It highlights the diverse delivery methods, including phishing emails with decoy Word documents and fake Azure pages, leading to the installation of SSLoad payloads. The investigation looks into the malware's functionality and payload execution chain, with a focus on flexibility and potential usage in Malware-as-a-Service operations.

Attack Vectors

- SSLoad is a stealthy malware that is used to infiltrate systems through phishing emails, gather reconnaissance and transmit it back to its operators while delivering various payloads. One attack vector involves a decoy Word document that delivers an SSLoad DLL, which eventually executes Cobalt Strike. The other attack utilizes a phishing email that leads to a fake Azure page, downloading a JavaScript script that ultimately downloads an MSI installer, which loads the SSLoad payload.
- Phantom Loader is a self-modifying loader. It first decrypts the stub function, which then extracts the payload from the resource section. The decoding logic employs an XOR decryption method. Each byte of the encrypted code at a specified address is XORed with a corresponding byte from a predefined encryption key. The key repeats cyclically if the code's length exceeds the key's length.
- Once the code is decrypted, the instruction pointer (EIP) will point to the first instruction. The stub then implements the same XOR decryption using the same key to extract the encoded payload from the resource section. After decoding the payload, the stub loads and executes it. This payload is another loader.
- The payload is a 32-bit DLL written in Rust, identified as SSLoad. This stage has not been documented in previous blogs, indicating it might be an additional step in the delivery chain. Key strings, such as the user agent and domains, are encrypted using a unique algorithm. This SSLoad variant begins by decrypting a URL and a user agent. The URL directs to a Telegram channel named SSLoad, which serves as a dead-drop site, as shown in the screenshot below. This channel contains another encrypted string that indicates the Command-and-Control (C2) server responsible for delivering the final payload.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 90f1511223698f33a086337a6875db3b5d6fbcce06f3195cdd6a8efa90091750 • 09ffc4188bf11bf059b616491fcb8a09a474901581f46ec7f2c350fbda4e1e1c • 265514c8b91b96062fd2960d52ee09d67ea081c56ebadd7a8661f479124133e9 • 6329244cfb3480eae11070f1aa880bff2fd52b374e12ac37f1eacb6379c72b80 • 73774861d946d62c2105fef4718683796cb77de7ed42edaec7affcee5eb0a0ee • 6aa3daefee979a0efbd30de15a1fc7c0d05a6e8e3f439d5af3982878c3901a1c
URL	• https[:]//t.me/+st2YadnCIU1iNmQy
IP address	• 85.239.53[.]219

Recommendation

- Avoid downloading files or attachments from external sources, especially if the source was unsolicited. Common file types include zip, rar, iso, and pdf. Zip files were used during this campaign.
- Monitor common malware staging directories, especially script-related activity in world-writable directories.
- Using a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) tool to detect and contain threats.
- Do not open attachments or web links that are presented in irrelevant emails and/or emails that are received from unknown, suspicious addresses.
- We recommend to regularly scan the operating system for threats with reputable antivirus or anti-spyware software, which should be kept up to date.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://intezer.com/blog/research/ssload-technical-malware-analysis/
- https://thehackernews.com/2024/06/cybercriminals-employ-phantomloader-to.html