Severity

High

Analysis Summary

Meterpreter — a trojan-type program — enables attackers to take control of affected machines remotely. This malware injects itself into compromised processes rather than creating new ones. Meterpreter can transmit and receive files, launch executable files, perform command shell operations, capture screenshots, and record keystrokes. The main objective of its distribution is either to generate revenue or infect devices with additional malware. Infected email attachments, malicious online advertisements, social engineering are some of its distribution methods. Cyber thieves can infect victims' systems with more malware, such as ransomware, by sending, receiving, and executing files using Meterpreter. Ransomware encrypts data, making it impossible for victims to use or access it unless they acquire decryption tools from the program's creators. Identity theft, banking information, and passwords theft are the main impact of this trojan

Impact

- Information Theft
- File Encryption

Indicators of Compromise

MD5

- 33e75e9fe89b6f9ac800241f77c65af9
- 754a201f853985b0c1c5a96d4637966d

SHA-256

- 05936ed2436f57237e7773d3b6095e8df46821a62da49985c98be34136594ebd
- 8b831ee82975d43456ee861115272d3923e17f07a702eb057feeed8ce76ff4ca

SHA-1

- 3b62c663e35bb3ca04afb75a839f25302579ebe5
- 12b6c8ab12dc04106e9ac74f790a1145bdb3d844

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.