Severity

High

Analysis Summary

Remcos malware has been operating since 2016. This RAT was originally promoted as genuine software for remote control of Microsoft Windows from XP onwards, and is frequently found in phishing attempts due to its capacity to completely infect an afflicted machine. Remcos malware attacks Windows systems and provides the attacker complete control over the machine.It is frequently distributed by malicious documents or archive files that contain scripts or executables. Remcos, like other RATs, offers the threat actor complete access over the infected PCs which allow them to record keystrokes, passwords, and other critical information. Remcos incorporates various obfuscation and anti-debugging techniques to evade detection. Regular updates of its features by its creators make this malware a challenging adversary.

Impact

- Breach of: Victim’s machine information (OS version, computer name, system type, product name, primary adapter).
- User information (user access, user profile, user name, user domain)
- Processor information (processor revision number, processor level, processor identifier, processor architecture)

Indicators of Compromise

MD5

- 424f139fef3d05a3d8f42eb102073c81
- 35cd4f06e75080637be9bd7b743bde67

SHA-256

- c67b333e520f360ef8defbcfe4441bd8fc8633f93d091c20009034d0e0aede6d
- 4d75269c71e85411f6c09ffa5b8be0a35e374aa316e8d645b7c04f852cae3cd8

SHA-1

- 7b69bb2175183c7568374fcbfa2bb2dc121d4d30
- 5d7006c2803bcb7131903517924 39c82c1645040

Remediation

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