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

- 3e974bea23a847c95bbab2f99b9dffa1

SHA-256

- 451ab9846f3c63a6b5f2e25ab5f58bb4180cf414062f52e280bd98eafea81963

SHA-1

- a24d39b29dc31600fa9b51567d7790c4c3e7a0e8

Remediation

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