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

- 59a1169aa2f5a65399e48682f0d5f17f

SHA-256

- 9f49bdbc65415452aa3b41ee52c745f66c2807a56a8052aff51aaee26e0fed21

SHA-1

- 3a258ef012a5e6f6148334158725e7a931216468

Remediation

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