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

- dbc66d92d35d9f3f8563a6d956740134
- ef24da63fc85b5740fe7b3c97d07b820
- 5a6b42a5e0c27c55ba79ce9effd31e57
- 38f2aeaec1fe65eec3273ee27a5facac
- 5c45b6d6395ab9a744a3145ebb211168

SHA-256

- d96a4429b78e6324c4da01ef3b54b26bc86a4b318fe09ff75d083dc200f5200e
- 7a099c2a919928941a4357553300018cd8847760df7b17c2e7bde1daef328305
- 01f5e461193a3adce502959e029cf52b8e9bf0a9cd1bf06c9088edddb4f643ab
- b6cbbd914e6466a18364e387503ecb099cb0b497807a85a1f5a8fb5e2df13213
- 6fd59cb70ad265325a16f30ccad2d0d4b938eda264f44b8133d21d0490c1aae2

SHA-1

- 1222c898ad325469acf7f224f496cc322037f7d7
- 2183daa057839b3f1eb72899f44d8d0ea4c3d2f7
- 926a17bfb8476ec6357ab444570ba444500a68bd
- 83cd77196c39b276dca9567af2ca29038f828594
- e9e0ec936680c4eaef88f983792f9ac887902649

Remediation

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