Unfolding Remcos RAT- 4.9.2 Pro

By Osama Ellahi

Published: 2024-08-10 · Archived: 2026-04-05 23:05:37 UTC

Malware Analysis of Remcos RAT: Exploitaion and Detection Explained

2 min read

Nov 23, 2023

Executive Summary

SHA256 hash:

> 2e5c4d023167875977767da513d8889f1fc09fb18fdadfd95c66a6a890b5ca3f

Remcos is a commercially available Remote Access Tool (RAT) marketed for legitimate use in surveillance and penetration testing. However, it has been leveraged in various unauthorized hacking initiatives. When deployed, Remcos establishes a backdoor, allowing comprehensive remote control over the affected system. The tool is a product of BreakingSecurity, a company specializing in cybersecurity solutions.

Hackers are getting smarter by using **tricks like hiding their code and adding fake code**, which makes it harder for security experts to figure out how their attacks work. They’re using things like image files and compression to

disguise their activities.

Get Osama Ellahi's stories in your inbox

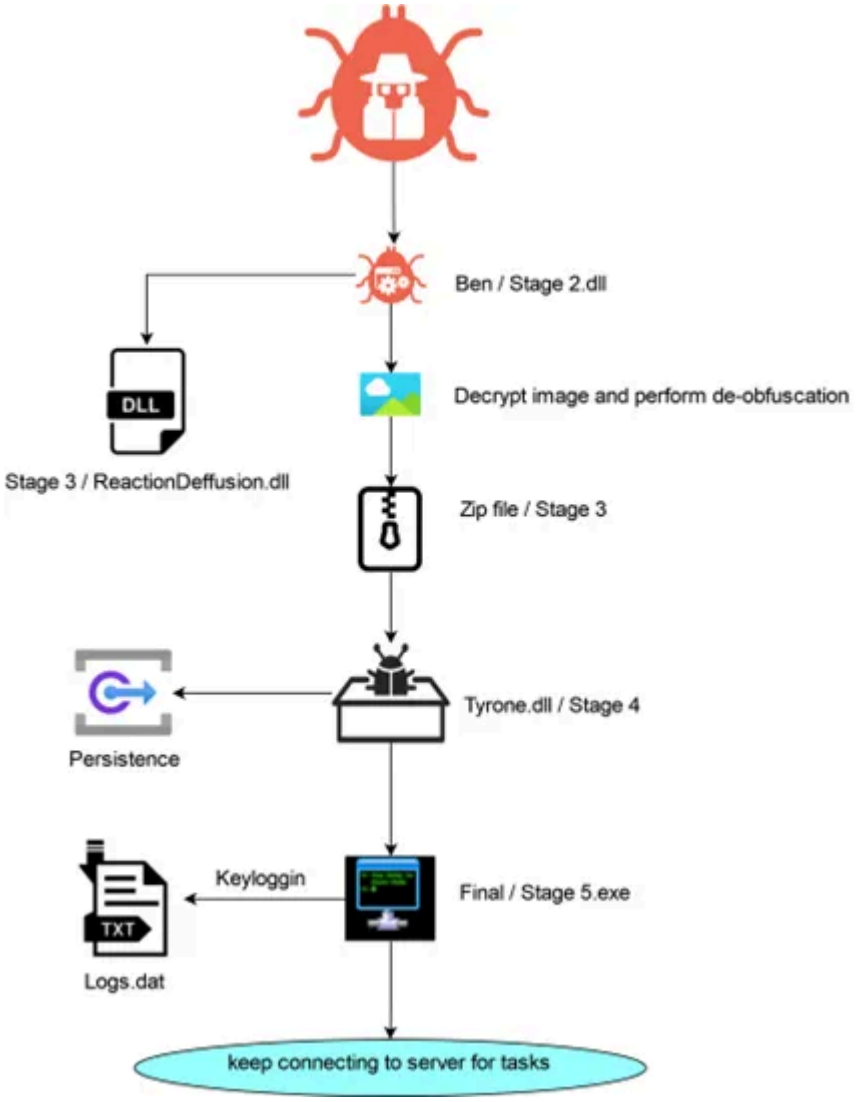
Join Medium for free to get updates from this writer.

Remember me for faster sign in

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

Remcos is an advanced remote access tool that breaks into computers using a series of hidden codes, starting with a malicious file which can be delivered from mail or dropper. It **cleverly disguises its next steps within an image file,** and then uses another DLL to make sure it stays on the computer even after it's restarted. Remcos can record keystrokes to steal passwords and other private information**, which it logs into a file**. It stays in contact with the hacker's server to send out this stolen information and to get new orders, allowing the hacker to keep a close watch and control over the infected computer.



Malware Composition

This composition of remcos consists of the following components:

> 2e5c4d023167875977767da513d8889f1fc09fb18fdadfd95c66a6a890b5ca3f
>
> Embedded_Remcos.exe

This blog is moved to personal blog website, to read full analysis on this RAT visit the following link. It will show how this was multi staged and how it perform malicious actions.

https://breachnova.com/blog.php?id=28
