Remcos RAT

Executive Summary

Remcos RAT, or remote access tool, is a legitimate application intended for use by administrators for remote access and maintenance. It has recently been used as part of attempted cyberattacks, leveraging COVID-related phishing themes to disguise it as part of the payload.

Overview and Functionality

Remcos is a Windows-based remote access tool (RAT), developed in both the C++ and Delphi languages, and maintained by a cybersecurity company called Breaking Security. As of May 2020, Remcos version 2.5.0 is available with limited features for free or as a full version offered under various licenses for a price ranging from €58.00 – €389.00. The most recent set of instructions for the use of version 2.4.7 can be found here. However, beginning in 2016, Remcos has been sold and exchanged in hacker forums and used for criminal purposes, often as part of a cyberattack. It's known to be distributed through phishing campaigns and delivered via malicious Microsoft Office documents and specifically macros, which help it bypass Microsoft Windows' User Account Control in order to execute the software at a high privilege level.

Remcos includes the following basic functionality:

- Remote Access – Remcos' primary functionality is remote access. It allows for remote access and administration of one or many systems over a local network or the Internet. This includes multithread, remote scripting and command line as well as service manager, remote proxy via the SOCKS5 protocol, point-and-click GUI access and other administrative functions.
- Operational Security and Reliability – Remcos utilizes a custom TCP-based protocol for encryption and a keepalive system and maintain security and availability of the connection with the remote section
- Surveillance, Data Collection and Monitoring – Remcos is capable of leveraging many functions of the remote system including tracking its location, deep inspection, file search and access to cameras and microphones.

There are two considerations when defending an information infrastructure from Remcos. First is the use of Remcos for unauthorized access to the enterprise network in question. This can be prevented with the implementation of generic security practices such as a hardened perimeter, defense in depth, security training for end users and patching along with continuous monitoring and a hunt capability. The second consideration is the prevention of Remcos use on an enterprise network for the purposes of further exploitation (either internally or externally). This can also be mitigated with the basic security practices previously noted, as well as implementation of the indicators of compromise at the end of this report.

There are some sources that characterize Remcos as malware because it is frequently part of criminal and other hostile activities in cyberspace. However, it appears that it is sold by its developers and intended to be used as a legitimate tool for authorized access and administration of systems, despite its abuse and misuse.

In early 2020, Remcos has been used in COVID-19 themed phishing campaigns with the apparent attempt to deploy the software and use it to steal credentials, control the target system remotely and even convert the system into a zombie as part of a botnet.

References

"Analysing Remcos RAT's Executable." KrabsOnSecurity, March 2, 2018. https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/.

"Analysis: New Remcos RAT Arrives Via Phishing Email." TrendLabs Security Intelligence Blog, August 16, 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/analysis-new-remcos-rat-arrives-via-phishing-email/.

"NJCCIC Threat Profile: REMCOS ." cyber.nj.gov, August 11, 2018. https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/remcos.

"Remcos Remote Control." Breaking Security. Accessed May 25, 2020. https://breaking-security.net/remcos/.

Bisson, David. "Attack Campaign Leveraged Coronavirus Theme to Deliver Remcos RAT." The State of Security,

"Remcos." Remcos, Software S0332 | MITRE ATT&CK®. Accessed May 25, 2020. https://attack.mitre.org/software/S0332/.

"Trojan.Remcos." Malwarebytes Labs. Accessed May 25, 2020. https://blog.malwarebytes.com/detections/trojan-remcos/.

Bacurio, Floser, and Joie Salvio. "REMCOS: A New RAT In The Wild," February 14, 2017. https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.html.

Brumaghin, Edmund, and Holger Unterbrink. "Picking Apart Remcos Botnet-In-A-Box." CISCO: Talos Blog, August 22, 2018. https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html.

Cimpanu, Catalin. "Microsoft Warns of Multiple Malspam Campaigns Carrying Malicious Disk Image Files." ZDNet. February 26, 2020. https://www.tripwire.com/state-of-security/security-data-protection/attack-campaign-leveraged-coronavirus-theme-to-deliver-remcos-rat/.

Frydrych, Melissa, Charlotte Hammond, and Ashkan Vila. "SBA Spoofed in COVID-19 Spam to Deliver Remcos RAT." Security Intelligence, April 27, 2020. https://securityintelligence.com/posts/sba-spoofed-in-covid-19-spam-to-deliver-remcos-rat/.

Greig, Jonathan. "Fake FedEx, DHL, and UPS Delivery Issues Used in COVID-19 Phishing Scams." TechRepublic. TechRepublic, May 1, 2020. https://www.techrepublic.com/article/fake-fedex-dhl-and-ups-delivery-issues-used-in-covid-19-phishing-scams/.
https://secrary.com/ReversingMalware/RemcosRAT/.

Klijnsma, Yonathan. "Espionage Campaign Spear Phishes Turkish Defense Contractors." RiskIQ, January 23, 2018. https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/.

O'Neill, Patrick Howell. "Remcos Software Is a Surveillance Tool Posing as Legitimate Software." CyberScoop. CyberScoop, August 22, 2018. https://www.cyberscoop.com/remcos-rat-surveillance-tool-talos-craig-williams/.

Stahie, Silviu. "Attackers Try to Deploy Remcos Malware with COVID-19-Related Messages." Security Boulevard, May 7, 2020. https://securityboulevard.com/2020/05/attackers-try-to-deploy-remcos-malware-with-covid-19-related-messages/.

Viotto. "Breaking Security." Home. Accessed May 25, 2020. https://breaking-security.net/.

"Remcos RAT." secrary[dot]com::blog. Accessed May 25, 2020.
ZDNet, May 4, 2020. https://www.zdnet.com/article/microsoft-warns-of-multiple-malspam-campaigns-carrying-malicious-disk-image-files/.

Appendix A: Indicators of Compromise

The following indicators will identify instances of Remcos. It's worth noting that the below list is not comprehensive and therefore not all versions, especially the most recent release, will be detected with the below IOCs.

Type	Indicator
Hash	8710e87642371c828453d59c8cc4edfe8906a5e8fdfbf2191137bf1bf22ecf81
Hash	fc0fa7c20adf0eaf0538cec14e37d52398a08d91ec105f33ea53919e7c70bb5a
Hash	ff64d7dc2f60fd79304639393cf70fed82e3eb1395d9f331ba123bd4e5f75923
SHA-256 Hash	cf624ccc3313f2cb5a55d3a3d7358b4bd59aa8de7c447cdb47b70e954ffa069b
SHA-256 Hash	1108ee1ba08b1d0f4031cda7e5f8ddffdc8883db758ca978a1806dae9aceffd1
SHA-256 Hash	6cf0a7a74395ee41f35eab1cb9bb6a31f66af237dbe063e97537d949abdc2ae9
SHA-256 Hash	abdcc6fbcd43d3c536d80127000ea469a4dc1c32ec819d32ab35ceb3070e0edd
SHA-256 Hash	af37a152c8605763868b29dbdfcc656514b815177982f40deb02315c83e68e2
MD5 Hash	4dfea420e3fcca712cf692cc3471bf8f
MD5 Hash	7096b341aafc041d91058d42045ab314
SHA1	3d39183fa5e6643fa449a950429e91457729c40c
SHA1	edbf6f6850cb089f86593207908e6dce0b12e576