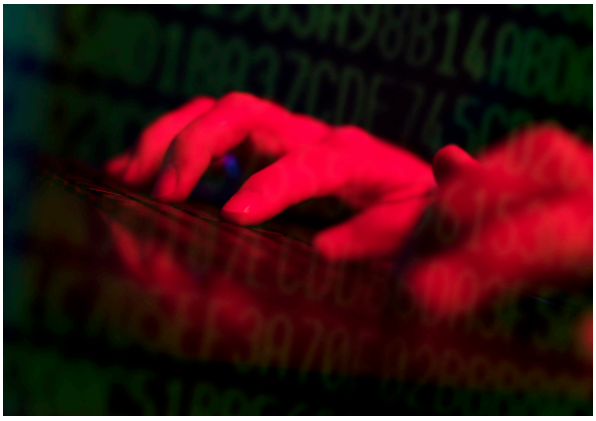
# Remcos RAT Malspam Campaign

*Author: Jeremy Ware*



## Overview

During the week of 9 November, we discovered a malspam campaign distributing the Remcos remote access trojan (RAT). The emails in this campaign carried malicious Microsoft Office documents that required the user to enable macros to execute the Remcos payload.

We previously reported on a similar Remcos campaign in July 2019. That campaign distributed Rich Text Format files (RTFs) and exploited the Microsoft Equation Editor remote code execution vulnerability.[1]

## Customer Impact

Remcos is short for remote control and surveillance, and is a tool created by the security company Breaking Security, based in Germany.[2] However, it has been abused by threat actors in numerous malspam campaigns since Breaking Security began selling it in 2016, with pricing starting at 58 Euros.[3,4,5]

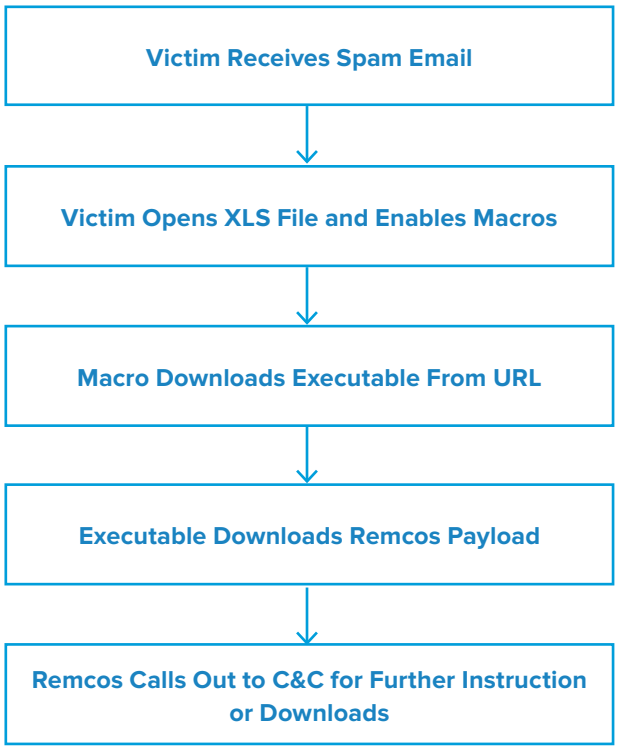
Remcos can control systems and cameras, act as a proxy for internet traffic, perform screen captures remotely, check browser cache and settings, and search files for password stores. It also includes a command-line interface (CLI) for full remote control.

## Campaign Analysis

The campaign we observed uses lures mentioning purchase orders or lists in the subject line *(Re: Item request list from Medigas SRL)* and file name *(Item List 09112020.xls)*. The emails all had the same subject line, file name and sender data, and the body of the message was empty.

## Attack Chain

When the victim opens the attached document, they are prompted to either enable macros or update the document. Esuerde.exe then begins to download, launches the Remcos payload (AddInProcess32.exe) and stores it in *C:\Users\admin\AppData\Local\Temp*. Next, the malware gathers data by checking stored credentials in files and reading browser cookies and cache settings. Remcos will continue to reach out to a command and control server (C&C) for further instructions or to receive additional payloads.




## Vulnerabilities & Mitigation

The Remcos RAT is spread via spam email and takes advantage of Microsoft Office vulnerabilities. Infoblox recommends the following actions to reduce the risk of infection:

- Keep Microsoft Office security patches up to date.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Do not open attachments from unfamiliar or unknown senders.
- Always be suspicious of unexpected emails, especially financial or delivery correspondence, documents or links.
- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Convert attachments to another format, for example, converting Microsoft Office documents to PDF documents can be an effective method of neutralizing malicious content.
- Never enable macros, and do not configure Microsoft Office to enable macros by default.

### Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--32
2. https://attack.mitre.org/software/S0332/
3. https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2
4. Given its usage in multiple malware campaigns, Cisco Talos conducted research on the German-registered company that builds and sells it - Breaking Security - and found them to be advertising on hacking websites. The software author claims many types of individuals visit such sites, not just hackers, and that he can shut down an instance of the tool if someone violates its terms and agreement.
5. As of 2018, the company also sold a crypter called Octopus Protector that was designed to allow software to bypass detection from anti-malware products by encrypting the software onto the computer's disk, thereby making it undetectable. https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html



Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com