Analysis: New Remcos RAT Arrives Via Phishing Email

By Aliakbar Zahravi (words)

Published: 2019-08-15 · Archived: 2026-04-05 21:56:18 UTC

In July, we came across a phishing email purporting to be a new order notification, which contains a malicious attachment that leads to the remote access tool Remcos RAT (detected by Trend Micro as BKDR_SOCMER.SM). This attack delivers Remcos using an AutoIt wrapper that incorporates various obfuscation and anti-debugging techniques to evade detection, which is a common method for distributing known malware.

Remcos RAT emerged in 2016 being peddled as a service in hacking forums — advertised, sold, and offered cracked on various sites and forums. The RAT appears to still be actively pushed by cybercriminals. In 2017, we reported spotting Remcos being deliveredopen on a new tab via a malicious PowerPoint slideshow, embedded with an exploit for CVE-2017-0199. Recently, the RAT has made its way to phishing emails.

The malicious actor behind the phishing email appears to use the email address rud-division@alkuhaimi[.]com (with a legitimate domain) and the subject "RE: NEW ORDER 573923". The email includes the malicious attachment using the ACE compressed file format, *Purchase order201900512.ace*, which has the loader/wrapper *Boom.exe*.

Analyzing the wrapper/loader

After converting the executable to AutoIt script, we found that the malicious code was obfuscated with multiple layers, possibly to evade detection and make it difficult for researchers to reverse. The top layer of obfuscation is shown in the following:

Figure 1. Obfuscated core functions

Figure 2. Functions used for deobfuscation

The main goal of the *Boom.exe* file is to achieve persistence, perform anti-analysis detection, and drop/execute Remcos RAT on an affected system. The above snippet code first calculates the value inside the array and then uses the ChrW() function to convert the Unicode number to the character.

Figure 3. Sample of string decoding

In some cases after decryption, the malware uses the AutoIt function called BinaryToString() to deobfuscate the next layer. The following code snippet demonstrates this behavior:

Figure 4. AutoIt Binary to String decoding

After deobfuscation, the AutoIt code can be seen containing large amounts of junk code meant to throw analysts off the track.

Figure 5. Sample of junk code

The malware then creates a copy of itself in *%AppData%\Roaming\appidapi\UevTemplateBaselineGenerator.exe* and loads the main payload (Remcos RAT) from its resource section. The malware then prepares the environment to execute the main payload. It achieves this by executing the following Shellcode (frenchy_shellcode version 1).

Figure 6. Frenchy_ShellCode_001

Figure 7. Executing and decoding Frenchy Shellcode

Figure 8. Frenchy Shellcode Mutant

Decoding and loading Remcos from resources

The DecData() function loads the data from its resource then reverses all data and replaces "%$=" with "/".

Figure 9. AutoIt decoding the main payload: Code + encoded resource (Remcos RAT)

Figure 10. AutoIt decoding the main payload: Code only

Then it uses the following to decode the base64 PE file, which is the main payload**:**

```
$a_call = DllCall("Crypt32.dll", "int", "CryptStringToBinary", "str", $sData, "int", 0, "int", 1, "ptr", 0,
"ptr", DllStructGetPtr($struct, 1), "ptr", 0, "ptr", 0)
```

Figure 11. Decoding Remcos from AutoIt

Loader features

Anti-VM

This AutoIt loader is capable of detecting a virtual machine environment by checking *vmtoolsd.exe* and *vbox.exe* in the list of running processes. However, it should be noted that this feature is not invoked in this sample.

Figure 12. AutoIt loader's Anti-VM

Bypass UAC

Depending on the Windows version, the malware uses either the built-in Event Viewer utility (eventvwr) or fodhelper to bypass the User Account Control (UAC).

Figure 13. UAC bypass

Anti-Debugging

If the loader detects *IsdebuggerPresent* in the system, it will display the message, "This is a third-party compiled AutoIt script." and exits the program.

Figure 14. AutoIt loader checks for a debugger

Examining the main payload, Remcos RAT

Originally marketed as a remote access tool that legitimately lets a user control a system remotely, Remcos RAT has since been used by cybercriminals. Once the RAT is executed, a perpetrator gains the ability to run remote commands on the user's system. In a past campaign, for instance, the tool was seen with a variety of capabilitiesopen on a new tab, which includes downloading and executing commands, logging keys, logging screens, and capturing audio and video using the microphone and webcam.

For the analysis of this payload, we looked into the sample Remcos Professional version 1.7.

Figure 15. Remcos version

Upon execution, depending on the configuration, the malware creates a copy of itself in *%AppData%\remcos\remcos.exe*, uses *install.bat* to execute *remcos.ex$* from the *%APPDATA%* directory, and finally deletes itself. It then creates the following Run key in the Registry to maintain persistence on the system.

Figure 16. Install.bat *dropped by Remcos*

Figure 17. Remcos RAT changes the Registry entry to maintain persistence

Figure 18. Reflected Remcos RAT change in the Registry

The malware retrieves the configuration called “SETTING” from its resource section.

Figure 19. Remcos loads the encrypted settings from its resources

The content of the configuration is encrypted using the RC4 algorithm, as seen below:

Figure 20. Remcos encrypted configuration

The following, on the other hand, is the RC4 algorithm used to decrypt the above configuration:

Figure 21. RC4 algorithm to decrypt the configuration

Figure 22. Decrypted configuration

The malware then creates the following mutex to mark its presence on the system:

Figure 23. Remcos RAT mutex

It then starts to collect system information such as username, computer name, Windows version, etc., which it sends to the command and control (C&C) server. The malware encrypts the collected data using the RC4 algorithm with the password “pass” from the configuration data.

Figure 24. Remcos collecting system information

Figure 25. Clear text data collected by Remcos, where “|cmd|” is the delimiter

Figure 26. Data is encrypted and sent to C&C server

Figure 27. Encrypted data

The following list shows some of the commands supported by the malware:

Commands	Description
Clipboarddata Getclipboard Setclipboard Emptyclipboard	Clipboard manager
deletefile	Delete file(s)
downloadfromurltofile	Download a file from specified URL and execute it on an infected system
execcom	Execute a shell command
filemgr	File manager
getproclist	List the running processes
initremscript	Execute remote script from C&C
keyinput	Keylogger
msgbox	Display a message box on an infected system
openaddress	Open a specified website

OSpower	Shutdown, restart, etc.
ping	Ping an infected system (used for network check)
prockill	Kill a specific process
regopened regcreatekey regeditval regdelkey regdelval regopen initregedit	Add, edit, rename, or delete registry values and keys
scrcap	Screen capture
sendfiledata	Upload data to C&C server
uninstall	Uninstall itself from an infected system

Table 1. Remcos RAT commands

The "consolecmd" command shown in the next figure, for instance, is used to execute shell commands on an infected system:

Figure 28. Some examples of Remcos RAT's commands

Figure 29. Browser/cookie-stealing feature

After analyzing this Remcos variant — its configuration data, communication mechanism, and functionalities — we saw that it had many similarities with its older variant (detected as Backdoor.Win32.Remcosrat.A). However, this particular campaign delivers Remcos using an AutoIt wrapper, which incorporates different obfuscation and anti-debugging techniques to avoid detection.

Prevention and Trend Micro Solutions

To defend against threats like Remcos RAT that use email-based attacks, we advise users to refrain from opening unsolicited emails — especially those with attachments — from unknown sources. Users should also exercise caution before clicking on URLs to avoid being infected with malware. For enterprises, if an anomaly is suspected in the system, report the activity to the network administrator immediately. We also recommend these best practices for added protection:

- Learn how to identify phishing emailsopen on a new tab and spot indicators of unwanted emails (i.e., misspellings, odd vocabulary)
- Update applications and systems regularly
- Apply whitelisting, block unused ports, and disable unused components
- Monitor traffic in the system for any suspicious behavior

Implementing security solutions with anti-spam filtering should weed out spam messages such as the one discussed here. The use of a multilayered solution such as Trend Micro™ Deep Discovery™open on a new tab will help provide detection, in-depth analysis, and proactive response to today's stealthy malware such as Remcos RAT, and targeted attacks in real-time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle. Trend Micro™ Deep Discovery™ Inspectoropen on a new tab prevents malware from reaching end users. For a more comprehensive security suite, organizations can consider the Trend Micro™ Cloud App Security™products solution, which employs machine learning (ML) in web reputation and URL dynamic analysis. The solution can also detect suspicious content in the message body and attachments as well as provide sandbox malware analysis and document exploit detection.

Indicators of Compromise (IoCs)

File Name and Email Address	Note	SHA-256 Hash	Trend Micro Pattern Det
Purchase order201900512.ace	Email attachment (ACE)	cf624ccc3313f2cb5a55d3a3d7358b4bd59aa8de7c447cdb47b70e954ffa069b	Backdoor.Win32.REMCO
Boom.exe (Loader/Wrapper)	ACE file content (Win32 EXE)	1108ee1ba08b1d0f4031cda7e5f8ddffdc8883db758ca978a1806dae9aceffd1	Backdoor.Win32.REMCO

remcos.ex$	Remcos RAT (Win32 EXE)	6cf0a7a74395ee41f35eab1cb9bb6a31f66af237dbe063e97537d949abdc2ae9	BKDR_SOCMER.SM
rud-division@alkuhaimi[.]com	Sender ID		
