New Variant of Remcos RAT Observed In the Wild

fortinet.com/blog/threat-research/new-variant-of-remcos-rat-observed-in-the-wild.html

October 21, 2019

FortiGuard Labs Breaking Threat Analysis

Recently, our LoneWolf Spampot Monitoring Systemcaptured several new spam samples. After a quick analysis, we identified it is a Remcos RAT campaign. The analysis in this blog focuses on the latest phishing email received by our system. However, we will include all IoCs related to this campaign at the end of this post.

Remcos RAT is a lightweight, fast and highly customizable Remote Administration Tool with a wide array of functionalities. In past years, it had been observed to act as an information collector, keylogger on a victim's device. Back to May 2018, we analyzed a variant of it, click here for more details.

From an online search, we can see that Remcos is being sold on a website. Figure 1 is a screenshot of that page.

Figure 1. REMCOS online order page

In this analysis, we would like to take you to an infected victim's device, where Remcos was downloaded, installed and executed, to see what this variant does.

Phishing Spam Sample Overview

The originating message spoofs the email address to appear coming from a valid domain. The attacker also performs a Social-Engineering attempt in the shape of a payment advisory email to persuade users to open the attached ZIP file with the included password.

Figure 2. Spam sample

The attached file is, in reality, a Windows Shortcut (.LNK). The malware author provided the ".TXT" extension as an attempt to obscure the real file extension once the file is extracted and viewed in the user's folder.

Figure 3. ZIP file asking for a password

When the user provides the given password and executes the attached file, it fetches a PowerShell script from an Internet address and executes it.

1st Stage Launcher & Downloader (payment-advice.txt.lnk)

Once the "payment-advice.txt.lnk" is executed by the victim user, it invokes the PowerShell interpreter (powershell.exe) with parameters that temporarily bypass the current PowerShell execution policy and then hides its window to ensure proper execution and hide its presence. The following picture shows the command argument passed to the PowerShell interpreter.

2nd Stage – Dropper (achremittance.ps1)

The downloaded PowerShell script "achremittance.ps1" is composed of six functions. The following table contains each function name along with its purpose.

Once the PowerShell script gets to execute, it performs the following actions (in sequential order):

1. Stores the string ".exe" in a variable encoded in base64, which is eventually decoded and stored in a variable

2. Generates the absolute path to the newly generated executable (C:\Users\Public\<random_name>.exe) by concatenating the previously received parameter (".exe" file extension), the system's public (%PUBLIC%) folder and a random string generated for the file name.

3. Decodes a base64 encoded executable file stored in a variable and then writes all bytes into the executable file

4. Performs a file extension check (either .exe OR .dll). This script targets the ".exe" file extension.

5. Starts the dropped file by calling the "Start-Process" PowerShell cmdlet

Figure 4. Base64 encoded Executable file

Executing the Dropped Remcos

Once the dropped EXE file executes, it first sleeps for a while (20 seconds) to confront sandboxing. Next, it relocates the EXE file to the %LocalAppdata% folder and renames it as "sysclient.exe" at the first run. It finally starts "sysclient.exe" after exiting the process.

The “sysclient.exe” starts a child process of itself with suspended state and then overwrites its code with extracted malicious code from the parent process. Finally, the malicious code executes in the child process, which is called process hollowing.

The figure below shows the process tree when first running the dropped Remcos, where the dropped EXE file is “etyq.exe”.

Figure 5. Process tree when first running the dropped Remcos

The “sysclient.exe” file was written in .NET Framework language, and the code was fully obfuscated, which creates a big challenge for analysts. It adds itself into the Auto-Start group of the system registry. In this way, Remcos can start automatically when the victim’s device restarts.

Figure 6 is a screenshot of when Remcos calls the function to write into the system registry.

Figure 6. Addition into Auto-Start group of system registry

Analysis of the Child Process

According to our analysis, the version of this variant is “2.5.0 Pro”, which is hardcoded in the malicious code, which just came out on September 20, 2019.

Like other previous versions, Remcos contains an encrypted resource named “SETTINGS”. After decrypting it, the data looks like Figure 7. It is an array where each item is split by hexadecimal “1E” that is highlighted with a red underscore.

Figure 7. Decrypted resource “SETTINGS”

This is the entire configuration data for Remcos. It contains many value fields, for example: C&C server host, license number, encryption seed for encrypting data, many RAT features’ default switch (“0” disable, “1” enable), and its home key name in system registry and so on.

Each value of the array could be fetched by calling a function with an index whenever it’s needed.

Remcos starts a keylogger by starting three threads. The log data is saved in a local file at “%Appdata%\remcos\logs.dat”. In previous version, the logs.dat file was encrypted. However, in this version, the logs.dat is not encrypted. The records are similar as the previous version, which is shown in Figure 8. When we opened Chrome, then entered a website and tested credential, you can see it recorded everything in Figure 8.

Figure 8. Example Keylogger logs.dat file content

Communicating with the C&C Server

The communication between Remcos and its C&C server is encrypted. Remcos uses RC4 to encrypt and decrypt traffic, as mentioned above that there is an encryption seed in the “SETTINGS” that is “Alibaba123” for this version, with which it can generate RC4 Key for traffic encryption and decryption.

It obtains the C&C server host from the decrypted “SETTINGS” array, whose index is 0. In Figure 7, you can see the host is “Sub[.]winkcaffe[.]waw[.]pl:10005”. Remcos puts all collected information from the victim’s device together in a buffer, which then gets encrypted and sent to the C&C server.

Figure 9. All collected data from victim’s device

Figure 9 is a screenshot taken when the buffer is about to be passed to the encryption function.

The entire data in the buffer is an array; each item is split by string “|cmd|”. This is the first packet sent to the C&C server, the buffer starts at memory address 0x1845959 and the buffer size is 0x253. The four-bytes at offset 0x0F is “4B 00 00 00” (0x4B for short), which is a control command number. In this packet, Remcos collected important information from the victim’s device, such as victim’s user name, location, Windows version, physical memory capacity, Remcos home name and version, keylogger log file full path, victim’s device running time, Remcos’s path, CPU information and so on.

The C&C server replied to this packet with the command control number “01 00 00 00” or 0x01 for short, which asks the client to collect the victim's topmost program title information and send back to the server.

The decrypted response packet is shown below:

The data structure is same as the one shown in Figure 9.

Control Commands that Remcos Supports

Besides the control command number 0x01 we detailed in the last section, Remcos supports many control commands to ask Remcos to perform various tasks on victim’s device. Because the attacker does not enable all the commands at server side, we find most of these command sub procedures in a control-command-handler function, which is a very large function. We manually and statically analyzed this function.

In this section, we show most of the control command numbers in a table as well as the features provided by them.

Cmd Number (hex)	Description

01	Obtain victim's topmost program title. GetForegroundWindow(), GetWindowTextW(), GetTickCount()
03	Collect all installed software information, including "Publisher", "DisplayVersion", "InstallLocation", "InstallDate", "UninstallString".
04	Download an executable file from given URL and run. URLDownloadToFileW(), ShellExecuteW()
05	Save data from packet into a local file and execute. WriteFile(), ShellExecuteW()
06	Collect all running processes information from infected device. CreateToolhelp32Snapshot(), GetModuleFileNameExW()
07	Kill a running process by given PID. TerminateProcess()
08	Enum all window and obtain titles. GetWindowTextW()
09	Close a window by given window handle. CloseWindow()
0A, 0B, AD	Show/hide a window by given window handle. ShowWindow()
0C	Obtain PID by given window handle. GetWindowThreadProcessId()
0D	Executes a given commandline command. _wsystem()
10	Could be handling jpeg stream and communicate with C&C server. SHCreateMemStream(), GdipSaveImageToStream()
11	Close socket used in command number 10. closesocket()
12	Collect the keyboard information. GetKeyboardLayoutName()
13	Start Online Keylogger.
14	Stop Online Keylogger.

15, 16	Read local file by given file path and send to C&C server. (for example the keylogger logs.dat file)
17	Delete a given file or directory. DeleteFileW(), RemoveDirectoryW()
18	Every five seconds, clear browser history like IE, Firefox, Chrome. To force victim enter when using browser, so that keylogger can record.
1B	Communicate with given C&C server to control victim's camera working.
1C	Close victime's camera. CloseCamera()
1D	Record victim's voice from audio input and send to C&C server. waveInOpen(), waveInStart()
1E	Stop recording victim's voice. waveInStop()
20	Delete a given file. DeleteFileW()
21	Exit Remcos process. exit()
22	Uninstall Remcos. It removes all Remcos files registry keys that Remcos created.
23	Execute a vbs script "restart.vbs" to restart Remcos. ShellExecuteW()
24, 25	Update Remcos. It downloads a file from given URL and exeutes it in a vbs script update.vbs. URLDownloadToFileW(), ShellExecuteW()
26	Show victim a warning message. MessageBoxW()
27	Log off the interactive user, shut down the system, or restarts the victim's system. ExitWindowsEx()
28	Obtain victim's system clipboard data. GetClipboardData()
29, 2A	Empty victim's system clipboard. EmptyClipboard()

2B	Create a share memory in Remcos address space and put data on it. CreateFileMappingA(), MapViewOfFileEx()
2C	Download data from a given URL and create a share memory in Remcos address space and put the download data on it. InternetReadFile(), CreateFileMappingA(), MapViewOfFileEx()
30	Connect to a given server and communicate with it. DisplayMessage(), GetMessage(), CloseChat()
31	Save a name value under its home key ("HKCU\Software\Remcos-CN7LIG\") in the system registry.
34	Perform service control (change service config, pause, stop, start) to specified service, and tell status to C&C server. ChangeServiceConfigW(), ControlService(), StartServiceW()
8F	Enumerate given directory file and send file names to C&C server.
92	Ues given file to set victim's desktop wallpaper style.
94	Modify window text by given window handle. SetWindowTextW()
95	Obtain real-time physical memory status, and report to C&C server. GlobalMemoryStatusEx()
98	Upload/download file to/from specified C&C server.
9E, A2	Play an alarm sound at victim's device.
A3	Control victim's device to play, stop audio.
AB	Elevate privilege is victim's logon user is not an administrator and tell C&C server of the result.
AC	Could show a pop menu to victim. TrackPopupMenu(),Shell_NotifyIconA()

Remcos supports starting a daemon program to protect itself from being killed. In previous version, it started a “svchost.exe” to do so. However, the attacker of this campaign did not enable the daemon program whose flag is set as “0” the in “SETTINGS” configuration.

Solution

The original downloading URL in the link file is rated as “**Malicious Websites**“ by the FortiGuard Web Filtering service.

The Shortcut (.lnk) file, downloaded PowerShell file and extracted exe file are all detected and blocked by the FortiGuard Antivirus service.

IOCs:

URLs

[C&C server]

Sub[.]winkcaffe[.]waw[.]pl:10005

Top[.]subaroone[.]waw[.]pl:5050

[URL of the PowerShell file]

hxxp[:]//globalpaymentportal[.]co/Admin/Logs/achremittance.ps1

hxxp[:]//transactionportal[.]co/Admin/Logs/transmission.ps1

Sample SHA-256

[Shortcut .lnk file]

914F19697F03015BB10AB5FBF96A8BC49F2F8D3C036235233B7CBB0F0E7A902C

0F47E91D77397032192F04FA35980793E400B3589BFAC2919ACC411340B903DE

DA2304FA78FAC37F2F093699BE418553A294FA9F394C1730482B3DDE66DE4CD5

3D03E32E7459ECFC94CA170CC07C54A87C75BACBCD92E5FA15657C46D474B59D

5626AC76C089BA66CC6B6294289A2BD04584F94F35D45198AA65F90E5F6E3EBB

[Downloaded PowerShell file]

55F4B78339A5172A24CA68FFB1D27EE1A791A6AA3821D6D5481B4B02BAED9B48

DF5DA147BCE2A9EDC6226E2EC6F4151AE1CF18C08EDF2C1568FBDD3099CE074A

[Extracted/Dropped EXE file]

55F4B78339A5172A24CA68FFB1D27EE1A791A6AA3821D6D5481B4B02BAED9B48

29FD2DD80F63AA43B34CD7EA2F7AEB9EA5259775233F29CB2205E0279495602D

Learn more about FortiGuard Labs and the FortiGuard Security Services portfolio.

Read about the FortiGuard Security Rating Service, which provides security audits and best practices.