Remcos RAT New TTPS – Detection & Response - Security Investigation

By BalaGanesh

Published: 2022-08-29 · Archived: 2026-04-06 00:31:06 UTC

Remcos is a remote access trojan – a malware used to take remote control over infected PCs.This trojan is created and sold to clients by a “business” called Breaking Security.

Although Breaking Security promises that the program is only available to those who intend to use it for legal purposes, in reality, Remcos RAT gives clients all the necessary features to launch potentially destructive attacks. The malware can be purchased with different cryptocurrencies.

Also Read: **Latest IOCs – Threat Actor URLs , IP’s & Malware Hashes**

It can also capture screenshots, record keystrokes on infected machines, and send the collected information to host servers.

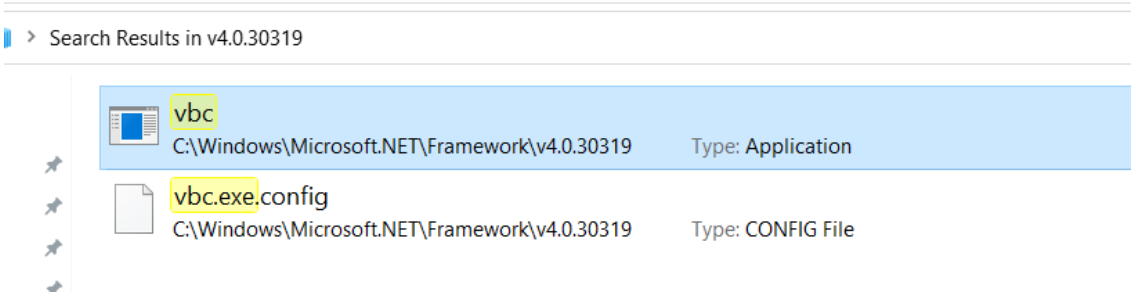
Remcos trojan can be delivered in different forms. Based on RAT’s analysis, it can be spread as an executable file with the name that should convince users to open it, or it pretends to be a Microsoft Word file to download and execute the main payload.

Recent distributions of malware work with both executable and Image files as payloads.

Also Read: **Process Injection Techniques used by Malware – Detection & Analysis**

Executable files as Payload

Infected machines leverage windows defaults such as Sctasks.exe which enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local and vbc.exe software component of the Microsoft .NET framework located at C:\Windows\Microsoft.NET\Framework64\v4.0.30319\vbc.exe to Compile attacker code on the system. Bypass defensive countermeasures.



Also Read: [What is a WAF? | Web Application Firewall Explained]

Image files as Payload

The second method uses ISO similar to **Qbot**. Infected machines will take **UAC bypass techniques** with **easinvoker.exe** and malicious Image files are mounted via \Device\CdRom and malware is getting executed.

event.code	rule.name	process.command_line	file.path	Target.process.thread.Ext.start_address_byte...
memory_signature	Windows.Trojan.Remcos	"C:\Windows\System32\iexpress.exe"	-	-
behavior	Remcos RAT Registry or File Modification	-	-	-
shellcode_thread	-	"C:\Windows\System32\iexpress.exe"	-	push ebp mov ebp, esp sub esp, 0x28 push ebx push esi push edi mov edi, 0x41ba38...
shellcode_thread	-	"F:\dhl AWB 3452778287 Shipping delivery notification,pdf.exe"	-	push ebp mov ebp, esp add esp, 0xfffffff8 mov eax, dword ptr [ebp+0x08] mov edx,...
malicious_file	-	"C:\Windows \System32\easinvoker.exe"	C:\Windows \System32\netutils.dll	-
behavior	UAC Bypass Attempt via Windows Directory Masquerading	"C:\Windows \System32\easinvoker.exe"	-	-
malicious_file	-	xcopy "netutils.dll" "C:\Windows \System32\" /K /D /H /Y	C:\Windows \System32\netutils.dll	-
malicious_file	-	"F:\dhl AWB 3452778287 Shipping delivery notification,pdf.exe"	C:\Users\Public\Libraries\Kxbbsknjt .exe	-
behavior	Suspicious String Value Written to Registry Run Key	-	-	-
behavior	Execution from a Downloaded ISO File	"F:\dhl AWB 3452778287 Shipping delivery notification,pdf.exe"	-	-

Source: https://twitter.com/SBousseaden

Also Read: [Soc Interview Questions and Answers – CYBER SECURITY ANALYST]

Indicators of Compromise

File hashes:

6d25e04e66cccb61648f34728af7c2f2

F331c18c3f685d245d40911d3bd20519

8cea687c5c02c9b71303c53dc2641f03

Domains:

http[:]//geoplugin.net/json.gp

falimore001[.]hopto.org

IP addresses:

178[.]237.33.50

194[.]147.140.29

Splunk:

```
source="WinEventLog:*" AND (((TargetFilename="*.iso" OR TargetFilename="*.img" OR TargetFilename="*.exe") AND (
```

Qradar:

```
SELECT UTF8(payload) from events where (LOGSOURCETYPENAME(devicetype)='Microsoft Windows Security Event Log' an
```

Elastic Query:

```
((file.path.text:(*.iso OR *.img OR *.exe) AND file.path.text:(*\\Users\*\\Downloads\* OR *\\Users\*\\Content.O
```

CarbonBlack:

```
((filemod_name:(*.iso OR *.img OR *.exe) AND filemod_name:(*\\Users\*\\Downloads\* OR *\\Users\*\\Content.Outlo
```

GrayLog:

```
((TargetFilename.keyword:(*.iso *.img *.exe) AND TargetFilename.keyword:(*\\Users\*\\Downloads\* *\\Users\*\\Co
```

Logpoint:

```
((TargetFilename IN ["*.iso", "*.img", "*.exe"] TargetFilename IN ["*\\Users\*\\Downloads\*", "*\\Users\*\\Cont
```

Microsoft Sentinel:

```
SecurityEvent | where (((TargetFilename endswith '.iso' or TargetFilename endswith '.img' or TargetFilename end
```

RSA Netwitness:

```
(((TargetFilename contains '.iso', '.img', '.exe') && (TargetFilename regex '.*\\Users\.*\\Downloads\.*', '.*\
```

Securonix:

```
index = archive AND (rg_functionality = "Microsoft Windows" AND (((rawevent CONTAINS ".iso" OR rawevent CONTAI
```

SumoLogic:

```
(_sourceCategory=*windows* AND ((((".iso" OR ".img" OR ".exe") AND (("\Users\" AND "\Downloads\") OR ("\Users\
```

Remcos RAT is a dangerous trojan available to attackers for a relatively low price. Despite its accessibility, it comes equipped with enough robust features to allow attackers to set up their own effective botnets. What's more, it is modernized with updates released nearly every month by the owner company.

Source: https://www.socinvestigation.com/remcos-rat-new-ttps-detection-response/