Remcos RAT New TTPS – Detection & Response

socinvestigation.com/remcos-rat-new-ttps-detection-response/

August 29, 2022

IOC

By

BalaGanesh

-

August 29, 2022

0

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.

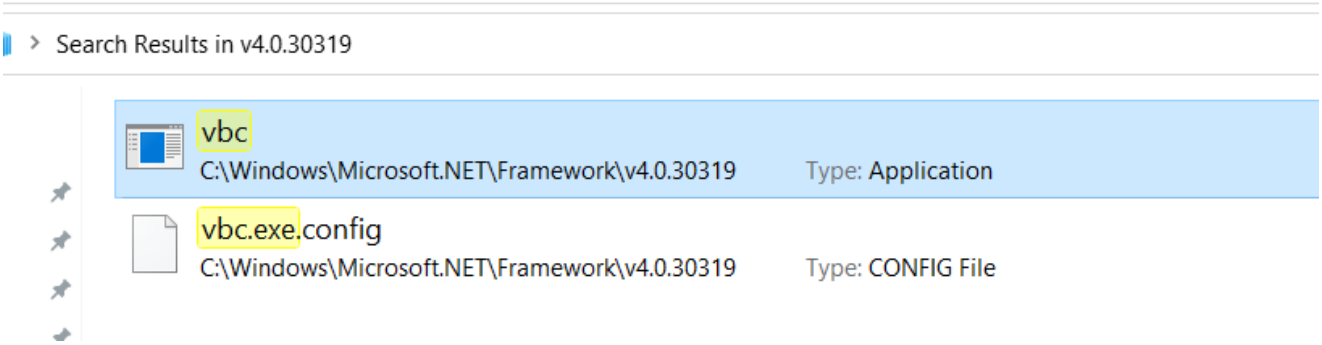
Remcos trojan can be delivered in different forms. Based on RAT's analysis, it can be spread as an executable file with the name that should convince users to open it, or it pretends to be a Microsoft Word file to download and execute the main payload.

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

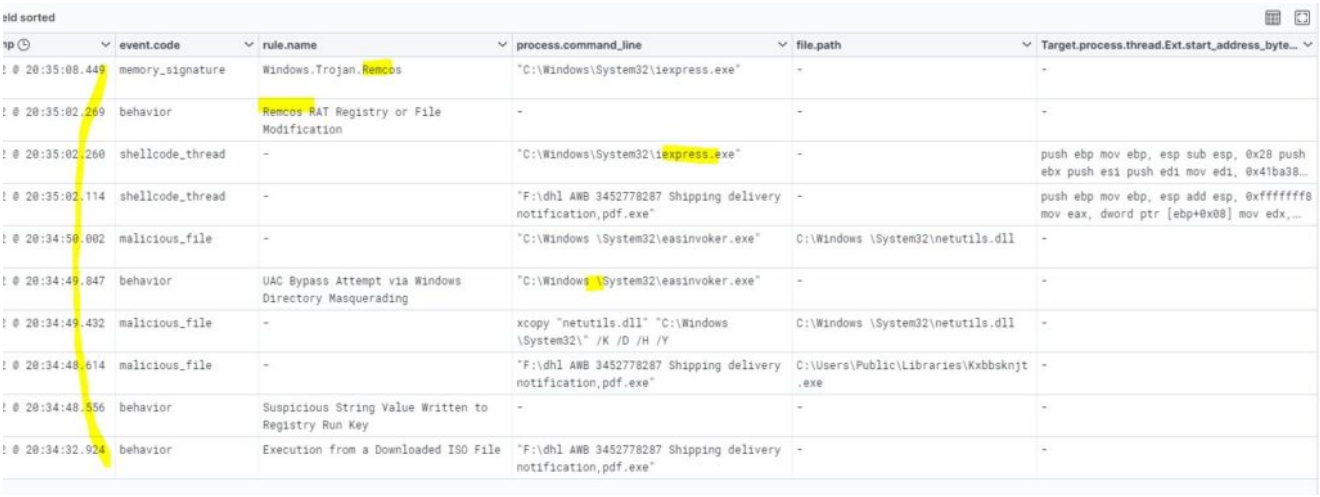
Infected machines leverage windows defaults such as Sctasks.exe which enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local and vbc.exe software component of the Microsoft .NET framework located at C:\Windows\Microsoft.NET\Framework64\v4.0.30319\vbc.exe to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



ld sorted					
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

Detection & Response

Splunk:

```
source="WinEventLog:*" AND (((TargetFilename="*.iso" OR TargetFilename="*.img" OR
TargetFilename="*.exe") AND (TargetFilename="*\\Users\*\\Downloads\*" OR
TargetFilename="*\\Users\*\\Content.Outlook\*" OR
TargetFilename="*\\Users\*\\AppData\\Local\\Temp\*") AND
TargetFilename="*:zone_identifier*" AND EventCode="4663" AND ObjectServer="Security"
AND ObjectType="File" AND ObjectName="\\Device\\CdRom*") OR (((TargetFilename="*.iso"
OR TargetFilename="*.img" OR TargetFilename="*.exe") AND (TargetFilename="*vbc.exe")
AND (CommandLine="*{path}*" OR CommandLine="*/target*" OR CommandLine="*\\temp\\*")
AND (TargetFilename="*schtasks.exe") AND (CommandLine="*/Create*" OR
CommandLine="*/TN*" OR CommandLine="*\\AppData\\Local\\Temp\\*")) OR
((TargetFilename="*easinvoker.exe") AND CommandLine="*netutils.dll*" AND
CommandLine="*xcopy*" AND CommandLine="*\\system32\\*")))
```

Qradar:

```
SELECT UTF8(payload) from events where (LOGSOURCETYPENAME(devicetype)='Microsoft
Windows Security Event Log' and (CATEGORYNAME(category) ILIKE 'File Created' or
CATEGORYNAME(category) ILIKE 'Successful File Modification')) and ((("Filename" ilike
'%.iso' or "Filename" ilike '%.img' or "Filename" ilike '%.exe') and ("Filename"
ilike '%\Users\%\Downloads\%' or "Filename" ilike '%\Users\%\Content.Outlook\%' or
"Filename" ilike '%\Users\%\AppData\Local\Temp\%') and "Filename" ilike
'%:zone_identifier%' and "EventID"='4663' and UTF8(payload) ILIKE 'Security' and
"ObjectType"='File' and "ObjectName" ilike '\Device\CdRom%') or ((("Filename" ilike
'%.iso' or "Filename" ilike '%.img' or "Filename" ilike '%.exe') and ("Filename"
ilike '%vbc.exe') and ("Process CommandLine" ilike '%{path}%' or "Process
CommandLine" ilike '%/target%' or "Process CommandLine" ilike '%\temp\%') and
("Filename" ilike '%schtasks.exe') and ("Process CommandLine" ilike '%/Create%' or
"Process CommandLine" ilike '%/TN%' or "Process CommandLine" ilike
'%\AppData\Local\Temp\%')) or (("Filename" ilike '%easinvoker.exe') and "Process
CommandLine" ilike '%netutils.dll%' and "Process CommandLine" ilike '%xcopy%' and
"Process CommandLine" ilike '%\system32\%')))
```

Elastic Query:

```
((file.path.text:(*.iso OR *.img OR *.exe) AND file.path.text:
(*\\Users\*\\Downloads\* OR *\\Users\*\\Content.Outlook\* OR
*\\Users\*\\AppData\\Local\\Temp\*) AND file.path.text:*\:zone_identifier* AND
winlog.event_id:"4663" AND winlog.event_data.ObjectServer:"Security" AND
winlog.event_data.ObjectType:"File" AND
winlog.event_data.ObjectName:\\Device\\CdRom*) OR ((file.path.text:(*.iso OR *.img OR
*.exe) AND file.path.text:*vbc.exe AND process.command_line.text:(*\{path\}* OR
*\/target* OR *\\temp\\*) AND file.path.text:*schtasks.exe AND
process.command_line.text:(*\/Create* OR *\/TN* OR *\\AppData\\Local\\Temp\\*)) OR
(file.path.text:*easinvoker.exe AND process.command_line.text:*netutils.dll* AND
process.command_line.text:*xcopy* AND process.command_line.text:*\\system32\\*)))
```

CarbonBlack:

```
((filemod_name:(*.iso OR *.img OR *.exe) AND filemod_name:(*\\Users\*\\Downloads\* OR
*\\Users\*\\Content.Outlook\* OR *\\Users\*\\AppData\\Local\\Temp\*) AND
filemod_name:*\:zone_identifier* AND EventID:"4663" AND ObjectServer:"Security" AND
ObjectType:"File" AND ObjectName:\\Device\\CdRom*) OR ((filemod_name:(*.iso OR *.img
OR *.exe) AND filemod_name:*vbc.exe AND process_cmdline:(*\{path\}* OR *\/target* OR
*\\temp\\*) AND filemod_name:*schtasks.exe AND process_cmdline:(*\/Create* OR *\/TN*
OR *\\AppData\\Local\\Temp\\*)) OR (filemod_name:*easinvoker.exe AND
process_cmdline:*netutils.dll* AND process_cmdline:*xcopy* AND
process_cmdline:*\\system32\\*)))
```

GrayLog:

```
((TargetFilename.keyword:(*.iso *.img *.exe) AND TargetFilename.keyword:
(*\\Users\*\\Downloads\* *\\Users\*\\Content.Outlook\*
*\\Users\*\\AppData\\Local\\Temp\*) AND TargetFilename.keyword:*\:zone_identifier*
AND EventID:"4663" AND ObjectServer:"Security" AND ObjectType:"File" AND
ObjectName.keyword:\\Device\\CdRom*) OR ((TargetFilename.keyword:(*.iso *.img *.exe)
AND TargetFilename.keyword:*vbc.exe AND CommandLine.keyword:(*\{path\}* *\/target*
*\\temp\\*) AND TargetFilename.keyword:*schtasks.exe AND CommandLine.keyword:
(*\/Create* *\/TN* *\\AppData\\Local\\Temp\\*)) OR
(TargetFilename.keyword:*easinvoker.exe AND CommandLine.keyword:*netutils.dll* AND
CommandLine.keyword:*xcopy* AND CommandLine.keyword:*\\system32\\*)))
```

Logpoint:

```
((TargetFilename IN ["*.iso", "*.img", "*.exe"] TargetFilename IN
["*\\Users\*\\Downloads\*", "*\\Users\*\\Content.Outlook\*",
"*\\Users\*\\AppData\\Local\\Temp\*"] TargetFilename="*:zone_identifier*"
event_id="4663" ObjectServer="Security" ObjectType="File"
ObjectName="\\Device\\CdRom*") OR ((TargetFilename IN ["*.iso", "*.img", "*.exe"]
TargetFilename IN "*vbc.exe" CommandLine IN ["*{path}*", "*/target*", "*\\temp\\*"]
TargetFilename IN "*schtasks.exe" CommandLine IN ["*/Create*", "*/TN*",
"*\\AppData\\Local\\Temp\\*"]) OR (TargetFilename IN "*easinvoker.exe"
CommandLine="*netutils.dll*" CommandLine="*xcopy*" CommandLine="*\\system32\\*")))
```

Microsoft Sentinel:

```
SecurityEvent | where (((TargetFilename endswith '.iso' or TargetFilename endswith
'.img' or TargetFilename endswith '.exe') and (TargetFilename matches regex '(?
i).*\Users\.*\Downloads\.*' or TargetFilename matches regex '(?
i).*\Users\.*\Content.Outlook\.*' or TargetFilename matches regex '(?
i).*\Users\.*\AppData\Local\Temp\.*') and TargetFilename contains ':zone_identifier'
and EventID == 4663 and ObjectServer =~ 'Security' and ObjectType =~ 'File' and
ObjectName startswith @'\Device\CdRom') or (((TargetFilename endswith '.iso' or
TargetFilename endswith '.img' or TargetFilename endswith '.exe') and (TargetFilename
endswith 'vbc.exe') and (CommandLine contains '{path}' or CommandLine contains
'/target' or CommandLine contains @'\temp\') and (TargetFilename endswith
'schtasks.exe') and (CommandLine contains '/Create' or CommandLine contains '/TN' or
CommandLine contains @'\AppData\Local\Temp\')) or ((TargetFilename endswith
'easinvoker.exe') and CommandLine contains 'netutils.dll' and CommandLine contains
'xcopy' and CommandLine contains @'\system32\')))
```

RSA Netwitness:

```
(((TargetFilename contains '.iso', '.img', '.exe') && (TargetFilename regex
'.*\\Users\.*\\Downloads\.*', '.*\\Users\.*\\Content\.Outlook\.*',
'.*\\Users\.*\\AppData\\Local\\Temp\.*') && (TargetFilename contains
':zone_identifier') && (reference.id='4663') && (ObjectServer='Security') &&
(ObjectType='File') && (ObjectName contains '\Device\CdRom')) || (((TargetFilename
contains '.iso', '.img', '.exe') && (TargetFilename contains 'vbc\.exe') &&
(CommandLine contains '{path}', '/target', '\temp\\\') && (TargetFilename contains
'schtasks\.exe') && (CommandLine contains '/Create', '/TN',
'\AppData\\Local\\Temp\\\')) || ((TargetFilename contains 'easinvoker\.exe') &&
(CommandLine contains 'netutils.dll') && (CommandLine contains 'xcopy') &&
(CommandLine contains 'system32\\'))))
```

Securonix:

```
index = archive AND (rg_functionality = "Microsoft Windows" AND (((rawevent CONTAINS
".iso" OR rawevent CONTAINS ".img" OR rawevent CONTAINS ".exe") AND (rawevent =
"*\Users*\Downloads*" OR rawevent = "*\Users*\Content.Outlook*" OR rawevent =
"*\Users*\AppData\Local\Temp*") AND rawevent CONTAINS ":zone_identifier" AND
@baseeventid = "4663" AND @destinationhostname = "Security" AND @customstring24 =
"File" AND @customstring56 STARTS WITH "\Device\CdRom") OR (((rawevent CONTAINS
".iso" OR rawevent CONTAINS ".img" OR rawevent CONTAINS ".exe") AND (rawevent
CONTAINS "vbc.exe") AND (@resourcecustomfield3 CONTAINS "{path}" OR
@resourcecustomfield3 CONTAINS "/target" OR @resourcecustomfield3 CONTAINS "\temp\")
AND (rawevent CONTAINS "schtasks.exe") AND (@resourcecustomfield3 CONTAINS "/Create"
OR @resourcecustomfield3 CONTAINS "/TN" OR @resourcecustomfield3 CONTAINS
"\AppData\Local\Temp\")) OR ((rawevent CONTAINS "easinvoker.exe") AND
@resourcecustomfield3 CONTAINS "netutils.dll" AND @resourcecustomfield3 CONTAINS
"xcopy" AND @resourcecustomfield3 CONTAINS "\system32\"))))
```

SumoLogic:

```
(_sourceCategory=*windows* AND ((((".iso" OR ".img" OR ".exe") AND (("\Users\" AND
"\Downloads\") OR ("\Users\" AND "\Content.Outlook\") OR ("\Users\" AND
"\AppData\Local\Temp\")) AND ":zone_identifier" AND EventID=4663 AND Security AND
File AND "\Device\CdRom") OR ((((".iso" OR ".img" OR ".exe") AND ("vbc.exe") AND
(CommandLine = "*{path}*" OR CommandLine = "*/target*" OR CommandLine = "*\temp\\*")
AND ("schtasks.exe") AND (CommandLine = "*/Create*" OR CommandLine = "*/TN*" OR
CommandLine = "*\AppData\Local\Temp\\*")) OR (("easinvoker.exe") AND
CommandLine="*netutils.dll*" AND CommandLine="*xcopy*" AND
CommandLine="*\system32\\*"))))))
```

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.

LEAVE A REPLY

Please enter your comment!

Please enter your name here

You have entered an incorrect email address!

Please enter your email address here