REMCOS RAT

Technical Analysis Report

Contents

Introduction

Marketed by Germany-based firm Breaking Security as legitimate software for remotely administering Windows systems, Remcos or Remote Control and Surveillance is now widely used by threat actors in numerous malicious campaigns. Remcos is an advanced remote access Trojan (RAT) that can be used to fully control and monitor any Windows computer from XP and later.

Information generally collected and sent to servers:

- Computer Information (OS version, computer name, system type, product name, gateway)
- User information (user access, user profile, username, user domain)
- Processor information (processor revision number, processor level, processor identifier, processor architecture)

General Behaviors

- Antivirus products are bypassed
- Provides persistence on the targeted machine
- Runs as legitimate process by injecting it into windows process
- Gains administrator privileges and disables user account control (UAC)

Summary

As soon as the malware runs on the computer, it creates and writes three data files, a .dll file. When the main process runs, it loads and calls eqvkptgalnkxk7m.dll. The eqvkptgalnkxk7m.dll file is analyzed and the three data files are written, and the same .exe file is run as a subprocess and the main process is closed.

The sub-process uses heaven's gate technique, so the process runs 64-bit code from time to time. It steals user information by making records and readings in the registry and creates a key for the application. The process creates a keylogger and records it in two ways, online and offline. Offline recordings are kept on the computer, while online recordings are transferred to the target server. The information transferred to the target server includes Google Chrome and FireFox cookies and databases where user passwords are kept.

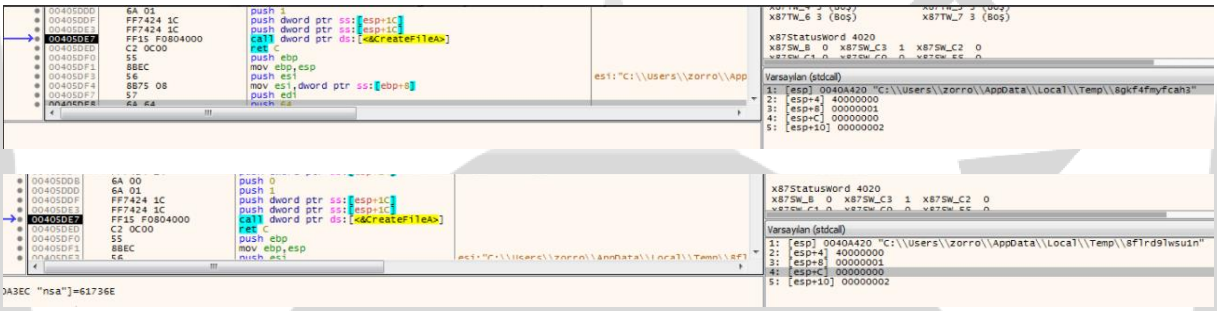
remcos.exe Analyses

MD5 hash: bab85d677cb634a42a890266e000fd79

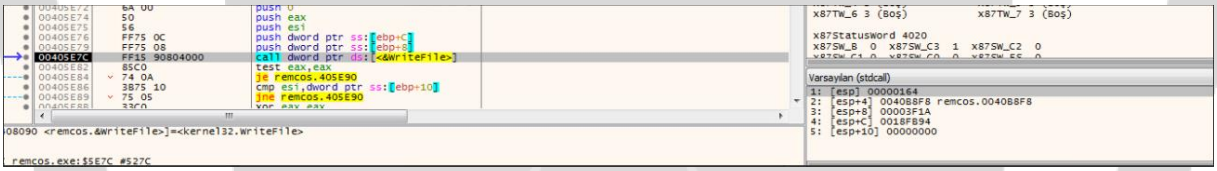
SHA1 hash: bcca157ab3520b1104411e86ea78f6a2efbb58ef

Sha256 hash: 0c0a9b0df586ceb12e6b76f86473a2bf2db7cb9d8101dc90217959e9d12d48b4

Creates a .tmp file named Random

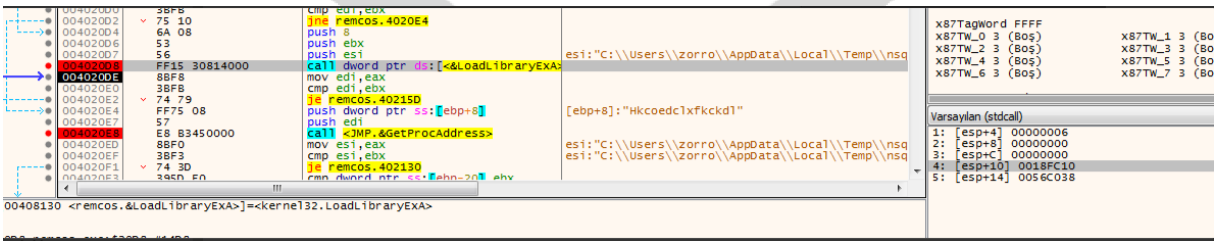


It creates 8gkf4fmyfcah3 and 8flrd9lwsu1n.



Writes the contents of the random .temp file.

Creates C:\Users\zorro\AppData\Local\Temp\nsu6D84.tmp\eqvkptgalnkxk7m.dll



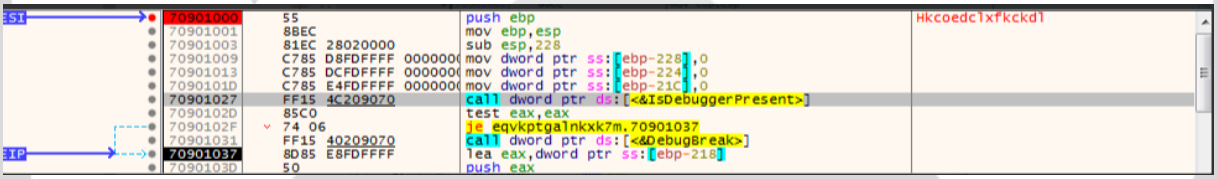
Loads and calls the export function of the eqvkptgalnkxk7m.dll file. When the eqvkptgalnkxk7m.dll file finishes its work, the process closes.

eqvkptgalnkxk7m.dll Analyses

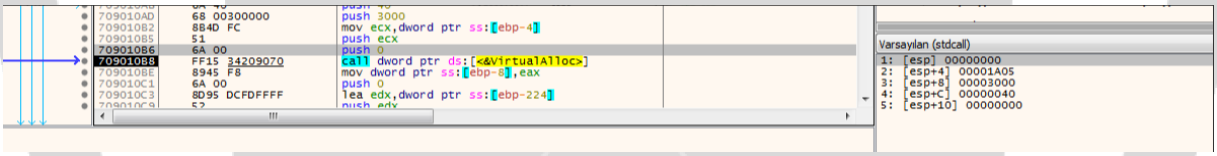
MD5: 8BC76CEF2080A1A62F8DF3A4E0CC8014

SHA1: 80B5675C93067E88B3F9848139090921283034 79

SHA-256: 84167EE64B337266442B7CB230DDF207203C7E53074CEF10F9755D50348B66B7



Checks if it is in debug with IsdebuggerPresnt.



Allocates virtual memory for the 8gkf4fmyfcah3 and 8flrd9lwsu1n file. It uses the AV bypass technique by loading the Kernel32.dll/Ntdll.dll files with the parsing algorithm (Figure 1) with the writing algorithm it uses (Figure 2).

Figure 1

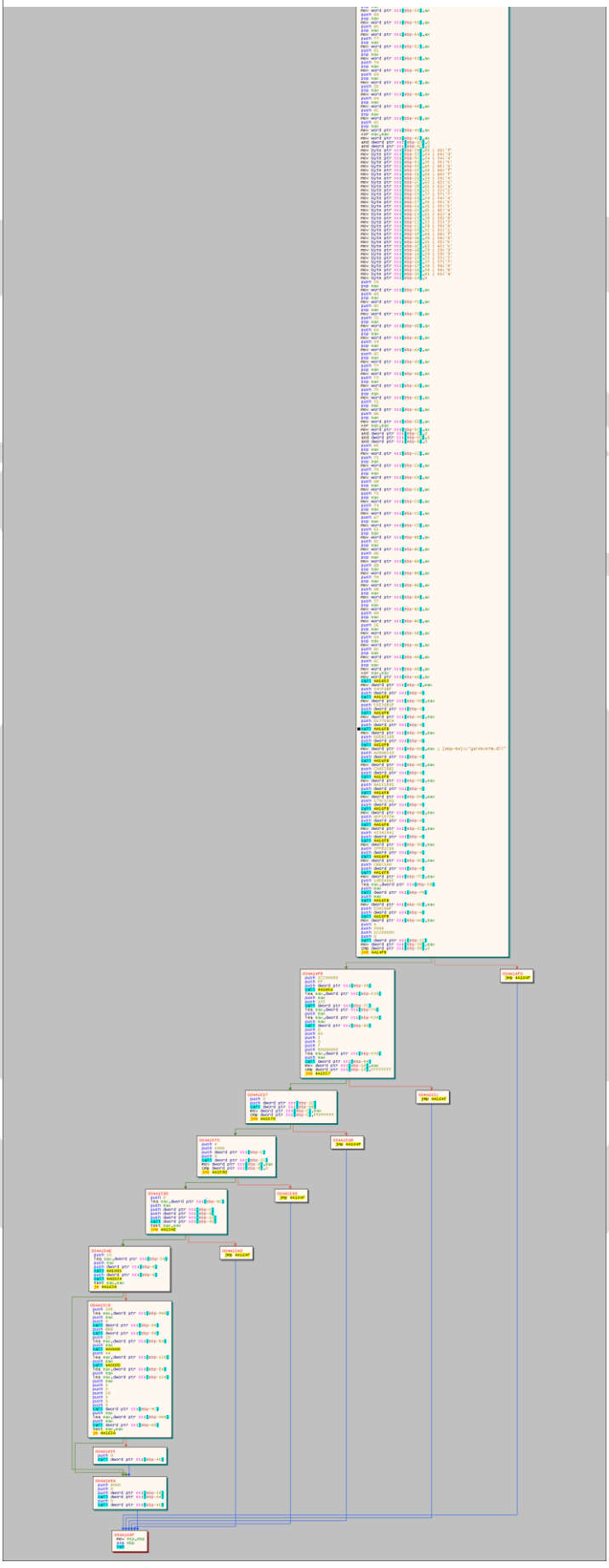
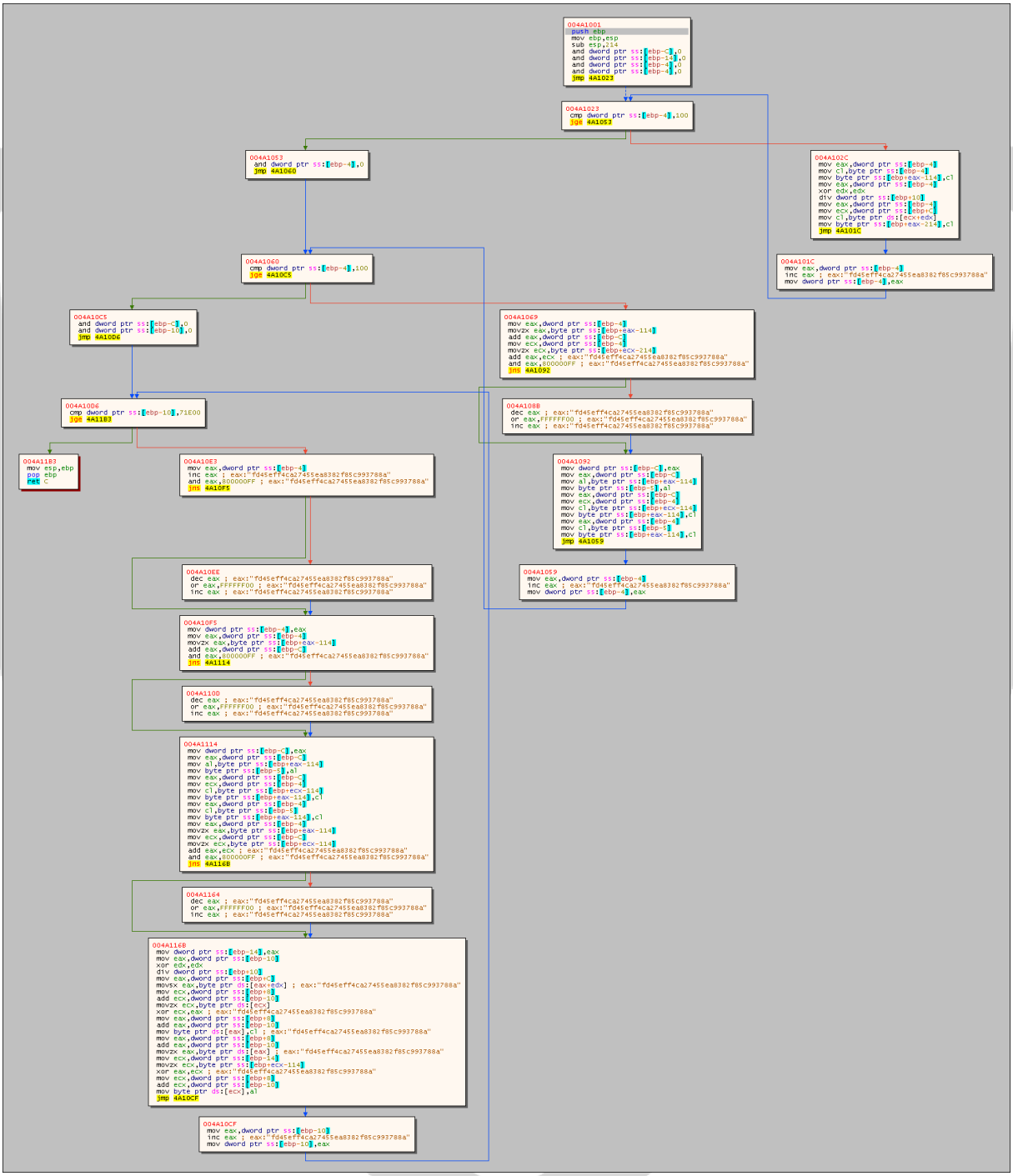
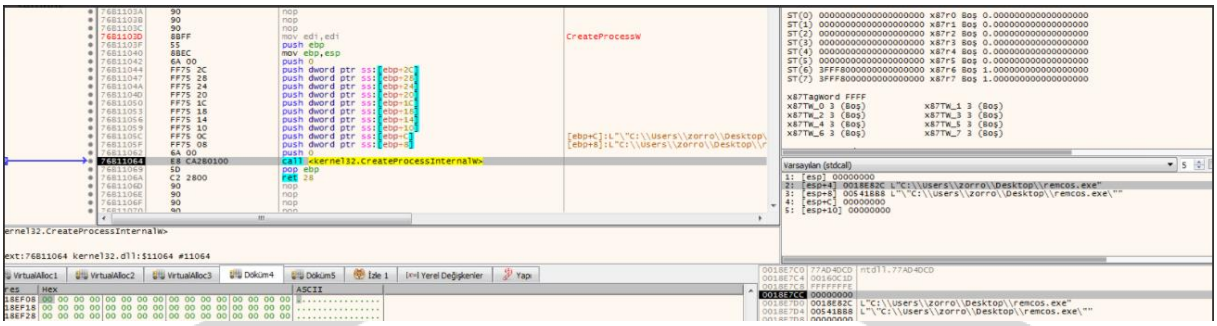
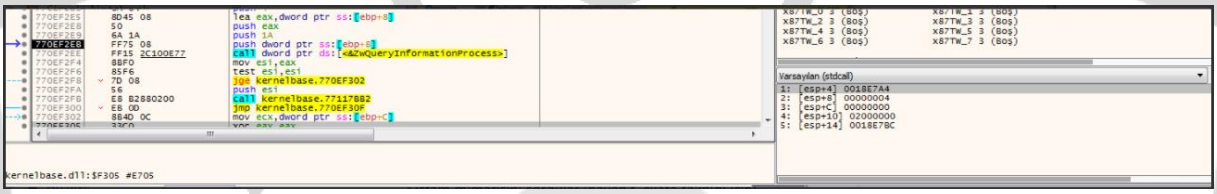


Figure 2

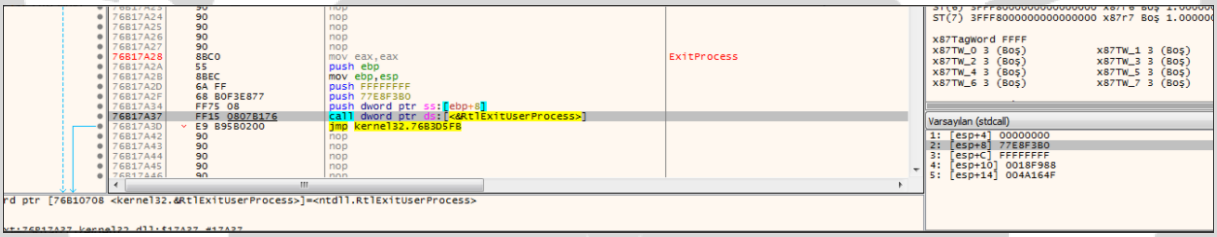

004A1001
push ebp
mov ebp,esp
sub esp,214
and dword ptr ss:[ebp-C],0
and dword ptr ss:[ebp-14],0
and dword ptr ss:[ebp-4],0
and dword ptr ss:[ebp-8],0
jmp 4A1023
004A1023
cmp dword ptr ss:[ebp-4],100
jge 4A1053
004A1053
and dword ptr ss:[ebp-4],0
jmp 4A1060
004A102C
mov eax,dword ptr ss:[ebp-4]
mov cl,byte ptr ss:[ebp-4]
mov byte ptr ss:[ebp+eax-114],cl
mov eax,dword ptr ss:[ebp-4]
xor edx,edx
div dword ptr ss:[ebp+10]
mov eax,dword ptr ss:[ebp-4]
mov ecx,dword ptr ss:[ebp-8]
mov cl,byte ptr ds:[ecx+edx]
mov byte ptr ss:[ebp+eax-214],cl
jmp 4A101C
004A1060
cmp dword ptr ss:[ebp-4],100
jge 4A10C5
004A101C
mov eax,dword ptr ss:[ebp-4]
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov dword ptr ss:[ebp-4],eax
004A10C5
and dword ptr ss:[ebp-C],0
and dword ptr ss:[ebp-10],0
jmp 4A10D6
004A10E9
mov eax,dword ptr ss:[ebp-4]
movzx eax,byte ptr ss:[ebp+eax-114]
add eax,dword ptr ss:[ebp-C]
mov ecx,dword ptr ss:[ebp-4]
movzx ecx,byte ptr ss:[ebp+ecx-214]
add eax,ecx ; eax:"fd45eff4ca27455ea8382f85c993788a"
and eax,800000FF ; eax:"fd45eff4ca27455ea8382f85c993788a"
jns 4A1092
004A10D6
cmp dword ptr ss:[ebp-10],71E00
jge 4A1183
004A108B
dec eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
or eax,FFFFFF00 ; eax:"fd45eff4ca27455ea8382f85c993788a"
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
004A1183
mov esp,ebp
pop ebp
ret C
004A10E3
mov eax,dword ptr ss:[ebp-4]
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
and eax,800000FF ; eax:"fd45eff4ca27455ea8382f85c993788a"
jns 4A10F5
004A1092
mov dword ptr ss:[ebp-C],eax
mov eax,dword ptr ss:[ebp-C]
mov al,byte ptr ss:[ebp+eax-114]
mov byte ptr ss:[ebp-5],al
mov eax,dword ptr ss:[ebp-C]
mov ecx,dword ptr ss:[ebp-4]
mov cl,byte ptr ss:[ebp+ecx-114]
mov byte ptr ss:[ebp+eax-114],cl
mov eax,dword ptr ss:[ebp-4]
mov cl,byte ptr ss:[ebp-5]
mov byte ptr ss:[ebp+eax-114],cl
jmp 4A1059
004A10EE
dec eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
or eax,FFFFFF00 ; eax:"fd45eff4ca27455ea8382f85c993788a"
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
004A1059
mov eax,dword ptr ss:[ebp-4]
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov dword ptr ss:[ebp-4],eax
004A10F5
mov dword ptr ss:[ebp-4],eax
mov eax,dword ptr ss:[ebp-4]
movzx eax,byte ptr ss:[ebp+eax-114]
add eax,dword ptr ss:[ebp-C]
and eax,800000FF ; eax:"fd45eff4ca27455ea8382f85c993788a"
jns 4A1114
004A1109
dec eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
or eax,FFFFFF00 ; eax:"fd45eff4ca27455ea8382f85c993788a"
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
004A1114
mov dword ptr ss:[ebp-C],eax
mov eax,dword ptr ss:[ebp-C]
mov al,byte ptr ss:[ebp+eax-114]
mov byte ptr ss:[ebp-5],al
mov eax,dword ptr ss:[ebp-C]
mov ecx,dword ptr ss:[ebp-4]
mov cl,byte ptr ss:[ebp+ecx-114]
mov byte ptr ss:[ebp+eax-114],cl
mov eax,dword ptr ss:[ebp-4]
mov cl,byte ptr ss:[ebp-5]
mov byte ptr ss:[ebp+eax-114],cl
mov eax,dword ptr ss:[ebp-4]
movzx eax,byte ptr ss:[ebp+eax-114]
mov ecx,dword ptr ss:[ebp-8]
movzx ecx,byte ptr ss:[ebp+ecx-114]
add eax,ecx ; eax:"fd45eff4ca27455ea8382f85c993788a"
and eax,800000FF ; eax:"fd45eff4ca27455ea8382f85c993788a"
jns 4A116B
004A1164
dec eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
or eax,FFFFFF00 ; eax:"fd45eff4ca27455ea8382f85c993788a"
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
004A116B
mov dword ptr ss:[ebp-14],eax
mov eax,dword ptr ss:[ebp-10]
xor edx,edx
div dword ptr ss:[ebp+10]
mov eax,dword ptr ss:[ebp-C]
movsx eax,byte ptr ds:[eax+edx] ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov ecx,dword ptr ss:[ebp-8]
add ecx,dword ptr ss:[ebp-10]
movzx ecx,byte ptr ds:[ecx]
xor ecx,eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov eax,dword ptr ss:[ebp-8]
add eax,dword ptr ss:[ebp-10]
mov byte ptr ds:[eax],cl ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov eax,dword ptr ss:[ebp-8]
add eax,dword ptr ss:[ebp-10]
movzx eax,byte ptr ds:[eax] ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov ecx,dword ptr ss:[ebp-14]
movzx ecx,byte ptr ss:[ebp+ecx-114]
xor eax,ecx ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov ecx,dword ptr ss:[ebp-8]
add ecx,dword ptr ss:[ebp-10]
mov byte ptr ds:[ecx],al
jmp 4A10CF
004A10CF
mov eax,dword ptr ss:[ebp-10]
inc eax ; eax:"fd45eff4ca27455ea8382f85c993788a"
mov dword ptr ss:[ebp-10],eax



After these processes, the application starts a suspend process under itself.



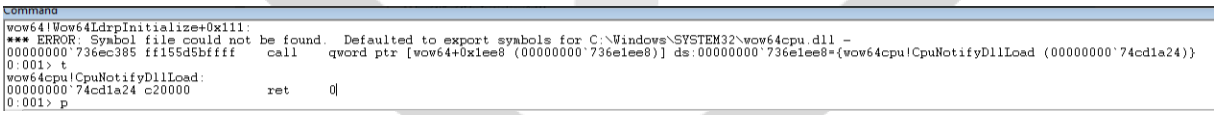
Queries the system architecture after the suspend process started



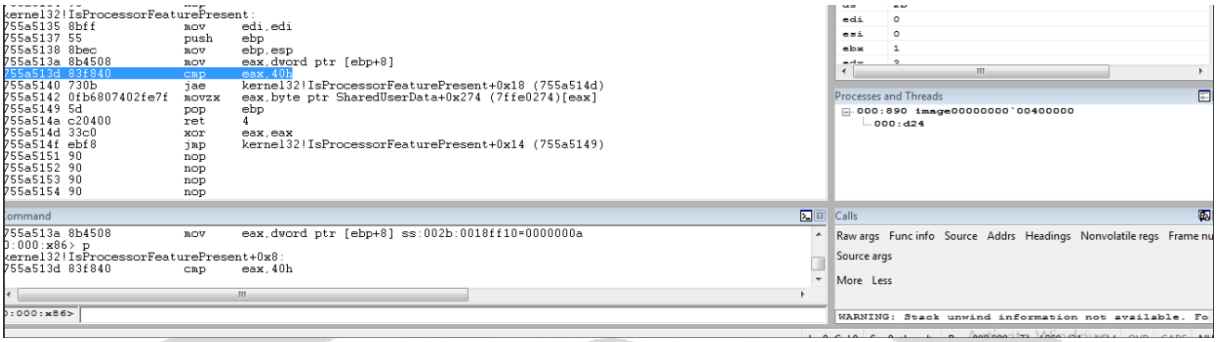
After the child process runs, the main exe closes.

Alt Süreç: remcos.exe Analyses

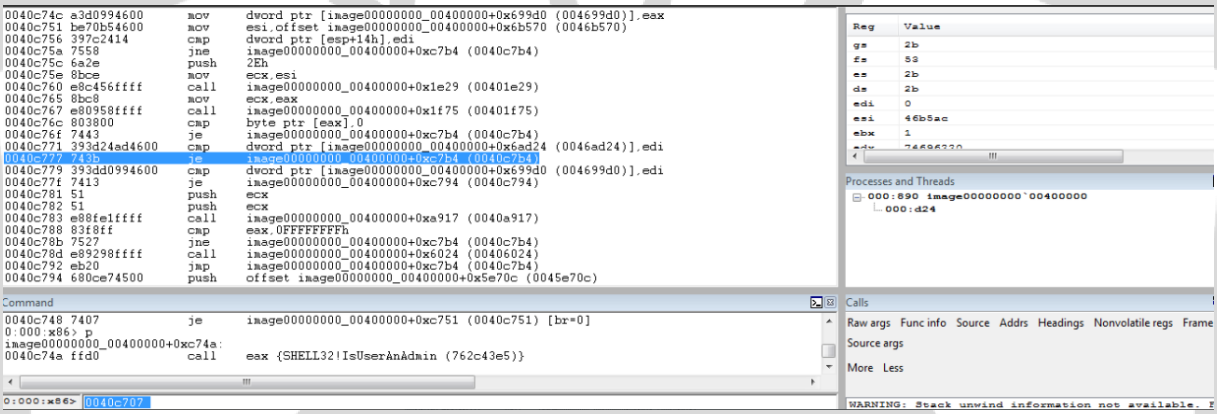
The remcos.exe run as a subprocess used heaven's gate technique with hooking in <ntdll.ZWContinue>.



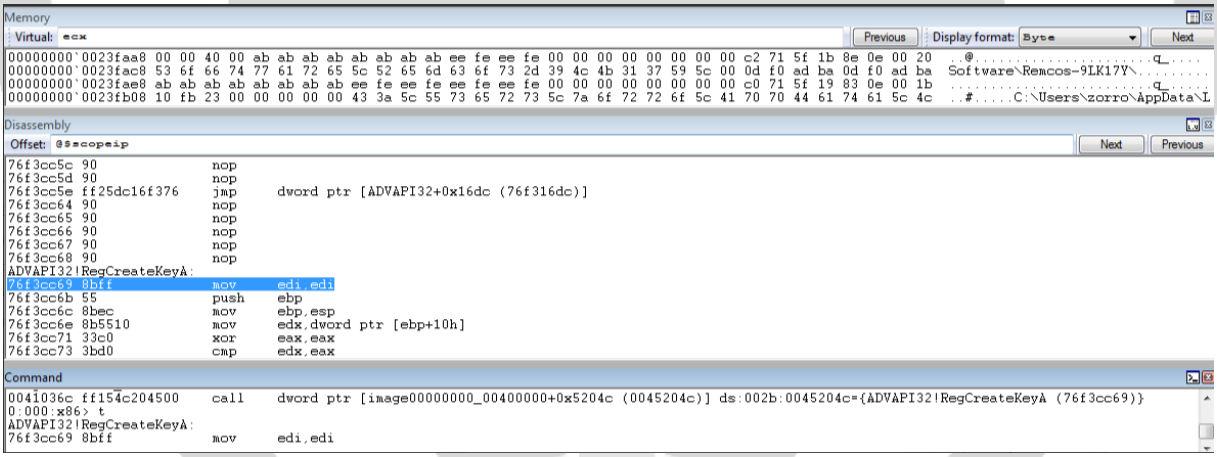
Loads the x64 system libraries.



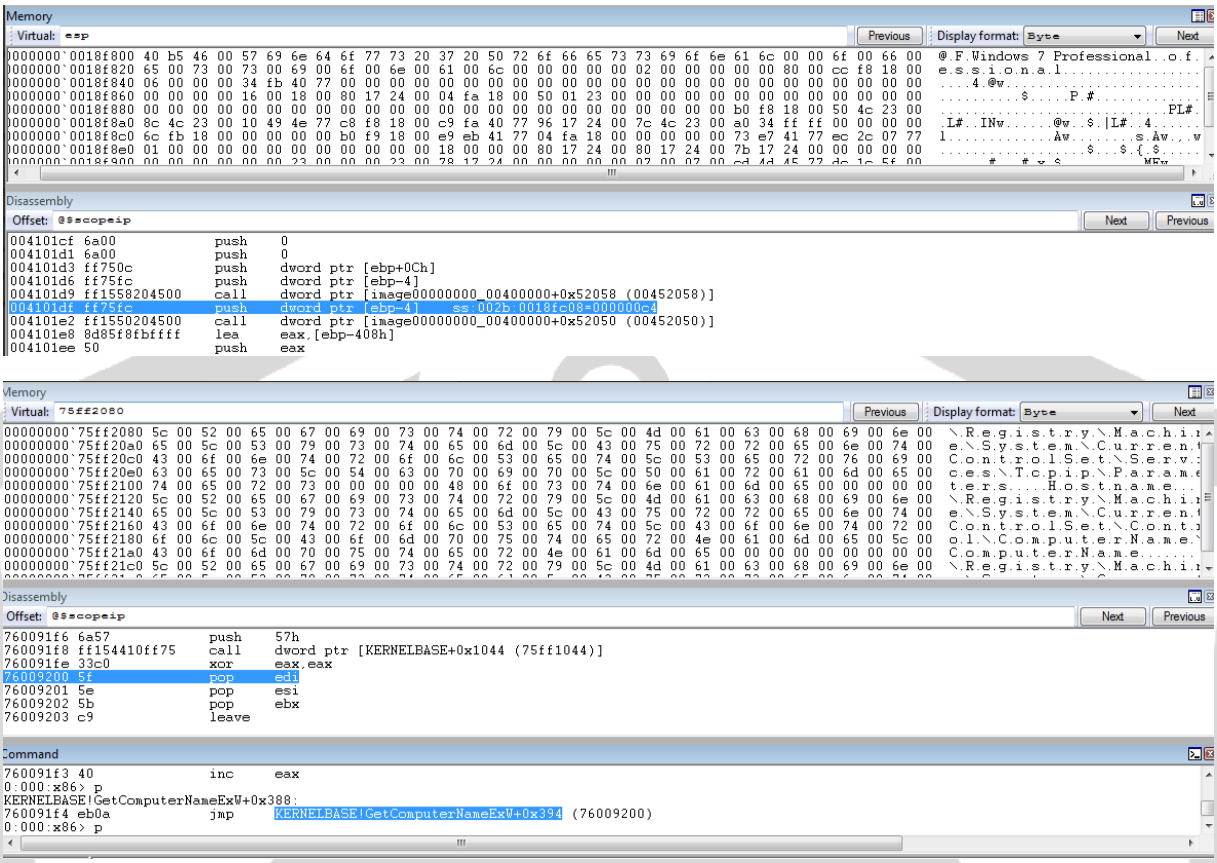
Tried to detect debugging with IsDebuggerFeaturePresent api.



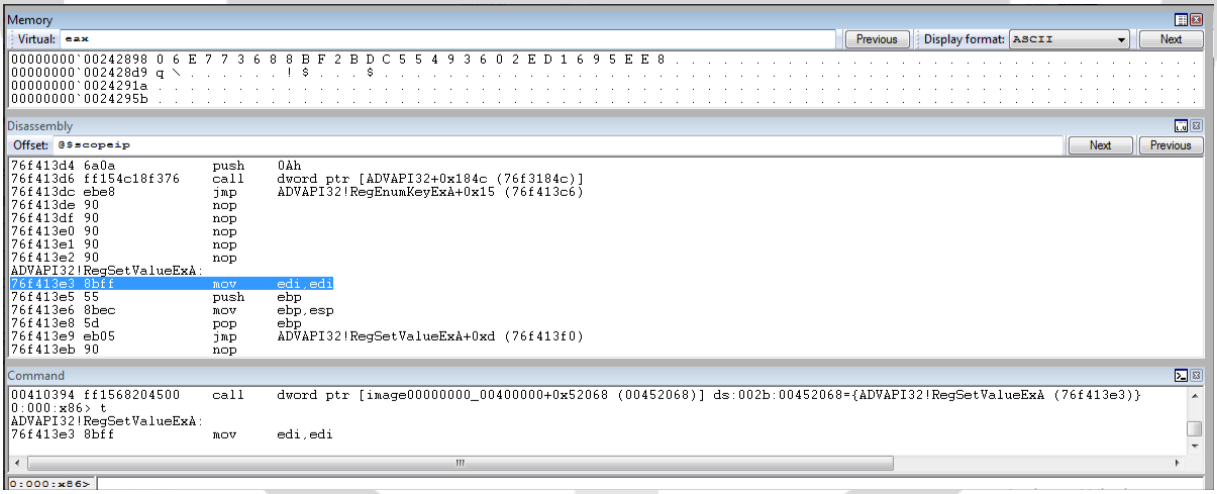
Queries whether the user is an administrator or not.



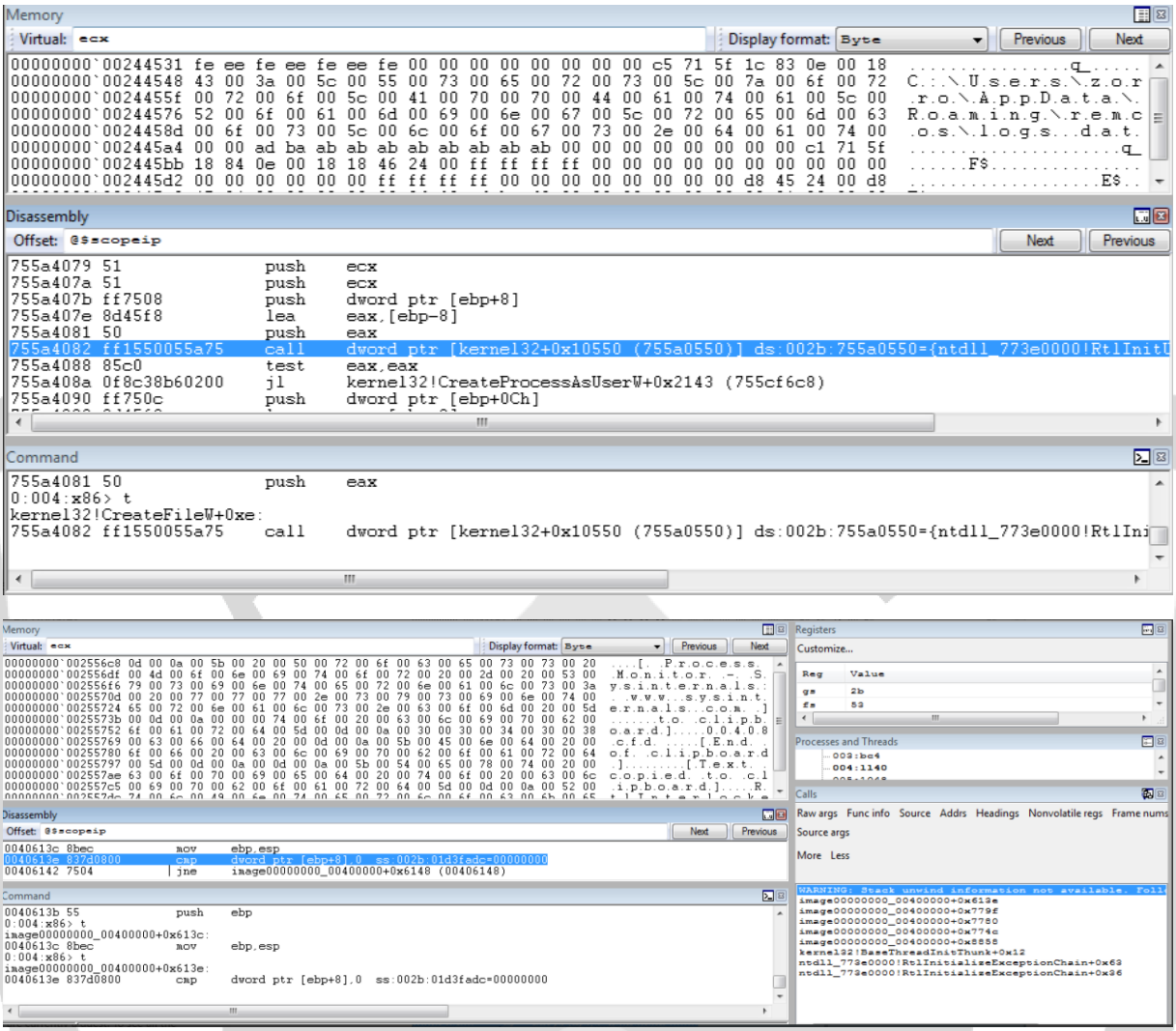
Creates key Software\Remcos-9LK17Y



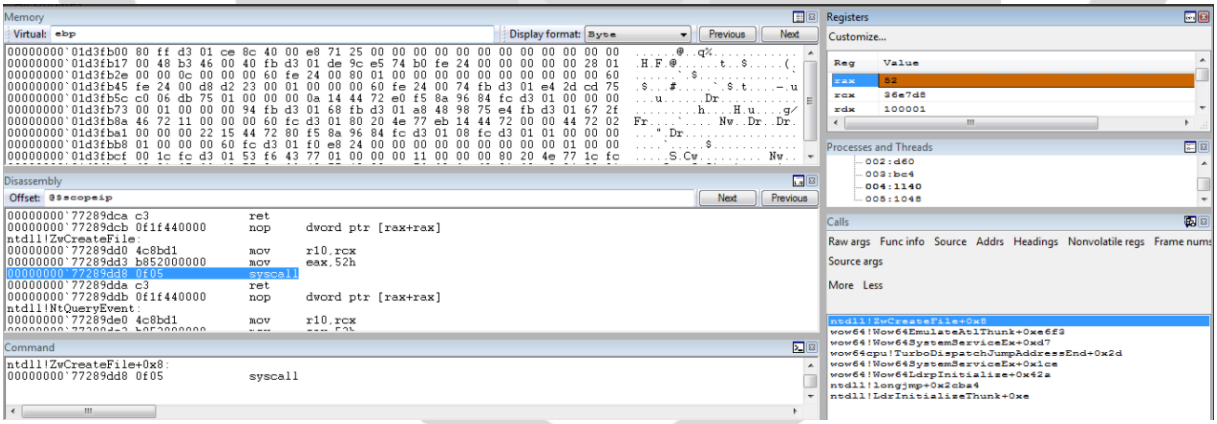
Retrieves the product name and information.



Creates exepath and license record for HKU Remcos key.



Creates a log.dat file and pulls what will be written to the file.



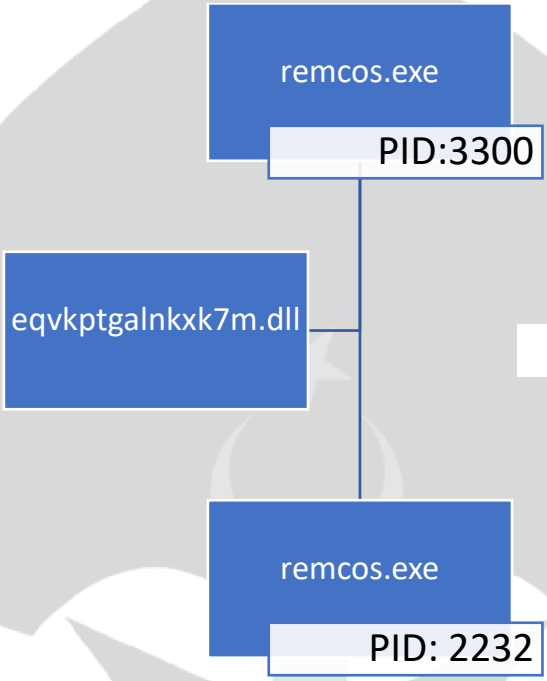
With syscall, it makes a system call to the NtOpenSection api and creates the log.dat file.

Network Analyses

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.4	23.19.227.243	TCP	66	49736 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	2.998975	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49736 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	8.999669	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49736 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	22.033375	192.168.2.4	23.19.227.243	TCP	66	49751 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	25.047821	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49751 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	31.048259	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49751 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	44.081608	192.168.2.4	23.19.227.243	TCP	66	49758 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	47.080906	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49758 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	53.081751	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49758 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	66.114794	192.168.2.4	23.19.227.243	TCP	66	49768 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	69.129576	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49768 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	75.130104	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49768 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	88.149004	192.168.2.4	23.19.227.243	TCP	66	49769 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	91.147146	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49769 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	97.147725	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49769 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	110.166344	192.168.2.4	23.19.227.243	TCP	66	49772 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	113.180382	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49772 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	119.180890	192.168.2.4	23.19.227.243	TCP	66	[TCP Retransmission] 49772 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

It sends a TCP request to the specified address (23.19.227.243), but there is no active server yet.

Behaviour Graph



Created Files

1. 8flrd9lwsu1n
2. 8gkf4fmyfcah3

8flrd9lwsu1n

MD5: A114322491F0917F2DC0BEE0A10E0088

SHA1: 41D03DE78CD844A167F0F4C5459FABC96FC66A2C

SHA-256: 7A90F1D6B97352E9727A9D440B0692A00F3857FF89ED406558C27655D0E9B0D3

8gkf4fmyfcah3

MD5: 6E170AC18CCCE60E6E19EB3E3E3A87A0

SHA1: B66BF0E08EC51FDA7628F9CA428B0819A3571FE6

SHA-256: EC9A222C20B4EBF39DA394D153B3825FDE3B6C70E418FC2607D287894255FC83

Protection Methods

Up-to-date anti-virus software should be used.

The operating system should be kept up to date.

File and printer sharing services should be disabled. If these services are required, strong passwords or Active Directory authentication should be used.

Multi-factor authentication should be used.

Users' permissions to install and run unwanted software applications should be restricted. Users should not be added to the local administrators group unless necessary.

Care should be taken when opening e-mail attachments.

Unnecessary services should be disabled on agency workstations and servers.

Suspicious email attachments should be scanned or removed.

Users' web browsing habits should be monitored and access to sites with negative content should be restricted.

Care should be taken when using removable media (eg USB flash drives, external drives, CDs).

All software downloaded from the internet should be scanned before running.

Awareness of the latest threats should be maintained and appropriate access control lists should be implemented.

Remcos.exe Yara Rule

```
import "hash"

rule REMCOS

{

   meta:

      author = "Bilal"

      first_date = "17.07.2021"

      report_date = "25.07.2021"

      description = "REMCOS"

      file_name = "remcos.exe"


   strings:

      $text_a = "nsq5333.tmp"

      $text_b = "8gkf4fmyfcah3"

      $text_c = "8flrd9lwsu1n"

      $text_d = "eqvkptgalnkxk7m.dll"

      $text_e = "Software\Remcos-9LK17Y"

      $text_licence = "06E773688BF2BDC55493602ED1695EE8"

      $text_f = "Log.dat"

      $text_ip = "23.19.227.243"


   condition:

      hash.md5(0, filesize) == "bab85d677cb634a42a890266e000fd79" or all

      text_a[0,2] and text_a[7,10]


}
```

eqvkptgalnkxk7m.dll Yara Rule

```
import "hash"
rule REMCOS
{
   meta:
      author = "Bilal"
      first_date = "17.07.2021"
      report_date = "25.07.2021"
      description = "REMCOS"
      file_name = "eqvkptgalnkxk7m.dll"

   strings:
      $text_a = "8gkf4fmyfcah3"
      $text_b = "8flrd9lwsu1n"

   condition:
      hash.md5(0, filesize) == "8BC76CEF2080A1A62F8DF3A4E0CC8014" or all
}
```

Prepared BY

BİLAL BAKARTEPE

linkedin.com/in/bilal-bakartepe