Necurs Revisited!

Necurs is family of malware components that can provide backdoor access to infected computer, can download and install additional malware. It was announced as prevalent threat by Microsoft Malware Protection Center in Nov 2012 when it infected 83000+ machines.

It is basically a backdoor and Downloader but also has a driver agent for persistence which blocks security tools from running. There were various blogs written on it but they mostly focused on driver agent, Downloader/Backdoor component was not covered in much detail.

This family is not seen in wild these but i have been working on Necurs family for some time. So i will share my analysis of Downloader/Backdoor part of Necurs in this blog post.

Objective of this Blog Post

Overview of features

Some feature of Necurs Trojan:

Contains encrypted configuration file in last section

- Can infect both 32-bit and 64-bit Systems. Checks and drops appropriate driver agent.
- Uses a special format for its commands to make detection and analysis of commands difficult.
- Bypasses KPP/PatchGuard using backdoor left by Microsoft for developers to test their drivers known as TESTSIGNING mode.
- Inject Dead Bytes in running processes.
- Create Service
- Connect to Remote locations and may download additional malware
- May Disable firewall
- Contains a troubleshooting and Error reporting module
- Encrypts network traffic

so lets start with analysis of important function of Necurs:

SHA256: 578a8fee2aeb18cd04b028940f73f12c55ca9df7b43764de8a7c968ce0ff4ec4

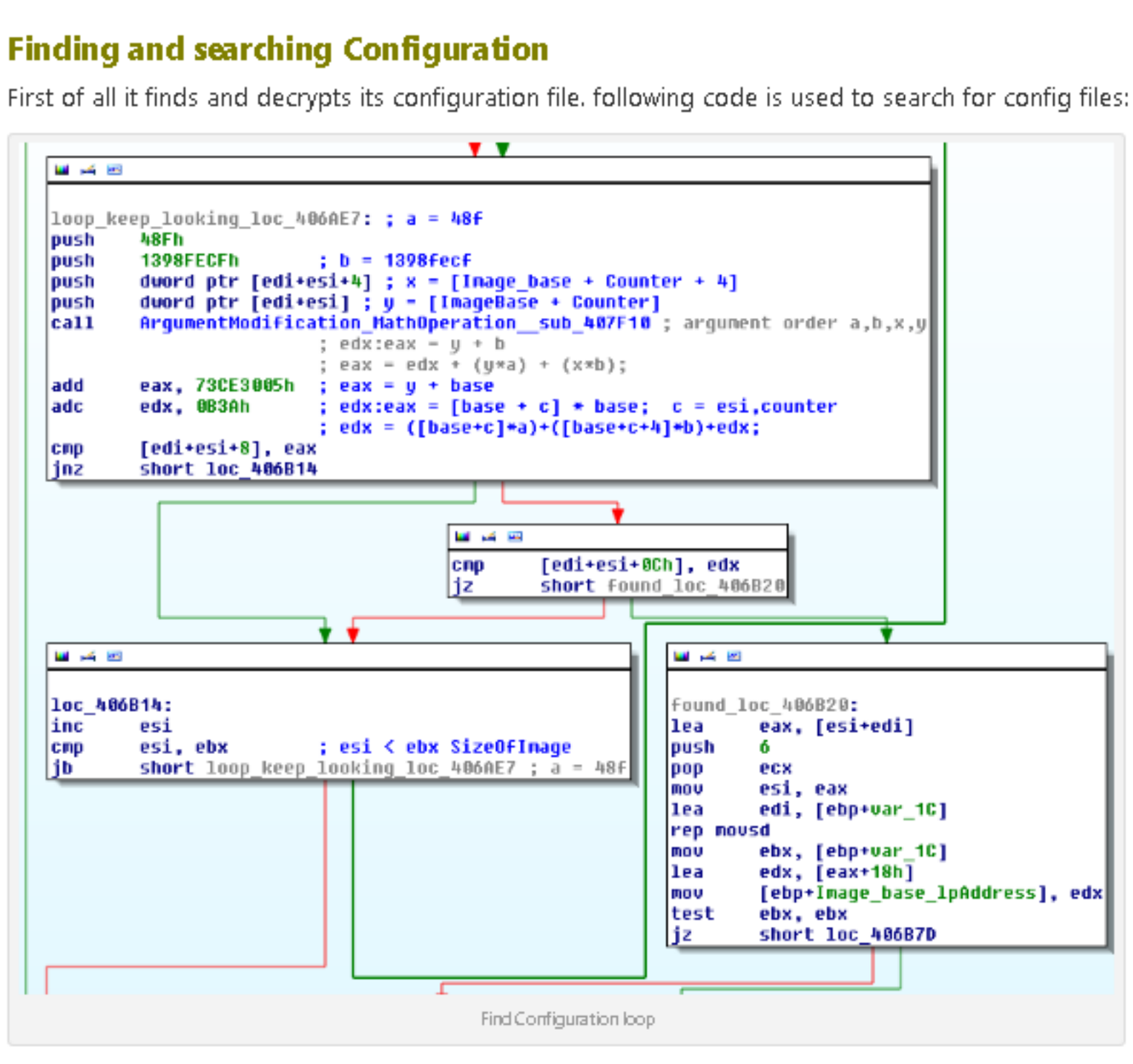
After unpacking some interesting strings in sample:

```
bcdedit.exe -set TESTSIGNING ON
%s\drivers\%s.sys
runas
ComSpec
\\.\NtSecureSys
.text
facebook.com
microsoft.com
svchost.exe
msvcrt.dll
SeShutdownPrivilege
IsWow64Process
Wow64DisableWow64FsRedirection
Wow64RevertWow64FsRedirection
ZwQuerySystemInformation
WinExec
CreateThread
```

Configuration File

Finding and searching Configuration

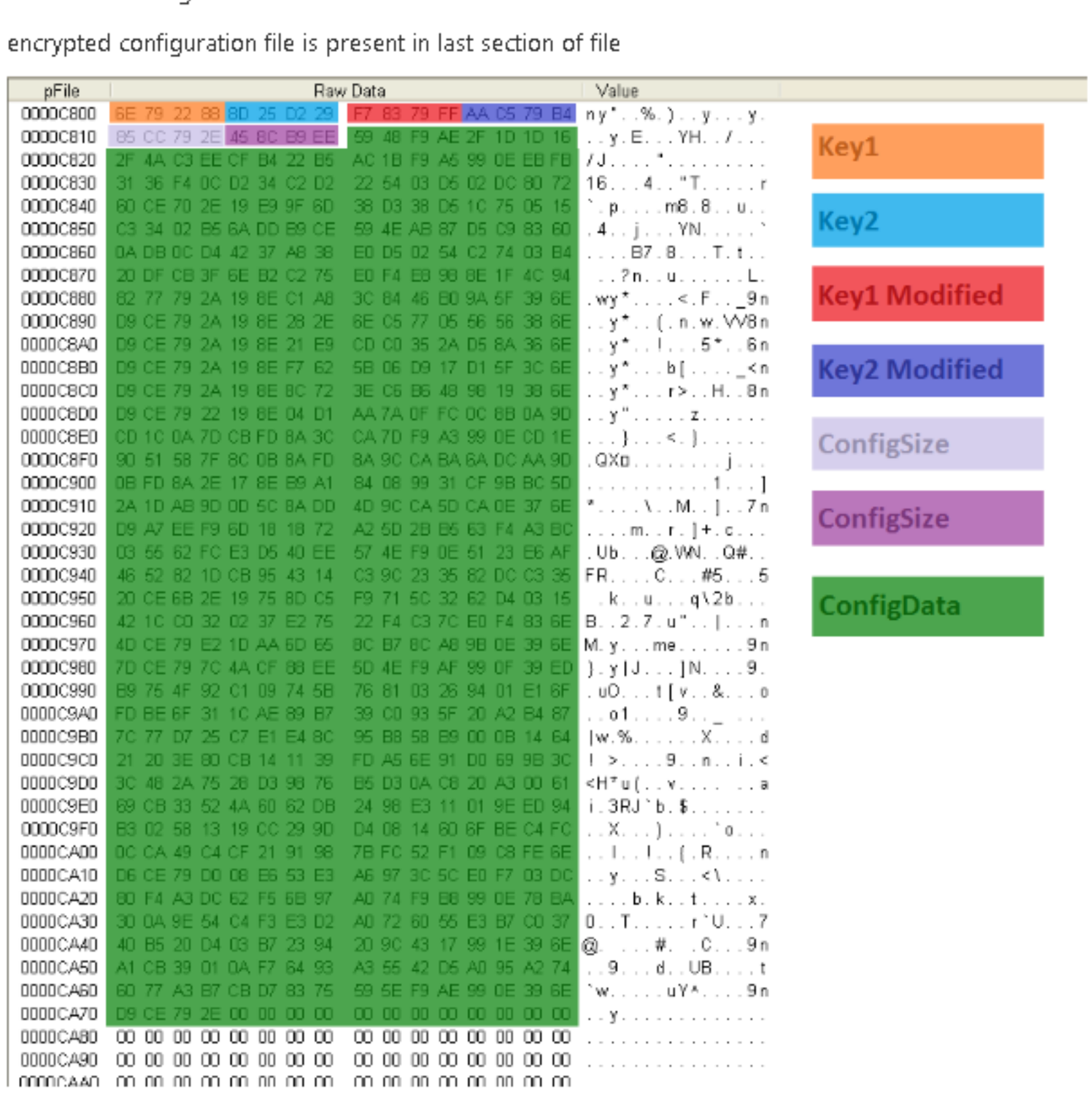
First of all it finds and decrypts its configuration file. following code is used to search for config files:



Find Configuration loop

it starts searching from start to end of file.

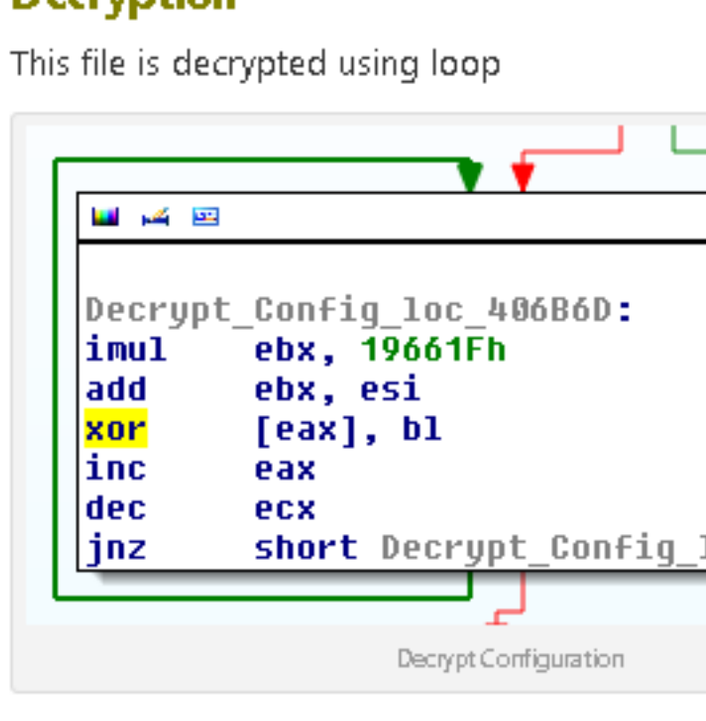
encrypted configuration file is present in last section of file



Two DWORDs are read and modified then compared with next two DWORDs if match config file is found. next two DWORDs are size of config file.

Decryption

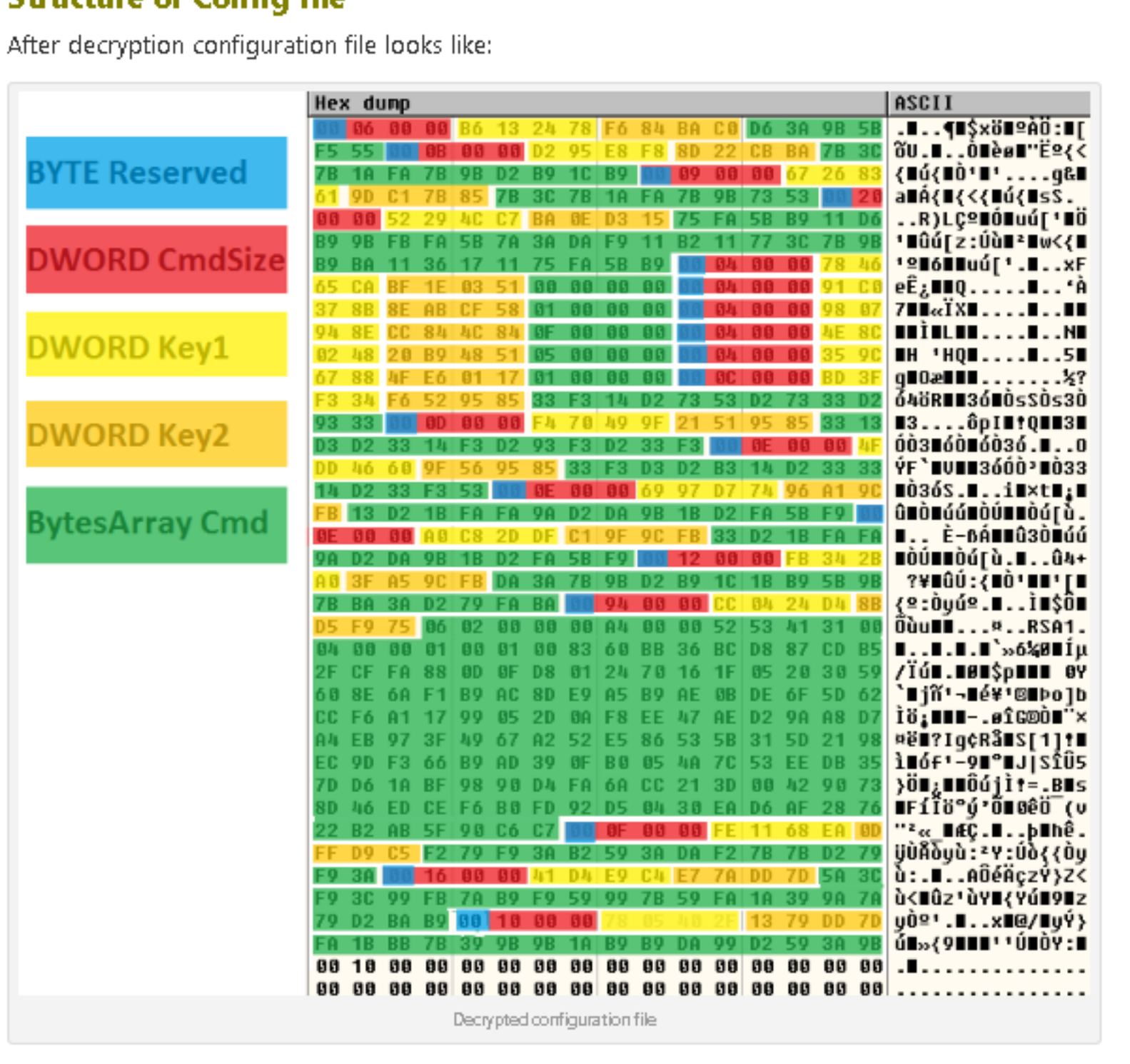
This file is decrypted using loop



Decrypt Configuration

Structure of Config file

After decryption configuration file looks like:



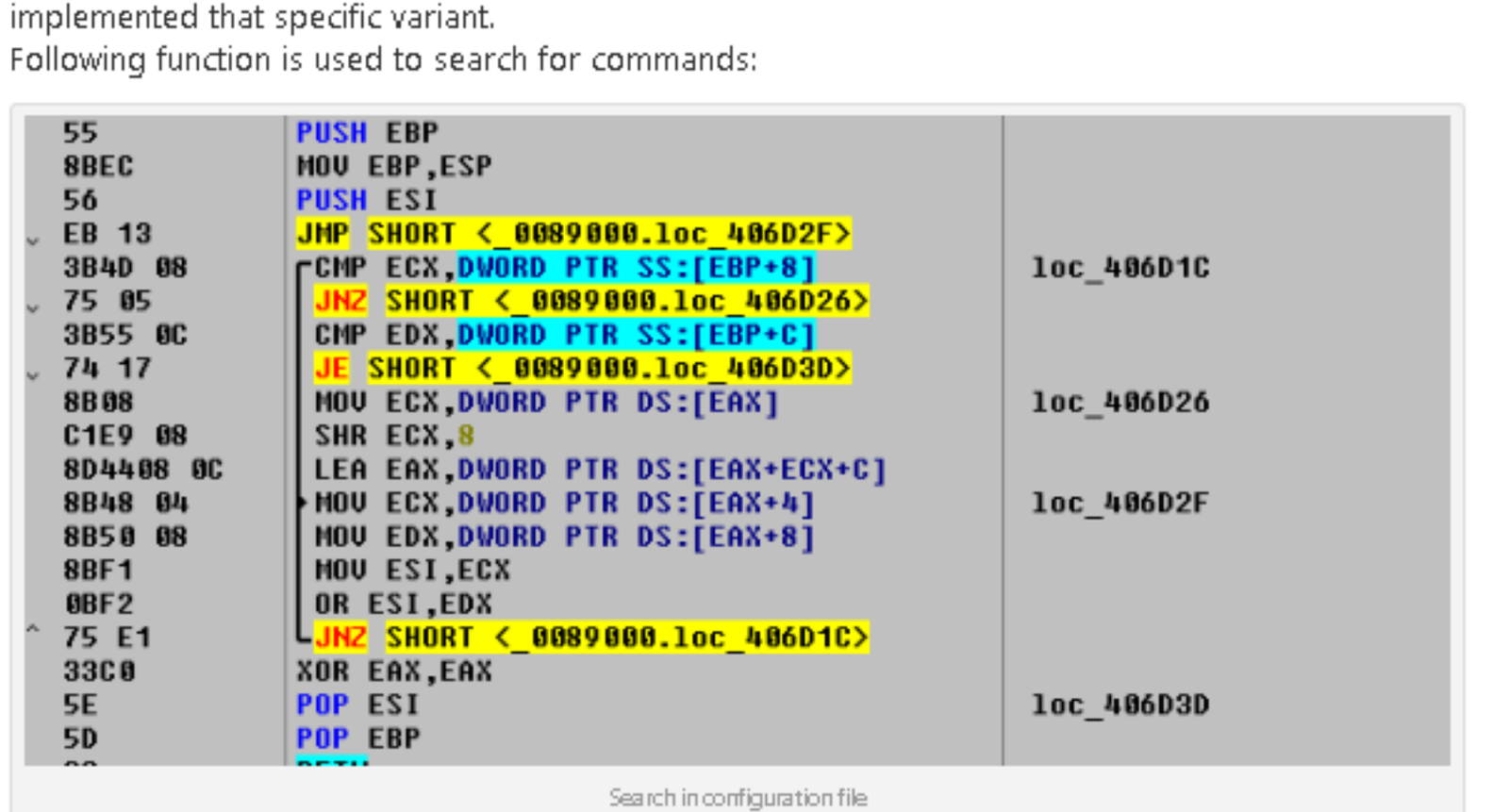
Decrypted configuration file

Configuration file is in format

```
Struct{
BYTE Reserved;
DWORD Size;
DWORD Key1;
DWORD Key2;
BYTEARRAY Data;
}
```

Command Searching

It uses special format for commands. Commands look like random data predefined Key1 and Key2 are used to search for commands in configuration file. if these keys are found it means commands are implemented that specific variant.
Following function is used to search for commands:



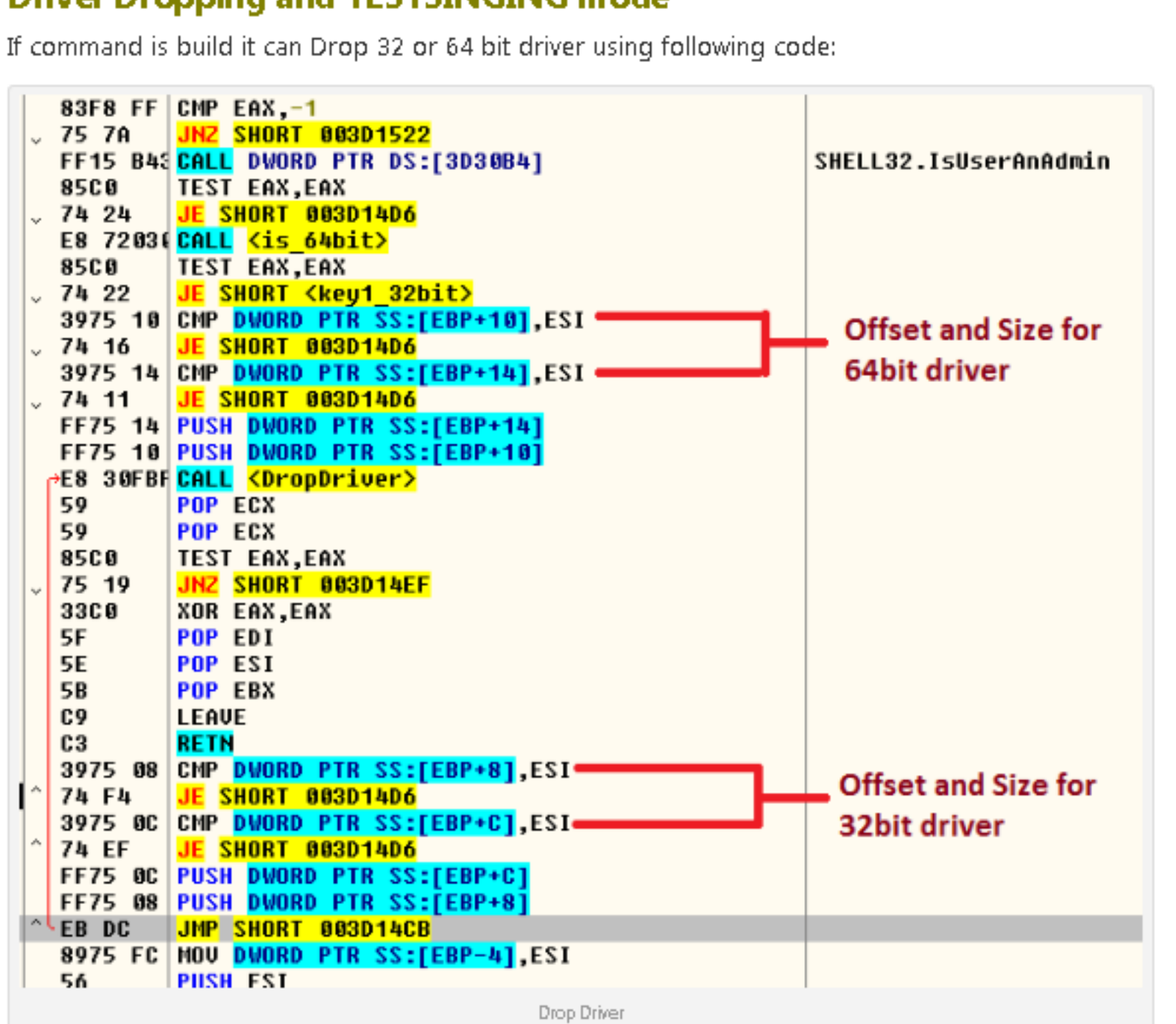
Search in configuration file

Copy Data from ".rdata" section

It copies code from ".rdata " section in newly allocated memory and uses that for some important functions. this trick is used to thwart static analysis.

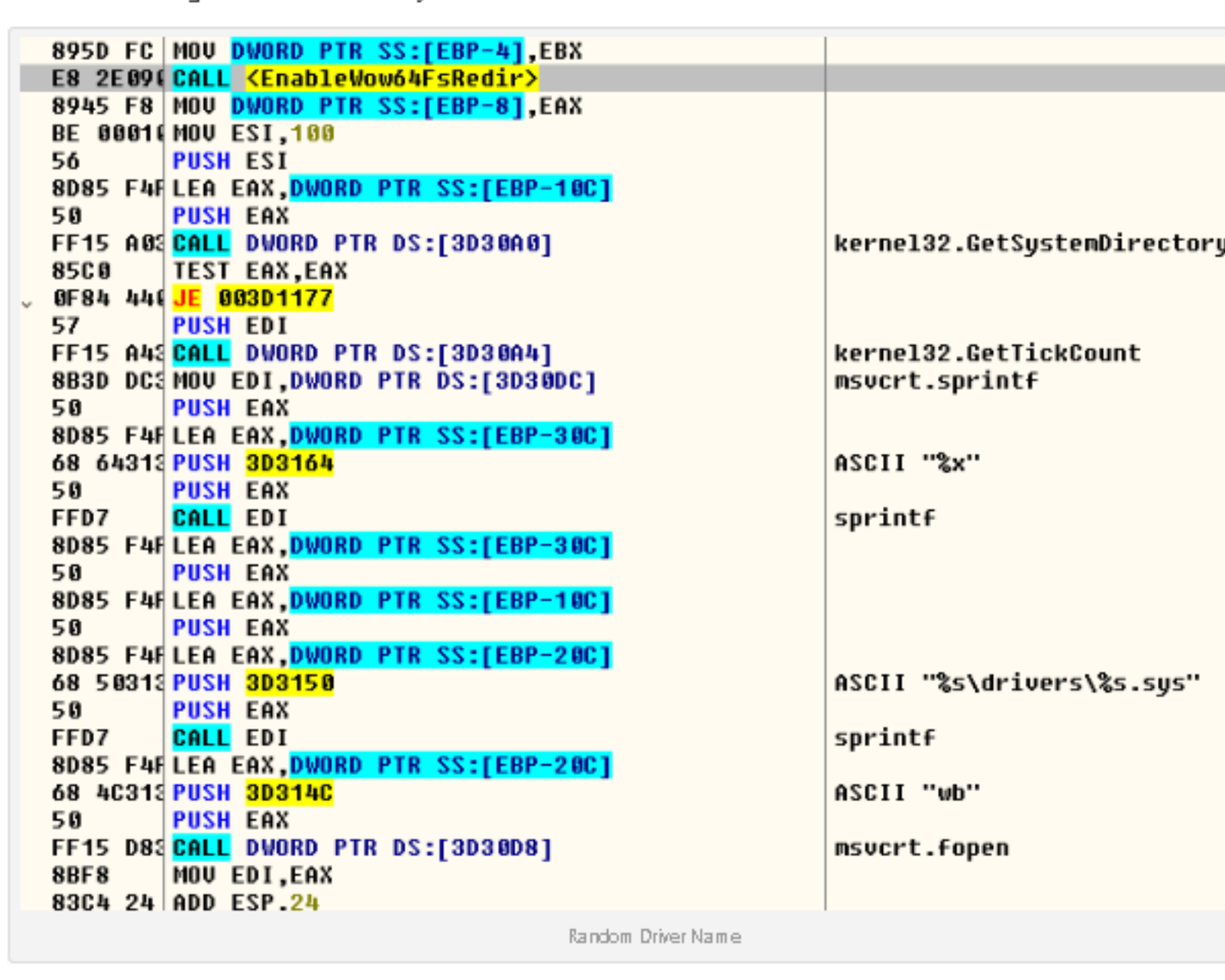
Driver Dropping and TESTSINGING mode

If command is build it can Drop 32 or 64 bit driver using following code:



Drop Driver

Driver name is generated randomly



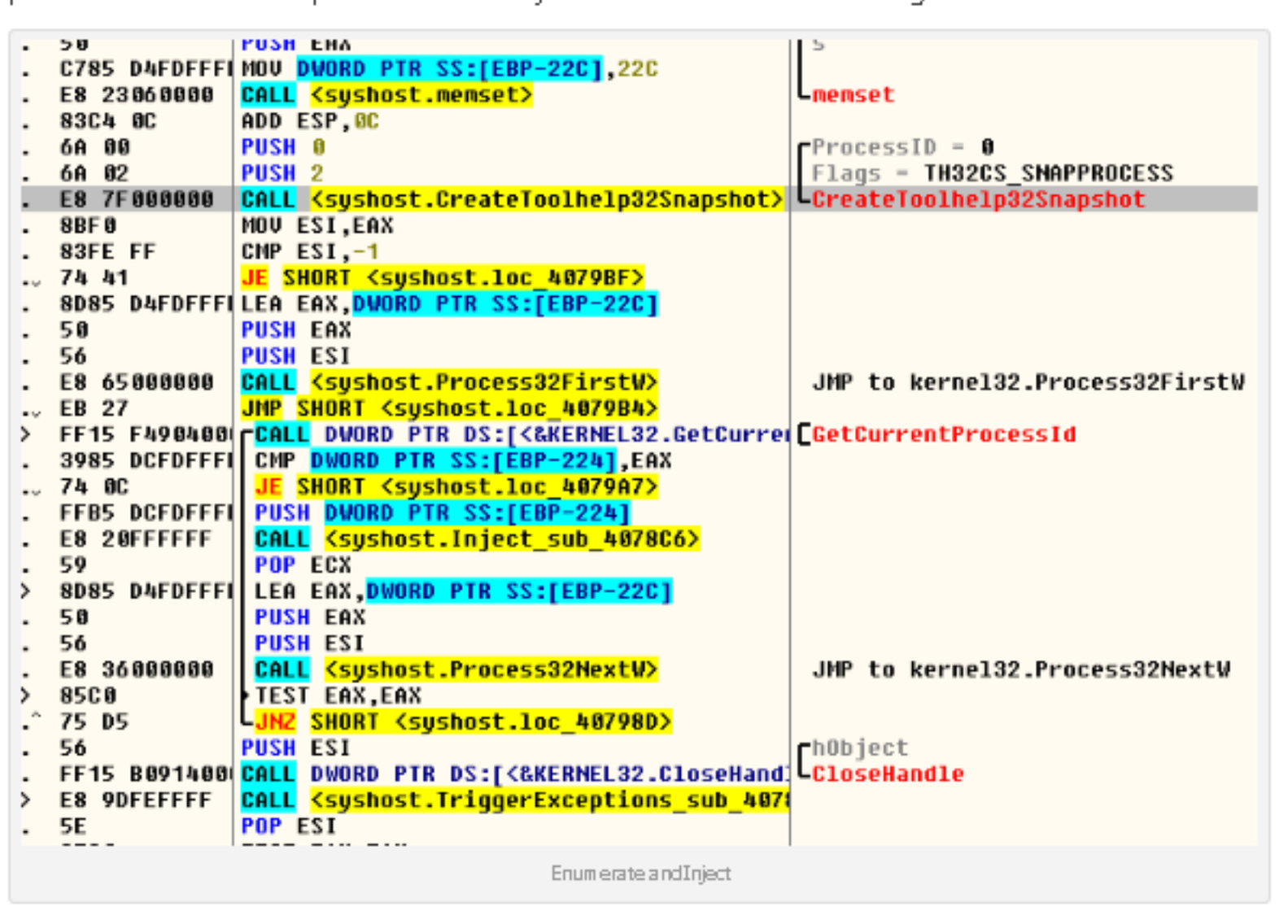
Random Driver Name

Service is created and if system is 64 bit "TESTSIGNING mode" is enables

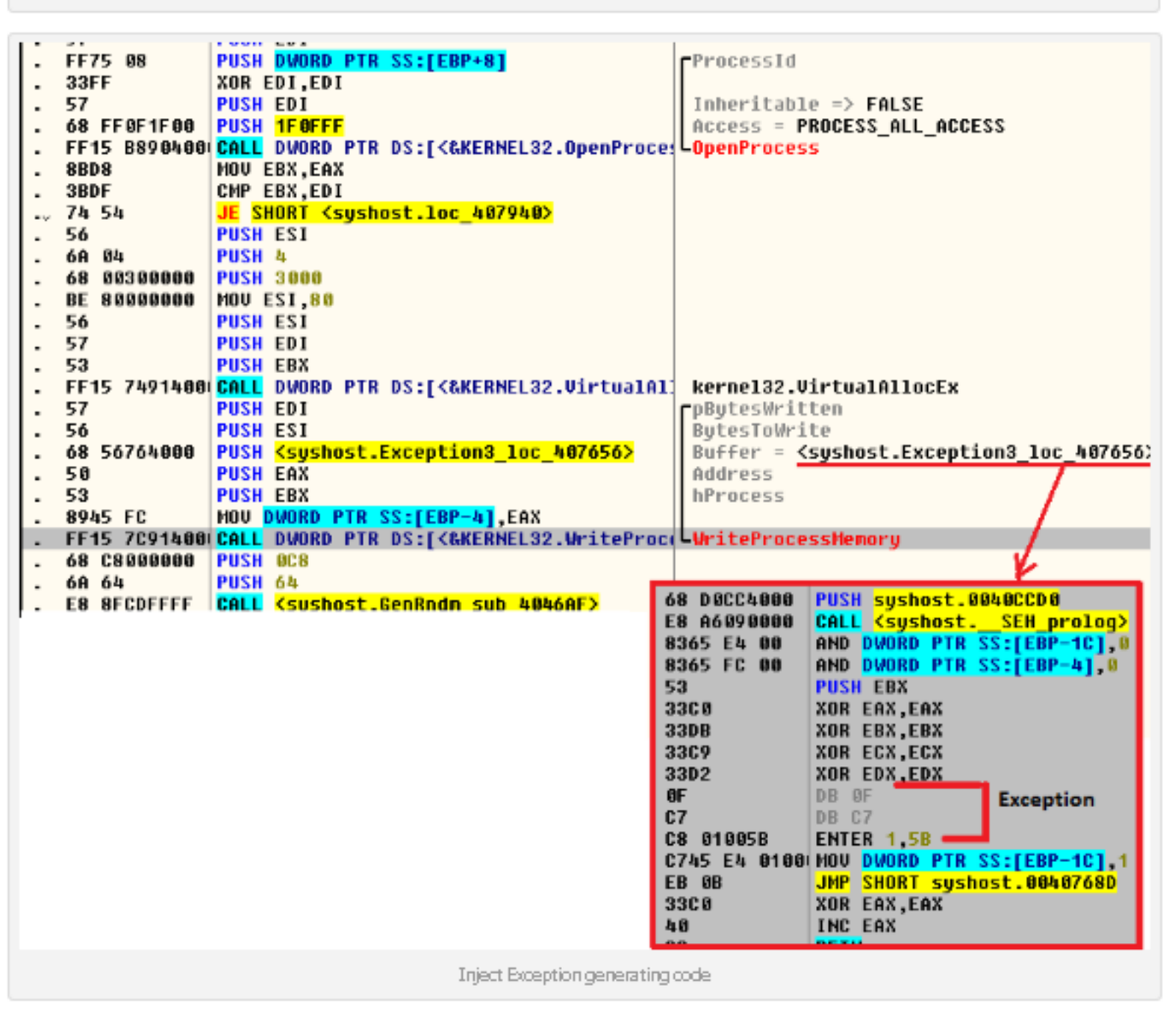
Enable TESTSIGNING mode

DeadByte Injection

May inject DeadBytes Into running processes. These bytes generate exceptions and can crash the process. if some critical process crashes system will restart and Driver agent will be activated.



Enumerate and Inject



Inject Exception generating code

Domain names and IP addresses

Then it will search and decrypt Domain names and IP's from configuration file and communicate with them.

In this file decrypted domain names are:

```
"jygydwkegbdsbohalkc.me"
"opusattheend.bit"
```

and IP addresses are:

```
"178.32.31.41"
"106.187.47.17"
"176.58.118.172"
```

Error Reporting function

Also Contains an Troubleshooting and error reporting module which send error report to specified remote address. If it is unable to perform some operation like unable to create thread then Error reporting function is called. This function collects System info and error code then encodes information and selects random domain from decrypted domains array,decrypt rest of URL path from config,append to URL and send information. In this case decrypted path : "/cgi-bin/ss.cgi"

Here is the link to Control Flow Graph of Necurs with functionality i have covered so far.

Main Thread call one function after doing all activity and also created some Threads. I am working on analysis of those threads and that function Analysis of those will be covered in future blog posts.
Regards,

Atinder

Analysis Necurs Threats

This entry was posted by Atinderpal Singh on August 2, 2013 at 1:05 pm, and is filed under Analysis, MDT, Threats, Uncategorized. Follow any responses to this post through RSS 2.0. You can leave a response or trackback from your own site.

4 comments

Reegun (2 MONTHS)

Nice analysis

Atinderpal Singh (2 MONTHS)

Thanks 😃

sheik (2 MONTHS)

nice post atinder!

Atinderpal Singh (2 MONTHS)

thanks seikh 😃

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

Search GO

ARCHIVES

- October 2013
- September 2013
- August 2013
- July 2013
- June 2013
- January 2013
- December 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010

META

- Register
- Log in