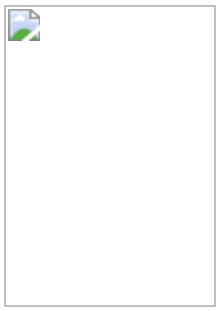
奇安信威胁情报中心

ti.qianxin.com/blog/articles/Blocking-APT:-Qianxin's-QOWL-Engine-Defeats-Bitter's-Targeted-Attack-on-Domestic-Government-and-Enterprises/

概述

蔓灵花（BITTER）是疑似具有南亚背景的APT组织，该组织长期针对中国，巴基斯坦等国家进行攻击活动，主要针对政府、军工业、电力、核能等单位进行定向攻击，窃取敏感资料。

近日，搭载了奇安信威胁情报中心自主研发反病毒引擎QOWL的奇安信安全终端“天擎”成功阻断蔓灵花组织针对国内企业的定向攻击活动，在此次攻击活动中，该组织依旧使用了其常用的攻击手法，企图释放执行其常用的下载者进行恶意软件部署，但被QOWL杀毒引擎成功拦截。



同时，奇安信威胁情报中心红雨滴团队在日常的威胁狩猎中也捕获了蔓灵花组织利用中文诱饵样本的攻击活动。捕获的样本为伪装成船舶工业相关诱饵的SFX文件，运行后将向受害者展示诱饵PDF，从而达到迷惑受害者的目的，同时部署恶意软件开展窃密活动。

在此轮攻击活动中，蔓灵花组织攻击手法变化不大，且仍然使用奇安信曾披露过的C2服务器进行通信，同时该C2服务器分发的插件模块也与此前攻击活动中的基本一致。此处仅以公开样本进行分析阐述。

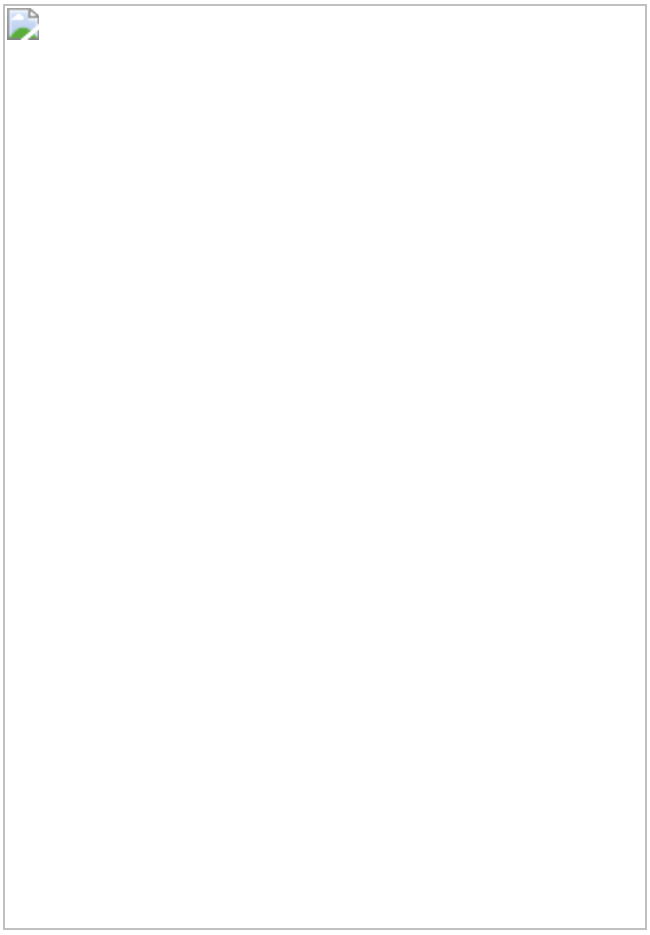
样本分析

此次捕获的公开样本信息如下：

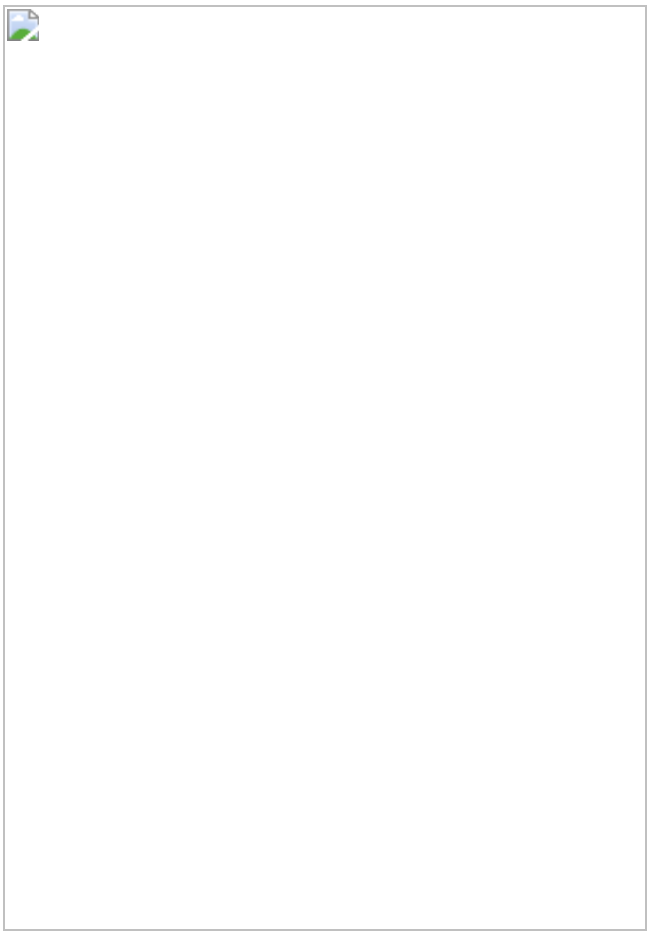
文件名	MD5	时间戳
CERT.msi	1475df569f8a31e49a659c6d9764ae93	1999-06-21 07:00:00
开证装期邮件.pdf.exe	806626d6e7a283efffb53b3831d53346	2017-11-08 13:54:11 UTC

开证装期邮件.pdf.exe

该样本为SFX自解压文件，运行在C:\intel\logs路径下部署dlhost.exe执行。



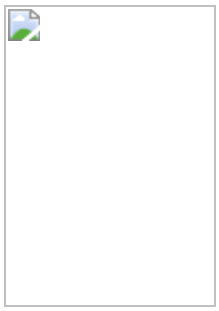
释放展示的中文诱饵文档如下：



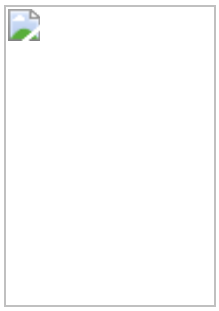
文件名	**dlhost.exe**
MD5	a39aa2ecbbb50c97727503e23ce7b8c6
时间戳	星期三, 02.09.2020 07:00:24 UTC

该文件为BITTER组织常用的下载器，运行后，首先解密相关配置信息：

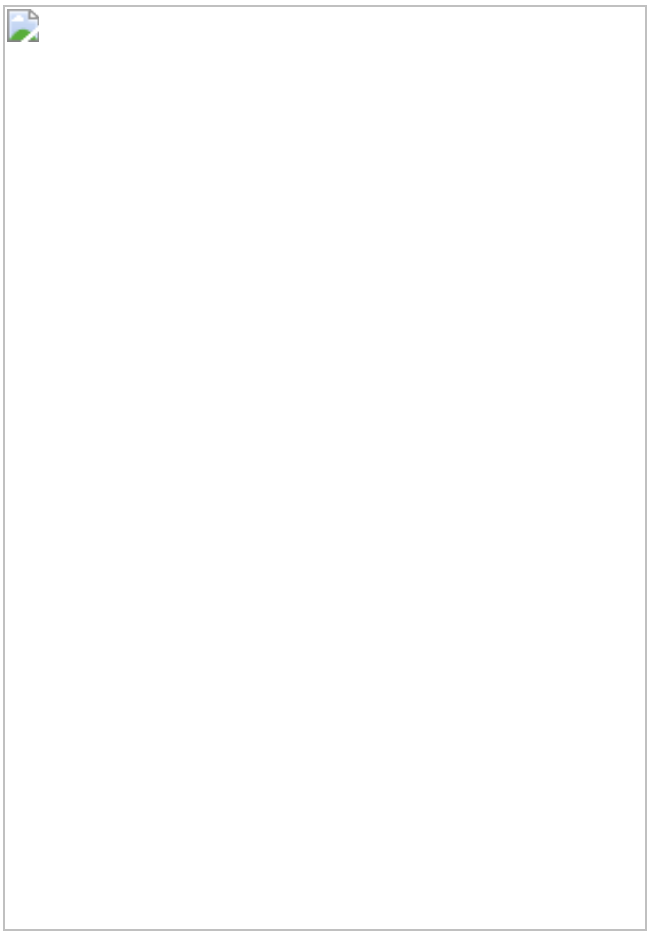
解密算法如下：



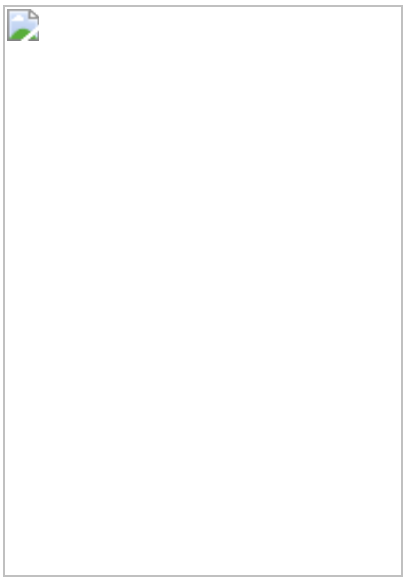
创建信号量，保证只有一个实例运行。



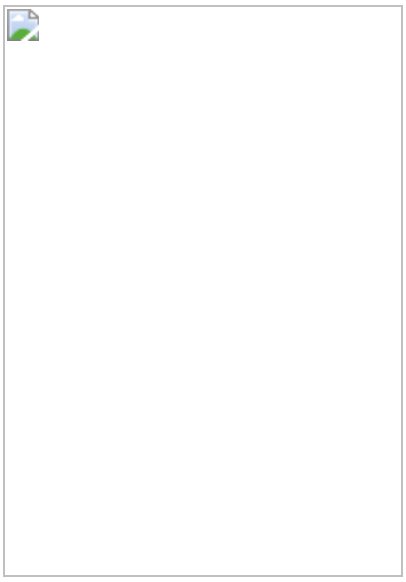
获取受害者基本信息，计算机名称，用户名，MachineGuid和SystemInfo各项信息



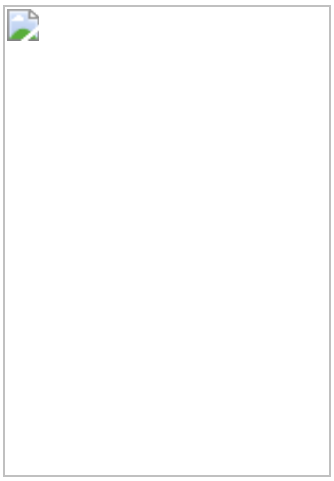
拼接收集的信息。

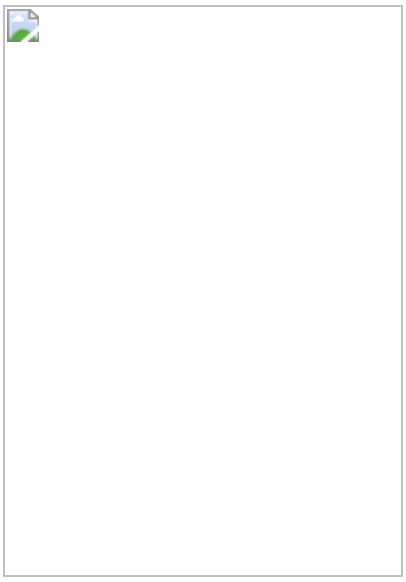


拼接后的信息如下：

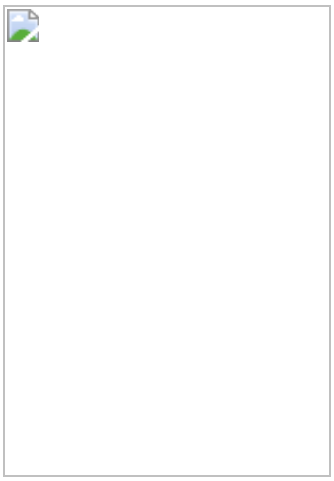


构造Get请求包数据，与C2通信，获取数据解析执行。





若返回数据包中存在“YES FILE”则获取其他插件模块执行。



在分析过程中，红雨滴安全研究员成功获取到部分插件，基本均为BITTER组织常用的插件模块，插件信息如下：

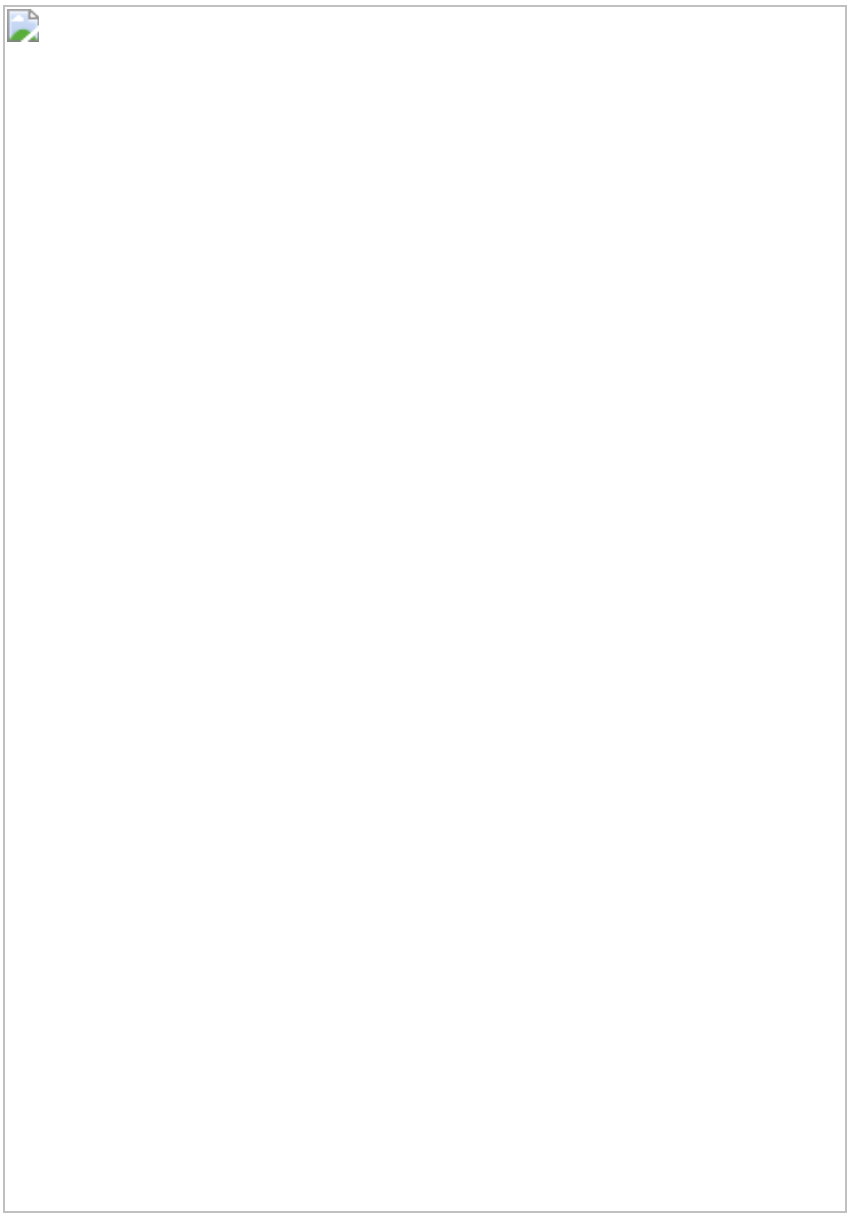
插件名	MD5	功能
lgfxsrvk	6778b6b56f4aebd73f78e4f7da4ac9aa	键盘记录器
Lsapip	660a678cd7202475cf0d2c48b4b52bab	文件，信息上传
MSAServices	58f4d479dd1888f43886118e3a9b2dab	远控
MSAServicet	f4daf0eccf9972bdefb79fbf9f7fb6ee	远控
rgdl	99dd93a189fd734fb00246a7a37014d3	设置audiodq.exe自启动

lgfxsrvk为键盘记录器模块，信息如下：

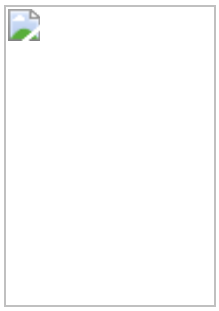
名称	lgfxsrvk
MD5	6778b6b56f4aebd73f78e4f7da4ac9aa
时间戳	星期四, 04.06.2020 06:39:02 UTC

名称	lgfxsrvk
导出模块名	myporj.exe

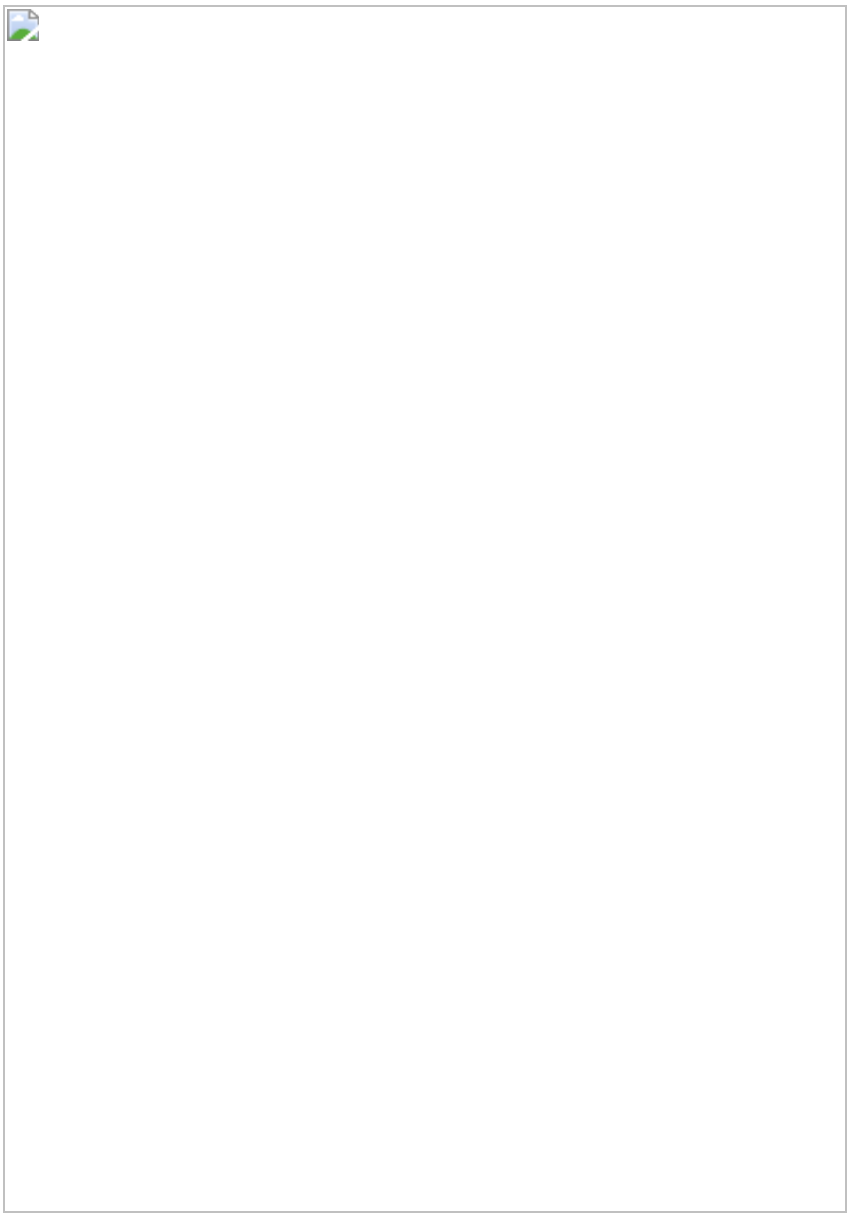
运行后，解密配置信息



之后创建信号量，保证只有一个实例运行。

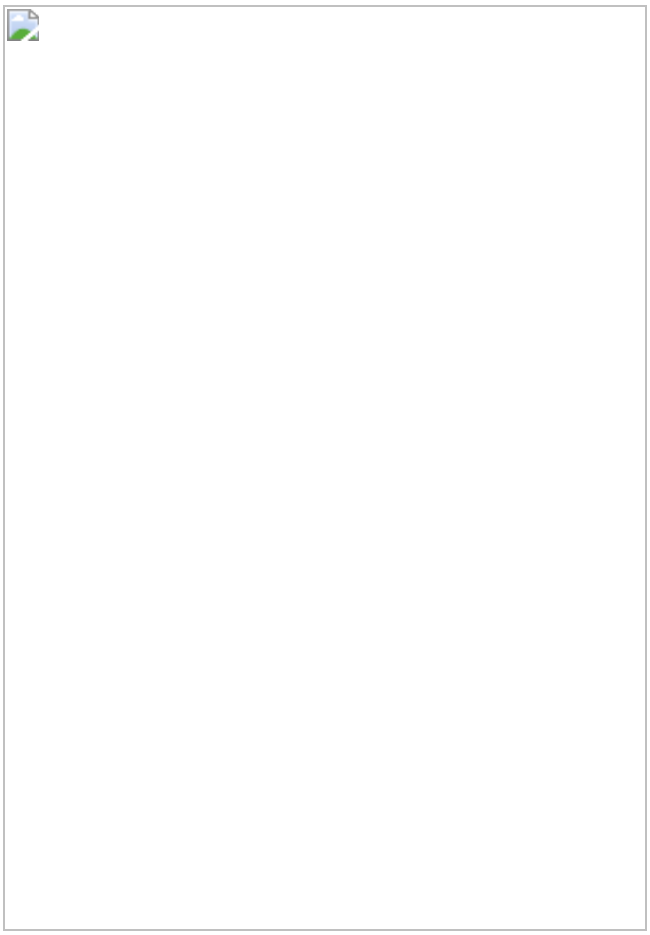


将解密的配置信息组成保存键盘记录信息的路径。



使用全局消息钩子SetWindowsHookExA进行Hook。

部分字符串下图所示：



将获取的键盘信息在每个字符+20进行加密，写入到后缀为tean的文件里。

文件名	lsapip
MD5	660a678cd7202475cf0d2c48b4b52bab
时间戳	星期二, 28.01.2020 06:14:17 UTC

Lsapip为文件上传模块，将其他模块收集的信息上传到C2: 72.11.134.216。

文件名	**MSAServices**
MD5	58f4d479dd1888f43886118e3a9b2dab

文件名	MSAServices
时间戳	星期五, 25.09.2020 06:22:59 UTC

文件名	MSAServicet
MD5	f4daf0eccf9972bdefb79fbf9f7fb6ee
时间戳	星期五, 25.09.2020 06:21:05 UTC

MSAServices，MSAServicet模块是功能相同的远控木马，通信的C2服务器均为pichostfrm.net。支持的命令功能如下表所示：

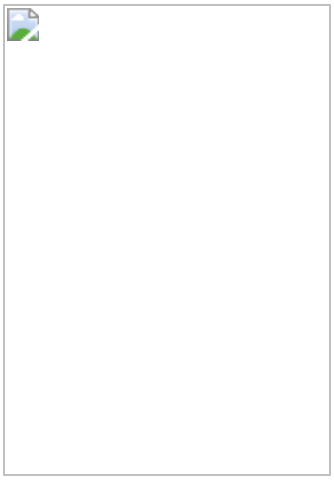
功能名	Opcode	功能描述
R_DeleteFile	2	删除文件
R_FileMgrGetDrives	18	获取驱动器信息
R_FileMgrGetFiles	19	获取目录下的文件信息
R_CreateFile	20	创建文件
R_CopyFily	21	拷贝文件
R_FileTransferBegin	38	传输文件
R_FileTransferSend	39	传输数据
R_FileTransferEnd	40	数据传输完成
R_FileTransferStart	41	传输文件
R_GetCommand	48	获取指令
R_StartCmd	49	开始命令并监控
R_StopCmd	50	结束命令
R_HeartbeatMessage	51	连接状态

CERT.msi

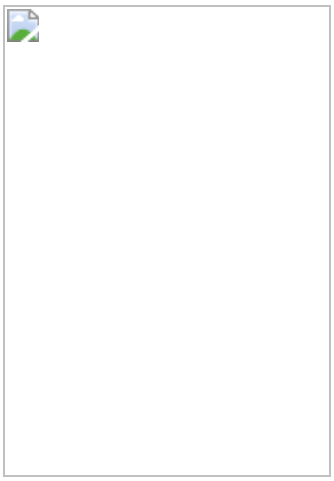
MD5	1475df569f8a31e49a659c6d9764ae93

MD5	**1475df569f8a31e49a659c6d9764ae93**
文件名	CERT.msi
时间戳	1999-06-21 07:00:00

该样本运行后弹出常规安装窗口,并让用户选择安装地址。默认地址为C:\intel\logs\



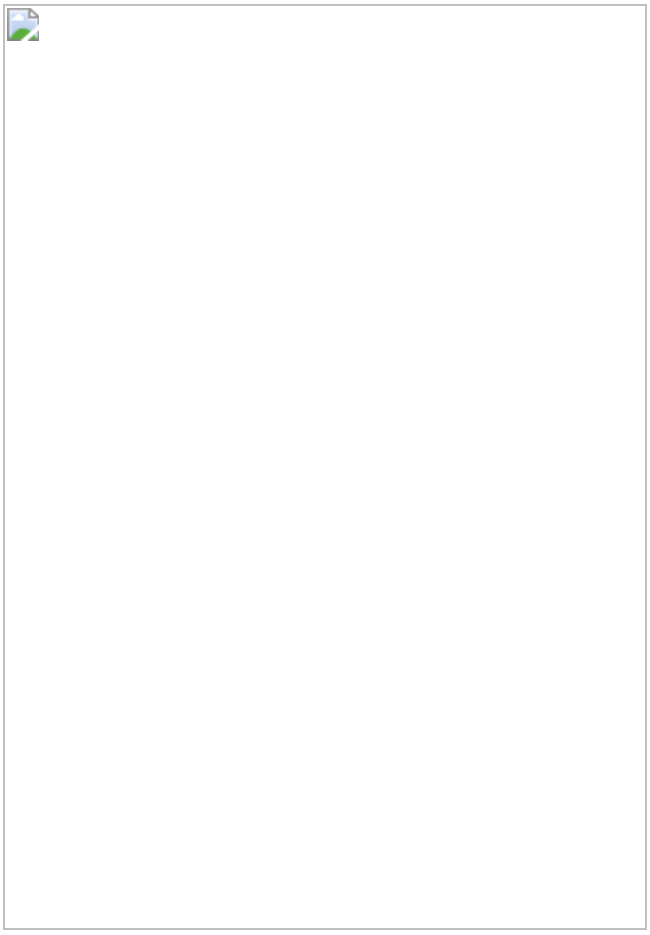
使用请等待安装界面，迷惑受害者，并后台释放执行下载器。



最后将在C:/intel/logs部署下载器模块dlhost.exe执行。

MD5	**25a16b0fca9acd71450e02a341064c8d**
文件名	C:/intel/logs/dlhost.exe
时间戳	星期四, 22.10.2020 05:02:38 UTC

该模块与上述dlhost.exe功能基本一致，此处不在赘述，解密的配置信息如下：



遗憾的是，该C2服务器仅获取到两个插件模块，相关信息如下：

插件名称	**MD5**	**功能**

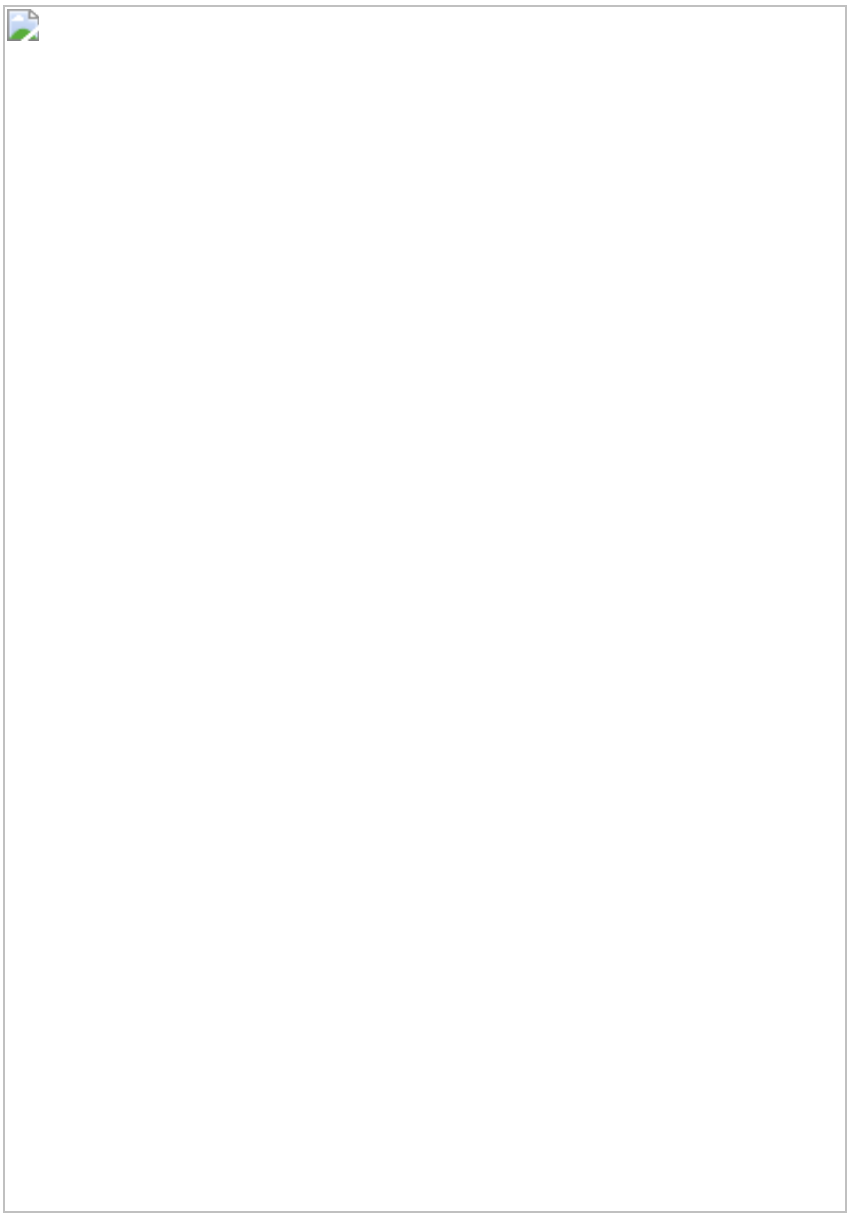
插件名称	MD5	功能
Rgdl	99dd93a189fd734fb00246a7a37014d3	注册audiodq.exe到Run注册表自启动
sht	f6b250aff0e2f5b592a6753c4fdb4475	执行 c:\windows\system32\shutdown.exe

溯源与拓展

奇安信威胁情报中心红雨滴团队结合威胁情报中心ALPHA ti.qianxin.com平台，对此次攻击活动得手法，恶意代码等方面关联分析发现，此次攻击活动与BITTER存在高度相似性。

与BITTER的关联

此次捕获的样本与BITTER组织历史活动中使用的下载器几乎一致，同时相关模块也与BITTER组织曾使用过的插件模块相同。

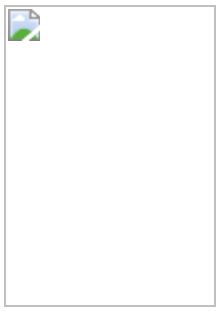


同时，此次捕获样本的C2服务器162.0.229.203已多次出现在蔓灵花组织相关活动中，奇安信威胁情报中心ALPHA平台已有相关标签：

拓展

2020年10月中旬，奇安信病毒响应中旬曾发布《网络安全主题诱饵，配合新型后门WinClouds肆虐南亚地区》《网络安全主题诱饵，配合新型后门WinClouds肆虐南亚地区》[1]一文，文章中提到WinClouds攻击活动中使用到的RTF公式编辑漏洞利用文档与BITTER组织使用的漏洞文档几乎一致。

在此次捕获的攻击行动中，我们再次发现BITTER也使用‘^’字符随机混淆隐藏命令行：



这让WinClouds活动与BITTER组织的关联性大增加，期待与安全社区一起完善相关组织拼图。

总结

BITTER APT组织是一个长期活跃的境外网络攻击组织，且长期针对国内开展攻击活动，安信红雨滴团队提醒广大用户，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，不运行夸张的标题的未知文件。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 进行简单判别。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

1475df569f8a31e49a659c6d9764ae93

25a16b0fca9acd71450e02a341064c8d

99dd93a189fd734fb00246a7a37014d3

f6b250aff0e2f5b592a6753c4fdb4475

806626d6e7a283efffb53b3831d53346

a39aa2ecbbb50c97727503e23ce7b8c6

660a678cd7202475cf0d2c48b4b52bab

f4daf0eccf9972bdefb79fbf9f7fb6ee

72[.]11.134.216

82[.]221.136.27

pichostfrm[.]net

162[.]0.229.203

D:\C++\Reg_Entry\reg_en\Release\reg_en.pdb

参考链接

[1]. https://mp.weixin.qq.com/s/R1YRFLa2cK1G2jRpOwMdfA

网络安全主题诱饵，配合新型后门WinClouds肆虐南亚地区