蔓灵花组织（APT-C-08）使用Warzone RAT的攻击活动披露

By 高级威胁研究院

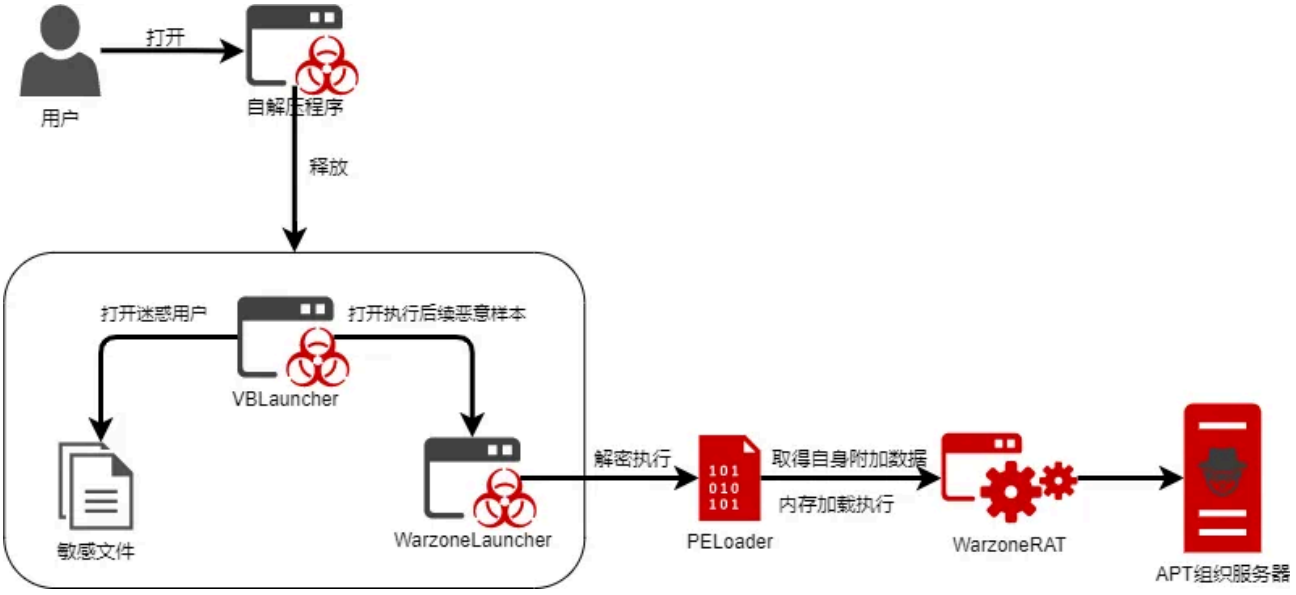
Archived: 2026-04-05 13:59:33 UTC

Warzone RAT是一款纯C/C++开发的商业木马程序，该程序在2018年出现在网络上以软件订阅的方式公开售卖，适配目前所有版本的Windows系统，具备密码采集、远程执行任意程序、键盘记录、远程桌面控制、上传下载文件、远程打开摄像头等多种远程控制功能。

近期，360安全大脑监控到蔓灵花组织在2020年末的攻击活动中，使用Warzone RAT针对我国研究南亚关系的多位社会科学学者进行了攻击。攻击者通过伪造研究讨论学会邀请信的形式发起攻击，最终在受害者机器中植入Warzone RAT进行远程控制。

攻击技术分析

攻击通过投递伪装成为邀请信文档的自解压程序，诱导用户打开自解压程序，通过自解压程序释放并打开诱饵文档以及后续的恶意样本。



恶意样本分析

自解压程序

样本名	MD5	类型
中国南亚**学会2020年会邀请函.exe	98b9ee58f23e50a27cc8fd93de2ef08a	自解压、PE（EXE）

该样本属于Chilkat Zip Sfx程序，首先创建目录%Temp%\ckz_****\zip\，其中****代表随机名，在调试中，此次目录路径为%Temp%\ckz_0CT6\zip\

解压释放后续的样本文件：onedrv.exe、file.pdf和winword.exe到目录%Temp%\ckz_****\zip\下，并启动onedrv.exe

在释放的文件中：

1.onedrv.exe为VB编写的后续样本的启动器

2.winword.exe为Warzone RAT加载器

3.file.pdf为伪装pdf文件，起到迷惑用户的作用

onedrv.exe

样本名	MD5	类型
onedrv.exe	85f2b9dace6497d42c370feeb69bd662	PE（EXE）

该样本的功能为打开当前目录下的WINWORD.exe和file.pdf文件

其中file.pdf为正常的文档文件，达到迷惑用户的效果，我们捕获的文件如下：

winword.exe

样本名	MD5	类型
winword.exe	626d639ecf5972f7cea034b18dbee0f4	PE（EXE）

该样本为Warzone RAT的启动器，存在PDB路径：C:\Users\W7H64\Desktop\VCSamples-master\VC2010Samples\ATL\General\AtlCon\database test1.pdb

该恶意样本的主要功能为解密shellcode数据，并跳转执行shellcode，该shellcode为后续加载Warzone RAT的PELoader。

PELoader

样本名	MD5	类型
PELoader	abdfe73b334851b5202059a02eae58da	Binary（Shellcode）

进入PELoader后，计算重定位偏移，然后动态获取需要的API地址

紧接着在内存中加载后续的恶意PE格式数据，最后跳转到该恶意PE的入口点执行，该PE格式文件为Warzone RAT

Warzone RAT

样本名	MD5	类型
Warzone RAT	c9430ce90e3dc79287251f69e5a872a8	PE（DLL）

该样本属于Warzone RAT，首先创建命名事件对象防止多开，并通过修改注册表项来设置浏览器最大并发连接数

随后获取并解bss节密数据，并判断系统版本，采取两种不同的方式来绕过UAC

如果是win10系统，则通过sdclt.exe来完成，其流程如下：

1.将恶意样本自身路径添加到注册表项HKCU\Software\Classes\Folder\shell\open\command中，执行COM劫持

2.当以普通用户启动sdclt.exe进程时，会以一个高权限运行另外一个sdclt.exe进程，之后高权限的sdclt.exe会启动control.exe进程，该进程会以高权限打开注册表项
HKCU\Software\Classes\Folder\shell\open\command

Warzone RAT在win10系统上通过COM劫持，来以一个高权限启动自身，以达到绕过UAC进行提权的目的

如果是非win10系统，则创建注册表项HKCU\SOFTWARE\hive_rptls\install指向自身路径，获取自身资源“WM_DSP”,并创建进程“cmd.exe”，将获取的资源数据装载到”cmd.exe”并执行。

装载的程序从资源”WM_DISP”获取数据，释放”dismcore.dll”,”ellocnak.xml”到”%TEMP%”目录，通过修改PEB结构，调用COM组件IFileOperation，从而实现绕过UAC，复制文件”dismcore.dll”到系统路径。

然后创建进程pkgmgr.exe，将“/n:%temp%\\ellocnak.xml”作为参数传入，使得pkgmgr.exe加载dismcore.dll，读取“ellocnak.xml”内容，进一步调用注册表项“HKCU\SOFTWARE\hive_rptls\install”内程序路径，即自身程序路径。最终实现自身提权。

之后，如果恶意样本运行于高权限下，则执行powershell命令添加排除项，以躲避windows defender的查杀

然后执行持久化操作，会有如下行为：

1.拷贝自身到%AppData%\images.exe，如果该样本运行于高权限下，则会将自身拷贝到C:\ProgramData\目录下

2.%AppData%\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start并写入数据

3.设置注册表HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Images为自身路径

最后，程序与服务器192.236.249.173:2709建立TCP连接，与服务器通信，数据采用RC4加密，密钥为：”warzone160”

该程序部分功能截图如下：

主要包含如下功能指令：

功能号	说明
0x0	获取被控制机器信息
0x2	获取进程列表信息
0x4	获取驱动器信息
0x6	获取目录信息
0x8	上传文件到服务器
0xA	删除指定文件
0xC	结束指定进程
0xE	远程shell
0x10	结束指定线程
0x14	开启摄像机
0x16	停止摄像机
0x1A	退出并删除自身文件
0x1C	下载文件到被控制端

0x20	获取浏览器密码
0x22	下载文件到被控端并执行
0x24	键盘记录，并上传
0x26	键盘记录（离线）
0x28	RDP
0x2A	启用反向代理
0x2C	停止反向代理
0x38	反向代理端口设置
0x3A	打开指定文件
0x48	注入指定进程
0x4A	遍历获取文件信息

关联归属分析

在《季风行动—蔓灵花（APT-C-08）组织大规模钓鱼攻击活动披露》一文中，我们对蔓灵花一系列行动进行了披露，该行动使用了域名为“coremailxt5mainjsp.com”的钓鱼网站，相关的诱饵样本为http://coremailxt5mainjsp.com/wzrpxierh875NORwnfot/Fileunst/unstr00000.exe（MD5：a8bd76238d96ea17990e4f2df126ecd4），其后门程序使用的C&C 为“192.236.249.173:2706”。而此次Warzone RAT同样使用的是192.236.249.173这一C&C基础设施，结合C&C、攻击目标和技术特点等，我们判断该次攻击属于蔓灵花组织。

总结

蔓灵花组织是近几年针对我国境内目标进行攻击活动的最活跃的APT组织之一，通过此次分析可以看到虽然该组织的攻击行动、后门程序和基础设施被多次曝光，但是该组织仍然肆无忌惮地选用商业木马程序和相关基础设施再次持续发起攻击，相关机构组织和个人仍需要提高警惕。目前360威胁情报云、360沙箱云、360APT全景雷达、360安全卫士团队版等360全线政企安全产品可支持对该组织的攻击检测，能有效保护政企机构免受该组织的攻击。

附录 IOCs
MD5

98b9ee58f23e50a27cc8fd93de2ef08a

85f2b9dace6497d42c370feeb69bd662

626d639ecf5972f7cea034b18dbee0f4

abdfe73b334851b5202059a02eae58da

c9430ce90e3dc79287251f69e5a872a8

faa6b6a113fc5d9286cc3a1ad32046db

15fb48dfb48e2be0cec8c8ed0235bbb5

ca76c811c3b0fbc61281b1fc83233f73

f77a5f62c2a697c684d1fc418f21c442

a8bd76238d96ea17990e4f2df126ecd4

C&C
192.236.249[.]173:2709
http://coremailxt5mainjsp[.]com/wzrpxierh875NORwnfot/Fileunst/unstr00000.exe

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。
