伏影实验室：“海莲花”(OceanLotus)最新攻击链揭秘——MsMpEng 侧载攻击

2020-08-07 伏影实验室 APT, MsMpEng, 伏影实验室, 侧载攻击, 海莲花

近期，伏影实验室的高级威胁分析系统检测到一系列采用相同混淆手段的恶意文件，通过对本次告警事件及多个关联事件的分析，伏影实验室确认该系列攻击事件的发起者为**海莲花（OceanLotus，APT32）**组织。此系列攻击事件仍然是以使用越南语的邮件用户为目标，除常规手法之外，海莲花组织在这几次攻击中使用了一个新的系统组件以加载恶意程序，并增加一种新的混淆技术，以及一款新的中间载荷。

```
loc_10001D5A:                           ; CODE XREF: .text:10001D53↑j
                push    ecx
                jmp     short loc_10001D61
; ---------------------------------------------------------------------------
                dd 700B53C8h
; ---------------------------------------------------------------------------

loc_10001D61:                           ; CODE XREF: .text:10001D5B↑j
                push    esi
                push    dword_1007D30B
                mov     ecx, edi
                push    offset unk_1001D73B
                jmp     short loc_10001D75
; ---------------------------------------------------------------------------
                dd 6E2E5CE9h
; ---------------------------------------------------------------------------

loc_10001D75:                           ; CODE XREF: .text:10001D6F↑j
                call    dword ptr [eax]
                mov     eax, eax
                mov     eax, [edi+4]
                mov     dword_1007D30B, 0
                mov     dword ptr [edi], offset off_1001C604
                push    edx
                mov     edx, eax
                and     edx, eax
                pop     edx
                jz      short loc_10001D9F
                mov     eax, eax
                push    eax
                call    sub_10002CE5
                add     esp, 4

loc_10001D9F:                           ; CODE XREF: .text:10001D92↑j
                push    edi
                call    sub_10002BE9
                add     esp, 4
                push    0
                nop
                call    esi             ; shellcode entry
```

MsMpEng.exe 是 Windows 反病毒程序 WindowsDefender 的组件之一，会在启动时加载同目录下的 DLL 文件。黑客利用这一特性，让合法 MsMpEng.exe 程序加载海莲花组织构造的恶意 DLL 文件，实现绕过 Windows 执行检测的侧载攻击。

本次攻击事件中涉及的恶意程序使用了新的混淆和字符串隐藏技术来对抗分析，典型的代码混淆方法有：

1. 使用 test 指令比较全局数据与一个固定的立即数，根据条件跳过不定长垃圾字节；
2. 使用 cmp 指令比较全局数据与立即数，根据条件跳过不定长垃圾字节；
3. 使用 jmp 指令直接跳过不定长垃圾字节；

这种混淆手法会导致 ida 无法定义这些 junkbytes 的类型，进而阻碍 ida 生成 CFG 和 Pseudocode。

该恶意程序隐藏字符串的方式有：使用加密表的方式对字符串进行加密，加密表中记录了每个程序字符串的位置、长度以及加密键。程序在运行时遍历该加密表，读取每个加密字符串，异或解密后写入原位置。

该恶意软件作者还在程序文件末尾加入大量无效数据，增加文件尺寸，影响一些安全程序的自动提交功能。

此次攻击事件中，攻击者开发了一个全新的后门程序 SnacksDownloader。该后门是由一段加密的 shellcode 加载的。SnacksDownloader 读取主机网卡信息与遍历进程信息，随后向硬编码的 C2 地址发起两次请求，通信协议为 tls。

第一次请求时，SnacksDownloader 将获取到的本机网卡硬件地址和进程列表发送给 C2 地址，攻击者可以通过这些信息判断受控主机的运行环境。第二次请求会获取一个以.png 结尾的压缩文件，存储到 C:\ProgamData 目录下，使用程序内载的 lzma 算法进行解压缩。最后，程序调用 taskschd.dll，注册名为 Windows Management Instrumentation 的任务计划程序，使被解压程序每隔 15 分钟运行一次。

根据上述攻击事件中采取攻击技术，伏影实验室的研究员回溯了过去几个月的数据，发现数起针对 64 位操作系统的攻击事件中所使用的诱饵文档。在回溯过程中发现，在 2020 年 6 月起，海莲花组织就已经采用相同的技术对字符串进行加密以及对代码进行混淆，并且恶意文件尾部的大量的垃圾数据也是由攻击链的中间件生成，使每个恶意 dll 文件都拥有庞大的体积与独特的文件哈希。

在跟踪分析的相关攻击事件中，我们发现不仅仅是恶意 dll 程序本体，其外层和内层载荷都使用了同样的对抗技术，这表明所有恶意程序可能是由同一个代码框架生成。同时，各事件中使用的组件虽然高度相似，但彼此之间都有一定程度的代码逻辑上的区别，该现象表明海莲花组织并不是量产了大批攻击工具进行大范围打击，而是在进行代码上的快速迭代的同时，使用直接投放的方式来评估当前版本攻击组件的隐蔽性。