Darkhotel（APT-C-06）使用“双星”0Day 漏洞（CVE-2019-17026、CVE-2020-0674）针对中国发起的 APT 攻击分析

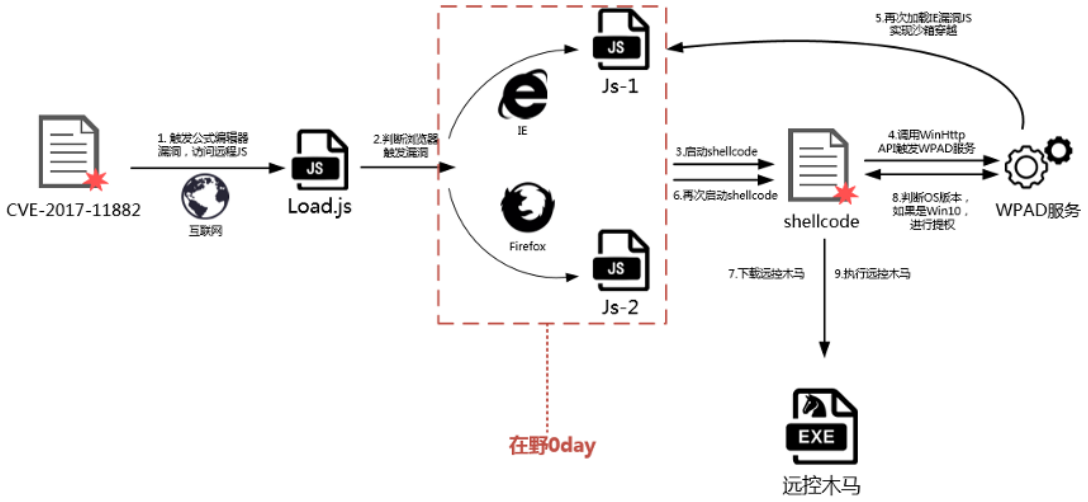
背景

2020 年 1 月 14 日，微软正式宣告 Windows 7 系统停止更新。在 Windows 7 正式停服关键时间节点的第二天，即 2020 年 1 月 15 日，360 安全大脑在全球范围内就捕获了首例同时利用 IE 浏览器和火狐浏览器两个 0day 漏洞进行的复合攻击，由于是全球首家捕获，我们将其命名为“双星”0day 漏洞攻击。

“双星”0day 漏洞的细节已第一时间分别报告给了微软和 Mozilla，在通过短暂的沟通后，微软和 Mozilla 官方都确认了 0day 漏洞，此次漏洞影响最新版本的火狐浏览器和 IE 浏览器及使用了相关浏览器内核的应用程序，同时官方为漏洞分别分配了 CVE-2019-17026（火狐浏览器）和 CVE-2020-0674（IE 浏览器）两个漏洞编号。通过 360 高级威胁应对团队的分析溯源判定，“双星”0day 漏洞是被活跃近十余年的半岛 APT 组织 Darkhotel(APT-C-06)所利用，主要针对我国商贸相关的政府机构进行攻击。

攻击流程分析

我们发现“双星”0day 漏洞的攻击是利用 office 漏洞文档、网页挂马和 WPAD 本地提权的多种攻击方式进行的复杂组合攻击。完整的攻击流程如下：



以 IE x86 为例：

1. IE 加载 JS-1 漏洞利用成功，获得代码执行权限，第一次执行 JS-1 中的 shellcode。
2. Shellcode 利用 winhttp API（winHttpOpen 和 WinHttpGetProxyForUrl） 触发 WPAD 服务的运行。
3. WPAD 服务运行后从远程加载 JS-1，再次运行脚本中的 shellcode，shellcode 通过判断进程名是否为 svchost 来判断是否在服务中被运行。
4. Shellcode 从远程下载后续文件，并获取当前系统版本来决定是否需要使用 DCOM 提权，win7 下的 WPAD 服务具有 system 权限，

不需要使用提权，win10 下的 WPAD 服务为 local Service，则利用 bits 服务来提权，最后运行下载的后续文件。

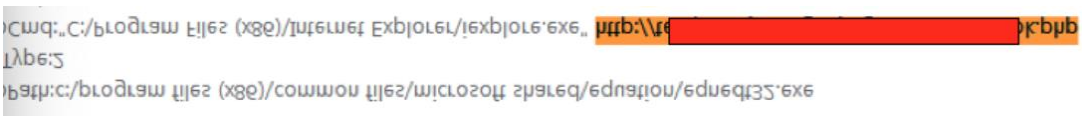
攻击细节分析

双星漏洞网页会判断当前浏览器为 IE 还是 Firefox，操作系统为 32 位还是 64 位，然后加载相应的 exploit 攻击代码。

攻击者可以直接利用双星漏洞进行网页挂马攻击，有意思的是我们发现了一例 Office 漏洞文档触发的双星漏洞，是默认打开 IE 浏览器进行攻击。

初始攻击使用了 office 公式编辑器漏洞（CVE-2017-11882），攻击者根据目标精心制作了诱饵文档。

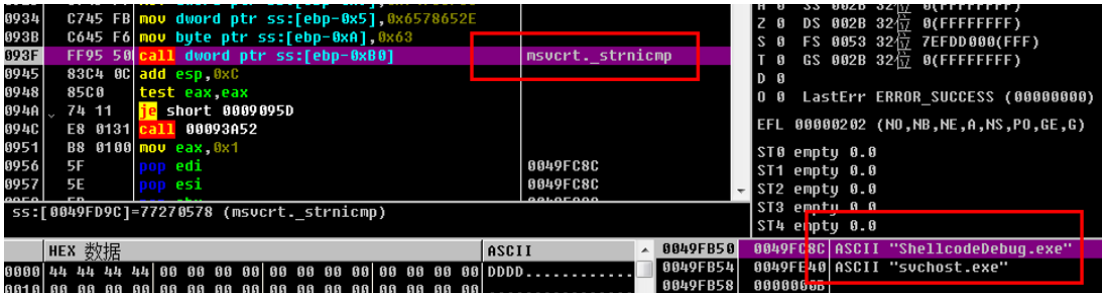
当受害者打开漏洞文档触发漏洞后，恶意代码会启动公式编辑器，利用公式编辑器进程再打开 IE 浏览器访问恶意网页触发“双星”漏洞。



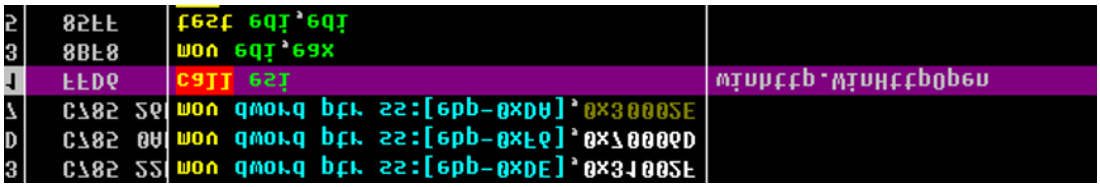
其中的 IE 浏览器漏洞（CVE-2020-0674）是 IE Jscript 引擎中的一个 UAF 漏洞，我们提取了部分漏洞代码，由于漏洞代码中 Array 对象的 Sort 函数回调参数没有被加入 GC 追踪链中，所以攻击者可以在回调中释放仍然被引用的对象，最终导致 UAF 漏洞可以执行任意代码。

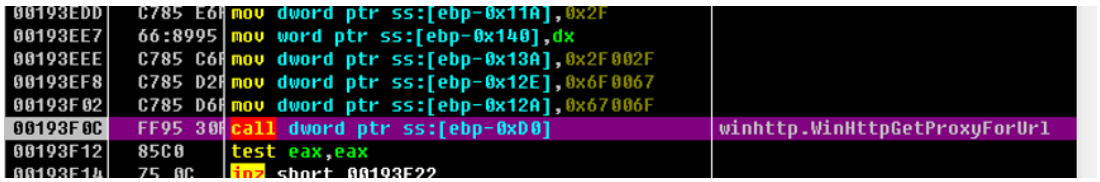
```
for (var i = 0; i < aaa; i++) {
    aaa_dummyArrs[i] = new Array(1, 2);
}
aaa_dummyArrs[0].sort(FreeingComparator);
function FreeingComparator(a, b) {
//a 和 b均不被GC追踪
}
```

IE 浏览器漏洞成功利用后，会执行 shellcode，首先会判断当前进程是否为 svchost.exe。

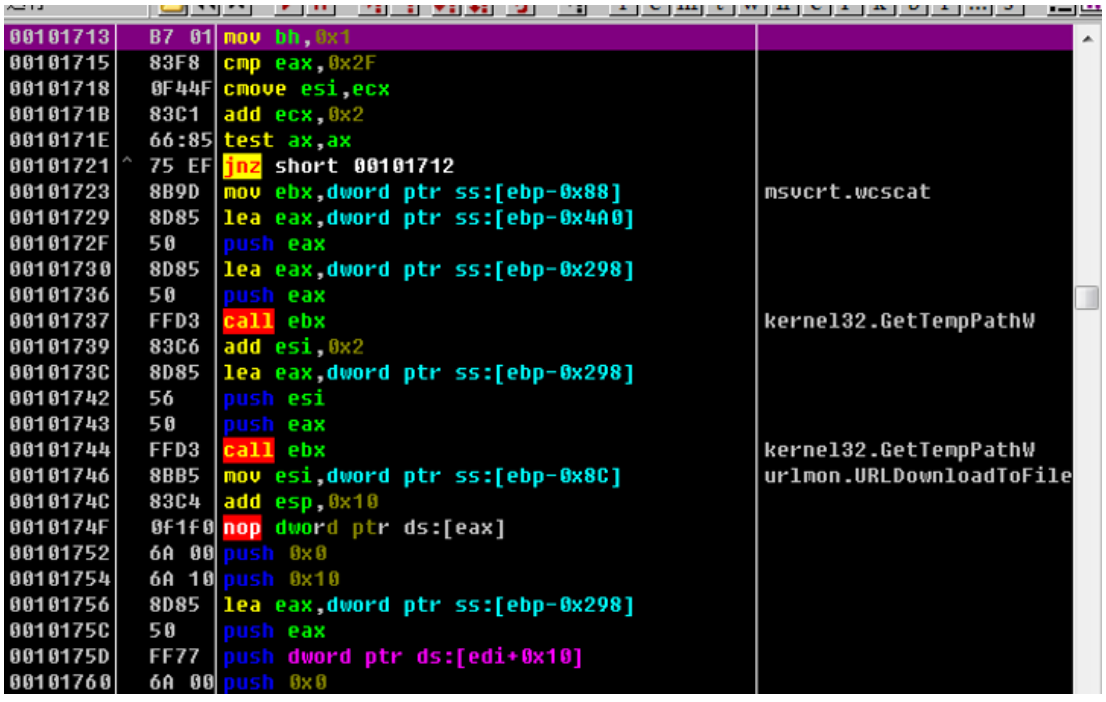


如果 shellcode 是在 IE 进程中执行，即第一次执行该 shellcode 时，shellcode 会调用 winHttpOpen 和 WinHttpGetProxyForUrl 来触发 WPAD 服务加载远程的 pac 文件执行，这个文件实际上还是包含 CVE-2020-0674 漏洞的 js 脚本。

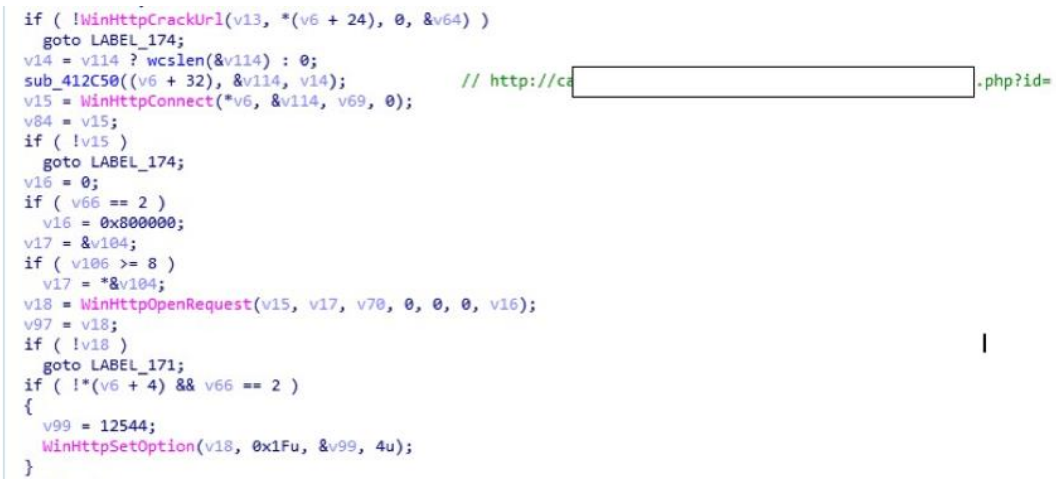




当 shellcode 得到第二次执行，发现当前进程名为 svchost.exe，已经成功从浏览器进程跨越到 WPAD 服务进程时，就开始执行另外一个流程，下载远程的木马文件释放到 temp 目录下并执行该程序。



最终的木马程序会接受固定 URL 地址的 C&C 命令，在受害者计算机中执行任意操作。



修复建议

目前火狐浏览器已经发布了 Firefox 72.0.1 and Firefox ESR 68.4.1，我们建议所有的火狐浏览器用户更新到最新版本。

针对 Windows 系统的用户，我们建议 Windows 10 系统用户尽快更新 2020 年 2 月份的微软安全补丁，而 Windows 7 系统用户可以使用 360 Win7 盾甲产品阻止“双星”0day 漏洞攻击。

参考

https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674