

丢人丢到国外去了，国内定制版Flash被国外安全厂商撕开了面纱！

IT之家 [莫理](#)



关注莫理！每天获取稀奇古怪的好东西

//

众所周知，目前以色列是仅次于美国的全球第二大网络安全产品和服务出口国。以色列国防军其在精英网络部队退伍人员在 2004 年成立了一家安全公司，名为 Minerva Labs，是以色列众多安全公司之一。

据 Minerva Labs

官方公告，他们的研究团队在过去一段时间中收到了大量关于“FlashHelperService.exe”可执行文件的恶意代码警报，而思科旗下的 Talos Intelligence 已将 FlashHelperService.exe 列为 2021 年 1 月最常见的威胁之一。

Title: Cisco urges users to update to new routers after vulnerabilities disclosed

Description: Cisco disclosed 74 vulnerabilities in some of its RV series of wireless routers last week, urging users to purchase new hardware rather than patching them. The vulnerabilities all exist in products that have already reached their end-of-life. The affected devices include the Cisco Small Business RV110W, RV130, RV130W and RV215W systems, which could all be use as firewalls, VPNs or standard routers. All of the vulnerabilities require that an attacker has login credentials for the targeted device, and therefore are not easily exploitable. This should give users a small runway to upgrade to new gear.

Snort SIDs: 56839 – 56845, 56866 – 56876, 56893, 56894

[Most prevalent malware files this week](#)

SHA 256: [8cb8e8c9fafa230ecf2f9513117f7679409e6fd5a94de383a8bc49fb9cdd1ba4](#)

MD5: 176e303bd1072273689db542a7379ea9

Typical Filename: FlashHelperService.exe

Claimed Product: Flash Helper Service

Detection Name: W32.Variant.24cl.1201

为了弄清楚这个程序究竟是不是恶意程序，他们开始对其反编译，试图从二进制文件中查询真相。

该文件是由“重橙网络”签名的，而“重橙网络”则是 Adobe 在中国的战略合作伙伴，负责 Flash 在中国的独家官方发行，以及对 Flash 中国版的后续支持。不过，Adobe 网站上已经有许多关于该公司及其软件的投诉。



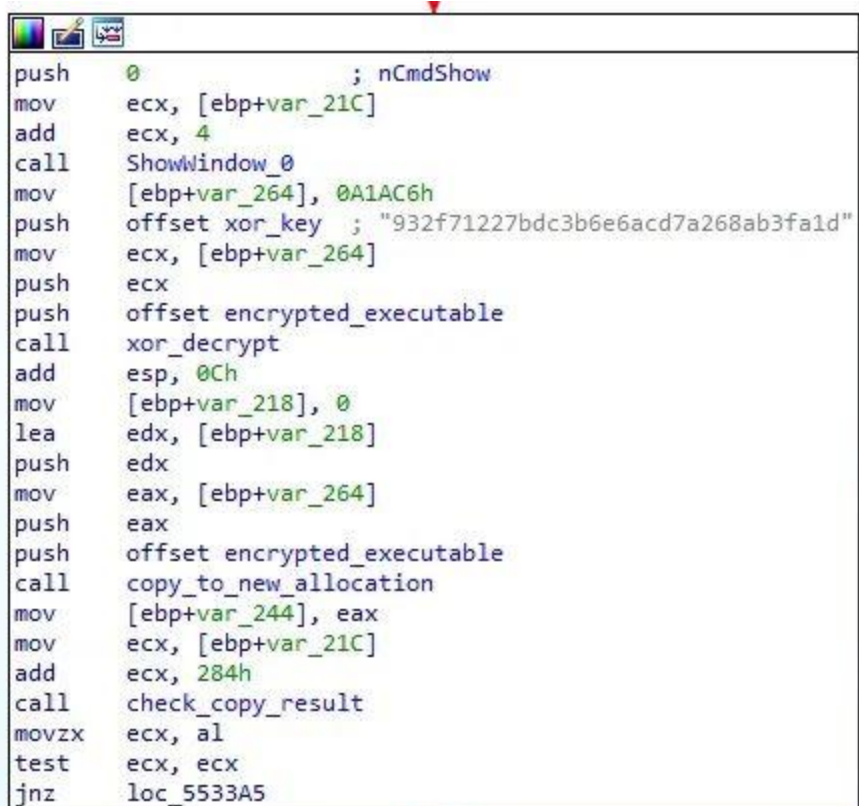
通过对重橙网络发行的中国特供版 Flash Player 附带的这一文件进行解包，研究人员最终在程序里发现了一些嫌疑代码。

emmm，戳一下趴！你的顺手将是我坚持的动力，万分感谢 🙏

👉 小卡片在此 👈

FlashHelperService 二进制文件包含一个嵌入式DLL，名为 ServiceMemTask.dll。这个 DLL 有一些奇怪的特性：

- 能够访问 flash.cn 网站、能够下载文件；
- 可以从网站上下载加密的 DLL 文件、以及解密和加载；
- 解密的二进制文件中存在许多分析工具的明文名称（未知）；
- 能够对操作系统进行概要分析，并将结果回传至服务器端。



```
push    0 ; nCmdShow
mov     ecx, [ebp+var_21C]
add     ecx, 4
call    ShowWindow_0
mov     [ebp+var_264], 0A1AC6h
push    offset xor_key ; "932f71227bdc3b6e6acd7a268ab3fa1d"
mov     ecx, [ebp+var_264]
push    ecx
push    offset encrypted_executable
call    xor_decrypt
add     esp, 0Ch
mov     [ebp+var_218], 0
lea     edx, [ebp+var_218]
push    edx
mov     eax, [ebp+var_264]
push    eax
push    offset encrypted_executable
call    copy_to_new_allocation
mov     [ebp+var_244], eax
mov     ecx, [ebp+var_21C]
add     ecx, 284h
call    check_copy_result
movzx   ecx, al
test    ecx, ecx
jnz     loc_5533A5
```

```

aWindgbExe:      text "UTF-16LE", 'softice.exe',0
aWindgbExe:      text "UTF-16LE", 'windgb.exe',0
                  db  0
                  db  0
aOllydbgExe:      text "UTF-16LE", 'ollydbg.exe',0
                  db  22h ; "
                  db  0
                  db  0
                  db  0
aOllyiceExe:      text "UTF-16LE", 'ollyice.exe',0
                  db  22h ; "
                  db  0
                  db  20h
                  db  0
                  db  0
                  db  0
                  db  0
                  db  0
aWiresharkExe:    text "UTF-16LE", 'wireshark.exe',0
aCsnasExe:        text "UTF-16LE", 'csnas.exe',0
aHttpalyzerst:    text "UTF-16LE", 'httpalyzerstd',0
aTcpmonExe:       text "UTF-16LE", 'tcpmon.exe',0
                  db  0
                  db  0
aSmsniffExe:      text "UTF-16LE", 'smsniff.exe',0
aNetworktraffic:  text "UTF-16LE", 'networktrafficview.exe',0
                  db  0
                  db  0
aHookmeExe:       text "UTF-16LE", 'hookme.exe',0
                  db  0
                  db  0
aSmartsniffExe:

```

此外，安全研究人员还发现该程序与内存有效负载与硬编码网址（[https://cloud.flash\[.\]dcb](https://cloud.flash[.]dcb)）有联系，并可以使用 XOR 编码密钥“932f71227bdc3b6e6acd7a268ab3fa1d”解密它下载的数据。

之后它输出的是一个混淆的 json 文件，它将充当服务器的作用：

```

debug150:00621228 aC96c2464c510Cc db '{',0Ah ; DATA XREF: Stack[00002194]:000FF
debug150:00621228 db ' "c96c2464c51" : "0",',0Ah
debug150:00621228 db ' "cc6d08273a8" : "2",',0Ah
debug150:00621228 db ' "d5052d494f1" : "08338C889E762B4001448D7F4DC1E2D2",',0Ah
debug150:00621228 db ' "dd893e56427" : 60,',0Ah
debug150:00621228 db ' "e6e3390f9bc" : "1",',0Ah
debug150:00621228 db ' "ee96cd4fa2f" : [' ,0Ah
debug150:00621228 db ' {' ,0Ah
debug150:00621228 db ' "a0ad825bb41" : 0,',0Ah
debug150:00621228 db ' "b4bd046cde2" : "" ,',0Ah
debug150:00621228 db ' "ccafb352bb3" : "https://cloud.flash.cn/fw/cz/tt.eae",',0Ah
debug150:00621228 db ' "d072df43184" : "29D8EE9B4FF07D197ADF94757E3F450E",',0Ah
debug150:00621228 db ' "e35e94f6803" : "d9cb8d46c5d6121e054a7578e0784651"',0Ah
debug150:00621228 db ' }',0Ah
debug150:00621228 db ' ]',0Ah
debug150:00621228 db ' }',0Ah,0

```

- ccafb352bb3 是下一个有效负载的网址。
- d072df43184 是加密有效负载的 MD5。
- e35e94f6803 是有效负载的 3DES 密钥。

DLL文件链接到某个网站，它可以下载文件“tt.eae”到模块主目录（C:\Users\Username\AppData\LocalLow\AdobeFlash\Flash Cfg）。

在解密和解压 (7zip)后，则得到了一个内部名为“tt.zip”的 PE 文件，DLL 再将其加载执行。

为了确定真相，研究人员从flash.cn下载了官方Flash安装程序（由 Adobe 签名）。

```
C:\Users\timi\Downloads\flashplayerax_install_cn_win8(1).exe:
Verified:      Signed
Signing date:  12:21 PM 1/4/2021
Publisher:     Adobe Inc.
Company:       Adobe Inc
Description:    Adobe Download Manager
Product:       Adobe Download Manager
Prod version:  3.0.0.579s
File version:  3.0.0.579s
MachineType:   32-bit
MD5:           9B33023CF86AD06ED699AAB10100DD30
SHA1:          36AA0607221EDF87B44B78B92D86DA3FF298EDE0
PESHA1:        94CD92D221D2A1ABE18F7925B79F517505C167C0
PE256:         534AA83768C6045CC622B15934DAA18285A457DA674790095C24CD4F6B7F3F11
SHA256:        94D1B8ED7E1CC785B8D6613B875D10890F93CE64E1C50A17D48C41139AD3F959
IMP:           0B2F7445F02CFF44B10BB9E8CD71C3C0
```

使用此二进制文件安装Flash之后，研究人员确定安装了附带的服务，经过进一步的逆向工程之后，他们设法下载并解密了该程序想要弹出的窗口，并生成了内部名为“nt.dll”的二进制文件。

最终发现，FlashHelperService中加载的这个文件，将以预定的时间戳打开一个令人讨厌的弹出窗口。也就是说，此文件的最终意图类似广告程序，想让用户在一定时间打开（或后天打开）某个网站进行推广。



Minerva Labs 指出，对于宣称要对 Flash Player 提供后续更新支持的服务提供商来说，大费周章地设计一个如此“灵活”的层层套壳的框架仅仅是为了插播广告，似乎显得浪费（多余），并且还导致用户电脑产生安全隐患。

据介绍，该程序会调用Windows API函数ShellExecuteW来打开Internet Explorer，其 URL 则是从另一个加密的json获取的，这堪称“多余”。

```

v12 = 0;
pszPath = 0;
memset(v11, 0, sizeof(v11));
SHGetSpecialFolderPath(0, &pszPath, 0x26, 0); // 0x26=CSIDL_PROGRAM_FILES
//
std::string::string((std::string *)path_to_program_files, (const char *)&pszPath);
LOBYTE(v12) = 1;
strcat_probably(
    (int)iexplore_path,
    (Concurrency::details::CancellationTokenRegistration *)path_to_program_files,
    (wchar_t *)L"\\Internet Explorer\\iexplore.exe");
v1 = (const WCHAR *)some_strlib_func(iexplore_path);
is_iexplorer_exists = 1;
hFile_iexplore = CreateFileW(v1, 0x80000000, 1u, 0, 3u, 0, 0);
if ( hFile_iexplore == (HANDLE)-1 )
    is_iexplorer_exists = 0;
CloseHandle(hFile_iexplore);
if ( is_iexplorer_exists )
{
    string_cusrom_url = (const WCHAR *)some_strlib_func(&url_from_json);
    string_iexplore_path = (const WCHAR *)some_strlib_func(iexplore_path);
    ShellExecuteW(0, L"open", string_iexplore_path, string_cusrom_url, 0, 1);
    v4 = 1;
}
}

```

此外，该文件包含通用的二进制分发框架可被攻击者用于加载恶意代码，从而有效绕过传统的 AV 磁盘签名检查，尤其是目前许多政企机关和事业单位都会安装 Flash，如果真的因为这个“小聪明”导致被不法分子恶意入侵，则后果不堪设想。



*声明：本文转载自IT之家，有删改，不代表本公众号观点。

歌事故里

周杰伦《花海》官方版

由网友“Jay”点歌

视频来源：腾讯视频

可能喜欢

[绝了！这才是真正的万能绿色便携软件！](#)

[那些年设置的奇葩密码，终于有救了...](#)

[这个小程序让Windows更人性化了！](#)

[看小说，音乐，漫画，视频的神器！](#)

[软件大厂开发的这些良心APP！](#)

[国家级平台！各类资源免费下载！](#)

顺手点下小卡片叭