APT37 위협 배후의 사이버 정찰 활동 분석

Genians ⋮⋮ 11/6/2024

Analysis of Cyber Recon Activities Behind APT37 Threat Actor

◈ 주요 요약 (Executive Summary)

- 국가배후 APT37 그룹의 은밀한 사이버 정찰 활동 분석
- 공격 타깃의 IP주소(위치정보), 웹 브라우저, 운영체제 등 정보 수집
- 바로가기(lnk) 악성파일을 주요 전략으로 사용하던 위협 주체
- 단말 보안 강화를 위한 이상 행위 탐지대응 솔루션(EDR) 적극 도입 필요

1. 개요 (Overview)

○ 국가배후 사이버 안보 위협군으로 알려진 APT37 그룹은 대한민국을 상대로 다양한 사이버 첩보활동을 주도하고 있습니다. 주로 북한인권단체, 탈북민, 북한취재 기자나 통일·국방·외교안보 및 대북분야 전문가와 교수 등이 대상입니다.

○ '지니언스 시큐리티 센터(GSC)'는 APT37 캠페인 유형별 여러 CTI 분석 보고서를 발간한 바 있습니다. 대표적으로 △북한인권단체 사칭, △macOS 이용자 공격, △CVE-2022-41128 취약점, △RoKRAT 분석 사례 등입니다.

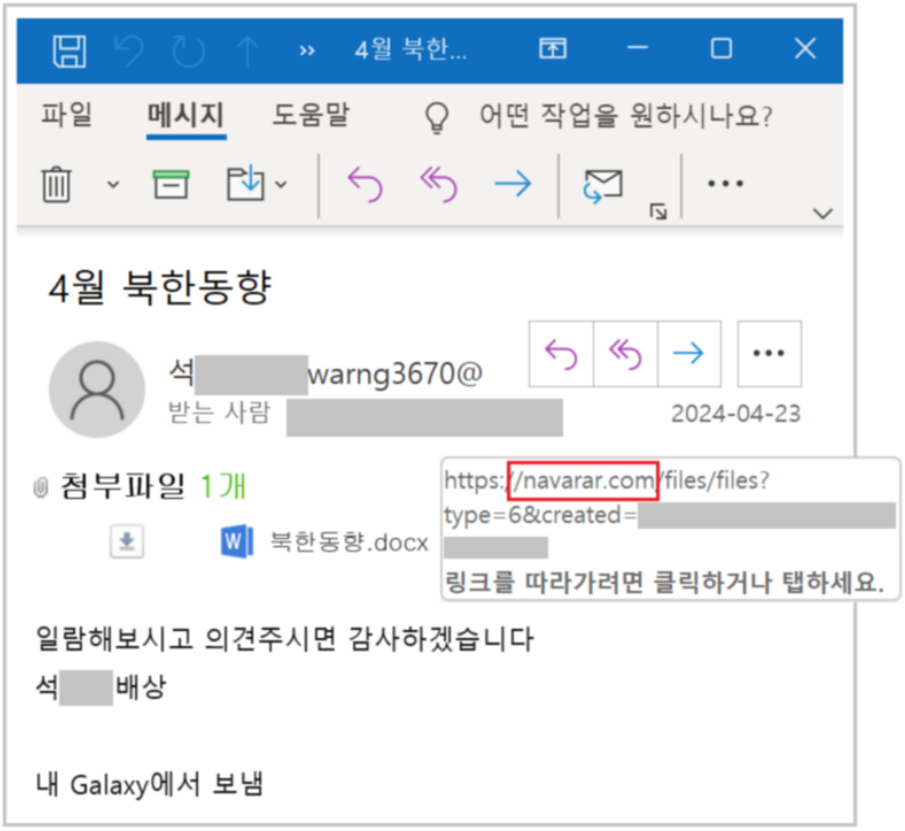
○ 위협 행위자들은 성공적인 단말 침투를 위해 주요 Anti-Virus 기반 시그니처 탐지 회피에 관심이 큽니다. GSC는 그들의 활동을 모니터링 중 흥미로운 행동패턴을 발견했습니다.

○ 미리 준비된 위협 인프라를 통해 사전정찰을 반복 수행하였고, 필요한 기초정보를 수집하였습니다. 이러한 공격전술에 적절히 대응하기 위해 단말 이벤트 흐름을 수집 분석하고 기존에 알려지지 않은 이상행위

자체를 폭 넓게 분석하고 판단할 수 있는 Endpoint Detection and Response (EDR) 구축이 요구되는 추세입니다.

2. 배경 (Background)

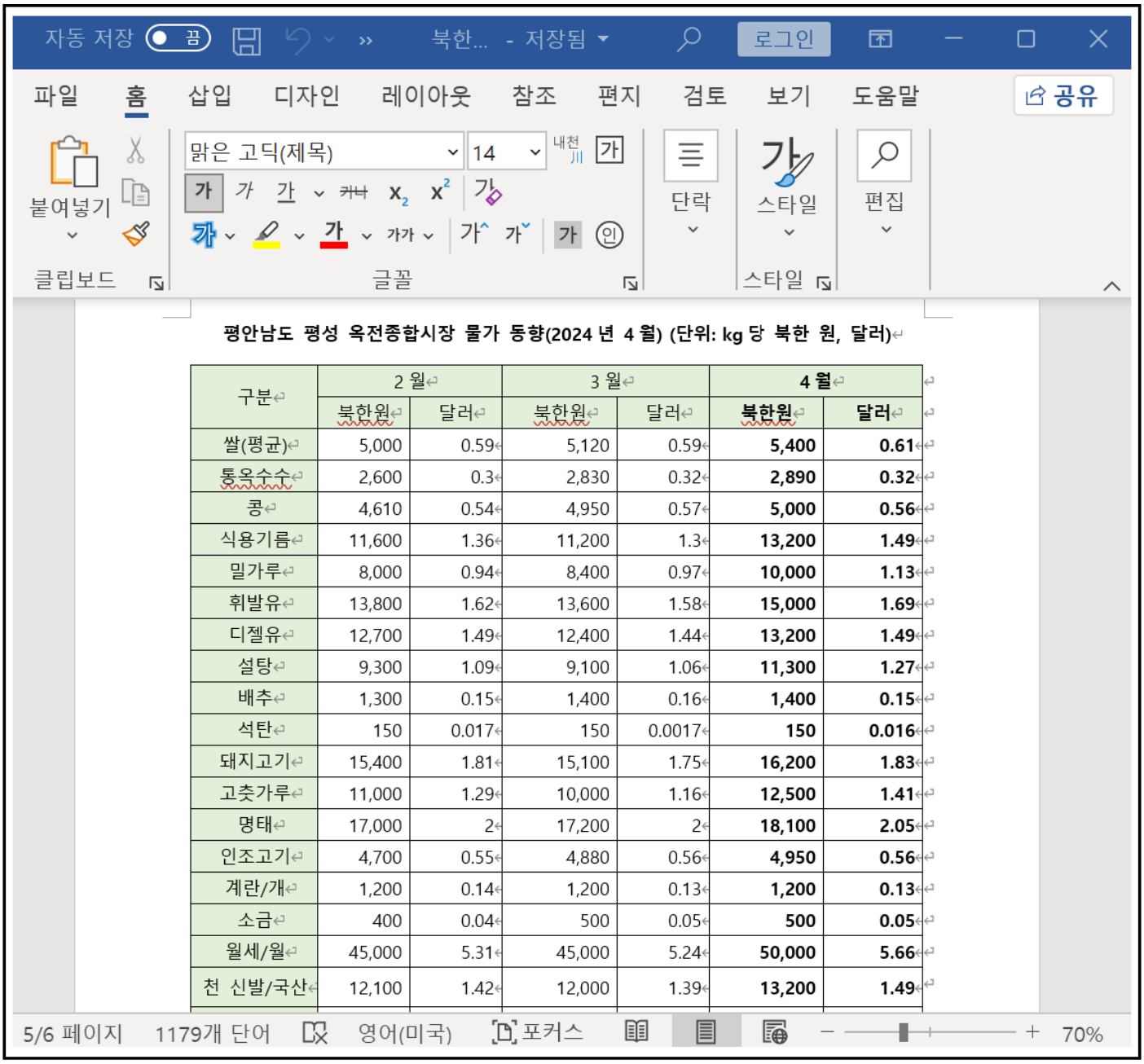
○ 먼저 지난 4월에 발견된 사례를 살펴보고자 합니다. 당시 공격은 특정 공직자 출신 신분의 현직 대학교수 명의로 발송된 것처럼 위장됐습니다. '4월 북한동향' 제목의 이메일과 '북한동향.docx' 문서가 첨부된 것처럼 디자인이 구성됐습니다. 이메일 발신지는 '61.97.243[.]2' VPN 아이피 주소가 사용됐습니다.



[그림 1] '북한동향' 문서로 위장한 공격 사례

○ 화면에 보이는 문서파일은 이메일에 직접 첨부된 형태가 아니라, 국내 포털사 도메인과 흡사하게 만들어진 'navarar[.]com' 주소에서 악성파일이 유포됐습니다. 이곳을 통해 다운로드된 압축내부의 '북한동향.lnk' 파일은 전형적인 바로가기 유형의 악성코드 입니다.

○ 해당 바로가기 파일 내부에는 이용자를 속이기 위한 '북한동향.docx' 이름의 정상문서와 악의적인 PowerShell 커맨드 명령이 포함돼 있습니다. 정상문서에는 실제로 북한의 4월달 동향정보가 포함돼 있습니다.

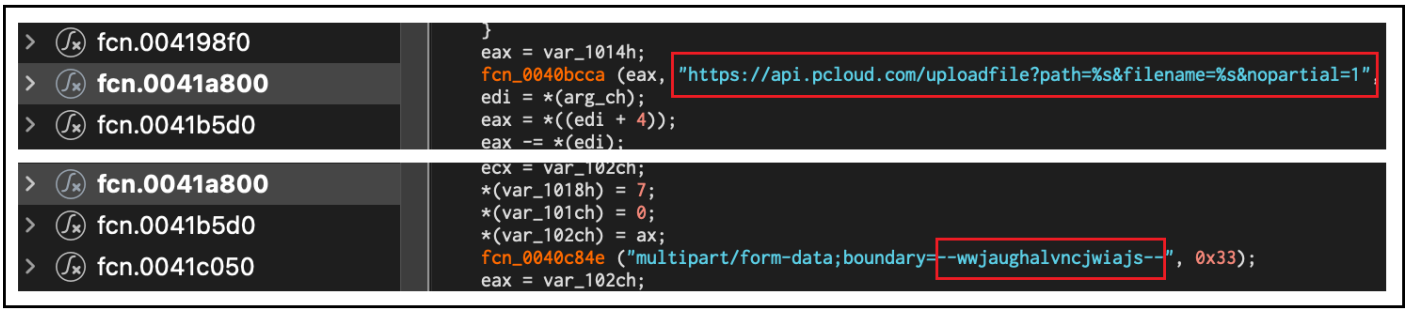


평안남도 평성 옥전종합시장 물가 동향(2024 년 4 월) (단위: kg 당 북한 원, 달러)

구분	2 월		3 월		4 월	
	북한원	달러	북한원	달러	북한원	달러
쌀(평균)	5,000	0.59	5,120	0.59	**5,400**	**0.61**
통옥수수	2,600	0.3	2,830	0.32	**2,890**	**0.32**
콩	4,610	0.54	4,950	0.57	**5,000**	**0.56**
식용기름	11,600	1.36	11,200	1.3	**13,200**	**1.49**
밀가루	8,000	0.94	8,400	0.97	**10,000**	**1.13**
휘발유	13,800	1.62	13,600	1.58	**15,000**	**1.69**
디젤유	12,700	1.49	12,400	1.44	**13,200**	**1.49**
설탕	9,300	1.09	9,100	1.06	**11,300**	**1.27**
배추	1,300	0.15	1,400	0.16	**1,400**	**0.15**
석탄	150	0.017	150	0.0017	**150**	**0.016**
돼지고기	15,400	1.81	15,100	1.75	**16,200**	**1.83**
고춧가루	11,000	1.29	10,000	1.16	**12,500**	**1.41**
명태	17,000	2	17,200	2	**18,100**	**2.05**
인조고기	4,700	0.55	4,880	0.56	**4,950**	**0.56**
계란/개	1,200	0.14	1,200	0.13	**1,200**	**0.13**
소금	400	0.04	500	0.05	**500**	**0.05**
월세/월	45,000	5.31	45,000	5.24	**50,000**	**5.66**
천 신발/국산	12,100	1.42	12,000	1.39	**13,200**	**1.49**

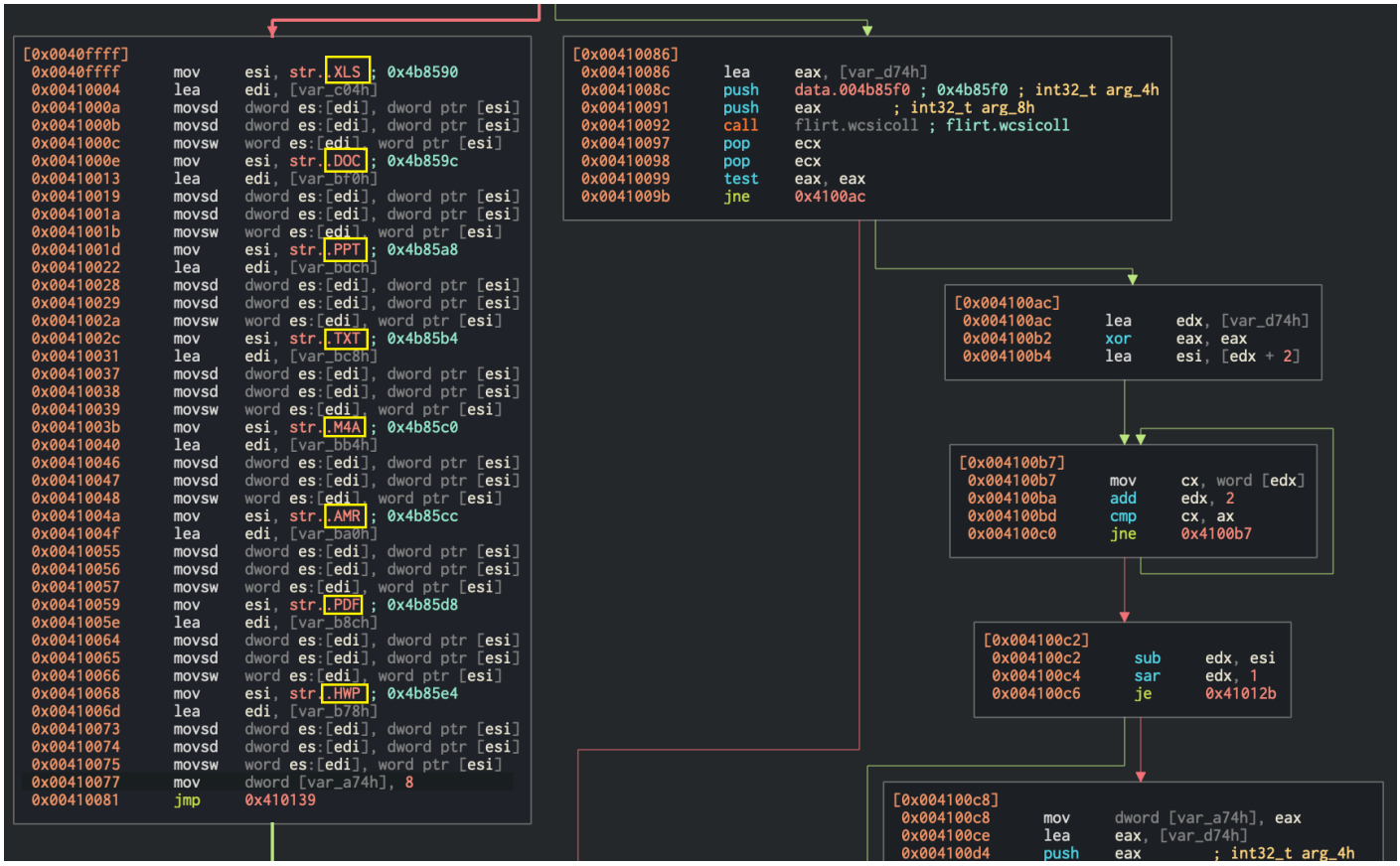
[그림 2] 공격에 사용된 정상문서 내용

○ lnk 파일을 분석해 보면, 내부에 XOR 로직으로 암호화된 RoKRAT 악성모듈이 숨겨져 있습니다. APT37 의 전형적인 pCloud API 통신 기술과 '--wwjaughalvncjwiajs—' 문자열 값이 포함된 것도 볼 수 있습니다.



[그림 3] RoKRAT 악성모듈 코드 분석 내용

○ 더불어 이용자 단말에서 다양한 문서와 스마트폰 녹음파일 확장자를 검색 수집하는 기능도 동일하게 포함되어 있습니다.



[그림 4] 단말 정보 수집 기능 화면

○ 유출 대상 확장자는 하기와 같습니다.

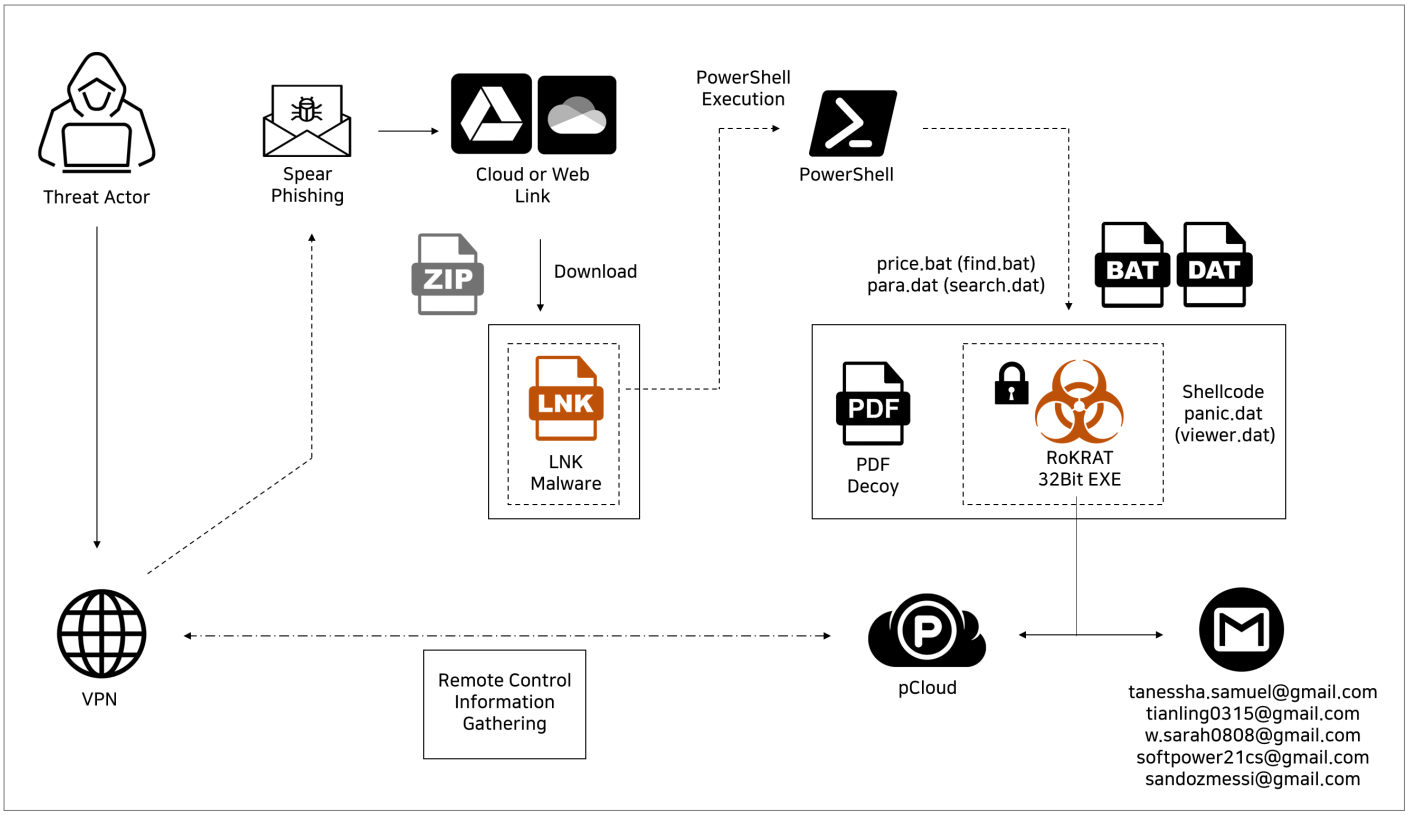
- .XLS
- .DOC
- .PPT
- .TXT
- .M4A
- .AMR
- .PDF
- .HWP

3. 유사 악성프로그램 (Similar malware)

○ 앞서 설명한 배경처럼, 지난 4월에는 다수의 바로가기(lnk) 파일에 의해 RoKRAT 모듈이 유포됐습니다.

○ 발견된 주요 파일명으로 △설비목록.lnk △동북공정(미국의회조사국(CRS Report).lnk △Gate access roster 2024.lnk △국가정보 아카데미 8기 통합과정 수료증(최종본).lnk 등이 있습니다.

○ 각 lnk 파일 내부에는 'panic.dat' 또는 'viewer.dat' 이름으로 숨겨진 RoKRAT 모듈이 숨겨져 있습니다. 여러가지 변종에 따라 'price.bat'(또는 'find.bat'), 'para.dat'(또는 'search.dat') 파일을 통해 호출이 진행됩니다. 물론, 그 이전 시점에는 'public.dat', 'docu1.dat' 등 다양한 파일명이 사용된 바 있습니다.

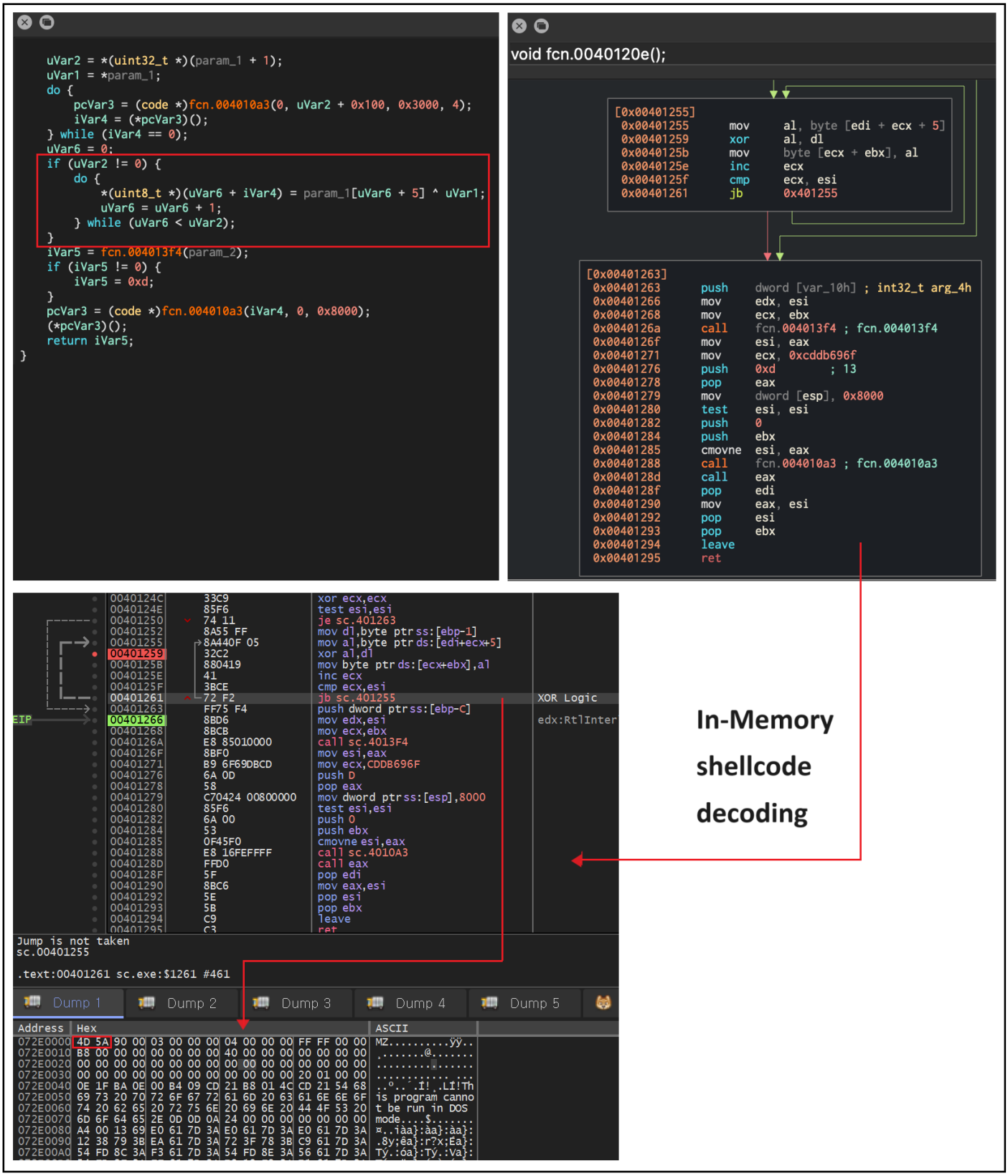


[그림 4-1] 위협 흐름도

○ 위협 행위자는 구글 지메일 계정을 이용해 클라우드 서비스에 가입하는 특성을 보이기도 합니다. 식별됐던 대표적인 이메일 계정은 다음과 같습니다.

- tanessha.samuel@gmail.com
- tianling0315@gmail.com
- w.sarah0808@gmail.com
- softpower21cs@gmail.com
- sandozmessi@gmail.com

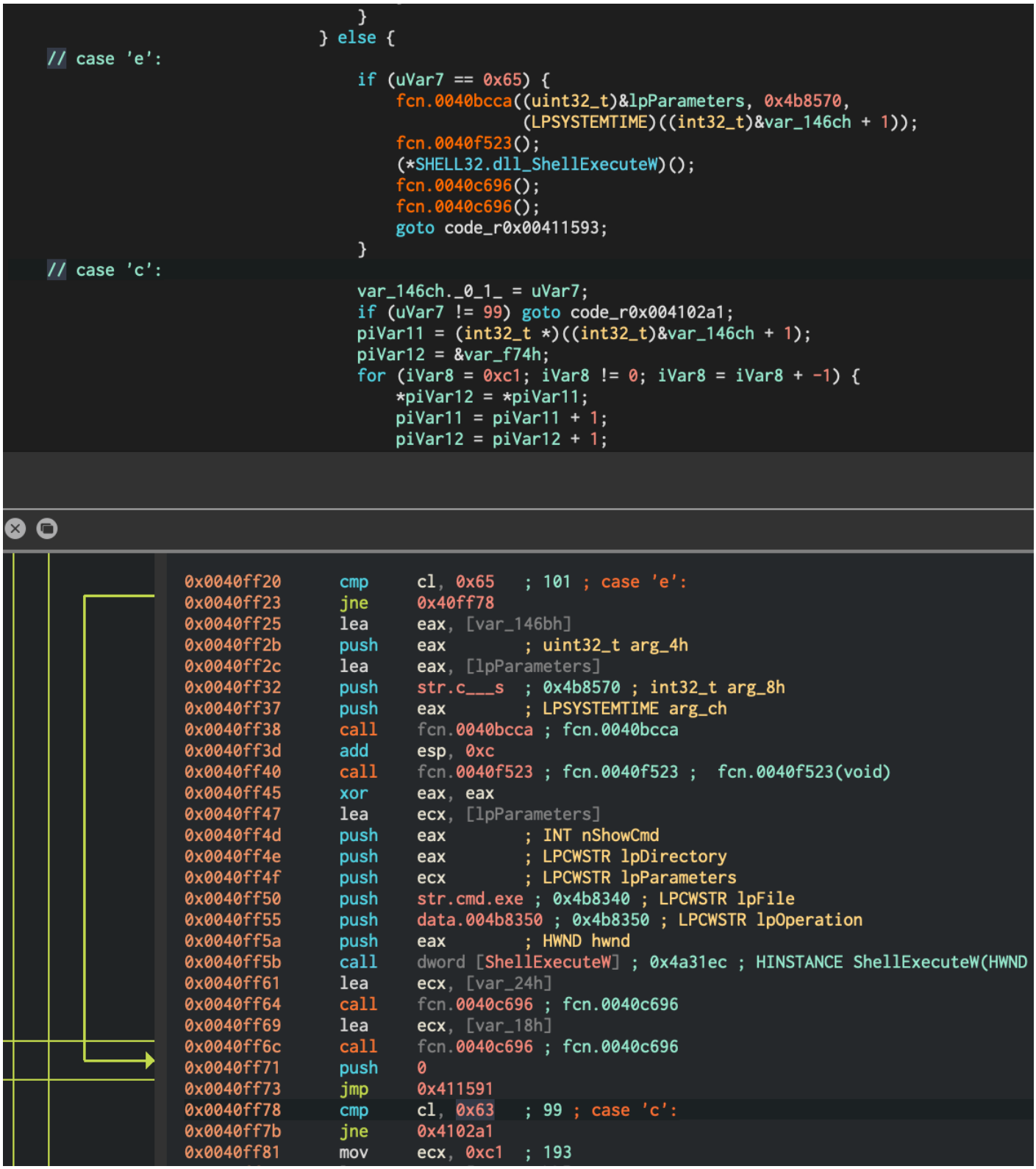
○ 'panic.dat' 파일은 Shellcode 루틴을 통해 암호화된 RoKRAT 모듈이 실행됩니다.



[그림 4-2] Shellcode 디코딩 화면

○ 주 스레드 실행 중에 RoKRAT 명령어는 피해 시스템을 제어하는 데 사용되며, case 조건문에 따라 다양한 기능을 수행합니다.

○ 예를들면 '-e' 조건은 ShellExecuteW 함수를 통해 'cmd.exe' 커맨드 명령을 호출하고, '-c' 조건은 앞서 설명한 특정 문서와 녹음 확장자의 파일을 수집해 C2 서버로 유출합니다.



```
                        }
                    } else {
// case 'e':
                        if (uVar7 == 0x65) {
                            fcn.0040bcca((uint32_t)&lpParameters, 0x4b8570,
                                         (LPSYSTEMTIME)((int32_t)&var_146ch + 1));
                            fcn.0040f523();
                            (*SHELL32.dll_ShellExecuteW)();
                            fcn.0040c696();
                            fcn.0040c696();
                            goto code_r0x00411593;
                        }
// case 'c':
                        var_146ch._0_1_ = uVar7;
                        if (uVar7 != 99) goto code_r0x004102a1;
                        piVar11 = (int32_t *)((int32_t)&var_146ch + 1);
                        piVar12 = &var_f74h;
                        for (iVar8 = 0xc1; iVar8 != 0; iVar8 = iVar8 + -1) {
                            *piVar12 = *piVar11;
                            piVar11 = piVar11 + 1;
                            piVar12 = piVar12 + 1;
```

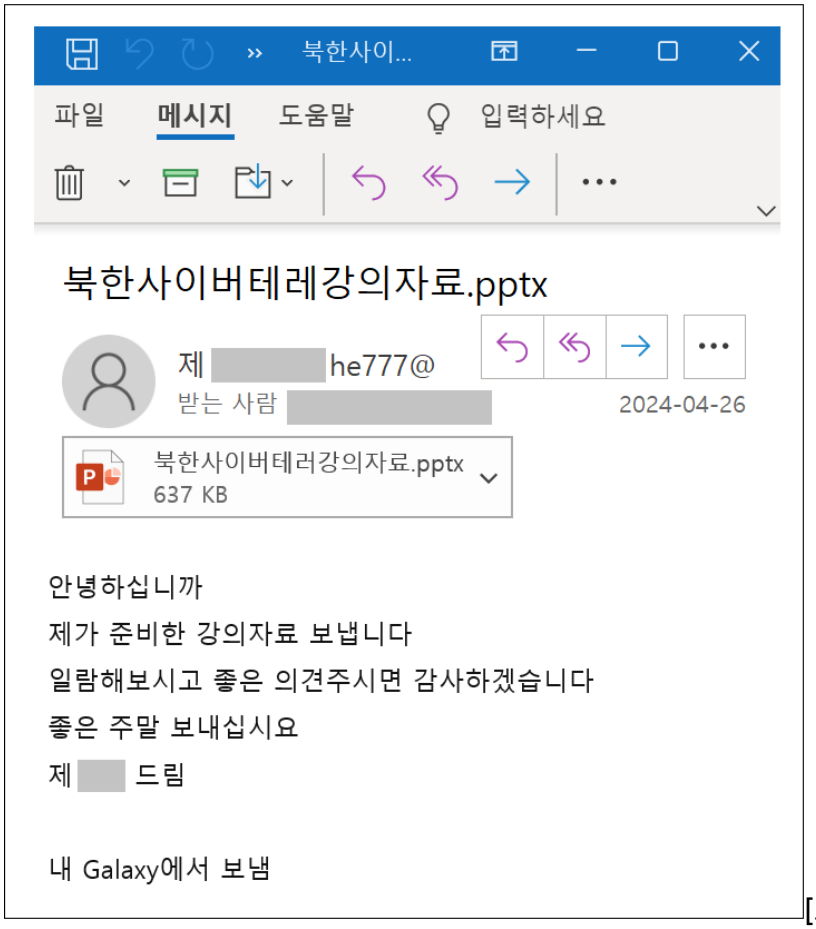
```
0x0040ff20      cmp     cl, 0x65    ; 101 ; case 'e':
0x0040ff23      jne     0x40ff78
0x0040ff25      lea     eax, [var_146bh]
0x0040ff2b      push    eax         ; uint32_t arg_4h
0x0040ff2c      lea     eax, [lpParameters]
0x0040ff32      push    str.c___s   ; 0x4b8570 ; int32_t arg_8h
0x0040ff37      push    eax         ; LPSYSTEMTIME arg_ch
0x0040ff38      call    fcn.0040bcca ; fcn.0040bcca
0x0040ff3d      add     esp, 0xc
0x0040ff40      call    fcn.0040f523 ; fcn.0040f523 ;  fcn.0040f523(void)
0x0040ff45      xor     eax, eax
0x0040ff47      lea     ecx, [lpParameters]
0x0040ff4d      push    eax         ; INT nShowCmd
0x0040ff4e      push    eax         ; LPCWSTR lpDirectory
0x0040ff4f      push    ecx         ; LPCWSTR lpParameters
0x0040ff50      push    str.cmd.exe ; 0x4b8340 ; LPCWSTR lpFile
0x0040ff55      push    data.004b8350 ; 0x4b8350 ; LPCWSTR lpOperation
0x0040ff5a      push    eax         ; HWND hwnd
0x0040ff5b      call    dword [ShellExecuteW] ; 0x4a31ec ; HINSTANCE ShellExecuteW(HWND
0x0040ff61      lea     ecx, [var_24h]
0x0040ff64      call    fcn.0040c696 ; fcn.0040c696
0x0040ff69      lea     ecx, [var_18h]
0x0040ff6c      call    fcn.0040c696 ; fcn.0040c696
0x0040ff71      push    0
0x0040ff73      jmp     0x411591
0x0040ff78      cmp     cl, 0x63    ; 99 ; case 'c':
0x0040ff7b      jne     0x4102a1
0x0040ff81      mov     ecx, 0xc1   ; 193
```

[그림 4-3] RoKRAT 조건문에 따른 수행 함수

○ 유출 대상 확장자는 앞서 배경에서 설명한 것과 동일합니다.

4. 정찰 시나리오 (Recon Scenario)

○ 앞서 기술한 '4월 북한동향' 제목의 스피어 피싱 공격 발생 이후 약 3일 후에 새로운 정찰활동이 수행됩니다.



[그림 5] 정찰 활동으로 쓰인 이메일 모습

○ 이메일 제목에는 오타가 포함되어 있으며, 첨부파일명을 제목으로 기재하는 과정에서 실수를 한 것으로 보입니다. 첨부파일로 포함된 '북한사이버테러강의자료.pptx' 파일은 정상적인 문서파일 입니다.

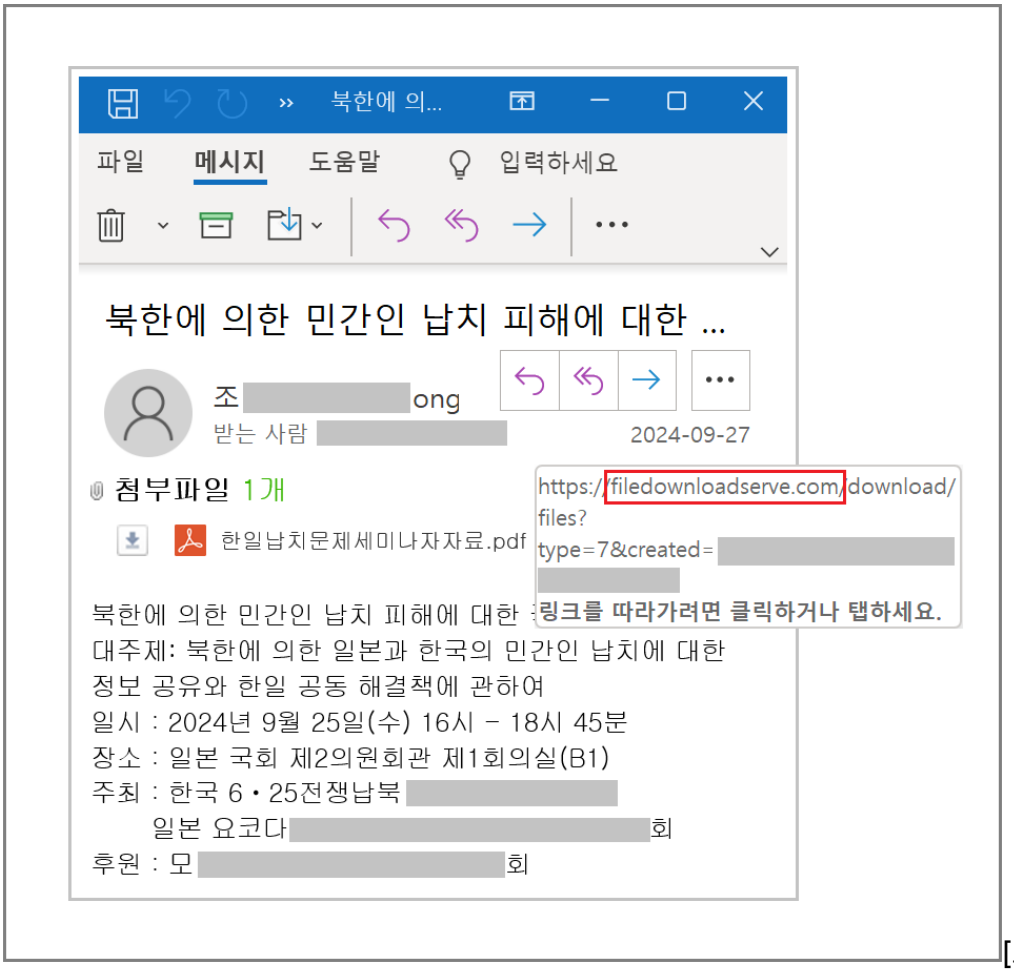
○ 흥미롭게도 lnk 악성파일 유포에 사용된 이메일 본문과 동일한 문장이 포함돼 있습니다.

날짜	2024-04-23	2024-04-26
이메일 제목	4월 북한동향	북한사이버테레강의자료.pptx
발신지 IP	61.97.243[.]2 [KR]	61.97.243[.]2 [KR]
본문 비교 (일부)	일람해보시고 의견주시면 감사하겠습니다 내 Galaxy에서 보냄	제가 준비한 강의자료 보냅니다 일람해보시고 좋은 의견주시면 감사하겠습니다 내 Galaxy에서 보냄
첨부파일명	북한동향.docx	북한사이버테러강의자료.pptx
공격 전략	lnk 바로가기 악성파일 전달	정상 pptx 문서 전달
명령제어(C2)	navarar[.]com 158.247.249[.]129 [KR]	N/A N/A

[표 1] 이메일 내용 비교

○ 발신지 아이피 뿐만 아니라, 이메일 본문 표현도 동일한 부분이 사용됐습니다. 이처럼 위협 행위자는 악성파일만 전달하는 것이 아닙니다. 정상내용을 보내 의심도를 낮추거나, 회신을 유도하여 후속 공격을 준비합니다. 이러한 정찰활동을 통해 초기 침투에 필요한 주변 정보 수집을 할 수 있습니다.

○ 한편, 9월 27일에는 '북한에 의한 민간인 납치 피해에 대한 국제 심포지엄' 제목의 이메일이 다수 유포됐습니다. 해당 이메일에는 '한일납치문제세미나자자료.pdf' 문서가 첨부된 것처럼 보입니다. 그리고 이메일이 발송된 곳은 '108.181.50[.]58' VPN 주소로 확인이 됩니다.



[그림 6] 한일납치문제 세미나 자료 첨부 위장 정찰 모습

○ 하지만, 해당 메일은 '4월 북한동향' 제목 사례와 같이 특정 서버로 링크된 파일입니다. 연결된 곳은 'filedownloadserve[.]com' 도메인이며, Passive DNS 이력으로 2개의 아이피가 사용됐습니다.

Domain 주소	IP 주소	국가 코드
filedownloadserve[.]com	158.247.219[.]10	[KR]
	141.164.60[.]110	[KR]
kakaofilestorage[.]com	158.247.219[.]10	[KR]
	141.164.62[.]19	[KR]

[표 2] C2 서버 정보

○ 특히, 이메일이 발송된 '108.181.50[.]58' VPN 주소의 경우 'UN 안전보장이사회 보고서(Security Council Report)' 567 페이지에 북한 연계 가상자산 위협활동 의심 IP 주소로 언급된 바 있습니다.

○ 참고로 동일 위협 행위자가 2023년에 사용했던 아이피 대역이 유사한 것을 알 수 있습니다. 하기 아이피들은 실제 공격에 활용됐던 중요한 지표이지만, 시계열 시점상 휘발성 특성도 고려해야 합니다.

108.181.50[.]58 108.181.52[.]169

108.181.52[.]229 108.181.52[.]231
108.181.52[.]234 108.181.52[.]235
108.181.52[.]236 N/A

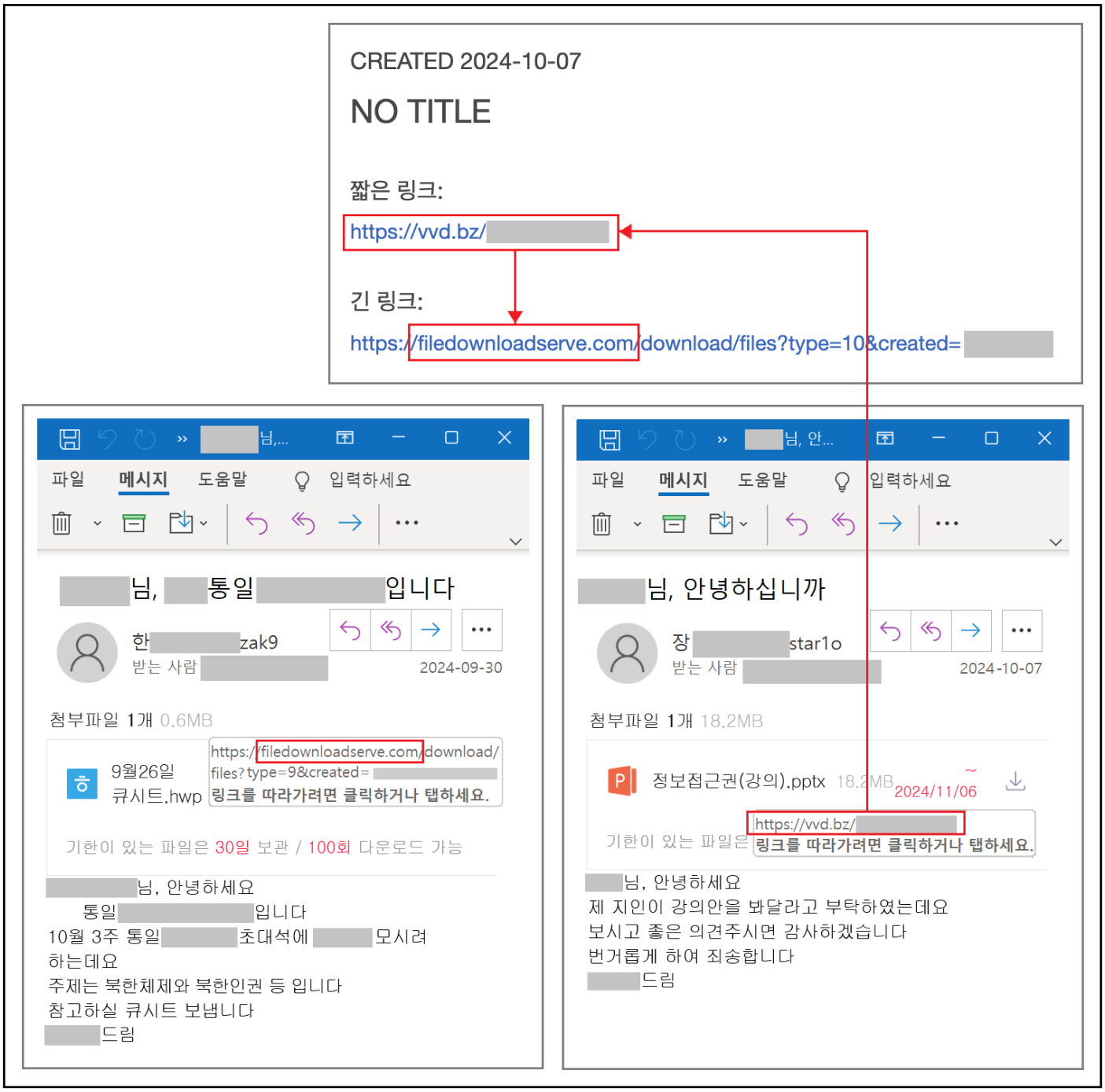
[표 3] 2023년 식별된 아이피 대역들

○ 한편, 지난 4월과 9월에 발견된 첨부파일 링크 주소를 비교해 보면, 도메인 주소는 변경됐지만 통신 인자값이 동일한 패턴인 점을 알 수 있습니다.

2024-04-23 (APT37 RoKRAT)	**2024-09-27**
북한동향.docx	한일납치문제세미나자자료.pdf
navarar[.]com/files/ files?type=(Count) &created=(Base64 Email)	filedownloadserve[.]com/download/ files?type=(Count) &created=(Base64 Email)
158.247.249[.]129 [KR]	158.247.219[.]10 [KR]

[표 4] C2 인자값 비교

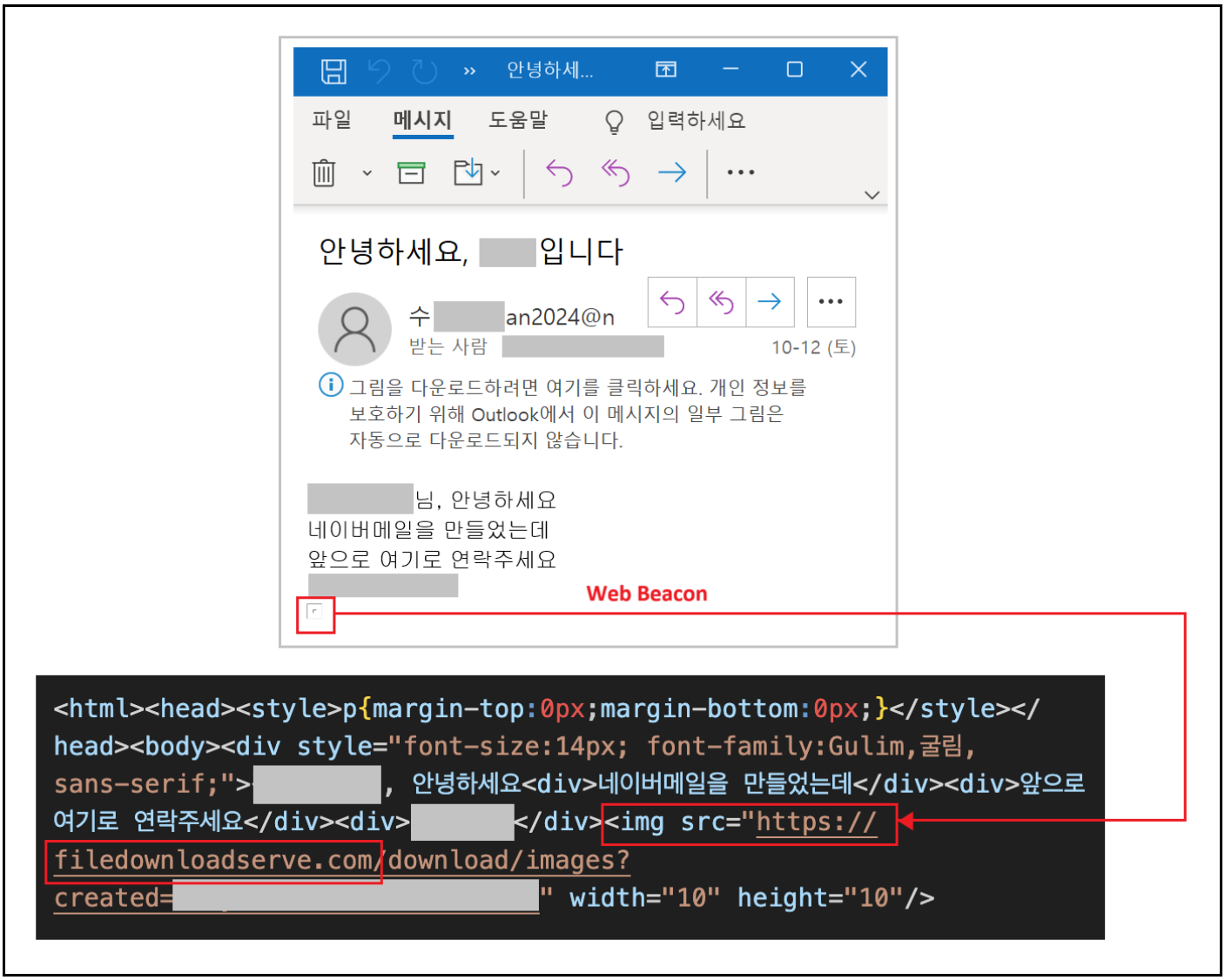
○ 이어서 9월 30일에는 마치 한국 방송사의 북한 관련 시사교양 프로그램 기자 또는 작가를 사칭해 정찰활동을 수행했습니다. 10월 7일에는 전 국가 공무원 출신 인물을 사칭해 강의안 검토요청처럼 접근을 시도합니다. 이때는 단축URL 서비스를 활용했지만 최종 연결 도메인은 동일합니다.



[그림 7] 통일 시사교양 프로그램 사칭 정찰활동

○ 그리고 10월 12일에는 첨부파일이나 링크를 포함하지 않은 형태의 정찰 방식을 사용합니다. 당시 위협 행위자는 북한인권 분야에서 활동하는 전문가로 위장했고, 새로 가입한 이메일 안내처럼 위장한 특징이 있습니다.

○ 이때는 별도의 링크나 첨부파일이 존재하지 않으며, 메일 본문 내부에 "img src" 태그를 삽입한 웹 비콘(Web Beacon) 정찰 방식을 사용합니다.



[그림 8] 웹 비콘 정찰 기술을 사용한 화면

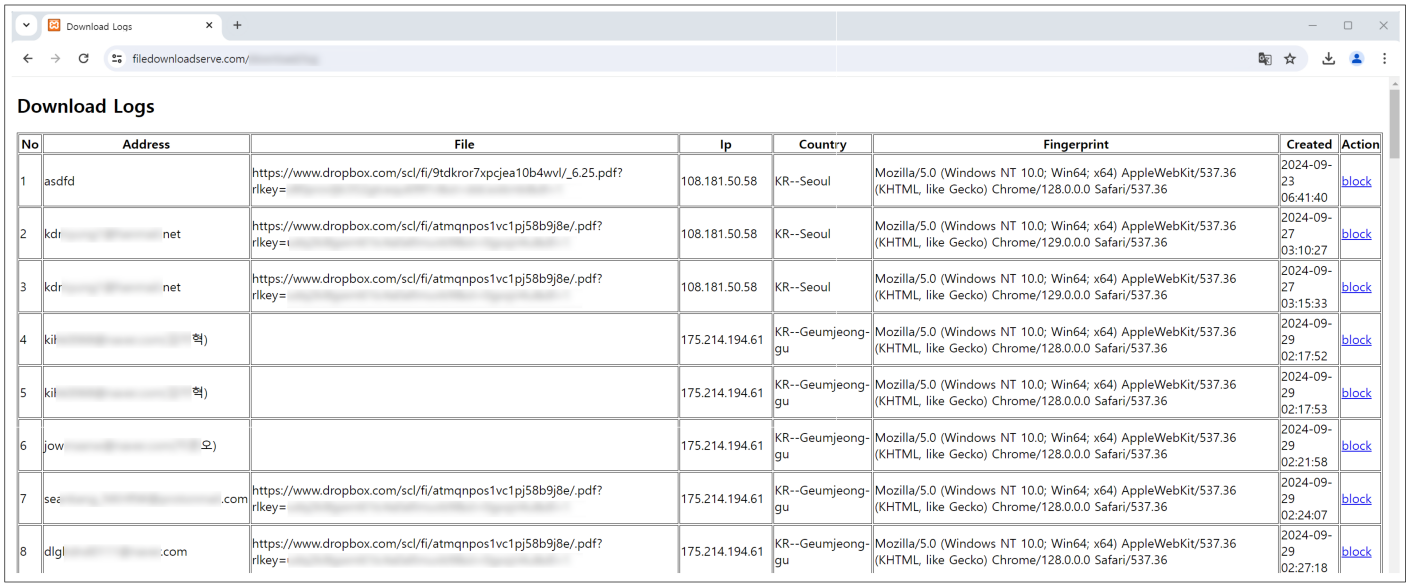
○ 웹 비콘은 원래 사용자 추적 기술로 쓰입니다. 웹 페이지나 이메일에서 수신자가 일부 콘텐츠에 액세스 했는지 확인하는 용도인데, 보통 순수한 웹 접속 통계나 수신여부 확인용으로 쓰입니다.

○ 위협 행위자들은 이 기능을 악용해 수신자의 아이피(지역정보) 주소나 웹 브라우저(OS) 정보 등 초기 정찰용 자료로 활용합니다. 이러한 자료는 본격 침투에 필요한 분석용으로 사용됩니다.

5. 위협 인프라 노출 (Threat Infra Exposure)

○ 위협거점으로 사용된 서버 인프라를 섭외하거나, 절차에 따라 내부를 조사하는 과정은 유관기관과 긴밀한 협력 외에도 많은 시간이 소요됩니다. 다만, 위협 행위자가 서버 접근 권한을 잘못 설정해 내부 자료가 외부에 노출(Opsec Fail)되는 경우가 간혹 발생합니다.

○ 정찰용 서버로 사용된 이번 케이스도 서버 설정문제로 로그기록이 외부에 고스란히 보이는 현상이 있었습니다.



Download Logs

filedownloadserve.com/

Download Logs

No	Address	File	Ip	Country	Fingerprint	Created	Action
1	asdfd	https://www.dropbox.com/scl/fi/9tdkror7xpcjea10b4wvl/_6.25.pdf?rlkey=	108.181.50.58	KR--Seoul	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36	2024-09-23 06:41:40	block
2	kdr net	https://www.dropbox.com/scl/fi/atmqnpos1vc1pj58b9j8e/.pdf?rlkey=	108.181.50.58	KR--Seoul	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36	2024-09-27 03:10:27	block
3	kdr net	https://www.dropbox.com/scl/fi/atmqnpos1vc1pj58b9j8e/.pdf?rlkey=	108.181.50.58	KR--Seoul	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36	2024-09-27 03:15:33	block
4	kil 혁)		175.214.194.61	KR--Geumjeong-gu	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36	2024-09-29 02:17:52	block
5	kil 혁)		175.214.194.61	KR--Geumjeong-gu	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36	2024-09-29 02:17:53	block
6	jow 오)		175.214.194.61	KR--Geumjeong-gu	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36	2024-09-29 02:21:58	block
7	sea .com	https://www.dropbox.com/scl/fi/atmqnpos1vc1pj58b9j8e/.pdf?rlkey=	175.214.194.61	KR--Geumjeong-gu	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36	2024-09-29 02:24:07	block
8	dlgl .com	https://www.dropbox.com/scl/fi/atmqnpos1vc1pj58b9j8e/.pdf?rlkey=	175.214.194.61	KR--Geumjeong-gu	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36	2024-09-29 02:27:18	block

[그림 9] 정찰 인프라 일부 노출 화면

○ 본격적인 정찰 수행 전인 9월 말경 여러번 자체 테스트를 수행하였고, 이때 위협 행위자가 사용한 아이피 주소가 일부 기록됩니다. 해당 아이피는 비콘 기능이 탑재된 이메일 발송에도 동일하게 사용됩니다.

○ 비콘 센서에 노출될 경우 이용자의 IP, User Agent 등이 수집됩니다. 그리고 위협 행위자는 아이피 주소에 따라 차단(block) 기능을 선택할 수 있습니다. 이를 통해 특정 아이피 대역은 정찰 대상에서 제외될 수 있는데, 이는 분석 등을 회피하기 위한 목적으로 사용됩니다.

○ 그리고 드롭박스 주소에 연결된 정상 (문서)파일을 전달하여, 이용자의 의심을 최소화 합니다. 정찰활동으로 공격 타깃의 반응을 살피고, 향후 본격 공격에 필요한 기초정보를 수집하고 있습니다.

○ 위협 배후는 정찰 활동에 여러가지 ID를 사용했는데, 대표적인 것은 하기와 같습니다. 주로 △전직 정부기관 공직자, △언론사 기자, △방송사 작가, △대북언론사, △프로그램 개발자, △북한인권분야 전문가 등으로 사칭합니다.

- c039911
- kirnchi122
- nkhumans
- sjwarng3670
- shjhe777
- moonjongjo
- hanzak99
- l026star1ove
- sujan2024
- samuel19920411
- alchemist880808
- senior.developer8688
- hyook.iri
- dailynk23
- nknews23
- komonrodny

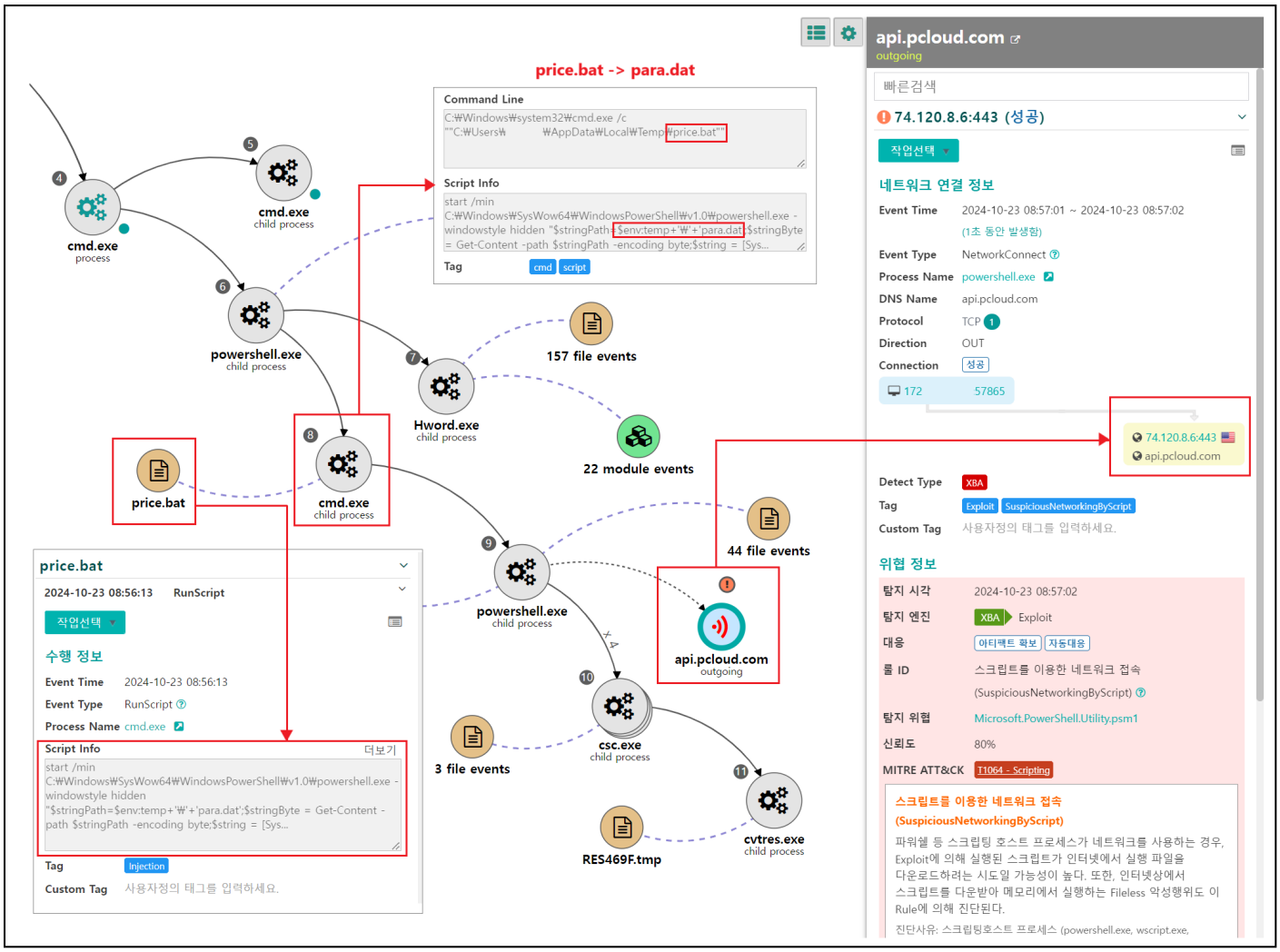
- johnbahu
- Dante

6. 결론 및 대응 (Conclusion)

○ 국가배후 해킹 그룹의 사이버 위협은 나날이 고도화되는 추세입니다. 실제 접근 기록이 확인된 이번 APT37 인프라를 통해 위협 행위자들의 지능적인 정찰활동이 식별됐습니다.

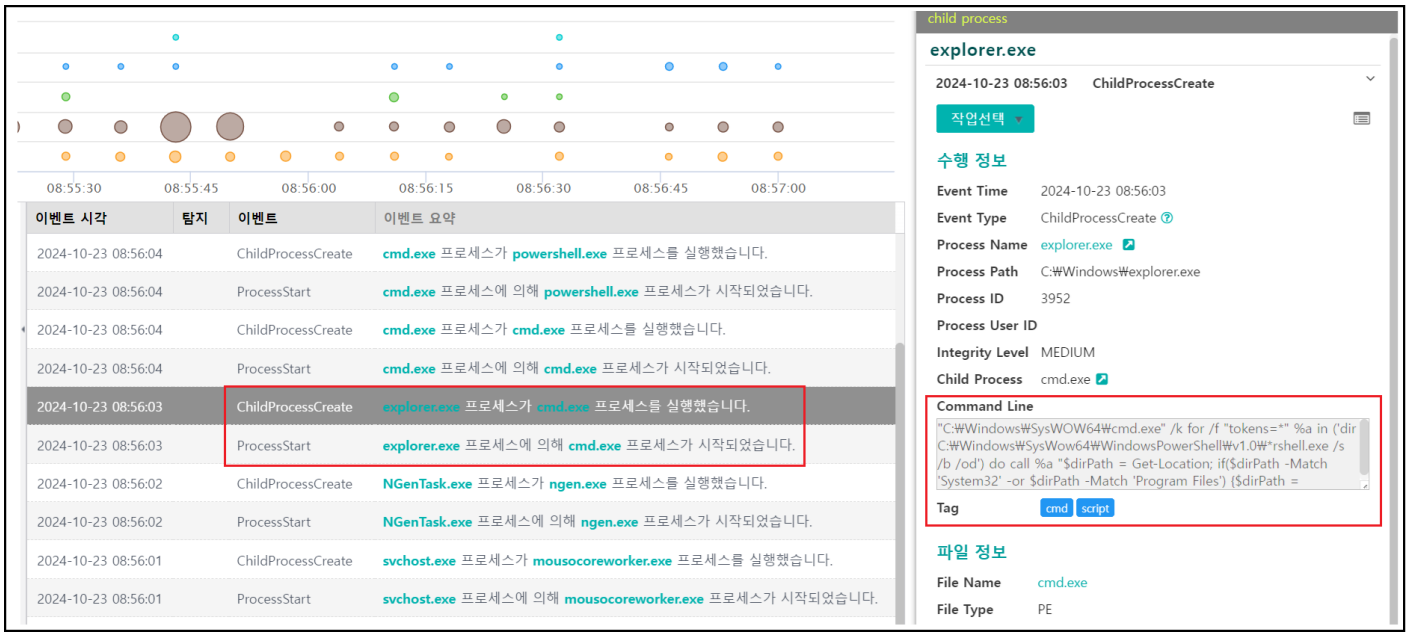
○ 따라서 기관 및 기업은 최신 사이버 위협의 동향을 파악하고, 기술적 공격 난이도에 따른 다양한 인사이트 습득이 필요합니다.

○ Genian EDR 제품은 이번 사례처럼 악성파일이 단말에 유입되어 커맨드로 실행되는 파일리스(Fileless) 중간 흐름을 파악하는데 유용합니다.



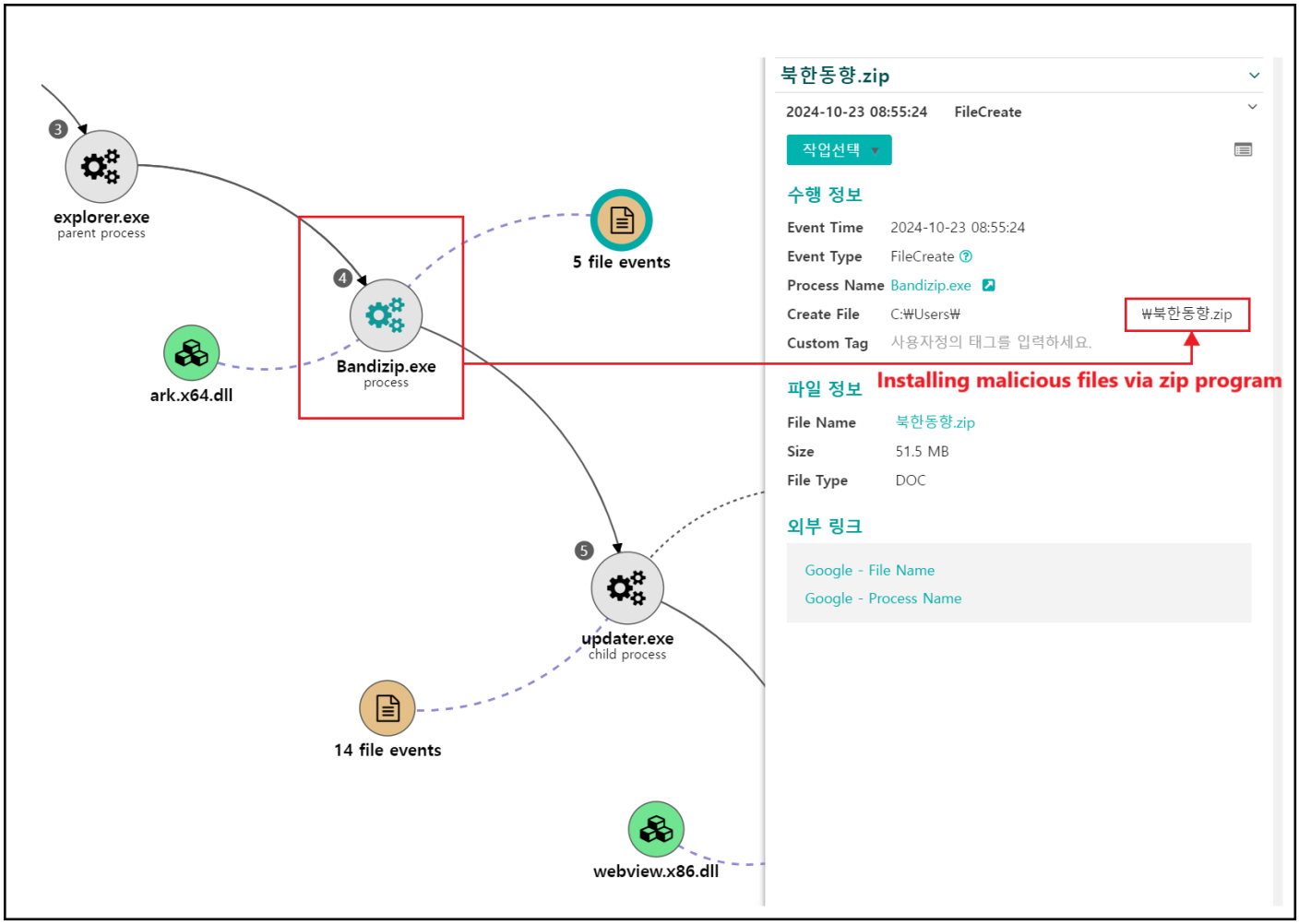
[그림 10] Genian EDR에서 파일리스 흐름 조사 화면

○ 단말에 설치된 기존 백신프로그램 패턴으로 초기 유입 탐지를 놓쳤더라도, Genian EDR 제품은 파일리스 과정과 C2 클라우드 통신 자체를 이상행위로 식별할 수 있습니다. 더불어 APT 공격에 쓰인 악성파일 역시 지니언스 IoC에 탑재된 패턴으로 2중 보호도 가능합니다.



[그림 11] 위협 이벤트 상세 정보 화면

○ 검색 필터 및 분류 등의 조건을 통해 이벤트의 시간대별 상세 흐름을 파악할 수 있습니다. 이를 통해 EDR 관리자는 단말에 유입된 위협의 시점 및 단계별 과정을 편리하게 조회하여, 후속 대응을 진행할 수 있습니다.



[그림 12] 압축파일 타입의 악성파일 설치 과정 조사

○ 압축 유틸리티를 통해 '북한동향.zip' 악성파일에 접근한 이력을 조회할 수 있습니다. 이를 통해 초기 유입 과정 파악과 후속 대응을 진행할 수 있습니다.

7. 침해 지표 (Indicator of Compromise)

● MD5
5f6682ad9da4590cba106e2f1a8cbe26
7a66738cca9f86f4133415eedcbf8e88
105ecd9f6585df4e1fe267c2809ee190
852544f01172b8bae14ec3e4d0b35115
358122718ba11b3e8bb56340dbe94f51
acf4085b2fa977fc1350f0ddc2710502
b85a6b1eb7418aa5da108bc0df824fc0
e4ddd5cc8b5f4d791f27d676d809f668

● C2
filedownloadserve[.]com
kakaofilestorage[.]com
navarar[.]com
108.181.50[.]58
158.247.219[.]10
158.247.249[.]129
141.164.62[.]19
141.164.60[.]110
223.104.236[.]114
175.214.194[.]61
61.97.243[.]2