

# 카카오톡 위장 악성코드 유포 주의 권고

<교육부 정보보호팀, '26. 4. 13>

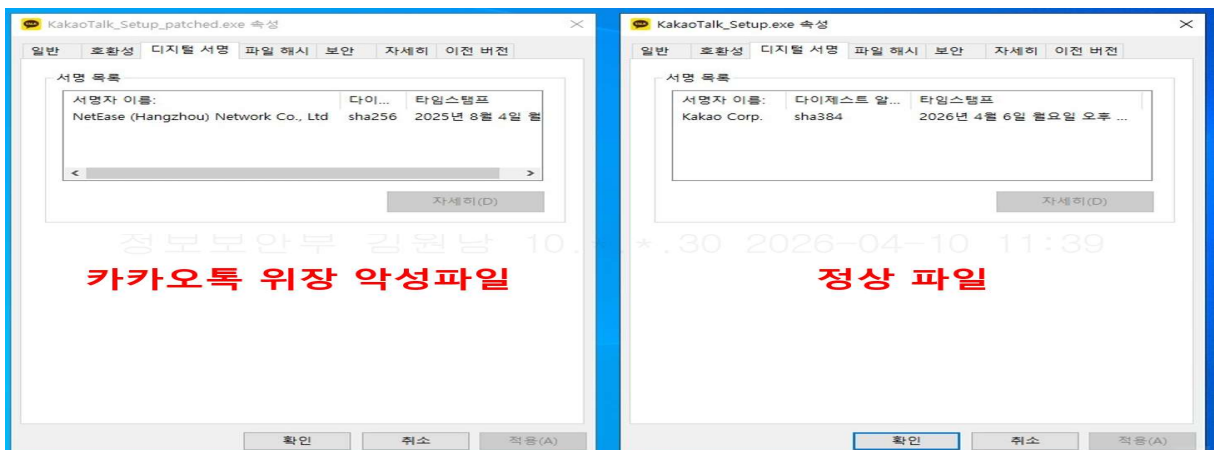
- ❖ 최근 주요 검색엔진에서 '카카오톡 PC 버전'에 대해 검색할 경우 공식 다운로드 페이지로 위장한 피싱사이트가 노출되어 악성코드에 감염되는 사례가 다수 확인

## □ 개요

- 카카오톡 공식사이트가 아닌 일부 다른 사이트에서 카카오톡으로 위장한 악성코드 배포 정황 확인
- 이에 따라 교육기관 아래 권고사항 실시 및 특이사항 발생 시 즉시 ECSC 신고(053-714-0777, cert1@ecsc.go.kr)

## □ 권고사항

- 카카오톡 PC 버전 설치 전 접속페이지가 아래 공식 도메인 URL과 일치하는지 확인
  - 카카오톡 공식 홈페이지 : <https://www.kakaocorp.com>
- 카카오톡 PC 버전 기 설치된 경우 설치 파일의 디지털 서명 정보 확인
  - 설치파일 마우스 우클릭 → 속성 → 디지털 서명 → 'Kakao Corp.' 확인



- 레지스트리 값 확인 및 레지스트리 값 존재 할 시 ECSC 신고

☞ HKCU\MicrosoftUser\KEY\_BOARD\_DATA

☞ HKCU\HKCU\MicrosoftUser\KEY\_BOARD\_DATA\_MD5

☞ HKCU\MicrosoftUser\YourSharedSecretKey

※ 악성코드 동작 시 아래 레지스트리 값이 신규 생성되며, 정상 PC의 경우 아래 그림과 같이 해당 레지스트리 값이 없음

```

C:\Windows\system32\cmd. X + v
Microsoft Windows [Version 10.0.22631.6783]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>reg query HKCU\MicrosoftUser\KEY_BOARD_DATA
오류: 오류: 시스템이 지정된 레지스트리 키 또는 값을 찾을 수 없습니다.

C:\Users\USER>reg query HKCU\HKCU\MicrosoftUser\KEY_BOARD_DATA_MD5
오류: 오류: 시스템이 지정된 레지스트리 키 또는 값을 찾을 수 없습니다.

C:\Users\USER>reg query HKCU\MicrosoftUser\YourSharedSecretKey
오류: 오류: 시스템이 지정된 레지스트리 키 또는 값을 찾을 수 없습니다.
  
```

[악성코드 감염 되지 않은 정상 PC 화면]

- EDR · 백신 등 엔드포인트 보안 솔루션을 최신 버전으로 유지하고 웹 보호 기능 및 실시간 감시 기능 활성화
- 아래의 피싱사이트 및 악성코드 설치파일 다운로드 페이지를 방화벽, 유해 사이트 차단 시스템 등에 즉시 접속 차단 정책 설정

카카오톡 설치 피싱사이트	악성코드 설치파일 다운로드 페이지
- <a href="https://apps-kakaocorp.com">https://apps-kakaocorp.com</a>	- <a href="https://download.i9616.top/KakaoTalk_Setup_patched.rar">https://download.i9616.top/KakaoTalk_Setup_patched.rar</a>
- <a href="https://apps-kakaotalk.com">https://apps-kakaotalk.com</a>	- <a href="https://download.i9616.top/KakaoTalk_S8542up.zip">https://download.i9616.top/KakaoTalk_S8542up.zip</a>
- <a href="https://pc-kakaocorp.com">https://pc-kakaocorp.com</a>	- <a href="https://xinjiapox.oss-ap-southeast-1.aliyuncs.com/KakaoTa2258.zip">https://xinjiapox.oss-ap-southeast-1.aliyuncs.com/KakaoTa2258.zip</a>