# 취약한 Innorix 악용한 악성코드 유포 - ASEC

By ATCP

Published: 2023-02-15 · Archived: 2026-04-05 17:31:20 UTC

ASEC(AhnLab Security Emergengy response Center) 분석팀은 취약한 버전의 Innorix Agent 사용자를 타겟으로 악성코드 유포 정황을 확인하였다. 확보된 악성코드는 백도어로 C&C 서버로 접속을 시도한다.

이노릭스 INNORIX Agent 취약점 보안 업데이트 권고 2022.05.31

□ 개요

o 이노릭스社 INNORIX Agent*에 대한 파일 다운로드 및 실행 취약점을 해결한 보안 업데이트 발표

* INNORIX Agent : 파일 전송 솔루션 클라이언트 프로그램

o 공격자는 해당 취약점을 악용하여 악성코드 감염 등의 피해를 발생시킬 수 있으므로, 해당 제품을 사용하는 이용자들은 최신 버전으로 업데이트 권고

□ 설명

o INNORIX Agent*에서 발생하는 파일 다운로드 및 실행 취약점

□ 영향 받는 제품 및 버전

o INNORIX Agent 9.2.18.450 및 이전 버전

□ 해결 방안

o 취약한 버전의 INNORIX Agent가 설치되어 있는 경우 삭제 조치

- [제어판]-[프로그램]-[프로그램 및 기능]에서 INNORIX Agent의 버전 확인 후 제거 클릭

프로그램 제거 또는 변경

프로그램을 제거하려면 목록에서 선택한 후 [제거], [변경] 또는 [복구]를 클릭하십시오.

구성 · 제거

| 이름 | 게시자 | 설치 날짜 | 크기 | 버전 |
|---|---|---|---|---|
| INNORIX Agent | INNORIX | 2022-05-13 | | 9.2.18.334 |
| IntelliJ IDEA Community Edition 2021.3.3 | JetBrains s.r.o. | 2022-04-01 | | 213.7172.25 |
| Java 8 Update 321 (64-bit) | Oracle Corporation | 2022-03-11 | 127MB | 8.0.3210.7 |
| Java(TM) SE Development Kit 11.0.14 (64-bit) | Oracle Corporation | 2022-04-01 | 255MB | 11.0.14.0 |
| Microsoft Edge | Microsoft Corporation | 2022-05-06 | | 101.0.1210.39 |
| Microsoft OneDrive | Microsoft Corporation | 2022-05-02 | 238MB | 22.077.0410.0007 |

o 아래 URL에서 최신 버전을 다운로드 받아 압축 해제 후 설치

- URL : http://dist.innorix.com:8080/download/INNORIX-Agent-Lastest_Version.zip

□ 기타 문의사항

o 이노릭스 : 02) 557-2757

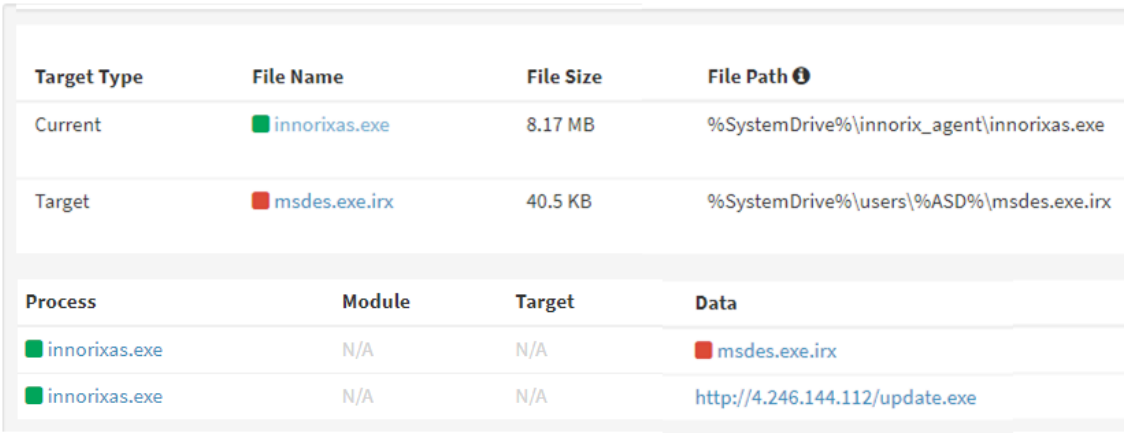
o 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118

□ 작성 : 취약점분석팀

출처 사이트 : https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=66748

[그림 1] 한국인터넷진흥원 취약점 보안 업데이트 공지[1]

유포에 악용된 Innorix Agent 프로그램은 파일 전송 솔루션 클라이언트 프로그램으로, 한국인터넷진흥원(KISA)[1]에서 취약점 관련 내용을 게시하고 보안 업데이트가 권고된 INNORIX Agent 9.2.18.450 및 이전 버전 에 해당하는 9.2.18.418 로 확인했다.

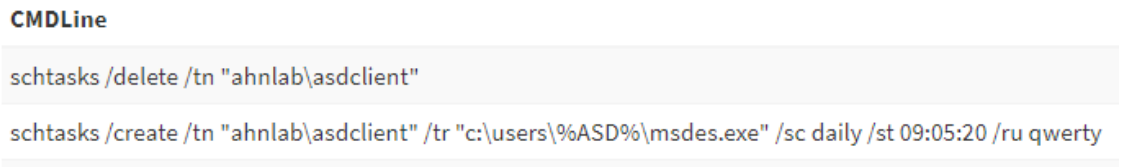


| Target Type | File Name | File Size | File Path |
|---|---|---|---|
| Current | innorixas.exe | 8.17 MB | %SystemDrive%\innorix_agent\innorixas.exe |
| Target | msdes.exe.irx | 40.5 KB | %SystemDrive%\users\%ASD%\msdes.exe.irx |

| Process | Module | Target | Data |
|---|---|---|---|
| innorixas.exe | N/A | N/A | msdes.exe.irx |
| innorixas.exe | N/A | N/A | http://4.246.144.112/update.exe |

[그림 2] ASD 인프라 탐지 로그

탐지된 백도어는 C&C 서버로 접속을 시도한다. 주요 기능으로는 사용자 PC의 정보를 수집하여 전달하는 기능이 있으며 화면캡처 기능과 파일 생성 및 실행 기능이 있다.



| CMDLine |
|---|
| schtasks /delete /tn "ahnlab\asdclient" |
| schtasks /create /tn "ahnlab\asdclient" /tr "c:\users\%ASD%\msdes.exe" /sc daily /st 09:05:20 /ru qwerty |

[그림 3] ASD 인프라 탐지 리포트

확인된 백도어는 두 가지 외형을 갖는 형태였으며, 초기 발견된 형태는 C/C++ 로 개발된 것으로 확인했으며 최근 탐지된 샘플은 닷넷으로 제작된 형태이다. 두 가지 형태 모두 기능에서는 차이가 없으며, 일부 탐지 리포트에서 악성코드를 작업 스케줄러에 등록할때 작업 이름에 자사명(AhnLab)을 사용하여 은닉 하려는 방식을 사용하는 것을 확인 했다.

```
do
{
  if ( !v5 )
    _report_rangecheckfailure(a1, a2, a3, a2);
  v18[v3++] = 0;
  v5 = (unsigned __int64)v3 < 16;
}
while ( v3 < 16 );
v6 = (int)a3;
if ( (int)a3 > 0 )
{
  v7 = a1 - (_QWORD)a2;
  do
  {
    v8 = 8i64;
    do
    {
      v9 = 15i64;
      v10 = (unsigned __int8)v18[15] >> 7;
      do
      {
        v18[v9] = __ROL1__(v18[v9 - 1], 1);
        --v9;
      }
      while ( v9 > 0 );
      v11 = 2 * v18[0];
      v18[0] *= 2;
      if ( v10 )
      {
        v13 = 0;
        v14 = 0i64;
        do
        {
          v15 = v13++ ^ v18[v14] ^ byte_140020900[v14];
          v18[v14++] = v15;
        }
        while ( v13 < 16 );
        v12 = v18[0];
      }
      else
      {
        v12 = v11 | 1;
        v18[0] = v12;
      }
      --v8;
    }
    while ( v8 );
    LOBYTE(v3) = v12 ^ v4[v7];
    *v4++ = v3;
    --v6;
  }
  while ( v6 );
}
return v3;
```

[그림 4]인코딩 및 디코딩 루틴

백도어로 구분되는 이 악성코드는 데이터를 수신 때 [그림 4] 의 루틴을 이용하여 데이터를 사용하며, 발신 때도 동일하게 사용하여 데이터를 전송한다. 데이터를 인코딩 및 디코딩 루틴을 통해 암호화해 전송하여 패킷 단위의 모니터링을 우회하며 자사 진단명 기준 Andardoor의 특징으로 볼 수 있다. 키 값은

74615104773254458995125212023273 로 2017년도에 작성된 CISA 보고서[2]에 명시된 XOR 키값과 동일하다. 최근 소프트웨어의 취약점으로 유포되는 형태가 확인되고 있어 기업 사용자 및 일반 사용자의 각별한 주의가 필요하다. 취약한 버전의 소프트웨어는 업데이트 후 사용하도록 관리되어야 한다.

**[파일 진단]**

- Backdoor/Win.Andardoor.R558252
- Backdoor/Win.Andardoor.C5381120
- Backdoor/Win.Andardoor.C5382662
- Backdoor/Win.Andardoor.C5382103
- Backdoor/Win.Andardoor.C5382101

**[References]**

1) https://knvd.krcert.or.kr/detailSecNo.do?IDX=5622 

2) https://www.cisa.gov/uscert/sites/default/files/publications/MAR-10135536-D_WHITE_S508C.PDF

MD5

0211a3160cc5871cbcd4e5514449162b

0a09b7f2317b3d5f057180be6b6d0755

1ffccc23fef2964e9b1747098c19d956

9112efb49cae021abebd3e9a564e6ca4

ac0ada011f1544aa3a1cf27a26f2e288

추가 IoC는 ATIP에서 제공됩니다.

FQDN
IP

109[.]248[.]150[.]179

139[.]177[.]190[.]243

27[.]102[.]107[.]224

27[.]102[.]113[.]88

4[.]246[.]144[.]112

추가 IoC는 ATIP에서 제공됩니다.