BYOVD 기법으로 백신 프로그램을 무력화하는 라자루스 공격 그룹의 악성코드 감염 사례

asec.ahnlab.com/ko/40495/

2022년 10월 24일

2022년 4월 안랩은 ASEC 블로그 (*INITECH 프로세스를 악용하는 라자루스 공격 그룹의 신종 악성코드*, https://asec.ahnlab.com/ko/33706)에서 라자루스 공격 그룹이 악성코드 감염을 위해 INITECH 프로세스를 악용한다는 내용을 소개했다.

본 글에서는 라자루스 공격 그룹이 워터링 홀 기법을 통해 시스템 해킹에 성공 후 내부 네트워크 내의 시스템들을 추가로 해킹하기 위해 드림시큐리티사의 MagicLine4NX 제품의 취약점을 이용하고 있으며, 취약한 드라이버를 이용해 백신 프로그램을 무력화하고 있다는 내용을 공유하고자 한다.

최초 침투

공격자는 피해 시스템에 침투하기 위해 워터링 홀 공격 방식을 사용하고 있다. 국내 웹 사이트를 해킹한 후, 해당 사이트에서 제공되는 컨텐츠를 조작한다. 특정 IP에서 접근하는 경우에만 동작되는 것으로 보아, 특정 기업이나 조직을 노리고 있는 것으로 추정된다.

취약한 INISAFECrossWebEX를 사용 중인 사용자의 PC가 해당 사이트에 웹 브라우저로 접근하게 되면, INISAFECrossWebEXSvc.exe의 취약점에 의해 악성코드 배포 사이트에서 라자루스 악성코드(SCSKAppLink.dll)가 다운로드된 후 실행된다.

악성코드 감염에 취약한 버전의 INISAFECrossWebEXSvc.exe 프로세스가 악용되고 있으므로, 해당 소프트웨어를 사용 중인 PC는 반드시 최신 패치를 적용해야 하며, 사용하지 않는 경우에는 삭제하도록 한다.

내부 시스템 접근

MagicLine4NX 취약점 이용

공격자는 내부 시스템에 접근하기 위해 MagicLine4NX(인증서 인증, 전자서명 및 데이터 암/복호화 기능을 수행하는 솔루션)의 취약점을 이용한다.

MagicLine4NX 1.0.0.17 이하의 버전에서는 CVE-2021-26606 취약점 (https://krcert.or.kr/data/secInfoView.do?bulletin_writing_sequence=36173)이 존재한다. 해당 취약점은 버퍼 오버플로우 취약점으로 원격에서 임의의 명령어를 전송하여 악성코드 감염 등의 피해를 유발할 수 있다.

공격자는 MagicLine4NX 프로세스를 이용해 ftp.exe에 악성 스레드를 인젝션시켜 악성 행위를 수행한다. ftp.exe가 사용된 이유는 MagicLine4NX에는 프로토콜(http,ftp)에 따라 입력받는 응용 프로그램을 호출하는 기능이 있는데, 취약점 공격시 이 기능이 사용되면서 ftp.exe에 악성 스레드가 인젝션되는 것으로 추정된다.

Symantec 블로그 (*Lazarus Targets Chemical Sector*, 2022.04.14, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical)에 따르면 라자루스 그룹은 WMI를 사용하여 원격 시스템의 MagicLine4NX를 호출하고 악성 스레드를 인젝션하는 것으로 확인됐다.

공격자는 취약한 MagicLine4NX을 악용해 내부 망 시스템을 장악해 나가므로, MagicLine4NX 1.0.0.17 이하 버전을 사용하는 경우, 반드시 최신 버전으로 업데이트하도록 한다.

RDP 접근

공격자는 내부 시스템에 접근하기 위해 RDP를 사용하기도 한다. 접근한 후에는 다음과 같은 악성 행위를 수행한다.

먼저, 제어권 유지를 위해 백도어를 생성하고, 백도어가 통신할 TCP 60012 포트를 호스트 방화벽에서 허용한다. 이후, 백도어 파일을 생성하고 서비스로 등록해 제어권을 유지한다. 그리고 루트킷 악성코드와 취약한 DLL 및 드라이버를 생성해 보안 제품을 무력화한다.

유형	행위
백도어 생성	netsh.exe로 방화벽 예외 추가 • smtp 이름으로 로컬 포트 60012 허용
	백도어 프로그램(imaadp64.acm) 생성 • C2 접속 및 파일 다운로드 기능이 포함된 악성코드 생성, 60012포트 사용
	백도어 로더(Nlas.dll) 생성 • 로딩 대상 파일: C:₩Windows₩System32₩imaadp64.acm
	백도어 로더 서비스 등록 • 서비스 명: Nla • 경로: C:₩Windows₩System32₩Nlas.dll
보안 제품 무력화	루트킷 로더 생성 (C:₩windows₩miblib.bin)
	루트킷 생성 (C:₩windows₩miblib.dat)
	취약한 DLL 및 드라이버 파일 생성 (악성파일은 아님) • C:₩Windows₩System32₩SB_SMBUS_SDK.dll (악성파일은 아님) • %SystemRoot%₩System32₩drivers₩dmvscmgr.sys (악성파일은 아님)
	취약한 드라이버를 서비스로 등록/실행 • %SystemRoot%₩System32₩drivers₩dmvscmgr.sys

[표] 공격자의 악성 행위

SSH 접근

공격자는 내부 네트워크에 존재하는 시스템들의 SSH 서버에 root 계정으로 로그인을 시도한다.

악성코드에 의한 V3 무력화

BYOVD 기법 사용

공격자는 시스템의 보안 제품을 무력화시키기 위해 BYOVD(Bring Your Own Vulnerable Driver, 취약한 드라이버 모듈을 통한 공격) 기법을 사용한다. BYOVD는 하드웨어 공급 업체의 취약한 드라이버 모듈을 악용하는 방식의 공격으로, 드라이버의 권한을 이용하므로 커널 메모리 영역에 읽고 쓰는 것이 가능해, 보안 제품을 포함한 시스템 내 모든 모니터링 프로그램을 무력화할 수 있다.

루트킷을 이용한 보안 제품 무력화 방식은 9월 22일 안랩 ASEC 블로그 “라자루스 그룹의 BYOVD를 활용한 루트킷 악성코드 분석 보고서”(https://asec.ahnlab.com/ko/38593/)에서 상세히 다루고 있다.

백신 무력화 과정

1. MagicLine4NX가 ftp.exe에 악성 스레드를 인젝션한다.
2. ftp.exe가 루트킷 파일을 생성한다.
3. 루트킷이 취약한 DLL 및 드라이버 파일을 생성하고, 서비스로 등록한다.
4. 루트킷이 취약한 DLL을 로드하여 드라이버의 호출자 검증을 통과하고 갓 모드(God Mode)를 획득한다.
5. 갓 모드에서 커널 영역 메모리를 수정해 백신 프로그램을 무력화한다.

루트킷 동작 방식의 변화

공격자는 여러 방법을 이용해 루트킷을 동작시키는 것으로 확인됐다.

1. 실행 중인 프로세스에 루트킷 악성코드 모듈이 로드된 형태로 악성 행위를 수행
2. 루트킷 악성코드가 독립적인 프로세스 형태로 악성 행위를 직접 수행

공격자는 지속적으로 공격 기법을 개선하고 있는 것으로 보인다.

백신 무력화 행위 탐지 및 차단

위의 백신 무력화 과정을 V3에서는 다음과 같이 차단하고 있으므로, V3를 사용하는 시스템에서는 V3의 “행위 기반 진단”을 활성화 하도록 한다.

- InitialAccess/MDP.Event.M4419 (2022.09.21.01)
- InitialAccess/MDP.Event.M4422 (2022.08.08.02)

공격자가 사용한 악성코드

정상 파일이나 악용된 파일 목록

유형	파일명	설명
취약한 파일 (정상파일)	umpassmgr.sys isapnpmgr.sys dmvscmgr.sys	• 원본 파일명: ene.sys • 취약한 드라이버 모듈로 BYOVD 공격을 통해 제품 무력화에 사용
	SB_SMBUS_SDK.dll	• 원본 파일명: msi.dll • 드라이버의 호출자 검증 우회를 위해 사용

악성코드 목록

유형	파일명	설명
로더	wpnsvc.dll helpsvcs.dll	• configmanager.tlb 파일을 디코딩
	Nlas.dll	• 파일을 메모리로 읽은 후 쉘코드 디코딩 • 대상: C:₩Windows₩System32₩imaadp64.acm
	miblib.dat	• 취약한 드라이버를 이용하여 커널 조작을 일으키는 루트킷 로더 • 이 파일로 인해 ene.sys 파일이 생성됨

	usoshared.dat	• 파일 드롭 후 파일 시간 조작
		  • C:₩Windows₩System32₩[랜덤명].dll
		  • C:₩Windows₩System32₩[랜덤명].dat
		• 레지스트리에서 C2 설정 값 확인 및 dll, dat 파일 저장 후 dll 파일 인젝션
		  • 레지스트리 경로: HKLM₩SOFTWARE₩Microsoft₩Print₩Device
		  • ClassInstaller: dat 파일명
		  • InternetPrinting: C2 등 설정 값 인코딩 데이터
		  • PrintUI: dll 파일명
		• C2 서버 주소
		  • hxxps://edu.cyber.co.kr/contents/mypage/inc/inc.php
		  • hxxps://pms.nninc.co.kr/ad_cms/inc/inc.aspx
		  • hxxps://www.kjcc.co.kr/html/course/inc/inc.aspx

	cylvc.dll	• usoshared.dat가 레지스트리에 저장한 dat 파일명 호출
		• dat 파일 읽은 후 디코딩하여 메모리상에 실행
		  • 레지스트리 경로: HKLM₩SOFTWARE₩Microsoft₩Print₩Device₩ClassInstaller
		  • 파일 경로: C:₩Windows₩System32₩[랜덤명].dat
		• HKLM₩SOFTWARE₩Microsoft₩Print₩Device₩InternetPrinting 경로에서 C2 설정 파일을 읽어 디코딩 후 C2에 접근하여 명령 수행

설정 파일	C_77706e.NLS	• C2 주소를 포함하며, configmanager.tlb 실행 시 참조됨
		  • hxxps://lightingmart.co.kr/admin/order/order_detail_print.asp
		  • hxxps://jjmhome.co.kr/data/base/board/community/community.asp
		  • hxxps://logici.co.kr/common/pop_event.asp

	C_68656c.NLS	• C2 주소를 포함하며, configmanager.tlb 실행 시 참조됨
		  • hxxps://www.winsystem.kr/include/comCache.asp
		  • hxxps://buygermany.co.kr/custom/qna_list.asp
		  • hxxps://lightingmart.co.kr/admin/goods/pop_categoryExcel.asp

백도어	configmanager.tlb	• 특정 파일 로더 및 파일 다운로드 • 읽는 파일: %systemroot%₩system32₩C_(16진수 6자리).NLS 16진수 6자리는 configmanager.tlb를 로드한 파일(wpnsvc.dll, helpsvcs.dll)의 앞의 3글자의 Hex 값 - 예) C_77706e.NLS -> 77706e -> wpn (wpnsvc.dll) C_68656c.NLS -> 68656c -> hel (helpsvcs.dll)
	imaadp64.acm	• HKLM₩SYSTEM₩CurrentControlSet₩Control₩WMI₩Security₩6d713465-64af-c83c-eea6cdef9 값을 읽어 60012번 포트 번호로 Bind함 • 공격자가 원격지에서 해당 포트로 접속 후, 추가 파일을 다운로드 받아 실행하거나 파일 탈취 및 여러가지 악성 행위 가능
	wdsvc.dll	• 아래 레지스트리 값을 읽어들여 C2 서버 주소를 가져옴 • HKLM₩SYSTEM₩CurrentControlSet₩Control₩WMI₩Security₩77647376-2790-10f2-dd2a-d92f482d094f • 이후, C2에 접속하여 백도어 행위를 수행

루트킷	miblib.bin	• 특정 파일을 인자로 받아 메모리 상에서 실행

	ole.bin	• 파일 다운로드
		  • C:₩Windows₩system32₩sb_smbus_sdk.dll
		  • C:₩Windows₩system32₩drivers₩isapnpmgr.sys
		• C2 주소와 네트워크 통신
		  • hxxps://hmcok.co.kr (20.194.29.89)
		  • hxxps://lightingmart.co.kr (119.207.79.175)
		  • hxxps://buygermany.co.kr (61.100.5.186)

	olesvc.bin	• ole.bin과 동일한 파일로 추정

	SPEProxy.bin	• 화면을 캡쳐한 뒤 인코딩하여 특정 경로에 저장
		• 옵션: <저장 파일 이름> <지속 시간> <대기 시간> [색 Bit수 지정(기본 4Bit)]
		  ex) "SPEProxy.bin C:₩Windows₩Temp₩~BIT3596.tmp 30 1"
		  30초 동안 1초 간격으로 C:₩Windows₩Temp₩~BIT3596.tmp에 스크린샷 저장(인코딩 상태)
		• 저장 파일 구조: [색 Bit 수/4 Bytes] [이미지 가로 크기/4 Bytes] [이미지 세로 크기/4 Bytes] [인코딩 된 Bitmap Image 크기/4 Byte] [인코딩 된 Bitmap Image/가변]
		• 이미지 인코딩 과정: (Raw_BitMap_Image) -> Zlib Compress -> Xor 0xE4

미확보	globaleds64(HostName).dll	파일 미확보
	wusa.bin	파일 미확보

[표] 공격자가 사용한 악성코드 목록

[취약점 정보]

- INITECH INISAFE CrossWEB EX V3 취약점 (2022.07.29): https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=66834
- 드림시큐리티 MagicLine 버퍼 오버플로우 취약점 CVE-2021-26606 (2021.08.06): https://www.krcert.or.kr/data/secInfoView.do?bulletin_writing_sequence=36173

[파일 진단]

- Downloader/Win.LazarAgent (2022.05.04.02)
- Backdoor/Win.Lazardoor (2022.07.06.00)
- Downloader/Win.LazarShell (2022.05.04.02)
- Trojan/Win.Lazardoor (2022.05.04.02)

- Trojan/Win.LazarLoader (2022.06.22.03)
- Trojan/Win.LazarLoader (2022.07.11.03)
- Data/BIN.EncPe (2022.09.07.00)
- Trojan/Win.LazarLoader (2022.09.07.00)
- Backdoor/Win.Lazardoor (2022.09.07.00)
- Data/BIN.EncodedPE (2022.09.07.00)
- Trojan/Win.LazarLoader (2022.09.07.00)
- Trojan/Win.Lazardoor (2022.08.02.03)
- Rootkit/Win.Agent (2022.08.02.03)
- Trojan/Win.Agent (2022.09.16.02)
- Data/BIN.Encoded (2022.10.05.00)
- Data/BIN.Encoded (2022.10.05.00)

[파일 MD5]

- 8F39A7AFA14541B709FE950D06186944
- CA6C08B58A35D7FA581DFB419CE5B881
- 1EDBD7AA68B1818A1EA98C0362CE84C7
- 4D91CD34A9AAE8F2D88E0F77E812CEF7
- FA868A38CEEB46EE9CF8BD441A67AE27
- 43F218D3A4B2199468B00A0B43F51C79
- 1F1A3FE0A31BD0B17BC63967DE0CCC29
- B457E8E9D92A1B31A4E2197037711783
- 202A7EEC39951E1C0B1C9D0A2E24A4C4
- 97BC894205D696023395CBD844FA4E37
- CA9B6B3BCE52D7F14BABDBA82345F5B1
- 013B4C4E9387D8FE1EAB738C42C451DA
- 98E58A39EDE26AF7980ED4DE2873CAAB
- 8DA35C64FFBFE33A3435A3E8DC1A5A42
- C16A6178A4910C6F3263A01929F306B9
- 8543667917A318001D0E331AEAE3FB9B

[IP/URL]

strivemktsupporters[.]com(3.39.208.187)를 제외하고, 아래 IP는 공격자에 의해 C2로 사용됐으나, 현재도 서비스 중인 정상 사이트들이다.

- hxxps://strivemktsupporters[.]com
- 3.39.208.187
- 222.118.225.33
- 211.110.1.17
- 20.194.29.89
- 119.207.79.175

- 61.100.5.186
- 110.10.189.167
- 14.63.165.32
- 211.110.1.93
- 182.252.138.31
- 114.207.112.19
- 1.249.169.5

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:침해사고 분석 사례

Tagged as:Forensics, 침해사고