공공 기관 및 대학 등에 널리 사용하는 공인인증서 소프트웨어 취약점을 이용한 Lazarus 공격 그룹 공격 사례

nuno 1주 ago

재작년(2021년 3월)부터 Lazarus 공격 그룹의 악성코드가 국내의 방산, 인공위성, 소프트웨어, 언론사 등 다수의 업체들에서 발견되고 있어, ASEC(AhnLab Security Emergency Response Center)은 Lazarus 공격 그룹의 활동 및 관련 악성코드를 지속적으로 추적 및 분석하고 있다.

이번 사례의 피해 고객사는 2022년 5월 Lazarus 공격 그룹에 의해 이미 한 차례 침해당한 업체였고, 동일한 소프트웨어의 0-Day 취약점으로 인해 침해가 재발했다. 2022년 5월 침해 당시 고객은 공공기관 및 대학 등에서 널리 사용되는 공인인증서 관련 프로그램의 취약한 버전을 사용하고 있었고, 사고 이후 해당 소프트웨어를 모두 최신 버전으로 업데이트해 운영하고 있었다. 하지만 이번에는 해당 소프트웨어의 0-Day 취약점에 의해 침해당했다.

ASEC에서는 해당 소프트웨어에 대해 KISA에 제보를 했으나, 취약점이 명확히 확인되지 않은 상태이며, 아직 소프트웨어 패치가 나오지 않아 본 글에서는 해당 제조사와 소프트웨어에 대해서는 공개하지 않는다.

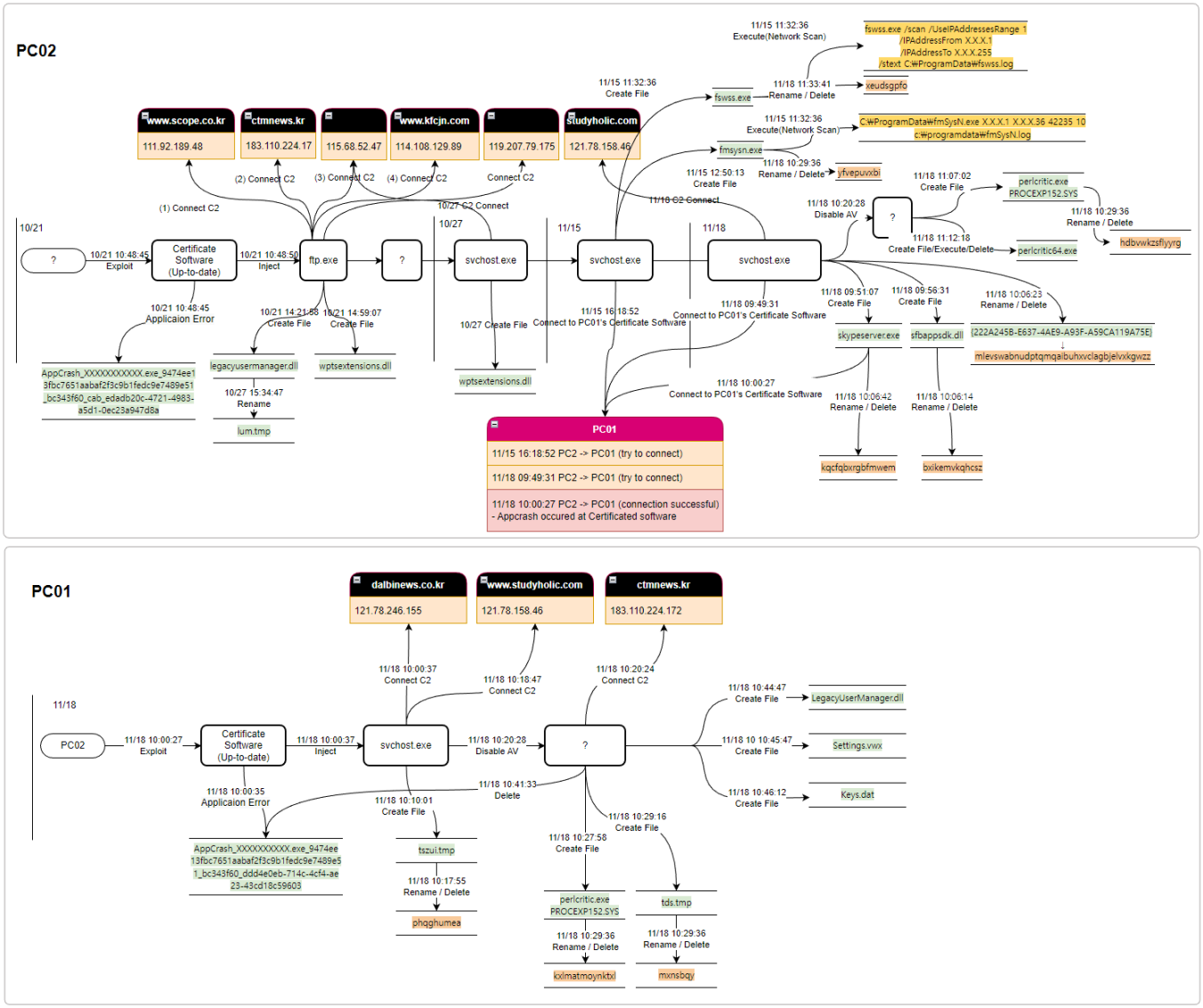
이 사건외에도 ASEC에서 분석했으나 아직 공개하지 못한 여러 사건을 종합해 볼 때, Lazarus 그룹은 국내 기관 및 기업에 침투하기 위해 지속해서 다양한 소프트웨어의 취약점을 연구하고 있으며, 보안 제품을 무력화하고, 안티포렌식 기술 등을 이용해 탐지 및 분석을 방해 및 지연 시키는 등 TTP를 지속적으로 변화시키고 있음을 알 수 있다.

본 보고서는 피해 고객사의 포렌식 분석 보고서를 기반으로 작성됐다. 본 보고서는 1월에 작성됐으나, 소프트웨어 취약점 패치 이슈로 공개를 늦춰오다 소프트웨어 정보를 익명화한 후 공개하기로 결정했다. 소프트웨어 패치가 공개되면, 해당 정보를 공개한 버전의 보고서를 재배포할 예정이다.

사건 개요

CATEGORY	DESCRIPTION
사건 발생 기간	2022/10/21 ~ 2022/11/18
피해 시스템 유형	Windows 10
피해 현황	백도어 악성코드 감염 및 C2 통신
공격 유형	• A사 공인인증서 프로그램의 0-Day 취약점을 이용한 래터럴 무브먼트 ※ 아직 패치가 나오지 않은 상태라 취약 소프트웨어 정보는 미공개 • BYOVD 공격을 통한 백신 무력화 • 안티 포렌식 ◦ 타임 스탬프 조작 ◦ 파일명을 랜덤하게 변경 후 삭제 ◦ 실행 아티팩트 삭제 ◦ 시스템 파일명과 동일한 파일명 사용
공격자	Lazarus
사건 TAG	#Lazarus #skypeserver.exe #0-day #루트킷 #BYOVD

[표] 분석 요약



[그림] 침해 흐름도

사례를 통한 교훈

- 공격자는 국내에서 널리 사용되는 공인인증서 소프트웨어의 0-Day 취약점을 이용했다. 해당 유형의 소프트웨어는 자동 업데이트가 되지 않으므로 사용 중인 소프트웨어는 반드시 최신 버전 패치를 수행하고, 사용하지 않을 경우 제거해야 한다.
- 공격자는 취약한 드라이버 커널 모듈을 악용하는 BYOVD라는 기법으로 보안제품을 무력화했다.
- 공격자는 악성 행위를 은닉하기 위해 파일명을 변경하여 삭제하거나, 시간 정보를 조작하는 등 안티포렌식 행위를 수행했다.
- 피해 고객사는 동일한 공격자로부터 유사 방법으로 재침해당했다. 사후 조치뿐 아니라 지속적인 모니터링을 통해 위협의 재발을 막아야 한다.

사건 상세

분석 결과 요약

고객사로부터 접수된 두 대의 PC를 분석한 결과, PC01과 PC02는 인증서 소프트웨어의 취약점을 이용한 래터럴 무브먼트 공격에 당한 것으로 확인됐다. PC02는 10월 21일에 확인되지 않은 내부 시스템으로부터 공격이 있었으며, PC01은 11월 18일에 PC02에 의해 공격당했다. PC01과 PC02에는 최신 버전의 인증서 소프트웨어가 설치돼 있었던

점으로 보아 공격자는 0-Day 취약점을 사용한 것으로 추정된다. 또한 PC01과 PC02에는 11월 18일에 V3가 무력화되는 증상이 발생했는데, 기존과는 다른 방법이 이용됐다.

이번에 분석된 시스템은 래터럴 무브먼트 공격을 받은 것으로, 공격자의 최초 유입과는 관련이 없었다. 피해 고객사의 인터넷망에는 지난 5월 침입에 성공한 Lazarus 공격 그룹의 위협이 잔존해 있었던 것으로 추정된다.

SYSTEM	DATE	DESCRIPTION
PC01	2022/11/18	인증서 소프트웨어 취약점에 의한 래터럴 무브먼트 공격 (PC02 → PC01)
	2022/11/18	V3 무력화 발생
PC02	2022/10/21	인증서 소프트웨어 취약점에 의한 래터럴 무브먼트 공격 (미확인 내부시스템 → PC02)
	2022/11/18	V3 무력화 발생

[표] 각 시스템별 주요 악성 행위

PC01 분석

PC01은 2022/11/18 10:00:35에 인증서 소프트웨어의 0-Day 취약점 공격으로 침해된 것으로 추정된다. PC02에서 PC01의 인증서 소프트웨어의 서비스 TCP 포트로 세 차례 네트워크 연결을 시도한 흔적이 확인됐다. 앞선 두 번의 연결 시에는 PC01에서 특별한 반응이 없었으나, PC02에서 svchost.exe를 이용해 생성한 skypeserver.exe(미확보)를 이용해 11/18 10:00에 PC01에 접근했을 때에는 PC01에서 인증서 소프트웨어의 오류(AppCrash)가 발생되고, 이후 악성 행위들이 시작됐다. AppCrash 발생 시 시스템에 저장된 에러 리포트(WER)나 메모리 덤프 파일들은 모두 삭제돼 확인할 수 없었다. 공격자가 의도적으로 삭제한 것으로 보인다.

DATE TIME	DESCRIPTION	REMARKS
2022/11/15 16:18:52	svchost.exe 네트워크 연결 10.20.XXX.125:XXXXX	공격 실패 혹은 접속 테스트로 추정
2022/11/18 9:49:31	svchost.exe 네트워크 연결 10.20.XXX.125:XXXXX	공격 실패 혹은 접속 테스트로 추정
2022/11/18 10:00:27	skypeserver.exe 네트워크 연결 10.20.XXX.125:XXXXX	취약점 공격 성공

[표] PC02에서 PC01의 인증서 소프트웨어 서비스 포트로 접근한 이력 (V3 행위 로그)

[그림] 인증서 소프트웨어의 Crashdump 파일 생성 기록

PC01에서 확인된 흔적 중 지난 5월에 발생된 공격과 달라진 점은 인증서 소프트웨어의 취약점 공격 후 사용되는 프로세스가 ftp.exe가 아닌 svchost.exe가 사용됐다는 점이며, 당시에는 취약한 버전의 소프트웨어가 설치돼 있었으나, 이번에는 모두 최신 버전이 설치돼 있어 알려진 취약점 정보가 없다는 점도 차이점이다.

TARGET	INSTALL DATE	SOFTWARE VERSION	COMPROMISED DATE
PC01	2022/07/01	Up-to-date	2022/11/18
PC02	2022/08/30	Up-to-date	2022/10/21

[표] PC01, PC02에 설치된 인증서 소프트웨어 버전

공격자는 PC01에 접근 후 정상 프로세스(svchost.exe)에 악성 스레드를 인젝션해 C2 통신 및 백도어 용도로 사용했다. 이후 시스템에 설치된 V3 제품을 무력화하고, 추가 악성 파일을 생성하고 실행했다.

또한 이번 분석에서는 악성 파일의 타임스탬프가 조작된 흔적이 확인됐으며, 파일 삭제 시 파일명을 랜덤하게 변경하고 삭제하는 등 안티 포렌식 행위가 발견된 점으로 보아 공격자가 분석을 적극적으로 방해하고 있는 것으로 보인다.

TIMELINE (PC01)

PC01에서 확인된 침해 행위의 타임라인은 다음과 같다.

TIME (22/11/18)	CATEGORY	BEHAVIORS
10:00:37	인젝션	svchost.exe가 악성 행위 시작 실행 중인 프로세스에 악성 스레드를 인젝션
10:00:37	C2 통신	svchost.exe가 공격자 C2주소로 네트워크 연결 121.78.246.155(dalbinews.co.kr)

10:10:01	악성 파일 생성	악성 파일 생성 C:\ProgramData\tszui.tmp (미확보)
10:17:55	안티 포렌식	악성 파일 이름 변경 및 삭제 이름 변경 : C:\ProgramData\tszui.tmp -> phqghumea파일 삭제 : C:\ProgramData\phqghumea (미확보)
10:18:47	C2 통신	svchost.exe가 공격자 C2주소로 네트워크 연결 121.78.158.46(www.studyholic.com)
10:20:28	보안 제품 무력화	V3가 보안 제품 무력화 행위 탐지(Exploit/Win.Lazardoor.GEN)
10:20:24	C2 통신	공격자 C2주소로 네트워크 연결 183.110.224.172(ctmnews.kr)
10:27:58	악성 파일 생성	악성 파일 생성 C:\ProgramData\perlcritic.exe (미확보)
10:28:53	취약한 드라이버 파일 생성	악성 파일 실행 C:\ProgramData\perlcritic.exe (미확보)드라이버 파일 생성 (악성파일은 아님) C\Windows\System32\drivers\PROCEXP152.SYS (확보)
10:29:16	악성 파일 생성	악성 파일 생성 C:\ProgramData\tds.tmp (미확보)
10:29:36	안티 포렌식	악성 파일 이름 변경 및 삭제 이름 변경 : C:\ProgramData\tds.tmp -> mxnsbqy파일 삭제 : C:\ProgramData\mxnsbqy (미확보)
10:41:33	안티 포렌식	AppCrash 파일 삭제 파일 삭제 : C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_XXXXXXXXXXXX.ex_9474ee13fbc7651aabaf2f3c9b1fedc9e7489e51_bc343f60_ddd4e0eb-714c-4cf4-ae23-43cd18c59603(미확보)
10:42:19	안티 포렌식	악성 파일 이름 변경 및 삭제 이름 변경 : C:\ProgramData\perlcritic.exe -> kxlmatmoynktxl파일 삭제 : C:\ProgramData\kxlmatmoynktxl (미확보)
10:44:31	악성 파일 생성	백도어 로더(LegacyUserManager.dll) 생성 (확보) 로딩 대상 파일 : C:\ProgramData\Microsoft\Crypto\Keys\Keys.dat (확보) C:\ProgramData\Microsoft\Settings\Settings.vwx (확보)
10:44:47	안티 포렌식	백도어 로더(LegacyUserManager.dll)의 타임스탬프(Standard Information) 조작 (확보)

10:45:47	악성 파일 생성	백도어 프로그램(Keys.dat) 생성 (확보) C2 접속 및 파일 다운로드 기능이 포함된 악성코드 생성
10:45:56	안티 포렌식	백도어 프로그램(Keys.dat)의 타임스탬프(Standard Information) 조작 (확보)
10:46:12	악성 파일 생성	백도어 프로그램(Settings.vwx) 생성 (확보) C2 접속 및 파일 다운로드 기능이 포함된 악성코드 생성
10:46:30	안티 포렌식	백도어 프로그램(Keys.dat)의 타임스탬프(Standard Information) 조작 (확보)

[표] PC01에서 발견된 공격자의 악성 행위

PC02 분석

공격자는 10/21 10:48:48 인증서 소프트웨어의 취약점을 악용해 PC02에 접근한 것으로 확인됐다. 해당 취약점 공격 시 AppCrash가 발생했으며, 이후 ftp.exe가 실행되고 악성행위가 시작됐다. 이는 5월에 피해 고객사에서 발생된 것과 동일한 방법이다. PC02에 접근한 시스템의 IP는 확인되지 않았다.

[그림] PC02에서 확인된 인증서 소프트웨어 에러 로그(Application.evtx)

[그림] PC02의 V3 MDP 로그에서 확인된 인증서 소프트웨어와 ftp.exe의 악성 스레드 인젝션 코드

공격자는 10/21 PC02에 최초 침투한 후, 인젝션한 ftp.exe를 통해 C2 서버 통신 및 백도어 기능을 수행하는 악성 파일을 생성했다.

10/27에는 21일의 공격과 달리 ftp.exe 대신 svchost.exe 프로세스에 악성 스레드를 인젝션했는데, 이후 11/18까지 제어권을 가지고 악성 행위를 수행했다.

11/15에는 fswss.exe 파일을 생성해 내부 네트워크를 스캔한 것으로 확인됐다. 이후 svchost.exe를 이용하여 PC01의 인증서 소프트웨어의 서비스 포트로 두 차례 접속한 이력이 확인됐다.

11/18에는 skypeserver.exe 파일을 생성하고 해당 파일을 이용하여 PC01의 TCP XXXXX에 접속했으며, 이때 PC01에서는 인증서 소프트웨어의 AppCrash가 발생했고, 이후, PC02에서는 PC01과 동일하게 백신 무력화, 악성파일 생성 및 실행 행위 등의 흔적이 확인됐다.

TIMELINE (PC02)

PC02에서 확인된 침해 행위의 타임라인은 다음과 같다.

DATE	TIME	CATEGORY	BEHAVIORS
22/10/21	10:48:50	C2 통신	ftp.exe가 공격자 C2 주소와 네트워크 연결 111.92.189.48(www.scope.co.kr)
	10:48:51		ftp.exe가 공격자 C2 주소와 네트워크 연결 183.110.224.172(ctmnews.kr)
	10:49:46		ftp.exe가 공격자 C2주소와 네트워크 연결 115.68.52.47(www.artinsight.co.kr)
	10:51:35		ftp.exe가 공격자 C2주소와 네트워크 연결 114.108.129.89(www.kfcjn.com)
	10:52:31		ftp.exe가 공격자 C2주소와 네트워크 연결 114.108.129.89(www.kfcjn.com)
	10:59:33		ftp.exe가 공격자 C2주소와 네트워크 연결 114.108.129.89(www.kfcjn.com)
	12:52:38		ftp.exe가 공격자 C2주소와 네트워크 연결 119.207.79.175(lightingmart.co.kr)
	14:21:58	악성파일 생성	ftp.exe가 파일 생성 C:\Windows\System32\lecacyusermanager.dll (확보)
	14:59:07		ftp.exe가 파일 생성 C:\Windows\System32\wptsextensions.dll (확보)
	15:34:47	안티 포렌식	악성 파일 이름 변경 이름 변경: C:\Windows\System32\legacyusermanager.dll -> C:\Windows\temp\lum.tmp (확보)
22/10/27	15:25:00	인젝션	정상 프로세스(svchost.exe)에 악성 스레드 인젝션
	15:26:05	C2 통신	svchost.exe가 공격자 C2주소와 네트워크 연결 115.68.52.47
	15:27:53	악성파일 생성	svchost.exe가 악성 파일 생성 C:\Windows\System32\wptsextensions.dll (확보)
22/11/15	11:32:36	파일 생성	svchost.exe가 악성 파일 생성 C:\ProgramData\fswss.exe (미확보)
	11:32:48	파일 실행	fswss.exe를 이용한 네트워크 스캔 C:\ProgramData\fswss.exe /scan /UseIPAddressesRange 1 /IPAddressFrom 10.20.XXX.1 /IPAddressTo 10.20.XXX.255 /stext C:\ProgramData\fswss.log
	11:33:41	안티 포렌식	악성파일 이름 변경 이름 변경: C:\ProgramData\fswss.exe -> xeudsgpfo (미확보)
	12:50:13	악성파일 생성	svchost.exe가 파일 생성 C:\ProgramData\fmsysn.exe (미확보)
	12:51:04	악성파일 실행	svchost.exe가 다른 프로세스 실행 C:\ProgramData\fmSysN.exe 10.20.XXX.1 10.20.XXX.36 XXXXX 10 c:\programdata\fmSysN.log

	13:06:49	안티 포렌식	악성파일 이름 변경 이름 변경: C:\ProgramData\fmsysn.exe -> yfvepuvxbi (미확보)
	16:18:52	네트워크 접근	svchost.exe가 PC01의 인증서 소프트웨어 포트에 접근 시도 10.20.XXX.125:XXXXX(PC01)
	16:33:06	악성파일 생성	svchost.exe가 파일 생성 C:\ProgramData\skypeserver.exe (미확보)
22/11/18	9:49:31	네트워크 접근	svchost.exe가 PC01의 인증서 소프트웨어 포트에 접근 시도 10.20.XXX.125:XXXXX(PC01)
	9:51:07	악성파일 생성	svchost.exe가 악성파일 생성 C:\ProgramData\skypeserver.exe (미확보)
	9:56:31		svchost.exe가 악성파일 생성 C:\ProgramData\sfbappsdk.dll (미확보)
	10:00:08	C2 통신	skypeserver.exe가 공격자 C2주소와 네트워크 연결 121.78.246.155(dalbinews.co.kr)
	10:00:27	네트워크 접근	skypeserver.exe가 인증서 소프트웨어 포트에 접근 성공 10.20.XXX.125:XXXXX(PC01)
	10:06:14	안티 포렌식	악성파일 이름 변경 이름 변경: C:\ProgramData\sfbappsdk.dll -> bxikemvkqhcsz (미확보)
	10:06:42		악성파일 이름 변경 변경 전: C:\ProgramData\skypeserver.exe -> kqcfqbxrgbfmwem (미확보)
	11:04:32	인젝션 C2 연결	정상 프로세스(svchost.exe)에 악성 스레드 인젝션 svchost.exe가 공격자 C2주소와 네트워크 연결 121.78.158.46(studyholic.co.kr)
	11:05:45	보안 제품 무력화	V3가 보안 제품 무력화 행위 탐지 (Exploit/Win.Lazardoor.GEN)
	11:06:56	취약한 드라이버 파일 생성	악성코드 생성 C:\ProgramData\perlcritic.exe (미확보)
	11:07:02		악성코드 실행 C:\ProgramData\perlcritic.exe (미확보)취약한 드라이버 파일 생성 C:\Windows\System32\drivers\PROCEXP152.SYS (확보)
	11:12:18		악성코드 생성 및 실행 C:\ProgramData\perlcritic64.exe (미확보)

[표] PC02에서 발견된 공격자의 악성 행위

주요 악성 행위

BYOVD에 의한 V3 무력화

PC01, PC02 두 시스템에서는 각각 11/18 10:20:28, 11:05:45에 V3 무력화 시도가 탐지(Exploit/Win.Lazardoor.GEN)됐으며, 이후 V3가 무력화된 기간은 다음과 같다.

- PC01: 11/18 10:20:28 ~ 11/18 11:25:00 (약 1시간)
- PC02: 11/18 11:05:45 ~ 11/21 14:07:08 (약 75시간)

해당 기간에는 V3 관련 프로세스는 동작 중이나, 정상적인 행위 탐지가 되지 않는다. 하지만 시스템이 재부팅되고 나면 V3는 다시 정상화된다.

[그림] PC01에서 확인된 V3 무력화 탐지 로그

공격자가 Windows 시스템에서 커널 메모리를 조작해 보안 제품의 동작을 방해하기 위해서는 커널 메모리에 접근할 수 있는 권한이 필요한데, 이를 위해 지난 5월에는 대만의 부품 업체인 ENE Technology의 ene.sys를 이용한 BYOVD 공격을 사용했었다.

PC01과 PC02의 V3 무력화 탐지 시점에는 공격 방법을 식별할만한 흔적이 발견되지 않았다. 오히려 V3 무력화 발생 이후 취약한 드라이버 파일이 시스템에 생성됐는데, 해당 드라이버 파일은 마이크로소프트사에서 무료로 제공하는 프로세스 관리 유틸리티인 ProcessExplorer의 PROCEXP152.SYS 드라이버 파일이며, BYOVD 공격에 사용 가능한 취약한 드라이버다. 하지만 이 드라이버 파일은 PC01, PC02 모두에서 V3 무력화 이후 생성됐고, 공격자가 생성한 perlcritic.exe(미확보) 파일에 의해 사용됐다.

즉, V3 무력화 발생 시간과 드라이버 파일 생성 시간의 순서의 전후가 맞지 않아 BYOVD 공격인지, PROCEXP152.SYS가 V3 무력화에 사용됐는지는 아직 단정지을 수는 없다

5월에 발생된 방법과 11월에 발생된 방법은 다음과 같은 차이점을 가진다.

CATEGORY	ATTACK IN MAY, 2022	ATTACK IN NOVEMBER, 2022
공격 기법	BYOVD 기법	확인되지 않음
취약한 드라이버	ENE Technology의 드라이버 • ene.sys	마이크로소프트사의 ProcessExplorer 드라이버가 V3 무력화 이후 생성됨 PROCEXP152.sys
로더	sb_smbus_sdk.dll	• perlcritic.exe (미확보)

		• perlcritic64.exe (미확보)
서비스 등록 여부	서비스 등록됨	서비스 등록 흔적 없음

[표] 5월과 11월에 발생한 V3 무력화 관련 흔적 비교

안티포렌식

PC01, PC02에서는 공격 흔적을 지우기 위해 안티포렌식 행위를 수행한 흔적이 확인됐다.

CATEGORY	SYSTEM	DESCRIPTION
파일의 타임스탬프 조작	PC01, PC02	[PC01] • C:\Windows\System32\LegacyUserManager.dll ◦ 조작된 생성시간 : 2019-03-19 13:49:35 • C:\ProgramData\Microsoft\Crypto\Keys\Keys.dat ◦ 조작된 생성시간 : 2019-03-19 13:49:35 ◦ 조작/된 생성시간 : 2019-12-25 23:24:06 • C:\ProgramData\Microsoft\Settings\Settings.vwx ◦ 조작된 생성시간 : 2022-05-13 16:09:19 [PC02] • C:\Windows\system32\wptsextensions.dll ◦ 조작된 생성시간 : 2019-03-19 13:49:35
파일명 변경 후 파일 삭제	PC01, PC02	[PC01] • C:\ProgramData\tszui.tmp -> phqghumea • C:\ProgramData\perlcritic.exe ->kxlmatmoynktxl • C:\ProgramData\tds.tmp -> mxnsbqy [PC02] • C:\ProgramData\fswss.exe -> xeudsgpfo • C:\ProgramData\fmsysn.exe -> yfvepuvxbi • C:\ProgramData\sfbappsdk.dll -> bxikemvkqhcsz • C:\ProgramData\skypeserver.exe -> kqcfqbxrgbfmwem
Prefetch 삭제	PC01	MSIEXEC.EXE-8FFB1633.pf, PERLCRITIC.EXE-2EB3AC0F.pf 외 다수

[표] PC01, PC02에서 확인된 안티포렌식 행위

공격자가 사용한 악성코드

악성코드 목록

CATEGORY	FILENAME	SYSTEM	DESCRIPTION
로더	wptsextensions.dll	PC02	• 경로: C:\Windows\System32\wptsextensions.dll • 백도어 파일 Keys.dat를 로드

	legacyusermanager.dll	PC01 PC02	• 경로: C:\Windows\System32\legacyusermanager.dll • 백도어 파일 Keys.dat를 로드
	lum.tmp	PC02	• 경로: C:\Windows\Temp\lum.tmp • 백도어 파일 configmanager.tlb를 로드
백도어	Keys.dat	PC01 PC02	• 경로: C:\ProgramData\Microsoft\Crypto\Keys\Keys.dat wptsextensions.dll에 의해 로드됨 • 2022/11/18 14:56:54 GMT +9 이후 동작하도록 설계되어 있으며, cmd.exe를 통해 추가 명령 수행 가능 • C2 서버로부터 추가 바이너리를 다운로드해 파일리스 형태로 실행함
	Settings.vwx	PC02	• wptsextensions.dll에 로드됨 • 아래 3개 C2 중 무작위로 접속 ◦ hxxps://www.artinsight[.]co.kr/data/admin/list.php ◦ hxxps://www.kfcjn[.]com/member/process/sms.php ◦ hxxps://ctmnews[.]kr/member/process/success.php
	Settings.vwx	PC01	• legacyusermanager.dll에 로드됨 • 아래 3개 C2 중 무작위로 접속 ◦ hxxps://www.artinsight[.]co.kr/data/admin/list.php ◦ hxxps://www.kfcjn[.]com/member/process/sms.php ◦ hxxps://ctmnews[.]kr/member/process/success.php
악용된 정상 파일	ProcEXP152.sys	PC01 PC02	• 경로: C:\Windows\System32\drivers\PROCEXP152.SYS • ProcessExplorer의 드라이버 • 취약한 드라이버 모듈로 BYOVD 공격을 통한 백신 무력화 가능
	fswss.exe	PC02	• 경로: C:\ProgramData\fswss.exe • NirSoft사의 유틸리티로, 네트워크를 스캔하거나 원격 컴퓨터를 켤 수 있는 기능 존재 • WakeMeOnLan: https://www.nirsoft.net/utils/wake_on_lan.html
미확보 파일	configmanager.tlb	PC02	• 경로: C:\Windows\System32\configmanager.tlb • lum.tmp에 의해 로드되는 백도어 추정
	perlcritic.exe perlcritic64.exe	PC01 PC02	• 경로: C:\ProgramData\perlcritic.exe • cmd.exe에 의해 실행되며, PROCEXP152.SYS를 로드함
	sfbappsdk.dll	PC02	• 경로: C:\ProgramData\sfbappsdk.dll • 인젝션된 svchost.exe가 생성

	fmSysN.exe	PC02	• 경로: C:\ProgramData\fmSysN.exe • 인젝션된 svchost.exe가 생성 • 다음과 같은 실행 흔적이 확인됨 ◦ fmSysN.exe 10.20.XXX.1 10.20.XXX.36 XXXXX 10 c:\programdata\fmSysN.log
	skypeserver.exe	PC02	• 경로: C:\ProgramData\skypeserver.exe • 인젝션된 svchost.exe가 생성 • C2 접속
	tds.tmp	PC01	• 경로: C:\ProgramData\tds.tmp • 랜덤한 파일명으로 변경된 후, 삭제됨
	tszui.tmp	PC01	• 경로: C:\ProgramData\tszui.tmp • 랜덤한 파일명으로 변경된 후, 삭제됨

[표] 악성코드 목록

공격자가 사용한 C2

CATEGORY	IP	DOMAIN	REMARKS
ftp.exe 최초 접근	111.92.189.48	www[.]scope.co.kr	
무력화 관련 C2 추정	121.78.158.46	www[.]studyholic.com	
	121.78.246.155	dalbinews[.]co.kr	
백도어 C2	183.110.224.172	ctmnews[.]kr	
	115.68.52.47	www[.]artinsight.co.kr	
	114.108.129.89	www[.]kfcjn.com	

[표] 공격자가 사용한 C2 목록

MITRE ATT&CK MAPPING

Tactics	TID	DESCRIPTION
Reconnaissance	–	–
Resource Development	T1587.001 Develop Capabilities: Malware	백도어 및 로더 제작
	T1587.004 Develop Capabilities: Exploits	인증서 소프트웨어 취약점 준비
	T1588.002 Obtain Capabilities: Tool	fswss.exe (Nirsoft의 wakemeonlan.exe)
Initial Access	N/A	
Execution	T1059.003 Command and Scripting Interpreter: Windows Command Shell	perlcritic.exe 실행
	T1203 Exploitation for Client Execution	인증서 소프트웨어 취약점 공격
Persistence	N/A	–

Privilege Escalation	T1068 Exploitation for Privilege Escalation	PROCEXP152.sys
Defense Evasion	T1562.001 Impair Defenses: Disable or Modify Tools	V3 무력화
	T1070 Indicator Removal	Prefetch 파일 삭제
	T1070.004 Indicator Removal: File Deletion	악성파일 삭제 – sfbappsdk.dll, fswss.exe, fmSysN.exe, skypeserver.exe, perlcritic.exe, perlcritic64.exe 크래시덤프 파일 삭제
	T1070.006 Indicator Removal: Timestomp	악성파일 시간정보 변경
Credential Access	N/A	–
Discovery	T1046 Network Service Discovery	fswss.exe, fmSysN.exe
Lateral Movement	T1210 Exploitation of Remote Services	인증서 소프트웨어 취약점을 이용한 내부 이동
Collection	N/A	–
Command and Control	T1071.001 Application Layer Protocol: Web Protocols	C2서버 통신
	T1102 Web Service	정상 도메인을 C2 서버로 악용
Exfiltration	N/A	–
Impact	N/A	–

IoC

악성 파일

No	MD5 Hash	File Name	AhnLab Detection Name
1	61B3C9878B84706DB5F871B4808E739A	wptsextensions.dll	Trojan/Win.Lazardoor.C5327680
2	C7256A0FBAB0F437C3AD4334AA5CDE06	legacyusermanager.dll	Trojan/Win.Lazardoor.C5327680
3	A6602EF2F6DC790EA103FF453EB21024	lum.tmp	Trojan/Win.Lazardoor.C5327681
4	FC8B6C05963FD5285BCE6ED51862F125	Keys.dat (PC01)	Data/BIN.Lazarus
5	6EA4E4AB925A09E4C7A1E80BAE5B9584	Keys.dat (PC02)	Data/BIN.Lazarus
6	27DB56964E7583E19643BF5C98FFFD52	Settings.vwx (PC01)	Data/BIN.Lazarus
7	BD47942E9B6AD87EB5525040DB620756	Settings.vwx (PC02)	Data/BIN.Lazarus

악성 IP/URL

No	IP	DOMAIN	Country
1	111.92.189.48	www[.]scope.co.kr	KR
2	121.78.158.46	www[.]studyholic.com	KR
3	121.78.246.155	dalbinews[.]co.kr	KR

4	183.110.224.172	ctmnews[.]kr	KR
5	115.68.52.47	www[.]artinsight.co.kr	KR
6	114.108.129.89	www[.]kfcjn.com	KR

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

Categories: 악성코드 정보

Tags: A-FIRST,BYOVD,DFIR,침해사고사례,Lazarus

Leave a Comment