National Cyber Security Centre
a part of GCHQ

2023. 11. 23

북한 해킹조직의 소프트웨어 공급망 공격 위협

개요(Overview)

대한민국 국가정보원(이하 국가정보원)과 영국 국가사이버안보센터(이하 NCSC)는 북한 해킹조직이 정부기관, 금융기관 및 방산업체 등에서 널리 사용 중인 소프트웨어 제품을 대상으로 다수의 공급망 공격 시도를 확인하였습니다.

국가정보원과 NCSC는 사전에 피해를 예방하고 이에 대한 경각심을 고취하기 위해 합동 사이버보안 권고문(CSA)을 발표합니다. 사이버보안 권고문에는 북한 해킹조직이 글로벌 공급망 공격에 사용한 전략, 전술 및 절차(TTPs)와 이를 예방하기 위한 대책을 포함하고 있습니다.

상세 정보

북한 해킹조직의 공급망 공격은 지속적으로 증가하고 있으며, 그 수법과 피해 규모는 확대·지능화되고 있습니다. 최근 국내외에서 다수기관이 사용중인 소프트웨어 제품에 대한 공격이 확인되었고, 여기에 제로데이(0-day) 및 소프트웨어 공급망 공격기법이 사용되었습니다.

국가정보원과 NCSC는 북한의 공급망 공격이 북한 정권의 우선목표 지원에 상당 부분 기여하고 있다고 간주합니다. 여기에는 수익 창출과 스파이 활동이 포함되며, 국방 분야에 국한하지 않고 다양한 분야에 걸쳐 첨단기술을 절취 합니다.

공급망 공격은 보안 수준이 높은 수많은 공격 대상을 감염시킬 수 있는 매우

효과적인 수단입니다. 소프트웨어 공급업체, 관리형 서비스 공급자(MSP), 클라우드 등 공급망의 여러 요소가 공격받기 쉽다는 것이 확인되었습니다. 이를 통해 공격자는 다수의 기관과 사용자를 무차별적으로 공격 대상으로 삼을 수 있습니다. 이 공격은 향후 랜섬웨어 공격으로 확대되거나 전환되어 금전을 요구하거나 시스템 파괴까지 초래할 수 있습니다.

공격자들은 정상적인 소프트웨어와 하드웨어를 사용하기 때문에 방어자 입장에서 공격을 탐지하기가 어려울 수 있습니다.

이런 위협이 증가하는 상황에서 기관 자체 실정에 맞는 소프트웨어 공급망 제품의 안전한 보안관리 및 피해 회복력 제고 등에 대한 보안대책 수립과 운영이 필요합니다.

기술적 사항(Technical Details)

북한 해킹조직들은 이번 소프트웨어 공급망 공격에서 제로데이 취약점 악용, 공개 취약점 및 도구를 사용하였으며, 다수 취약점을 연쇄적으로 사용하여 특정 타깃을 집중적으로 공략하는 치밀한 형태도 확인되었습니다.

다음은 북한 해킹조직들이 최근 공급망 공격사례에 대한 공격 절차 및 수법입니다.

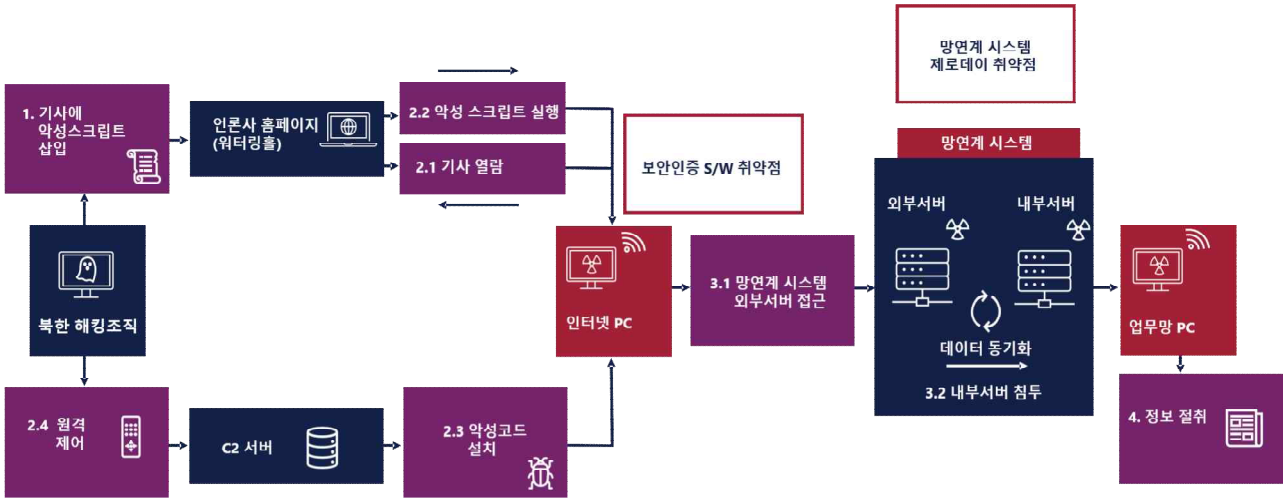
① 제로데이 취약점을 이용한 다양한 공급망 제품 공격

2023년 3월, 공격자는 물리적으로 망분리된 타깃 기관의 내부망에 침투하기 위해 보안인증 소프트웨어, 망연계 장비 소프트웨어의 취약점을 연쇄적으로 악용하였습니다. 최초 MagicLine4NX 보안인증 소프트웨어 취약점을 통해 타깃의 인터넷 PC에 침투한 후 망연계 장비의 제로데이 취약점을 악용하여 내부망으로 확산, 정보절취를 시도하였습니다.

아래에는 2개 공급망 제품에 대한 복합적이고 연쇄적인 공격 절차를 설명하고 있습니다.

공격 절차

Figure 1.



1. 공격자는 언론사 홈페이지를 해킹하여 특정 기사에 악성 스크립트를 은닉, 워터링홀을 구축합니다. 악성 스크립트는 특정 IP 대역이 접속할 경우 동작하게 구현되어 있습니다.

2. 피해자는 보안인증 소프트웨어가 설치된 인터넷 PC로 해당 기사를 열람하면 소프트웨어에 내재된 취약점에 의해 악성 스크립트가 동작합니다. 피해자 PC가 C2 서버에 접속하면 악성코드가 설치되고, 공격자는 C2 서버를 통해 피해자 PC에 대한 원격제어 권한을 획득합니다.

3. 공격자는 망연계 제품 취약점을 통해 인터넷 PC에서 외부서버로 권한없이 접근할 수 있었으며, 망연계 제품의 데이터 동기화 기능을 악용하여 내부서버에 악성코드를 전파합니다. 공격자는 최종적으로 업무 PC에 정보 절취용 악성코드를 감염시킵니다.

4. 업무 PC에 설치된 악성코드는 2개의 C2 서버주소를 가지고 있습니다. 1차 C2 서버는 망연계 제품 내부서버인데, 중간에서 게이트웨이 역할을 담당합니다. 2차 C2는 실제 외부 인터넷에 위치한 서버입니다. 이 악성코드는 초기 감염신호를 전송하고 암호화된 추가 페이로드를 다운로드 받아 실행

하는 기능이 있습니다. 악성코드는 초기 감염신호를 C2서버에 전송하기 위해 망연계 제품 내부서버에서 외부서버로 이동을 시도하지만 다행히 제품의 보안 정책에 의해 차단되게 됩니다. 차단되지 않았다면 내부망에 저장된 대량의 정보가 유출될 수 있었습니다.

C2 서버, 악성코드 MD5, 암호화 알고리즘 및 실행파일 인증서는 침해지표 섹션을 참고하시기 바라며, 보안인증 소프트웨어 공격에 대한 자세한 정보는 다음 블로그에서 확인할 수 있습니다.

Ahnlab - https://asec.ahnlab.com/en/57736, https://asec.ahnlab.com/ko/50134

요약 및 예방조치

공격자는 초기에 워터링홀 공격을 통해 목표를 확보하고, 이중 특정 타깃에 대해 추가 공격을 시도했습니다. 이는 공급망침해가 또 다른 공급망침해로 이어진 사례로, 특정 타깃 대상의 정밀공격이었습니다. 공격자는 망연계 장비의 알려지지 않은 취약점과 정상기능을 악용하여 내부망으로 직접 침투하는 고도의 공격기법을 사용하였습니다.

이러한 공격의 예방을 위해서는 프로그램 설치목록 중 취약한 버전의 소프트웨어가 설치되어 있는지 확인하고 최신버전으로 업데이트하기를 권고합니다.

취약한 버전은 MagicLine4NX 1.0.0.1 ~ 1.0.0.26 입니다.

망연계 장비 관리자페이지에 대한 접근제한을 적용하고 비인가서비스, 통신 유무 등을 점검하시기 바랍니다.

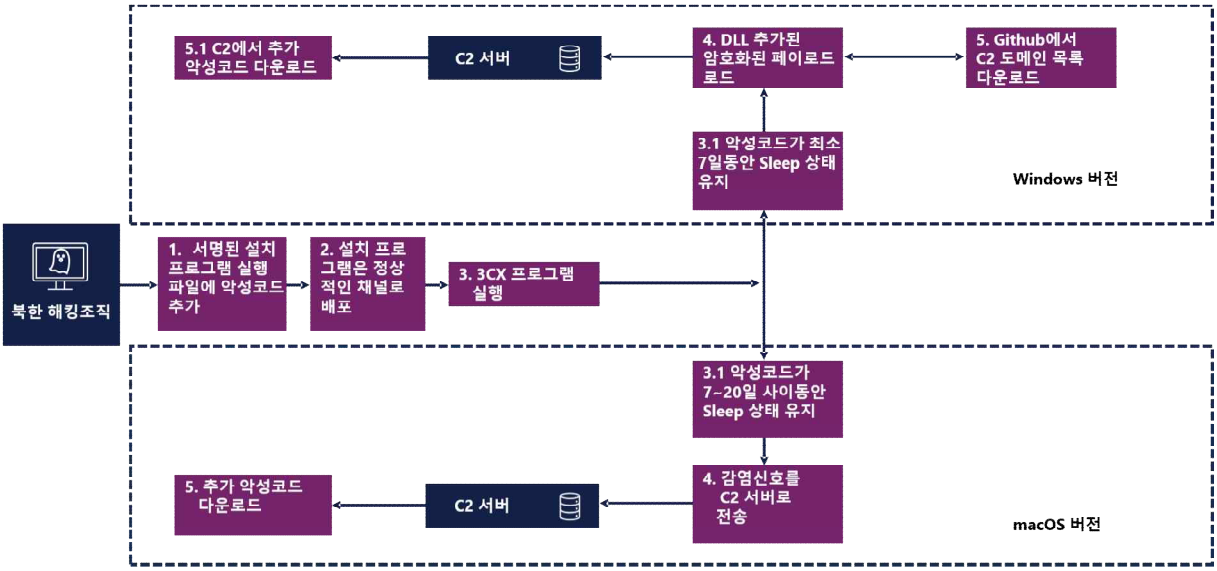
취약 버전 확인 방법에 대한 자세한 정보는 아래 대한민국 국가사이버안보센터 홈페이지의 보안 권고문을 참고하시기 바랍니다

보안인증 S/W 舊버전 보안조치 안내

② 3CX 소프트웨어 감염

2023년 3월, 3CX가 배포하는 Desktop App 소프트웨어가 손상되었으며 macOS와 Windows 운영체제 모두에 영향을 미치는 악성프로그램이 포함되어 있다는 공개 보고서가 SentinelOne과 Sophos에 등록되었습니다. 이는 중대한 글로벌 공급망 공격으로 이어졌습니다. 이 해킹사고는 나중에 3CX에 의해 확인되었습니다.

Figure 2.



2023년 6월, NCSC는 3CX 공급망 공격에 관련된 macOS 악성코드에 대한 악성코드 분석보고서를 발표했습니다. 이름은 Smooth Operator입니다.

Windows 버전의 공격 절차

1. 공격자들은 3CX 소프트웨어를 위해 서명된 설치 프로그램 실행파일 내부에 악성코드를 추가했습니다.

2. 설치 프로그램은 합법적인 경로를 통해 고객들에게 배포되었으며, 공격자들은 3CX 네트워크를 침투하여 3CX 소프트웨어의 빌드 프로세스를 조작할 수 있는 위치에 있었던 것으로 알려졌습니다.

3. 3CX 소프트웨어가 실행되었을 때 악성코드는 최소 7일 동안 백그라운드에서 대기(Sleep)하고 있지만, 3CX 소프트웨어는 정상적으로 계속 실행됩니다.

4. 대기시간이 지나면 악성코드는 암호화된 페이로드를 로드하며, 페이로드는 3CX 소프트웨어에 포함된 DLL에도 추가됩니다.

5. 페이로드는 GitHub 저장소에서 공격자가 제어하는 명령 및 제어(C2) 도메인 목록을 다운로드한 후 다음 단계를 다운로드하기 위해 해당 도메인 중 하나와 연결하는 역할을 합니다.

6. 이후로 관찰된 유일한 단계는 브라우저 정보절취로 Brave, Chrome, Edge 및 Firefox 브라우저에서 기본 피해자시스템 데이터, 피해자 3CX 계정정보 및 브라우저 기록을 추출하고 필터링합니다.

Windows 공격에 대한 자세한 정보는 ESET과 Sophos 업체 블로그에서 확인할 수 있습니다

macOS 버전의 공격 절차

1. 공격자들은 서명 및 인증된 3CX 어플리케이션 실행파일 내부에 악성코드를 추가했습니다.

2. 어플리케이션은 합법적인 경로를 통해 고객들에게 배포되었습니다. 공격자들은 3CX 네트워크를 침투했기 때문에 3CX 소프트웨어의 빌드 프로세스를 조작할 수 있는 위치에 있었던 것으로 알려져 있습니다.

3. 3CX 소프트웨어가 실행되었을 때 악성코드는 7~20일 사이에 백그라운드에서 대기(Sleep)하고 있지만, 3CX 소프트웨어는 정상적으로 계속 실행됩니다.

4. 사용자 지정 난독화 방법을 사용하여 악성코드가 공격자가 제어하는 C2

(명령제어) 서버에 감염신호를 전송하고, 이때 기본적인 감염 컴퓨터 정보가 포함됩니다.

5. C2 서버는 피해자 컴퓨터가 실행할 추가 악성단계를 제공할 수 있으며, 유일하게 관찰된 추가단계는 피해자 컴퓨터의 구성파일에서 3CX 계정 정보를 수집하고 이를 공격자가 제어하는 C2 서버로 전송합니다.

macOS 공격에 대한 자세한 정보는 NCSC 악성코드 분석리포트를 확인하시면 됩니다.

요약 및 예방조치

2023년 4월초, NCSC는 3CX Desktop App 보안문제에 대한 조언을 웹사이트에 게시했습니다.

엔드포인트 탐지 및 대응 솔루션에 의해 악성 업데이트가 신속하게 탐지되었기 때문에 이러한 보안 침해의 부정적인 영향은 제한적이었습니다.

사용자가 영향을 받는 버전을 실행하는 경우 소프트웨어 제거를 위해 공급업체에서 게시한 가이드라인을 따르도록 권고합니다.

피해 완화(Mitigations)

공급망 공격은 규모와 시점에 상관없이 발생할 수 있으므로 다양한 대책을 수립해야 합니다. 국가정보원과 NCSC는 공급망위협을 억제하기 위해 아래와 같은 완화 조치, 공급망 라이프사이클에 따른 사이버 보안원칙, 관리 및 기술적 보안 조치를 시행할 것을 권고합니다.

관리적 보안대책

- 공급망 사이버보안에 대한 조직의 인식을 높이고 이 문제에 대한 이해를 촉진합니다.

- 조직 구성원이 악의적인 전술과 공격을 탐지하고 이를 보고하도록 정기적으로 사이버보안에 대한 교육을 제공합니다.

- 조직의 공급망에 대한 위협을 파악하고, 위협 우선순위를 결정하며, 악의적인 사이버 활동이 발생했을 때의 영향을 평가하여 사각지대를 제거합니다.

- 중요 데이터에 대한 액세스포인트를 확인하고 액세스권한을 가진 구성원을 식별하여 제공함으로써 액세스권한을 최소화합니다.

기술적 보안대책

- 알려진 취약점으로 인한 위협을 완화하기 위해 공급망 소프트웨어, 운영체제 및 백신 프로그램의 최신 버전을 유지관리합니다.

- 권한 없는 사용자의 무단 로그인을 방지하기 위해 관리 및 운영 로그인 정책에 대해 2단계 인증을 채택합니다. NCSC는 온라인 서비스에 대한 다중 요소 인증 및 단말 보안 가이드라인을 제공하고 있습니다.

- 공급망 소프트웨어 애플리케이션에서 비정상적인 트래픽이 감지되는 경우도 있으므로 네트워크 인프라를 정확하게 모니터링합니다.

- 공급망보안 위협을 완화하기 위해 다양한 기관에서 발행된 문서들을 참고하시기 바랍니다.

  1. 공급망 공격의 이해(국문) – 대한민국 국가사이버안보센터(NCSC)

  2. 공급망 사이버보안 평가 – 영국 국가사이버안보센터(NCSC)

  3. 공급망 보안의 원칙 – 영국 국가사이버안보센터(NCSC)

  4. 소프트웨어 공급망 보안: 소프트웨어 자제명세서(SBOM) 사용에 대한 권장 사례 – 미국 CISA, NSA

5. 사이버 공급망 위험관리(C-SCM) – 미국 국립표준기술원(NIST)

6. SBOM를 위한 최소 요소 – 미국 전기통신정보국(NTIA)

해킹사고 신고 안내

해킹사고 의심 및 유사사례 발견 시 아래 기관에 문의하시기 바랍니다.

대한민국 기관 : 국가정보원(https://www.nis.go.kr, 111)

영국 기관 : 국가사이버안보센터(NCSC, https://report.ncsc.gov.uk)

관련 침해지표(IoC)

보안인증 SW 제로데이 취약점을 이용한 다양한 공급망 제품 공격

구분	침해지표	비고
경유지	[C2 URL]/search/sch-result3.asp	HTTPS 통신
복호화키	0x0c2a351837454a2661026f162530361a394e1d143334	ChaCha20 Key1
	0x0102350423062f085c000e02	ChaCha20 Key2
악성코드 (MD5)	316c088874a5dfb8b8c1c4b259329257	다운로더 (SamsungDeviceControl.exe)
	33ca34605e8077047e30e764f5182df0	다운로더 (SamsungDevicePanel.exe)
위장 인증서	Samsung SDS Co., Ltd.	업체명
	0139981ad983bf73e9514d2d4237929e	일련번호
	2022.12.13 ~ 2023.07.20	시작일~만료일

3CX 소프트웨어 감염, macOS 버전

구분	침해지표	비고
경유지	https://msstorageazure[.]com/analysis	
	https://officestoragebox[.]com/api/biosync	
	https://visualstudiofactory[.]com/groupcore	
	https://azuredeploystore[.]com/cloud/images	
	https://msstorageboxes[.]com/xbox	
	https://officeaddons[.]com/quality	
	https://sourceslabs[.]com/status	
	https://zacharryblogs[.]com/xmlquery	
	https://pbxcloudeservices[.]com/network	
	https://pbxphonenetwork[.]com/phone	
	https://akamaitechcloudservices[.]com/v2/fileapi	
	https://azureonlinestorage[.]com/google/storage	
	https://msedgepackageinfo[.]com/ms-webview	
	https://glcloudservice[.]com/v1/status	
	https://pbxsources[.]com/queue	
	https://sbmsa[.]wiki/blog/_insert	데이터 유출 URL
	msstorageazure[.]com	
	officestoragebox[.]com	
	visualstudiofactory[.]com	
	azuredeploystore[.]com	
	msstorageboxes[.]com	
	officeaddons[.]com	
	sourceslabs[.]com	
	zacharryblogs[.]com	
	pbxcloudeservices[.]com	

구분	침해지표	비고
	pbxphonenetwork[.]com	
	akamaitechcloudservices[.]com	
	azureonlinestorage[.]com	
	msedgepackageinfo[.]com	
	glcloudservice[.]com	
	pbxsources[.]com	
	sbmsa[.]wiki	데이터 유출 도메인
악성코드 (MD5)	d5101c3b86d973a848ab7ed79cd11e5a	3CX DMG
	660ea9b8205fbd2da59fefd26ae5115c	3CX dylib, libffmpeg.dylib
	5faf36ca90f6406a78124f538a03387a	Smooth Operator 2단계 페이로드, UpdateAgent
악성코드 (SHA1)	3dc840d32ce86cebf657b17cef62814646ba8e98	3CX DMG
	9e9a5f8d86356796162cee881c843cde9eaedfb3	Smooth Operator 2단계 페이로드, UpdateAgent
	769383fc65d1386dd141c960c9970114547da0c2	3CX dylib, libffmpeg.dylib
악성코드 (SHA-256)	e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	3CX DMG
	a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67	3CX dylib, libffmpeg.dylib
	6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59	Smooth Operator 2단계 페이로드, UpdateAgent
기타	.main_storage	피해자 ID 및 sleep time 파일
	UpdateAgent	2단계 페이로드