Bundesamt für Verfassungsschutz

2024. 2. 19

북한의 방산분야 대상 사이버위협 주의

요약(Summary)

대한민국 국가정보원(NIS)과 독일 헌법보호청(BfV)은 북한 해킹조직이 방위산업 분야의 기업·연구소를 대상으로 한 사이버공격의 피해 예방을 위해 두 번째 합동 사이버보안 권고문을 발행합니다.

북한은 자국 국방력 강화를 정권 우선순위에 두고 전 세계를 대상으로 방산 첨단기술 절취에 주력하고 있습니다. 북한은 절취한 무기 기술로 현재 보유 중인 재래식 무기에 대한 성능개량 및 현대화를 비롯해, 탄도미사일·정찰위성·잠수함 등 전략무기를 개발하는 데도 활용하고 있는 것으로 추정됩니다. 북한에 있어서 사이버 첩보활동은 무기 기술을 획득하기 위한 저비용의 효율적인 수단입니다.

이 사이버보안 권고문은 북한이 해킹 활동에 사용된 공격 전략·기술·절차(TTPs)와 침해지표(IoCs)를 포함하고 있으며, 2가지 대표적인 방산 시설 침투 사례를 소개하고 있습니다.

국정원과 헌보청은 이번 권고문에 포함된 방산분야 해킹 사례의 공격 주체를 북한의 라자루스 및 기타 북한 해킹조직으로 평가하고 있습니다.

첫 번째 북한 해킹조직은 전통적으로 외교·안보전문가 대상으로 스피어피싱 공격을 주로 수행하는 것으로 알려져 있으나, 최근에는 방산과 금융분야까지 공격을 확대하는 양상을 보이고 있습니다. 두 번째 라자루스 해킹조직은 광범위한 사이버 공격들에 연루되어 국제적으로 주목받는 악명높고 정교한 해킹조직

입니다. 라자루스는 고난도 공격 역량을 가지고 있으며 금전 탈취·랜섬웨어 공격·사이버 첩보활동 등 세간의 이목을 끄는 사건에 연루되어 있습니다. 방산 분야 사이버 공격으로 전 세계에서 절취한 민감·기밀정보는 북한 국방력 강화에 도움을 줄 수 있습니다.

해킹조직은 공격 인프라를 빈번하게 변경하며 전 세계 기관들을 지속해서 공격하기 때문에 앞으로도 유사한 공격이 있을 것으로 예상하고 있습니다. 이번 합동 사이버보안 권고문은 방산 분야 등에 보안을 강화하고 사이버 위협 정보를 제공하기 위해 발행되었습니다.

기술적 사항(Technical Details)

다음은 2가지 대표적인 방산 분야 대상 체계적인 공격사례를 설명합니다. 공격에 사용된 TTPs를 적용했을 때 첫 번째 사례는 북한 해킹조직이 방산 연구시설을 공격한 것이며, 두 번째는 라자루스 해킹조직의 사회공학적 공격사례를 서술한 것입니다.

① 웹사이트 유지보수 업체를 통해 방산 연구 시설 침투

최근들어 북한은 2023년 9월 신형 잠수함을 건조하는 등 해군력 강화에 주력해 왔는데, 그에 앞서 2022년 연말에 북한 해킹조직이 해양·조선 기술을 연구하는 기관에 침투하는 사건이 발생하였습니다. 당시 공격자는 기관에 직접 침투하기보다 홈페이지 서버 유지보수 업체를 해킹하고 이를 교두보로 기관에 침투하는 공급망 공격 수법을 사용하였습니다.

또한, 공격자는 기관의 패치관리시스템(PMS)을 통해 원격제어 악성코드를 유포하여 침투하고 다양한 업무시스템의 계정정보 및 이메일 내용을 절취 하였습니다. 아래는 침투 과정을 MITRE ATT&CK[1]와 연계하여 설명합니다.

1) MITRE ATT&CK는 실제 관찰을 기반으로 한 공격자의 전술·기술을 공격 단계별로 기술하고 있는 지침서이며, 전 세계적으로 활용되고 있습니다.

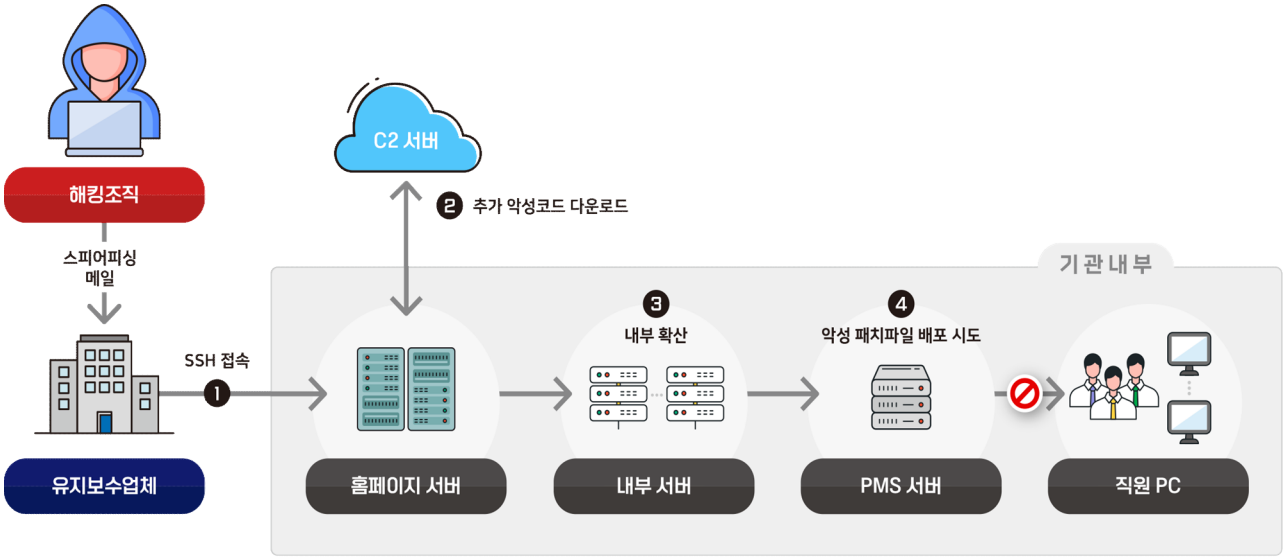

그림 1 공격 절차 개요도

공격 절차

1. 공격자는 기관 홈페이지 유지보수 업체를 침투하여 기관의 SSH 접속 계정을 절취 하였습니다. 이를 통해 공격자는 원격에서 기관 홈페이지 서버(Linux)에 접근하였습니다. (T1133)

2. 공격자는 curl 등 정상 도구를 사용하여 C2 서버에서 추가적인 악성파일을 내려받았고, 그중에는 원격 접속을 위한 터널링 도구(Ngrok), Base64 인코딩된 파이썬 스크립트(다운로더 기능)도 포함되어 있습니다. (T1059)

3. 공격자는 내부 확산을 위해 홈페이지 관련 다른 서버들까지 SSH 접속하였고, 접속한 서버에서 tcpdump를 실행하여 패킷을 수집하였습니다. 수집된 패킷을 통해 네트워크에 대한 추가정보를 확보한 후 직원들의 계정정보도 절취하였습니다. (T1040, T1046, T1021)

4. 공격자는 절취한 전산 담당자 계정정보로 이메일에 접속하여 PMS의 운영 방식에 대한 정보를 수집하였습니다. 이후 공격자는 전산 담당자를 사칭해 PMS 유지보수업체 직원에게 패치파일 제작을 의뢰하는 이메일을 보냈습니다. 해당 패치파일은 정상파일로 위장되었으나 악성코드가 삽입된 패치파일로, 해당 담당자가 사전에 이를 인지하여 PMS를 통한 악성 패치파일 배포 시도는

실패하였습니다. 해당 악성코드는 파일 업·다운로드, 프로그램 실행, 시스템 정보수집 등의 기능을 포함하고 있습니다. (T1041, T1001, T1071)

5. 기관의 보안 조치 이후에도 공격자는 웹사이트 파일 업로드 취약점을 이용하여 웹쉘을 업로드하거나, 직원에게 악성코드가 포함된 스피어피싱을 발송하는 등 공격을 지속 시도하였습니다.

MITRE 공격 매트릭스 for Enterprise Linux platform(v14)

공격 전술 (Tactics)	공격 기술 (Techniques)	사용 형태 (Description)
초기 접근(TA0001)	외부원격 서비스(T1133)	SSH
실행(TA0002)	명령 및 스크립트(T1059)	tcpdump, ngrok, curl
지속성(TA0003)	유효한 계정(T1078)	서버 관리자 계정, 직원 이메일 계정, SSL-VPN 계정
방어 회피(TA0004)	침해지표 삭제(T1078) 파일 또는 정보 난독화·디코딩 (T1140)	파일 삭제, 파일 암호화·디코딩
자격증명 접근 (TA0006)	네트워크 스니핑(T1040)	tcpdump
탐색(TA0007)	네트워크 스니핑(T1040) 네트워크 서비스 검색(T1046)	tcpdump
내부 확산(TA0008)	원격서비스(T1021)	SSH
수집(TA0009)	정보 저장소의 데이터(T1213)	웹사이트 소스코드, 서버 환경설정 정보
명령 및 제어 (TA0011)	데이터 난독화(T1001) 애플리케이션 프로토콜(T1071) 프로토콜 터널링(T1572)	AES-256, HTTP 프로토콜 사용, ngrok
유출(TA0010)	C2를 통한 유출(T1041)	HTTP C2 서버

주요 사항(Key Findings)

공격자는 기관을 직접 침투하는 방법보다는 협력업체를 먼저 공격하였습니다. 기관들은 코로나-19 팬데믹을 겪으면서 전산 인프라에 대한 현장 유지보수가 어렵게 되자 원격 유지보수를 허용해주었는데, 접근제어 없이 상시 접속을

허용하는 등 보안이 미흡한 상태로 운영하였습니다.

통상 공격자는 공격이 발각되어 보안조치를 하게 되면 당분간 공격을 멈추는 것이 일반적이나, 이번 사례의 경우 PMS 배포가 차단되고 SSH 원격 접속이 막히자 공격자는 공격 지속성을 유지하기 위해 웹페이지에 웹쉘을 올리고 직원들에게도 스피어피싱 이메일을 발송하는 등 다양한 추가 공격을 시도하였습니다.

또한, 공격자는 보안수준이 높은 기관에 직접 침투하기보다는 상대적으로 침투가 용이한 유지보수업체를 우회하여 공격하였습니다. 이는 기관과 유지보수업체 간 신뢰를 악용한 것으로, 유지보수업체의 접근에 대한 무조건적인 신뢰는 권장하지 않습니다.

대한민국 국가·공공기관에서 협력업체의 원격 유지보수가 필요한 경우 대한민국 국가정보보안기본지침 제26조(용역업체 보안)를 참고해주십시오. 독일 국가·공공기관은 독일 연방 정보보안청(BSI)의 OPS.2.1과 OPS.1.2.5 지침을 참고하시면 예방에 도움이 됩니다.

② 북한 해킹조직의 사회공학적 공격

두 번째 사례는 라자루스 해킹조직의 사회공학적 공격사례입니다. 북한은 적어도 2020년 중반 이후로 이 수법을 악용하여 방산업체에 침투하였습니다. 모든 확인된 사례에서 공격대상이 구인과 관련된 난독화 악성파일을 받았기 때문에 “꿈의 직장 작전(Operation Dream Job)”으로 불리고 있습니다. 라자루스 해킹조직은 3년 이상 방산 분야에 공격 작전을 교묘하고 능숙하게 수행하였습니다. 이러한 조직화된 해킹조직은 사이버보안과 글로벌 보안에 위협이 됩니다.

그림 2 공격 절차 개요도

공격 절차(Attack Flow)

사회공학적 공격은 사람의 신뢰·호기심·두려움 또는 급박함을 이용하여 악의적인 목적을 달성하는 비기술적 수단입니다. 현재 사회공학적 공격은 인간의 심리를 이용하고 사람들을 조정하여 악성코드 감염을 유도하는 매우 효과적인 방법으로 알려졌습니다. 각 기업들의 보안활동이 강화되어 침투가 어려워지자 공격자들은 사회공학적 공격 수법을 널리 사용하게 되었습니다. 라자루스 해킹 조직의 기술적 전술은 달라졌지만, 사회공학적 공격 방법은 이전과 동일합니다.

1. 사회공학적 공격의 첫 번째 단계는 온라인 직업 포털에 프로필을 만드는 것입니다. 지금까지 조사된 사례들에서 해커는 실존 인물 프로필을 도용하거나 가짜 데이터를 이용하여 프로필을 만들었습니다. 두 유형 모두 프로필을 채용 담당자처럼 보이게 만들어 방산 분야 직원들에게 접근하였습니다. 프로필이 진짜인 것처럼 보이면 다음 단계로 넘어갑니다.

2. 공격자는 관심 회사 직원의 프로필을 살펴보고 공격대상을 물색합니다. 이들 중 내부 시스템과 같은 주요 자산에 접근 권한이 있을 것 같은 대상을 찾습니다.

3. 공격대상으로 적합한 직원을 찾을 경우, 친밀감과 신뢰를 얻기 위해 대상자의 소셜 미디어 연락망에 가입합니다. 이후 공격대상자에게 직업 포털 메시지로 대화를 시도합니다. 대화는 대부분 영어로 하며 최소 하루에서 몇 달까지

간단한 사업 이야기를 나누며 친밀감을 얻습니다. 이후 일자리를 권유하며 대상자가 관심 없어 할 때는 해당 일자리의 고연봉을 강조하는 등 설득합니다. 이후 채용을 위해 필요한 것처럼 대상자에게 WhatsApp, Telegram, Skype, Discord 등 다른 SNS에서의 소통을 요구합니다.

4. 공격자는 대상자를 다른 SNS로 유인에 성공한 경우, 회사의 보안을 회피하기 위해 아래와 같이 다양한 접근 방법을 사용했습니다.

   a. 공격자는 대상자가 관심이 있어 하는 고연봉의 일자리 제안 PDF와 악성코드가 포함된 PDF 리더를 보냅니다.

   b. 공격자는 일자리의 간략한 정보만을 가진 파일을 전송합니다. 만일 대상자가 자세한 정보를 알고 싶어 하는 경우, 공격자는 대상자의 회사 메일로 상세정보가 담긴 파일 링크 주소를 전송하여 대상자가 회사에서 열어보도록 유도합니다. 링크된 파일은 클라우드 서비스에 저장되어 있으며 악성코드가 포함되어 있습니다.

   c. 최근에는 프로그래머에게 일자리를 제안하며 채용 절차 중 하나로 코딩 테스트용으로 보이는 ISO 이미지가 담긴 압축파일을 전송합니다. 프로그래머가 코딩테스트를 위해 파일을 실행하면 기기가 악성코드에 감염됩니다.

   d. 최근 라자루스 해킹조직은 악성 VPN 클라이언트가 삽입된 압축파일을 전송하여 회사 네트워크의 접근 권한을 획득하려 합니다.

일반적으로 직장인은 주변 동료들에게 다른 일자리에 관해 이야기를 나누지 않기 때문에 공격자의 손에 놀아날 수 있습니다. 또한, 라자루스 해킹조직은 사이버 공격 중에 해킹 도구를 변경하고 상황에 맞게 도구도 개발하였습니다.

피해 완화(Mitigations)

합동 사이버보안 권고문에 포함된 예방 지침은 국정원과 헌보청의 실제 조사에 근거하여 작성된 것입니다.

- 직원들에게 사이버 공격의 최신 동향을 정기적으로 설명합니다. 이를 통해 구성원들은 변화되는 공격 수법도 이해하고 지속된 교육을 통해 실제 상황에서도 적절히 대처할 수 있습니다.

- 북한 해킹조직의 해킹 공격은 대부분 사회공학적 공격과 협력업체를 통해 우회하여 이루어지기 때문에 몇 가지 예방책을 고려해야 합니다.

협력업체를 통한 우회 공격 관련 주의사항

- 원격지에서 온라인 유지보수를 할 경우 기관에서 지정된 시스템에만 접근을 허용하여야 하며, 사용자 인증 후 접근 권한에 따른 접근통제가 필요합니다.

- 시스템 접속 이력 등 감사로그를 저장하고 유지하여야 하며 주기적으로 모니터링하여 비정상 접속을 탐지할 수 있어야 합니다.

- PMS 시스템은 공급망 공격에 활용될 가능성이 높으므로 사용자 인증체계, 패치 파일에 대한 검증, 최종 배포 단계에서 적절한 검증 및 확인 절차가 필요합니다.

- 웹사이트 구축시 항상 SSL/TLS 통신을 구현하면 공격자가 패킷을 캡쳐하더라도 계정정보 등 중요 정보가 노출되는 것을 방지할 수 있습니다.

- 직원들이 원격근무를 위해 SSL-VPN을 사용하는 경우 ID·PW 인증과 함께 다중 인증 수단을 적용하기를 권장합니다. 이 경우에도 다중 인증에 사용되는 OTP 인증키 등이 타인에 노출되지 않도록 주의하여야 합니다.

- 스피어피싱에 대한 예방법은 지난 韓獨 합동 사이버보안 권고문(2023.3) 피해완화 부분을 참고하시기 바랍니다.

사회공학적 공격 : 예방조치와 모범사례

- 사회공학적 공격에 대응하기 위한 주요 예방조치는 직원들에게 일반적인 사회공학적 공격사례에 대한 교육에서 시작됩니다. 여기에는 비밀번호가 걸려있는 문서나 링크와 같이 의심스러운 상황에 대해 경계심을 갖고 신속하게 판단하고 대처하는 것, 그리고 의심스러운 행위를 직원들이 편하게 보고할 수 있는 개방적인 문화를 조성하는 것이 포함됩니다.

- 민감정보에 대한 접근 권한을 최소화하는 것은 또 다른 완화 요인이 될 수 있습니다. 공통 취약점을 해결하기 위해 조직에 속한 모든 장비를 업데이트하고 패치하는 정기적인 계획을 수립하여야 합니다.

- 이러한 예방조치는 조직의 주요 부서와 지역 거점을 포함하여, 조직의 모든 국내외 지역에 적용하여야 합니다.

해킹사고 신고 안내

귀하의 기관에서 국가 배후 해킹사고 의심 및 유사사례 발견 시 아래 관련 당국에 문의하시기 바랍니다.

대한민국 기관 : 국가정보원(www.nis.go.kr, +82 111)

독일 기관 : 헌법보호청(www.verfassungsschutz.de, +49(0)30-18/792-3322)

관련 침해지표(IoC)

방산 분야의 웹사이트 유지보수 업체 대상 사이버 공격 침해지표

구분	침해지표(IoC)	비고
C2	connection.lockscreen.kro[.]kr/index.php	C2 URL
	updating.dothome.co[.]kr/microsoft/app/google	C2 URL
MD5	3c2aa3687ac9f466ce909e2cb12b07a5	원격제어 (EncryptModule_ Patch.exe)
	4631ef8db9c36b0f2534ac7193f2587e	악성스크립트 (JSE)
	607a2a8d2863c3144b8e901a16a76c33	웹쉘 (_banner.jsp)

방산 분야의 사회공학적 공격 침해지표

구분	침해지표(IoC)	비고
C2	chrysalisc[.]com	도메인
	sifucanva[.]com	도메인
	thefrostery.co[.]uk	도메인
	rginfotechnology[.]com	도메인
	job4writers[.]com	도메인
	contact.rgssm[.]in	도메인

SHA-1	7da62cdb447a7ae3ae7b5f67a511e7cf2b26c7df	Boeing_Asia_ERP_IT_SA.zip
	2e0d374f1e706ae1fa24558b54c5a1630302eab1	Boeing_Asia-ERP_IT_SA.iso
	294706ae0585abaf4e6c5e66a7f5141ac4281d57	Amazon VNC.exe
	127ced578e041f53b5988a7fefaa6e09e64f4bf9	AmazonVNC Viewer.exe
	3bc8acdd07c6d91652101d9c8b3326bee372a007	
	7906270679014234b70aa63dd89e8282a945919c	
	7b4d0d8e3bfcd634bc7d7a17fb546b7e8316a681	Amazon VNC.zip
	d5c8edb84e4ff33aea8865676ffe801ff0a71701	AMAZON_BSA_SKILL_ ASSESSMENT_V2.ZIP
	ac9021eb798de8323702a5aeb7c590f1ebaa3786	
	d5c8edb84e4ff33aea8865676ffe801ff0a71701	Amazon_BSA_SA_v2.iso
SHA-256	F3482A38BEFDCD7D0B87D86F24CDB209 028BD8471BAA6610548FB721086F5B85	Accenture_IT_SA.zip
	47999FA014B6CC5A2A71BE590C938303 71E259242DFDBA7FFA2698F1900919EC	Accenture_IT_SA.iso

사회공학적 공격 관련 YARA[2] 탐지규칙

다음 YARA 규칙은 Amazon VNC Viewer 파일의 동작을 분석한 결과이며, 위에서 제공한 해시값으로 적어도 세 개의 다른 Amazon VNC Viewer 샘플을 탐지할 수 있습니다. 아래 규칙은 제공된 IoC를 사용하여 어떻게 사이버 위협을 탐지하는지 보여줍니다.

(아래 Yara 규칙이 작동하려면 URL의 대괄호([])를 제거해야 합니다. 누군가 실수로 악의적인 링크를 클릭하는 것을 방지하기 위해 추가되었습니다.)

2) YARA는 패턴을 기반으로 악성코드를 식별하고 분류하는 데 유용한 탐지 프레임워크입니다.

```
rule operation_DREAMJOB_AMAZON_VNC {
meta:
        target_entity = “file”
condition:
        for any vt_behaviour_command_executions in
        vt.behaviour.command_executions:
                ( vt_behaviour_command_executions ==
                “C:\\Windows\\System32\\wuapihost.exe-Embedding”
        or
        vt_behaviour_command_executions == “\”%SAMPLEPATH%\\AmazonVNC
                Viewer.exe\” “)
        and
        for any vt_behaviour_http_conversations in vt.behaviour.http_conversations: (
                vt_behaviour_http_conversations.url == https://sifucanva[.]com/wp-
        includes/fonts/public/common.php)
}
```