JOINT CYBER SECURITY ADVISORY

사이버안보정보공동체
KCIC, Korea Cybersecurity Intelligence Community

2024. 8. 5

북한 해킹조직의 건설·기계 분야 기술절취 주의

요약(Summary)

대한민국 국가정보원·검찰청·경찰청·국군방첩사령부·사이버작전사령부 등 사이버안보 정보공동체(이하 정보공동체)는 북한 해킹조직이 우리나라의 건설·기계 분야를 대상으로 자행한 사이버공격의 위험성을 알리고 피해 예방 및 완화를 위해 합동 사이버 보안권고문을 배포합니다. 북한 해킹 활동에 사용된 공격 전략·기술·절차(TTPs) 및 침해지표(IoCs)를 포함하였습니다.

북한은 올해 1.15 개최한 제14기 제10차 최고인민회의에서 김정은이 '지방발전 20×10 정책'을 공식화한 후, 매년 20개 시·군에 현대화된 공업공장 건설을 추진하고 있습니다. 북한의 黨·軍·政은 앞다퉈 정책 관철을 위해 매진하고 있으며, 북한 해킹조직도 이와 다르지 않습니다. 정보공동체는 건설·기계 단체 및 지자체 공무원 대상 해킹 공격이 전년 대비 급증한 것을 확인하였으며 북한이 무단 절취한 우리나라의 건설·기계 및 도시건설 분야 자료들을 공업공장 건설과 지방발전 계획에 사용할 것으로 추정합니다.

정보공동체는 금번 사이버보안 권고문에 포함된 해킹 활동의 주체를 북한 정찰총국 산하 김수키[1] 및 안다리엘[2] 해킹조직으로 평가하며, 정찰총국 산하 2개 해킹조직이 같은 시기에 동일한 정책적 목적을 달성하기 위해 특정 분야를 집중 공격하는 것은 이례적인 것으로 철저한 대비가 필요합니다.

1) 산업계에서는 김수키(Kimsuky)를 루비슬릿(Ruby Sleet), APT43, 벨벳천리마(VelvetChollima) 등으로 명명

2) 안다리엘(Andariel)은 다크서울(Dark Seoul), 싸일런트천리마(Silent Chollima), 오닉스슬릿(Onyx Sleet) 등으로 불림

기술적 사항(Technical Details)

다음은 두 해킹조직의 대표적인 건설·기계분야 해킹공격 사례입니다.

CASE 1 ‘건설분야 직능단체’ 대상 악성코드 대량 유포

2024년 1월 북한 김수키 해킹조직은 우리나라 건설 분야 직능단체 홈페이지를 통해 악성코드를 유포하였습니다. 악성코드는 홈페이지 로그인 시 사용되는 보안인증 S/W에 은닉되어 있었으며, 이로 인해 홈페이지에 접속한 지자체, 공공기관, 건설기업의 관련 업무 담당자 PC가 감염되었습니다. 분석 결과, 정상 배포 채널을 변조한 ‘공급망 공격3)’과 건설·설계 전문가가 자주 방문하는 홈페이지를 통해 유포하는 ‘워터링홀4)’이 결합된 공격으로 확인되었습니다.

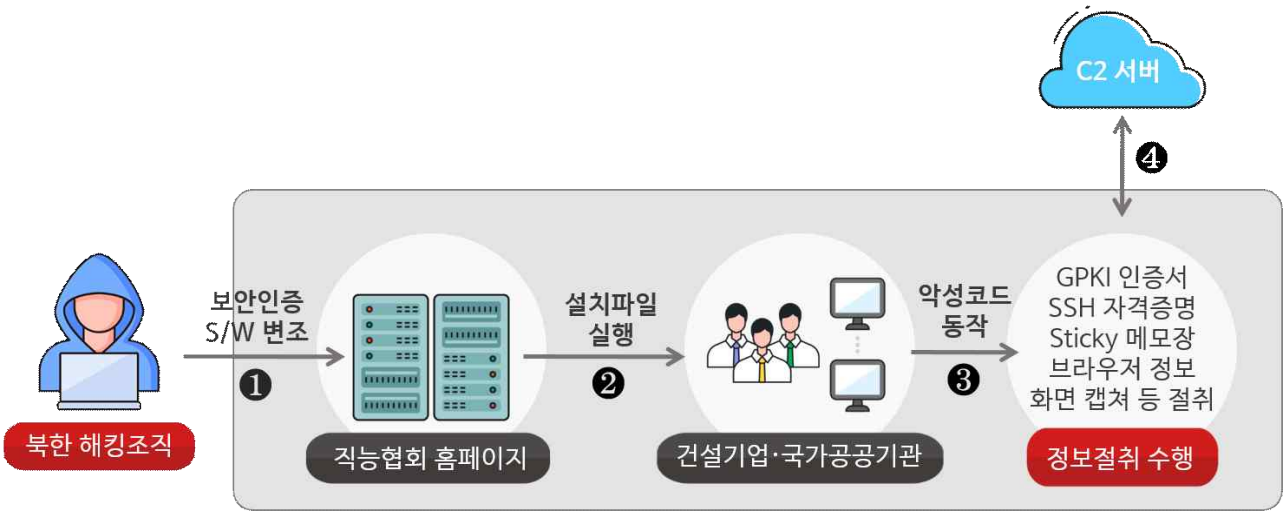

그림1. 북한 김수키 해킹조직의 악성코드 유포 과정

공격 절차

❶ 공격자는 웹사이트 파일 업로드 취약점을 악용하여 직능단체 홈페이지의 보안인증 S/W를 변조한 것으로 추정됩니다. 보안인증 S/W는 홈페이지 로그인을 강화하기 위해 설치하는 필수 프로그램(5개)인데, 해커는 이 중 1개를 변조하여 악성코드를 은닉하였습니다.

3) 공격자가 소프트웨어 개발·유통 등 과정에 침입해 악성코드를 사용자 기기에 감염시키는 공격방식

4) 사용자가 자주 방문하는 웹사이트에 악성코드를 숨겨두고, 사용자가 해당 웹사이트 방문시 악성코드에 감염되는 형태

❷ 사용자는 홈페이지 로그인 단계에서 변조된 보안인증 S/W(NX_PRNMAN) 설치파일을 실행하게 됩니다. 특히, 변조된 보안인증 S/W는 합법적인 인증서[5](D2Innovation社 소유)로 서명되어 있어 일부 웹브라우저·백신의 탐지를 우회할 수 있습니다.

❸ 변조된 보안인증 S/W 설치파일이 실행되면 %APPDATA% 경로에 DLL 형태의 악성코드가 실행되고, 이와 함께 정상적인 프로그램도 실행됩니다. 이 악성코드는 백그라운드 상태에서 정보절취 기능을 수행해 사용자는 악성 행위를 인지하기 어렵습니다. 이 악성코드는 Go 프로그래밍 언어로 작성되었고, 일부 보안업체는 해당 악성코드를 'TrollAgent[6]' 라고 명명한 바 있습니다.

❹ 악성코드는 시스템 정보를 수집하고 사용자 화면을 캡처하는 기능을 보유하고 있으며, 네이버 웨일·구글 크롬·마이크로소프트 엣지 등 브라우저에 저장된 정보(자격증명·쿠키·북마크·히스토리 등)를 수집할 수 있습니다. 감염PC에 보관 중인 GPKI 인증서와 SSH 인증키, Sticky Note, 파일질라 정보를 절취하는 기능도 가지고 있습니다.

Key Finding

김수키 해킹조직은 유효한 디지털 인증서를 사전에 절취하여 변조된 S/W파일(보안인증 S/W)에 서명하고, 정상 보안인증 S/W와 함께 유포하는 등 치밀한 준비 작업을 거쳤습니다. 이 공격은 건설 관련 국가기관·기업들의 접속 빈도가 높은 홈페이지를 유포 경로로 활용하였고, 정보절취 악성코드에 GPKI 인증서 절취 기능이 포함된 것으로 보아 건설분야 공직자 해킹을 교두보 삼아 주요 건설사업 정보와 사업에 참여한 건설기업의 기술자료 절취를 시도한 것으로 추정됩니다.

5) 합법적인 인증서는 개발자가 S/W 배포시 제3자에 의해 코드가 손상되거나 해킹 당하지 않았음을 증명하기 위해 적용한 '코드 서명 인증서'가 유효하다는 뜻. 만약 해커가 사용했다면 인증서의 소유자가 해킹으로 인증서를 탈취당했다는 의미

6) 국내 보안업체 안랩社는 '보안 프로그램 설치 과정에서 감염되는 TrollAgent' 제하 분석보고서 공개(https://asec.ahnlab.com/ko/61666)

MITRE[7] 공격 매트릭스 for Enterprise Windows(v15)

공격 전술(Tactics)	공격 기술(Techniques)	사용 형태(Description)
초기 접근(TA0001)	드라이브바이 감염(T1189)	웹사이트 감염(워터링홀)
	공급망 공격(T1195)	정상적인 배포 파일 변조
실행(TA0002)	사용자 실행:악성파일(T1204.002)	사용자가 설치파일 실행
방어회피(TA0004)	파일 난독화:패킹(T1027.002)	VMProtect 패킹사용
	위장(T1036)	합법적인 인증서 및 보안인증 S/W 설치파일 사용
탐색(TA0007)	파일 및 폴더 탐색(T1083)	GPKI 폴더·파일 탐색
	브라우저 정보 탐색(T1217)	자격증명·쿠키·북마크·히스토리 탐색
수집(TA0009)	로컬저장소 데이터(T1005)	CMD 명령을 통한 시스템 정보수집
	로컬데이터 보관(T1074.001)	유출자료 파일로 저장
	화면캡쳐(T1113)	화면 캡쳐 수집
	자동화 수집(T1119)	SSH Key, %APPDATA% Sticky Note, 파일질라 등 수집
명령 및 제어(TA0011)	어플리케이션 프로토콜:웹프로토콜(T1071.001)	C2와 HTTP 통신
	암호화 채널:비대칭암호화(T1573.002)	RSA 암호화
유출(TA0010)	C2를 통한 유출(T1041)	C2 서버에 파일 전송

CASE 2 ‘정보보안제품 취약점’ 악용하여 국내 기계분야 공격

2024년 4월 북한 안다리엘 해킹조직은 국내 정보보안 S/W(VPN·서버보안)에 대한 취약점을 악용해 업데이트 파일을 악성코드로 교체·실행하는 수법을 사용하였는데, 이를 통해 건설·기계업체 등에 원격제어 악성코드(DoraRAT)를 유포하였습니다.

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

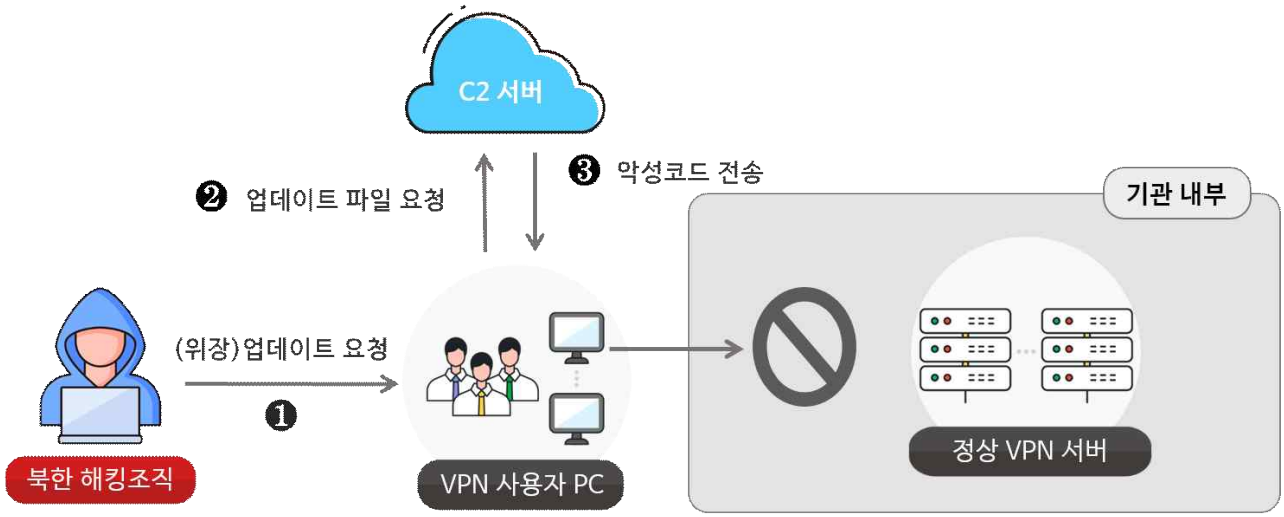

그림2. 북한 안다리엘의 'VPN SW' 취약점 악용, 악성코드 유포 과정

공격 절차

❶ 공격자는 사전에 VPN 정보보안 S/W의 기능 중 클라이언트와 서버간 통신 프로토콜에 존재하는 취약점(업데이트시 인증 절차가 미흡)을 공격에 사용하였습니다. 공격자는 정상 서버에서 발신한 것으로 위장된 통신패킷(HTTP)을 사용자의 PC에 전송합니다. 사용자 PC의 VPN 클라이언트(이하 클라이언트)는 통신패킷 검증 과정 미흡으로 이를 정상 서버가 보내온 통신으로 인식하게 됩니다.

❷ 클라이언트는 정상 VPN 서버가 아닌, 공격자의 C2 서버로 업데이트 파일을 요청하게 되는데, 공격자는 C2 서버에 VPN 서버로 위장한 프로그램을 동작시켜 클라이언트를 기만합니다. 이 과정에서 클라이언트 요청 및 서버 응답의 정상 여부, 업데이트 파일의 무결성 체크 등 다수의 검증 단계가 존재하나 이를 모두 우회한 것으로 확인됩니다.

❸ 최종적으로 C2 서버에서 원격제어 악성코드를 사용자 PC에 전송하게 되고, 클라이언트는 업데이트 파일로 인식하고 실행하게 됩니다. 국내 보안업체에서는 원격제어 악성코드를 DoraRAT[8] 라고 명명하고 있습니다. 이후 C2 서버로부터 명령코드를 수신해 악성 기능을 수행합니다.

8) 국내 보안업체 안랩社는 'DoraRAT을 이용한 국내 기업 대상 APT 공격 사례 분석' 분석 보고서 발표(https://asec.ahnlab.com/ko/65495)

명령코드	서브 명령코드	기능
2	download	C2에서 파일 다운로드
	upload	파일 업로드 준비 작업
	–	명령 실행
3	–	파일 업로드
6	–	파일 업로드 종료

Key Finding

공격에 사용된 원격제어 악성코드(DoraRAT)는 파일 업·다운로드, 명령 실행 등 단순하고 경량화된 형태로 만들어졌습니다. 워터링홀 기법으로 유포하다 보니 노출 가능성이 높아 기존에 고도화된 APT 공격에서 보여진 악성코드(Black RAT[9]))와 달리 최소한의 기능만 포함한 것으로 보입니다.

또한, 국내 보안업체에 따르면 원격제어 악성코드 감염PC에서 대용량·다량의 파일 절취가 가능한 '파일절취형 악성코드'도 확인되었습니다. 정보공동체는 이 악성코드가 파일 용량이 매우 큰 기계·설비 관련 설계도를 C2 서버로 전송하기 위해 설치된 것으로 평가하고 있습니다.

안다리엘은 위에서 언급된 VPN 제품 외에도 서버보안 제품에 대한 취약점도 악용한 것으로 확인되었습니다. 안다리엘이 정보보안제품 등 IT관리 S/W 취약점을 노리는 것은 대량 감염이 가능하고, 제품들이 기본적으로 높은 수준의 시스템 접속·관리 권한을 가지기 때문입니다.

피해 완화(Mitigations)

이 권고문에 소개된 북한의 해킹사례는 개인의 부주의 때문에 발생한 문제가 아닌, 홈페이지와 정보보안 S/W의 취약점으로 인해 발생하였습니다. 앞으로도 북한 해킹조직은 서비스·제품에 대한 취약점을 지속 노릴 것으로 전망되는 만큼, 아래와 같이 조직 구성원과 더불어 조직의 IT·보안 담당자의 피해 완화 노력이 중요합니다.

9) 안다리엘이 사용중인 원격제어형 악성코드로 Go언어로 제작되어 원격명령실행, 파일다운로드, 화면캡쳐 등 다양한 악성행위 수행

- 조직 구성원 대상으로 지속적인 보안교육이 중요합니다. 일반 구성원·IT조직 대상으로 맞춤형 교육이 필요합니다.

- 사용자는 운영체제·응용프로그램에 대한 최신 버전을 유지하고, 백신 업데이트 및 실시간 탐지 설정으로 피해를 예방할 수 있습니다.

- S/W 배포에 대해 엄격한 승인 정책은 피해를 완화할 수 있습니다. 최종 배포 단계에서 관리자의 인증을 거치게 되면 자동 배포단계의 취약점을 예방할 수 있습니다.

- 정부의 사이버보안 권고에 관심을 갖고, 자신의 조직에 해당하는 제품이 있으면 즉시 제조사를 통해 조치를 받아야 합니다. 일부 긴급 사안의 경우 제조사가 고객사에 직접 연락을 하는 경우도 있습니다.

- S/W 공급망 보안대책은 국가정보원·과학기술정보통신부·디지털플랫폼정부위원회가 합동으로 마련한 'S/W 공급망 보안 가이드라인[10]'을 참고하시면 됩니다.

- 개발자는 안전한 소프트웨어를 개발하기 위해 한국인터넷진흥원(KISA)에서 발간한 '소프트웨어 개발보안 가이드[11]'를 참고할 수 있습니다.

- 건설·기계 등 직능단체 홈페이지 운영자는 보안관리에 지원이 필요하다면 한국인터넷진흥원(KISA)에 신청하여 보안점검을 받을 수 있습니다.

해킹사고 신고 안내

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

- 국가정보원(www.nis.go.kr, 111)
- 검찰청(www.spo.go.kr, 1301)
- 경찰청(ecrm.police.go.kr, 112)
- 국군방첩사령부(www.dcc.mil.kr, 1337)

10) https://ncsc.go.kr/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=133991&menuNo=070000&subMenuNo=070300

11) https://kisa.or.kr/skin/doc.html?fn=20220104_2030303_5.pdf&rs=/result/2022-01

관련 침해지표(IoC)

CASE 1 ‘건설분야 직능단체’ 대상 악성코드 대량 유포

구분	침해지표(IoC)	비고
MD5	19C2DECFA7271FA30E48D4750C1D18C1	드로퍼 NX_PRNMAN.exe
	C8E7B0D3B6AFA22E801CACAF16B37355	정보절취 (TrollAgent)
C2	aerosp.p-e.kr	HTTP
	kostin.p-e.kr	HTTP
	netup.p-e.kr	HTTP
	appofficer.kro.kr	HTTP
	limsjo.p-e.kr	HTTP
	coolsystem.co.kr	HTTP
	ol.neqapa.p-e.kr	HTTP
	main.winters.r-e.kr	HTTP
	216.189.159.197	도메인 맵핑 IP주소 (2023.12~2024.2)

CASE 2 ‘정보보안제품 취약점’ 악용하여 국내 기계분야 공격

구분	침해지표(IoC)	비고
MD5	fee610058c417b6c4b3054935b7e2730	원격제어 (DoraRAT)
	094f9a757c6dbd6030bc6dae3f8feab3	
	d92a317ef4d60dc491082a2fe6eb7a70	
	5df3c3e1f423f1cce5bf75f067d1d05c	
	afc5a07d6e438880cea63920277ed270	
C2	kmobile.bestunif.com	TCP
	206.72.205.117	TCP