2026. 7. 30

금융보안원

국가배후 해킹조직의 우리 국민·기업 해킹 공격 주의 권고

□ 요약

대한민국 국가정보원(NIS), 경찰청(KNPA), 한국인터넷진흥원(KISA), 금융보안원(FSI), 민·관 합동분석협의체(안랩·에스투더블유·엔키화이트햇·플레인비트) (이하 "작성기관")는 국가배후 해킹조직의 해킹메일·워터링홀[1] 공격에 대한 위협을 경고하고, 피해 최소화를 위해 공격 방법·피해 유형 및 피해 완화 방안에 관한 합동 사이버보안 권고문을 발표합니다.

국가배후 해킹조직은 이력서·채용 제안 등으로 위장한 피싱 메일을 발송한 뒤 열람토록 유도해 악성코드를 감염시키거나, 우리 국민 다수가 이용하는 인터넷 뉴스·병원 사이트뿐만 아니라 보안관리가 미흡한 소규모 웹 사이트를 해킹해 악성코드 유포 발판으로 이용하는 사례가 지속 확인되고 있습니다.

이 공격 방법은 사용자의 컴퓨터에 오래전 설치된 보안프로그램의 취약점과 결합하여 웹 사이트 접속만으로도 감염될 수 있다는 점에서 매우 위험합니다. 특히, 기업의 경우 피해 발생 시 내부 문서·고객정보·영업자료 등의 자료를 외부로 빼돌리며 이를 인질로 협박·유포 등으로 피해가 확산할 수 있어 각별한 주의가 필요합니다.

1) 정상 사이트를 해킹한 뒤 악성코드를 은닉하고, 접속만으로 방문자를 감염시키는 공격 방법

□ 공격 방법

❶ 사회공학적 기법의 해킹메일(이력서 · 투자 등 메일 위장)

해킹조직은 채용 · 기부 등을 가장해 수신받는 사람이 관심을 가질만한 내용의 해킹메일을 보냅니다. 감염 방식은 두 가지입니다.

1. 첨부된 악성 링크

링크를 통한 해킹메일 역시 오래된 보안프로그램 취약점과 결합해 링크 연결만으로도 감염될 수 있습니다. 채용지원으로 위장한 해킹메일을 발송하고, 이력서를 첨부파일이 아닌 링크 형태로 본문에 함께 전달합니다. 메일에 포함된 링크는 해킹조직이 미리 개설하거나 해킹한 블로그 또는 깃허브 등의 사이트로 연결됩니다.

> 제목: 안녕하세요. OOO입니다.
>
> 안녕하세요.
> 귀사의 채용공고를 보고 회사에 지원하게된 OOO입니다.
> 귀사에 지원하고자 이력서를 송부하오니,
> 긍적적인 검토를 부탁드립니다.
> https://OOOOO.github.io/main/ ← (악성링크)
>
> 감사합니다.

또한, 이미 해킹한 정상 웹 사이트에 악성코드를 심어놓고 그 사이트 주소를 메일 본문에 링크로 넣어 보내기도 합니다. 수신자가 보기에는 정상 사이트이므로 의심 없이 클릭하게 되고, 악성코드에 감염됩니다.

제목: OOO입니다.

안녕하세요.
귀사에 기부를 하고자 연락드린 OOO 상무입니다.
기부 관련 물품은 아래 사이트를 통해 확인 부탁드립니다.
https://OOO.co.kr/site/site.asp ← (해킹된 웹 사이트)

감사합니다.

2. 악성 첨부파일

'고연봉 일자리 제안' 같은 내용의 채용 제안으로 가장하여 첨부파일이나 링크를 열도록 유도합니다. 첨부된 파일에는 악성코드가 함께 포함되어있어 열람하는 즉시 감염됩니다. 이때 실제 헤드헌터의 계정을 도용하기도 합니다.

보낸사람 : 「헤드헌터」 김OO 부장 <recruit@OOOOO.com> ← (해킹된 계정)
제목: OOOOO 인사팀입니다.

안녕하세요.
OOOOO 인사팀입니다.
귀하의 경력을 검토한 결과, 저희 회사에 매우 적합하다고 판단되어 연락드립니다.
보안 정책에 따라 DRM 문서 보호가 설정된 파일과 뷰어파일을 함께 첨부해드립니다.
비밀번호는 OOOO입니다.
편하실 때 천천히 확인하시고 긍정적인 회신을 부탁드립니다.
감사합니다.

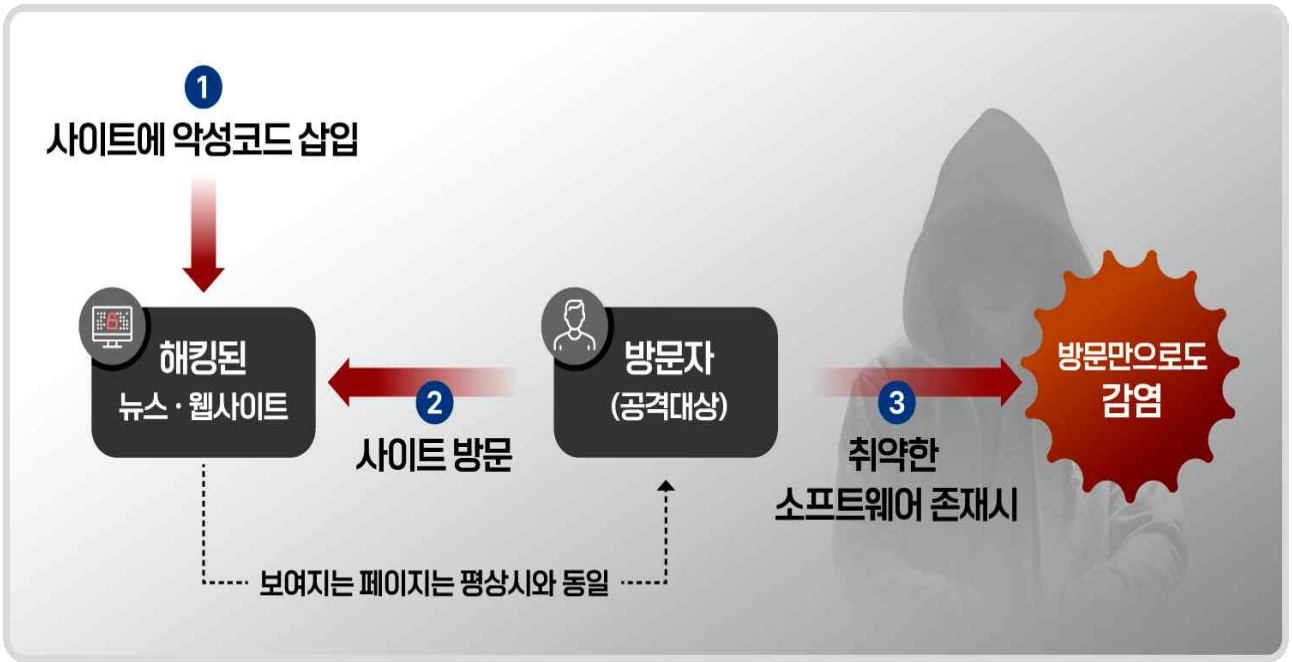
첨부파일 : 채용제안서_ 및_상세조건.zip ← (악성코드)

❷ 워터링홀 공격(웹 사이트 악용 + 보안소프트웨어 취약점)

해킹조직은 평소 사용자가 자주 접속하는 웹 사이트 또는 방문자가 많은 뉴스 사이트 등을 미리 해킹한 뒤 악성코드 유포 매개체로 활용합니다. 사용자가 평소처럼 해당 웹 사이트에 접속만 하더라도 PC에 설치되어 있는 오래된 버전의 보안프로그램을 통해 악성코드가 자동으로 설치됩니다.

최근의 워터링홀 공격 수법은 악성코드를 은닉하거나 웹 사이트의 소스코드를 직접 변조하여 숨기는 등 수법이 더욱 정교해지고있어 보안관제를 통한 탐지가 더욱 어려워지고 있습니다.

또한, 악성코드 유포에 악용된 웹 사이트 화면은 평소와 동일할 뿐만 아니라 '설치하시겠습니까?' 등의 안내도 없어 사용자가 전혀 인지하지 못한 상태에서 악성코드에 감염됩니다. 이때, 전자서명·보안인증·키보드보안 프로그램 등 특정 웹 사이트 이용을 위해 설치한 보안프로그램이 최신 버전이 아니라면 감염 위험이 더욱 높습니다.



□ 피해 유형

악성코드에 감염되면 조직 또는 개인에게 다음과 같은 피해가 발생할 수 있습니다. 아래 과정은 사용자가 인지하지 못하는 사이에 이루어집니다.

❶ 계정정보·비밀번호 탈취

크롬·엣지 등 웹브라우저에 자동 저장해 둔 계정·비밀번호 정보 및 직접 입력하는 아이디·비밀번호·카드번호 등의 정보가 그대로 유출됩니다.

❷ 개인정보·파일 유출

사용자 PC에 있는 문서·사진·연락처 및 연결된 공용 폴더·내부 클라우드 저장자료와 화면캡처 등을 통해 메신저 대화 내용·현재 활동을 감시하거나 자료들을 유출할 수 있습니다.

❸ 추가 확산

감염 PC를 교두보로 같은 사무실·집에서 인터넷 공유기·공유 폴더 등 네트워크에 연결된 다른 PC로 악성코드를 확산하여 주변 PC 연쇄 감염으로 번질 수 있습니다.

❹ 금전요구·협박

소스 코드, 내부 문서, 고객·인사 정보, 영업비밀, 계정정보 등 중요 자산과 자료를 탈취하고, '돈을 주지 않으면 자료를 공개·유포하겠다'며 협박합니다.

□ 결론

이 공격은 그간 우리가 신뢰하던 인터넷 뉴스·웹 사이트를 접속하는 것만으로도 악성코드에 감염될 수 있다는 점에서 특히 주의가 필요합니다. 대응 및 조치를 위해 다음의 피해 완화 방법을 지키고 이상징후 발견 시 즉시 신고하는 것이 중요합니다.

□ 피해 완화

개인 사용자를 위한 조치

- PC에 설치된 전자서명·보안인증 등의 보안소프트웨어를 포함한 모든 소프트웨어에 대해 최신 버전으로 업데이트하고, 사용하지 않는 오래된 소프트웨어는 삭제
- 운영체제·인터넷브라우저(엣지·크롬·웨일 등) 등 주기적 최신 업데이트 실시
- 중요 계정은 2단계 인증(OTP·인증앱)을 활성화하고, 웹 브라우저에 계정정보(비밀번호) 저장 자제
- 백신을 설치하고 항상 최신 상태로 유지하며 실시간 감시 활성화
- 모르는 메일의 첨부파일·링크는 열지 않고, 업무상 메일도 공식 홈페이지 또는 연락처(전화번호)로 직접 연락해 한 번 더 확인

조직 내 보안 담당자를 위한 조치

- 전자서명·보안인증 등 보안소프트웨어를 포함해 조직 내 활용 중인 소프트웨어를 일괄 점검·시스템을 최신화하고 미사용 소프트웨어는 제거
- 자산·패치 관리·네트워크 분리·접근 통제 등 보안 방안과 자산을 체계화하고 침해지표 기반 공격 탐지 등 모니터링 강화
- 중요 서버·업무 PC는 물리적·논리적 망분리 또는 인터넷 직접 접속을 차단
- 업무용PC·사내 시스템의 기본·단순 비밀번호 사용은 지양하고, 시스템별 비밀번호 차등 사용 및 다중 인증(MFA) 등 추가 보안대책 수립
- 주기적 직원 보안 교육(워터링홀·헤드헌팅 위장 피싱 메일 등 사례 공유) 시행 및 모의훈련 실시
- 침해사고 인지 즉시 관할기관에 신고하고, 필요시 수사기관에 수사 의뢰

호스팅 사업자 및 홈페이지 운영자

- 불필요 포트·서비스 차단·관리자페이지 접근 통제·최신 보안패치 적용 등 웹서버 및 관리시스템 보안 강화
- 주기적 불필요 파일·계정점검 및 제거(웹셸, 미사용 관리자 계정, 임시파일 등)
- 홈페이지 위·변조 여부 및 악성 스크립트 삽입 여부 상시 모니터링
- 웹 방화벽 운영 및 접근 로그를 보관하고 및 정기 점검시행

소프트웨어 개발사

- 보안 패치 개발·배포 체계 확립 및 취약점 신고 대응 프로세스 마련
- 개발단계별 정기 취약점 점검 실시(설계·구현·배포 전 보안점검)
- 개발 환경 및 소스 코드에 관한 보안관리(접근 통제·소스코드 유출 방지·빌드환경 무결성 등)
- 오픈소스 활용시 알려진 취약점 사전점검 및 공급망 보안관리(SBOM, 신뢰할 수 있는 저장소 사용)

□ 연락

국가 배후 해킹사고 의심 및 유사사례 발견 시 아래 관련 기관에 문의하시기 바랍니다. 또한, 이 합동 사이버보안 권고문과 관련된 기술적 정보를 포함하여 모든 비정상적인 활동이나 행위를 신고하시기 바랍니다.

국가정보원(www.nis.go.kr, 111)

경찰청 안보수사국(www.police.go.kr, ncsi113@police.go.kr)

한국인터넷진흥원 인터넷침해대응센터(www.boho.or.kr, 118)

금융보안원 침해대응부(www.fsec.or.kr, 02-3495-9494)

국가정보원 국가사이버안보센터(NCSC)에서는 사이버위협에 대한 유가치한 신고 내용에 대해서 신고 포상금을 지급하고 있습니다. 자세한 내용은 관련 웹사이트[2]를 참고하시기 바랍니다.

□ 참조

합동 사이버보안 권고문은 아래 국가정보원 민·관 합동분석협의체에 참여중인 보안전문기업과 함께 작성되었습니다. 이 권고문에서 언급된 국가배후 해킹조직의 전술 및 기법은 아래 기술보고서를 참조하십시오.

- 안랩(ASEC): https://asec.ahnlab.com/ko/94695/
- 엔키화이트햇(ENKI): https://www.enki.co.kr/media-center/blog/joint-cybersecurity-advisory-watering-hole-malware-analysis
- 에스투더블유(S2W): https://s2w.medium.com/detailed-analysis-of-signbt-malware-cluster-504fc3ab4ecf
- 플레인비트(Plainbit): https://plainbit.co.kr/kr/insight/tech_hub?bgu=view&idx=72

2) https://ncsc.go.kr/ko/main/PageLink.html?token=MDEyMzQ1Njc4OWFiY2RlZrBvBnCd4cC_Aqu-HrYk1bh05fRnAJ2iMVcEdzCp8kuY2yJI3KrtCG2HaHTmLhGNHw