경찰청 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2023. 4. 19.(수) 조간 누리망·방송 2023. 4. 18.(화) 12:00

보안인증프로그램 취약점 악용 해킹 사건, 북(北) '라자루스' 소행으로 확인

- 대규모 피해가 우려되는 북(北)의 사이버공격 시도 선제적 확인·차단
- 보안프로그램 취약점 및 언론사 사이트 해킹을 통한 '워터링홀' 공격 기법 확인
- 추가 피해 예방을 위해 금융보안인증 프로그램 업데이트 중요

경찰청 국가수사본부(안보수사국)에서는 지난해 11월부터 금융보안인증 소프트웨어 취약점 악용 공격 사건을 수사한 결과, 이번 사건이 북한 정찰총국이 배후인 것으로 알려진 일명 '라자루스*' 해킹조직의 소행인 것으로 확인하였다.

* '라자루스': '14년 미국 소니픽처스 해킹 사건, '16년 방글라데시 중앙은행 해킹사건, '17년 워너크라이 랜섬웨어 사건 등에 연루된 것으로 알려진 북(北) 해킹조직으로, 정부는 사이버 분야 대북 독자 제재 대상으로 '라자루스' 해킹조직을 지정('23. 2. 10.)

이번 사건은 북한이 인터넷뱅킹 등 전자금융서비스 이용에 필수적으로 설치되는 소프트웨어의 취약점을 악용하고, 국민 대다수가 접속하는 언론사 사이트를 악성코드 유포 매개체로 활용하여 피해가 대규모로 확산될 위험성이 있었던 해킹 사건으로 밝혀졌다.

이와 관련하여, 지난 3월 30일 정부 관계기관은 국민들에게 관련 보안 취약점을 공개하고 신속한 금융보안인증 프로그램 업데이트를 당부하는 한편, 발견된 악성코드를 백신 프로그램에 반영하고 피해업체에 대한 보안조치를 완료하는 등 추가적인 피해를 방지한 바 있다.

수사 결과, 북한은 지난 2021년 4월 국내 유명 금융보안인증 업체를 해킹하여 소프트웨어의 취약점을 찾아내고, 공격에 활용할 웹 서버와 명령·제어 경유지 등 공격 인프라를 장기간 치밀하게 준비한 것으로 확인되었다.

경찰청은 취약 버전의 금융보안인증 소프트웨어가 설치된 컴퓨터가 특정 언론사 사이트에 접속할 경우 자동으로 악성코드가 설치되는 워터링홀* 수법을 통해 국내 61개 기관이 해킹된 것으로 확인하였다. 국내 1,000만 대 이상의 컴퓨터에 설치된 금융보안인증 프로그램의 취약점을 활용해 대규모 사이버 공격을 준비했을 가능성도 배제할 수 없지만, 관계기관 합동대응을 통해 이를 사전에 확인·차단한 사례라고 밝혔다.

* Watering hole: 방문 가능성이 높거나 많이 사용하는 사이트를 감염시킨 후 피해자가 해당 사이트에 접속시 컴퓨터에 악성코드를 추가로 설치하는 공격 방식

경찰청은 국정원·한국인터넷진흥원 등 관계기관 합동분석 결과, ▵공격 인프라 구축 방법 ▵'워터링홀' 및 소프트웨어 취약점을 악용한 공격 방식 ▵악성코드 유사성 등을 토대로, 이번 사건을 북한 해킹조직 일명 '라자루스'의 소행으로 판단하였다.

경찰청은 북한의 해킹 수법이 날로 고도화되고 있는 만큼, 추가적인 피해 예방을 위해 보안인증 프로그램을 최신 버전으로 업데이트해 줄 것을 다시 한번 강조하였다.

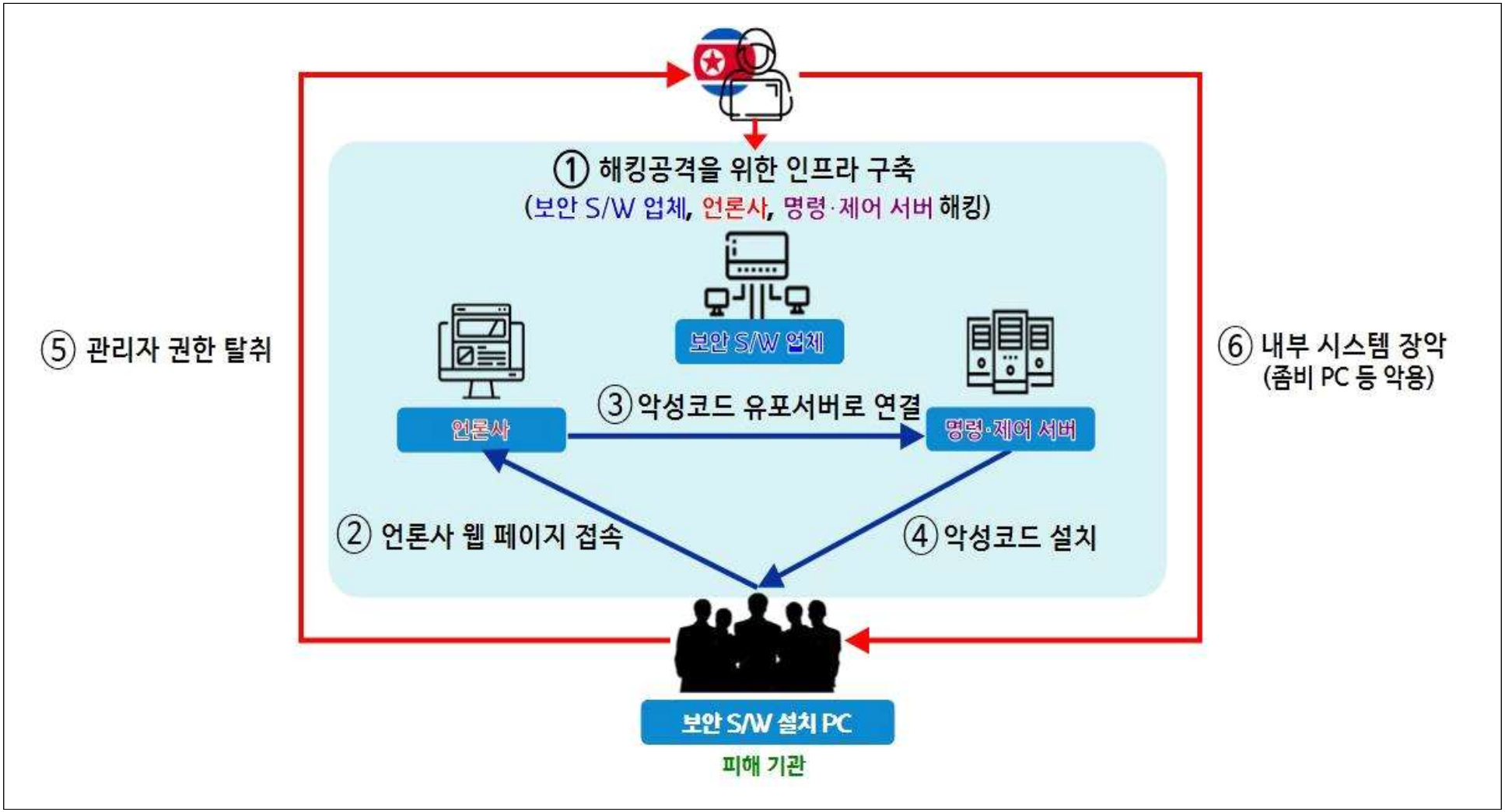
※ 4. 14. 현재, 취약점 악용된 금융보안인증 프로그램 업데이트 약 80% 수준

경찰청은 이번 사건에서 확인된 해외 공격·피해지에 대한 국제 공조수사를 진행하는 한편, 추가 피해 사례 및 유사 해킹 시도 가능성에 대한 수사를 계속 이어 나갈 계획이라고 밝혔다.

붙임 1. 사건 개요도
2. 금융보안인증 소프트웨어 취약 버전 확인 및 업데이트 방법

담당 부서	안보수사국 안보수사지휘과	책임자	과 장	김근만 (02-3150-2092)
		담당자	계 장	박현준 (02-3150-2492)

붙임1 | **사건 개요도**


① 해킹공격을 위한 인프라 구축
(보안 S/W 업체, 언론사, 명령·제어 서버 해킹)
보안 S/W 업체
언론사
③ 악성코드 유포서버로 연결
명령·제어 서버
② 언론사 웹 페이지 접속
④ 악성코드 설치
⑤ 관리자 권한 탈취
⑥ 내부 시스템 장악
(좀비 PC 등 악용)
보안 S/W 설치 PC
피해 기관

붙임2	금융보안인증 S/W 취약 버전 확인 및 업데이트 방법

□ S/W 취약 · 해결 버전 구분

○ (취약 버전) 'INISAFE CrossWeb EX V3 3.3.2.40' 이하

○ (해결 버전) 'INISAFE CrossWeb EX V3 3.3.2.41'

□ S/W 버전 확인 및 업데이트 방법

① **(버전 확인)** 사용 중인 PC에서 검색 기능을 통해 [제어판] 검색 후 클릭 → [프로그램] → [프로그램 및 기능]을 순서대로 클릭, 'INISAFE CrossWeb EX V3' 버전 확인

② **(취약 버전 삭제)** 'INISAFE CrossWeb EX V3 3.3.2.40' 이하의 취약한 버전으로 확인될 경우 [제거] 클릭하여 삭제

③ **(해결 버전 설치)** 이용 중인 금융사이트 등에 접속하거나 개발사 홈페이지에 직접 접속하여 취약점이 해결된 버전(3.3.2.41) 재설치

※ http://demo.initech.com/initech/crosswebex_pack/3.3.2.41/INIS_EX_SHA2_3.3.2.41.exe

– 서비스 운영자의 경우, 개발사를 통해 해결 버전으로 교체