Bundesamt für Verfassungsschutz

2023. 3. 20

킴수키[1] 해킹조직의 구글 브라우저 및 앱 스토어 서비스 악용 공격 주의

요약(Summary)

- 대한민국 국가정보원(NIS)과 독일 헌법보호청(BfV)은 킴수키(탈륨,벨벳 천리마 등으로도 불림) 해킹조직이 한반도·대북 전문가를 공격하기 위해 구글에서 제공하는 브라우저 및 앱 스토어 서비스를 악용한 사례를 확인한바, 이에 대한 경각심을 고취하기 위해 합동 보안권고문을 발표합니다.

- 이 보안권고문은 킴수키 해킹조직이 크로미움 브라우저의 확장프로그램과 안드로이드 앱 개발자 지원 기능을 악용하는 해킹공격에 대한 전략·수법·절차(TTP)와 침해지표(IoC)를 포함하고 있습니다.

- 국가정보원과 헌법보호청은 앞서 기술한 해킹 공격이 한반도·대북 전문가를 주요 타깃으로 하고 있다고 판단하고 있으나, 이에 악용된 기술이 범용적으로 사용 가능하기 때문에 전 세계 외교·안보 싱크탱크 관계자는 물론 불특정 다수로 공격 대상이 확대될 수 있다고 평가하고 있습니다.

기술적 사항(Technical Details)

- 킴수키 해킹조직은 이미 널리 알려진 것과 같이 포털 관리자 및 지인을 사칭한 스피어 피싱을 통해 한반도·대북 전문가를 대상으로 계정정보 절취 공격을 수행하고 있습니다.

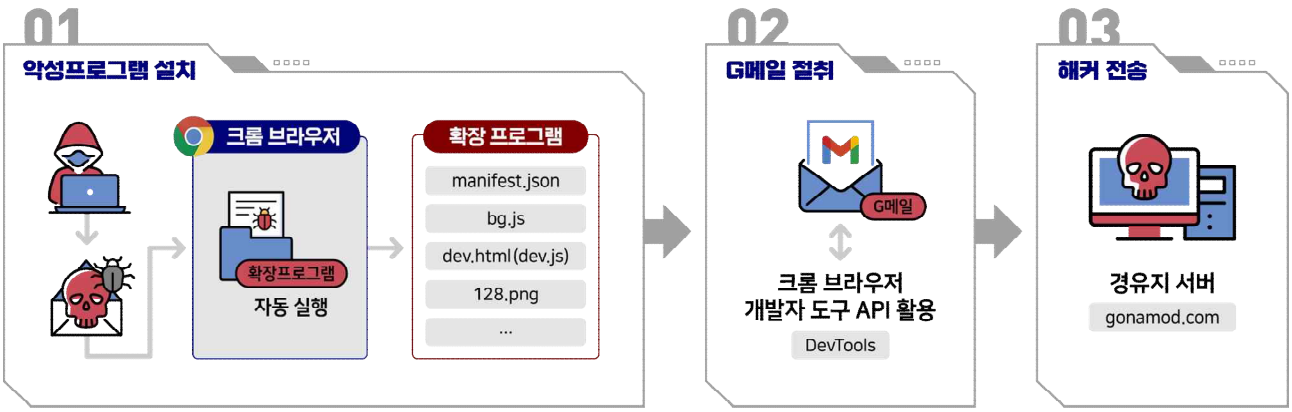
1) IT 보안업체에 따르면 킴수키(KIMSUKY)는 북한 정찰총국과 연계되어 있다고 알려져 있음

- 이 해킹조직은 절취한 계정을 이용해 공격 대상자의 포털사이트와 연동된 이메일뿐만 아니라, 클라우드 서비스에 저장된 자료를 절취하기도 하였습니다.

- 한편, 이번에 새롭게 확인된 킴수키 해킹조직의 2가지 공격 수법은 구글 웹 브라우저 확장프로그램과 웹-스마트폰 연동 서비스를 악용한 것입니다. 아래는 해킹조직이 악용한 수법을 간략히 설명한 것입니다.

① 크로미움[2] 브라우저 확장프로그램(Extension)을 악용한 구글메일 절취

- 스피어피싱 이메일을 통해 악성 크로미움 확장프로그램 설치를 유도한 후, 피해자가 G메일 로그인시 자동으로 확장프로그램이 동작하여 이메일을 절취 합니다.



* 크롬 브라우저 대상 G메일 절취 예시

01. 공격자는 악성 링크가 포함된 스피어피싱 이메일을 발송, 악성코드가 포함된 확장프로그램 설치를 유도합니다.

02. 공격 대상자가 크로미움 기반 웹브라우저를 통해 자신의 G메일에 접속할 경우, 이미 설치된 악성 확장프로그램이 동작하게 됩니다. 이때 개발자 도구(Devtools API) 기능을 활용하여 공격 대상자의 G메일을 자동으로 절취 합니다.

2) 크로미움은 구글이 개발한 오픈소스 웹 브라우저이며, 크롬・엣지 등 다양한 브라우저들이 크로미움 기반으로 제작

03. 절취한 이메일 내용은 공격자의 경유지 서버로 자동으로 전송됩니다.

- 이러한 공격수법은 메일 서비스에서 제공하는 2차 인증 등 개인이 설정한 보안설정을 우회하면서 공격 대상자의 이메일을 은밀하게 절취하기 위한 것으로 평가하고 있습니다.

- 악성 확장프로그램이 설치되면 피해자 PC에 %APPDATA%AF 폴더가 생성되고, 웹 브라우저 주소창에 (chrome|edge|whale)://extensions 입력시 확장프로그램 목록에 'AF'가 표시됩니다.

② 구글 플레이 동기화 기능을 악용한 스마트폰 악성앱 설치

- 공격자는 피싱메일 등으로 사전에 절취한 피해자 구글 계정으로 로그인 후 구글 플레이의 웹-스마트폰 동기화 기능을 악용하여 공격 대상자가 별도 조작 없이도 안드로이드 스마트폰에 악성 앱을 설치합니다.

01. 공격자는 사전에 피싱메일 등을 통해 대상자의 구글 계정정보를 절취 합니다.

02. 공격자는 악성앱을 구글 플레이 콘솔(앱 개발자 사이트)에 '내부 테스트용'으로 등록하고 공격 대상자 계정을 테스트 대상으로 추가합니다.

03. 공격자는 PC에서 피해자 구글 계정으로 로그인 후 구글 플레이스토어에 접속하여 악성앱 설치를 요청합니다. 이때 악성앱을 설치할 디바이스로 구글 계정과 연동된 공격 대상자의 스마트폰을 선택합니다.

04. 악성앱은 구글에서 제공하는 '구글 플레이 동기화 기능'을 통해 공격 대상자의 스마트폰에 자동으로 설치됩니다.

- 공격자가 악성앱을 '내부 테스트용'으로 등록하고 제한적으로 배포하는 것은 탐지를 최소화하고 특정 타깃을 대상으로 공격하기 위한 것으로 평가하고 있습니다.

- 스마트폰에 설치된 앱 목록을 점검(침해지표 참고)하여 악성앱 설치여부를 확인할 수 있습니다.

피해 예방(General mitigations and best practices)

- 국가정보원과 헌법보호청은 자주 발생하는 스피어 피싱 공격을 토대로 이번 보안 권고문에 예방 가이드를 수록하오니 참고해주시기 바랍니다.
- 상기와 같은 해킹사고 의심 및 유사사례 발견 시 아래 기관에 연락하여 주십시오.

  – 대한민국 기관 :

    · 국가정보원(www.nis.go.kr, 111)

    · 한국인터넷진흥원(boho.or.kr, 118)

    · 경찰청(ecrm.police.go.kr, 182)

  – 독일 기관 :

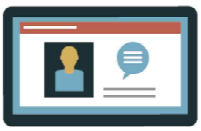
    · 헌법보호청(www.verfassungsschutz.de, +49(0)228-99/792-6000)

- 계정 절취에 대한 위협을 줄이기 위해 2단계 인증을 사용하십시오.
- 이번 해킹조직의 공격은 대부분 스피어피싱을 통해 이루어지기 때문에 악성 이메일을 판별하고 이메일 수신시 유의사항 준수를 통해 피해를 예방할 수 있습니다.

- 스피어피싱 이메일 판별법

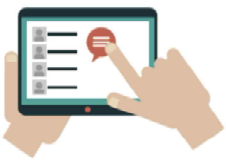
1) 메일 주소가 이상하지 않은지 먼저 확인해보세요!

예시	1) @naver.com → naver-com.cc 2) @google.com → @goog1e.com 3) @daum.net → @dauum.net 4) @web.de → @webb.de 5) @gmx.net → @gnx.net



2) 모르는 사람에게 온 메일 궁금해 하지 마세요!

예시	1) OO 이벤트 당첨 2) 항공권 파격 특가! 3) 당신의 의견이 매우 흥미롭습니다.



3) 사전에 안내되지 않은 메일 열람하지 마세요!

예시	1) 경찰 출석 요구서 2) 국내 및 국외 정세 자료 3) 정책 자료 4) 각종 업무 메일 등

4) 믿을 수 없는 첨부 파일 절대 열람하지 마세요!

예시	1) “연구 결과 보고서” 2) “이력서” 3) “Invoice No. 28629” 4) “연말정산 자료” 5) “연봉 계약서” 등

5) 클릭 할까? 말까? 함부로 클릭 금지!

예시	1) “본문내용 상세 보기” 2) “패스워드 변경하기” 3) “메일함 용량 초과” 등 내용

- 이메일 수신 시 유의사항

1) 백신 설치 및 최신 업데이트

- 바이러스 백신 소프트웨어 설치 및 최신유지
- 운영체제(OS) 및 업데이트 포함

2) 로그인 보안 강화

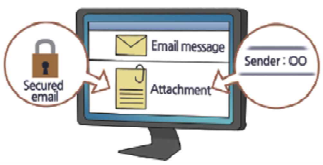
- 이메일 비밀번호 수시 변경
- 문자(SMS), 모바일OTP 등 2단계 인증 로그인 설정

3) 의심메일 열람금지

- 예정되지 않은 업무 메일, 스팸 메일 등 열람금지
- 의심 메일 수신시 발신자에게 유선으로 확인

4) 패스워드 입력금지

- 이메일에 링크된 홈페이지를 통한 비밀번호 입력금지
- 패스워드 변경은 해당 홈페이지에 직접 방문



5) 첨부파일 실행주의

- 보안 메일 또는 사전 인지시에만 실행
- 그외의 경우에는 발송자에 확인 후 실행

6) 로그인 이력 수시점검

- '로그인 이력' 조회를 통해 비정상 로그인 수시 확인
- '해외 로그인 차단' 기능 적극 활용

관련 침해지표(IoC)

크로미움 브라우저 악성 확장프로그램

구분	침해지표	비고
경유지	gonamod[.]com	HTTPS
	siekis[.]com	HTTPS
	mode=cd2&ver=3.0	HTTP param
악성코드	012D5FFE697E33D81B9E7447F4AA338B	manifest.json
	582A033DA897C967FAADE386AC30F604	bg.js
	51527624E7921A8157F820EB0CA78E29	dev.js
	%APPDATA%\AF	Download folder
문자열	AF	브라우저 확장프로그램 이름

구글 플레이 '동기화 기능'을 악용

구분	침해지표	비고
경유지	navernnail[.]com	HTTP
	lowerp.onlinewebshop[.]net	HTTP
	mc.pzs[.]kr	HTTP
	23.106.122[.]16	HTTP
악성앱	3458DAA0DFFDC3FBB5C931F25D7A1EC0	FastViewer (com.tf.thinkdroid.secviewer)
	89F97E1D68E274B03BC40F6E06E2BA9A	Fastspy DEX 파일
	04BB7E1A0B4F830ED7D1377A394BC717	Fastfire (com.viewer.fastsecure)