



북한 김수키 조직의 싱크탱크・학계・미디어 대상 사회공학적 기법을 악용한 해킹공격

요약(SUMMARY)

대한민국 국가정보원(NIS)・경찰청(NPA)・외교부(MOFA)와 미합중국 연방수사국(FBI)・국무부(DoS)・국가안보국(NSA)은 공동으로 북한 정권과 연계된 사이버 행위자들이 전세계의 연구소・싱크탱크・학술기관・언론사 관계자들을 대상으로 사회공학적 기법을 악용한 컴퓨터 네트워크 탈취(CNE) 공격에 대한 경각심을 높이기 위해 합동 주의보를 발표합니다. 이러한 북한 사이버 행위자들은 주로 실존하는 기자, 학자 또는 대북정책 그룹과 신뢰할만한 연관성을 가진 개인들을 사칭하여 스피어피싱 공격을 수행하는 것으로 알려져 있습니다. 북한은 공격 대상의 사적인 문서, 연구 결과 및 통신 내용에 불법적으로 접근하여 지정학적 사안들, 외교정책 및 전략, 그리고 북한 정권의 이익에 영향을 주는 외교적 사안들에 대한 정보를 수집하기 위해 사회공학적 기법을 사용합니다.

배경(BACKGROUND)

북한의 사이버 프로그램은 북한 정권에 폭넓은 정보와 첩보활동 역량을 제공합니다. 한미 양국 정부는 이러한 북한 사이버 행위자들의 지속적인 정보 수집 시도를 목격해왔습니다. 특히, 북한의 주요 군사 정보기관이자, 유엔 안보리 결의 제재 대상인 <정찰총국>은 북한 사이버 행위자들의 네트워크와 활동을 주도하고 있습니다.

한미 정부는 북한 정권의 사이버 프로그램이 한・미 양국 및 여타 이해당사국들과 관련된 최신 정보에 대해 지속적으로 접근함으로써 정권의 생존과 안정에 위협이 되는 모든 정치적, 군사적, 경제적 위협을 저지하는 것을 주요 목표로 삼고 있는 것으로 평가합니다.

현재 한미 양국 정부와 민간 사이버 보안 업체들은 사회공학적 기법을 사용하여 대규모 공격을 감행하는 특정 북한 사이버 행위자들을 <김수키(Kimsuky)>, <탈륨(Thallium)>, <APT43>, <벨벳천리마(VelvetChollima)>, <블랙 밴시(Black Banshee)> 등으로 명명하여 추적하고 있습니다. 김수키는 정찰총국 산하 조직이며, 최소 2012 년부터 정찰총국의 목표 달성을 돕기 위해 광범위한 사이버 작전을 펼쳐왔습니다. 김수키 해커들의 주된 임무는 탈취한 정보와 중요한 지정학적 통찰력을 북한 정권에 제공하는 것입니다.

이들의 표적이 된 몇몇 기관들은 사회공학 캠페인이 야기하는 위협의 수준을 평가절하 할지도 모릅니다. 이는 그들이 자신들의 연구 및 통신 내용이 본질적으로 민감하지 않다고 생각하거나, 이러한 공격 시도들이 어떻게 북한 정권의 보다 폭넓은 사이버 첩보활동을 가능케 하는지 모르기 때문입니다. 그러나 동 주의보에 언급된 바와 같이 북한은 정책 분석가들을 공격함으로써 획득한 정보에 크게 의존하고 있습니다. 나아가, 성공적이었던 공격들은 김수키 해커들이 더 민감하고 가치 있는 공격 대상들에 대해 사용할 수 있는 보다 신뢰성 있고 효과적인 스피어피싱 이메일을 작성하는 데 기여합니다. 동 주의보를 집필한 기관들은 북한 사이버 공격에 대한 경각심 제고 및 기본적인 사이버 보안 조치 실시를 통해 김수키가 실시하는 스피어피싱 작전의 효과를 저하시킬 수 있을 것으로 생각합니다. 동 주의보는 김수키의 활동 방식, 공통된 주제와 작전 수행 과정으로부터 도출할 수 있는 위험 신호들, 김수키의 컴퓨터 네트워크 탈취(CNE) 작전으로부터 스스로를 더 잘 보호하기 위해 전세계 기관들이 시행할 수 있는 일반적인 조치들에 대해 구체적인 정보를 제공할 것입니다.

만약 이러한 스피어피싱 작전들의 공격 대상이 되었다고 생각된다면, 실제 침해가 발생했는지 여부와 관계없이 (특히 귀하께서 주요 표적 분야들의 일원이라면) www.ic3.gov 에 접속 후 사건 설명란에 #KimsukyCSA 라고 표기하여 신고해주시기 바랍니다.

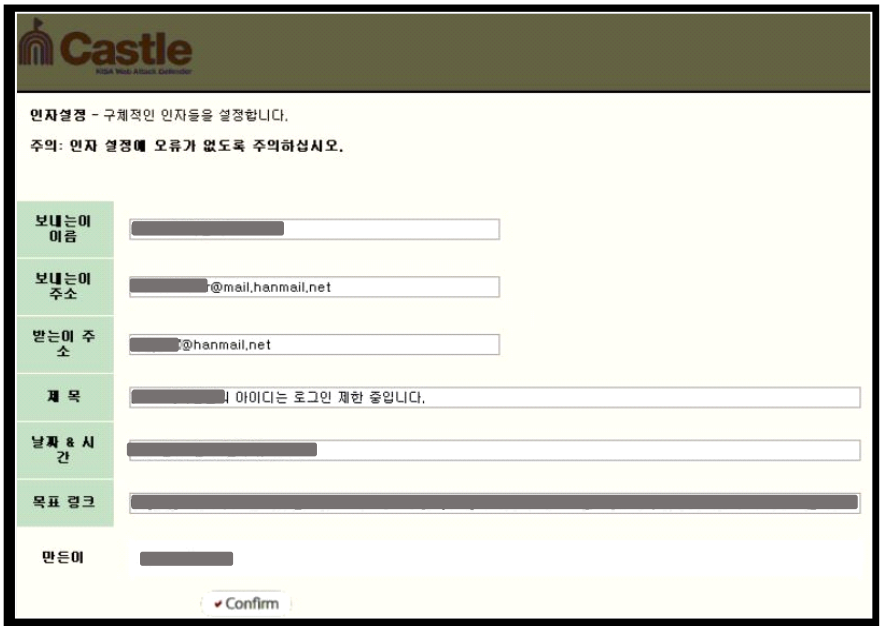
신고시, 발신자 이메일 주소, 이메일 본문 내용, 구체적인 링크 · URLs · 도메인 주소 등을 포함하여 사건에 관련된 정보들을 최대한 구체적으로 제공하여주시기 바랍니다. 또한, 귀하께서 이메일에 답장하셨는지, 링크를 클릭하셨는지 또는 첨부파일을 열어 보았는지도 기술하여 주시기 바랍니다. 수사관으로부터 추가적인 정보를 요청하는 연락을 받으실 경우를 대비하여 이메일 원문과 첨부파일들을 보관하여주시기 바랍니다.

- www.ic3.gov 에 접속하시고, 신고시 #KimsukyCSA 표기 바랍니다.
- 미국 정부는 피해자들이 북한 소행으로 의심되는 사이버 활동을 포함하여 모든 의심스러운 활동들을 FBI 지역 현장 사무소에 신고하도록 권장합니다.
- 한국 정부에 신고하기를 원할 경우, 국정원(www.nis.go.kr, 111), 경찰청(ecrm.police.go.kr, 182) 또는 한국인터넷진흥원(boho.or.kr, 118)에 신고할 수 있습니다.

김수키 공격수법 : 사회공학적 기법 악용

사이버 안보의 맥락에서, 사회공학이란 기만을 통해 인간의 실수를 파고들어 공격 대상이 자신도 모르는 사이에 기밀이나 민감한 정보를 누설하도록 악의적인 목적 하에 조종하는 것이라는 넓은 의미를 가지고 있습니다. 북한 사이버 행위자들은 악의적 컴퓨터 네트워크 탈취(CNE)를 수행하기 위해 많은 경우 사회공학 기법을 사용합니다. 여러 사회공학 기법들 중 김수키는 스피어피싱을 공격 개시 및 공격 대상의 기기와 네트워크에 대한 접근 확보를 위한 주요 수단들 중 하나로 사용합니다. 10 년이 넘는 기간 동안 김수키는 사회공학 기법들을 계속해서 발전시키면서 자신들이 자행하는 스피어피싱 공격을 식별하기 더욱 어렵도록 만들었습니다.

김수키 조직의 스피어피싱 공격은 방대한 사전조사 및 준비를 거쳐 시작됩니다. 북한 사이버 행위자들은 가치있는 대상을 식별하기 위해 종종 오픈소스 정보를 활용하고, 피해자에게 더욱 현실적이고 매력적으로 보일 만한 온라인 페르소나를 맞춤 제작합니다. 김수키는 그들이 사칭하고자 하는 대상의 실제 이메일 주소와



킴수키에 의해 사용된 이메일 발송 프로그램 예시

유사한 이메일 주소를 생성하고, 스피어피싱 메시지와 같은 악의적 컨텐츠를 담은 도메인을 생성합니다. 북한 행위자들은 공격 대상을 속이기 위해 일반적인 인터넷 서비스 및 미디어 사이트와 유사한 도메인을 활용합니다.

- 예를 들어, 김수키는 잘 알려진 언론사나 기자들을 사칭하는 것으로 알려져 있는데, 실제로 "@XYZnews.com"이라는 이메일 주소를 사용하는 언론사를 사칭하여, "@XYZkoreas.news" 라는 유사 도메인을 사용할 수 있습니다.
- 일반적으로 북한 사이버 행위자들은 공격 대상과 온라인으로 소통하면서 신뢰관계를 형성하고자 하며, 이를 위해 실존 인물들의 신분을 도용합니다. 김수키가 사칭 대상의 이메일 계정을 이미 탈취했을 가능성도 있습니다. 이러한 침해 행위는 해커들이 업무자료 및 신상자료(퇴직자·동호회·주소록)에 중점을 두고 탈취한 계정의 메일 내용을 열람하며 공격 대상을 물색할 수 있도록 합니다. 이들은 피해자의 이메일 서명, 주소록, 과거 이메일 수발신 기록 등을 재가공하여 더욱 설득력 있는 스피어피싱 메일을 제작합니다. 북한 사이버 행위자들은 외교정책 전문가 소유 이메일 계정을 탈취하여 부계정을 만들고, 이들의 이메일 계정과 신분을 도용하여 다른 주요 표적들과 소통하기도 하는 것으로 알려져 있습니다.
- 김수키는 공격 대상에 접근하기 위해 다수의 위조 신분을 사용하기도 합니다. 공격 대상에 최초 접근시 하나의 신분을 사용하고, 또 다른 신분으로는 최초 접근에 대한 후속 연락을 취하며 잠재적 피해자가 자신이 교류하고 있는 사람의 진짜 신분이 무엇인지 파악하는 것을 방해하는 것입니다. 또 다른 전술은 공격 대상이 신뢰하는 발신자로부터 발송된 이메일을 "재발송"하거나 "전달"하는 것입니다.
- 때때로 최초의 피싱 메일에는 보고서나 기사로 위장한 악성 링크나 문서가 포함되어 있기도 합니다. 많은 경우 첨부된 악성 문서에 비밀번호를 설정하여 백신이나 보안장비에서 탐지할 수 없도록 합니다. 그러나, 최초의 스피어피싱 메일에는 악성 링크나 첨부물을 포함시키지 않음으로써 공격 대상자와의 신뢰 형성을 시도하는 경우가 더 많습니다.
- 북한 사이버 행위자들은 일단 공격 대상과의 접촉이 이루어지면, 악성 매크로가 심어진 악성 컨텐츠를 공격 대상 소유의 계정, 기기, 네트워크에 주입함으로써 침해를 시도합니다. 이 문서는 메일에 직접 첨부되어있거나, Google Drive 또는 Microsoft OneDrive 같은 파일 저장 서비스 등에 저장되어 있기도 합니다. 이러한 악성 매크로들은 실행되면 김수키 소유의 명령·제어

(command and control) 시스템과 은밀하게 연결되며, 결과적으로 공격 대상 소유의 기기에 대한 김수키의 접근을 가능케 합니다.

- 몇몇 경우에서 김수키는 "사칭되거나" 가짜이지만 진짜처럼 보이는 웹사이트, 포털 또는 모바일 애플리케이션을 개발하고, 공격 대상들이 비밀과 여타 정보들을 입력하도록 유도하여 입력한 정보들을 절취하였습니다. 일단 공격 대상의 계정을 침해하면, 김수키가 종종 사용하는 BabyShark 라는 악성코드를 통해 피해자의 통신 내용에 대해 지속적으로 접근할 수 있는 권한을 얻게 됩니다. 김수키 해커들은 피해자의 모든 이메일들이 자신들의 통제 하에 있는 또 다른 이메일 주소로 자동 전달되도록 설정해놓는 것으로도 알려져 있습니다.

이 같은 스피어피싱 공격을 통해 수집된 피해자의 답변 및 반응은 북한에 외교정책 분야에 대한 통찰력이라는 추가적인 이점을 제공합니다. 북한 연구 집단을 대상으로 하는 이 같은 은밀한 정보 수집 행위는 김정은 정권에 매우 가치 있을 것으로 추정되며, 이들에게 컴퓨터 네트워크 운영(CNO)을 통해서 얻을 수 있는 것 이상의 정보 채널을 제공합니다.

비록 모든 북한 소속 APT 조직들이 사회공학 기법을 사용하기는 하지만, 이 권고문에서 설명하고 있는 수법과 주제들은 김수키에 특정된 것입니다.

공격 위협 지표

김수키의 주요 공격 분야 대상들은 악의적인 북한 사이버 행위자들의 특징이라고도 할 수 있는 이하 행위들을 잘 인지하고 있어야 합니다.

- 초기 소통은 종종 악성 링크나 첨부파일 없이 이루어지며, 일견 무해해 보입니다. 그 이후의 소통 과정에서 주로 컴퓨터 또는 네트워크에 대한 공격을 개시하기 위한 악성 링크 및 문서가 첨부됩니다.

- 피싱 이메일 본문에는 피해자가 공격당하기 전 다른 사람들과 정상적으로 주고받았던 연락 내용에서 추출한 실제 메시지가 포함되어있을 수도 있습니다.

- 영어로 작성된 이메일에서는 때때로 어색한 문장구조와 부정확한 문법이 발견되기도 합니다.

- 이메일 본문에 북한에서만 사용되는 한국어가 사용되었을 수도 있습니다.
- 정책 관련 정보에 대한 직간접적 지식을 보유한 피해자들(예 : 북한・아시아・중국・동남아시아 관련 업무에 종사하는 한미 정부 인사들, 높은 수준의 비취인가를 보유한 한미 정부 인사들, 군 관련 인사들)에 대한 접근은 이 주의보에 언급된 공통 주제 및 질문들을 통해 이루어집니다.
- 공격에 사용되는 이메일 도메인은 일견 정상적인 언론사 웹사이트 같지만, 기업에서 공식적으로 사용하는 웹사이트 도메인과 일치하지 않습니다. Virus Total 같은 오픈소스 악성 프로그램 점검 사이트 등을 통해 이러한 가짜 도메인들을 식별할 수 있습니다.
- 사칭된 이메일 계정들의 철자는 대학교 안내 책자 또는 공식 웹사이트에 나열된 정상적인 이름 및 이메일 주소의 철자와 비슷하지만 미세하게 다릅니다.
- 공격에 사용되는 악성 문서들은 문서 열람을 위해 "매크로 실행" 버튼의 클릭을 요구합니다.
- 해커들은 공격 대상이 첫 번째 스피어피싱 메일에 응답하지 않아도 끈질기게 접근하며, 첫 번째 연락으로부터 2-3 일 내에 후속 메일을 보낼 가능성이 높습니다.
- 발신자가 스스로 공식적인 사람 / 기관임이라고 주장하나, 실제 메일은 비공식적인 이메일 서비스를 통해 발송되는 경우도 있습니다.

공격수법 및 주제

김수키는 공격 대상, 메시지 내용, 초기 공격 개시에 사용된 악의적 메커니즘 또는 속임수 등으로 특징지어지는 주제들로 스피어피싱 작전을 전개합니다. 기자, 학자 혹은 싱크탱크 연구자들을 사칭하거나 겨냥하여 아래와 같은 주제로 요구 및 제안하는 것에 주의해야 합니다.

- 외교정책 관련 질문에 응답해줄 것을 요청
- 설문조사 참여 요청
- 인터뷰 요청

- 문서 검토 요청
- 이력서 송부 요청
- 연구물 작성에 대한 보수 지급 제안

김수키는 공격 대상의 관심사에 맞추어 주제를 조정하고, 북한 업무 관계자들 사이에서 논의될만한 현안들을 반영하여 내용을 업데이트할 것입니다.

아래 사례들은 상기 공통 주제들이 다양한 형태로 반영된 김수키의 실제 스피어피싱 공격 시도 사례들입니다. 몇몇 경우에서 사이버 행위자들은 기자를 사칭하여 싱크탱크 연구원들을 표적으로 삼기도 하고, 또 다른 경우들에서는 학자를 사칭하여 다른 학자들을 공격하기도 합니다. 사실상 이러한 주제와 속임수의 모든 가능한 조합들이 이미 관찰되었습니다.

1. 기자 사칭

김수키는 믿을만한 사람으로 가장하여 북한 관련 업무에 종사하는 유명인사들에게 질문하기 위해 실제 기자들과 방송 작가들을 사칭하기도 합니다. 일반적으로 질문들은 현안과 관련된 것이며, '미국 전문가들이 보기에 북한이 미국과 대화를 재개할 것 같은지, 북한이 미사일 시험을 재개할 것 같은지, 중국이 어떻게 반응할 것 같은지' 등의 주제들과 관련되어 있습니다. 대부분의 경우 김수키 해커들은 첫 번째 이메일에는 악성 프로그램을 첨부하지 않습니다. 대신, 그들은 인터뷰 가능 여부를 문의하는 소개 메일을 먼저 보냅니다.

이메일 교신 사례 1:

제목 : [<**실제 한국 언론사 프로그램 이름**>] 인터뷰 요청

<**박사 이름**>박사님 안녕하세요, <**한국 언론사 프로그램 이름**> <**작가 이름**>작가입니다.

다름이 아니오라 제가 요즘 북한 관련 프로 준비중인데 전문가님의 도움이 필요해서입니다.

그저 간단히 몇 가지 질문에 대한 답변글 주시면 됩니다.

<대학교 이름> <교수 이름> 교수님께 부탁했더니 박사님 추천하시더라구요.

그럼 긍정적 답변 기다리겠습니다. 감사합니다.

후속 이메일 : 만약 공격 대상이 인터뷰에 응하기로 하면, 공격자들은 악성 컨텐츠를 포함한 두 번째 이메일을 발송합니다.

> 제목 : RE: RE: [<**한국 언론사 프로그램 이름**>] 인터뷰 요청
>
> 박사님 질문지 보내드립니다.
>
> 매 질문에 대한 답변글을 4-5 줄 정도로 해주시면 됩니다.
>
> 잘 부탁드립니다. <**작가 이름**> 작가 드림
>
> @첨부 파일 : [<**한국 언론사 프로그램 이름**>] 질문지. docx

김수키 해커들이 싱크탱크 직원들을 공격하기 위해 실제 기자를 사칭하는 사례도 발견되었습니다. 김수키 해커들이 보낸 스피어피싱 이메일들에서는 흔히 △러시아의 우크라이나 침공, △북-미 관계, △북핵문제 및 안보 관련 주제들, △아시아 지역에 대한 정책 입안자들의 입장, △북중·북러 관계 등 '현안'과 관련된 질문들이 발견됩니다.

이메일 교신 사례 2:

> 안녕하세요, <**실제 미국 언론사 이름**>의 <**실제 기자 이름**>입니다. 잘 지내고 계시죠?
>
> 북한은 지난 10 월 4 일 또다시 미사일을 발사하는 등 변화한 시대에도 불구하고 여전히 구식 전략을 사용하고 있습니다. 북한이 일본 열도 상공을 통과하는 미사일을 발사한 것은 트럼프 前 대통령이 집권하고, 김정은이 미국과의 갈등 수위를 고조시키려는 의도인 것처럼 보였던 2017 년 이후 처음입니다.
>
> 현재 상황에 관련된 질문을 몇 가지 드리고 싶습니다.
>
> 1) 10 월 중순으로 예정된 중국의 당대회 직후 북한이 핵실험을 감행할까요?
>
> 2) 북한의 공격에 대한 보다 조용한 접근법이 더 타당할까요?
>
> 3) 일본이 방위 예산을 늘리고 보다 적극적인 방위정책을 들고 나올까요?
>
> 질문들에 대한 답변을 5 일 이내에 보내주시면 감사드리겠습니다.
>
> 좋은 주말 보내십시오. <**실제 기자 이름**> 드림

2. 학자 사칭

김수키는 한국 학자들을 사칭하여, 싱크탱크 연구원들을 대상으로 스피어피싱 메일을 발송하기도 합니다. 스피어피싱 메일의 내용은 북핵 및 한반도 비핵화에 대한 전문가 설문조사 또는 이메일 인터뷰에 참여해줄 것을 요청하는 것이었습니다.

이메일 교신 사례 3:

제목 : [<**한국 싱크탱크 이름**> 설문조사 요청의 건]

<**싱크탱크 직원 이름**>선생님, 안녕하십니까?

<**한국 싱크탱크 이름**>의 <**연구원 이름**> 연구원입니다.

사전연락 없이 메일 드린 점 양해 해주길 바랍니다.

다름이 아니오라 현재 저희 연구소에서 진행중인 북한의 핵고도화 정책과 관련하여 선생님께 설문조사를 의뢰드리기 위해서입니다.

본 설문조사의 주제는 '북핵 고도화와 한반도 비핵화에 대한 국내 전문가 인식조사'이며, 이번 설문조사를 통하여 북해문제 해결 및 한반도 비핵화를 위한 정책 방안을 모색하고자 합니다.

모든 응답 내용은 비공개로 처리되며 본 연구를 위해서만 사용되오니 아무쪼록 성심성의껏 도와주시길 바랍니다.

설문에 응해주실 경우 소정의 사례비(30 만원)을 지급하고자 합니다. 수락 여부 회신주시면 설문지 보내드리도록 하겠습니다.

긍정적 답변 기다리겠습니다.

감사합니다.

<**연구원 이름**> 드림

후속 이메일 : 이후 공격대상이 설문 참여 요청에 응할 경우, 김수키는 악성 컨텐츠가 포함된 설문지와 사례비 지급 서류를 송부합니다.

제목 : RE: RE: [<**한국 싱크탱크 이름**> 설문조사 요청의 건]

<**한국 싱크탱크 직원**> 선생님 회신이 늦어 죄송합니다. (요즘 정신이 없다보니...)

성심껏 답해주시느라 고생하셨습니다.

사례비 지급 관련 필요한 서류(개인정보동의서)를 별첨 송부드리니,

소속/성명/주민번호/은행명 및 계좌번호/자필서명을 기입하시고 통장 및 신분증 사본을 첨부하셔서 회신해주시면 대단히 감사하겠습니다.

공사로 다망하시겠으나 <기한 날짜>까지 회신해주시면 대단히 감사하겠습니다. 관련하여 문의사항이 있으시면 언제든 편하게 연락 부탁드립니다.

갑사합니다.

<**한국 대학교 연구소 연구원 이름**> 드림

P.S. 문서를 보호하였습니다. 비번은 password.txt 파일로 함께 보내드립니다.

@첨부 파일 : 개인정보이용동의서

이메일 교신 사례 4:

아래는 김수키 해커들이 대학 교수나 연구원생을 가장하여 답변을 요청하고, 질문 리스트나 클라우드 서비스로 연결되는 악성 링크를 발송하여 공격대상 소유 문서에 접근권한을 얻고자 하는 사례입니다.

수신 : <**외교 문제 전문가 이름**>

제목 : Re : 인터뷰 요청

<**외교 문제 전문가 이름**>께,

교수님들이 바쁘신 관계로 답변이 늦어 죄송하고 친절하게 답변해주셔서 정말 감사드립니다.

<실제 미국 대학교 교수 이름> 교수님과 협의 결과 약간의 수정사항이 발생하였는데, 아래 링크를 확인해보시고 만약 다른 의견이 있으시면 알려주십시오.

https: <악성 드라이브 링크>

비밀번호 : <비밀번호>

<**가상의 대학생 이름**> 드림

수신 : <**외교 문제 전문가 이름**>

참조 : <**학자 이름**>

빠른 회신 감사드립니다. <**실제 미국 대학교 교수 이름**> 교수님과 다시 협의한 결과 선생님께서 말씀해주신 방향으로 마무리짓기로 하였습니다. 아래 업데이트된 내용을 확인해주시기 바랍니다.

https: <악성 드라이브 링크>

비밀번호 : <비밀번호>

현재로서는 최종 검토를 마친 뒤 일주일 내에 저희 웹사이트에 업로드할 계획입니다. 관련하여 궁금하신 점이 있으시면 언제든지 연락주십시오. <**가상의 대학생 이름**> 드림

3. 싱크탱크 연구원 사칭

김수키 해커들은 실제 한국 싱크탱크 연구원들을 사칭하여 정치 전문가와 북한 전문가들에게 스피어피싱 이메일을 보냅니다. 이들은 유대관계를 형성하기 위해 정상 이메일을 발송하여 소통을 시작하고, "북한의 외교정책과 우리의 대응" 등 다양한 주제들에 대한 의견을 구합니다.

이메일 교신 사례 5:

제목 : [의견요청] <**한국 싱크탱크 명**>] <**부원장 이름**>입니다.

안녕하십니까? <**한국 싱크탱크명**> 부원장 <**부원장 이름**>입니다.

현재 연구소에서 적성중인 글에 대해 논의하기 위해 연락드렸습니다.

주제는 "북의 외교정책과 한국의 대응"입니다.

전공과 다소 거리도 있고 연구도 미약하여 되도록 많은 분들과 의견을 함께 하였으면 합니다.

교수님이 적중한 분이라 생각 들어 메일 드리는 것이오니 양해 바랍니다.

일전에 교수님이 쓰신 글 읽으면서 literally 한줄 한줄 무릎을 치며 공감했습니다.

이렇게 코멘트 요청을 드린 이유이기도 합니다.

그럼 답장 기다리겠습니다. 감사합니다.

후속 이메일 : 김수키 해킹조직은 상기 메일에 대한 답장이 온 경우, '악성 링크 및 파일'이 포함된 메일 및 '첨부파일 열람 방법 안내' 메일 등 여러 차례에 걸쳐 후속 이메일을 주고 받는 과정을 거칩니다. 심지어 피해자 계정정보를 절취하고 악성코드에 감염시킨 후에도 '감사 인사' 메일을 피해자에게 추가로 발송하기도 합니다.

제목 : RE: RE: [의견요청] <**한국 싱크탱크명**> <**부원장 이름**>입니다.

<대용량파일 1 개>

흔쾌히 수락해 주셔서 감사합니다.

자료 파일 별첨하여 송부드립니다.

자료 일독하신 후 의견 몇자 주시면 감사하겠습니다.

보안상 비번(<비밀번호>)을 추가하였습니다.

해킹이 심한 시대라...

아직 편집중의 초고라 많이 미숙한 점 양해 바랍니다.

그럼 귀하신 의견 기다리겠습니다.

이메일 교신 사례 6:

아래는 김수키 해킹조직이 싱크탱크 직원을 공격하여 절취한 계정정보를 이용하여 다른 싱크탱크 직원을 대상으로 공격을 감행하는 사례입니다. 공격 대상자가 요청에 응하면 김수키 해킹조직은 악성첨부물이 포함된 후속 이메일을 발송합니다.

<**싱크 탱크 직원 이름**>님 안녕하세요

<**사칭하는 싱크 탱크명**>을 대표하여, 최근 북한 도발 관련 1,200 단어 분량의 분석 글 작성을 청하게 되어 영광입니다.

지난 10 월 4 일 최근 일본 열도를 넘어 발사한 중거리탄도미사일(IRBM)과 10 월 6 일 2 발의 단거리탄도미사일(SRBM) 발사를 포함하여 최근 일련의 북한 미사일 발사는 북한이 추진중인 수많은 미사일 개발을 상기 시켜주고 있습니다.

서술을 요청드린 논고의 주제는 다음과 같습니다.

1) 10 월 중순 중국공산당대회 직후 북한이 차기 핵실험을 실시할 것인지?

2) 북한의 침략에 대해 보다 조용한 접근이 보장될 수 있는지?

3) 일본은 국방예산을 증액하고 보다 적극적인 국방정책을 펼칠 것인지?

제게 10 월 21 일까지 회신하여 주시기를 부탁드립니다. 또한, 글의 제목은 원하시는 대로 하셔도 무방합니다. 또한, 480 달러 가량의 소정의 원고료를 지급할 수 있음을 알려드립니다.

귀하께서 작성에 응해주신다면 대단히 감사하겠습니다.

감사합니다.

선임 연구원, <**사칭하는 싱크탱크 직원 이름**>

부서명, <**사칭하는 싱크탱크 명**>

후속 이메일 : 김수키 해킹조직은 이후 악성코드가 첨부된 두 번째 메일을 발송하였습니다.

<**싱크 탱크 직원 이름**>님 안녕하세요

답변이 늦어 죄송합니다.

말씀드린대로, 첨부파일을 확인해 주시고, 혹시 문제가 있는 경우 알려주십시오.

PW: <0000>

감사합니다.

선임 연구원, <**사칭하는 싱크탱크 직원 이름**>

부서명, <**사칭하는 싱크탱크 명**>

4. 정부 관료, 법집행 기관, 포털사이트 관리자 사칭

아래는 김수키가 한국 국회나 대통령실 등 정부기관 내 북한 관련 정책을 담당하는 인물을 사칭하여 공격 대상에 접근하는 방식을 보여주는 사례입니다. 이들이 사칭하는 인물은 사전 공격을 통해 계정을 탈취 당했을 가능성이 있습니다. 김수키는 대상자의 메일 송수신 내용이나 주소록 정보로부터 획득한 대상자의 특정 직위, 일정 등 구체적인 정보를 언급하기도 합니다.

이메일 교신 사례 7:

제목 : <**국회의원**> 국회의원실 세미나 "윤정부 통일정책 제언"

안녕하세요, <**국회의원**> 국회의원실 <**국회의원 비서**>입니다.

어제는 바쁘신 와중에도 장시간 저희 세미나를 위해 함께해 주시고 귀한 말씀 들려주셔서 정말 감사했습니다. 덕분에 좋은 회의가 되었습니다.

번거로우시겠지만, 어제 발언하신 취지를 A4 1 장 정도로 요약하셔서 제게 보내주시면, 회의 증빙으로서 큰 도움이 되겠습니다.

그리고 어제 계셨던 분들은 사례비 지급의뢰서를 작성해주셔서 다 받았습니다만, 차장님께서는 양식대로 작성하신 후에 저에게 회신해 주시면 감사하겠습니다.

비번 : <비밀번호>

서류들을 취합하면 다음주에 사례비를 기안하여 진행하겠습니다.

그럼, 조만간 또 모실 기회가 있기를 바라겠습니다. 즐거운 주말 되세요. 감사합니다.

<**국회의원 비서**> 드림

또한 김수키는 대상자의 이메일 계정이 불법 사건에 연루되었다고 속이기 위해 수사 기관 또는 사법당국을 사칭하기도 합니다. 이들은 수사 기관의 권위를 이용하여 공격 대상에 접근함으로써, 대상자의 계정이 탈취되어 국가 안보 또는 범죄와 관련된 사건에 연루되었을 가능성이 있다고 피해자를 협박합니다.

이메일 교신 사례 8:

제목 : <**합법적인 한국 수사기관**>의 <**합법적인 수사관**>입니다.

안녕하세요, <**합법적인 한국 수사기관**>의 <**합법적인 수사관**>입니다.

귀하의 이메일 계정을 이용하여 유튜브에 국가보안법에 위반되는 게시물이 등록되었습니다.

링크: <비디오 링크> 귀하가 <날짜: 0000. 0. 0>에 올린 영상입니다.

게시자명: <**대상자**>

위의 게시자는 탈북민들을 음해하는 게시물을 올리기도 하였습니다. 정확한 게시물 등록자를 찾아내는데 협조바랍니다.

1) 귀하의 컴퓨터 매체 접근 제어 주소(MAC 주소), 이더넷 하드웨어 주소(고유식별정보) 등이 요구됩니다. 이는 귀하의 이메일 계정에 대한 불법 접속을 추적하는데 반드시 필요한 사항입니다.

2) 컴퓨터에서 두 주소를 얻어 메일로 회신하시든가 아니면 아래의 첨부파일에 의해 얻어지는 문서를 회신해 주시기 바랍니다. <점검툴.zip>

3) 메일을 받으신 후 24 시간 내로 회신해주시고 메일은 바로 삭제하여 주시기 바랍니다.

또한, 김수키는 유명 포털사이트 운영자나 관리자를 사칭하여, 계정에서 비정상적인 활동이 감지되었거나 불법 계정으로 등록되어 대상자의 계정 사용이 중지되었다고 주장합니다. 그리고 피해자들이 개인 정보 보호 및 계정 잠금 해제를 위해 메일에 첨부된 링크를 클릭하여 비밀번호 변경 등 조치를 수행하도록 권고합니다. 첨부된 링크는 합법적인 포털 사이트의 로그인 창으로 위장된 피싱 페이지로 연결되어 대상자의 계정 아이디, 비밀번호를 포함한 개인정보를 입력하도록 하며, 이 때 입력된 개인정보가 북한 사이버 행위자들에 의해 탈취됩니다.

이메일 교신 사례 9:

제목 : 회원님의 <**합법적인 포털 사이트**> 계정 비밀번호가 유출되었습니다.

누군가가 미승인 애플리케이션을 사용하여 회원님의 계정(<**이메일 주소**>)에 로그인을 시도했습니다. 세부정보는 다음과 같습니다.

일시 : 0000 년 00 월 00 일 (요일) 00:00 (한국 표준시)

IP 주소 : 00.00.000.00

위치 : 미국(워싱턴)

회원님의 소중한 계정정보를 보호하기 위해 지금 바로 비밀번호를 변경해주세요. 아래 링크를 통해 비밀번호를 변경할 수 있습니다.

<메일 변경하기 링크>

즉시 비밀번호를 변경하지 않는 경우, 계정보호정책에 따라 회원님의 계정이 영구삭제 또는 폐쇄됩니다.

위협 완화 가능 조치

이메일 수신자를 위한 조치:

- 강력한 암호, 다단계 인증, 바이러스 백신 설치 등 기본적 사이버 보안 조치를 이행합니다. 보다 자세한 사항에 대해서는 미국 국가안보국(NSA)의 'NSA's Best Practices for Securing Your Home Network' 또는 국가정보원(NIS)의 '해킹메일 대응요령' 을 참고하십시오.
- 출처가 확인되지 않는 이메일을 통해 받은 문서의 매크로를 실행하지 마십시오.
- 출처가 확인되지 않는 이메일을 통해 공유되는 클라우드 호스팅 서비스 상의 문서를 열람하지 마십시오.
- 신분, 연관된 소셜미디어 또는 계정 등의 진위 여부를 철저하게 확인하십시오. 아래 사항에 특별히 유의하십시오.

  - 상용 공급자를 사칭하는 비공식 또는 개인 이메일 계정에서 오는 공식적인 메시지
  - 북한 사이버 행위자들이 허위 도메인으로 사용하는 것으로 알려진 도메인 및 하위 도메인 변형들 (예시 : johndoe@abccompany.live → johndoe@abccompany.com)

- 특정인과 기존에 소통하고 있었을 경우, 악성일 가능성이 있는 새로운 이메일 주소 또는 계정과 소통하지 말고 기존에 알고 있던 정상적인 연락처를 이용하십시오.
- 수상하다고 의심되는 경우, 올바른 연락처 정보를 얻기 위해 해당 단체의 공식 웹사이트에 문의하십시오.
- 상대의 신분을 여전히 확신할 수 없을 경우, 소통을 계속하기 전에 유선 또는 화상전화를 통해 신분을 확인하십시오. 북한 사이버 행위자는 가상환경 밖에서는 소통하지 않는 것으로 알려져 있으며, 유선 또는 화상 연락을 피할 것입니다.
- 수신된 문의 이메일의 출처를 확인할 수 없는 경우에는 이에 회신하기 전에 위험요소를 고려하십시오.
- 이메일로 제공된 URL 을 클릭하지 말고 검색엔진을 통해 웹사이트를 검색하는 방안을 고려하십시오.
- 별도의 메시지 플랫폼으로 이동하여 소통하자고 요청이 올 경우 주의하십시오.
- 문서를 보낼 때에는 확인된 이메일 주소로만 전송하십시오.

이메일 수신자의 시스템 관리자를 위한 조치:

- 사용자 교육 프로그램과 피싱 대비 훈련을 실시하여 웹사이트 방문, 링크 클릭, 첨부파일 열람으로 인한 위험에 대해 사용자들의 경각심을 높이십시오.
- 가능한 많은 서비스, 특히 웹메일, 가상사설망(VPN), 핵심 시스템 접속 계정, 백업 관리 주요 계정들에 대해 피싱을 방지하기 위한 다단계 인증(MFA)을 요구하십시오.

- 정기적으로 서비스 포트 점검을 통해 당신의 네트워크가 데스크톱 공유 소프트웨어나 가상사설망(VPN), 가상사설서버(VPS)를 통해 원격 접속되고 있는지 확인하십시오. 특히, 데스크톱 공유 소프트웨어 또는 가상사설망 서비스 사용을 통한 계정 접속이 통상적인 관행이 아니라면 확인이 필요합니다.

- 원격 데스크톱 프로토콜(RDP) 또는 여타 잠재적으로 위험한 원격 서비스의 사용을 허용하고 있을 경우, 면밀히 주시하고 보안조치를 취하십시오.

    - 원격 데스크톱 프로토콜을 제한하고 데스크톱 가상화(VDI)를 이용하는 등 내부 네트워크 자원에 대한 접근을 제한하십시오. 위험요소를 평가하고 나서 원격 데스크톱 프로토콜의 운용이 필요하다고 판단될 경우에는, 접속자를 제한하고 피싱 방지 다단계 인증을 요구하는 등 계정 탈취 및 재사용의 위협을 줄이십시오. 원격 데스크톱 프로토콜을 외부에서 사용하도록 허용하는 것이 꼭 필요한 경우에는, 원격 데스크톱 프로토콜이 내부 기기에 접속 가능하도록 허용하기 이전에 가상사설망, 데스크톱 가상화, 또는 다른 방안을 사용하여 연결 관련 인증 및 보안 조치를 취하십시오. 원격 접속 및 원격 데스크톱 프로토콜 로그를 주시하고, 무차별 암호 대입 공격을 차단하기 위해 지정된 횟수만큼 접속 실패시 계정을 잠그도록 설정하고, 원격 데스크톱 프로토콜 로그인 시도를 기록하며, 사용하지 않는 원격 접속/원격 데스크톱 프로토콜 포트를 비활성화 하십시오.

    - 기기 설정을 적절하게 유지하고, 보안 기능이 활성화되도록 유지하십시오. 업무 목적(원격 데스크톱 전송제어 프로토콜 포트 3389 등)으로 사용하지 않는 포트와 프로토콜을 비활성화 하십시오.

    - 네트워크 내 서버 메시지 블록(SMB) 프로토콜에 대한 접근을 필요 서버에 한해 제한하고, 서버 메시지 블록의 예전 버전(SMB 버전 1 등)을 삭제 또는 사용안함으로 설정하십시오. 공격자는 서버 메시지 블록을 이용하여 조직 내 악성코드를 전파합니다.

    - 제3자 공급업체 및 귀하의 단체와 상호 연결된 대상들의 보안 상태를 점검하십시오. 제3자 공급 업체와 외부 소프트웨어/하드웨어 간 모든 연결과 관련하여 수상한 활동이 있는지 모니터링 하고 점검하십시오.

  - 이미 인지하고 있는 승인된 프로그램만이 실행되도록 어플리케이션 통제 정책을 적용하십시오.

- 액티브 콘텐츠(Active Content) 공격이 실행되지 않도록 보호된 보기 모드에서는 문서 뷰어를 통해 열람하도록 적용하십시오.

- 운영체제, 소프트웨어 및 펌웨어에 대한 업데이트가 나오는 즉시 설치하십시오. 시의 적절한 패치 설치는 각 기관이 사이버 위협에 대한 노출을 최소화하기 위해 취할 수 있는 가장 효율적이고, 비용 대비 효과적인 방법 중 하나입니다. 소프트웨어 업데이트와 서비스 기한 만료 공지를 정기적으로 확인하고, 이미 알려진 보안 취약점에 대한 패치에 우선 순위를 부여하십시오. 이러한 과정을 자동적으로 신속하게 수행하기 위해서, 중앙화된 패치관리 시스템을 사용하는 것을 고려하십시오.

- 바이러스 백신 및 악성프로그램 방지 소프트웨어를 모든 계정에 설치하고, 정기적으로 업데이트하십시오.

- 소프트웨어를 설치할 때 관리자 자격 증명을 요구하는 것을 고려하십시오.

- 조직 외부에서 오는 이메일에 대해 위험도가 더 높다는 것을 사용자가 인지하도록 이메일 배너를 추가하십시오.

- 이번 주의보에 포함된 이메일 사례들과 일치하는 이메일을 차단하기 위해 관련 규칙을 추가하는 것을 고려하십시오. 아직 열어보지 않은 악의적 이메일들을 이메일 서버 상에서 확인하는 방법을 알아두십시오. 이는 악의적 이메일 인자들을 확인함으로써, 이러한 방식의 공격이 누구를 대상으로 하는지 이해하기 위한 준비 과정에서 가장 핵심적인 조치입니다.

- 이메일 도메인에 DMARC[1] 및 DKIM[2]을 적용하는 것은 위에서 기술한 공격 수법들에 대한 위험을 직접적으로 완화시키진 못할 수 있으나, 일반적으로는 특정한 방식의 이메일 스푸핑을 어렵게 만들어줍니다.

---

1)DMARC(Domain-based Message Authentication, Reporting and Conformance): 이메일 도메인 소유자가 무단 사용으로부터 도메인을 보호하기 위해 사용하는 이메일 인증 프로토콜

2)DKIM(Domain Keys Identified Mail): 이메일 발신자가 위조되지 않았음을 검증하는 방식

북한 관련 정의에 대한 보상 제도

한미 정부는 피해자들로 하여금 북한의 사이버 활동으로 추정되는 것들을 포함하여, 의심스러운 활동들을 유관 기관에 신고하도록 독려하고 있습니다. 과거 또는 현재 진행 중인 활동을 포함하여 사이버 공간에서 북한의 불법 활동에 대한 정보를 제공하는 경우, 보상을 받을 수 있습니다. 과거 또는 현재 진행 중인 활동을 포함하여 사이버 공간에서 북한의 불법 활동에 대한 정보를 가지고 있는 경우 국무부의 정의에 대한 보상 프로그램을 통해 정보를 제공하면 최대 500 만 달러의 보상을 받을 수 있습니다. 자세한 내용은 https://rewardsforjustice.net/index/?north-korea=north-korea 를 참조하십시오.

부록: 추가 스피어피싱 메일 샘플

메일 교신 사례 10:

제목 : <**그럴듯한 비미국 언론사 이름**>의 <**그럴듯한 언론인 이름**> 입니다.

베이징 동계올림픽이 끝난 후 북한의 향후 방향에 대한 귀하의 생각을 알고자 이 글을 씁니다. 많은 사람은 최근 북한이 도발을 하지 않는 것은 북한이 유일한 주요 동맹국인 중국의 올림픽 분위기를 해치지 않기로 결정했기 때문이라고 생각하지만, 올림픽이 마무리되면 북한이 1 월에 중단한 일련의 미사일 발사 실험을 재개할 가능성이 있다는 추측이 커지고 있습니다.

북한이 미사일 발사 실험을 재개할 것으로 보십니까? 그렇다면 최적의 시기는 언제이며 어떤 종류의 미사일을 선택할 것으로 보십니까?

중국은 3 월 4 일부터 13 일까지 전국인민대표대회와 중국인민정치협상회의를 개최할 예정인데, 그 일정으로 인해 북한의 미사일 시험 발사가 더 연기될 것이라고 보십니까?

북한이 미사일 발사·핵실험 모라토리엄을 해제하겠다고 밝혔는데, 북한이 모라토리엄을 걸고 미국과의 대화를 제의할 가능성이 있다고 보십니까? 그렇다면 미국의 반응은 어떠할 것이라고 보십니까? 이번 주 안에 답변을 보내주시면 대단히 감사하겠습니다.

메일 교신 사례 11:

제목 : 정책자문위원 참고자료 보내드립니다

안녕하세요 위원님,

<**북한 관련 정책 부처**> 의 <**부처 직원**> 입니다.

미 국부무 비건 특별대표 방한 관련자료를 붙임과 같이 보내드리오니 참고하시기 바랍니다.

민감한 사안이 있으니 취급주의 부탁드립니다.

대용량 첨부파일 1 개

<첨부파일 이름.pdf>

메일 교신 사례 12:

친해하는 <**대학교 교수**>님:

안녕하세요, 저는 <**합법적인 비미국 언론사**>의 <**합법적인 언론인**>입니다. 러시아의 우크라이나 침공이 북한을 둘러싼 정세에 어떤 영향을 미칠지에 대한 교수님의 의견을 듣고 싶어서 메일을 드립니다. 아래 질문에 대한 교수님의 의견을 말씀해주실 수 있으실까요?

1) 일부 분석가들은 우크라이나가 부다페스트 각서에 따라 안보보장을 받는 대가로 핵무기를 포기한 후 결국 러시아의 침공을 받게 되었다는 점에서 러시아의 우크라이나 침공으로 인해 북한이 핵 포기를 훨씬 더 꺼리게 되었을 수도 있다고 주장하고 있습니다. 2018 년 싱가포르에서 트럼프 대통령과 김정은이 맺은 합의와 부다페스트 각서는 확실히 유사한 것으로 보이는데, 이러한 주장에 대해서는 어떻게 생각하시는지요?

2) 바이든 행정부가 우크라이나 관련 사태의 전개에 집중하고 있고, 이로 인해 아태지역에서의 경계태세가 어쩌면 느슨해진 틈을 타 북한은 신형 ICBM 을 발사했고 핵실험을 시도할 가능성 또한 있습니다. 북한의 향후 행보를 어떻게 전망하십니까?

3) 북한은 바이든이 이미 레임덕이라고 믿고 현 시기를 신형 무기 개발에 집중할 수 있는 좋은 기회로 보고 있다는 말에 동의하십니까?

4) 중국이 북한의 탄도미사일 발사와 핵실험 가능성을 용인할 것으로 예상하십니까? 북한이 중국과 안정적이고 우호적인 관계를 유지할 수 있거나 유지할 것이라고 생각할 것이라고 생각하십니까? 러시아는 북한에 관심을 가질 여유가 없을까요?

5 일 이내에 답변을 보내주신다면 대단히 감사하겠습니다. 시간 내어 숙고해주심에 미리 감사드립니다.

친애하는,

<**합법적인 언론인**> 드림

메일 교신 사례 13:

제목 : 회원님의 메일계정이 정지되었습니다.

회원님께서 발송하신 메일은 법령 위반의 우려가 있고, 경우에 따라서는 회원님께서 법적 책임을 부담하실 수 있기 때문에 메일계정이 정지되었음을 알려드립니다. 회원님께서 직접 <**한국 포털 사이트**> 메일계정에서 스팸메일을 발송한 적이 없는데 이 메일을 받으셨다면 다른 사람이 회원님의 아이디를 도용하였을 가능성이 있습니다. 이메일 환경설정을 확인하셔서 POP/IMAP 가 '사용됨'으로 설정되어 타인에 의한 도용히 가능하게 되지는 않았는지 확인해주십시오.

만약 이메일 환경설정에서 아무런 문제도 발견되지 않는다면, 회원님의 계정이 해킹되어 개인정보가 도용되었을 가능성이 있습니다. 우선 아래 버튼을 눌러 사용중지를 해제하시고 <**합법적인 수사부서**>의 안내에 따라 필요한 조치를 취하세요.

<포털로그인 창으로 위장한 피싱 페이지 버튼>

메일 교신 사례 14:

제목 : 회원님의 아이디가 사기성 계정으로 등록되었습니다.

안녕하세요, <**합법적인 포털사이트**> 메일 운영팀입니다. 유감스럽게도 회원님의 아이디 <**아이디**>가 사기성 계정으로 등록되었음을 알려드리는 바입니다. 추가 피해를 방지하기 위하여 아래의 조치를 지금 즉시 취하실 것을 권고드립니다.

회원님 계정의 안전과 보안을 보장하기 위하여 가능한 한 빨리 회원정보 페이지를 방문하여 등록된 이름을 확인하시고, 비밀번호를 변경하셔서 계정을 보호해주십시오.

사기성 계정 등록 일시: 0000 년 00 월 00 일 00:00

사기성 계정 등록을 해제하려면 아래의 링크를 클릭하시기 바랍니다.

<사기성 계정 등록 해제 링크>

<**합법적인 포털사이트**>를 이용해주셔서 감사합니다. 더욱 편리한 서비스를 제공하기 위해 최선을 다하겠습니다.