asec.ahnlab.com /ko/86522/

일본을 노리는 Larva-24005 그룹의 피싱 메일 공격 사례

⋮ 2/26/2025

ASEC(AhnLab SEcurity intelligence Center)은 Larva-24005가 국내에서 운영되고 있는 서버를 침해한 뒤, 피싱 메일 발송을 위한 웹 서버, 데이터베이스, PHP 환경을 구축하는 행위를 확인했다.

Larva-24005는 공격 거점을 이용해 국내 뿐만 아니라 일본도 공격 대상으로 삼고 있는 것으로 확인됐다. 주요 공격 대상은 대북 관련 종사자와 북한 체제와 관련된 연구를 하는 대학 교수 등이며 피싱 메일 공격을 위해 C2 서버를 구성하고, 메일 본문에 ZOOM 회의 링크나 웹 포탈 로그인 페이지로 위장해 사용자의 클릭을 유도하고 있다.

본 블로그에서는 Larva-24005가 공격 인프라를 확보하는 과정과 일본을 타깃으로 한 피싱 메일 공격 사례를 설명하고자 한다.

1. Larva-24005

Larva-24005는 북한의 지원을 받는 것으로 알려진 Kimsuky 공격 그룹의 하위 그룹으로, 자사의 위협 관리 분류 체계에 따라 새롭게 명명된 이름이다. 이들은 취약하게 운영되고 있는 Windows 시스템의 RDP 취약점을 통해 최초 침투하는 것으로 보이며, 침투 후에는 Windows 운영 체제에서 원격 데스크톱 프로토콜(RDP) 연결을 활성화하는 오픈소스 유틸리티 RDPWrap과 자체 제작 키로거를 시스템에 설치한다.

2. 공격자가 피싱 메일을 발송하기 위해 사전에 수행하는 행위

2.1 공격 인프라 확보

공격자는 피싱 메일 발송 인프라를 구축하기 위해 원격 데스크톱 프로토콜(RDP)를 이용해 국내 시스템으로 침투한다. 침투 과정에서 사용된 자격 증명 정보의 획득 경로는 명확히 확인되지 않았으나, 무차별 대입 공격이나 사전에 확보한 인증 정보를 활용한 것으로 추정된다.

Larva-24005는 일부 인프라를 확보할 때 Bluekeep 취약점을 이용하는 것으로 확인된다. Bluekeep 취약점(CVE-2019-0708)은 원격 데스크톱 프로토콜(RDP)에서 발견된 원격 코드 실행(RCE) 취약점으로, RDP 서비스에 악의적인 패킷을 전송해 원격 명령을 실행할 수 있다. Kimsuky 공격 그룹은 과거부터 Bluekeep 취약점을 이용했으며, 관련 내용은 ASEC 블로그 '[Kimsuky] Operation Covert Stalker'에서 확인할 수 있다. Bluekeep 취약점은 Windows 2008 R2 버전 이하의 취약한 버전의 운영체제 대상으로만 공격을 수행할 수 있으며, 최신 OS를 사용하는 경우에는 취약점의 영향을 받지않는다.

2.2 XAMPP 설치

공격자는 공격 인프라를 확보한 후, 시스템에 웹 서버 구동에 필요한 Apache, MariaDB, PHP, Perl 등이 포함된 통합 패키지인 XAMPP를 설치한다. XAMPP를 이용해 전체적인 C2 환경을 관리하며, 키로거 결과 파일 및 피싱 메일 피해자 정보를 텍스트 파일 형태로 저장한다. 또한, 공격자는 피싱 메일 발송 기능을 구현하기 위해 PHPMailer를 설치한다. PHPMailer는 PHP 코드를 통해 이메일을 쉽게 발송할 수 있는 라이브러리이며, 구성 요소 중 mailer.lib.php 파일에 피싱 메일 발송자 주소를 명시해둔다. 공격에 사용된 계정은 웹 포털 관련 계정이였으며, 현재는 모두 정지된 상태이다.

- "invoice_nerolpy@kakao.com"
- "naver-no-reply@kakao.com"
- "www.invoice@kakao.com"
- "www.navercorp@kakao.com"
- "www.naver.reply@kakao.com"
- "invoice_hometax@kakao.com"

- “navercorp-rep1y@daum.net”
- “invoice.norep1y@daum.net”
- “nonghyupcorp@daum.net”
- “f****07@knd.biglobe.ne.jp”

표 1. 공격자가 피싱에 이용한 메일 주소 목록

2.3 일본어 입력기 설치

공격자는 공격 인프라에 일본어 입력기(IME)를 설치한다. IME(Input Method Editor)는 사용자가 키보드에 없는 문자 및 기호를 입력할 수 있게 해주는 소프트웨어다. 일반적으로 국내 Windows 시스템들은 일본어 입력기가 설치되어 있지 않다. 공격자는 일본을 타깃으로 한 피싱 메일 발송이나 일본어로 검색을 위한 목적을 가지고 일본어 입력기(IME)를 공격 인프라에 설치한 것으로 보인다.

그림 1. 공격자가 피해 시스템에 설치한 일본어 입력기

2.4 피싱 페이지 준비

공격자는 IIS_USER 계정의 다운로드 폴더와 XAMPP 홈 폴더에 미리 제작한 피싱 페이지를 저장한다. IIS_USER 계정은 Larva-24005가 공격 인프라를 확보한 후, 생성하는 계정이다. 피싱 페이지들은 iCloud, OneDrive, Outlook, Naver, Google 등 정상 서비스로 위장하여 사용자의 로그인 정보를 탈취하는 데 사용된다. 다만, 피싱 페이지들은 공격 인프라에서 흔적만 확인됐으며, 파일들은 이미 삭제되어 확보할 수 없었다.

Path
C:\Users\IIS_USER\Downloads\login_outlook\OneDrive.html
C:\Users\IIS_USER\Downloads\login_outlook\outlook_login.html
C:\Users\IIS_USER\Downloads\outlook_login.html
C:\Users\IIS_USER\Downloads\outlook_login1.html
C:\Users\IIS_USER\Downloads\outlook_login_t.html
C:\Users\IIS_USER\Downloads\qweWEwerSDFertypk\login_outlook\OneDrive.html

그림 2. 공격자가 사용한 피싱 페이지 목록

3. 공격자의 피싱 타깃 선정 방식

공격자는 확보한 공격 인프라의 웹 브라우저(Chrome, MS Edge)를 이용해 Google 검색을 수행하며, 관련 키워드를 추가하고 반복 검색을 통해 목표에 대한 정보를 수집한다. 또한, 피싱 이메일을 통해 확보한 계정 정보를 이용해 웹 포털, 메일 플랫폼(Outlook 등)에 직접 로그인하고, 피해자의 이메일 함에서 추가 공격 대상과 관련 정보를 찾아낸다. 주로 일본에서 북한 관련 활동을 수행하는 대학 교수와 비영리 단체가 표적이 된다.

- 大阪高等裁判所(오사카 고등 법원 판결)
- 기사다 국회 연설
- 사에키 히로아키
- 북한 귀국자의 생명과 인권을 지키는 모임 사에키 히로아키
- 나카무라 쇼키 북한 납치
- 일본 로켓 말레이시아
- 산케이정치부 정치부장
- 오사카 유신회
- 북한인권 인도네트워크 대표 도쿠노
- 한일지방자치제도연구회
- 북한 일본 회담

표 2. 공격자가 Chrome 웹 브라우저에서 검색한 키워드 일부

공격자는 일본 정세와 관련된 뉴스도 지속적으로 수집한다. 주로 일본 니케이(nikkei) 신문을 통해 북한, 일본과 관련된 기사를 열람하며, Chrome 웹 브라우저 방문 이력을 통해 확인된 기사 목록으로는 '북한, 탄도미사일 발사 방위성 「일본의 EEZ 외 낙하」', '북한과의 대화를 이끌어낼 열쇠는 일본의 새로운 요구일 수 있다', '닛케이 평균, 장중 지난해 최고가 경신… 33년 만의 최고 수준' 등이 있다.

그림 3. 공격자가 열람한 기사 #1 (북한, 탄도미사일 발사 방위성 「일본의 EEZ 외 낙하」)

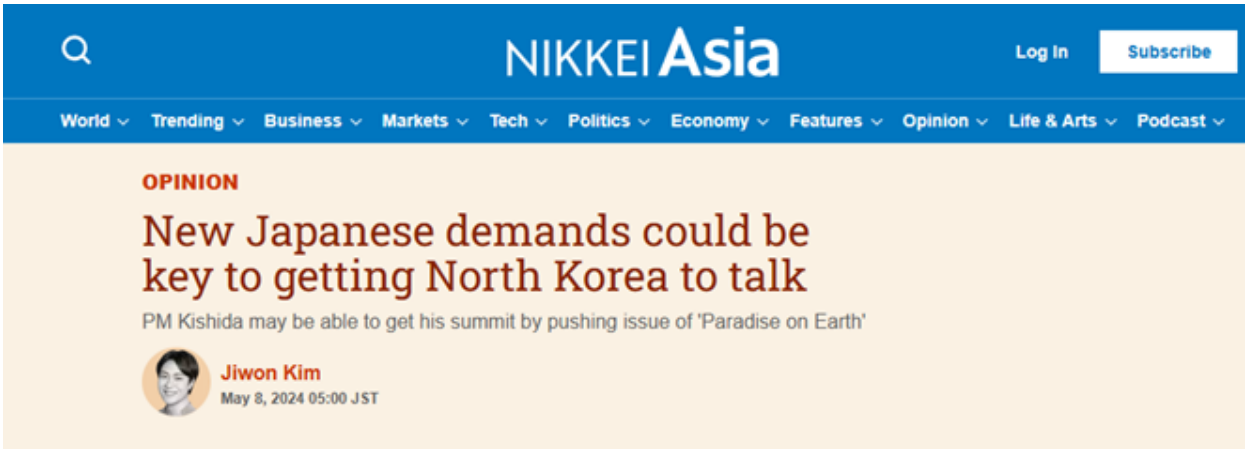

그림 4. 공격자가 열람한 기사 #2 (북한과의 대화를 이끌어낼 열쇠는 일본의 새로운 요구일 수 있다)

4. 피싱 메일 발송

공격자는 공격 타깃의 대한 정보를 충분히 습득하고 나서, 공격 인프라에 설치된 PHPMailer를 이용하거나 수집한 피해자의 계정으로 로그인해 피싱 메일을 발송한다.

Larva-24005가 사용하는 피싱 메일은 크게 두 가지 방식으로 구분된다. 악성 파일을 압축하여 첨부하거나, 메일 본문에 악성 URL을 삽입하는 것이 특징이다. 이번 사례에서 확인된 방식은 메일 본문에 악성 URL을 삽입하는 방식이였으며, 피싱 메일 내용에는 수신자가 관심 가질만한 소재나 주변 사람을 가장한 내용이 포함되어있다.

공격자가 구글 번역기를 통해 한국어를 일본어로 번역한 정황도 존재한다. 아래 그림 같이 피싱 메일 본문 작성에 사용할 문구를 번역한 것으로 확인된다.

그림 5. 공격자가 구글 번역기를 통해 한국어를 일본어로 번역한 모습

아래에 소개할 사례들은 공격자가 피해 시스템에 설치한 키로거의 로그 파일에서 확인된 내용들로 구성됐다.

4.1 첫 번째 사례

공격자는 일본 한 대학교의 국제커뮤니케이션과 교수를 타깃으로 Zoom 회의 초대장으로 위장한 피싱 메일을 발송했다. 해당 교수는 북한 체제의 생존과 관련한 논문을 집필한 이력이 있으며, 교수가 사용하는 대학교 이메일 주소는 인터넷상에서 쉽게 확인할 수 있다.

- From: FROM.teamzoom_reply@daum.net
- 메일 제목: 0000 さんがあなたを予約されたZoomミーティングに招待しています (0000씨가 당신을 예약하신 줌 미팅에 초대하고 있습니다)

메일 본문 내용은 안보 외교 정책 연구회의를 위한 프로그램 안내 내용이며 발표자와 발표 내용, 발표 시간 등이 포함된다. 또한, 외교 정책 연구회의 참가를 위한 Zoom URL이 포함되어 있었으나, 해당 URL은 정상 URL이 아닌 공격자의 C2 서버 주소와 연결되어 있다.

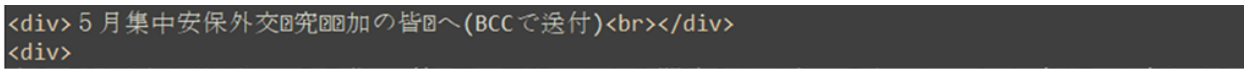

그림 6. 공격자가 발송한 피싱 메일 본문 내용 #1

공격자는 피싱 메일을 발송한 뒤 피해자가 메일을 열람했는지 확인하기 위해 수신 확인 기능도 이용한다.

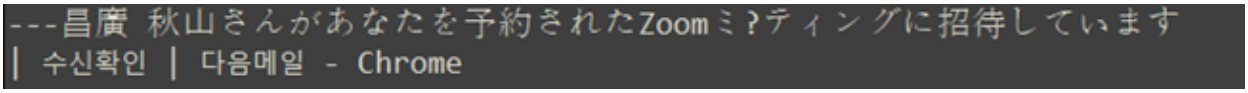

그림 7. 피싱 메일 수신 확인 이력

4.2 두 번째 사례

공격자는 공격 대상의 계정 정보를 탈취하기 위해 Microsoft의 로그인 페이지로 위장한 링크를 첨부해 메일을 전송한다. 피해자가 이를 인지하지 못하고 해당 페이지에 계정 정보를 입력하면 입력된 계정 정보는 공격자의 C2 서버로 전송된다. 공격자가 사용한 메일 주소는 다음과 같다.

- noreply_microprotect@naver.com
- office365_service@naver.com

공격자는 메일 본문에 하이퍼 링크를 삽입하여 피해자를 피싱 페이지로 유도한다. 아래 그림은 공격자가 피해 시스템에 설치한 키로거에 의해 기록된 내용으로, 메일 본문에는 일본어가 포함되어 있다. 또한, 공격에 활용된 polypheou.jp는 일본의 건강보조회사 관련 웹사이트인데 공격자는 C2 주소로 서브 도메인을 변경해 사용한 것으로 확인된다.

그림 8. 공격자가 발송한 피싱 메일 본문 내용 #2

해당 링크를 통해 피싱 페이지로 이동하면 다음과 같이 타깃의 이메일 주소가 포함되어 있는 로그인 페이지를 확인할 수 있다. 공격자는 공격 타깃별 맞춤형 피싱 페이지를 제작하여 스피어 피싱 메일을 발송한다.

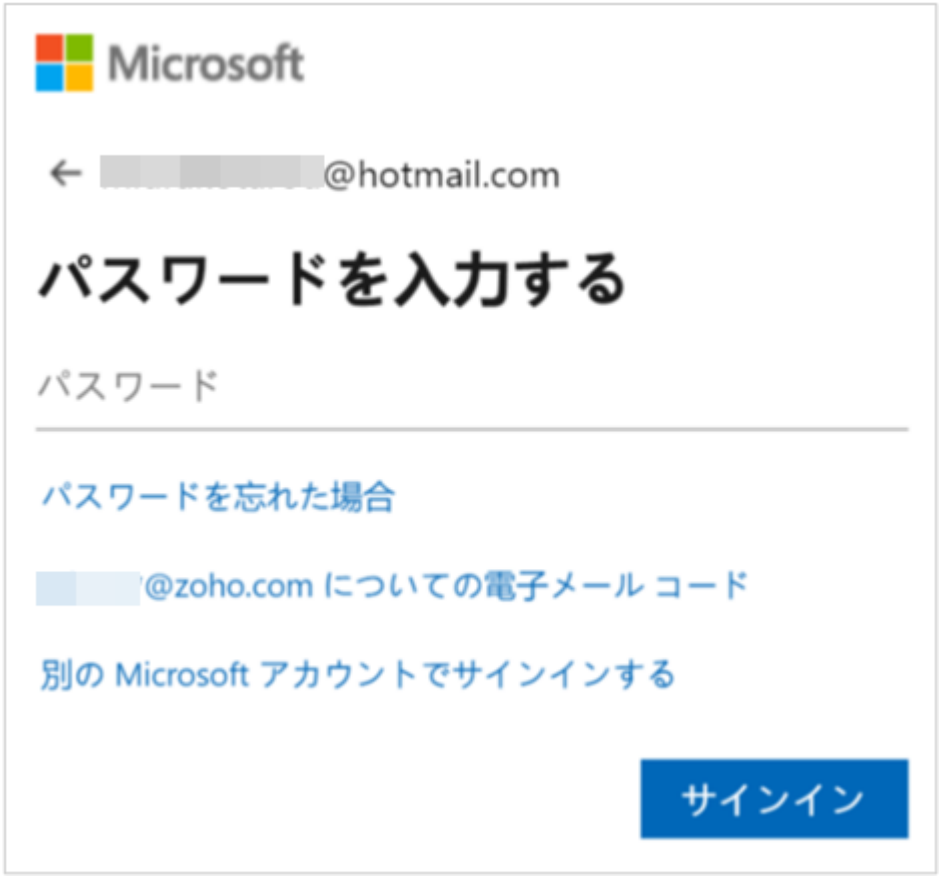

그림 9. Microsoft 로그인 피싱 페이지

5. 결론

앞서 설명한 사례에서 볼 수 있듯이, Larva-24005 공격 그룹은 한국과 일본을 대상으로 다양한 유형의 피싱 메일을 이용한 공격을 지속적으로 수행하고 있는 것으로 확인된다.

공격자는 피싱 메일을 통해 수신자의 클릭을 유도하고, 정상 사이트로 위장한 피싱 사이트로 리다이렉트하는 등 지속적인 악성 행위를 시도하고 있다.

이들은 단순히 정상 사이트를 위장하는 것에 그치지않고, 타깃의 관심사나 관련 인물을 사칭하여 메일 본문을 작성하기 때문에, 메일 수신시 발신자 정보를 꼼꼼히 확인하고 첨부 파일이나 링크 클릭에 각별한 주의를 기울여야 한다.

특히 이메일에서 외부 사이트로 연결되는 경우, 연결된 사이트 주소가 정상 사이트 주소와 일치하는지 반드시 확인해야 하며, 조금이라도 의심스러운 경우에는 계정 정보를 입력하지 않도록 주의해야 한다.

MD5

b500a8ffd4907a1dfda985683f1de1df

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//auth[.]portal[.]pikara[.]ne[.]polypheou[.]jp/

http[:]//download[.]mail[.]naver[.]corn-file[.]kro[.]kr/

http[:]//t[.]infomail[.]microsofit[.]com[.]polypheou[.]jp/

http[:]//us06web[.]zoom[.]us[.]meet[.]polypheou[.]jp/

http[:]//www3[.]icloud[.]vbox[.]l[.]up[.]tcmp[.]polypheou[.]jp/

추가 IoC는 ATIP에서 제공됩니다.