No.185 | 2025.2

ESRC 보안동향보고서

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.

ESTsecurity

ESRC 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 URL 통계

1. 악성코드 동향

2025 년 새해부터 크고작은 해킹 공격이 많이 발생하였습니다.

GS 리테일이 해킹 공격을 당해 고객 9 만명의 개인정보가 유출되었으며, 하이트진로역시 랜섬웨어 공격을 당했으며 이 과정에서 고객의 개인정보가 유출된 것으로 추정되고 있습니다. 한국예술종합학교(한예종) 역시 해킹당해 1 만 8000 여명의 학생들 개인정보가 유출된 것으로 확인되었습니다.

본인의 개인정보가 유출된 것으로 의심된다면, 해당 홈페이지 계정의 비밀번호 뿐만 아니라 동일한 계정을 사용하고 있는 다른 사이트의 비밀번호들도 일괄 변경이 필요합니다. 또한 2 단계 인증 설정 등 추가적인 보안조치를 취해 놓으시는 것이 좋습니다.

국가의 지원을 받는 해킹 조직들의 공격도 점점 거세지고 있습니다.

북한의 지원을 받는 라자루스(Lazarus)는 오픈소스 프로젝트를 악용한 대규모 공급망 공격을 통해 전 세계적으로 피해를 입혔습니다. 이번 공격은 주로 개발자와 암호화폐 종사자들을 대상으로 진행되었으며, 24 년 9 월부터 시작해서 25 년 1 일까지 수차례 진행된 것으로 확인되었습니다.

뿐만아니라 라자우스는 노트패드++의 플러그인인 '컴페어플러스'를 위장한 '쿠키플러스' 악성코드를 유포하기도 했습니다. 이 공격의 대상은 2019 년 암호화폐 기업을 대상으로 시작되었지만, 최근에는 핵, 방위, IT 등 중요 산업까지 공격 대상을 확대하였습니다. 특히 이러한 악성파일을 링크드인 등 구직 플랫폼을 통해 전파하여 타깃화 된 감염을 시도하였습니다.

라자루스의 공격 대상 범위는 계속 넓어지고 있으며, 공격도 지속적으로 정교해 지고 있어 글로벌 사이버 보안에 큰 위협으로 자리매김 하고 있습니다.

북한의 해킹 조직 뿐만 아니라 중국 해킹 조직의 공격 역시 날로 거세지고 있습니다 .

최근 일본 경찰청과 내각 사이버보안센터(NISC)가 합동 발표문을 발표했는데, 중국계 해커단체인 '미러페이스(MirrorFace)'가 2019~2024 년까지 일본의 항공우주 등 첨단기술 정보 탈취를 목표로 수백 건의 사이버 공격을 감행했다고 밝혔습니다. 일본은 이 미러페이스 조직이 중국이 배후로 있는 'APT10'조직과 관련이 있는 것으로 추정하고 있습니다.

24 년 12 월, 미국 재무부 전산시스템이 해킹을 당했는데 이 공격의 배후에는 중국 정부와 연계된 것으로 보이는 해킹조직이 있는 것으로 추정되고 있습니다. 또한 트럼프 대통령 대선 캠프의 통화 데이터와 메타데이터를 탈취한 공격이 발생했는데 '솔트 타이푼'이라는 중국해커조직의 소행으로 밝혀졌습니다.

필리핀과 대만 역시 중국발 해킹에 시달리고 있지만 정작 중국 정부는 해킹 공격의혹을 강하게 부인하고 있습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2025 년 1 월에는 Gen:Variant.Graftor.927510, Trojan.GenericKD.71231591, Worm.IM-VB.as, Win32.Grenam.Dam.G 악성코드가 새롭게 Top 15 에 진입하였습니다.

루트킷 악성코드 탐지명인 Gen:Variant.TDss.49 이 지난 10 월 이후로 여전히 최상위권을 유지하고 있으며, Microsoft Windows 및 Office 제품의 라이선스 인증을 우회하는 데 사용되는 KMS 기반 불법 인증 도구에 대한 탐지명 Misc.HackTool.AutoKMS, Application.Hacktool.BBJ, Misc.HackTool.KMSActivator 도 Top15 에 포함되었습니다.

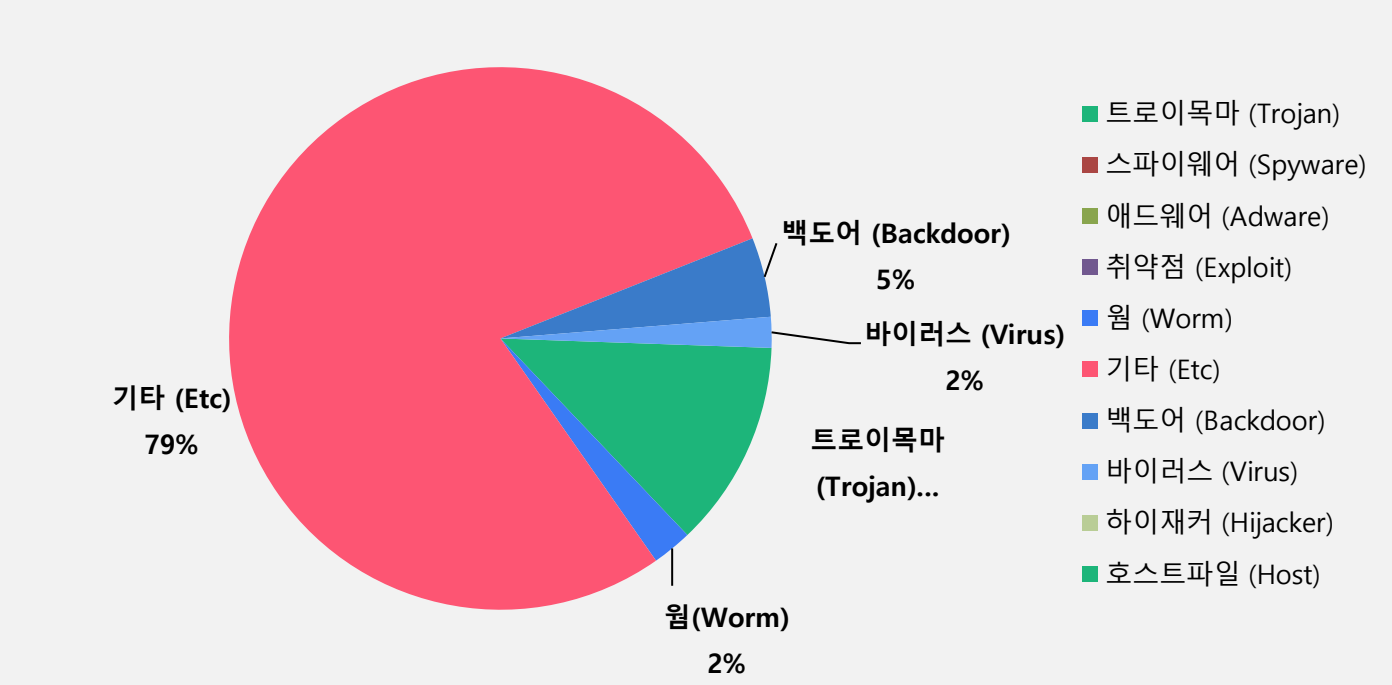
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.TDss.49	ETC	162290
2	-	Gen:Variant.Lazy.266772	ETC	93356
3	↑1	Gen:Variant.Tedy.675091	ETC	39996
4	↓1	Misc.HackTool.AutoKMS	ETC	28819
5	↑1	Trojan.DDoS.Nitol.gen	Trojan	27312
6	NEW	Gen:Variant.Graftor.927510	ETC	26541
7	↓2	Backdoor.Generic.792814	Backdoor	23814
8	NEW	Trojan.GenericKD.71231591	Trojan	20368
9	↑2	Trojan.Acad.Bursted.AK	Trojan	14323
10	↓3	Application.Hacktool.BBJ	ETC	13017
11	NEW	Worm.IM-VB.as	Worm	11948
12	↓4	Gen:Variant.Lazy.20522	ETC	11489
13	↓4	Gen:Variant.Ulise.144799	ETC	10051
14	↓4	Misc.HackTool.KMSActivator	ETC	9791
15	NEW	Win32.Grenam.Dam.G	Virus	9198

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025 년 1 월 1 일 ~ 2025 년 1 월 31 일

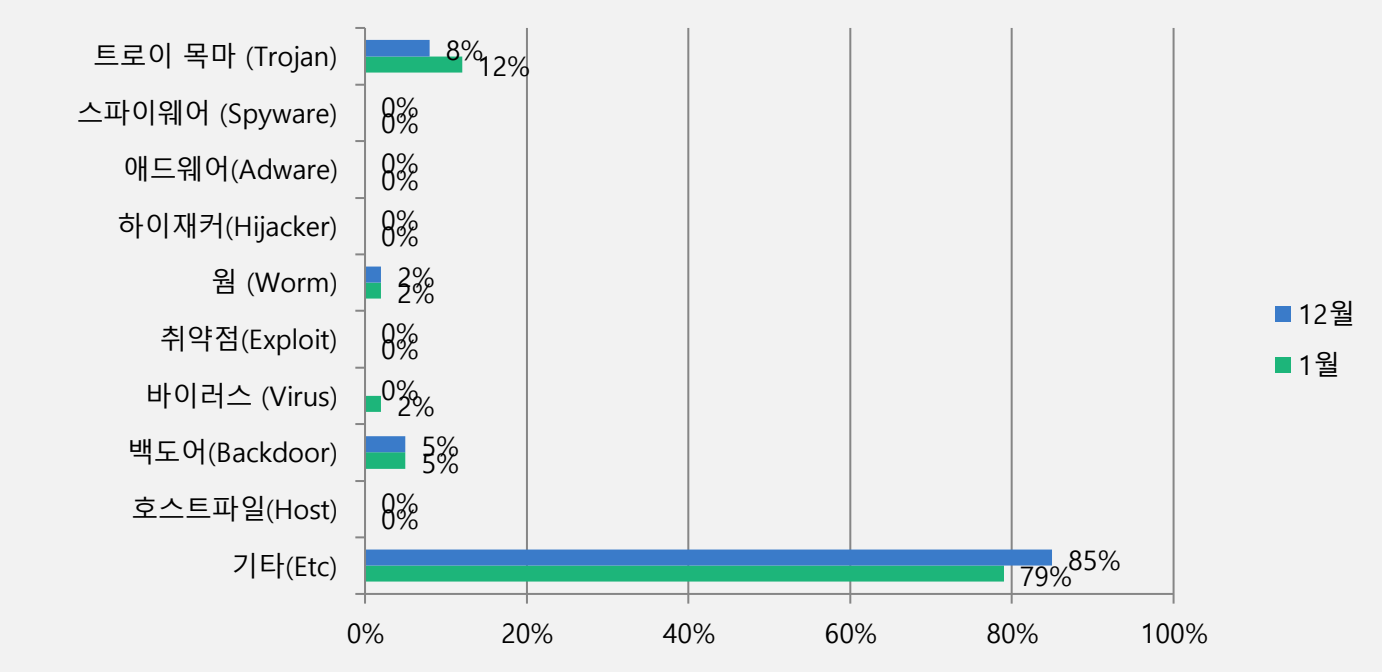
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 79%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 12%, 백도어(Backdoor) 유형이 5%, 웜(Worm) 유형이 2%, 바이러스(Virus) 유형이 2%로 확인되었습니다. 2025 년 1 월과 비교하여 전체 감염 건수는 7.8% 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

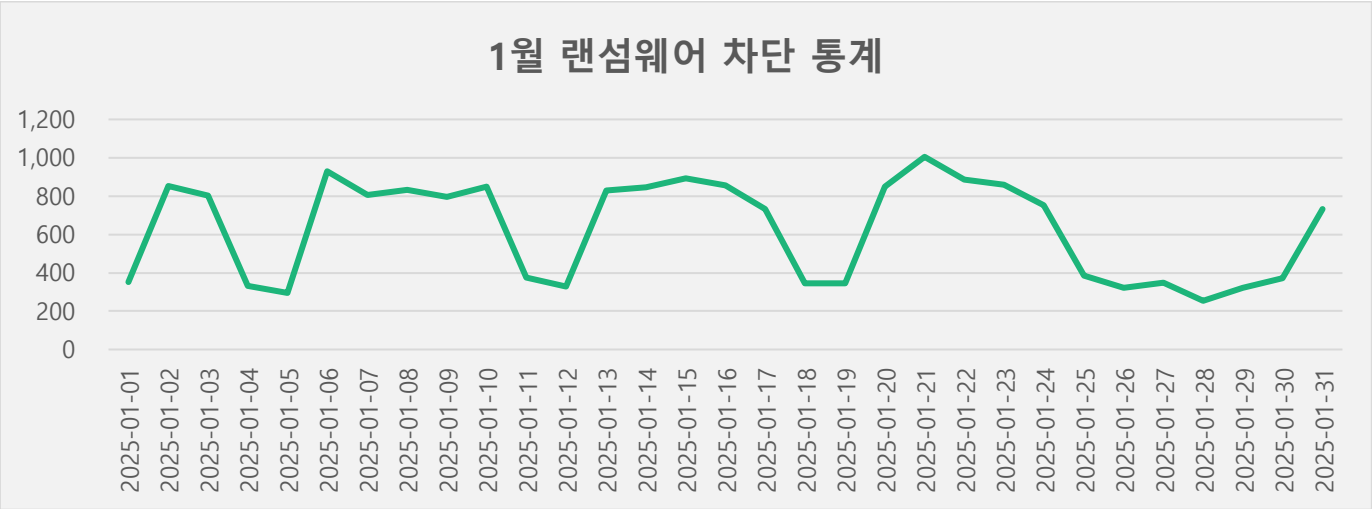
2025 년 1 월에는 24 년 12 월과 비교하여 트로이목마(Trojan) 유형이 4%, 바이러스(Virus) 유형이 2% 증가하였으며, 웜(Worm)유형과 백도어(Back door) 유형은 각각 2%와 5%로 동일하였습니다. 기타(ETC)유형은 6% 감소하였습니다.



3. 랜섬웨어 차단 통계

1 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 1 월 1 일부터 1 월 31 일까지 총 19,480 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 25 년 1 월 한 달간 총 13,788,126 건의 URL 이 확인되었습니다. 이 수치는 24 년 12 월 한 달간 확인되었던 7,621,037 건의 악성코드 경유지/유포지 URL 수에 비해 약 80.9% 가량 증가한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.

2

최신 보안 동향

계정정보 탈취를 시도하는 피싱 공격 진행 중! 북 배후 추정

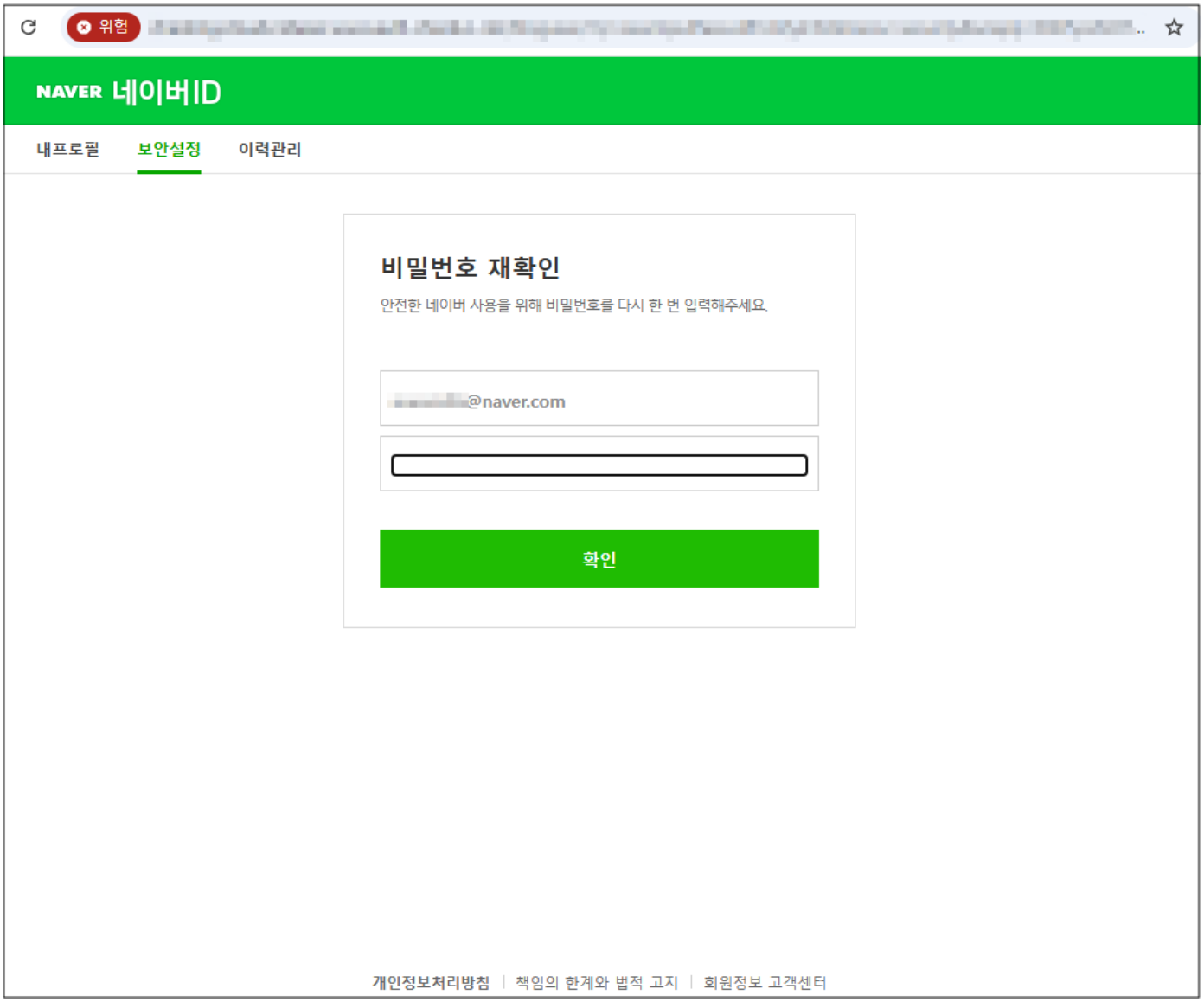
최근 전자문서 도착 알림, 회원정보 변경 알림, 약관 위반 알림 등 다양한 주제로 국내 포털사이트 고객센터를 사칭한 피싱 메일이 유포되고 있어 사용자들의 각별한 주의가 필요합니다.

[그림 1] 정상 메일을 위장한 피싱 메일

해당 피싱 메일은 '작성하신 게시물이 게시중단 처리되어 안내드립니다.' 라는 제목으로 유포되고 있으며, 실제 공식 사이트에서 게시 중단 요청을 접수 받아 진행하는 게시중단 처리 안내 메일과 매우 흡사하게 제작되었습니다.

[그림 2] 정상 메일 (좌) / 피싱 메일 (우)

이메일 내에는 피싱 페이지 주소가 링크된 [확인하러 가기] 버튼이 포함되어 있으며 사용자가 해당 버튼을 클릭하면 공격자가 제작해 둔 피싱 페이지로 접속됩니다.



[그림 3] 계정정보 입력 피싱 페이지

피싱 페이지는 실제 공식사이트 로그인 페이지와 매우 유사하게 제작되어있으며, 다만 사용자의 아이디 정보가 미리 입력되어 있습니다.

사용자가 피싱 페이지에 비밀번호를 입력하면 비밀번호 오류라는 문구와 함께 재 입력을 요구합니다. 하지만 입력된 사용자 정보는 백그라운드에서 공격자 서버로 전송되며 공격이 종료됩니다.

해당 피싱 메일은 공격자들이 대량으로 피싱 메일을 발송할 때 자주 사용하는 PHPMailer 를 통해 발송되었습니다.

```
Subject: =?UTF-8?B?7J6R7ISx7ZWY7IugIOqyjOyLnOusvOydtCDqsozsi5zspJHri6gg7LKY66as?=
 =?UTF-8?B?65CY7Ja0IOyViOuCtOuTnOumveuLiOuLpC4=?=
Message-ID: <[redacted]>
X-Mailer: PHPMailer 5.2.14 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="b1_cc58ab43f87eb1fd021eabdca8fa630f"
Authentication-Results: exim-smtp-6758d5575c-628dv; auth=pass smtp.auth=mailsender24@mail.ru
X-Mailru-Src: smtp
```

[그림 4] PHPMailer 정보

ESRC 는 최근 발견된 계정정보 탈취를 시도하는 피싱 페이지들에 대한 분석을 진행했으며 다음과 같은 공통점을 발견했습니다.

1) 피싱 페이지에서 사용된 주요 도메인 리스트

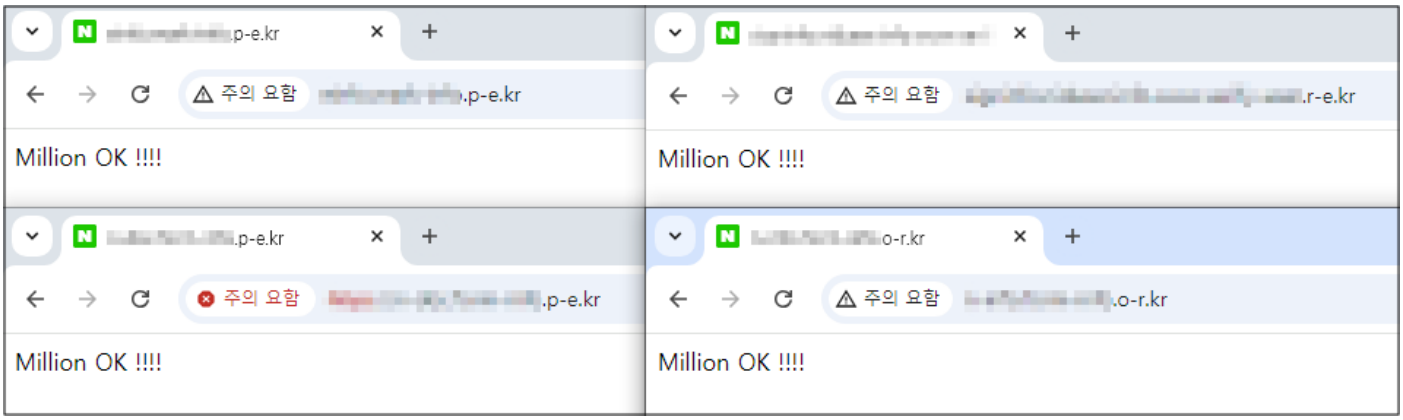
피싱 페이지들은 o-r.kr, r-e.kr, p-e.kr 도메인을 사용하였습니다.

o-r.kr, p-e.kr, n-e.kr, p-e.kr, r-e.kr, kro.kr 도메인들은 김수키 조직이 공격을 할 때 자주 사용하는 도메인으로 알려져 있으며, 지난 포스팅에서 해당 도메인이 사용된 사례를 확인할 수 있습니다.

▶ 북 김수키(Kimsuky) 조직의 정책 자문 위장 스피어 피싱 주의!

2) 네트워크 응답 메시지 문자열

피싱 페이지 도메인에 접속하면 “Million OK!!!!” 메시지를 볼 수 있습니다. Million OK 메시지는 김수키 조직이 사용하는 인프라로 알려져 있습니다.



[그림 5] Million OK!!!! 응답 메시지

3) 웹 서버 스택 정보

웹 서버 스택 정보가 모두 Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.6.15 로 동일합니다.

[그림 6] 웹 서버 스택 정보

4) URL 특징

피싱 URL 에서 특정 파라미터 및 경로를 사용하는 것을 발견했습니다.

hxxps://도메인주소/blog/?wreply=[네이버이메일계정] &m=hxxps://nid[.]naver.com/nidlogin.login?url=hxxp://mail[.]naver.com/	hxxp://도메인주소/bloguser/?wreply=[base64로 인코딩 한 이메일주소] &m=hxxps://nid[.]naver.com/nidlogin.login?url=hxxp://mail[.]naver.com/	hxxp://도메인주소/bloguser/?q=viewInputPasswdForMyInfo&menu=security&wreply=[base64로 인코딩한 이메일 주소] &m=hxxps://nid[.]naver.com/nidlogin.login?url=hxxp://mail[.]naver.com/

위와 같은 정보들을 바탕으로 최근 동일 조직의 의한 공격이 진행 중이며, 해당 공격조직은 북한 배후의 김수키(kimsuky)그룹으로 추정하고 있습니다.

사용자 분들께서는 이메일 수신 시 필히 발신자 주소와 접속한 페이지의 URL 을 확인하는 습관을 가지셔야 하며, 정상적인 메일의 경우 발신자 주소 앞에 공식 로고가 표시된다는 점을 반드시 기억하시기 바랍니다.

만약 이러한 형태의 피싱 메일을 통해 계정정보를 입력한 경우에는 즉시 계정 비밀번호를 변경하시고 2 단계 인증 및 타 지역 로그인 제한 등의 추가적인 보안조치 통해 계정도용 등으로 이어질 수 있는 2차 피해를 예방하시기 바랍니다.

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com