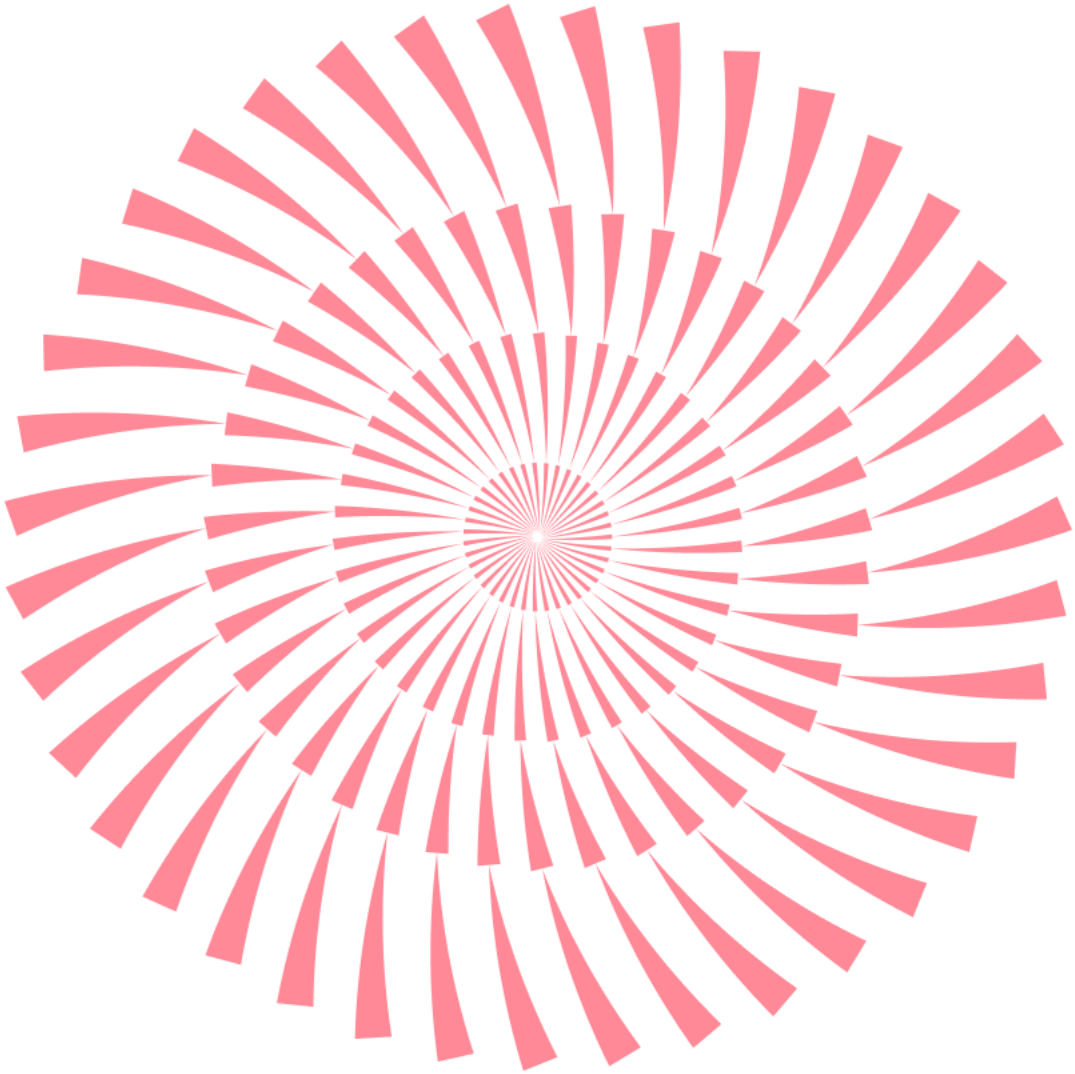
No.176 | 2024.5

ESRC 보안동향보고서

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



Copyright©2024 ESTsecurity Corp. All rights reserved.

EST SECURITY

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 08-12

금융위원회, N 관리자 등 정상 이메일을 위장하여 계정정보 탈취를 시도하는 피싱 캠페인 주의!

1

악성코드 통계 및 분석

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

 Copyright ⓒ 2024 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

올해 출시된 XZ Utils 버전 5.6.0 과 5.6.1 에 심각하게 영향을 미치는 소프트웨어 공급망 공격이 발생했습니다. 이번에 발견된 취약점은 CVE-2024-3094 로, 다양한 리눅스 배포판에서 중요한 패키지로 포함되어 있습니다. 이 공격은 CVSS(공통 취약성 점수 평가 시스템)의 최대 점수인 10.0 으로 측정되었습니다. 해당 취약점에 노출되었을 경우 심각한 위험을 초래하는 원격 액세스 무단 허용 백도어가 설치되고, 백도어가 동작하면 공격자는 SSH 인증 없이 서버에 접속이 가능하게 됩니다.

이는 오픈소스 프로젝트의 저장소에 접근한 진화된 방식의 공급망 공격입니다. 피해 규모에 있어 치명적인 위험성을 내포하고 있어 CISA, KISA 등 주요 보안기관에서는 피해 최소화를 위한 보안공지가 즉시 게시되었고, XZ Utils 관련 GitHub 저장소가 일시적으로 폐쇄되기도 하였습니다.

라자루스(Lazarus) 조직의 LinkedIn 을 통한 블록체인 및 코인 관련자 타깃 대규모 사회공학적 Node JS 공격이 이어지고 있습니다. 공격자는 합법적인 면접관으로 가장하여 소프트웨어 개발자와 같은 특정 전문그룹을 표적으로 삼는 사회공학적 공격 기법을 사용합니다. 이 방법은 신뢰, 두려움, 돕고자 하는 마음 등 사회적 특성을 악용하며, 합법적인 조직의 면접관으로 모방하여 개발자을 대상으로 가짜 면접을 설정하는 경우가 대표적입니다.

이 때 공격자는 메일, 채팅 어플 등을 통해 타깃과 충분히 인간적인 유대를 쌓은 후 공격을 진행하는 치밀함을 보입니다. 피해자와의 관계가 어느 정도 형성되었다고 판단되면 GitHub 와 같이 합법적인 오픈소스를 통해 채용에 필요한 테스트를 가장한 소프트웨어 다운로드 및 실행하는 작업을 요청을 하며, 이 소프트웨어에는 시스템을 손상시키는 악성 Node JS 페이로드가 포함되어 있습니다.

생성형 AI 인 OpenAI 의 ChatGPT, Google 의 Gemini 등을 활용하여 위협 행위그룹의 악성 PowerShell 스크립트 공격이 공개되었습니다. 이들은 2022 년 3 월에 독일의 수십 개 기관을 겨냥한 이메일 캠페인에서 이 악성 스크립트를 사용해 Rhadamanthys 인포스틸러를 유포하였고, 최근에는 Metro Cash & Carry 라는 독일 브랜드를 위장한 송장을 미끼로 독일의 여러 산업군을 타깃으로 한 이메일 캠페인이 이어지고 있습니다. 메일에 첨부된 압축파일 안에는 악성 바로가기(lnk)가 포함되어 있고, 이 파일을 실행하면 PowerShell 원격 스크립트가 Base64 로 인코딩된 Rhadamanthys 인포스틸러를 불러오게 됩니다.

여기서 주목할 점은, 이 PowerShell 스크립트 코드에는 사람이 생성한 코드에서는 드물게 나타나는 "#" 기호가 포함되어 있으며, 각 구성 요소에 대한 특정 주석이 있었습니다. 이러한 특징은 ChatGPT, Gemini 와 같은 생성형 AI 솔루션에서 짜여진 코드의 전형적인 특징입니다.

ESTSECURITY Copyright©2024 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.

2024 년 4 월에는 새롭게 탐지된 Gen:Variant.Cerbu.109340 이 1 위를 차지하였습니다. 그 밖에도 Trojan.GenericFCA.Agent.7232, Gen:Variant.Doina.18540, Heur.BZC.YAX.Linx.15.05E78B67, Trojan.Shadow Brokers.A, Gen:Variant.Razy.76762, Trojan.GenericKD.46718480 등 다수의 새로운 탐지명이 순위권에 자리하였습니다.

주목할만한 점으로는 바로가기(lnk)로 위장한 악성코드 Heur.BZC.YAX.Linx.15.05E78B67 의 등장과 OS/SW 불법 인증툴 관련 탐지 Gen:Variant.Doina.18540, Misc.HackTool.AutoKMS 가 강세를 보인 것을 꼽을 수 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Gen:Variant.Cerbu.109340	ETC	872,091
2	NEW	Trojan.GenericFCA.Agent.7232	Trojan	383,251
3	NEW	Gen:Variant.Doina.18540	ETC	277,067
4	NEW	Heur.BZC.YAX.Linx.15.05E78B67	ETC	270,994
5	NEW	Trojan.ShadowBrokers.A	Trojan	262,361
6	NEW	Gen:Variant.Razy.767621	ETC	237,924
7	NEW	Trojan.GenericKD.46718480	Trojan	236,355
8	↓3	Misc.HackTool.AutoKMS	ETC	220,386
9	NEW	Trojan.Agent.Injector.Gen	Trojan	200,805
10	NEW	Trojan.Agent.Zpevdo.A	Trojan	195,634
11	NEW	Backdoor.Generic.792814	Backdoor	187,153
12	NEW	Worm.ACAD.Bursted	Worm	182,494
13	↑1	Trojan.HTML.Ramnit.A	Trojan	163,756
14	NEW	Gen:Variant.Razy.864420	ETC	142,151
15	NEW	Dropped:Trojan.GenericKD.40639357	Trojan	19,295

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

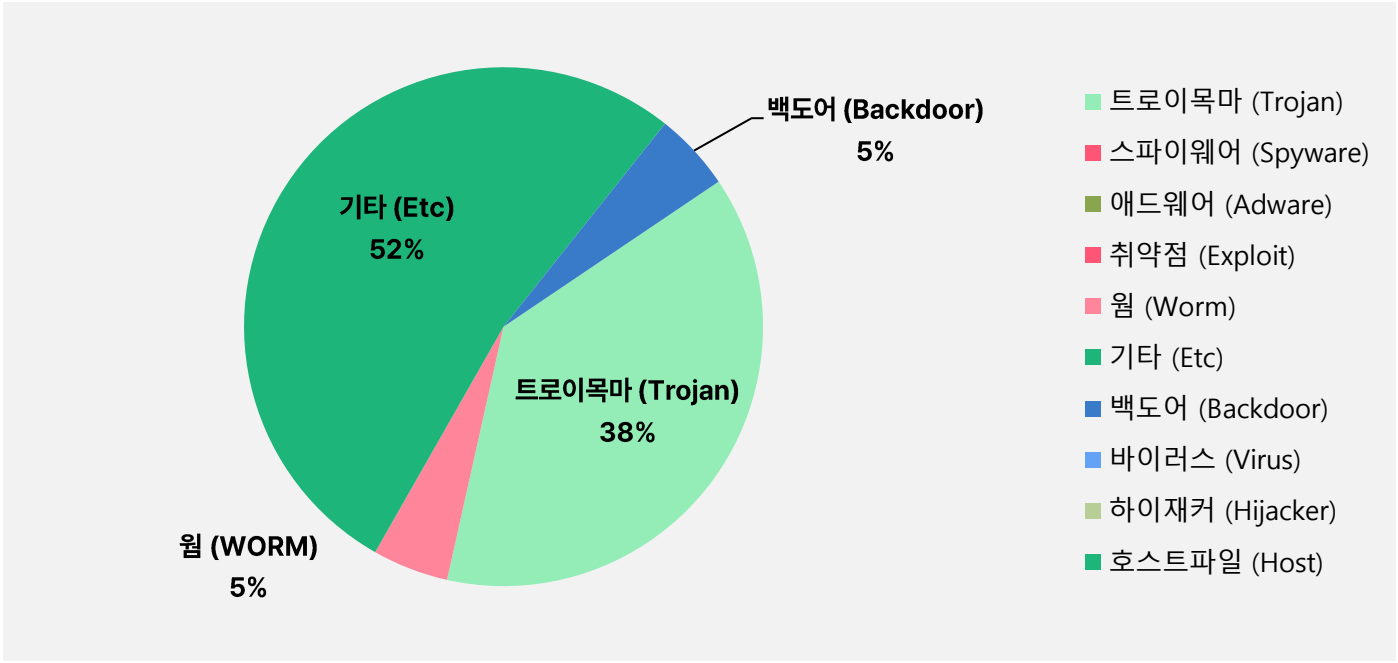
2024 년 4 월 1 일 ~ 2024 년 4 월 30 일

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

악성코드 유형별 비율

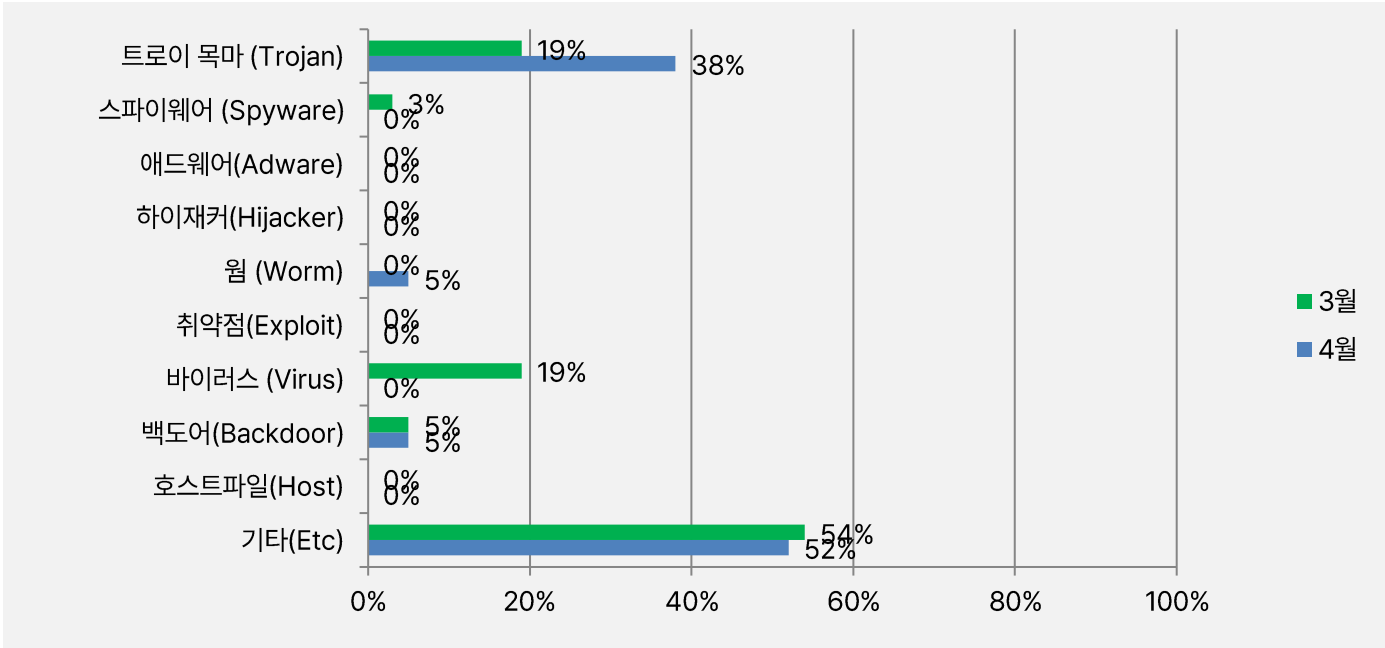
악성코드 유형별 비율에서 기타(ETC) 유형이 52%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 38%, 백도어(Backdoor), 웜 Worm) 유형이 각각 5%로 확인되었습니다.

2024 년 4 월과 비교하여 전체 감염 건수는 5.7 배 가량 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

2024 년 4 월에는 지난 3 월과 비교하여 트로이목마(Trojan) 유형이 19% 대폭 증가하였고, 기타(ETC) 유형이 2% 감소하였습니다. 또한, 웜 (Worm) 유형이 5%로 새로 등장하였고, 백도어(Backdoor) 유형은 지난 달과 동일한 5%를 차지하였습니다.

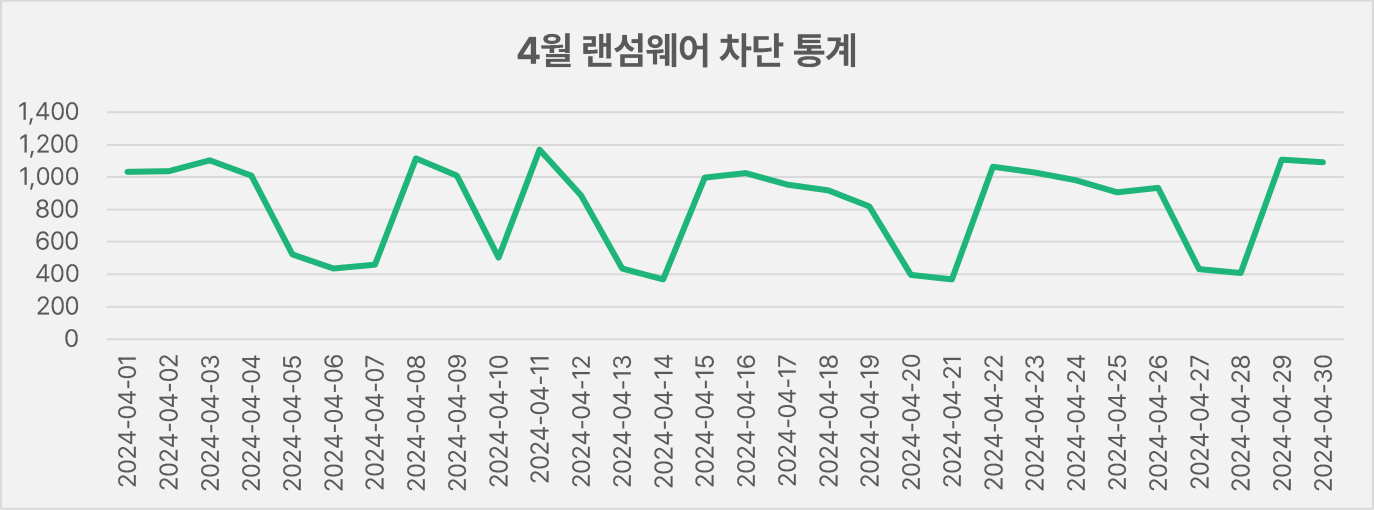


 Copyright©2024 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

4 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. 4 월 1 일부터 4 월 30 일까지 24,522 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 4 월 한 달간 총 7,893,329 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 3 월 한 달간 확인되었던 8,022,475 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.2.% 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.

금융위원회, N 관리자 등 정상 이메일을 위장하여 계정정보 탈취를 시도하는 피싱 캠페인 주의!

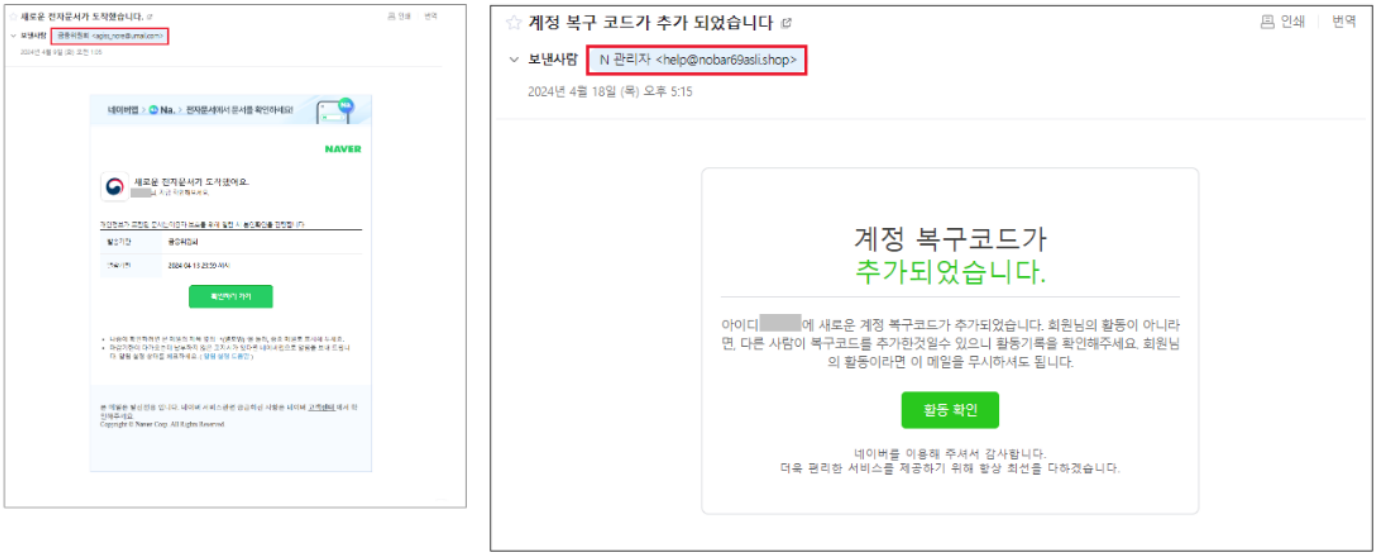
최근 정상 이메일을 위장하여 사용자 계정정보 탈취를 시도하는 피싱 메일이 증가함에 따라 사용자들의 각별한 주의가 필요합니다.

피싱 메일들은 '새로운 전자문서가 도착했습니다.', '계정 복구 코드가 추가되었습니다.', '새로운 통지서 안내문이 도착했어요.'와 같은 사용자를 현혹할 만한 제목으로 유포됩니다.



[그림 1] 정상 이메일을 위장한 피싱메일들

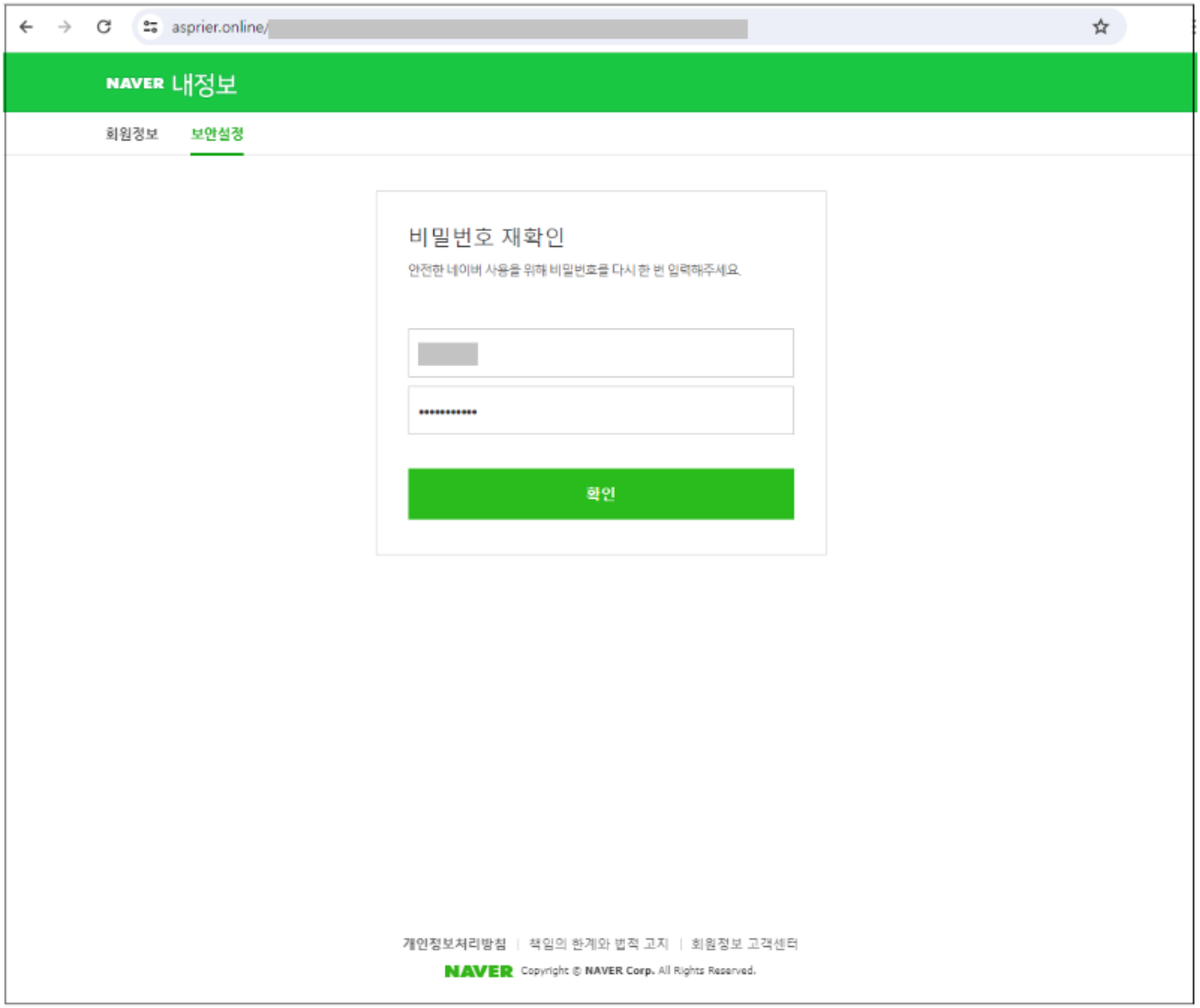
해당 메일들을 정상 메일과 매우 유사하게 제작되어 있어 주의 깊게 보지 않으면 정상 메일로 오인할 가능성이 높습니다.



[그림 2] 정상 메일을 위장한 피싱 메일

 Copyright©2024 ESTsecurity Corp. All rights reserved.

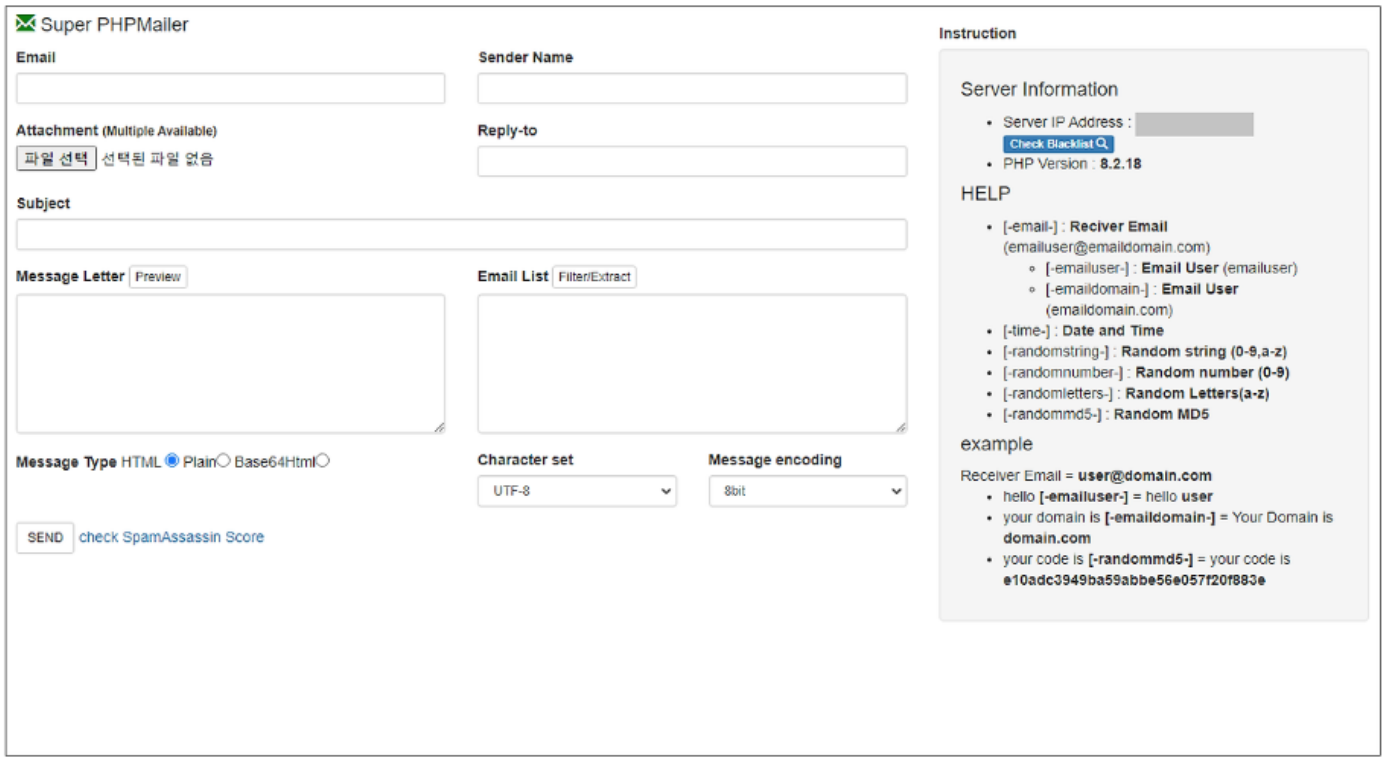
해당 메일들은 본문 내 링크가 연결된 버튼이 포함되어 있으며, 해당 버튼 클릭 시 피싱 페이지로 이동되며 계정정보 입력을 유도합니다.



[그림 3] 계정정보 입력을 유도하는 피싱 페이지

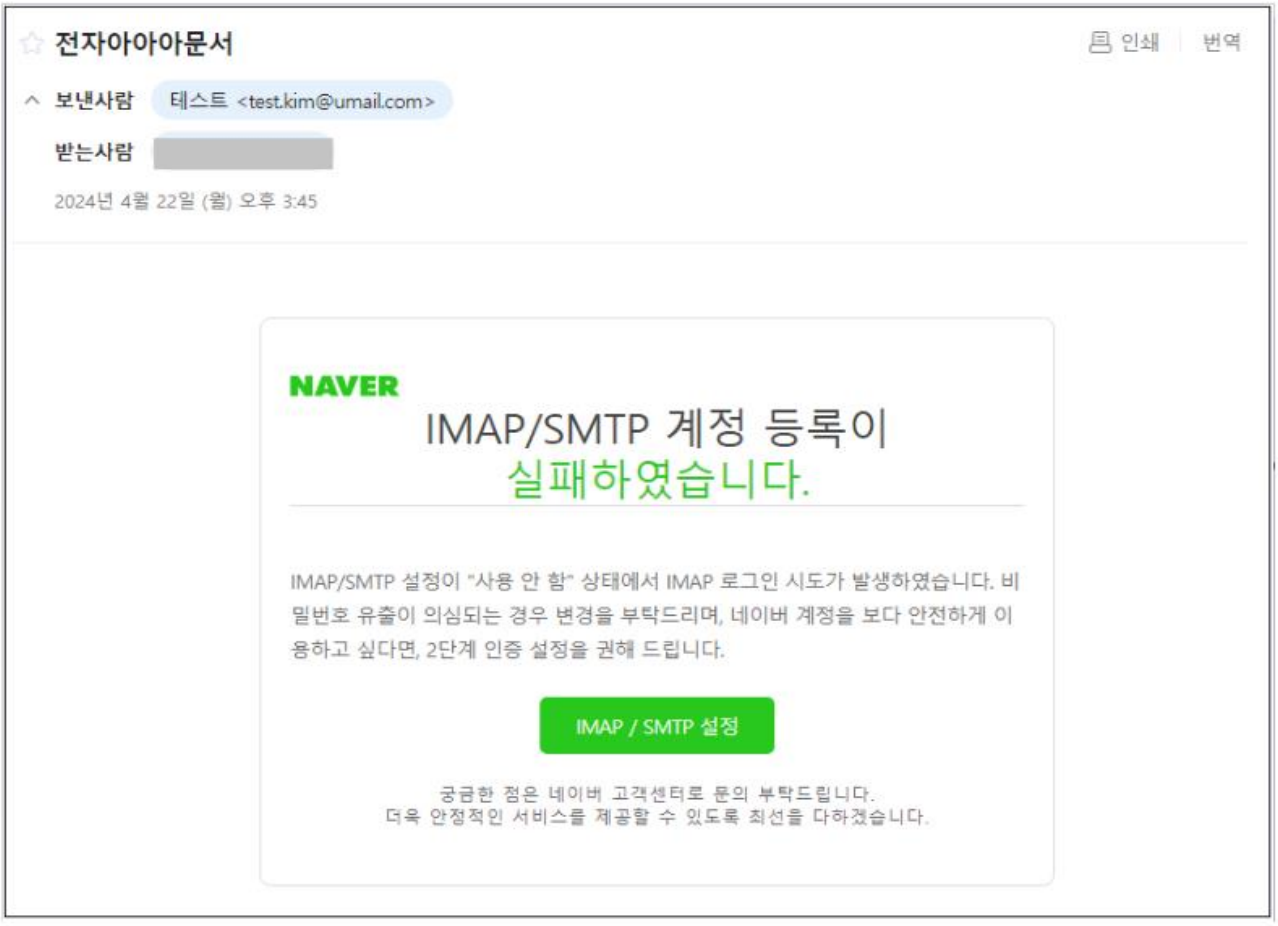
사용자가 계정정보를 입력하면 입력한 계정 정보는 공격자 서버로 전송되며 공격이 종료됩니다. ESRC 는 피싱 메일들에 대해 분석을 진행하였고, 공격자가 PHPMailer 를 이용하여 대량으로 피싱 메일을 발송하고 있는 것을 확인하였습니다.

 Copyright ⓒ 2024 ESTsecurity Corp. All rights reserved.



[그림 4] 해킹된 페이지 내 업로드 되어있는 PHPMailer

실제 공격자의 PHPMailer를 사용하여 테스트 메일을 발송해 본 결과 정상적으로 수신되는 것이 확인되었습니다.



[그림 5] PHPMailer를 활용해 보내본 테스트 메일

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

발신일	발신자	X-PHP-Script	피싱페이지 도메인 / IP
4월 22일	서비스 메일 <help@18wenxue.top>	da******ke.com/wp-send.php	mopkxsb.shop 79.133.51.174
4월 18일	N 관리자 <help@nobar69asli.shop>	ne ***** et.com/wp-send.php	vocmo.shop 79.133.51.174
4월 11일	N 메일 <help@dogcages.pet>	co *********ee.com/wp-send.php	nobol.store 79.133.51.174
4월 9일	금융위원회 <agiss_nore@umail.com>	na*******eb.com/wp-main.php	artiech.online 27.255.75.159
3월 18일	국민연금 <nopskr.adirect.noreply@dshinhan.com>	m*******eal.com/wp-main.php	corumbknets09io.site 45.64.153.42
1월 31일	고 객 센 터 <noreply@stpe.co>	la*******t.com/wp-send.php	mollsovop.fun 79.133.51.174
1월 29일	알 림 <aecoply@fiservforum.online>	y*******es.space/wp-send.php	mollsovop.fun 79.133.51.174
1월 12일	인증기한임박 <no-replys.yoeongumnet@inaver.com>	hap*********s.com/main.php	nuserguards.website 8.218.16.183
1월 12일	국민연금 <kees.yeongumkr@umail.com>	ny *******nd.tech/wp-main.php	nuserguards.website 8.218.16.183

[표1] 현재까지 수집한 피싱 메일

현재까지 ESRC 에서 수집한 정보들을 토대로 확인해보면, PHPMailer 가 모두 워드프레스 홈페이지에 업로드 되어 있어 공격자들은 워드프레스 취약점을 이용하고 있는 것으로 추정되며, 다수의 정보에서 유사성이 확인되어 현재 유포 중인 스팸메일들은 동일한 공격자 혹은 공격 집단의 소행으로 추정하고 있습니다.

이러한 피싱 공격은 수 년 전부터 지속되던 고전적인 공격 방식이지만 여전히 많은 사용자들이 피해를 당하고 있습니다.

사용자 여러분들께서는 수상한 이메일 수신 시 반드시 이메일 앞 공식 로고와 발신자 주소를 확인하시고, 네이버로 수신되는 전자문서의 경우 웹이 아닌 네이버 앱에서만 확인이 가능하다는 점 반드시 기억하시기 바랍니다.



[그림 6] 웹에서 네이버 전자문서 열람 시 보이는 알림창

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com