

# SECURITY DAILY REPORT

MSS(Managed Security Service)



24x365



Security



AI analytics

## 1. 보안동향

### 붕어낚시 씨 생산 및 쇼핑몰 '군계일학', 해킹으로 개인정보 유출

#### [미리보기]

1999년 붕어낚시 씨 전문업체로 창업...올바른 낚시이론 정립에 힘써이달 17일 발생...이름, 아이디, 패스워드, 전화번호, 생년월일, 이메일 등 6개 항목 유출[보안뉴스 김영명 기자] 붕어낚시 씨 전문업체로 씨 맞춤법, 채비법 등 올바른 낚시이론을 정립하는데 앞장서 온 씨 전문 제조기업이자 관련 쇼핑몰을 운영하는 '군계일학'이 해킹으로 개인정보가 유출

[바로가기](#)

### 깃허브를 공격에 사용한 새로운 해킹 전략 드러나

#### [미리보기]

요약 : 보안 외신 해커뉴스에 의하면 깃허브(GitHub)라는 공공 코드 리포지토리를 공격에 악용하는 해커들이 빠르게 증가하는 중이라고 한다. 비밀 기스트(gist)와 깃 커밋(git commit) 메시지를 공격에 활용하는 방법이 주로 인기를 끌고 있는 것으로 분석됐다. 이렇게 했을 때 탐지 기술을 회피하는 게 더 쉬워진다. 비슷한 이유로 드롭박스나 구글

[바로가기](#)

## 연말 연시 노렸나...호텔 노리는 사이버 공격 급증하고 있어

### [미리보기]

요약: 보안 외신 해리드에 의하면 최근 호텔과 숙박 업체들을 겨냥한 사이버 공격이 크게 증가하고 있다고 한다. 연말 연시에 여행 다니는 사람들을 노리는 건데, 최근 증가하는 캠페인의 특징 중 하나는 비다(Vidar)라는 정보 탈취형 멀웨어를 피해자 시스템에 심는 것이다. 호텔 정보는 물론 투숙객의 정보까지도 노리는 것으로 보인다. 아직까지 피해 규모는 파

[바로가기](#)

## 올해 3 월부터 시작된 멀웨어 캠페인, 이제야 들킬 정도로 은밀해

### [미리보기]

요약: 보안 외신 블리핑컴퓨터에 의하면 2023 년 3 월부터 시작된 멀웨어 캠페인이 현재까지 진행되고 있으며 북미, 남미, 유럽, 일본에서 40 개 은행, 5 만 명 사용자가 피해를 입었다고 한다. 이 캠페인의 궁극적 목적은 자바스크립트로 만들어진 웹 인젝션을 사용해 은행 및 금융 정보를 훔치는 것이다. 공격자들은 이미 2022 년 12 월부터 공격에 활용될 도메

[바로가기](#)

## 록빗 3.0, 이탈리아 유명 클라우드 업체 공격해 사회적 혼란 야기

### [미리보기]

요약: 보안 블로그 시큐리티어페어즈에 의하면 록빗 3.0(LockBit 3.0)이라는 악명 높은 랜섬웨어 조직이 이탈리아의 클라우드 업체인 웨스트폴(Westpole)을 공략하는 데 성공했다고 한다. 이 때문에 웨스트폴의 고객사 여러 곳이 마비되거나 정상 운영이 제대로 되지 않고 있다. 여기에는 여러 정부 기관들도 포함되어 있어 행정 업무에 차질이 빚어지고

[바로가기](#)

## 2. 보안권고문

금일 최신 패치 및 업데이트는 없습니다.



주소 | 서울특별시 서초구 서초대로 255 고덕빌딩 2 층(06595)

전화 | 02-2105-4400 (영업문의-1 번, 보안관제문의-2 번, 기술문의-3 번)

팩스 | 02-2105-4456

영업문의 | [sales@eosec.co.kr](mailto:sales@eosec.co.kr) 보안관제 및 기술 문의 | [tech@eosec.co.kr](mailto:tech@eosec.co.kr)

©EYEON SECURITY All Right Reserved.