1. 보안동향

가정용 라우터 노리던 중국 APT 볼트타이푼, FBI 의 원격 킬 스위치로 무력화 돼

[미리보기]

중국의 APT 인 볼트타이푼이 한 방 먹었다. 미국 수사 기관이 원격에서 킬 스위치를 전송해 볼트타이푼이 운영하던 공격 인프라를 무력화시킨 것이다. 영구적인 조치가 되지는 못하지만, 적잖은 피해를 입힌 것으로 보인다.[보안뉴스 문정후 기자] 미국 사법부가 악명 높은 중국의 사이버 공격 단체인 볼트타이푼(Volt Typhoon)의 공격 인프라를 와해시켰다고 발

바로가기

구글 플레이에 악성 앱 업로드 한 후 피해자들에게 로맨틱하게 다가간 패치워크

[미리보기]

견원지간인 인도와 파키스탄 간에 또 다른 공격 정황이 발견됐다. 이번에는 인도의 해커들이 파키스탄의 개인과 조직들을 노리고 있었다. 주로 로맨스 스캠 전략으로 접근한 인도 해커들은 구글 플레이마저 농락했다.[보안뉴스 문가용 기자] 인도의 APT 단체인 패치워크(Patchwork)가 구글 플레이라는 공식 애플리케이션 스토어를 통해 여섯 가지 악성 앱을 유포하

바로가기

맥 OS 생태계에서 광범위하게 진행되는 공격 캠페인, 목적은 오리무중

[미리보기]

액티베이터라는 캠페인이 맥 OS 환경에서 공격적으로 진행되고 있다. 크랙된 소프트웨어를 통해 퍼지고 있는데, 지금은 잠깐 휴식을 취하는 것으로 보인다.[보안뉴스 문가용 기자] 최근 맥 OS 사용자들을 겨냥하여 백도어를 유포하고 있는 악성 캠페인이 발견돼 경고가 나왔다. 공격자들은 소프트웨어 제품이라고 속이며 백도어를 퍼트리고 있는 것으로 파악됐다. 다른 OS

바로가기

'웨비나' 행사 안내장 사칭 APT 공격 포착... ROKRAT 변종형 악성 파일

[미리보기]

전형적인 스피어 피싱 공격 기법 사용...시즌 상관없이 진행되는 일상 위협 캠페인바로가기(LNK) '파일 압축형 공격', 'LNK', 'CHM' 등 파일 확장자 및 '화살표' 포함 여부 확인[보안뉴스 이소미 기자] '2023 년 북한 정세 평가 및 2024 년 전망' 행사 안내장을 사칭해 문서처럼 속여 해킹 공격을 수행한 징후가 포착됐다. 공격자들은 성공률을

바로가기

에스넷 랜섬웨어, '.SNet' 확장자로 모든 파일 암호화하며 공격

[미리보기]

랜섬웨어 실행 파일 작업 스케줄러 및 시작 프로그램 조건에 등록돼...자동 재실행 가능에브리존 안티랜섬웨어 화이트디펜더, 에스넷 랜섬웨어 분석 노트 공개[보안뉴스 김영명 기자] 에스넷 랜섬웨어(SNet Ransomware)는 C++ 언어를 기반으로 제작됐으며, 해당 랜섬웨어에 감염된 파일은 '파일명.확장자.SNet' 포맷으로 모든 파일을 변경하고 있는 모습

바로가기

---

2. 보안권고문

Mastodon 플랫폼 보안 업데이트 권고

[미리보기]

Mastodon 플랫폼 보안 업데이트 권고 2024.02.05 ㅁ 개요 o 오픈소스 Mastodon 에서 발생하는 보안 취약점 해결을 위한 업데이트 공개 [1] o 영향받는 플랫폼을..

바로가기

---

glibc 보안 업데이트 권고

[미리보기]

glibc 보안 업데이트 권고 2024.02.05 ㅁ 개요 o 리눅스 GNU C Library 에서 발생하는 취약점에 대한 업데이트 정보 공개 [1] [2] o 영향받는 버전을 사용..

바로가기

Eyeon Security
information security company

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 보안관제 및 기술 문의 | tech@eosec.co.kr