Criminal IP

2024 사이버 보안 인식의 달:

주요 보안 이슈 타임라인

*하단의 제목을 클릭하면 해당하는 블로그 글로 이동합니다.

1

2024년 1월

#선박해킹 #소프트웨어공급망

- 선박 해킹 주의: 공격 표면에 노출된 1,600개 이상의 선박 장치 발견
- 개발자 및 소프트웨어 기업을 위한 2024 소프트웨어 공급망 보안 가이드라인

2

2024년 2월

#MS익스체인지 #제로데이

- MS 익스체인지 서버 제로데이, 16만 대 이상 공격에 노출(CVE-2024-21410)

3

2024년 3월

#포티넷 #RCE #스크린커넥트

- 포티넷 RCE 버그에 취약한 장치 1천 대 이상 발견(CVE-2024-21762)
- CVSS 10점짜리 스크린커넥트 취약점에 노출된 서버 탐지(CVE-2024-1709)

4

2024년 4월

#텔레스퀘어 #팔로알토_네트웍스 #신용카드 #메시에이전트 #C2

- HTTP 서버 응답 콘텐츠 길이로 취약한 텔레스퀘어 장비 탐지하기
- 팔로알토 네트웍스 OS 명령 주입 취약점 CVE-2024-3400에 취약한 장비 탐지하기
- 국내 신용카드 부정 사용 사례로 본 간과된 기본 사기 대응 전략
- 메시에이전트 C2 탐지: 잠재적 악성코드 공격을 예방하는 방법

5

2024년 5월

#Veeam #이상금융거래탐지 #미연방준비제도 #사기분류모델 #USPS

- CVE-2024-29212: RCE 취약점 영향을 받는 노출된 Veeam Service Provider Console
- 2024년 금융감독원 이상금융거래탐지시스템 가이드라인에 따른 기업 및 기관 권고사항
- 미국 연방준비제도 사기 분류 모델에 따른 사기 탐지 방법
- 링크 스캐너로 USPS 피싱 사이트와 스미싱 사기를 식별하는 방법

6

2024년 6월

#자동차_번호판 #인식시스템 #OTT #개인정보유출 #신용카드정보

- 외부에 노출된 자동차 번호판 인식 시스템, 개인정보 유출 주의
- 중국 불법 OTT 서비스에서 유출된 개인정보, 신용카드 정보와 주소까지 노출

7

2024년 7월

#regreSSHion # OpenSSH #Polyfill #KYC인증 #NuGet #Brickstream

- regreSSHion(CVE-2024-6387): 치명적 RCE 취약점에 노출된 978만 OpenSSH, "긴급 조치 필요"
- Polyfill 공급망 공격: 10만 개 이상 도메인에 악성코드 주입
- KYC 인증 시스템에서 신분증과 개인정보 노출되고 있어
- NuGet 악성 패키지와 npm 악성코드 사례로 보는 오픈소스 공급망 공격
- '인증 없는' Brickstream 피플카운팅 시스템, 촬영·설정 페이지 무방비 노출

8

2024년 8월

#파리올림픽 #트렐로 #Bing #홈트레이딩시스템 #Quasar_RAT #Jenkins

- 파리 올림픽 티켓 판매 사칭 '피싱' 기승... AI 피싱 탐지 URL 스캐너로 예방하는 방법
- 트렐로 개인정보 유출: API 취약점으로 공격에 노출된 협업 툴
- 홈 트레이딩 시스템 악용 Quasar RAT 공격, 위협 헌팅 도구로 C2 IP 주소 분석한 결과
- Bing 검색엔진 악용한 다단계 악성코드 공격, 위협 헌팅 도구로 공격 IP 주소와 도메인 분석
- CVE-2024-43044: Jenkins의 심각한 RCE 취약점, 8만 개 노출된 장치 발견

9

2024년 9월

#NXDomain_Hunter #서브도메인 #내부관리시스템 #방화벽_자동화 #크립토재킹

- NXDomain Hunter 서브 도메인 스캔 공격으로 보는 공격 표면 관리의 중요성
- OSINT 위협 인텔리전스를 활용한 내부 관리 시스템 노출 예방법
- Criminal IP 'C2 서버 위협 피드'로 방화벽 정책의 악성 IP 자동 차단 방법
- 금융 망분리 규제 완화로 높아진 공격 표면 관리 중요성
- CVE-2023-22527 악용 크립토재킹 공격, 100만 개 이상 컨플루언스 서버 위협
- 국내 언론사 공격 표면 관리 분석 보고서, "4곳 중 1곳 CVE 취약점 보유"

10

2024년 10월

#멀버타이징 #ClickFix #CCTV #어웨이큰리코 #메시에이전트

- 멀버타이징 이란? "슬랙 광고 클릭하면 악성코드 다운로드" 공격 사례 분석
- ClickFix: 가짜 오류 메세지와 복사 붙여넣기를 활용한 새로운 위협 주의
- 러시아 공격 해킹그룹 '어웨이큰리코'가 활용한 메시에이전트, 감염 서버 위협 헌팅
- CCTV 서버 보안: 위협 인텔리전스로 CCTV 노출 위협 차단

이 리포트는 사이버위협인텔리전스 검색엔진 *Criminal IP*의 데이터를 바탕으로 작성되었습니다.
지금 바로 *Criminal IP* 무료 계정을 생성하면 리포트에 인용된 검색 결과를 직접 확인하거나,
더 방대한 위협 인텔리전스를 자유롭게 검색할 수 있습니다.