1. 보안동향

모든 파일을 '.sola' 확장자로 암호화하는 '솔라' 랜섬웨어 주의보

[미리보기]

SHGetKnownFolderPath 라는 API 이용해 다른 프로필 공개 경로도 공격, 암호화 진행에브리존 화이트디펜더, 솔라 랜섬웨어 침해사고 분석 및 발표[보안뉴스 김영명 기자] 감염된 컴퓨터의 모든 파일을 '.sola' 확장자로 암호화하는 형태로 추정되는 솔라(sola) 랜섬웨어가 최근 발견돼 사용자들의 주의가 필요하다. 이번에 발견된 솔라 랜섬웨어는

바로가기

올해 3 분기, 러시아·북한·중국·이란 등 주요국 해커그룹은 어떤 위협을 가했나

[미리보기]

러시아, UAC-0198 및 코지베어 랜섬웨어 공격...우크라이나 주기관 내 100 대 이상 기기 공격국내 사이버안보 정보공동체, 북한 해커그룹의 건설·기계분야 공격 담긴 보안권고문 발표잉카인터넷, 2024 년 3 분기 국가별 해커그룹 동향 보고서 발표[보안뉴스 김영명 기자] 2024 년 3 분기에도 다양한 국가의 해킹그룹이 사이버 공격을 펼친것으로 확인됐다. 잉카

바로가기

중국의 APT 조직, 돈 노리고 도박 업체들 공격하고 있어

[미리보기]

요약 : 보안 외신 해커뉴스에 의하면 중국의 APT 조직들이 도박 산업을 집중적으로 공략하고 있다고 한다. 특히 APT41 이라는 조직이 이런 움직임을 활발하게 보이는 중이라고 하는데, 그 이유는 돈을 벌기 위해서다. 보안 업체 시큐리티조스(Security Joes)에 의하면 이러한 캠페인은 최근 6 개월 동안 진행됐는데 도박 업체들로부터 고객들의 개인정보는

바로가기

보안 업체 소포스, XDR 플랫폼 내세우는 시큐어웍스를 8.5 억 달러에 인수

[미리보기]

요약 : 보안 외신 시큐리티위크에 의하면 보안 업체 소포스(Sophos)가 또 다른 보안 업체 시큐어웍스(SecureWorks)를 8 억 5900 만 달러에 인수하기로 결정했다고 한다. 이 가격 모두 현금으로 지불된다. 즉, 주식과 같은 형태로 거래가 완료되지 않는다는 것이다. 시큐어웍스가 자랑하는 태지스(Taegis) XDR 플랫폼과 소포스의 탐지 및 대응

바로가기

---

10 월에만 두 차례 해킹으로 사용자 정보 유출시킨 인터넷아카이브

[미리보기]

요약 : 보안 외신 핵리드에 의하면 인터넷아카이브(Internet Archive)가 한 달 새 두 번의 해킹 사고를 당했다고 한다. 이 사건으로 젠디스크 토큰과 관련된 정보들이 새나간 것으로 분석됐다. 사건 발생일은 10 월 20 일이다. 공격자들이 젠디스크 토큰과 관련된 정보를 입수했다는 것은 기술 지원 관련 기록들에 접근할 수 있다는 뜻이 되는데, 이 때문

바로가기

---

2. 보안권고문

Cisco 제품 보안 업데이트 권고

[미리보기]

Cisco 제품 보안 업데이트 권고 2024.10.22 ㅁ 개요 o Cisco 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1][3] o 영향받는 버전을 사용 중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o Cisco 의 Cisco Nexus Dashboard Fabric Controller(NDFC)에서 발생하는 임의 명령 실행 취약점(CVE-2024-20432) [1][2] o Cisco 의 Cisco Nexus Dashboard Fabric

바로가기

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-10-21)

[미리보기]

2024-11-11 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. ScienceLogic SL1 (formerly EM7) is affected by an unspecified vulnerability involving an unspecified third-party component. 2024-10-21 ScienceLogic SL1 Unspecified Vulnerability ScienceLogic CVE-2024-9537

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