도대체
제로데이(Zero Day)
취약점이 뭐야?

과학기술정보통신부

KISA 한국인터넷진흥원

제로데이 공격(ZERO DAY ATTACK)이란?

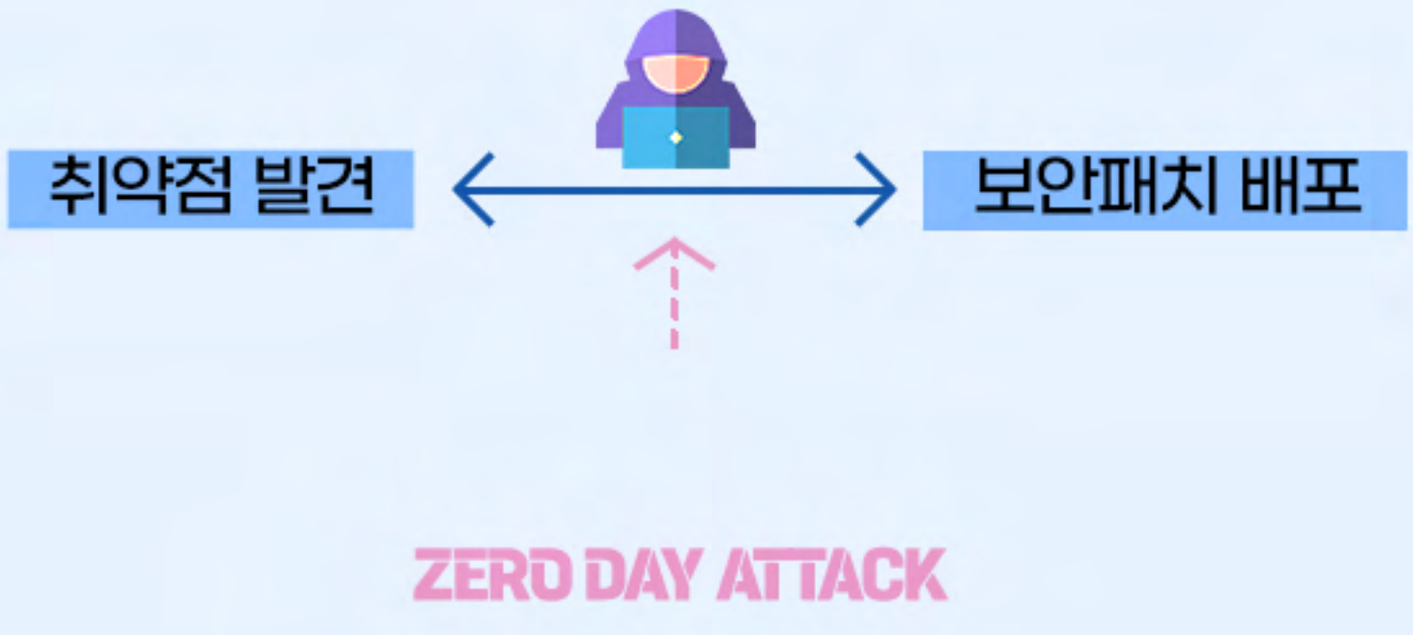
최근 사용자가 많고, 파급력이 큰 분야에서 취약점이 많이 발생하고 있습니다.
특히, 제로데이 취약점을 악용한 공격은 피해가 더욱 크게 발생하고 있는데요

그렇다면 제로데이 공격이 뭔지 함께 살펴볼까요?

⚠ **제로데이(Zero-day)란?** 해당 취약점이 공표 혹은 발견된 날

⚠ **제로데이 취약점이란?** 취약점이 발견되고 보안패치가 배포 전까지의 취약점

⚠ **제로데이 공격이란?** 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격



최근 발견되는 제로데이 취약점

사례1

CVE-2022-41040, CVE-2022-41082

Microsoft

MS社는 Microsoft Exchange Server 2013, Exchange Server 2016 및
Exchange Server 2019에 영향을 미치는 2개의 제로데이 취약점 발견('22.10)

⚠ 설명

- Microsoft Exchange Server에서 발생하는
  SSRF(Server-Side Request Forgery) 취약점(CVE-2022-41040)
- Microsoft Exchange Server에서 발생하는
  원격 코드 실행 취약점(CVE-2022-41082)

⚠ 영향을 받는 제품

- Microsoft Exchange Server 2013, 2016 및 2019

⚠ 해결 방안

* On-premise 환경 사용자의 경우 조치가 필요하며,
  Microsoft Exchange Online 사용자는 별도 조치 불필요

- Microsoft Exchange Server 2016 및 2019에서
  Exchange Emergency Mitigation Service(EEMS)가 활성화된 사용자는
  취약점 완화 정책이 자동으로 적용

- MS에서 배포한 취약점 완화 스크립트(EOMTv2) 다운로드 및 실행

최근 발견되는 제로데이 취약점

사례2

CVE-2022-32917

Apple社는 자사제품에서 발생하는 제로데이 취약점(CVE-2022-32917)을 해결한 보안 업데이트 발표('22.09)

⚠ 설명

- 특수하게 조작된 응용프로그램을 이용하여 커널 권한으로 임의코드 실행이 가능한 취약점(CVE-2022- 32917)

⚠ 영향을 받는 제품

- iPhone 6s 이상 및 iPad Pro(모든모델), iPad Air 2 이상, iPad 5세대 이상, iPad mini 4 이상, iPod touch(7세대 및 macOS Big Sur 11.7 및 macOS Monterey 12.6을 실행하는 Mac)

⚠ 해결 방안

- macOS Monterey 12.6, iOS 15.7 및 iPadOS 15.7, macOS Big Sur 11.7 로 업데이트

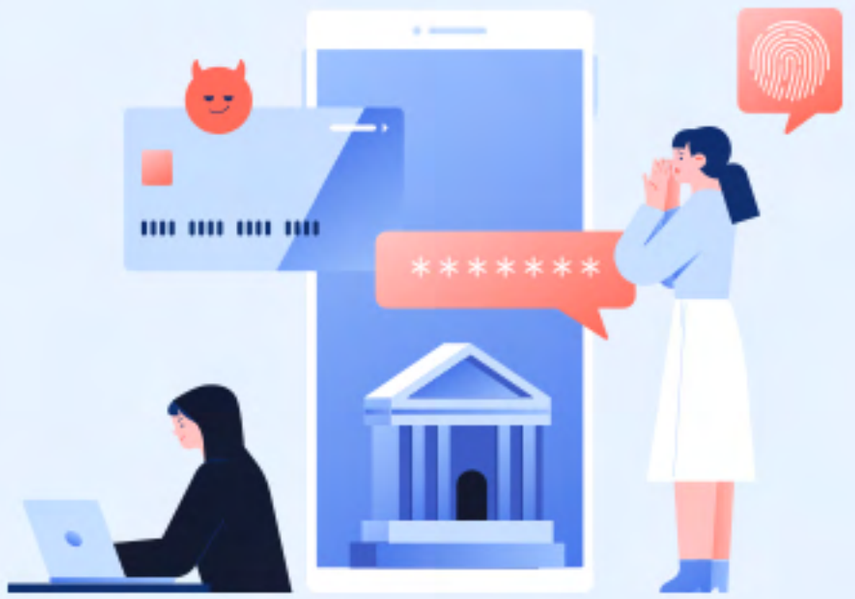
제로데이 공격를 악용한 사이버 공격은 어떤 것들이 있을까?

랜섬웨어 (ransomware)

'몸값'(Ransom)과 '소프트웨어'(Software)의 합성어로 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성 프로그램

피싱 (phishing)

개인정보(Private Data)와 낚시(Fishing)의 합성어로 해커들이 만든 용어로, 사회공학적 방법 및 기술적 은닉기법을 이용해서 민감한 개인 정보, 금융계정 정보를 절도하는 신종 금융사기 수법



제로데이 공격를 악용한 사이버 공격은 어떤 것들이 있을까?

DDoS (분산서비스 거부공격, Distributed DoS attack)

서비스가 불가능하게 하려는 목적으로 공격자는
특정 서버를 대상으로 지속적인 트래픽을
유발함으로써 서버가 감당할 수 없을 만큼의
리소스를 발생시켜 서버를 마비시킴

Cloud-Native Breach

공격자가 IoT클라우드 환경에 침투하여
클라우드로 전송되는 데이터를
훔치는 경우로, 클라우드 배포 내의
취약점을 악용하여 전송 및 저장 단계에서
데이터를 하이재킹하여 액세스 권한을 얻는 수법

제로데이 공격은 어떻게 대비해야 할까?

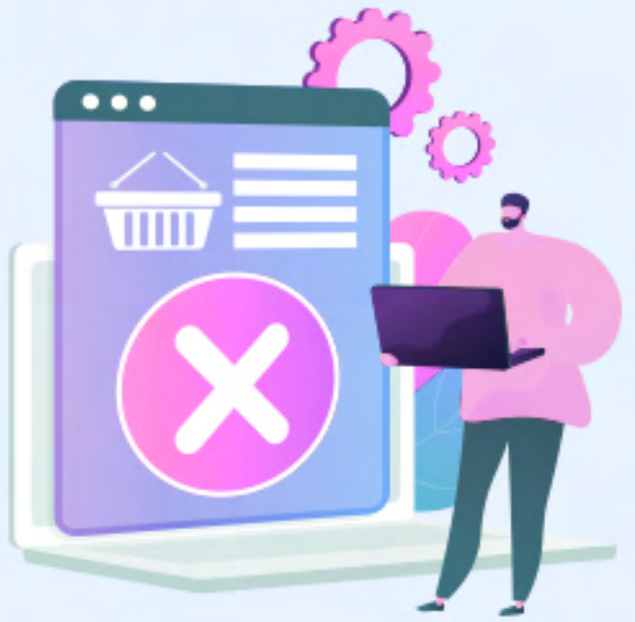
기본적으로 제로데이 자체가 알려지지 않은 취약점이기에
선제적으로 취약점을 찾아내서 막는 것은 어렵다.
다만, 제로데이 공격에 대한 예방 및 차단 할 수 있는 연구가 계속되고 있으며,
우리는 예방을 위한 다음과 같은 방법을 활용해야 한다.

1 모든 소프트웨어, 운영체제 최신상태 유지

모든 소프트웨어와 운영체제를 최신 버전 유지 및
바이러스 백신 소프트웨어 솔루션을 이용

2 필수 애플리케이션만 사용

소프트웨어가 많을수록 잠재적인 취약성이
높아지므로, 필수 애플리케이션만 사용하여 위험



제로데이 공격은
어떻게 대비해야 할까?

3 적절한 방화벽 구성 및 운영

방화벽은 앞단에서 시스템을 보호하는 중요한 역할을
함으로 필요한 수행 업무만 허용하도록 구성하여 운영

4 조직 내에 보안 교육 실시

제로데이 공격은 다양한 방법과 해마다 증가하고 있고
특히, 공격자는 인적 오류를 이용함으로
보안 교육을 통하여 사이버 보안위협을 보호하고
예방할 수 있는 환경 구축 필요