Technical Brief

플래시어레이 세이프모드와 랜섬웨어 예방

퓨어스토리지의 플래시어레이(FlashArray™) 세이프모드(SafeMode™) 스냅샷으로 데이터를 보호하세요.

파일을 암호화하고 이를 풀어주는 대가로 돈을 요구하는 랜섬웨어는 조직에 치명적일 수 있습니다. 데이터 손실과 금전적인 피해만 문제가 되는 것이 아니라, 많은 경우 공격으로 인해 며칠 동안 회사 운영이 완전히 중단되고, 대중의 부정적 시선을 받게 됩니다. 결국 비즈니스 평판과 브랜드 가치도 손상될 수 있습니다. 2020년 미국 스마트워치 제조사 Garmin은 랜섬웨어 공격을 받아 거의 5일 동안 운영이 중단되었으며, 구체적인 수치는 알려지지 않았지만 대략 1,000만 달러를 랜섬으로 지불한 것으로 추정되고 있습니다.

랜섬웨어란?

보안 소프트웨어 기업 Bitdefender의 'Threat Landscape Report 2020' 보고서(영문자료)에 따르면, 2020년 상반기, 전 세계 랜섬웨어 발생 건수는 전년 대비 715% 증가했습니다. 전 세계적으로 코로나19로 인한 원격 근무의 증가와 비즈니스 환경의 변화가 사이버 범죄자들에게는 기회로 작용한 것입니다.

랜섬웨어는 기술, 보험, 석유 및 가스, 고등교육 등 모든 업계에 영향을 미칩니다. 2019년에는 500여 개의 학교(영문자료)가 랜섬웨어 공격을 받았습니다. 랜섬웨어 피해 사례는 날로 늘어나고 있으며, 정상 운영을 재개하기 위해서는 엄청난 금액을 지불해야 합니다.

랜섬웨어 공격 소프트웨어를 상용 소프트웨어만큼 쉽게 구할 수 있다는 사실을 아는 사람은 많지 않을 겁니다. 이러한 소프트웨어는 쉽게 다운로드하고 구매할 수 있으며, 피해자로부터 받은 금액의 일부가 개발자에게 전달되는 경우도 많습니다. 특별한 지식이나 기술이 없어도 공격을 감행할 수 있습니다. 중요한 인프라에 대한 액세스 권한을 가진 직원이 회사에 불만을 품고 공격을 하는 경우도 있습니다. 다크 웹에서 소프트웨어를 간단하게 다운로드하면, 직원 계정이 비활성화되기 전에 랜섬웨어 공격을 시작할 수 있습니다.

보호

악의적인 랜섬웨어 공격, 기업 평판 손상, 막대한 비용 손해로부터 데이터를 보호해줍니다.

보안

어떤 공격을 받든 데이터는 퓨어스토리지 팀의 지원이 있어야만 삭제 가능합니다.

간단

세이프모드는 단 3단계로 설정이 가능하며, 무료로 사용할 수 있습니다.

세이프모드의 데이터 보호 방법

공격자가 플래시어레이에 대한 관리자 권한을 얻었다고 가정하고, 두 가지 잠재적인 공격의 예를 살펴보겠습니다.

1. **공격자가 볼륨을 암호화하고 원본을 삭제하는 경우:** 이 시나리오에서는 원본 볼륨이 삭제됩니다. 볼륨이 '파괴'되면, 플래시어레이의 특수 영역에 존재하는 볼륨 인벤토리에서는 제거되지만, 삭제 버킷에는 여전히 존재합니다. 삭제 버킷에는 오브젝트를 복구하거나 영구적으로 삭제할 수 있는 24시간 타이머가 기본적으로 설정되어 있습니다. 공격자가 이 볼륨까지 제거했다면, 모든 볼륨 데이터가 사라져 이제 공격자의 요구에 따라야 합니다. 정확하게 말하면, 세이프모드가 활성화된 상태에서는 공격자가 관리자 권한이 있더라도 삭제 버킷에서 볼륨 데이터를 제거할 수 없습니다. 이 예시에서 공격자가 볼륨을 삭제할 수 있었던 이유는 세이프모드가 활성화되지 않았기 때문입니다.
2. **공격자가 볼륨을 암호화하고 그 볼륨 외에 모든 스냅샷을 삭제하는 경우:** 이 경우, 스냅샷을 통해 되돌릴 수 있는 복구 지점이 있습니다. 그러나 공격자가 스냅샷을 파괴하고 삭제했기 때문에 복원할 것이 남아 있지 않습니다. 이러한 공격은 위의 예시와 마찬가지로 세이프모드가 활성화되지 않아 공격자가 스냅샷을 삭제했기 때문에 가능했습니다.

두 시나리오에서 세이프모드를 활성화하면, 타이머에 설정된 기간 동안 볼륨이나 스냅샷이 삭제되지 않습니다. 삭제 타이머를 14일로 설정하면 중요한 서비스를 복원하는 데 필요한 복구 데이터가 2주 동안 완벽하게 보호됩니다. 세이프모드는 권한이 가장 높은 사용자 계정으로도 볼륨과 스냅샷을 삭제하지 못하도록 합니다. 뿐만 아니라, 플래시어레이의 스냅샷은 변경이 아예 불가능합니다. 스냅샷과 함께 세이프모드를 활용하면, 공격을 받은 후에도 항상 복구 지점이 보장됩니다.

랜섬웨어 공격에 대한 복구 방법

다시 살펴보면, 첫 번째 예시에서 세이프모드가 활성화된 경우, 공격자가 암호화한 볼륨을 완전히 삭제한 다음 기존 볼륨을 즉시 복원해, 볼륨이 암호화되기 전의 상태로 바로 돌아갈 수 있습니다.

두 번째 예시에서도 프로세스는 동일합니다. 공격자가 암호화한 볼륨을 완전히 삭제하고 스냅샷으로 복원할 수 있습니다. 공격자가 스냅샷을 제거할 수 없기 때문에 복구할 수 있는 상태로 유지되는 것입니다. 두 예시 모두 공격 경로를 조사해 재발을 방지할 수 있는 조치를 취하는 것이 매우 중요합니다.

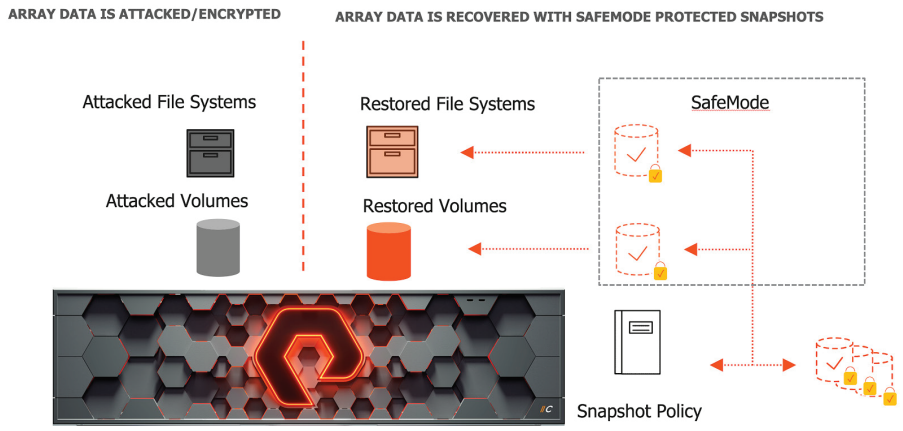

그림 1. 공격을 받은/암호화된 볼륨은 이전 시점의 스냅샷으로 쉽게 교체됩니다.

세이프모드 설정

세이프모드는 쉽게 설정할 수 있습니다. 퓨어스토리지 지원팀에 전화해 세이프모드 활성화를 요청하고, 세이프모드 변경을 요청할 수 있는 권한이 있는 사용자(최대 5명)의 연락처를 제공해 주시면 됩니다. 지원팀은 권한이 있는 각 사용자에게 향후 변경에 사용할 수 있는 6자리 PIN을 발급합니다. 세이프모드는 On이나 Off 상태뿐이지만, 삭제 타이머는 원하는 대로 설정이 가능합니다. 대부분의 고객은 14일로 기한을 설정하지만, 최대 30일까지 연장할 수 있습니다.

데이터를 보호하려면 세이프모드에 대한 스냅샷 정책을 생성하는 것이 필수입니다. 이는 호스트, 볼륨, 볼륨 그룹, 파일 및 디렉터리를 정기적으로 자동으로 스냅샷할 수 있는 플래시어레이 보호 그룹(FlashArray Protection Groups)을 통해 수행됩니다. 스냅샷 보존 기간이나 빈도는 사용자가 설정할 수 있습니다. 제3의 장치를 '타깃'으로 추가하여 다른 플래시어레이나 클라우드 서비스, 플래시블레이드(FlashBlade®)로 스냅샷을 보낼 수도 있습니다.

예를 들어, 어레이로 데이터를 마이그레이션한 후 플래시어레이 용량을 복구해야 할 경우, 어떤 항목이든 영구적으로 제거하려면 두 명의 승인된 사용자가 퓨어스토리지 지원팀과 함께 컨퍼런스 콜을 해야 하며 할당된 PIN이 필요합니다. 그러나 제거 대기 중인 오브젝트의 즉각적인 복구에는 이러한 절차가 필요하지 않습니다.

결론

세이프모드는 관리자의 실수나 악성 랜섬웨어 공격으로 인한 데이터의 영구적인 손실을 방지하는 간편한 기능으로, 추가 비용이 발생하지 않습니다. 설정된 기간 동안 오브젝트의 삭제가 방지되는 원리입니다. 공격이 발생하면, 공개적으로 다운타임을 겪고 복구 노력을 하다 결국 랜섬을 지불하고 마는 상황에 처하는 대신, 공격자가 암호화한 데이터를 제거하고 이전 시점의 데이터를 즉시 복원할 수 있습니다.

이 기능을 활성화하려면, 지원팀에 전화를 걸어 담당자의 연락처를 제공하고 타이머 기간을 설정하기만하면 됩니다. 이 세 단계는 잠재적인 재난이 닥치기 전에 간단하고 효과적인 보호책을 제공합니다.

PS2024-01 03/2021