(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0086501
(43) 공개일자 2021년07월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06F 21/52* (2013.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06F 21/52 (2013.01)
(21) 출원번호 10-2020-0180677
(22) 출원일자 2020년12월22일
심사청구일자 2020년12월22일
(30) 우선권주장
1020190179649 2019년12월31일 대한민국(KR)

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
조은선
대전광역시 유성구 어은로 57 한빛아파트, 110동 1504호
백준영
대전광역시 중구 문화로87번길 72
최중현
세종특별자치시 금남면 진동길 65-3
(74) 대리인
이은철, 김재문

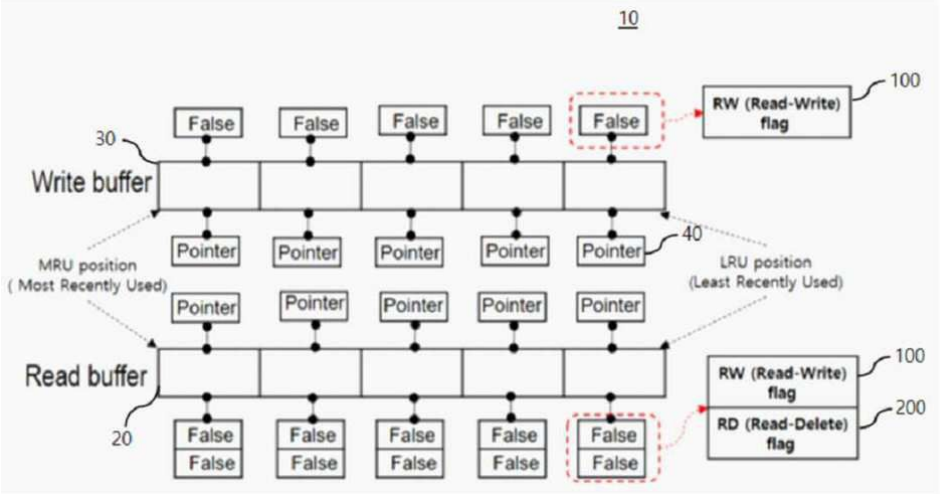
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **랜섬웨어 공격을 식별하는 버퍼 관리 시스템 및 방법**

(57) 요 약

본 기술은 랜섬웨어 공격을 식별하는 버퍼 관리 시스템 및 방법에 관한 것이다. 본 기술의 구현 예에 따르면, 저장장치 내부버퍼가 랜섬웨어의 데이터 읽기 쓰기 패턴을 감지하여 랜섬웨어 공격을 식별할 수 있도록 관리되어 플래쉬 기반 저장장치 뿐만 아니라 HDD에서도 랜섬웨어 공격을 식별하여 데이터를 보호할 수 있는 이점이 있다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	1711103337
과제번호	2019-0-01343-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	융합보안핵심인재양성사업
연구과제명	융합보안석사과정
기 여 율	1/1
과제수행기관명	한국인터넷진흥원
연구기간	2020.04.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

저장장치의 읽기 버퍼와 쓰기 버퍼를 포함하는 내부 버퍼 관리 시스템에 있어서,

상기 내부 버퍼에 저장된 데이터의 상태를 나타내고, 상기 저장장치에 대한 데이터 읽기 요청 또는 데이터 쓰기 요청 수행 시 소정의 조건에 따라 변경되는 RW플래그; 및

상기 내부 버퍼에 저장된 데이터의 상태를 나타내고, 상기 저장장치에 대한 데이터 삭제 요청 수행 시 상기 내부 버퍼에 저장된 데이터의 적중 여부에 따라 변경되는 RD 플래그를 포함하는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 시스템.

청구항 2

제1항에 있어서,

상기 RD 플래그는 상기 삭제 요청 수행 시 상기 읽기 버퍼에 저장된 데이터의 적중 여부에 따라 변경되는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 시스템.

청구항 3

제1항에 있어서,

상기 RW 플래그는 상기 읽기 요청 수행 시 상기 쓰기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RW 플래그 상태에 따라 변경되는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 시스템.

청구항 4

제1항에 있어서,

상기 RW 플래그는 상기 쓰기 요청 수행시 상기 읽기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RD 플래그 상태에 따라 변경되는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 시스템.

청구항 5

저장장치의 읽기 버퍼와 쓰기 버퍼를 포함하는 내부 버퍼 관리 방법에 있어서,

상기 내부 버퍼에 저장된 데이터의 상태를 나타내는 RW 플래그를 상기 저장장치에 대한 데이터 읽기 요청 또는 데이터 쓰기 요청 수행 시 소정의 조건에 따라 변경하는 단계; 및

상기 내부 버퍼에 저장된 데이터의 상태를 나타내는 RD 플래그를 상기 저장장치에 대한 데이터 삭제 요청 수행 시 상기 내부 버퍼에 저장된 데이터의 적중 여부에 따라 변경하는 단계를 포함하는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 방법.

청구항 6

제5항에 있어서,

상기 RD 플래그는 상기 삭제 요청 수행 시 상기 읽기 버퍼에 저장된 데이터의 적중 여부에 따라 변경되는 것을

특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 방법.

청구항 7

제5항에 있어서,

상기 RW 플래그는 상기 읽기 요청 수행 시 상기 쓰기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RW 플래그 상태에 따라 변경되는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 방법.

청구항 8

제5항에 있어서,

상기 RW 플래그는 상기 쓰기 요청 수행시 상기 읽기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RD 플래그 상태에 따라 변경되는 것을 특징으로 하는 랜섬웨어 공격을 식별하는 버퍼 관리 시스템.

발명의 설명

기 술 분 야

[0001] 랜섬웨어 공격을 식별하는 버퍼 관리 시스템 및 방법에 관한 것으로, 더욱 상세하게는 저장장치 계층에서 랜섬웨어 공격을 식별하여 피해를 방지할 수 있는 랜섬웨어 공격을 식별하는 버퍼 관리 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 암호화 랜섬웨어는 사이버 보안을 위협하는 가장 큰 위험 요인이다. 암호화 랜섬웨어는 유저 파일을 잠그고 그들의 파일을 푸는데 돈을 요구한다.

[0004] 랜섬웨어가 이용하는 복호화 키 없이는 데이터 복구가 불가능하도록 하는 강력한 암호화 알고리즘과 토르 네트워크 또는 비트코인과 같은 결제 거래원을 추적하기 어렵게 하는 최첨단 익명성 메카니즘 관련 기술은 높은 레벨에 도달하였다.

[0005] 또한, 랜섬웨어를 위한 새로운 비즈니스 모델과 개발 툴들은 기술적 지식 없이도 랜섬웨어를 만들고 퍼뜨리는데 용이하다. 워너크라이는 23만대 이상의 컴퓨터 시스템을 감염 시켰고 약 40억 달러의 재산상 손해를 2017. 5. 12. 하루만에 끼쳤다.

[0006] 진화하는 랜섬웨어에 맞서기 위하여 다양한 대응책이 제안되었다. 기존 기술은 반복적인 파일 액세스 패턴과 파일 리네임하는 것과 같은 랜섬웨어의 행동 특징을 식별함으로써 랜섬웨어를 감지하고 막는 기술들이다.

[0007] 기존 랜섬웨어 감지기의 다수는 원본과 암호화된 파일의 내용 혼잡도의 차이를 이용하는 Shannon 엔트로피를 이용하기도 한다.

[0008] 오작동을 감지하는데 효율적인 머신러닝 기술이 나타난 이래로 많은 데이터 주도 감지기가 제안되었다.

[0009] 이러한 방어 전략의 특성은 호스트 시스템(OS와 응용프로그램)이 접근 가능한 시맨틱 정보(파일 메타데이터, 파일 오퍼레이션, 시스템 콜)를 주로 사용한다.

[0010] 최근, 저장장치에서의 랜섬웨어 방지가 유망한 해법으로 조명되고 있다. FlashGuard와 SSD-insider는 랜섬웨어로부터 데이터를 보호하는 기능을 저장장치가 갖도록 한다. 이들은 모두 플래쉬 메모리의 외부 업데이트 속성과 같은 독특한 속성을 이용한다. 이러한 특성은 저장장치가 데이터 복구를 위한 자연스러운 백업공간을 갖게 한다.

[0011] 한편, 저장장치는 HDD, SSD로 분류할 수 있다. HDD는 1956년 IBM에서 발명한 표준 저장장치이다. HDD는 몇 개의 플래터, 스핀들 그리고 몇 가지 구동 파트로 구성된다. 플래터는 데이터를 저장하는 자기 매체로 코팅되어 있다. SSD는 일반적으로 플래쉬 기반 저장 장치를 말한다. 플래쉬 기반 SSD는 더 이상 기계적인 부품을 필요로

하지 않아 HDD보다 높은 성능을 가진다.

[0012] 그러나, 랜섬웨어에 대응한 기존 저장장치 연구들은 오로지 SSD에 관하여 이루어지고 있다. 이러한 플래쉬 기반 저장장치에 대한 접근은 HDD에 저장된 데이터가 랜섬웨어로부터 보호되지 못하는 심각한 문제를 가진다.

선행기술문헌

특허문헌

[0014] (특허문헌 0001) 1. 한국등록특허 제10-1970993호

발명의 내용

해결하려는 과제

[0015] 본 발명은 상기와 같은 문제를 해결하기 위한 것으로서, 저장장치에 정의된 액세스 패턴 및 콘텐츠에 따라 랜섬웨어 공격을 식별하여 SSD는 물론 HDD에도 적용될 수 있는 보편성을 가진 랜섬웨어 공격을 식별하는 버퍼 관리 시스템 및 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0017] 상기와 같은 과제를 해결하기 위한 본 발명의 랜섬웨어 공격을 식별하는 버퍼 관리 시스템은, 저장장치의 읽기 버퍼와 쓰기 버퍼를 포함하는 내부 버퍼 관리 시스템에 있어서, 상기 내부 버퍼에 저장된 데이터의 상태를 나타내고, 상기 저장장치에 대한 데이터 읽기 요청 또는 데이터 쓰기 요청 수행 시 소정의 조건에 따라 변경되는 RW 플래그; 및 상기 내부 버퍼에 저장된 데이터의 상태를 나타내고, 상기 저장장치에 대한 데이터 삭제 요청 수행 시 상기 내부 버퍼에 저장된 데이터의 적중 여부에 따라 변경되는 RD 플래그를 포함하는 것을 특징으로 한다.

[0018] 바람직하게는, 상기 RD 플래그는 상기 삭제 요청 수행 시 상기 읽기 버퍼에 저장된 데이터의 적중 여부에 따라 변경되는 것이다.

[0019] 바람직하게는, 상기 RW 플래그는 상기 읽기 요청 수행 시 상기 쓰기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RW 플래그 상태에 따라 변경되는 것이다.

[0020] 바람직하게는, 상기 RW 플래그는 상기 쓰기 요청 수행시 상기 읽기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RD 플래그 상태에 따라 변경되는 것이다.

[0021] 본 발명의 다른 실시예에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 방법은, 저장장치의 읽기 버퍼와 쓰기 버퍼를 포함하는 내부 버퍼 관리 방법에 있어서, 상기 내부 버퍼에 저장된 데이터의 상태를 나타내는 RW 플래그를 상기 저장장치에 대한 데이터 읽기 요청 또는 데이터 쓰기 요청 수행 시 소정의 조건에 따라 변경하는 단계; 및 상기 내부 버퍼에 저장된 데이터의 상태를 나타내는 RD 플래그를 상기 저장장치에 대한 데이터 삭제 요청 수행 시 상기 내부 버퍼에 저장된 데이터의 적중 여부에 따라 변경하는 단계를 포함하는 것을 특징으로 한다.

[0022] 바람직하게는, 상기 RD 플래그는 상기 삭제 요청 수행 시 상기 읽기 버퍼에 저장된 데이터의 적중 여부에 따라 변경되는 것이다.

[0023] 바람직하게는, 상기 RW 플래그는 상기 읽기 요청 수행 시 상기 쓰기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RW 플래그 상태에 따라 변경되는 것이다.

[0024] 바람직하게는, 상기 RW 플래그는 상기 쓰기 요청 수행시 상기 읽기 버퍼에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RD 플래그 상태에 따라 변경되는 것이다.

발명의 효과

[0026] 전술한 바와 같은 본 발명에 따르면, 저장장치에 정의된 액세스 패턴 및 콘텐츠에 따라 랜섬웨어 공격을 식별함으로써 SSD와 같은 플래쉬 기반 저장장치는 물론 HDD와 같은 저장장치에도 보편적으로 적용되어 랜섬웨어의 공격을 식별하여 데이터를 보호할 수 있는 이점이 있다.

도면의 간단한 설명

[0028] 도 1은 세 가지 유형의 랜섬웨어가 파일에 접근하는 액세스 패턴을 도시한다.

도 2는 랜섬웨어 유형 1의 저장장치에 대한 액세스 패턴을 도시한다.

도 3은 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 시스템의 블록도를 도시한다.

도 4은 읽기 요청에 관한 알고리즘 1의 의사코드를 도시한다.

도 5는 쓰기 요청에 관한 알고리즘 2의 의사코드를 도시한다.

도 6은 삭제 요청에 관한 알고리즘 3의 의사코드를 도시한다.

도 7은 랜섬웨어 유형 1에 감염된 읽기 및 쓰기 버퍼의 상태를 도시한다.

도 8은 랜섬웨어 유형 2에 감염된 읽기 및 쓰기 버퍼의 상태를 도시한다.

도 9는 랜섬웨어 3 유형에 감염된 읽기 및 쓰기 버퍼의 상태를 도시한다.

도 10은 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 방법의 흐름도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 후술되어 있는 실시예들을 참조하면 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 이에 앞서 본 발명에 관련된 공지 기능 및 그 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 구체적인 설명을 생략하였음에 유의해야 할 것이다.

[0030] 도 1은 세 가지 유형의 랜섬웨어가 파일에 접근하는 액세스 패턴을 도시한다.

[0031] 도 2는 랜섬웨어 유형 1의 저장장치에 대한 액세스 패턴을 도시한다.

[0032] 저장장치에 대한 요청에는 요청의 유형과 대상 주소 및 요청된 데이터의 크기만 포함되므로 저장장치는 파일에 대한 이러한 종류의 의미 정보를 사용할 수 없다.

[0033] 저장장치 레벨의 액세스 패턴은 주어진 요청의 주소를 기반으로 정의되고, 주소는 호스트 시스템이 액세스하려는 파일의 위치를 나타낸다.

[0034] 파일 엔트로피는 랜섬웨어 공격의 대표적인 지표이다. 랜섬웨어에 의해 암호화된 파일들은 매우 높은 엔트로피 값을 가진다. 그러나, 파일에 대한 정보(예를 들면 파일이름)에 액세스 할 수 없으므로 저장장치에서 파일의 정확한 내용이 식별되지는 않는다. 콘텐츠는 저장장치에서 주소에 의해 식별될 뿐이다.

[0035] 내부버퍼는 저장 매체의 긴 액세스 타임을 감추고 성능을 높이기 위해 저장장치에 위치한다. 읽기 요청 페치 및 쓰기 요청이 저장하려고 하는 데이터는 일시적으로 버퍼에 유지된다. 따라서 버퍼는 자연스럽게 읽기, 쓰기, 삭제 요청의 최근 히스토리를 보유할 수 있고, 이들은 랜섬웨어 행동과 연관된 액세스 패턴과 콘텐츠에 대한 중요한 정보를 제공한다.

[0036] 본 발명에 따른 저장장치의 내부 버퍼 시스템은 랜섬웨어 식별을 위한 고유한 액세스 패턴에 대한 정보를 보유할 수 있도록 구축된다.

[0037] 도 3은 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 시스템의 블록도를 도시한다.

[0038] 도 3을 참조하여 예를 들면, 쓰기 버퍼(30)의 한 요소(예를 들면 4KB)는 추가적인 두 데이터 구조 Read-and-Write(RW) 플래그(100), 그리고 RW-Pointer(40)를 가지고, 읽기 버퍼(20)의 한 요소는 RW 플래그(100), RW-Pointer(40) 그리고 Read-and-Delete(RD) 플래그(200)를 가진다.

[0039] 또한, 도 3을 참조하면, 랜섬웨어 공격을 식별하는 버퍼 관리 시스템(10)은 분리된 읽기 버퍼(20)와 쓰기 버퍼(30)가 있고, 분리된 읽기 버퍼(20)와 쓰기 버퍼(30)는 읽기, 쓰기, 삭제 요청의 구별되는 패턴을 식별하는데 도움을 준다.

[0040] 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 시스템(10)은 저장장치의 읽기 버퍼(20)와 쓰기 버퍼(30)를 포함하는 내부 버퍼 관리 시스템에 있어서, RW 플래그(100), RD 플래그(200)를 포함한다.

[0041] RW 플래그(100)는 주어진 데이터가 읽기 및 쓰기 패턴을 유발한다는 것을 나타내고, RD 플래그(200)는 주어진 데이터가 읽기 및 삭제 패턴에 속함을 나타낸다.

[0042] RW 플래그(100)의 True 값은 주어진 데이터 형태가 읽기 및 쓰기 패턴임을 나타내고, RD 플래그(200)의 True 값은 주어진 데이터 형태가 읽기 및 삭제 패턴임을 나타낸다. RW-Pointer(40)는 데이터와 읽기 버퍼(20) 또는 쓰기 버퍼(30)의 관계를 나타내고, 버퍼와 데이터의 관계는 읽기 및 쓰기의 패턴을 만들어 낸다.

[0043] RW 또는 RD 플래그가 True인 의심스러운 데이터는 읽기 및 쓰기 버퍼의 주소에 의해 액세스 된다.

[0044] RW 플래그(100)는 내부 버퍼에 저장된 데이터의 상태를 나타내고, 저장장치에 대한 데이터 읽기 요청 또는 데이터 쓰기 요청 수행 시 소정의 조건에 따라 변경된다.

[0045] RW 플래그(100)는 저장장치에 대한 데이터 읽기 요청 수행 시 쓰기 버퍼(30)에 저장된 데이터의 적중 여부 및 적중된 데이터의 RW 플래그(100) 상태에 따라 변경되는 것일 수 있다.

[0046] 또한, RW 플래그(100)는 저장장치에 대한 쓰기 요청 수행시 읽기 버퍼(20)에 저장된 데이터의 적중 여부 및 적중된 데이터의 RD 플래그(200) 상태에 따라 변경되는 것일 수 있다.

[0047] RD 플래그(200)는 내부 버퍼에 저장된 데이터의 상태를 나타내고, 저장장치에 대한 데이터 삭제 요청 수행 시 내부 버퍼에 저장된 데이터의 적중 여부에 따라 변경된다.

[0048] RD 플래그(200)는 저장장치에 대한 데이터 삭제 요청 수행 시 읽기 버퍼(20)에 저장된 데이터의 적중 여부에 따라 변경되는 것일 수 있다.

[0049] 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 시스템은 전통적인 읽기 및 쓰기 버퍼의 다음 두가지 기본 원칙을 준수한다.

[0050] 1) 각 버퍼의 요소는 가장 최근에 사용된 요소를 버퍼에 유지시키고, 가장 오래전에 사용된 요소를 제거하는 정책(LRU : least recently used) 에 의하여 제거되고, 2) 읽기 요청이 수신되면 항상 쓰기 버퍼가 먼저 탐색되고 이는 쓰기 버퍼가 항상 최신 데이터를 포함하고 있기 때문이다.

[0051] 또한, 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 시스템은 상기 두 가지 기본 원칙 외에 다음과 같은 7가지 새로운 원칙을 고려할 수 있다.

[0052] 원칙 1 : 읽기 버퍼(20)의 데이터에 'False'의 RW 플래그(100)와 'False'의 RD 플래그(200)가 있고 해당 데이터 주소가 들어오는 쓰기 요청이 지시 된 주소와 동일한 경우 읽기 버퍼(20)의 데이터에 RW 플래그(100)가 'True'로 표시된다. 이후, 쓰기 요청에 속하는 데이터는 쓰기 버퍼에 'True' RW 플래그(100)와 함께 저장된다.

[0053] 원칙 2 : 쓰기 요청이 원칙 1을 호출하는 경우, 읽기 버퍼(20)의 데이터는 쓰기 버퍼(30)의 해당 데이터와 쌍을 이루고 이는 RW-Pointer(40) 플래그에 의해 구현된다.

[0054] 원칙 3 : 삭제 요청이 읽기 버퍼(20)에서 데이터를 제거하려고 할 때, 데이터에 'False'의 RW 플래그(100)가 있으면 RD 플래그의 값은 'True'가 된다.

[0055] 원칙 4 : 삭제 요청이 쓰기 버퍼(30)에서 데이터를 제거하려고 하면 쓰기 버퍼(30)에서 데이터가 즉시 제거된다.

[0056] 원칙 5 : 읽기 버퍼(20)의 데이터에 'True'의 RD 플래그(200)가 있고 해당 데이터 주소가 들어오는 쓰기 요청이 향하고 있는 주소와 같으면 그 데이터는 읽기 버퍼(20)에서 제거된다.

[0057] 원칙 6 : 쓰기 버퍼(30)가 가진 데이터의 주소가 들어오는 읽기 요청이 향하는 주소와 일치하는 경우, 만약 그 데이터의 쓰기 버퍼(30) RW 플래그(100)가 'True'이면, 그 데이터의 쓰기 버퍼(30) RW 플래그(100) 값은 'False'로 변경된다.

[0058] 원칙 7. RW 플래그(100)가 'True'인 데이터가 삭제 요청에 의해 쓰기 버퍼(30)에서 제거되거나, LRU 교체 정책

에 의해 제거되거나, 쓰기 버퍼(30)에 있는 데이터의 RW 플래그(100)가 'True'에서 'False'를 가지면 상기 해당 데이터와 쌍을 이루는 데이터가 읽기 버퍼(20)에서 제거된다.

[0059] 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 시스템은 위와 같은 원칙들에 기반하여 읽기, 쓰기, 삭제 요청의 알고리즘을 제공할 수 있다.

[0060] 모든 알고리즘에서 입력은 저장 장치의 기본 작동 단위에 대한 요청이다. 즉, 데이터에 대한 단위 보다 큰 원래 요청은 저장 장치에 도착하자마자 여러 개의 하위 요청으로 나뉜다. 하위 요청은 한 번에 한 개씩 처리된다.

[0061] 도 4은 읽기 요청에 관한 알고리즘 1의 의사코드를 도시한다.

[0062] 도 4을 참조하면, 알고리즘 1은 먼저 쓰기 버퍼(30)를 탐색한다. 만약 쓰기 버퍼(30)가 입력 요청과 같은 주소의 데이터를 가지고, 적중 데이터가 'True' RW 플래그(100)를 가지면, 그 RW 플래그(100)는 'False'가 된다. 이후, 만약 적중 데이터가 RW-Pointer(40)를 통해 읽기 버퍼의 데이터에 링크된다면, 연결된 데이터가 읽기 버퍼에서 제거되고 링크 연결을 끊는다(알고리즘 1 라인 5). 쓰기 요청 이후의 읽기 요청 패턴은 랜섬웨어의 전형적인 것이 아니기 때문이다. 그리고, 적중 데이터가 리턴된다.

[0063] 반면에, 쓰기 버퍼(30)에 적중 데이터가 없을 때에는 읽기 버퍼(20)가 탐색된다. 만약 읽기 버퍼(20)가 읽기 요청에 따른 적중 데이터를 가진다면, 그 적중 데이터는 반환된다. 그렇지 않으면, 요청의 요구 데이터는 저장매체로부터 페치되고, 페치된 데이터가 리턴된다.

[0064] 도 5는 쓰기 요청에 관한 알고리즘 2의 의사코드를 도시한다.

[0065] 도 5를 참조하면, 쓰기 요청에 대한 알고리즘 2는 랜섬웨어 유형 1과 유형 3에서 관찰되는 읽고 쓰기 패턴의 식별에 초점을 맞춘다. 이 패턴은 읽기 버퍼(20)에서 RD 플래그(200)가 'False'인 어떤 데이터와 동일한 주소를 가지는 쓰기 요청이 있을 때 식별된다. 읽기 버퍼(20)의 적중 데이터는 RW 플래그(100) 'True' 값을 가지고, 쓰기 요청은 마찬가지로 쓰기 버퍼에서 RW 플래그(100) 값이 'True'인 그것의 새로운 데이터를 저장한다(알고리즘 2 라인 14). 그런 다음 쓰기 버퍼(30)의 새 데이터는 RW-Pointer(40)를 통해 읽기 버퍼(20)의 해당 데이터에 연결된다(알고리즘 2 라인 15). 알고리즘 2는 저장장치의 버퍼가 랜섬웨어 유형 3이 데이터 복구를 피하기 위해 원본 파일을 더티 데이터로 한 번 이상 덮어 쓰는 읽기 및 쓰기 패턴을 식별할 수 있도록 허용한다(알고리즘 2 라인 3-6).

[0066] 도 6은 삭제 요청에 관한 알고리즘 3의 의사코드를 도시한다.

[0067] 도 6을 참조하면, 알고리즘 3이 삭제 요청을 어떻게 진행하는지 기술하고 있다. 랜섬웨어 유형 2는 원본 파일을 제거하기 위한 삭제 요청이 문제된다. 알고리즘 3은 읽기 요청 다음에 따라오는 삭제 요청의 패턴을 포착한다. 삭제 요청이 쓰기 버퍼(30)에서 읽기 및 쓰기 패턴과 관련된 데이터를 제거하려고 하면 일치하는 데이터가 쓰기 버퍼(30)에서 제거된다. 또한, 읽기 버퍼(20)가 제거된 데이터와 쌍을 이루는 데이터를 가질 때, 해당 데이터는 읽기 버퍼(20)로부터 제거된다. 반면에, 읽기 및 삭제 패턴은 읽기 버퍼(20)의 데이터가 쓰기 버퍼(30)의 삭제 요청에 의해 적중될 때 결정된다. 따라서 적중 데이터는 읽기 버퍼(20)에서 적중 데이터를 삭제하는 대신 RD 플래그(200) 값 'True'를 얻는다(알고리즘 3 라인 6).

[0068] 랜섬웨어 유형 1의 공격에서는 반복적인 읽기 요청 후 쓰기 요청 패턴이 저장장치에 있는 파일에 생성된다. 이러한 액세스 패턴은 대부분의 읽기 버퍼(20) 및 쓰기 버퍼(30)가 RW 플래그(100) 'True'로 표시된 데이터로 구성되도록 한다.

[0069] 이러한 유형의 랜섬웨어에 의한 새로운 암호화 데이터는 읽기 버퍼(20) 내의 해당 원본 데이터의 주소와 동일한 주소로 향하고 있다. 이러한 패턴은 들어오는 쓰기 요청의 데이터와 그에 매치되는 읽기 버퍼(20)의 데이터가 RW 플래그 'True'의 값을 얻게 한다. 양 데이터는 RW-Pointer(40)를 통해 짝지어진다.

[0070] 도 7은 랜섬웨어 유형 1에 감염된 읽기 및 쓰기 버퍼의 상태를 도시한다.

[0071] 도 7을 참조하면, 두 개의 희생 파일이 랜섬웨어에 감염된 시나리오에서 버퍼가 읽기 및 쓰기 요청을 처리한 후 읽기 버퍼(20) 및 쓰기 버퍼(30)의 결과 상태를 나타낸다. 읽기 버퍼(20)와 쓰기 버퍼(30)에서의 RW 플래그(100)가 'True' 값인 모든 데이터가 RW-Pointer(40)로 연결되어 있다.

[0072] 도 8은 랜섬웨어 유형 2에 감염된 읽기 및 쓰기 버퍼의 상태를 도시한다.

[0073] 도 8을 참조하면, 원본 파일 복구를 방지하기 위해 랜섬웨어 유형 2는 읽기 요청에 따라 삭제 요청을 집중적으

로 생성한다. 삭제 요청은 읽기 버퍼(20)에 있는 희생 파일의 데이터에 액세스하기 때문에 데이터는 읽기 버퍼에 RD 플래그(200) 'True' 값을 갖는다. 읽기 버퍼(20)는 이러한 RD 마킹된 데이터에 점령된다.

[0074] 도 9는 랜섬웨어 3 유형에 감염된 읽기 및 쓰기 버퍼의 상태를 도시한다.

[0075] 도 9를 참조하면, 랜섬웨어 유형 3은 희생 파일 뿐만 아니라 새로운 암호화 파일에 대한 쓰기 요청을 생성한다. 쓰기 버퍼(30)의 절반 정도가 RW 플래그(100) 'True' 값인 데이터에 점령되었고 이는 희생 파일과 새로운 암호화 파일이 쓰기 버퍼(30)를 얻기 위해 노력하기 때문이다. RW 플래그(100)가'True'값인 데이터는 읽기 버퍼의 그러한 RW 마킹된 데이터가 원칙 7을 기반으로 쓰기 버퍼(30)에 있는 각 데이터의 존재와 밀접한 관련이 있기 때문에 읽기 버퍼(20)의 절반을 구성한다.

[0076] 상술한 바와 같은 예시에서 본 발명의 실시예에 따르면, 읽기 버퍼(20) 및 쓰기 버퍼(30)의 상태에서 랜섬웨어 공격을 밝히는 표지를 확인할 수 있다.

[0077] 도 10은 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 방법의 흐름도를 도시한다.

[0078] 본 발명에 따른 랜섬웨어 공격을 식별하는 버퍼 관리 방법은 저장장치의 읽기 버퍼(20)와 쓰기 버퍼(30)를 포함하는 내부 버퍼 관리 방법에 있어서, 내부 버퍼에 저장된 데이터의 상태를 나타내는 RW 플래그(100)를 저장장치에 대한 데이터 읽기 요청 또는 데이터 쓰기 요청 수행 시 소정의 조건에 따라 변경하는 단계(S100) 및 내부 버퍼에 저장된 데이터의 상태를 나타내는 RD 플래그(200)를 상기 저장장치에 대한 데이터 삭제 요청 수행 시 내부 버퍼에 저장된 데이터의 적중 여부에 따라 변경하는 단계(S200)를 포함한다.

[0079] 이 때, RD 플래그(200)는 저장장치에 대한 데이터 삭제 요청 수행 시 읽기 버퍼(20)에 저장된 데이터의 적중 여부에 따라 변경되는 것일 수 있다.

[0080] 이 때, RW 플래그(100)는 저장장치에 대한 데이터 읽기 요청 수행 시 쓰기 버퍼(30)에 저장된 데이터의 적중 여부 및 적중된 데이터의 RW 플래그(100) 상태에 따라 변경되는 것일 수 있다.

[0081] 이 때, RW 플래그는 저장장치에 대한 데이터 쓰기 요청 수행시 읽기 버퍼(20)에 저장된 데이터의 적중 여부 및 적중된 데이터의 상기 RD 플래그 상태(200)에 따라 변경되는 것일 수 있다.

[0082] 이상에서 설명된 시스템은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0083] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0084] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가

능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media),CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드 뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0085] 이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것이 아니며, 기술적 사상의 범주를 일탈함이 없이 본 발명에 대해 다수의 변경 및 수정이 가능함을 잘 이해할 수 있을 것이다. 따라서, 그러한 모든 적절한 변경 및 수정과 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

부호의 설명

[0087] 10 : 랜섬웨어 공격을 식별하는 버퍼 관리 시스템

20 : 읽기 버퍼

30 : 쓰기 버퍼

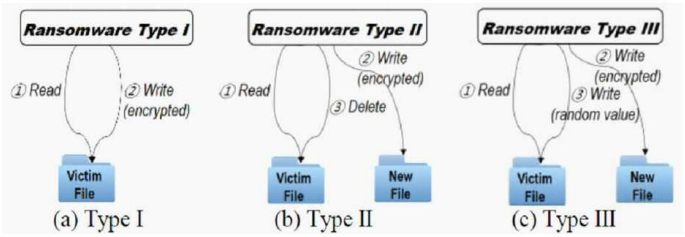
40 : RW-Pointer

100 : RW 플래그

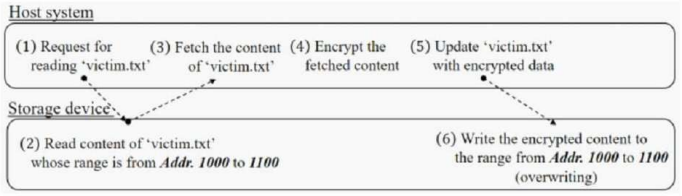
200 : RD 플래그

도면

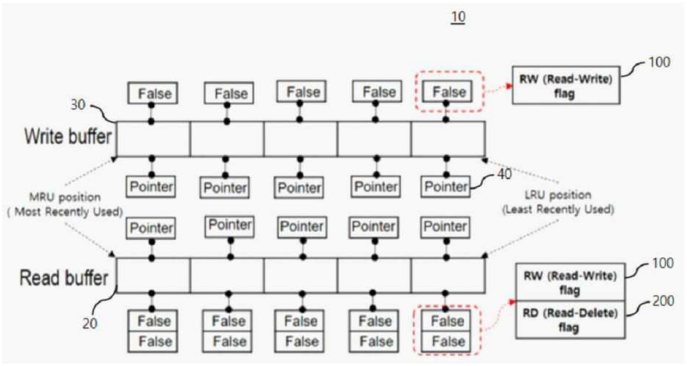
도면1



도면2



도면3



도면4

Algorithm I. Algorithm for a read request.

```
Input: Address
Output: Demanding data
1     if there is a hit by Address in write buffer
2       if RW flag of the hit data is TRUE
3         set RW flag of the hit data to FALSE
4         if there are its paired data in read buffer
5           remove the paired data
6       return the hit data
7     else /*search read buffer*/
8       if there is a hit by Address in read buffer
9         move the hit data to the MRU position of read buffer
10        return the hit data
11      else
12        fetch the demanding data from the storage medium
13        store the fetched data to the MRU position of read buffer
14        return the fetched data
```

도면5

Algorithm II. Algorithm for a write request.

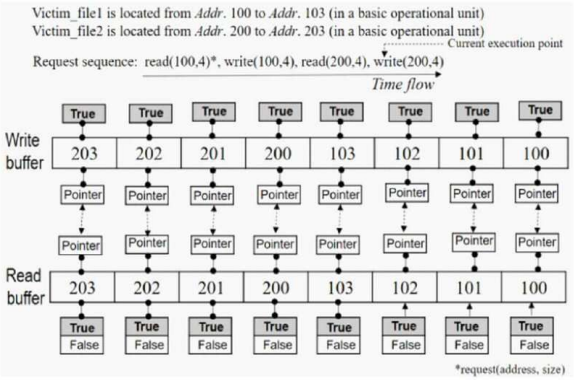
```
Input: Address
1     if there is a hit by Address in write buffer
2       remove the hit data
3       if RW flag of the hit data was TRUE
4         store new data with RW flag of TRUE to the MRU
              position of write buffer
5         if there were data paired with the hit data in read buffer
6           the data in read buffer are paired with the new data
              in write buffer
7       else
8         store new data to the MRU position of write buffer
9     else if there is a hit by Address in read buffer
10      if RD flag of the hit data is TRUE
11        remove the hit data from read buffer
          store new data to the MRU position of write buffer
12      else
13        set RW flag of the hit data to TRUE
14        store new data with RW flag of TRUE to the MRU
            position of write buffer
15        the hit data in read buffer are paired with the new data
            in write buffer
16    else
17      store new data to the MRU position of write buffer
```

도면6

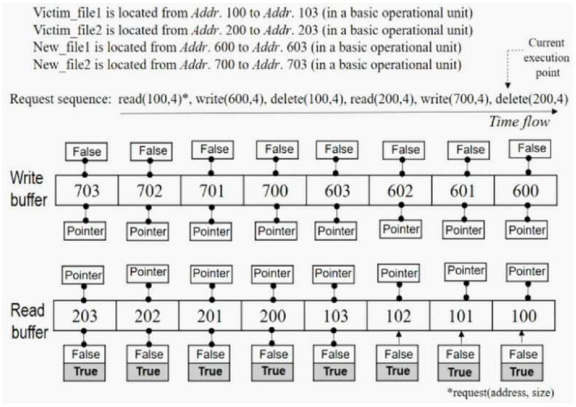
Algorithm III. Algorithm for a delete request.

```
Input: Address
1     if there is a hit by Address in write buffer
2        remove the hit data
         if RW flag of the hit data was TRUE
3           if there are its paired data in read buffer
4              remove the paired data
5     else if there is a hit by Address in read buffer
6           set RD flag of the hit data to TRUE
```

도면7



도면8



도면9

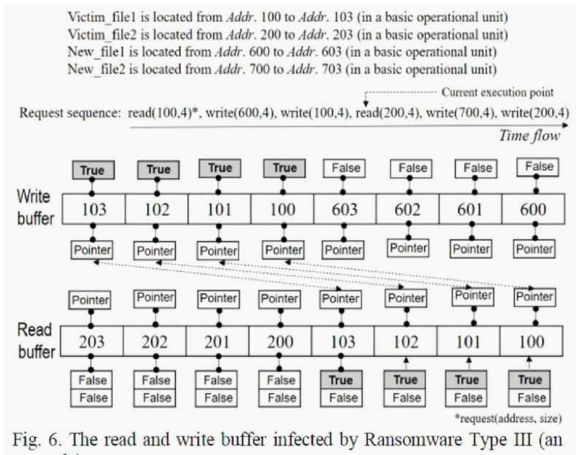


Fig. 6. The read and write buffer infected by Ransomware Type III (an example).

도면10

