정 보 보 호 학 회 지
제26권 제5호, 2016. 10

악성코드에 의해 파괴된 저장장치 복구 방안

김 진 국*

요 약

저장장치 파괴가 피해 효과를 가장 극명하게 보여줄 수 있다는 점 때문에 최근 침해사고에서 자주 사용된다. 저장장치 파괴는 공격 목적을 모두 달성한 후 마지막 수단으로 사용되기도 하지만 공격의 목적 자체인 경우도 종종 있다. 침해사고에서는 주로 저장장치 전체를 파괴하기 보다는 짧은 시간에 파괴 효과를 극대화할 수 있도록 파일시스템의 주요 데이터 구조를 파괴한다. 본 논문에서는 윈도우 운영체제 환경을 대상으로 악성코드에 의해 파괴된 저장장치 유형을 소개하고 복구 방안을 기술한다.

Ⅰ. 서 론

2013년 3월 20일 발생한 사이버테러에서 볼 수 있듯이 공격자는 피해 효과를 극명하게 보여줄 수 있다는 점에서 저장장치를 파괴하는 방법을 사용한다. 저장장치를 파괴하면 운영체제 부팅이 불가능하기 때문에 사용자는 침해를 바로 인지할 수 있다. 이 때문에 저장장치 파괴는 공격 목적을 이룬 후 마지막 수단으로 사용되는 것이 일반적이다. 하지만 대상 조직의 혼란 야기를 원하는 경우 저장장치 파괴가 목적이 되는 경우도 있다.

저장장치 파괴로 자주 사용되는 방법은 저장장치의 주요 데이터 구조를 덮어쓰는 것이다. 부팅을 위한 필수 구조나 운영체제가 설치된 파일시스템의 데이터 구조를 덮어써 운영체제가 정상 부팅이 불가능하도록 만든다. 파괴된 저장장치를 복구하기 위해서는 데이터 구조를 100% 복구해야만 하는 것은 아니다. 침해사고를 당한 저장장치이기 때문에 복구의 주된 목적은 저장장치 재사용이라기보다는 이전 데이터 추출이다. 이전 데이터를 추출하려면 파괴된 저장장치를 새로운 운영체제나 마운트 도구를 이용해 마운트시켜야만 한다.

본 논문에서는 최신 윈도우 운영체제에서도 사용되는 NTFS 파일시스템 환경에서 일어난 저장장치 파괴 방식을 살펴보고 이를 복구하기 위한 최소한의 요건을 기술한다.

Ⅱ. 저장장치와 파일시스템 구조

[그림 1]은 MBR 방식을 사용하는 저장장치의 추상적 구조를 보여준다. 모든 저장장치는 맨 앞쪽에 512바이트의 마스터부트레코드(MBR, Master Boot Record)가 온다. MBR은 부트 코드와 저장장치 각 파티션의 정보를 담고 있는 파티션 테이블로 구성된다. MBR의 주 역할은 파티션 테이블을 검색하여 부팅 가능한(운영체제가 설치된) 파티션을 찾고, 파티션(볼륨)의 시작에 위치한 VBR을 로드하고 실행한다. MBR이 할당되면서 뒤이어 일정 부분의 섹터가 함께 할당되는데 이 부분은 보통 사용되지 않는다. 이 부분은 MBR이 할당되면서 생성되는 영역이라고 하여 MBR 슬랙이라 부른다. 윈도우 XP까지는 MBR 슬랙으로 62섹터 공간이 할당되었지만 Vista 이후부터는 2,047 섹터가 기본 할당된다. MBR과 MBR 슬랙 이후에는 볼륨 영역이 온다. 볼륨은 크게 볼륨의 시작을 담당하는 볼륨부트레코드(VBR, Volume Boot Record)와 볼륨 데이터로 구성되는데 파일시스템은 이 볼륨 영역에 포맷된다. MBR과 MBR 슬랙의 처리 단위가 섹터 단위인 반면, VBR부터는 볼륨의 영역으로 처리 단위는 여러 섹터를 묶은 클러스터이다. 이로 인해 VBR은 파일시스템의 클러스터 크기만큼 할당된다. VBR은 부트섹터와 추가적인 부트코드로 구성된다. 부트섹터는 부트로더를 로드하여 운영체제를 부팅하는 역할을 한다.

* 주식회사 플레인비트 대표 (jinkook.kim@plainbit.co.kr)

MBR	MBR Slack	VBR	Volume Data	VBR	Volume Data

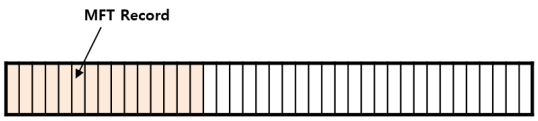
〔그림 1〕 저장장치 추상적 구조

[그림 2]는 파일시스템의 추상적 구조를 보여준다. 대부분의 파일시스템은 파일의 이름, 시간정보, 속성 등이 저장되는 메타 영역과 실제 파일데이터가 저장되는 데이터 영역으로 나눌 수 있다. NTFS 파일시스템에서 메타 영역은 마스터파일테이블(MFT, Master File Table)이라고 불리는 $MFT 파일이다. $MFT 파일은 1,024 바이트 크기의 MFT 레코드라고 불리는 레코드의 집합으로 [그림 3]과 같다. 각각의 MFT 레코드는 NTFS 상에 존재하는 각 파일, 폴더의 정보를 표현한다.

$MFT 파일에서 앞쪽에 할당된 MFT 레코드는 파일시스템 메타데이터 파일이라고 불리는데 NTFS 파일시스템 관리를 위해 가장 중요한 데이터이다.

META Area	DATA Area

〔그림 2〕 파일시스템 추상적 구조



〔그림 3〕 $MFT, Master File Table

Ⅲ. 악성코드 저장장치 파괴 유형

악성코드에 의해 파괴된 저장장치의 파괴 유형을 살펴보면 크게 MBR 파괴, VBR 파괴, 파일시스템 메타데이터 파괴로 나눌 수 있다.

3.1. MBR 파괴

컴퓨터의 부팅은 BIOS가 담당하는데 BIOS는 POST (Power On Self Test)를 마치고 난 후, BIOS에 설정된 첫 번째 장치의 첫 512 바이트를 로드하여 실행하는데 이 영역이 MBR이다. MBR은 부팅 가능한 파티션(볼륨)을 찾아 파티션 처음에 위치한 VBR을 로드하여 실행한다. 따라서, MBR 영역이 손상되면 정상적인 부팅이 불가능하다. 악성코드는 MBR 영역을 0으로 초기화하거나 3.20 사이버테러에서와 같이 특정 문자[1]로 덮어쓴다.

3.2. VBR 파괴

VBR은 MBR에 의해 로드되어 실행되는데 주요 역할은 부트 로더를 로드하여 실행하는 것이다. 따라서, VBR도 MBR과 마찬가지로 운영체제 부팅을 위해서는 반드시 무결성이 유지되어야 한다. 악성코드는 VBR 영역을 초기화하거나 3.20 사이버테러에서와 같이 특정 문자로 덮어쓴다.

3.3. 파일시스템 메타데이터 파괴

MBR, VBR이 정상적인 구조를 가지고 있더라도 파일시스템 관리를 위한 메타데이터 파일이 손상되면 부팅에 필요한 파일을 로드하여 실행할 수 없다. 파일시스템 메타데이터 파괴는 보통 MBR, VBR 파괴와 함께 일어난다. MBR, VBR만 파괴하게 되면 부팅은 불가능하지만 데이터 복원은 비교적 쉽게 가능하므로 데이터 복원을 어렵게 하기 위한 방법으로 파일시스템의 주요 메타데이터도 함께 파괴한다. 파괴 방식은 MBR, VBR과 마찬가지로 초기화하거나 특정 문자로 덮어쓰는 방식이 주로 사용된다.

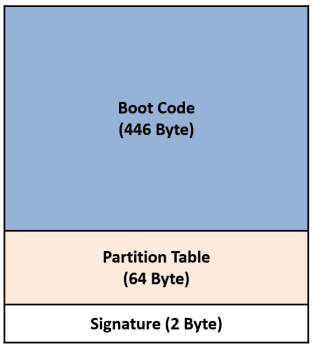
Ⅳ. 악성코드 저장장치 파괴 유형별 복구 방안

악성코드에 의해 파괴된 저장장치의 복구 목적은 저장장치 재사용이기 보다는 파괴되기 이전 데이터를 추출하기 위한 목적이 대부분이다. 따라서 정상 부팅이 가능한 수준까지의 복구가 아닌 널리 알려진 마운트 도구에서 마운트될 수준으로만 복구하면 된다. 앞서 살펴본 저장장치 파괴 유형별로 어떻게 복구할 수 있는지 살펴보자.

1) 3.20 사이버테러에 사용된 문자 : ‘HASTATI’, ‘PRINCPES’

4.1. MBR 파괴 복구

MBR은 [그림 4]와 같은 구조를 가진다. 부트코드는 부팅을 위한 데이터이므로 마운트가 목적이라면 불필요한 데이터이다. 마운트를 하려면 VBR 위치를 식별할 수 있도록 파티션 테이블을 복구해주어야 한다. 각 파티션의 정보는 16바이트의 파티션 테이블 엔트리로 표현되고 파티션 테이블에 최대 4개까지 파티션 정보를 기록할 수 있다[2].



〔그림 4〕 MBR 구조

[표 1]은 파티션 테이블 영역에 저장되는 파티션 테이블 엔트리의 데이터 구조다. CHS 주소 방식은 현재 사용되지 않기 때문에 마운트를 위한 최소 요건은 음영으로 표시된 파티션 유형, LBA 시작 주소, 전체 섹터 수이다.

〔표 1〕 파티션 테이블 데이터 구조

크기(바이트)	설명
1	Boot Flag
3	Start of Partition (CHS)
1	Partition Type
3	End of Partition (CHS)
4	LBA Address of Start Sector
4	Total Sectors

NTFS의 파티션 유형은 항상 0x07 값을 가지므로 실제 복구해주어야 하는 값은 LBA 시작 주소와 전체 섹터 수이다. LBA 시작 주소는 파티션의 시작 섹터 주소로 별도의 파티션 도구를 사용하지 않았다면 XP는 63 섹터, Vista 이후는 2,048 섹터부터 파티션이 시작하기 때문에 해당 위치로 이동하여 VBR 구조가 정상적인지 확인해보거나 VBR의 시그니처를 이용해 저장장치의 시작부터 4,096 섹터만큼 검색을 해보면 쉽게 파티션의 시작 위치를 찾을 수 있다. 파티션의 전체 섹터 수는 식별된 VBR을 이용해 정확하게 복구할 수도 있지만 저장장치 전체 영역을 할당해도 대부분의 마운트 도구에서 정상 마운트해준다. 마지막으로 파티션 테이블 엔트리 정보와 함께 꼭 복구해주어야 하는 정보가 2 바이트의 시그니처 값이다. 시그니처 값은 0x55AA로 고정된 값이다. 정리하면, 손상된 MBR 복구를 위한 최소한의 요건은 [표 2]와 같다.

〔표 2〕 MBR 복구 최소 요건

요건	복구 방안
Partition Type	'0x07'
LBA Address of Start Sector	63, 2048 섹터 검색 혹은 4096내 VBR 시그니처 검색
Total Sectors	VBR 해석 혹은 저장장치 전체 영역
Signature	'0x55AA'

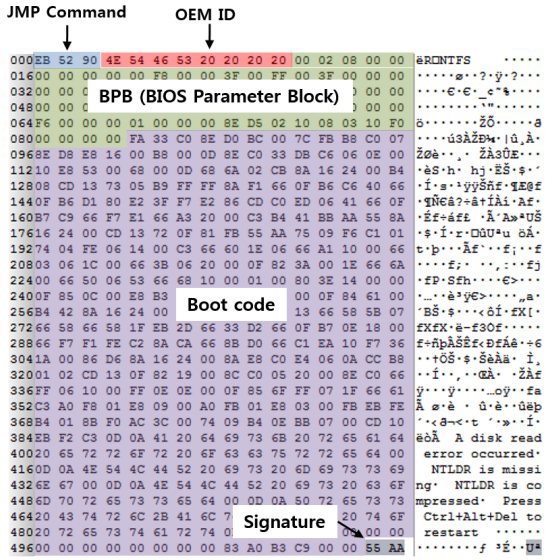
4.2. VBR 파괴 복구

NTFS의 VBR은 파일시스템의 클러스터 크기만큼 할당되는데 사용자가 임의로 설정하지 않는 이상 저장장치 크기가 2 GB 보다 크면 클러스터 크기는 4,096 바이트로 기본 설정된다. 따라서 보통 VBR은 512 바이트의 섹터 8개로 구성된다. 이 중 가장 중요한 구조는 첫 섹터인 부트섹터다. 부트섹터 이후에 오는 7개의 섹터는 부트섹터의 기능을 보조하기 위한 추가 부트코드가 저장된다.

[그림 5]는 부트섹터의 구조를 보여준다. 첫 3바이트는 부트코드로 점프하기 위한 명령이고, 파일시스템 형식을 표현하는 OEM ID가 뒤이어 온다. 다음으로 볼륨에 설치된 파일시스템의 메타 정보를 표현하는 BPB[3] 구조가 온다. 점프 명령이나 부트코드는 부팅을 위한 데이터이므로 마운트할 경우 불필요하다. 마운트를 위해

2) MBR 파티션 테이블에 기록되는 파티션은 '주 파티션'이라고 불린다. 4개를 초과하는 파티션은 또 다른 MBR 구조를 이용해 확장 파티션으로 구성해야 한다.

3) BPB, BIOS Parameter Block



〔그림 5〕 VBR - 부트섹터 구조

서라면 OEM ID와 BPB의 주요 정보만 복구해주면 되는데 NTFS의 OEM ID는 “NTFS”(4E 54 46 53 20 20 20 20)로 고정값을 사용하기 때문에 BPB의 주요 정보만 복구해주면 된다.

[표 3]은 BPB의 데이터 구조로 마운트를 위한 요건은 음영으로 표시된 데이터다. 마운트 도구에 따라 음영으로 표시된 데이터를 모두 요구하는 경우도 있고 이 중

〔표 3〕 BPB 데이터 구조

크기(바이트)	설명
2	Bytes Per Sector
1	Sectors Per Cluster
1	Reserved Sectors
5	Unused
1	Media Descriptor
18	Unused
8	Total Sectors
8	Start Cluster for $MFT
8	Start Cluster for $MFTMirr
1	Cluster Per MFT Record
3	Unused
1	Cluster Per Index Buffer
3	Unused
8	Volume Serial Number
4	Unused

〔표 4〕 마운트 도구별 마운트 최소 요건

요건	FTK Imager	X-Ways Forensics
OEM ID	O	O
Bytes Per Sector	O	X
Sectors Per Cluster	O	X
Total Sectors	O	O
Start Cluster for $MFT	O(X)	O(X)
Start Cluster for $MFTMirr	X(O)	X(O)
Clusters Per File Record	O	X

일부만 요구하는 경우도 있다. [표 4]는 대표적인 마운트 도구인 FTK Imager와 X-Ways Forensics 도구를 이용해 VBR 마운트를 위한 최소 요건을 비교한 것이다.

$MFTMirr는 파일시스템 주요 메타데이터 파일을 백업한 파일로 $MFT와 상호보완적인 관계이다. 둘 중 어느 것이라도 하나만 복구되면 마운트가 가능하다.

[표 4]에서 확인할 수 있듯이 FTK Imager에 비해 X-Ways Forensics 도구가 좀 더 최소한의 검증만 수행한다. 단지 OEM ID, 전체 섹터 수, $MFT 시작 클러스터 위치만 복구해주면 정상 마운트가 가능하다. VBR 복구 시에는 섹터 마지막의 시그니처를 복구해주지 않아도 마운트가 가능하다. 정리하면, 손상된 VBR 복구를 위한 최소 요건은 [표 5]와 같다.

VBR의 부트섹터는 볼륨의 중요 구조이기 때문에 파일시스템을 포맷하면 볼륨의 마지막에 백업이 된다. 따라서 VBR이 손상되면 1차적으로 볼륨 마지막에 백업된 부트섹터를 이용하면 쉽게 복구할 수 있다. 백업된 부트섹터까지 손상되었다면 [표 5]의 VBR 복구 최소 요건을 참고하여 복구를 진행하면 된다.

〔표 5〕 VBR 복구 최소 요건

요건	복구 방안
OEM ID	“NTFS”
Total Sectors	부트 섹터를 검색하여 각 볼륨 구간 식별
Start Cluster for $MFT/$MFTMirr	VBR 이후 “FILE” 시그니처로 검색하여 $MFT 위치 식별

4.3. 파일시스템 메타데이터 파괴 복구

MBR이나 VBR은 일부 혹은 전체가 손상되어도 마운트 가능하도록 완벽하게 복구가 가능하다. 반면, NTFS의 메타데이터인 $MFT가 손상된 경우에는 완벽하게 복구하는 것이 어렵다. 특히 [그림 3]에 나타난 것처럼 $MFT의 앞쪽 MFT 레코드는 파일시스템 관리를 위한 중요 데이터로 이 부분이 손상된 경우 온전하게 볼륨 데이터를 복구하는 것은 불가능하다.

하지만 각각의 MFT 레코드는 부모 폴더에 대한 주소값을 가지고 있어 주소가 연결 가능한 경우 볼륨의 폴더 구조를 복구할 수 있다. 연결이 불가능한 파일의 경우 부모가 없는 고아(orphan) 상태의 파일로 복구가 가능하다. 파일메타데이터와 관계없이 파일의 특성만으로 복구하는 파일 카빙 기법을 사용하면 메타데이터 전체가 손상된 경우에도 복구가 가능하지만, 파일명, 시간정보 등 메타데이터 정보를 알 수 없기 때문에 활용에 많은 제약이 생긴다. 그로인해 가능하면 남아있는 메타데이터 정보를 최대한 활용해 복구할 필요가 있다.

메타데이터를 이용한 복구는 자동화된 파일 복구 도구에서 대부분 지원한다. 대표적인 도구로는 MiniTool Solution 사의 Power Data Recovery가 있다.

Ⅴ. 결 론

3.20 사이버테러 사고와 같이 다수 시스템의 저장장치가 동시에 파괴된 경우 조직은 많은 혼란을 겪는다. 저장장치 복구는 보통 전문 복구 업체에 맡기는 것이 일반적이지만 다수 시스템을 빠르게 복구해야 하는 경우 복구 업체를 이용하면 오히려 오랜 시간이 걸릴 수 있다.

최근까지 유행한 저장장치 파괴 악성코드의 경우 대부분 MBR, VBR, 파일시스템 메타데이터를 파괴시킨다. 이런 데이터가 파괴된 경우에는 앞서 살펴본 것과 같이 최소 복구 요건만 만족시켜주면 마운트가 가능하므로 사전에 자동화할 수 있는 방안을 마련해 사고 발생 시 피해를 최소화할 필요가 있다.

참 고 문 헌

[1] forensic-proof, “MBR”, http://forensic-proof.com/archives/435
[2] forensic-proof, “파일시스템 구조”, http://forensic-proof.com/archives/353
[3] forensic-proof, “NTFS - MFT 엔트리 소개”, http://forensic-proof.com/archives/470
[4] forensic-proof, “3.20 사이버테러 저장매체 복구 관점에서”, http://forensic-proof.com/archives/5111
[5] 이상진, “디지털 포렌식 개론”, 이룬출판사, 2010
[6] MiniTool, “Power Data Recovery”, https://www.powerdatarecovery.com/

〈저 자 소 개〉

김 진 국 (Jinkook Kim)
2011년 2월 : 고려대학교 정보보호대학원 석사 졸업
2015년 3월~현재 : 고려대학교 정보보호대학원 박사 과정
2013년 8월~현재 : 주식회사 플레인비트 대표

관심분야 : 디지털 프로파일링, 침해사고 포렌식, 디지털 증거 분석