랜섬웨어 Petya에 대한 분석과 대응방안

김선용[*] · 김기환[**] · 이훈재[***]

[*]동서대학교 컴퓨터공학부

[**]동서대학원 유비쿼터스 IT

[***]동서대학교 컴퓨터공학부

Analysis and response of Petya to Ransomware

Seon-Yong Kim[*] · Ki-Hwan Kim[**] · Hoon-Jae Lee[***]

[*]Dept. of Information and Communication Engineering, Dongseo University

[**]Dept. of Ubiquitous IT Graduate School of Dongseo University

[***]Dept. of Computer Engineering, Dongseo University

E-mail : itkindyong@naver.com, ghksdl90@naver.com, hjlee@dongseo.ac.kr

요 약

랜섬웨어는 주로 정부기관과 금융기관, 기업 등을 대상으로 파일 또는 디스크 부팅 영역을 암호화하여 금전적인 피해뿐만 아니라 개인정보 탈취 등의 보안 이슈를 초래해 왔다. 본 논문에서는 NTFS(New Technology File System) 및 랜섬웨어 Petya에 대해 설명하고, 포렌식 기법을 적용하여 감염 후를 분석하며, MBR 영역 복구에 대한 방법을 서술한다.

ABSTRACT

Ransomware has caused a lot of damage by attacking disks of government agencies, financial institutions and corporations. This has been exploited for monetary damages and Taking personal information.

In this paper, we describe the NTFS. Also describe Petya as the example of Ransomware. We used forensic techniques to analyze post-infection status and describes the method for MBR area recovery.

키워드

NTFS, MBR, MFT, VBR, Restoration

Ⅰ. 서 론

최근 보안이슈에서 빠지지 않는 보안 악성코드 관련 주제로 랜섬웨어가 있다. 랜섬웨어(Ransomware)는 컴퓨터 사용자가 이메일 혹은 악의적인 링크를 이용하였을 시 사용자의 데이터 혹은 디크스 영역을 암호화한 뒤, 금전을 요구하는 악성 프로그램이다.

2장에서는 파일 시스템의 하나의 NTFS에 대해 기술한다.

3장에선 랜섬웨어의 Petya에 대해 설명하고, 감염된 후에 디스크의 변화된 점을 기술한다.

Ⅱ. NTFS

2장에서는 NTFS와 구조에 대해 설명한다.

2.1 NTFS

NTFS는 사용자가 저장한 데이터를 읽거나, 쓰는 등 효율적으로 관리하기 위해 논리적인 접근 방식을 사용하는 것으로 사전에 정의된 기록 방식 중에 하나이다. NTFS 구조는 VBR(Volume Boot Record) 영역, MBR(Master File Table) 영역, Data Area 영역 순서로 구성되어 있다.

2.2 VBR

VBR(Volume Boot Record) 영역은 NTFS 구조에서 가장 앞부분에 위치하고, 구조는 부트 섹터와 추가적인 VBR 영역이 있다. 부트섹터는 파티션에 설치된 운영 체제를 로드 하기 위한 코드를 가질 수 있다. 추가적인 VBR 영역은 NT 로더를 빠르게 로드하기 위해 NT로더의 위치를 저장하고 있다.

2.3 MFT

MFT(Master File Table)는 파일과 디렉터리 관리 하기 위해 MFT Entry로 구성되어 있다. 일반적으로 12.5% 정도를 MFT 영역으로 할당하며, MFT Entry 0 ~ 15번은 파일 시스템 생성과 동시에 생성되는 예약된 영역이다.

III. 랜섬웨어 Petya

3장에서는 랜섬웨어 Petya에 대해 설명하고, 감염된 후에 디스크 내부 영역에 변화된 점을 기술한다.

3.1 Petya

Petya는 유저가 메일을 통해 PDF파일이나 SFX 파일로 위장한 실행파일을 다운로드한 후 UAC를 우회하지 않고 실행된다. 강제 재부팅과 MBR 영역이 변조되어 파일 접근을 할 수 없도록 한다. 그런 다음 토르 브라우저를 이용하여 몸값으로 비트코인을 요구한다.

그림 1. Petya 감염된 PC 화면

3.2 감염 후 디스크 내부 영역 변화

0번째 섹터에서 512byte 만큼의 크기를 갖는 MBR 영역은 0x37 XOR 연산으로 변조가 되지만 파티션 테이블 영역은 달라지지 않는다. 다른 영역은 악성 데이터들로 값이 변경되어 있다.

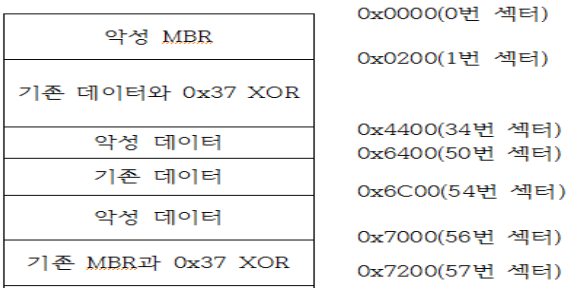

그림 2. Petya 감염된 PC 디스크 변화

3.3 MBR 영역 복구

MBR 영역은 기존의 데이터를 0x37의 값과 XOR 연산한 것으로 암호화가 아닌 변조가 일어났다. 그래서 변조된 MBR 영역만 추출하여 0x37로 다시 XOR 연산을 하면 기존의 MBR의 값으로 복구가 가능할 것이다.

IV. 결 론

본 논문에서는 랜섬웨어 Petya에 대한 분석과 대응방안에 대해서 다루었다. 분석 Petya는 단순하게 디스크의 MBR 영역을 XOR 연산을 하는거지만 변종들이 발생한다면 이보다 더 악질적인 랜섬웨어가 등장할 수도 있다. 이렇듯 사용자들은 자신의 중요한 데이터 백업은 일상화해야한다.

감사의 글

이 논문은 2016년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: NRF-2016R1D1A1B01011908).

또한 부산광역시에서 지원하는 BB21 과제에서 지원받았음.

참고문헌

[1] 이준형, 조정원, “디지털 포렌식의 세계”
[2] 이상진, “디지털 포렌식 개론”