제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

USB 기반 악성코드 감염 윈도우 피해시스템 분석 연구

최윤미*, 정지훈*, 황현욱*, 노봉남*
*전남대학교 시스템보안연구센터
e-mail:unia1012@lsrc.jnu.ac.kr

The Analysis of Windows system that infected by USB-Based Malware

Yun-Mi Choi*, Ji-Hoon Jung*, Hyeon-Uk Hwang*, Bong-Nam Noh*
*System Security Research Center, Chonnam National University

요 약

악성코드는 P2P, 전자메일, 메신저나 저장매체, 인터넷 사이트 등 여러 가지 경로를 통해 전파된다. 특히 USB 기반 악성코드는 USB가 시스템에 연결될 때 악성코드를 자동 실행시키고, 로컬 드라이브 영역에 자기복제를 하는 등 특정 행위를 보인다. 포렌식 수사에서는 이러한 악의적 행위를 빠르게 분석하고 여러 가지 증거를 수집하여 감염의 원인을 신속하게 파악하는 것이 요구된다. 본 논문에서는 USB 기반 악성코드에 감염된 시스템의 피해 흔적을 분석하고 패턴을 정형화하여 USB 기반 악성코드의 감염 여부를 판별하는 방법론을 제시한다.

1. 서론

악성코드는 인터넷의 발달과 함께 다양한 형태로 진화해왔다. 지금도 계속해서 새로운 악성코드가 등장하고 있으며, 이에 대응하여 많은 보안 업체들이 새로운 악성코드를 수집, 분석하고, 악성코드의 대응 기술을 개발하여 대처하고 있다. 하지만 지속적인 신종/변종 악성코드의 출현으로 분석 대응에는 어느 정도 한계가 존재하며, 보안 의식의 결여로 인한 사용자의 부주의나 최신 보안패치를 받지 않아 그대로 취약점이 노출되어 악성코드에 감염되는 사례가 발생하고 있다.

악성코드는 P2P를 이용한 파일 공유나 전자메일의 첨부 파일, 메신저를 통한 파일 전송과 USB와 같은 저장매체 및 악성코드가 심어진 사이트의 방문 등 많은 감염 경로를 통해 전파된다. 특히 USB를 통해 전파되는 악성코드는 USB가 시스템에 연결될 때 악성코드가 자동 실행됨에 따라 시스템에 1차 감염을 일으키고, 사용자가 감염된 시스템에 USB를 사용하면서 2차 감염을 일으킨다. 그리고 사용자가 2차 감염된 USB를 다른 시스템에 사용하면서 악성코드를 전파시켜 감염 피해가 크게 증가한다[1]. 따라서 악성코드에 감염된 시스템이 이상 행위를 보였을 때 빠르게 상황을 분석하고 신속하게 원인을 찾아 대처함으로써 피해의 확산을 줄이는 노력이 필요하다.

본 논문의 2장에서는 USB 기반 악성코드에 감염된 시스템을 분석하여 감염 원인을 판단할 수 있는 흔적을 찾는다. 3장에서는 2장에서 언급된 감염 흔적을 바탕으로 피해 시스템의 USB 기반 악성코드 감염 여부를 판별하는 방법론을 제안하고, 마지막으로 결론을 내리며 활용 방안을 기술한다.

2. USB 기반 악성코드에 감염된 시스템

악성코드에 감염된 USB 장치는 시스템에 연결될 때 autorun.inf 파일을 통해서 악성코드를 자동 실행한다[2]. 실행된 악성코드는 로컬 드라이브 영역 임의의 공간에 자신을 복제하고, 레지스트리의 자동실행 프로그램 영역에 값을 추가하여 시스템이 부팅될 때마다 악성코드가 실행되도록 한다. 그리고 다른 USB 장치가 시스템에 연결되면 악성코드가 동작하여 추가 감염을 일으키고, 그 밖에 특정 인터넷 사이트에서 다른 악성코드 파일을 다운로드하여 실행시킨다. 이러한 악성코드의 행위를 통해 시스템에 흔적이 남기게 되고, 이를 분석함으로써 USB 기반 악성코드에 감염 여부를 판별하는 근거로 제시될 수 있다.

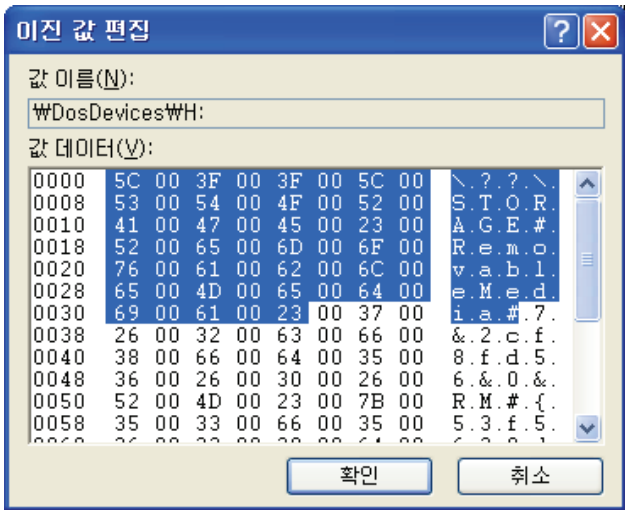
2.1 Shell Hardware Detection 서비스

Shell Hardware Detection은 윈도우에서 제공하는 서비스로 쉘(윈도우 탐색기)이 드라이브나 메모리 카드와 같은 장치를 자동으로 인식/반응하도록 지원하는 서비스이다. 이 서비스는 초기 값이 수동으로 설정되어 있으나, 자동으로 설정되어 있는 경우 USB 기반 악성코드에 감염될 수 있는 위험을 갖게 된다. USB 기반 악성코드는 autorun.inf 파일을 생성하여 악성코드를 실행하는 코드를 삽입하는데, Shell hardware detection 서비스가 자동으로 설정되어 시작된 상태인 경우 시스템에 USB를 연결시키면 autorun.inf 파일이 자동으로 실행되어 뒤따라 악성코드가 실행된다. 따라서 감염 시스템의 원인을 파악할 때 Shell Hardware Detection 서비스가 현재 시작된 상태인지의 여부와 속성의 시작 유형은 자동으로 설정되어 있는지를 조사하고, 만약 자동 실행이 가능하도록 설정되어 있다

면 USB를 통한 감염의 충분조건이 될 수 있다. 그리고 악성코드가 시스템을 감염시킨 이후 서비스를 중지시키거나 속성 정보를 변경하는 경우도 있기 때문에 이벤트 로그를 분석하여 서비스를 중지시켰거나 속성이 바뀐 기록이 남아 있는지를 확인해야 한다.

2.2 MountedDevices 레지스트리 정보

시스템에 연결된 디스크 드라이브 정보는 윈도우 레지스트리 편집기의 HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices에서 확인할 수 있으며, C:\WINDOWS\system32\config\SYSTEM 하이브 파일에 저장된다. MountedDevices 키의 값은 \??\Volume{GUID}와 \DosDevices\[드라이브명], 두 가지 형식으로 된 이름이 존재한다[3]. 여기서 \DosDevices\[드라이브명]으로 된 값의 이름은 현재 또는 가장 최근에 각 드라이브에 연결되었던 장치 정보이다. 값의 데이터는 12byte 또는 12byte 이상의 이진 데이터를 갖는데 12byte 데이터의 경우는 하드 디스크 장치의 MBR 정보를 통해 생성한 것이고, 12byte 이상의 데이터의 경우는 USB와 같이 MBR이 정보가 없는 장치에 대해 운영체제가 정의한 형식으로 임의로 생성한 값이다. USB 장치가 시스템에 연결되면 드라이브명이 할당되면서 MountedDevices 키의 값인 \DosDevices\[할당된 드라이브명]의 데이터에 장치 정보가 나타난다. 이때 레지스트리 편집기에서 해당 값의 이름에 오른쪽 마우스를 클릭하고 [수정]을 누르면 데이터를 쉽게 볼 수 있다. USB 장치에 대한 데이터는 (그림 1)에 표시된 것처럼 \??\STORAGE#RemovableMedia#로 시작한다. 따라서 악성코드에 감염된 USB가 연결되었던 드라이브를 찾기 위해서는 레지스트리 값에 나타난 모든 드라이브명에서 하드 디스크 드라이브, 플로피 디스크 드라이브, CD-ROM 드라이브에 대한 드라이브명을 제외하고 남은 드라이브명을 USB가 연결될 수 있는 드라이브 후보로 선별해내는 과정이 필요하다.

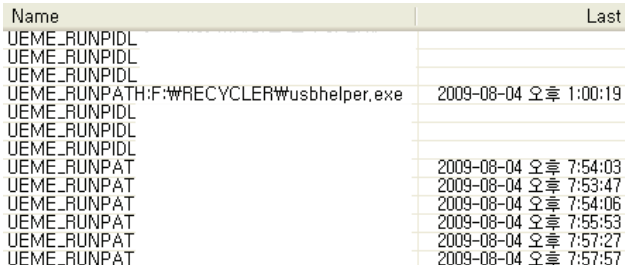


(그림 1) MountedDevices의 \DosDevices\H: 값

2.2 UserAssist 레지스트리 정보

윈도우 레지스트리의 UserAssist 영역에는 최근에 실행된 프로그램 목록이 저장된다. UserAssist 정보는 윈도우 레지스트리 편집기의 HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist에서 확인할 수 있으며, 시스템 드라이브의 C:\Documents and Settings\[사용자 이름]\NTUSER.DAT 파일에 저장된다. UserAssist 키는 전역 고유 식별자(GUID)로 된 두 개의 서브키를 가지는데 {5E6AB780-7743-11CF-A12B-00AA004AE837}는 Internet Toolbar에 대한 정보이고, 다른 서브키 {75048700-EF1F-11D0-9888-006097DEACF9}는 ActiveDesktop에 대한 정보이다. USB가 시스템에 연결될 때 악성코드가 실행되면 {75048700-EF1F-11D0-9888-006097DEACF9} 키의 서브키인 Count에 실행 정보가 남게 된다. Count 키에 남은 정보는 실행 파일의 경로, 실행 횟수, 마지막으로 실행된 시간 정보이다[4]. 윈도우 레지스트리 편집기에서는 값의 이름 정보가 ROT13으로 인코딩 되어있고, 값의 데이터는 이진 형식으로 나타나므로 디코딩 및 분석이 필요하다.

(그림 2)는 UserAssist에 남아있던 악성코드 usbhelper.exe의 실행 정보를 도구를 사용하여 보여준 것이다. usbhelper.exe가 USB 기반 악성코드라는 것을 모르는 상태에서 이 정보를 확인했다면 먼저 F:\ 드라이브가 USB가 연결될 수 있는 드라이브인지를 조사해야 한다. 그리고 USB 연결이 가능한 드라이브라면 F:\ 드라이브에서 실행된 실행 파일은 USB 기반 악성코드일 가능성이 있고, 악성코드로 의심되는 실행 파일이 8월 4일 오후 1시 19초에 실행되었음을 알 수 있다. 만약 (그림 2)에 나온 실행 파일 정보 외에 USB 후보 드라이브에서 실행된 실행 파일이 있다면 악성코드로 의심될 수 있고, 따라서 USB 후보 드라이브에서 실행된 모든 실행 파일 정보를 추출해야 한다.



(그림 2) UserAssist의 실행 파일 정보

2.4 Prefetch 정보

윈도우에서 제공하는 프리패치 캐쉬 서비스는 실행 파일이 사용하는 시스템 자원 정보를 특정 파일에 미리 저장하여 사용자가 파일을 실행할 때 미리 저장된 정보를 통하여 실행 속도를 향상시키기 위한 윈도우 제공 서비스이다[5]. 프리패치 파일은 C:\Windows\Prefetch 폴더에 [실행파

일명.exe-Hash].pf 형식으로 생성되며, 이때 Hash는 실행파일이 존재하는 경로의 해쉬 값이다[6]. 파일에는 실행 위치(디스크 볼륨)와 실행 시간, 실행 횟수 및 참조 목록 리스트 등의 정보를 포함하고 있으며, 해당 실행 파일이 삭제되어도 프리패치 파일은 제거되지 않고 그대로 남아있다. 따라서 USB가 시스템에 연결되어 악성코드가 자동 실행되면 악성코드의 프리패치 파일이 생성되고, 그 이후 USB 장치가 시스템에서 해제되면서 USB 드라이브의 악성코드 파일이 제거되어도 해당 악성코드의 프리패치 파일이 남아 분석에 활용할 수 있다.

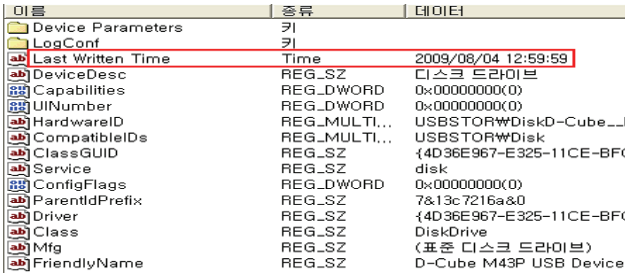
(그림 3)은 악성코드 usbhelper.exe가 실행되고 Prefetch 폴더에 생성된 USBHELPER.EXE-31EA7891.pf 파일을 분석한 결과이다. 앞의 UserAssist 정보에서 USB 후보 드라이브에서 실행된 실행 파일 정보를 추출해냈다면, 실행 파일명(usbhelper.exe)이 같고 실행된 시간(8월 4일 오후 1시 19초)이 같은 프리패치 정보를 추출하여 참조 목록 리스트와 실행된 위치 정보를 알 수 있다.

(그림 3) 프리패치 분석 정보

2.5 USBSTOR 정보

USB 장치가 시스템에 연결되면 레지스트리 HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR 키의 아래에 [장치 클래스ID] 서브키가 생성되며, [장치 클래스ID] 아래에 해당 장치를 유일하게 식별하는 [인스턴스ID] 서브키가 생성되어 장치에 대한 정보가 저장된다. 이 [인스턴스ID] 키의 값에는 클래스, 클래스GUID, 하드웨어ID를 포함한 몇몇 정보가 저장되는데[7], 여기서 주목해야 할 정보는 USB 장치가 시스템에 연결될 때, [인스턴스ID] key가 생성되면서 저장된(또는 업데이트된) 타임스탬프 정보이다. 이 정보는 Last Write Time, 즉 USB 장치가 마지막으로 연결된 시간으로 해석될 수 있으며 윈도우 레지스트리 편집기에서는 이 값을 제공하지 않는다. 따라서 Last Write Time 값을 확인하기 위해서는 레지스트리 구조를 분석하여 찾거나 레지스트리의 시간 정보까지 제공해주는 도구를 사용해야 한다.

(그림 4)는 시스템에 연결된 USB 장치 정보에 대한 레지스트리 정보를 분석한 결과이다. 시스템에 연결된 USB 장치는 D-Cube M43P USB Device이며 이 장치가 연결된 시각은 8월 4일 오후 12시 59분 59초이다. 따라서 이 USB 장치가 연결된 이후 usbhelper.exe가 실행되었음을 알 수 있다. 이처럼 앞에서 악성코드로 의심되는 실행파일 정보를 추출했다면 실행된 시간 정보와 시스템에 연결된 USB 장치의 연결 시간 정보를 비교하여 파일이 실행된 시간 바로 이전에 연결된 장치를 찾는다.



(그림 4) 시스템에 연결된 USB 장치 정보

3. USB 기반 악성코드 감염 판별 방법론

피해 시스템의 USB 기반 악성코드 감염 여부를 판별하는 방법론은 총 3가지 단계로 나뉜다. 1단계는 피해 시스템의 환경을 분석하는 단계로, USB 장치가 시스템에 연결될 때 악성코드가 자동 실행될 수 있도록 설정되어 있는지 조사하고, MountedDevices 레지스트리 데이터를 분석하여 피해 시스템의 USB 후보 드라이브를 식별한다. 2단계는 악성코드의 실행 흔적을 분석하는 단계로 UserAssist 레지스트리 데이터와 프리패치 데이터를 분석하여 USB 장치에서 실행된 악성코드 정보를 추출해낸다. 마지막 3단계는 USB 장치를 매칭하는 단계로 USBSTOR 레지스트리 데이터를 분석하여 시간 정보를 대조해 매칭되는 USB 장치를 추출해내는 단계가 되겠다. USB 기반 악성코드의 판별 흐름도는 (그림 5)와 같다.

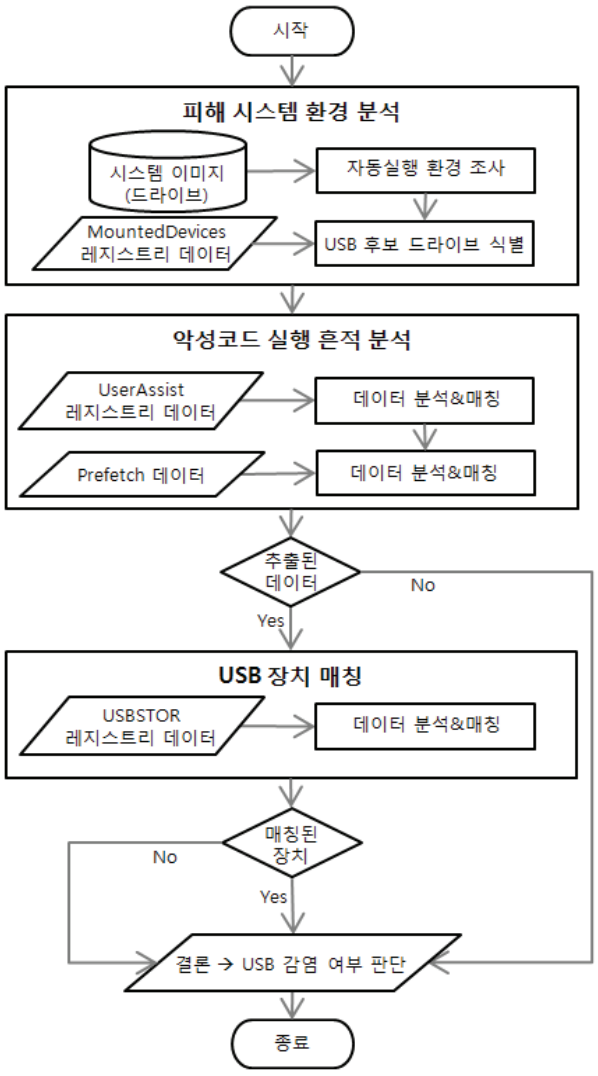
3.1 피해 시스템 환경 분석

악성코드에 감염된 피해 시스템을 가지고 시스템 환경 분석을 실행한다. 시스템이 USB 기반 악성코드가 자동 실행될 수 있도록 설정되어 있는지 확인하기 위해서 윈도우의 Shell Hardware Detection 서비스 정보를 조사한다. 그 다음 MountedDevices 레지스트리 데이터를 파싱하고,

모든 \DosDevices\[드라이브명] 값의 데이터를 분석하여 USB 드라이브로 사용될 수 있는 후보 드라이브명을 추출한다. 이때 추출된 드라이브명은 악성코드에 감염된 USB 장치가 연결되었던 드라이브 후보가 되어 다음 단계로 데이터가 전달된다.

3.2 악성코드 실행 흔적 분석

악성코드 실행 흔적 분석 단계에서는 피해 시스템 환경 분석 단계에서 추출된 USB 후보 드라이브명 데이터를 가지고 진행된다. 먼저 UserAssist 레지스트리 데이터를 분석하여 모든 실행 파일 정보를 추출해낸다. 실행 파일 경로의 드라이브명과 USB 후보 드라이브명이 매칭되는 실행 파일 정보를 추출한다. 이렇게 추출된 정보는 프리패치 데이터를 분석하여 추출된 실행 파일 정보의 파일명과 시간 데이터를 매칭시켜 추가 정보를 획득한다. 이 단계에서 마지막으로 추출된 실행 파일 데이터들은 USB 기반 악성코드의 후보군이 된다.



(그림 5) USB 기반 악성코드 판별 흐름도

3.3 USB 장치 매칭

악성코드 실행 흔적 분석 단계에서 추출된 악성코드 후보군 데이터는 파일의 실행 시간 정보를 포함하고 있다. 따라서 USBSTOR 레지스트리 데이터를 분석하여 시스템에 연결되었던 USB 장치와 그 데이터를 추출해내고 악성코드 후보군의 실행 시간 정보와 USB 장치 연결 시간 정보를 매칭시킨다. USB 장치가 연결된 시점과 악성코드가 실행되는 시점은 시스템별로 약간의 시간차가 존재할 수 있다. 따라서 악성코드 후보군의 파일 실행 시각 이전의 임계치 시간 내에 연결된 USB 장치를 찾아 매칭되는 USB 장치가 있는지 확인한다. 만약 매칭되는 USB 장치가 있다면 해당 장치가 시스템에 연결되었을 때 악성코드가 자동 실행된 것으로 판단하여 USB를 통한 감염임을 판별할 수 있다.

4. 결론

본 논문에서는 USB 기반 악성코드에 감염된 시스템의 피해 흔적을 분석하여 피해 시스템의 감염 원인이 USB 기반 악성코드에 의한 것인지 판별하는 방법론을 제시하였다. 이 방법론을 기준으로 피해 시스템에 대한 USB 기반 악성코드 감염 여부를 빠르게 판별할 수 있고, 포렌식 수사에 증거로 활용이 가능하다.

향후에는 USB 기반 악성코드뿐만 아니라 P2P나 이메일, 인터넷 사이트 등을 통한 악성코드 감염 시스템의 피해 흔적을 분석하고 통합 설계함으로써, 피해 시스템의 감염 원인을 빠르게 판별하는 도구를 개발하여 포렌식 수사에 활용할 수 있도록 한다.

참고문헌

[1] 한국정보보호진흥원, “USB 이동형 저장장치를 이용하여 전파되는 악성코드 분석”, 2, 2008

[2] Stephane St-Michel, Brian Aust, "Autoplay in Windows XP: Automaticcally Detect and React to New Devices on a System", MSDN, http://msdn.microsoft.com/en-us/magazine/cc301341.aspx, November, 2001

[3] Harlan Carvey, Cory Altheide, "Tranking USB storage: Analysis of windows artifacts generated by USB storage devices", Digital Investigation, 2005

[4] AccessData, "Understanding the UserAssist Registry Key", ACCESSDATA SUPPLEMENTAL APPENDIX, Sep, 2008

[5] 이동찬, 박정흠, 이상진, “삭제된 실행파일 분석에 활용 가능한 윈도우 프리패치 데이터베이스 구축”, 디지털 포렌식 기술 워크샵, 2009

[6] Allan S Hay, “Windows File Analyser Guidance”, WFA Guidance, November, 2005

[7] Harlan Carvey, "Windows Forensic Analysis DVD Toolkit", SYNGRESS, 2007