情 報 保 護 學 會 誌
第21卷 第7號, 2011. 10

스턱스넷(Stunxet)의 감염 경로와 대응방안

허 재 준*, 이 상 철**

요 약

2010년에 최초로 발견된 스턱스넷(Stuxent)은 2011년 한해 동안 보안업계 사이에서 많은 논란이 되었다. 이는 악성코드가 사이버 무기가 될 수 있다는 가능성을 현실로 만들었고, 기술적으로도 현존하는 악성코드의 모든 기술이 포함 될 정도로 정교하고 복잡한 것으로 평가받고 있다. 특히 2011년에는 스턱스넷의 소스코드 일부가 공개되어 스턱스넷의 두 번째 버전으로 알려진 변형Duqu가 나타나기도 하여 변형에 따른 공격 우려도 높아지고 있다. 이번 논문에서는 과거 발생한 스턱스넷을 알아보고 유사한 사이버 공격에 대비하기 위한 대응 방안도 함께 살펴 볼 예정이다.

Ⅰ. 서 론

2011년의 보안 키워드 중 빼놓을 수 없는 부분은 스턱스넷(Stuxnet)과 같은 사이버 무기로 사용될 수 있는 악성코드를 빼 놓을 수 없을 것이다. 스턱스넷은 2010년부터 꾸준히 해외 보안 컨퍼런스에서도 빼 놓을 수 없는 단골 주제로 삼을 만큼 큰 관심을 끌고 있다. 특히 그 동안 보아왔던 악성코드와는 다른 특정 산업 시스템을 공격 대상으로 삼고 있으며, 발견 초기에는 알려지지 않은 취약점을 이용한 공격과 특유의 복잡한 구조로 인하여 분석을 더욱 어렵게 하였다.

Ⅱ. 스턱스넷(Stuxnet)에 대한 이해

2.1 발견과 이슈의 시작

스턱스넷(Stunxet)은 2010년 7월 벨라루스(Belarus)에 본사를 두고 있는 바이러스블로카(VirusBlockAda)라는 보안회사가 최초로 발견, 보고한 것으로 기록되고 있다. 최초 발견날짜와는 다르게 스턱스넷에 일부 파일의 빌드(Build)된 날짜가 2009년 1월로 되어있는 것으로 보아 2009년 중반이나 그 이전부터 확산된 것으로 추정된다. 영문 'Stuxnet'의 이름은 코드에 'Stuxnet'으로 시작하는 명칭이 많아 붙여진 이름으로 알려졌다.

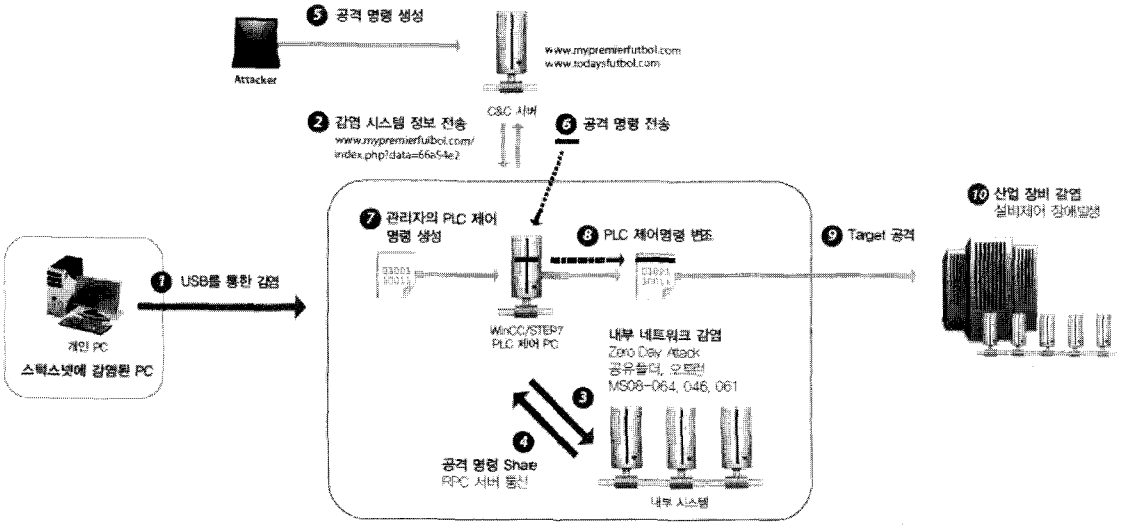
스턱스넷은 발견 초기에 모듈의 일부분만 수집되어 전체 기능을 파악하기가 쉽지 않았으며, 감염이나 증상이 나타나는 상황을 재현할 수 없어 분석에 많은 시간이 소요되었다. 이후 전세계의 많은 보안전문가와 업체들이 분석을 진행하면서 스턱스넷의 공격 대상이 보편적인 컴퓨터 환경이 아닌 집중 원격감시 제어데이터수집 시스템인 SCADA(Supervisory Control And Data Acquisition)의 일종이라는 것이 확인되었다. SCADA 시스템은 국가 및 산업의 중요 기반 시설에 주로 사용되고 있는데, 이 사실이 알려지면서 그 동안 공격 사나리오나 영화등에서 가설로만 언급되던 기계 설비나 장치 등에 물리적인 피해를 줄 수 있는 사이버 테러의 실체와 심각성이 현실화 되었다. 그리고 곧 스턱스넷은 세계적인 보안 이슈가 되었다.

2.2 공격 대상 시스템에 대한 이해

스턱스넷은 일반적인 사용자 컴퓨팅 환경에서는 기능이 정상적으로 동작하지 않는다. 또한 다양한 전파 방법에 의해 일반 컴퓨팅 환경에서 감염되었다 할지라도 원하는 조건이 불충분하다면 동작하지 않는다. 현재 발견된 스턱스넷의 동작 환경은 SCADA라고 불리는 발전소, 공항 철도 등과 같은 기간시설에 매우 폭넓게 사용되는 시스템이다.

스턱스넷은 SCADA 시스템 중 독일 지멘스(Siemens)사의 SIMATIC PCS7 시스템을 공격하도록 설계

* 안철수연구소 (jaejun@ahnlab.com)
** 안철수연구소 (chita000@ahnlab.com)



〔그림 1〕 스턱스넷 악성코드의 감염과 동작 원리

되어 있다. PCS7의 다양한 컴포넌트 중 SIMATIC WinCC7와 SIMATIC Step7이라 불리는 통합 관리도구를 공격 대상으로 삼고 있다. SIMATIC WinCC는 통제 및 모니터링 시스템으로서 PLCs(Programmable logic controllers)와 통신을 담당하는 소프트웨어인데, 스턱스넷은 WinCC의 존재하는 취약점을 이용하여 침투하게 된다. 또 다른 컴포넌트인 Step7은 제어 PC와 산업자동화 제어시스템간에 블록(동작명령)파일 교환을 담당한다. 스턱스넷은 Step7의 일부 구성 요소를 자신이 생성한 파일로 교체시켜 산업자동화 제어 시스템을 모니터링 하거나 임의의 블록(악성 명령어 블록)을 생성시켜 제어하게 된다. 이렇게 장악된 시스템은 공격자가 의도한 명령으로 동작하게 되는데, 현재 발견된 스턱스넷은 모든 PLC의 영향을 주진 않고, PLC 타입 6ES7-315-2와 6ES7-417만 감염의 영향을 받는 것으로 알려졌다.

2.3 피해사례

스턱스넷의 공격 대상이 분석을 통해 알려진 후 감염 정도와 피해를 입은 사례가 언론을 통하여 알려지기 시작했다. 전체 감염 사례의 60%가 이란(Iran)에 집중되어 있으며, 중국에서는 600만대의 컴퓨터와 1,000여 곳의 산업설비 시설이 감염된 것으로 보도 되었다. 감염 사례가 많은 이란의 핵 시설에 사용된 소프트웨어들은 대부분 불법 소프트웨어인 것으로 알려져 있다. 국내에서는 아직 감염으로 인한 어떠한 피해 사례도 접수되지 않은 상황이다.

Ⅲ. 스턱스넷(Stuxnet)에 다양한 확산 방법

3.1 네트워크를 통한 전파 방법

스턱스넷은 네트워크 공유 폴더 및 윈도우 서버 서비스 취약점을(MS08-067)을 사용하여 확산을 시도한다.

3.1.1 공유 폴더를 이용한 전파

스턱스넷은 자신의 전파를 위해 공유 폴더를 이용하는데, NetShareGetInfo API를 이용하여 같은 네트워크에 존재하는 시스템의 C$와 Admin$를 검색하게 된다. 여기서 검색된 공유 폴더가 쓰기가 가능하다면, 'DEFRAGXXX.TMP'라는 파일명으로 스턱스넷의 메인 파일 모듈을 생성하게 된다. 이 파일의 파일명 마지막 3자리 'XXX'는 GetTickCount API를 사용하여 랜덤하게 파일명을 만들어낸다.

3.1.2 MS08-067 취약점을 이용한 전파

스턱스넷의 네트워크를 통한 확산 방법 중 두 번째는 윈도우 서버 서비스 취약점을 이용하는 것이다. 스턱스넷

은 매우 다양한 취약점을 이용하여 전파되는데, 그 중 윈도우 서버 서비스 취약점은 RPC Service 관련 취약점에 해당한다. 이것은 NetPathCanonicalize 오버플로우(Overflow)로 인해 원격코드가 실행되는 취약점이다. 재미있는 점은 스턱스넷에서 사용하는 몇 가지 확산 방법은 과거 네트워크 웜으로 유명했던 컨피커(Conficker)웜에 의해 사용되었으며, MS 보안 패치가 제공되고 있다.

공격자는 윈도우 서버 서비스에서 원격 코드 실행이 가능한 취약점이 존재한다는 것을 알고 조작된 RPC (Remote Procedure Call) 요청을 전달하는 방식으로 시스템을 장악할 수 있다. 스턱스넷도 이 취약점을 그대로 이용하여 원격 코드 실행이 가능한 상태로 만든다. 스턱스넷은 이 취약점을 무조건 이용하지 않고, 다음의 조건을 만족해야만 수행하도록 설계되어 있다.

- 감염 시스템의 날짜가 2030.1.1. 이전
- 몇 가지 Anti-Virus의 시그니처 버전을 조사하여 시그니처 날짜가 2009.1.1. 이전
- Kernel32.dll과 Netapi32.dll의 패치 날짜가 2008.10.12. 이전

3.1.3 MS10-061 취약점을 이용한 전파

원격 시스템에 프린터가 공유되고 있고 문서 프린트를 위한 연결이 설정되어 있다면 공격자는 윈도우 API를 이용해서 원하는 데이터를 원격 시스템에 복사할 수 있다. 스턱스넷은 이런 점을 이용하여 프린트 스플러 제로제이(Zero-day) 공격으로 네트워크를 통한 자신의 확산을 가능하게 했다.

이 취약점은 2009년 4월에 IT 보안 매거진인 'Hackin9'에 의해 'Print your shell'란 주제로 처음 소개되었다. 그 중 타깃(Target) 시스템에 데이터를 복사하기 위해 공유된 프린터를 사용하는 부분을 이용하여 스턱스넷은 드롭퍼 기능이 있는 메인 DLL을 'Winsta.exe'이라는 이름으로 타깃 시스템의 '시스템' 폴더에 복사한다. 이 공격이 성공하기 위해서는 타깃 시스템에 파일과 프린터 공유가 사용 가능하게 활성화되어 있어야 한다. 그러나 이 취약점은 게스트(Guest) 계정으로 단지 파일 쓰기만 허용되었기 때문에 복사한 파일을 실행하기 위한 방법이 필요했다. 그 방법은 'Winsta.exe'를 실행하기 위한 WMI 코드가 포함되어 있는 WMI BMF(Binary Managed Object Format) 파일인 'Sysnullevnt.mof' 파일을 MOF 자체 설치 디렉터리인 '(시스템폴더)\wbem\mof'에 생성하는 것이다. 이 폴더에 있는 파일은 자동적으로 컴파일되고 등록되는 과정을 통해 자신을 전파시킨다.

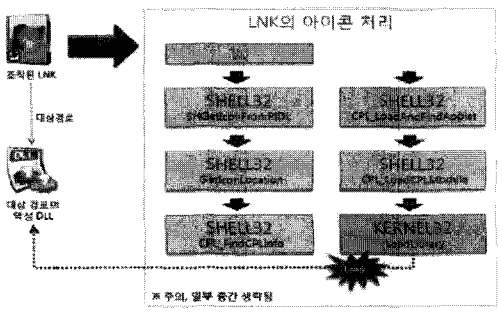
3.2 이동식 저장 매체(USB)를 이용한 전파 방법

스턱스넷의 대표적인 확산 방법인 LNK 취약점을 이용한 전파 방법은 2010년 7월에 MS에서 발표되었던 '악의적으로 조작된 LNK,PIF 파일'을 통해 원격의 코드를 사용자의 권한으로 실행할 수 있는 취약점이다.

이 취약점은 '제어판 바로가기'의 아이콘을 탐색기에 보여주는 과정에서의 부적절한 모듈 로드로 인해 발생한다.이로 인해 사용자가 탐색기나 유사 커맨더 프로그램 등을 이용해 바로가기의 아이콘을 로딩하는 순간 대상 파일로 지정된 파일이 사용자 권한으로 로드되는 취약점이 발생한다.

스턱스넷은 이동식 저장 매체인 USB를 통한 전파 과정에서 Autorun.inf를 통한 감염과 더불어 LNK 취약점을 이용한 감염을 모두 이용한다. LNK 취약점을 이용한 USB 감염은 대상 파일의 경로를 지정하는데 어려움이 있다. 이유는 시스템마다 USB의 물리적인 경로가 달라지기 때문이다. 이러한 한계를 극복하고 확실하게 감염 동작을 수행하기 위해 스턱스넷은 네 가지 종류의 바로가기를 생성하는 치밀함을 보여주고 있다.

- Copy of Shortcut to.lnk
- Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Copy of Shortcut to.lnk



〔그림 2〕 취약점이 발생하는 LNK 처리 과정

위와 같은 이름으로 생성된 LNK 파일들이 로드하는 스턱스넷 메인 모듈의 이름은 아래의 두 가지 이름으로 존재한다.

- "~WTR4141.tmp"
- "~WTR4132.tmp"

이 모듈은 역시 스턱스넷의 메인 모듈에 해당하는데, 취약점이 존재하는 LNK 파일을 다양한 이름을 만들고, 이 LNK 파일이 다시 메인 모듈을 로드하는 식으로 제작하였기 때문에 취약점이 존재하는 시스템에서는 탐색기로 파일 목록을 보기만 해도 감염 동작이 시작된다.

3.3 권한 상승 취약점을 이용한 스턱스넷의 실행

스턱스넷이 이용한 또 다른 취약점은 'Win32k.sys' 내의 키보드 레이아웃을 로딩할 때 함수 포인터의 인덱스를 체크하지 않아 발생하는 권한 상승 취약점이다. 윈도우XP/2000에서 일반 계정, 즉 관리자 권한이 아닌 곳에서 스턱스넷이 실행될 때 해당 취약점을 이용하여 악성 쉘코드를 실행하게 된다. 이렇게 실행하게 되면 스턱스넷은 항상 관리자 권한으로 실행되므로 시스템의 모든 부분을 이용할 수 있게 된다.

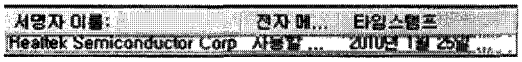
Ⅳ. 스턱스넷이 사용하는 자기 보호 기술

스턱스넷은 여러개의 드라이버 파일을 사용하여 자신을 로드 하는데 사용하거나 자신을 보호하는데, 이용한다. 드라이버를 이용한다는 것은 커널 레벨 기술을 이용하여 좀 더 강력한 자기 보호 기술을 실현하는 것을 의미하며, 이러한 기술을 통하여 악성코드 자체의 생존 시간을 늘리게 된다.

4.1 파일 은폐 루트킷(Rootkit) 드라이버

스턱스넷은 이동식 디스크를 통하여 확산시에 "Mrxnet.sys"라는 루트킷 드라이버를 통하여 .LNK파일을 은폐시키는데, 무조건 모든 .LNK파일을 은폐시키지는 않고 다음의 조건을 따져 은폐하도록 설계되어 있다.

- 파일의 확장자가 ".LNK"이며, 파일의 사이즈가 1,471 bytes(변형에 따라 사이즈는 변경될 수 있다.)



〔그림 3〕 정상 파일처럼 위장하기 위해 Realtek 디지털 서명을 도용

- 파일의 확장자가 ".tmp"이며, 파일의 사이즈가 4,096~8,388,608 bytes 이며, 파일 이름의 길이가 12이고 첫 번째 문자열이 "~"이다. 그리고 5번째 bytes부터 나오는 숫자의 합이 10이어야 한다. (예, ~WTR4321.tmp) 이 루트킷 드라이버는 정상 파일처럼 위장하기 위해 "Realtek" 디지털 서명을 가지고 있다.

4.2 파일 로드 포인트(Load Point) 드라이버

로드 포인트(Load Point)루트킷은 스턱스넷에서 지정된 프로세스에 악성 모듈을 삽입 후 실행을 목적으로 한다. 스턱스넷의 악성 핵심 모듈이 모두 메모리상에 복호화하고, 동작을 하기 때문에 PC의 재부팅 시 메모리는 모두 소멸된다. 따라서 스턱스넷은 로드 포인트 루트킷을 이용하여 재부팅 시점에서 다시 감염을 시켜 동작하려는 목적을 가지고 있다.

로드 포인트는 "Mrxcls.sys"라는 파일명으로 존재하며, 재부팅 시 인젝션 될 프로세스를 찾아 인젝션을 시도하는데, 대상 프로세스명은 "oemXX.PNF" 형식으로 암호화 되어 있다.(여기서 XX는 랜덤 한 이름) 이 암호화된 데이터를 해제하면 아래의 프로세스 리스트를 인젝션 대상으로 삼고 있다는 것을 알 수 있다.

〔표 1〕 모듈 정보에서 복호화된 프로세스 이름

프로세스 이름	암호화 모듈 정보
services.exe	oem7A.PNF
S7tgtopx.exe	oem7A.PNF
CCProjectMgr.exe	oem7A.PNF
explorer.exe	oem7M.PNF

Ⅴ. 스턱스넷의 명령 및 제어 기능

일반적인 봇(Bot)류의 악성코드와 같이 스턱스넷도 제작자 또는 악의적인 배포자의 명령을 받아 수행하는 Bot기능이 존재한다. 이 기능은 C&C서버로부터 명령

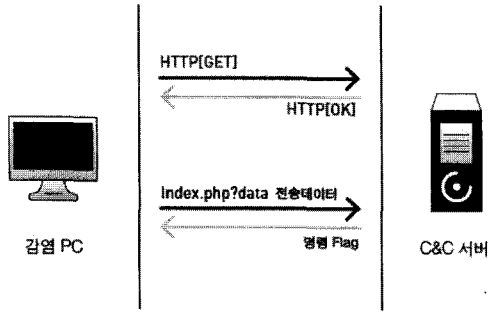
을 전송받거나 수집한 정보를 전송하는 방식으로 이루어지는데, 이 기능을 수행하기에 앞서 윈도우 업데이트 사이트(windowsupdate.com)과 MSN사이트(msn.com) 도메인으로 DNS쿼리 후 성공하면, 다음의 C&C서버로 접속하게 된다.

- www.mypreminrfutbol.com
- www.todaysfutbol.com

위 도메인은 각각 말레이시아와 덴마크에 위치한 것으로 알려졌으며, 서버는 더 이상 동작하지 않는다. C&C 서버 운용의 주요 목적 중 하나는 감염된 시스템의 정보를 수집 후 전송하는 것인데, 시스템이 C&C 서버와 통신에 성공하면, 다음의 정보를 C&C 서버로 보낸다.

- 감염된 시스템의 컴퓨터 이름
- 감염 시스템의 도메인 이름
- 운영체제 종류와 버전
- Step7, WinCC의 설치 여부(SCADA시스템 운용 소프트웨어)

이러한 통신을 할 때 스턱스넷은 iexplorer.exe 또는 기본 웹 브라우저 프로세스에 인젝션하여 동작하게 된다. 이유는 인터넷 연결시 다른 프로세스라면 의심의 여지가 있지만, 웹 브라우저가 하는 일 자체가 인터넷 연결이기 때문에 상당히 자연스러운 작업으로 위장할 수 있기 때문이다. 따라서 감염 시스템에 대한 분석이나 일반 사용자가 이를 알아채기가 쉽지 않다.



〔그림 4〕 감염된 시스템과 C&C 서버 간의 통신 흐름

Ⅵ. SCADA 시스템 공격이 최종 목적

스턱스넷은 SCADA(Supervisory Control and Data Acquisition, 이하 SCADA)라는 특정 산업용 시스템을 공격 목표로 하고 있는데, 이러한 공격은 스턱스넷이 지멘스사의 SCADA 시스템에서 사용되는 전용 소프트웨어의 여러 취약점을 이용하면서 가능해졌다.

6.1 특정 SCADA 시스템을 공격 대상으로 선정

SCADA 시스템은 생산 공정을 감시하고 제어하기 위해 산업체에서 사용되는 시스템으로, PLCs(Programming Logic Controllers)라고 불리는 시스템을 통해 연결된다. 스턱스넷의 공격 목표는 이 PLCs에 전달되는 관리자의 제어명령 코드 블록을 변조시켜 악의적인 동작을 발생시키는 것이다. SCADA 시스템은 여러 제조/공급 업체가 존재하지만, 스턱스넷은 지멘스사의 SCADA 시스템을 공격 목표로 삼았다.

6.2 운용 소프트웨어 장악을 위한 모듈 변조

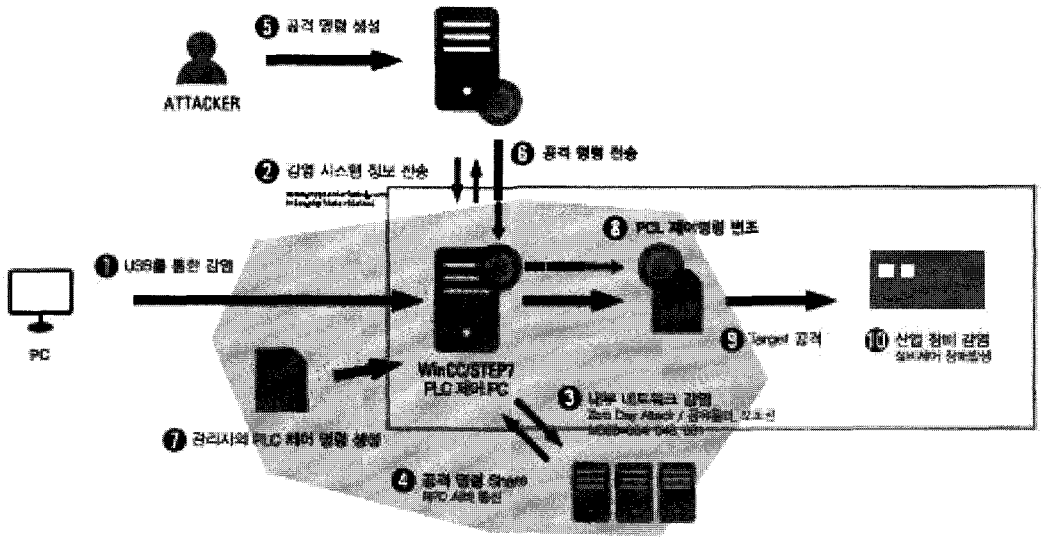
공격의 최종 목표는 SCADA시스템이 악의적인 제작자가 원하는 대로 움직이도록 하는 것인데, 이를 위해서는 각종 운용 소프트웨어를 장악해야 한다. 스턱스넷은 이를 위해 SIMATIC Step7이라는 운영에 관련된 소프트웨어의 각종 취약점을 이용하게 된다.아래 표는 분석을 통하여 밝혀진 Step7 소프트웨어 모듈 중 후킹 또는 변조 대상이 되는 파일 목록이다.

6.3 PLC코드 블록 변조를 통한 제어 시스템 공격

스턱스넷의 최종 목표는 PLC코드 블록 변조를 통하여 제어 시스템이 의도하지 않은 동작을 수행하게 하는

〔표 2〕 변조되는 Step7 소프트웨어 모듈

파일명	변조 형태 및 용도
s7tgtopx.exe	메인 실행 파일로서 이 프로세스를 오픈하고 함께 로드된 파일을 메모리상에서 변조시킨다.
s7apromx.dll	Step7의 OM Project 모듈
mfc42.dll msvcrt.dll	정상 파일이지만, 일부 API를 후킹하는 용도로 사용된다.
Ccprojectmgr.exe	WinCC관련 실행 파일



〔그림 5〕 붉은 선으로 표시된 부분이 명령어 변조가 나타나는 부분

〔그림 6〕 교체된 s7otbxdx.dll로 변조된 명령어 전송

것에 있다. Step7소프트웨어와 PLC사이에 통신을 담당하는 정상적인 "s7otbxdx.dll" 파일을 "s7otbxsx.dll" 이라는 이름으로 변경시키고, 원본 "s7otbxdx.dll"파일을 악의적인 파일로 교체하면서 동작하게 된다.

정상적인 파일이 교체된 상태에서는 악의적인 목적을 가진 제작자가 언제든지 의도한 명령으로 정해진 시스템을 공격할 수 있게 된다. 특히 산업용 시스템에서는 오작동으로 치명적인 결과를 초래할 수도 있다. 이러한 환경은 일반적인 환경에서는 쉽게 접할 수 없기 때문에 일반적인 악성코드를 제작하듯이 제작하는 데에는 한계가 존재한다. 따라서 공격 대상 시스템의 구성과 환경 및 사용되는 소프트웨어를 정확하게 파악하고 있는 전문 그룹에 의하여 제작되었을 것으로 추측하고 있다. 또한 악성 제작자가 변조하는 PLC제어 명령어는 스턱스넷의 또 다른 기능인 C&C(Command and Control) 기능을 통하여 수정/업데이트 될 수 있다.

Ⅶ. 스턱스넷의 미래와 대응 방안

7.1 화이트 리스트 기반의 보안 대책

초기에 발견된 스턱스넷은 특정 산업용 시스템의 동작을 방해할 목적으로 전문적으로 제작된 악성코드였다. 기술적으로는 지금까지 알려진 웬만한 악성코드의 기능을 모두 포함하고 있으며, 알려지지 않은 취약점을 이용한 감염 기법은 전문 집단에 의해 제작 되었다는 것을 짐작할 수 있다. 이것을 시발점으로 앞으로도 이와 유사한 형태의 전문적인 악성코드가 제작될 가능성이 높고 실제도로 2011년 10월에는 스턱스넷에 두 번째 버전이라고 알려진 Duqu가 발견되기도 하였다. 악성코드의 특성상 특정 시스템을 노리기 때문에 범용적인 안티바이러스(Anti-Virus)제품에만 의존하기보다는 운용환경 분석에 따른 추가적인 방어 대책이 필요하다.

산업용 시스템은 운영을 담당하는 관리자가 지정한 소프트웨어만이 허용된다는 가정하에 화이트 리스트(White List) 기반의 보안 정책을 세울 수 있다. 보편적으로 안티바이러스 프로그램은 블랙 리스트(Black list) 기반에 알려진 악성코드 혹은 학습된 알고리즘에 의하여 비슷한 유형의 악성코드만을 발견하는 방식을 가지고 있다. 이와 반대로 허용된 소프트웨어 또는 행위만이 동작할 수 있도록 하는 것이 화이트 리스트기반의 정책이라 할 수 있다. 이러한 화이트 리스트 정책은 작은 보

안 사고라도 커다란 재앙이 될 수 있는 환경에서는 기존 안티바이러스 기반의 보안 대책보다는 한 단계 상향된 방법이라 할 수 있다.

7.2 기본에 충실한 보안 대책

대부분의 산업용 시스템 환경은 폐쇄된 환경 구축을 원칙으로 하고 있다. 하지만 해외에서 스턱스넷의 피해가 발생한 사례가 실제로 있다는 것은 어딘가에 분명 보안상 허점이 존재한다는 것을 보여주고 있다. 이러한 사고의 상당수는 기본적인 보안 수칙을 지키지 않아 발생한 경우인데, 몇 가지 단순한 기본 보안 수칙을 소개하며 논문을 마친다.

- 피해가 발생한 시스템에서 사용된 소프트웨어는 대부분 불법 복제된 소프트웨어였다고 한다. 따라서 반드시 정품 소프트웨어를 사용하여 제작사의 지속적인 업데이트 서비스를 받아야한다.
- 하드웨어의 납품 과정이 투명하지 않은 제품을 확인 없이 그대로 반입하여 사용하는 경우는 없어야 한다.
- 외부 시스템은 꼼꼼한 보안 검수 후 내부에 반입되어야 한다. (이동식 디스크)
- 보안 담당자들의 꾸준한 교육과 시대에 맞는 보안 기술향상이 필요하다.

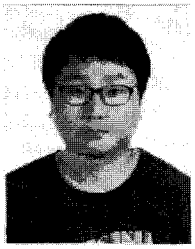
참고문헌

[1] 안철수연구소, 월간 安 "*스턱스넷 기술 분석 보고서*", 안철수연구소, 1월-4월 2011

[2] Nicolas Falliere, Liam O Murchu, Eric Chien "*W32.Stuxnet Dossier*", Symantec, November 2010

[3] Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho "*Stuxnet Under the Microscpe*", ESET, 2010

〈著者紹介〉



허 재 준 (Heo, Jaejun)
비회원
2004년 2월: 인덕대학교 전산과 졸업
2009년~현재: 한국방송통신대학교 컴퓨터과학과 재학
1999년 7월~2005년 2월: (주)하우리 분석팀 근무
2006년 12월~현재: (주)안철수연구소 ASEC/분석1팀 선임연구원 근무
2008년 12월~2009년 12월: (주)안철수연구소 중국 분석센터 근무
관심분야 : 악성코드, 리버스엔지니어링, 커널루트킷

이 상 철 (Lee, Sangchoul)
비회원
1999년 2월: 강원대학교 컴퓨터공학과 졸업
2002년 2월: 강원대학교 컴퓨터정보통신공학과 석사
2002년 3월~2003년 7월: 한국지식웨어 근무
2003년 8월~현재: (주)안철수연구소 ASEC/분석1팀 팀장 근무
관심분야 : 악성코드, 리버스엔지니어링