White Paper

Stuxnet과 AhnLab TrusLine

Revision Version: Stuxnet White Paper ver. 1.0

Release Date: October 14, 2010

AhnLab, Inc.
6th Fl., CCMM Bldg.
12 Yeouido-dong,
Yeongdeungpo-gu, Seoul 150-869,
Korea
82-2-2186-6000
www.ahnlab.com

이란 부셰르 원전을 감염시킨 '스턱스넷(Stuxnet)'으로 전 세계가 들썩이고 있다. 각국의 보안 전문가들이 '스턱스넷'을 주목하고 있다. 이 악성코드가 '국가의 주요 산업 시설 파괴'를 타깃으로 만들어졌기 때문이다. 이는 지금까지의 위험과는 차원이 다른 보안 위협의 새로운 패러다임 시대가 열린 것을 의미한다.

이에 앞서 안철수연구소는 지난 9월 산업용 시스템 전용 보안 솔루션 'AhnLab TrusLine(안랩 트러스라인)'을 선보였다. 트러스라인은 시스템의 안정적 운용에 대한 민감도가 높고, 정해진 프로그램만 사용하는 산업용 시스템에 최적화된 전용 보안 솔루션이다.

이 글에서는 스턱스넷에 대한 상세 분석 및 특징에 대해 알아본다. 또한 트러스라인이 스턱스넷과 같이 산업용 시스템을 타깃으로 하는 악성코드를 어떻게 효과적으로 방어하는지 살펴보자.

스턱스넷(Stuxnet)

스턱스넷(Stuxnet)은 보안 위협의 패러다임을 바꾸는 차원이 다른 악성코드이다. 지금까지 등장한 악성코드가 자기 과시나 금전적인 이득을 목적으로 한 것과 달리 스턱스넷은 단지 핵심 시설의 파괴만을 목표로 하고 있다. 이로 인해 스턱스넷은 악성코드가 사이버 무기화된 첫 번째 사례로 주목 받고 있는 것이다. 또한 현존하는 악성코드 가운데 가장 정교한 것으로도 평가 받고 있다.

스턱스넷(Stuxnet)은 폐쇄망으로 운용되는 대규모 산업 시설을 겨냥해 제작된 악성코드로서, 특정 산업 자동화 시스템만을 공격 목표로 제작된 프로그램이다. 이 악성코드는 원자력, 전기, 철강, 반도체, 화학 등 주요 산업 기반 시설의 제어 시스템에 오작동을 유발함으로써 시스템 마비 및 파괴 등의 치명적인 손상을 입힐 수 있다.
실제로 이란 부셰르 원자력핵발전소와 중국 1천여 개 주요 산업 시설을 비롯해 전세계 여러 국가에 감염이 확산된 것으로 알려지고 있다.

스턱스넷 공격 동향

- **이란의 핵 시설에 스턱스넷 공격 (2010년 1월 ~ 9월)**
  - 부셰르 원전핵발전소 운영 시스템과 운영자 PC에 스턱스넷 침투
  - 나탄즈 우라늄 농축시설 스턱스넷 감염으로 수 차례 오작동 유발
- **중국 내 주요 산업기반시설에 스턱스넷 공격 (2010년 7월 ~)**
  - 중국 600만 PC가 스턱스넷에 감염, 주요 산업시설 공격 (1천여 개)
  - 중국의 철강, 전력, 원자력 등 주요 산업시설 스턱스넷 공격 피해 조사 중
- **미국•인도네시아•인도•파키스탄에서도 스턱스넷 발견**

[출처: 2010년 10월, 행정안전부]

이 악성코드는 C&C(Command & Control) 서버를 통해 SCADA 시스템의 PLCs(programmable logic controllers)를 제어하기 위한 프로그램 명령어를 받아와서 임의로 변경함으로써 악성코드 제작자가 원하는 동작을 수행하는 것을 가능하게 한다.

*** SCADA**(Supervisory Control and Data Acquisition)
산업 기반 시설의 감시와 제어를 담당하는 감시 제어 데이터 수집 시스템

*** PLC(Programmable Logic Controllers)**
산업 자동제어 시스템에서 실제 장비들을 제어하기 위한 장치(device).

이 악성코드에 영향을 받는 환경은 다음과 같다.

*** WinCC/Step 7**
STL 또는 SCL 과 같은 언어로 PLC 를 실행/제어/모니터할 수 있는 코드를 작성할 수 있는 통합 환경의 관리 도구

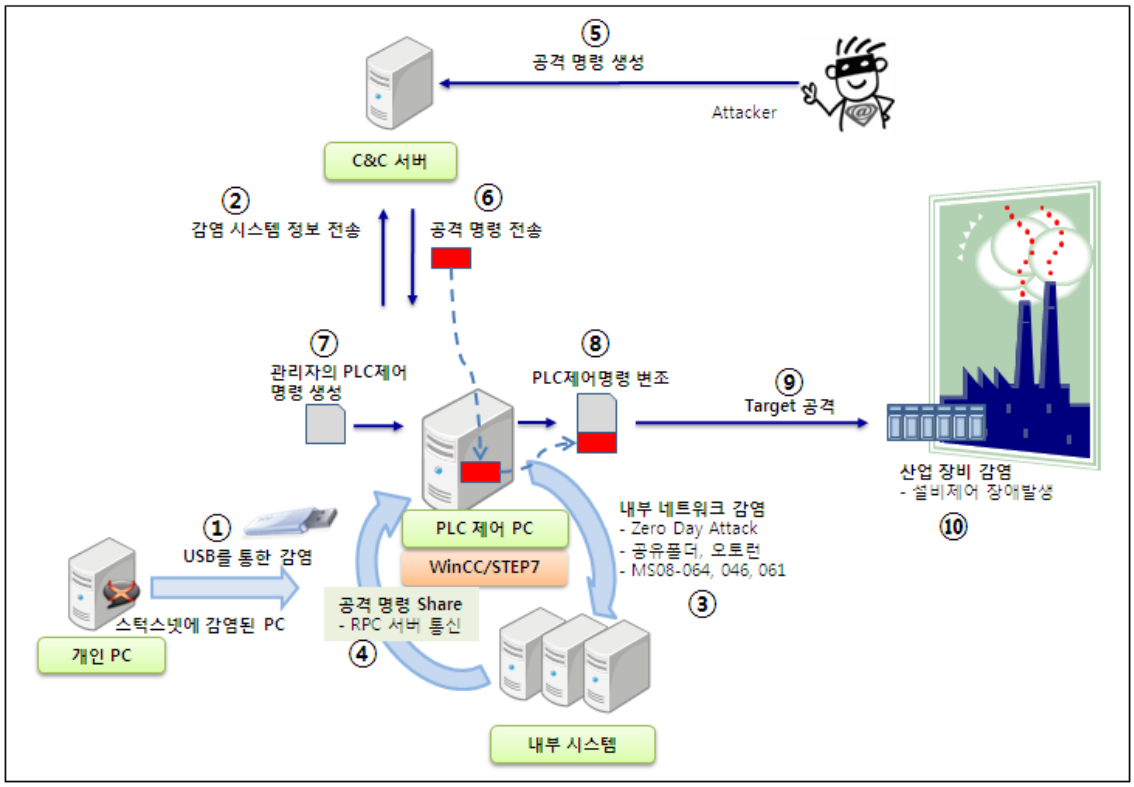
- SCADA 시스템에 지멘스(Siemens)의 WinCC/Step7 통합관리도구가 설치되어 있어야 함
- PLC 타입이 6ES7-315-2 또는 6ES7-417인 경우
- Windows OS 기반의 시스템

이처럼 스턱스넷의 동작 조건이 한정적이기 때문에 일반 사용자들의 PC가 감염되더라도 크게 위협이 되지는 않는다. 그러나 관련 업계에 종사하는 사용자가 악성코드에 감염된 PC에서 감염된 USB를 SCADA 시스템을 운영하는 시스템과 동일한 네트워크의 PC에 삽입하여 감염되는 경우에 감염될 수 있으므로 주의가 필요하다.

스턱스넷 감염 프로세스

안철수연구소 시큐리티대응센터의 분석에 따르면 '스턱스넷'은 여러 개의 파일로 구성되며, 알려지지 않은 여러 개의 취약점을 이용해서 산업자동화 제어시스템을 제어하는 PC 에 드롭퍼(Dropper, 스턱스넷의 핵심 모듈 파일을 생성하는 하는 파일)가 실행된다.
이 드롭퍼는 정상 s7otbxdx.dll 파일의 이름을 변경해 백업하고 정상 s7otbxdx.dll 파일과 동일한 이름으로 자신의 파일을 생성한다. 이후 업자동화제어시스템을 통합 관리하는 도구인 Step7 을 실행하면 원래의 정상 파일이 아닌 스턱스넷이 실행된다.
'Step7'의 기능은 s7otbxdx.dll 파일을 통해서 제어 PC 와 산업자동화 제어시스템 간에 블록 파일을 교환하는 것이다. 이 파일을 스턱스넷의 DLL 파일로 바꾸면 산업자동화 제어시스템을 모니터링하거나 제어(수정 또는 악성 블록 생성)할 수 있다.
이후 공격자는 모터, 컨베이어 벨트, 펌프 등의 장비를 제어하거나 심지어 폭발시킬 수도 있다. 즉, 산업 시설이 관리자가 아닌 악의적 공격자에게 장악될 수 있는 것이다.

스턱스넷의 공격 과정은 [그림 1]을 통해 자세히 살펴보자.



[그림 1] 스턱스넷 악성코드 감염 개념도

① 스턱스넷에 감염된 PC에서 USB를 통해 PLC를 제어하는 메인 PC에 스턱스넷 전파

- 스턱스넷은 메인 악성코드 설치를 위해 ~WTR4141.tmp 파일과 ~WTR4132.tmp 2개의 파일을 사용하고 최초 악성코드 실행을 위해 Autorun.inf와 MS10-046 취약점을 공격하는 .lnk 파일을 이용한다.

② 감염된 PC에서 C&C 서버로 감염 시스템 정보 전송

- IExplorer.exe 프로세스에 Injection되어 C&C 서버와 통신
- 감염 PC의 OS버전, 감염시간, IP정보, 감염된 Project 파일 등 정보를 C&C 서버에 전송
- C&C 서버의 명령에 따라 감염된 다른 시스템들의 버전 업데이트를 위한 RPC 서버로 동작

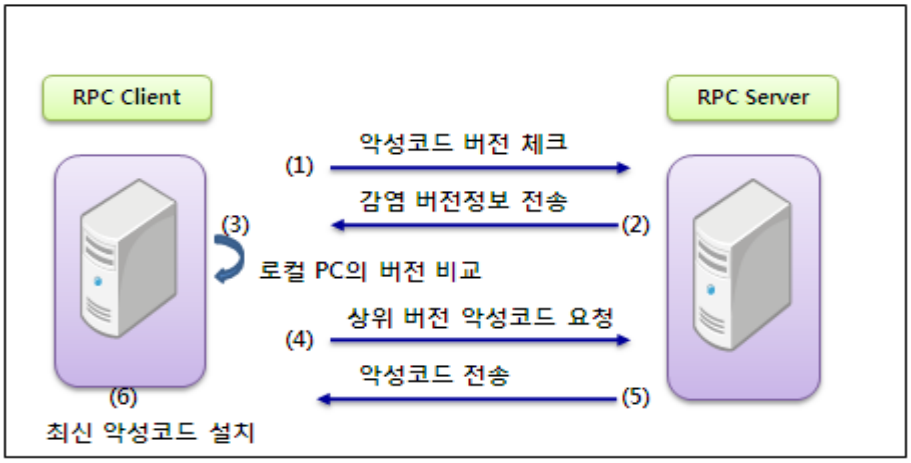
③ 악성코드 유포를 위해 내부 네트워크의 타 시스템 공격

- WINCC database를 이용한 감염, 네트워크 공유를 이용한 감염, MS 10-061 프린터 스풀러 보안취약점을 이용한 감염, MS 08-067 및 MS10-046 취약점을 이용한 감염 등의 방법으로 네트워크 내의 다른 시스템을

감염시킨다.

④ 감염된 메인 PC와 추가 감염된 내부 시스템간의 공격 명령 공유

- 악성코드 감염 시 RPC 서버가 동작하여 네트워크상의 다른 감염된 클라이언트로부터 감염된 버전 체크를 위한 통신을 수행하고 버전이 낮은 경우 상위 버전의 악성코드를 받아 설치한다.



[그림 2] RPC 서버를 이용한 최신 버전의 악성코드 공유 프로세스

⑤ 악성코드 제작자의 공격 명령 생성

- 악성코드 제작자는 임의의 공격 명령의 생성해 C&C 서버에 전송한다.

⑥ 공력 명령 전송

- C&C 서버는 악성코드 제작자가 제작한 암호화된 바이너리 코드를 받아와 실행한다.

⑦ 관리자의 PLC 제어 명령 생성

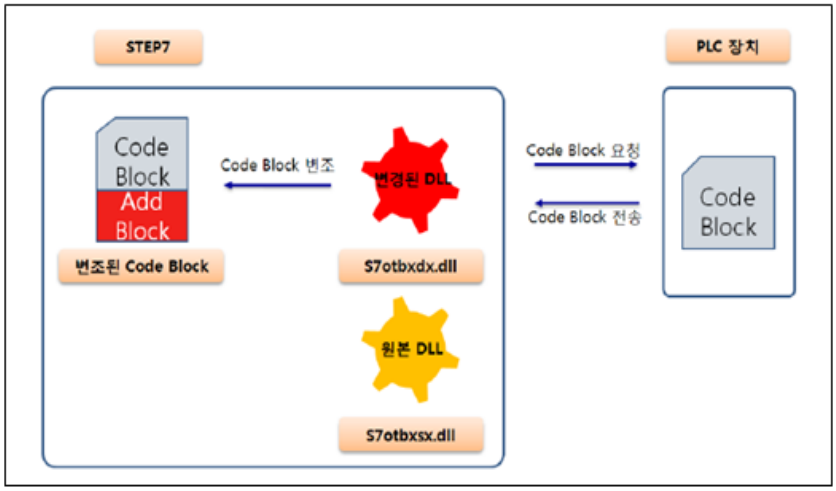
- PLC 장치를 제어하기 위한 Step7 프로그램은 STL이나 SCL과 같은 언어로 제작된 데이터와 코드의 Block들을 MC7 형태의 파일로 컴파일해서 PLC 장치에 전송해주고 PLC 장치는 이 Block들을 받아 메모리에 저장한 후 로드하여 동작한다.

⑧ PLC 제어 명령 변조

- 스턱스넷 악성코드가 의도하는 것은 PLC 장치에 공격자가 의도한 명령어를 삽입하는 것이다. 이를 위해 공격자는 특정 버전의 Step7 프로그램에서 사용하는 s7otbxdx.dll 파일을 공격자가 임의로 제작한 것으로 교체한다. s7otbxdx.dll 파일은 PLC 장비와 관리 프로그램간의 데이터 교환을

해주는 기능을 가진 파일이다. 스턱스넷 악성코드에 감염된 경우 악성코드는 원래 프로그램에서 동작하고 있는 정상 dll 파일을 s7otbxsx.dll 파일로 이름을 변경한 후 악성코드 제작자가 임으로 제작한 악의적인 dll 파일을 동일한 파일명으로 생성한다. dll 파일이 변경됨으로 인해 다음과 같은 행위가 가능하게 된다.

- Step7 프로그램과 PLC 장비간에 교환되는 PLC Block들에 대한 모니터링을 할 수 있다.
- 관리자가 생성한 데이터 Block들에 공격자가 의도하는 명령어가 들어있는 Block을 삽입하거나 Block을 교체함으로써 PLC 장치가 공격자의 의도대로 동작하게 한다.
- 감염된 PLC 장치의 정보를 확인할 수 있다.



[그림 3] 악성 s7otbxdx.dll을 이용한 PLC의 Code Block 변조

스턱스넷에 의해 변조된 s7otbxdx.dll 파일은 원본 dll 파일이 가지고 있던 모든 정보들을 가지고 있고 여기에 공격자가 의도한 임의의 코드가 추가된 형태이기 때문에 이미 제작해서 사용중인 Block을 이용한 업무 수행에 문제가 없다. 따라서 작업자는 감염이 되더라도 이상 징후를 쉽게 인지하기 힘들다.

⑨ 타깃(Target) 공격

- 이렇게 변조된 명령어를 통해 악성코드 제작자가 의도한 타깃에 대한 공격을 시도한다.

⑩ TLC 장비 감염 – 설비제어 장애 발생

- 악성코드 제작자는 자신의 의도에 따라 모터, 컨베이어 벨트, 펌 등의 장비를 제어하거나 마비 등의 장애를 일으킬 수 있다.

스턱스넷 감염 예방을 위한 일반적인 조치 사항

스턱스넷은 기존 악성코드와는 다른 패턴을 보여주고 있다. 하지만 감염과 유포 방식에 있어서는 USB라는 이동형 저장장치와 윈도우 OS의 취약점을 이용하고 있다. 이 부분에 초점을 맞춰 기업 보안 담당자가 취할 수 있는 예방 방법은 다음과 같다.

■ **최신 버전으로 업데이트된 백신 소프트웨어 사용**

스턱스넷 악성코드의 확산도가 7월 이후 전세계적으로 점점 증가하고 있는 추세이고 변형 또한 많이 발견되고 있는 상황이므로 최신 버전의 백신 프로그램을 사용해서 감염을 예방해야 한다.

■ **USB 자동 실행 방지**

대부분의 SCADA 시스템은 폐쇄망에서 운영되므로 실제 감염이 발생하는 경로로 이용될 수 있는 것은 USB일 가능성이 높다. 따라서 폐쇄망에서 사용되는 시스템의 경우 V3의 CD/USB 자동실행 방지 옵션을 활성화하여 감염을 예방한다.

■ **최신 보안 패치 적용**

사내 시스템이 윈도우 OS의 취약점을 이용한 공격에 의해 감염되는 것을 예방하기 위해 최신 보안 패치를 업데이트하는 것이 중요하다

1. Microsoft 보안 공지 MS10-046 - 긴급

Windows 쉘의 취약점으로 인한 원격 코드 실행 문제점(2286198)

http://www.microsoft.com/korea/technet/security/bulletin/ms10-046.mspx

2. Microsoft 보안 공지 MS10-061 - 긴급

인쇄 스풀러 서비스의 취약점으로 인한 원격 코드 실행 문제점(2347290)

http://www.microsoft.com/korea/technet/security/bulletin/ms10-061.mspx

3. Microsoft 보안 공지 MS08-067 - 긴급

서버 서비스의 취약점으로 인한 원격 코드 실행 문제점 (958644)

http://www.microsoft.com/korea/technet/security/bulletin/ms08-067.mspx

4. Privilege escalation via Keyboard layout file

- 패치 미제공

5. Privilege escalation via Task Scheduler

- 패치 미제공

■ **공유폴더 사용 주의**

불필요한 공유 폴더 생성은 금지하고 생성한 공유 폴더에는 접근이 필요한 사용자 계정에게만 읽기 권한 주도록 하고 함부로 쓰기 권한은 주지 않도록 한다.

스턱스넷 감염 예방을 위한 제언

- 산업용 시스템 전용 보안 솔루션 AhnLab TrusLine

앞서 언급했듯이 스턱스넷은 기존의 악성코드와는 완전히 다른 목적성을 띠고 있다. 일반적인 악성코드가 유포나 확산을 목적으로 하는 반면, 스턱스넷은 정확한 타깃을 노려 제작되었다. 따라서 악성코드 샘플 수가 적기 때문에 수집 자체에 어려움을 겪을 수 밖에 없다. 또한 샘플이 수집되었더라도 특정 시스템에서만 동작하므로 악성코드 여부를 확인할 수 있는 테스트 실시도 쉽지 않은 일이다.
스턱스넷뿐만 아니라 최근 발생하고 있는 악성코드들은 날로 새로운 기법으로 무장하고 있어 전통적인 블랙리스트 기반의 안티바이러스 솔루션으로 방어하기엔 역부족인 상황이다. 특히, 악성코드 침해로 인해 운영상의 장애가 발생할 경우 엄청난 피해로 이어지는 산업용 시스템의 경우에는 안정성 확보를 위한 새로운 컨셉의 보안 솔루션 도입이 반드시 필요하다.

안철수연구소가 지난 9월 출시한 AhnLab TrusLine(안랩 트러스라인, 이하 트러스라인)은 산업용 시스템 환경에 적합한 최적의 보안 솔루션이다. 트러스라인은 허용된 프로그램만 실행 가능하게 하는 화이트리스트 기반의 보안 솔루션으로 불필요한 프로그램 작동이나 악성코드 침입 등으로 시스템의 작동에 차질이 생기지 않도록 해주는 제품이다.

[그림 4] AhnLab TrusLine 개요

트러스라인의 특징은 다음과 같다.

■ 악성코드의 감염 및 신종 악성코드에 대한 예방

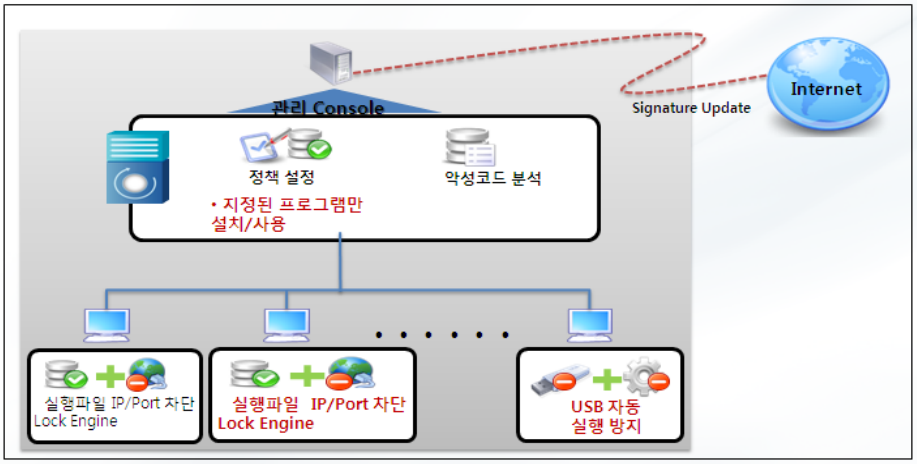
트러스라인에서 적용한 화이트 리스트 방식은 현존 악성코드는 물론 미발견 변종/신종 악성코드까지 막을 수 있다. 기존 백신 제품은 엔진에 포함된 악성코드 시그니처를 기반으로 악성코드 유무를 판단하기 때문에 사후 처리만 가능하다. 반면, 트러스라인은 허용된 프로그램만 실행하게 함으로써 현존 악성코드뿐 아니라 향후 발생할 변종 및 신종 악성코드까지 원천적으로 막을 수 있다.

즉, 애플리케이션 제어, 비허가 실행 코드 차단, USB 등 매체 제어, IP/Port 차단 등과 같은 기능을 갖추고 있기 때문에 스턱스넷과 같은 악성코드가 실행조차 되지 않는 환경을 만들어주는 것이다.

[그림 5] White List vs. Black List 비교

트러스라인은 기존 일반적인 화이트 리스트 방식의 제품과도 다른 차별점을 지니고 있다. 즉, 다른 제품은 각 클라이언트 PC 에 설치된 파일의 안전 여부를 PC 용 백신으로 검증하는 데 반해 트러스라인은 관리 서버에서 검증한다. 따라서 클라이언트 PC 용 백신을 추가로 설치하지 않아도 된다.

트러스라인이 적용되어 Locking 된 시스템은 화이트 리스트를 기반으로 운용되기 때문에 이 리스트에 존재할 수 없는 악성코드의 실행이 차단된다. USB 메모리를 통한 오토런(autorun)의 실행과 감염, 포트를 통하여 전파되는 웜 등의 실행 자체가 불가능해지며, 신종 악성코드도 리스트에 등록될 수 없기 때문에 감염이 되지 않는다.



[그림 6] AhnLab TrusLine 구성도

■ 악성코드 침입 루트를 차단하기 위한 IP & Port 차단 기능

트러스라인은 실행 프로그램의 제어 만으로는 해결하기 힘든 악성코드의 침입에 대비하기 위해 산업용 시스템에 설치된 프로그램이 사용하는 IP 와 Port 만 오픈 함으로써 보다 완벽한 보안 환경을 구축할 수 있다.

■ 시스템 관리 정책의 자연스러운 적용

사용자들에게 USB 메모리나 공유 폴더 사용을 금지해도 100% 막을 수 없다. 하지만 트러스라인은 불필요한 프로그램 실행을 차단하므로 위험의 수준을 낮추고 관리의 편의성을 자연스럽게 확보할 수 있다.

스턱스넷과 같은 악성코드의 최종 목표는 타깃 대상인 산업용 시스템에 치명적인 타격을 입히는 것이다. 이는 악성코드가 전략적으로 이용될 가능성이 있음을 보여주는 구체적인 사례이며, 앞으로도 이 같은 공격은 더욱 늘어날 것으로 예상된다. 이를 대응하기 위해서는 트러스라인과 같은 화이트 리스트 기반의 전용 솔루션으로 대비하는 방안이 필요하다.