Missile of cyber terrorism, APT

- How to defend?

2013. 2.

보안솔루션팀 송인혁

Section List

[Section Ⅰ]

공격의 진화

공격하는 자

뚫어야 한다 !!!

방어하는 자

막아야 한다 !!!

우리는 지켜야할
소중한 것(자산)이 있다.

공자의 입장에서 생각하기

공격자

Massmarket Attack

방어자

공자의 입장에서 생각하기

- 공격자

- 방어자

공자의 입장에서 생각하기

- 공격자

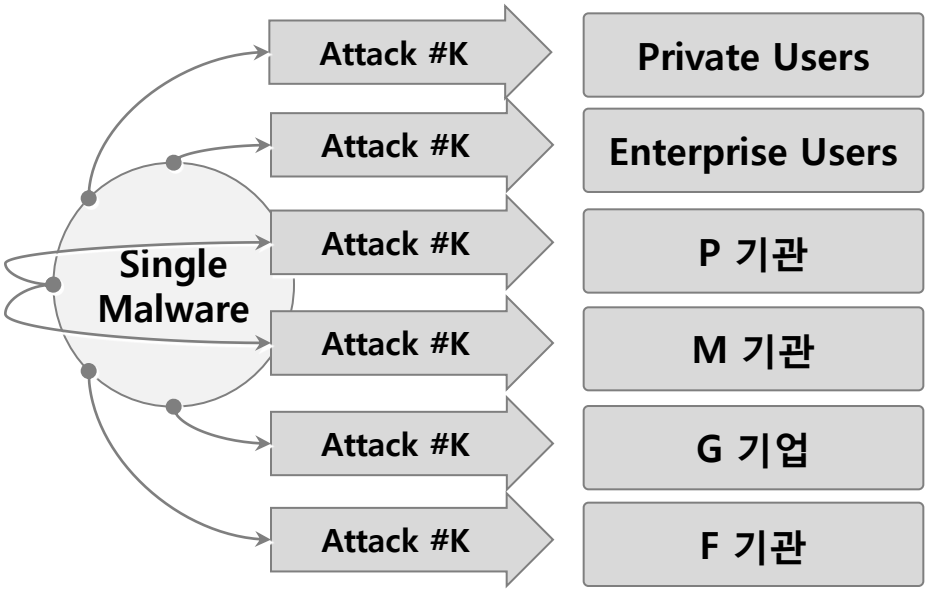
Targeted Attack

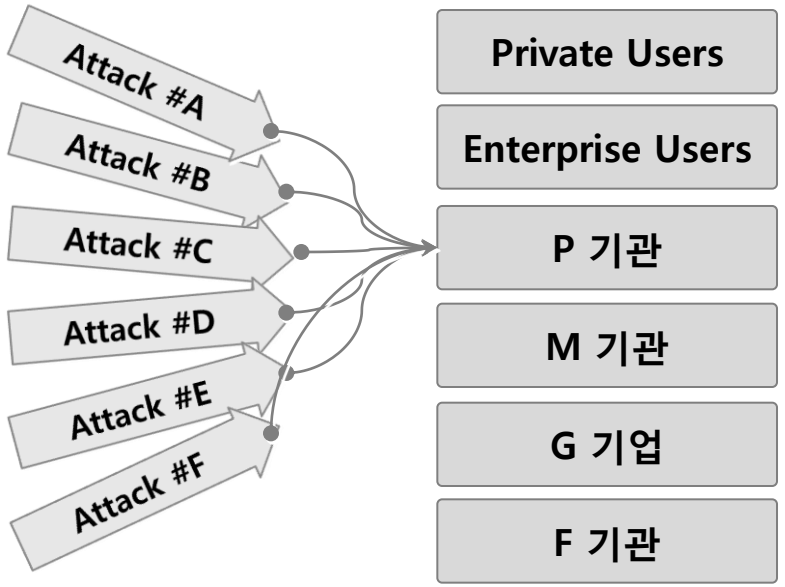
- 방어자

❑ 공격의 진화

Massmarket Attack

Targeted Attack





[Section Ⅱ]

사고사례 분석

1. APT 위협, 해외 피해사례 소개

APT 공격은 주로 정부나 공공기관, 사회 기반시설 등을 표적으로 감행되었으나, 최근에는 민간 부문에도 급속도로 확산되는 추세임

□ 국외(해외) 사고사례

대상	피해 기관(시설)명	내 용	상 세 내 용
민간	S_ Company 해킹 (2011년 4월)	고객정보 유출 (1억여건)	- 자신을 룰즈섹이라고 밝힌 해커 그룹에 의해 - 2011년 4월 이후부터 16차례 이상 해킹을 당했으며 - 소니 가입자의 개인정보 유출건수는 1억여건에 이름.
민간	E_Company 해킹 (2011년 3월)	보안인증 기술 (OTP) 유출	- SNS를 이용하여 공격대상에 대한 정보를 수집하고, - 사회공학적 기법을 통해 악성코드를 감염시킴. - 이후 범용 SW의 제로데이 취약점을 이용해 정보를 유출함.
민간	Mor_Company 해킹 (2010년 1월)	산업기밀 유출	-G사와 M사를 해킹하여 내부 중요정보를 훔쳐간 사건임. -2009년 6월에 시작하여 6개월간 지속된 것으로 확인됨.
기반	글로벌 에너지 기업 해킹 (2011년)	제조/ 영업관련 기밀자료 유출	- 취약점이 존재하는 웹 서버에 SQL 인젝션 공격으로 악성파일 업로드 - 스피어-피싱을 통해 접속을 위한 계정정보 획득 & 내부PC 감염 - 획득한 계정정보로 계정 추가수집 및 시스템 접속 - 표적 대상서버에 서서히 접근하여 획득 후 외부 유출 (2009년부터 2년간)
기반	이란 원자력 발전소 마비 (2010년 7월)	발전시설 시스템 마비	- 독일 지멘스의 산업자동화 시스템인 SCADA 시스템을 임의로 제어 - Microsoft 사의 4개 제로데이 취약점 이용, USB를 통한 확산
기반	미국 국방부 / 항공우주국 해킹 (1999년)	국가기밀 유출 (핵무기 정보, 군사시설지도, 병력구성 등)	- 1998년부터 1년 동안 지속되었음. - 미국방부는 침입자의 경로를 역추적하여 구소련 해커의 소행임을 주장하였으나 러시아는 이에 대해 관련여부를 거부하였음.

2. APT 위협, 국내 피해사례 소개

국내의 경우, 현재까지 APT 공격은 대량의 중요정보를 보관한 민간기업, 금융기관 등을 대상으로 발생함

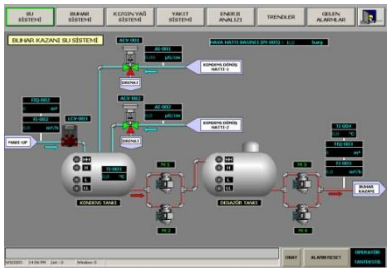
□ 국내 사고사례

대상	피해 기관(시설)명	내 용	상 세 내 용
민간	N_Company 해킹 (2011년 11월)	고객정보 유출 (1,320만건)	- 해커 그룹은 내부 직원 PC에 악성코드를 설치한 뒤, 서버 운영관리팀장 PC에 침투함. 정보수집을 통해 백업시스템 접근 계정 획득 후, 개인정보를 외부로 유출함.
민간	S_Company 해킹 (2011년 7월)	고객정보 유출 (3,500만건)	- 해커그룹은 웹서버 취약점 및 내부 임직원의 비인가 SW 사용실태를 악용하여 내부에 악성코드를 유포한 뒤, 이를 통해 중요서버의 접근계정을 획득하고 이를 통해 고객정보를 외부로 유출함.
금융	N_Institution 해킹 (2011년 4월)	서비스 마비 (6일)	- IBM 외주업체 직원의 서버관리용 업무 노트북을 외부에 반출입하여 악성코드 감염. 해커들은 이를 통해 내부를 확산 점령해 나갔고 중요서버에 대한 계정 및 비밀번호 등 정보들을 수집, 사건 발생일 4월 12일에 서버들은 서로를 파괴공격하여 30분만에 서버 운영시스템의 절반이 파괴되었음.
금융	H_Company 캐피탈 (2011년 4월)	고객정보 유출 (175만건)	- 해커 그룹은 퇴직한 직원의 계정을 습득한 뒤, 메일서버 및 업무서버에서 화면캡쳐 및 다운로드를 통해 고객정보 175만건을 해킹함.
민간	A_Company 해킹 (2008년 2월)	고객정보 유출 (1,081만건)	- 해커 그룹은 이메일을 통해 내부 직원 PC에 침투한 뒤, 서버 관리자 PC에 키로거 프로그램을 설치하여 서버접근 계정을 탈취함. 이를 통해 고객정보 유출.

3-1. 스턱스넷(Stuxnet) 분석

스턱스넷은 이란 원자력 발전소를 공격하여 가동중인 우라늄 원심분리기 1,000대(전체의 약 10%)를 작동 불능상태로 만들었음

❑ Stuxnet 개요



• 이란 원자력 발전소의 SCADA 시스템 공격

• 실제로 이란 대통령이 핵발전 원심분리기가 악성코드에 의해 훼손됐다고 시인[1)]

• 악성코드의 사이버무기 가능성 실현

• 사이버테러의 심각성과 실체가 드러나 현실화

1) 가동중인 우라늄 농축용 원심분리기 1,000대(약10%)가 '09.11~'10.1 사이에 파괴되었으며, 이를 완전히 복구하기 위해서는 2년이 소요 추정

❑ SCADA[2)] 시스템 이해

정의

• SCADA 시스템은 대규모 산업시설을 감시, 통제하는 정보통신 기반 시스템으로써 집중 원격감시 제어데이터 수집시스템이라 명명됨

활용 분야

• 전력·가스·수도 공급 및 교통관리 등 대부분의 국가 기반시설과 대규모 산업시설이 정상적으로 작동하도록 직접적인 제어 수행

작동 방식

• 제어대상 시스템 및 네트워크에 각종 센서들을 설치하고, 관리자가 이를 통해 정보를 수집 및 분석하여 필요한 조치를 수행

피해 대상

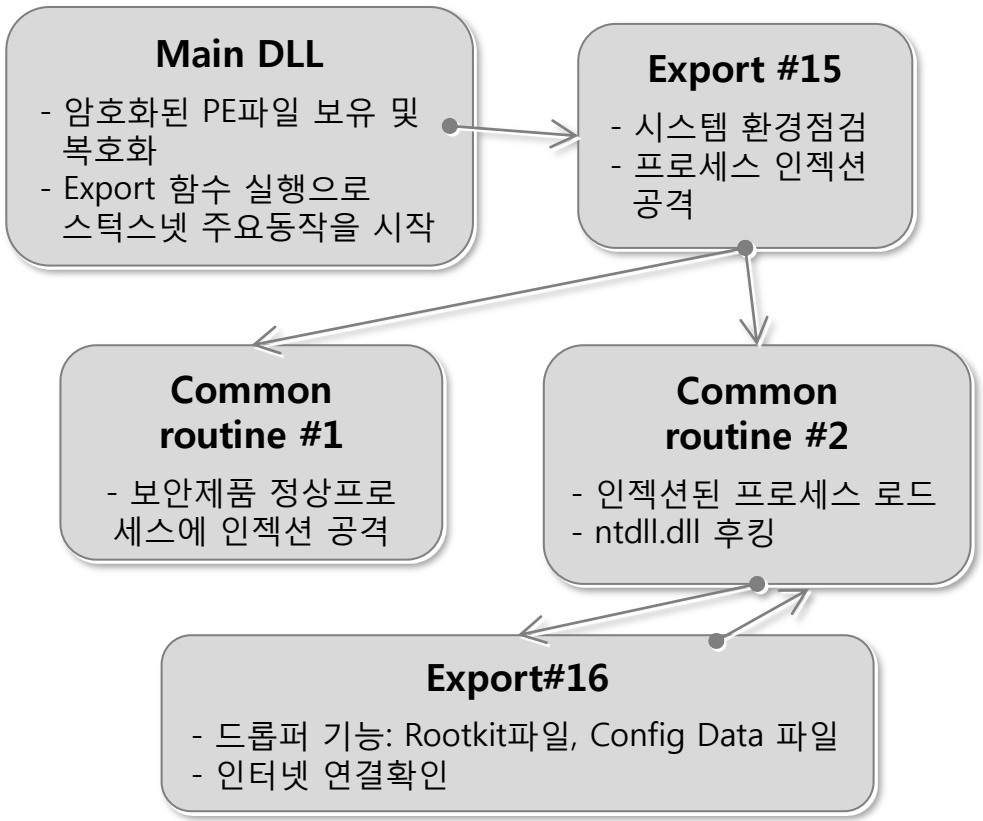
• 독일지멘스(Simens)사의 SIMANTIC PCS7
- 이의 컴포넌트 프로그램을 (WinCC/Step7, 통합관리도구) 공격

2) SCADA(Supervisory Control And Data Acquisition)

3-1. 스턱스넷(Stuxnet) 분석

❑ Stuxnet - Architecture

다수의 export 함수와 resource를 갖는 .dll 파일로 구성



Routine	Function summary
Main DLL	- 암호화된 PE파일 복호화 - KERNEL32.DLL.ASLR.xxxx 형태의 파일(명)을 생성
Export #15	- 시스템 환경 점검 : 인터넷 연결여부, 운영체제 64bit여부, 동작 가능한 운영체제인지 여부, 사용자 실행권한 확인
Common Routine #1	- 10종 보안제품 관련 프로세스 존재유무 확인 - 해당 프로세스를 인젝션 공격 (Kernel32.dll.ASLR.xxx 데이터로)
Common Routine #2	- ntdll.dll 후킹 - Kernel32.dll.ASLR.xxx 로드
Etc Export #16	- 리소스(Resource) 영역에서 재감염과 파일 은폐 기능을 가진 루트킷(Rootkit) 2개와 Configuration Data 파일을 드롭 - 인터넷 연결확인 - Step7 시스템에 인젝션(Injection) 공격을 하기 위한 준비

3-1. 스턱스넷(Stuxnet) 분석

최초 감염은 USB 플래시 드라이브를 통해 이루어졌고, 이후에는 윈도 컴퓨터간의 원격 프로시저 호출 등의 프로토콜을 통해 인터넷에 노출되지 않은 내부망으로 연결된 컴퓨터에 감염되었음

❑ Stuxnet 의 다양한 전파경로

네트워크 공유폴더 (MS08-067)

• 네트워크 공유폴더를 통한 방법
- 네트워크에 존재하는 시스템의 C$ 와 Admin$를 검색
- 쓰기권한이 있다면 스턱스넷 메인파일 생성
- 해당 파일이 실행될 수 있도록 작업스케줄러에 등록

• 윈도우 서버 서비스 취약점 exploit
- RPC취약점을 이용하여 원격에서, 권한과 무관하게, 감염대상PC에게 명령을 요청할 수 있음. 이를 통해 악성코드를 전송 및 실행함.
※ 단, 실행조건
: 안티바이러스 프로그램의 버전을 조사
: Kernel32.dll, Netapi32.dll의 패치일자가 2008.10.12 이전

프린트 스풀러 취약점 공격 (MS10-061)

• 제로데이였음
• 메인DLL을 타겟시스템에 복사 (이 과정에 프린트스풀러 취약점 이용)
- 조건 : 타깃시스템에 프린터 공유 및 파일공유 기능 활성화
- 수행파일 : 메인DLL의 모듈인 KERNEL32파일
- 파일기능 :
: 악성코드를 변환하여 PC의 버퍼에 저장
: 프린터 구조체를 조작하여 변경
- 수행내용 : 감염된 PC에 사용자가 인쇄작업 요청시 PC의 버퍼에 있던 악성코드가 프린터로 이동됨. 이러한 상황에서 정상적인 PC가 프린터에게 인쇄를 요청했을때 프린터에 있던 악성코드가 해당PC로 복사됨.

권한상승 취약점 공격 (MS10-073)

• Windows 커널 모드 드라이버가 개체에 대한 참조 수를 적절히 유지하지 않는 취약점을 이용해 권한 상승을 성공함
• 이 취약점 악용에 성공한 공격자는 임의 코드를 실행하여 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있음.

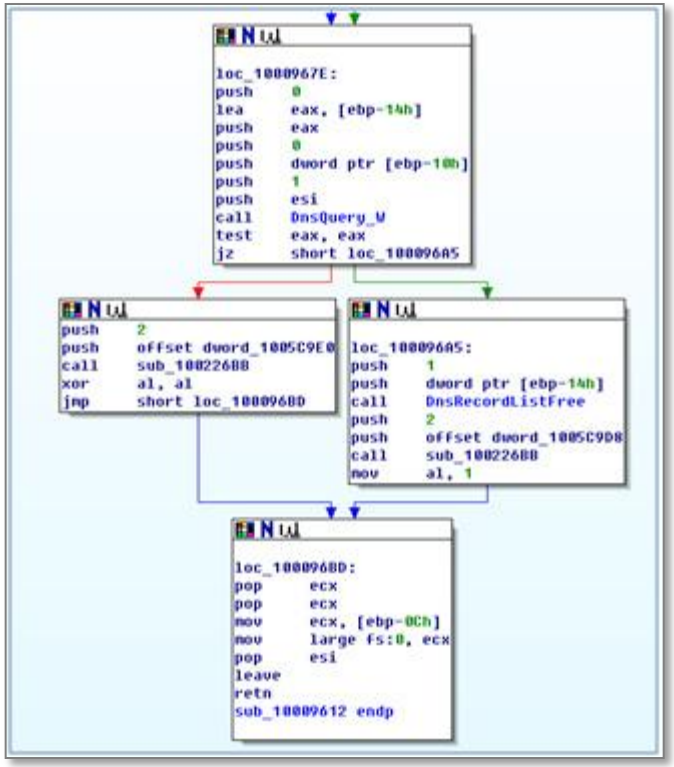
USB를 통한 전파

• Autorun.inf 취약점을 통한 방법
※ 제약사항 : PC내 자동실행 기능 비활성화시 작동 불능
• LNK 취약점을 통한 방법 (MS10-046)
- 내용 : 탐색기 or 내컴퓨터를 통해 USB장치 드라이브를 열었을때 바로가기 아이콘이 로딩되는 순간, 대상파일로 지정된 파일이 사용자권한으로 로드되는 취약점 이용

3-1. 스턱스넷(Stuxnet) 분석

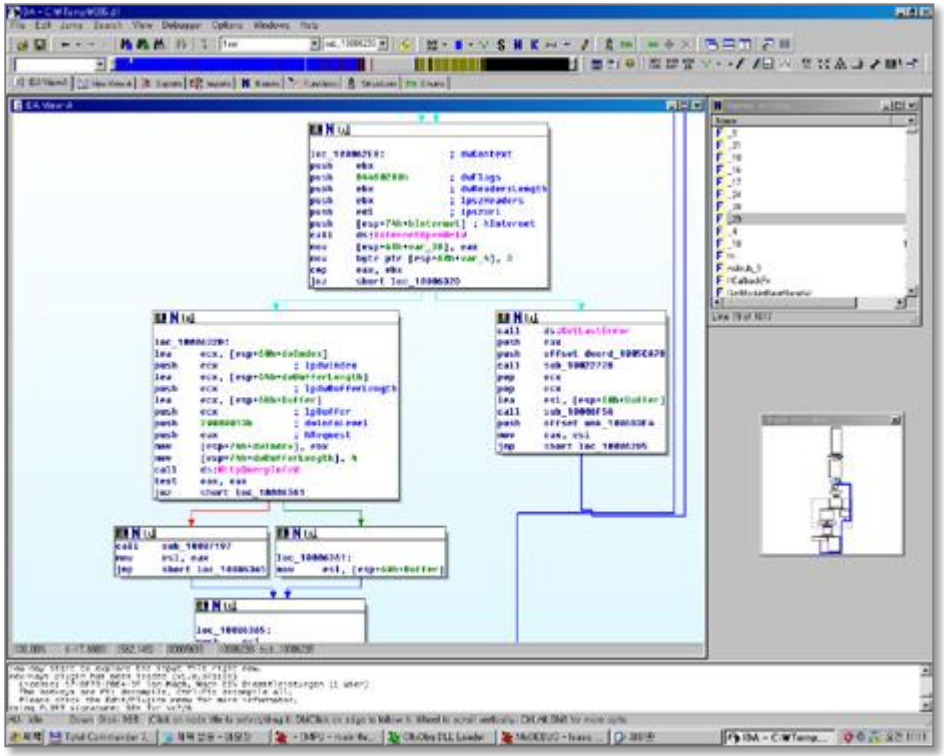
❑ Stuxnet C&C Server – Routine Analysis (1/2)

- 스턱스넷은 C&C 서버에 접속을 시도하기 전, 인터넷 연결 여부를 확인하기 위해 윈도우업데이트사이트와 msn사이트를 먼저 접속함



- 인터넷 접속이 가용한 환경일때, 준비된 2개의 C&C서버에 접속
  - www.mypreminrfutbol.com
  - www.todaysfutbol.com

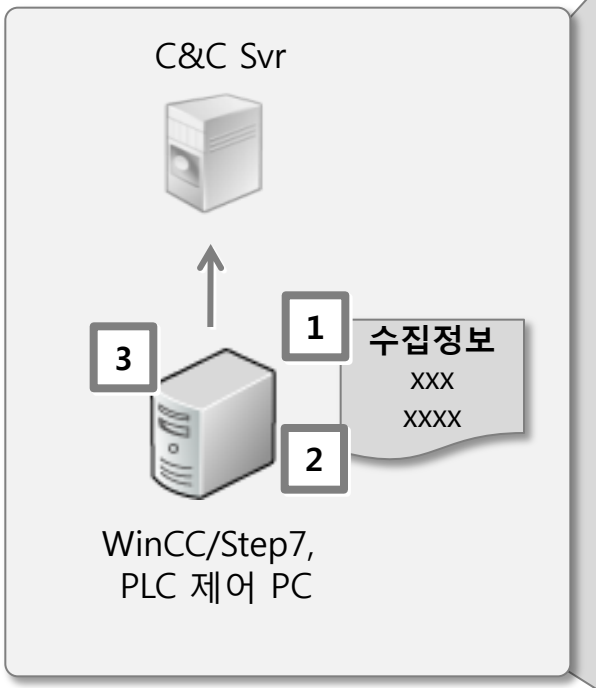
  (※ 해당 URL은 하드코딩되어 있지 않고 동작실행시 URL 문자구성)



3-1. 스턱스넷(Stuxnet) 분석

❑ Stuxnet C&C Server – Routine Analysis (2/2)

C&C 서버 접속가능 확인후 동작 개념도



1 **http://www.mypremierfutbol.com/index.php?data=전송데이터**

- 위의 형태로 정보 전송
- 정보 수집 항목
  - 감염 시스템의 컴퓨터 이름
  - 감염 시스템의 도메인 이름
  - 운영체제의 종류와 버전
  - Step7, WinCC 설치 여부

2 **0x67, 0xA9, 0x6E, 0x28, 0x90, 0x0D, 0x58, 0xD6, 0xA4, 0x5D, 0xE2, 0x72, 0x66, 0xC0, 0x4A, 0x57, 0x88, 0x5A, 0xB0, 0x5C, 0x6E, 0x45, 0x56, 0x1A, 0xBD, 0x7C, 0x71, 0x5E, 0x42, 0xE4, 0xC1**

- 수집 데이터를 31Bytes 키를 이용해 암호화

3

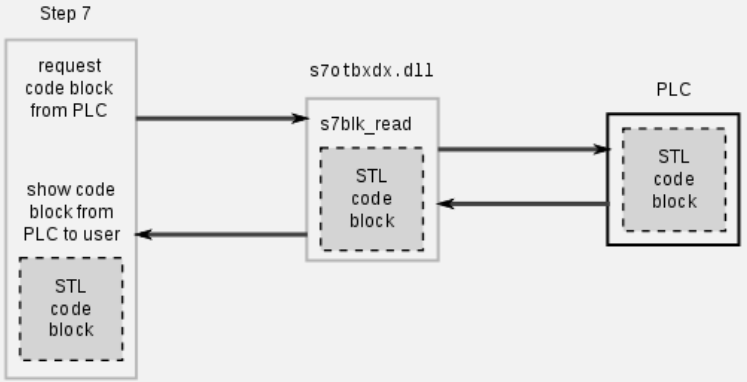
- iExplorer.exe 혹은 기본 웹브라우저를 통해 전송

※ 최대한 자연스러운 작업으로 위장

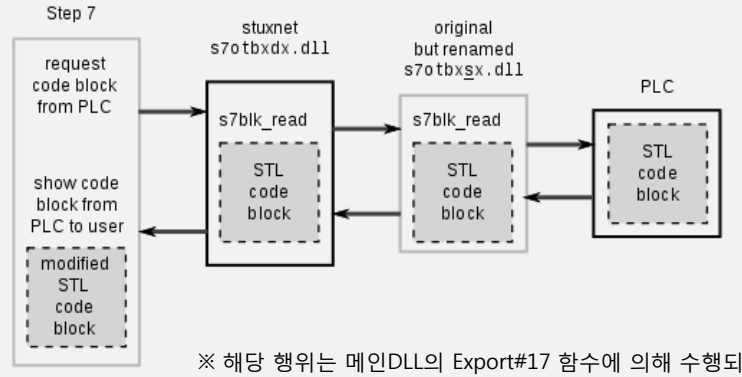
3-1. 스턱스넷(Stuxnet) 분석

❑ SCADA System Attack

Step7과 지멘스 PLC의 정상 통신경로

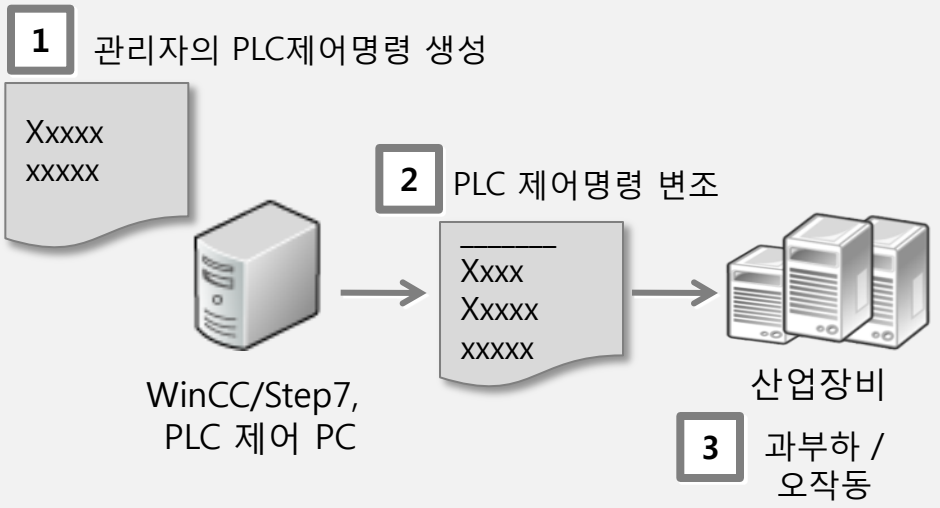


Step7과 PLC사이의 통신을 가로채는 모습



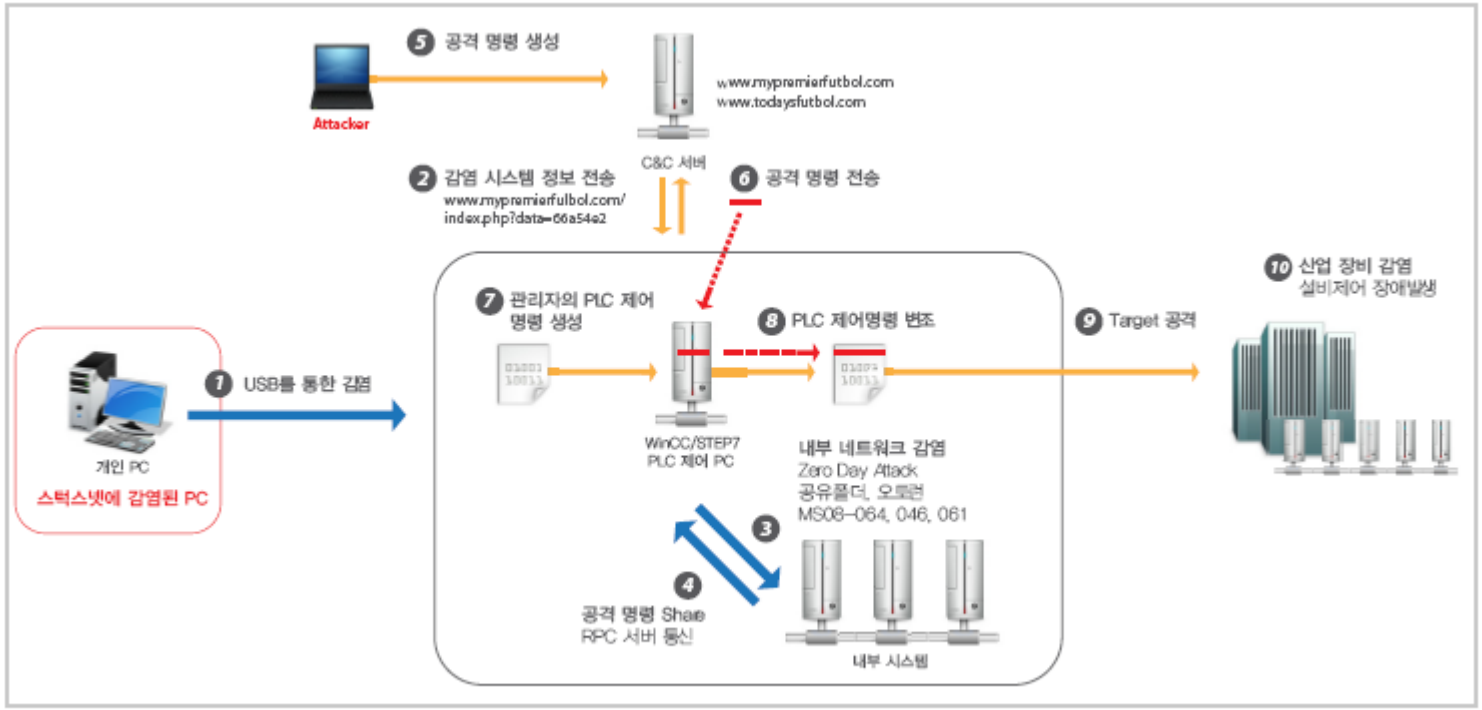
※ 해당 행위는 메인DLL의 Export#17 함수에 의해 수행되어짐

SCADA 시스템 공격에 대한 분석 개념도



3-1. 스턱스넷(Stuxnet) 분석

❑ Stuxnet Attack Routine (concept)



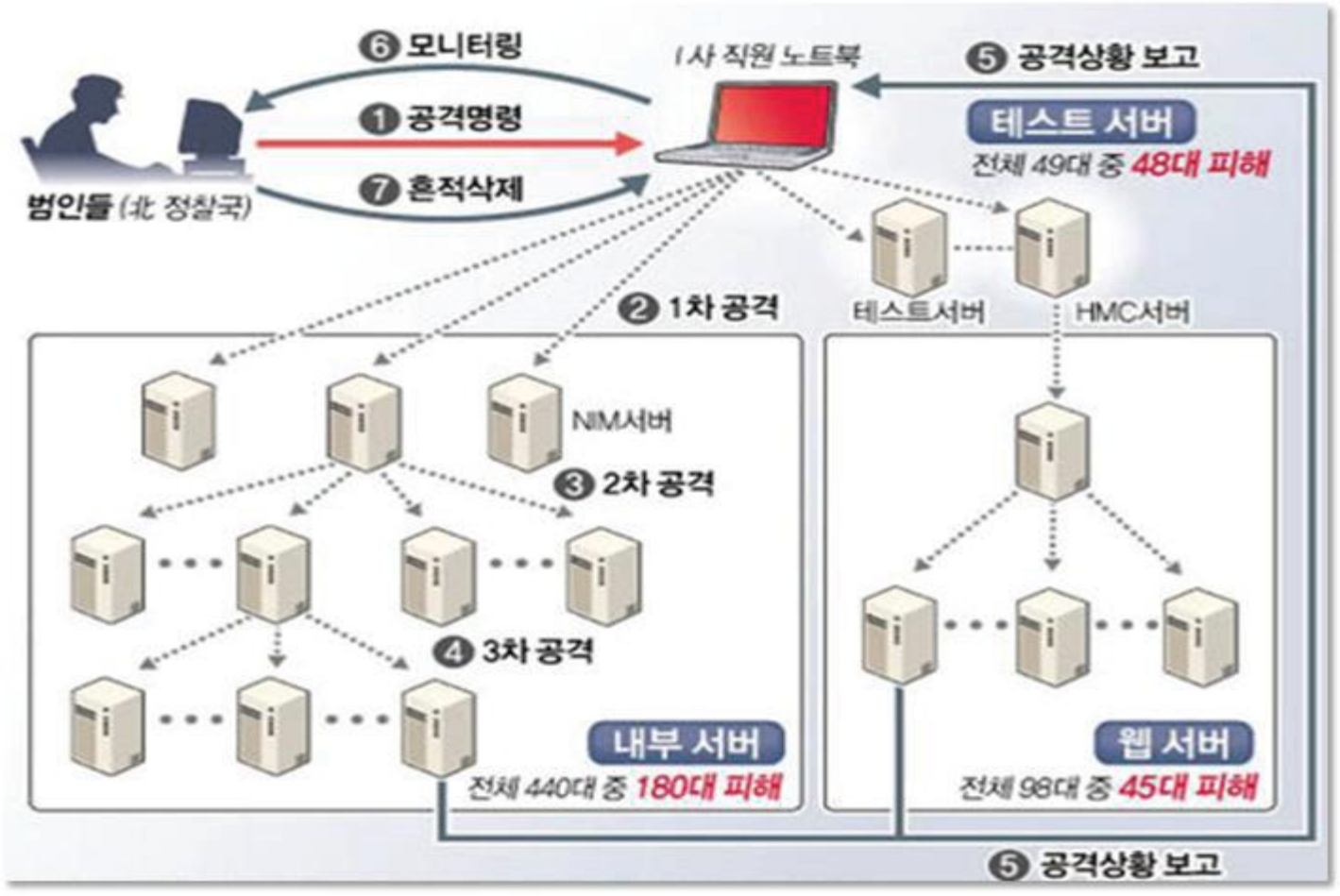
[그림 2-2] 스턱스넷 악성코드의 감염과 동작 원리

Findings.

- 클라이언트 PC감염을 통한 확산 및 권한상승 시도
- 이동식 디스크를 통한 감염
- 불법SW사용은 취약점노출
- 13개월의 활동기간

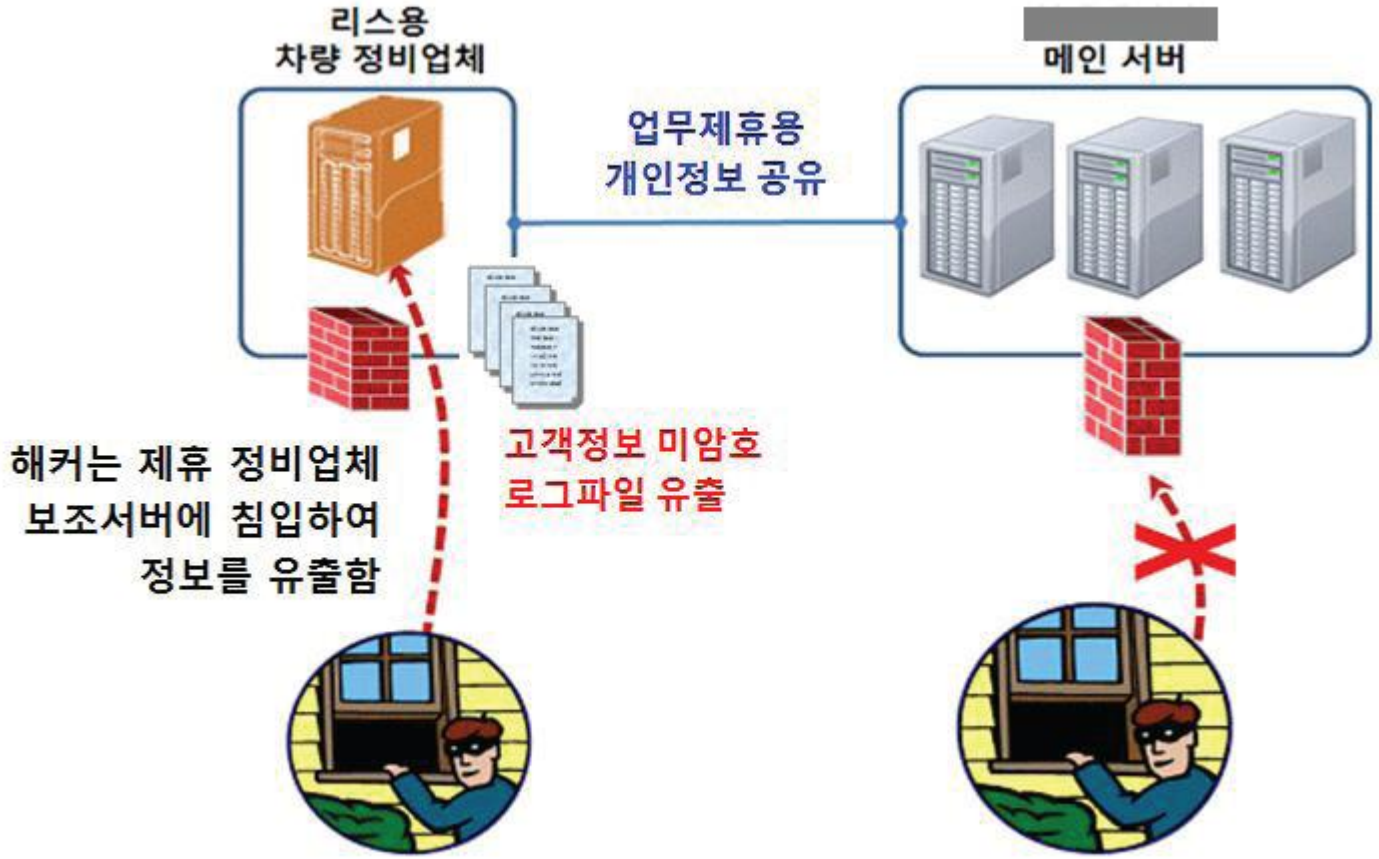
3-2. N 금융기관 해킹사고 분석

❑ #A Company Attack Routine (concept)



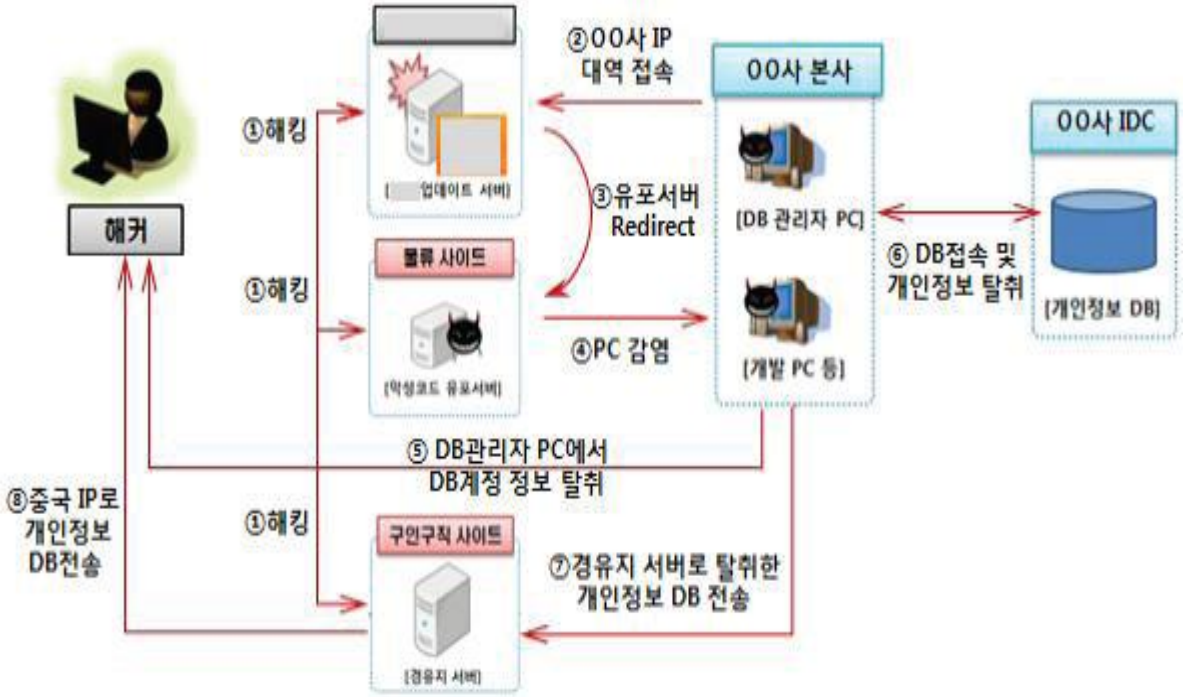
3-3. S 카드사 해킹사고 분석

❑ #B Company Attack Routine (concept)



3-4. S 포털사이트 해킹사고 분석

❑ #C Company Attack Routine (concept)



3-5. 종합 분석 결과

차후 공개

[Section Ⅲ]

대응방안 및 전략

차후 공개

[Section IV]

별 첨

차후 공개

Thank you

감사합니다