글. 이선응 차장 / 김영준 과장 아이크래프트㈜ SNT본부 기술1팀

방송시스템의 보안강화 - 3

- Part 3. DDoS 공격과 APT 공격

연재 목차

디도스(DDoS) 공격

'디도스(DDoS) 공격'이란 Distributed Denial of Service의 약자로써 분산 서비스거부 공격이라고 번역할 수 있다. 즉 여러 개로 분산된 공격지점에서 시간을 맞추어 지정된 목적지(Web, Mail, DNS 서버 등)로 막대한 양의 트래픽을 보내, 해당 서버가 처리할 수 있는 용량을 초과하게 만들어 정상적인 사용자가 서비스를 이용할 수 없도록 만드는 공격이다.

지난 2011년 10월 26일 선거 당일 날 선거관리위원회 홈페이지의 부재자 투표 위치 검색을 방해할 목적으로 선관위 홈페이지에 DDoS 공격을 수행하여, 약 2시 30분 동안 홈페이지 접근이 중단된 사건이 있었고, 경쟁업체의 청부를 통해 온라인 게임 서버를 공격하여 게임서버에 접속이 되지 않게 한다든지, 금품갈취 목적으로 온라인 쇼핑몰에 협박을 하고 돈을 보내지 않으면 공격을 하는가 하면, 올해는 국제 해킹그룹이 국내 시중은행 7곳에 가상화폐인 비트코인을 보내지 않으면 DDoS 공격을 하겠다고 협박하는 등 다양한 공격이 과거부터 현재까지 지속적으로 발생되고 있다.

그림 1. '디도스 공격' 뉴스 검색결과

[그림 1]과 같이 '디도스 공격'이란 검색어로 뉴스검색을 해보니 다양한 기사 중에 "좀비 PC"라는 단어가 자주 보인다. 기사의 내용은 좀비 PC가 DDoS 공격에 이용된다는 내용이다. 좀비 PC란 원래부터 있던 존재가 아니라, 해커가 일반 사용자의 PC에 악성코드를 설치하여, 해커가 원격에서 원하는 시간에 원하는 방법으로 PC를 조정하여, DDoS 공격을 일으키는 수단으로 활용되는 PC를 말하며, 다시 설명하면 좀비처럼 바이러스에 감염되어 소유자의 의도와 관계없이 악용되는 PC를 말한다. 이런 좀비 PC를 많이 확보할수록 공격의 강도를 높일 수 있기 때문에 이런 좀비 PC를 거래하는 경우도 있으며, 많은 경우 자기 PC가 좀비 PC로 감염되었는지도 모르는 경우가 대부분이다.

보통 토렌트 등의 P2P를 이용한 파일공유서비스를 통해 상용프로그램이나 영화 등의 동영상을 다운로드하는 용도로 주로 사용하

는데, 24시간 계속 작동하는 가정용, 사무용 PC나 관리가 잘 되고 있지 않은 교육기관, 기업 등의 서버 등이 이런 좀비 PC로 많이 감염된다. 또한 스마트폰의 성능과 네트워크 속도가 빨라 지면서, 악성코드 링크가 포함된 문자 혹은 SNS 메시지를 발송하여, 클릭을 유도한 다음 정상적인 스마트폰을 공격에 악용하는 경우도 증가하고 있다.

정상 PC가 좀비 PC로 보통 감염되는 경로는 크게 2가지가 있다.

1. 영화, 동영상, 상용프로그램 P2P 자료 공유사이트 방문하거나 데이터 다운로드
2. 출처를 알 수 없는 이메일이나 문자에 첨부된 첨부파일 열람 혹은 URL 링크 클릭

사람들 간의 기본적인 신뢰를 기반으로 하는 심리를 이용하여 무심결에 클릭을 유도하게 만드는 방법을 '사회공학'이라고 말하는데, 이런 방법은 기술자라기보다는 사기꾼의 수법에 가깝다. 사실 아무리 기술적인 보안을 완벽히 하더라도, 인간적인 신뢰 심리까지 완벽히 관리하기는 어렵다. 전설적인 해커인 케빈미트닉는 사람은 아래와 같은 명언을 남겼다.

"기업 정보 보안에 있어서 가장 큰 위협은 컴퓨터 바이러스,
패치가 적용되지 않은 중요한 프로그램이나 잘못 설정된 방화벽이 아니다. 가장 큰 위협은 바로 당신이다."

DDoS 공격의 동작 방법은 [그림 2]와 같이, 공격자가 정상 PC를 악성코드로 감염시켜 좀비 PC로 만들고 이렇게 만든 많은 수의 좀비 PC에 공격명령을 내려, 동시에 여러 대의 좀비 PC가 공격대상 서버로 트래픽을 집중하는 방식으로 공격을 수행한다. 결국 얼마나 좀비 PC를 많이 확보했는지가 공격 성공의 관건인데, 최근에는 대부분의 PC 성능이 향상되고, 연결된 네트워크의 속도가 100Mbps 이상을 지원하는 환경이라, 과거보다 적은 수의 PC로도 충분한 파괴력을 일으킬 수 있게 되었다.

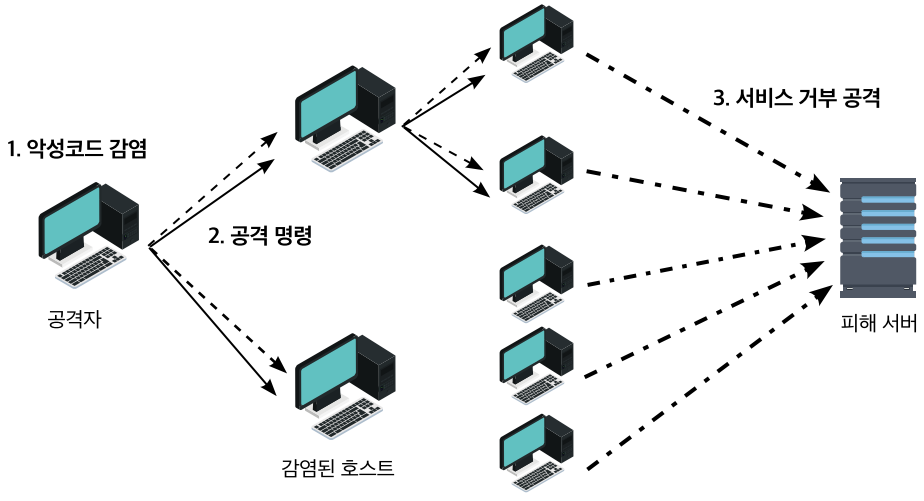

그림 2. DDoS 공격 구조

그럼 이런 공격을 막기 위한 DDoS 공격 방어기법에 대해 알아보자. 방어단계는 크게 두 단계로 나눌 수 있다.

1. **공격탐지** : 정상 트래픽과 공격 트래픽을 정확하게 구분하는 기능
2. **공격차단** : 정상 트래픽은 통과시키고 공격 트래픽만 정확하게 차단하는 기능

초기 DDoS 방어방식은 일단 정상과 공격을 구분하지 않고 대용량의 트래픽이 들어오면, 정상 트래픽과 공격 트래픽을 구분하지 않고, 피해 서버로 가는 트래픽을 모두 차단하는 방법으로 방어를 수행하였다. 이런 방식을 블랙홀 라우팅(blackhole routing)이라고

이선응 차장/김영준 과장
아이크래프트㈜ SNT본부 기술1팀

하는데, 현재까지 차단기법의 한가지로 KT, SKT, LGT 등의 회선 사업자에서 이런 방식을 일부 사용하고 있다.

피해 서버로 오는 트래픽에 "내가 공격 트래픽입니다"라고 표시되어 있지 않기 때문에 정상적인 사용자가 해당 서버에 접속하려고 하는 트래픽인지, 실제 공격 트래픽인지는 어떤 한가지 기준으로 판단하기에는 매우 어려우며, 보통 임계치(Threshold) 값을 설정하여 이 값을 경계로 판단하거나, 통계적인 기법을 이용하여 특정 시간 안에 특정한 트래픽이 얼마나 들어오는지를 평상시 학습하고 있다가, 평균값에서 일정 수준 벗어나는 트래픽 양이 들어오면 공격으로 인식하는 등 다양한 방식이 활용되고 있다.

실제 있었던 예를 조금 각색하여 설명하면, 뉴스를 제공하는 홈페이지가 있는데, 평일 오전 10시에는 100Mbps 정도의 트래픽이 일상적으로 발생되고 있었다고 한다. 그런데 갑자기 오늘 오전 10시에 트래픽이 1Gbps로 증가하여, 뉴스검색이 정상적으로 되지 않고, 뉴스제공 서버가 다운되고 방화벽도 CPU가 90%에 육박하여 정상동작을 못하는 증상이 발생하였다고 하면, 이것을 무조건 DDoS 공격으로 단정 지을 수 있을까? DDoS 공격으로 판단하여, DDoS 방어서비스를 급하게 설치하였는데도 정상적으로 공격이 차단되지 안았다고 한다. 어떤 문제가 있었던 걸까?

결론을 얘기하면, 어느 유명 연예인의 자살사건으로 해당 신문사의 기사가 네이버, 다음 등의 포털사이트의 대문에 노출되어, 많은 사람들이 궁금증에 해당 기사를 클릭하게 되면서 정상적인 기사 검색 트래픽이 폭주하여 발생한 경우로 확인되었다. 명절 귀성 기차표 예매, 대학 학기 초 수강신청, 인기 연예인의 콘서트 티켓 예매, 국가대표 경기의 입장권 예매 등 많은 트래픽이 일시에 몰리는 이벤트성 폭주 현상을 실제 공격과 정확히 구분하기는 무척 어렵다.

과거에 비해 공격을 탐지하는 방법이 많이 발전하였지만 현재도 100% 정확하게 공격 여부를 판단하는 것은 어려운 실정이다. 현재의 전략은 서버의 성능이 많이 발전하였고 서버 자체적으로도 DDoS 공격을 일정 수준 방어할 수 있는 기능을 추가하여, 웬만한 공격은 견딜 수 있게 구성한 후, 확연히 공격으로 판단되는 많은 양의 트래픽만 공격으로 경보를 발령하고, 일정 수준 이하의 트래픽 양은 그냥 서버로 전달하여 서버에서 자체적으로 방어하는 방법을 많이 사용하고 있다.

공격을 탐지하는 방법이 100% 정확할 수 없기 때문에 공격을 차단하는 방법도 조심스러울 수밖에 없다. 정말 확실히 공격 트래픽으로 판단될 경우에만 차단하고, 공격 여부를 판단하기 모호한 경우는 트래픽을 통과시켜야, 고객 서비스에 문제가 없기 때문이다. 보안관리자는 조직의 비즈니스성격과 보안운영지침에 따라 공격 트래픽이 통과되는 한이 있더라도 정상 트래픽이 차단되는 일이 없도록 할 건지, 아니면 정상 트래픽이 차단되는 경우가 있더라도 공격 트래픽은 100% 차단할지를 적정한 수준에서 결정하여 운영하여야 하는 딜레마가 생기게 된다.

예를 들면 인터넷회선을 제공하는 KT, SKT 같은 회선사업자의 경우 DDoS 공격으로 탐지했다고 하더라도, 실제 정상적인 서비스일 확률이 1%라도 있다면, 고객의 데이터를 마음대로 차단하였다가는 고객에게서 항의를 받을 수 있기 때문에 명백히 공격으로 확신이 되는 트래픽만 차단하게 되고, 반대로 고객사에서는 자체적으로 장비를 구축하여, 정상적인 트래픽이 일부 차단되는 경우가 있더라도, 고객서비스에 지장이 없는 것이 최우선 순위로 1%라도 의심이 되는 트래픽이라면 일단 차단하는 정책을 설정하는 것이 바람직한 방향이다. DDoS 트래픽에 대한 세부적인 차단방식은 기술적인 내용이 많이 포함되어, 이번 연재의 성격에 맞지 않아 자세하게 소개해 드리지 못하나, 기회가 있다면 다음 기회에 자세히 다루도록 하겠다.

APT 공격

다음으로 'APT 공격'이란 Advanced Persistent Threat의 약자로 지능적이고(Advanced) 지속적인(Persistent) 해킹공격의 통칭이다. 디도스 공격과 같이 공격 여부를 이용고객과 공격피해 대상이 모두 알 수 있도록, 비교적 단시간 동안 서비스를 방해하는 것이 목적이라면, APT 공격은 스파이침투와 동일하게 아무도 모르게 조용히 악성코드를 사내 PC에 설치하여 실제 피해를 당하는 당사자도 알 수 없게 오랫동안 몰래 조직의 전산자원을 대상으로 지속적으로 정보를 탈취하거나 특정한 날에 전산자원을 마비, 파괴하는 형태의 공격이다. [표 1]은 DDoS 공격과 APT 공격의 특성을 비교한 표이다. 두 공격은 여러 가지 특성에서 많은 차이가 있다.

DDoS 공격이 서비스를 마비시키는 한가지 목적을 달성하기 위해 수행하는 공격이라면, APT 공격은 여러 가지 방식을 조합하여 내부 자원에 침투한 다음 장시간 동안 여러 가지 목적으로 활용될 수 있는 최근에 유행하고 있는 지능화된 위협을 통칭한다고 볼 수 있다. 아직까지 용어 자체에 대한 개념 정립이 완료되지 않은 상태라 설명하는 사람에 따라서 다양한 공격형태로 정의되고 있다.

	DDoS 공격	APT 공격
공격 목적	대 고객 서비스 마비	정보 탈취 & 조작, 협박, 금품 요구 사보타지(서비스 중단 & 파괴)
공격 대상	한정적임	광범위함
	외부에 공개된 서버(Web, Mail, DNS)	내부 서버, 업무PC 등(그룹웨어, ERP, DB)
공격 기간	단시간(분 ~ 일 단위)	장시간(일 ~ 년 단위)
증상 확인	쉬움 (공격사실 확산이 목적)	어려움 (은밀한 침투가 생명)
탐지 난이도	중간 (트래픽 모니터링)	어려움 (PC, 트래픽, 서버 모니터링)
차단 난이도	중간 ~ 어려움 (서버증설, 대피소이전, 차단장비설치 대응필요)	중간 ~ 어려움 (공격사실 인지 후 모든 전산자원의 악성코드 탐지필요)
공격 대응 대상	네트워크 관리자 (네트웍 장비레벨에서 대응 및 차단이 가능)	조직 모든 구성원 (개인PC, 스마트폰을 포함한 사내 모든 전산자원에서 대응 필요)

표 1. DDoS 공격과 APT 공격 특성 비교

그럼 다음으로 APT 공격이 어떤 형태로 이루어지는지 살펴보자. [그림 3]은 전형적인 APT 공격방식을 이용하여 2016년에 발생한 인터파크 개인정보 유출 사고 공격 시나리오로써 4단계로 구분해 보았다.

1. 정찰, 유인

A. 공격대상조직을 선별한 후 권한이 높을 것 같은 임직원(전산담당자, CEO 등)의 이메일을 포함한 공격대상의 다양한 정보 등을 수집하여, 이메일 수신자가 의심 없이 악성코드를 실행할 수 있도록 이메일 내용을 위장하기 위한 자료수집단계

B. 수집된 정보를 바탕으로 타겟에게 악성코드가 포함된 파일을 제작하거나, URL 링크가 포함된 메일을 보내서 파일을 열어보거나, 링크를 클릭하게 유도함.

C. 예를 들면, 방송기술관련 종사자에게 최근 이슈가 되고 있는"UHD 방송기술 관련 동향 및 이슈 사항"이나"최신 스마트폰 보조금 최대로 지급합니다"라는 링크를 달아 클릭을 유도하여, 악성코드가 사용자도 모르게 PC나 스마트폰에 설치되게 만듦

2. 내부 PC 감염, 백도어(Backdoor) 설치

A. 설치된 악성코드는 사전에 지정된 외부 서버에 접속하여 해커에게 감염 사실을 알리고, 향후 공격에 필요한 추가 악성프로그램을 다운로드하여 실제 수집 및 공격 동작이 가능하게 준비함

B. 향후 관리를 위해 언제나 원격 접속 가능한 수단으로 백도어를 설치한다. 즉 아무도 모르게 공격자만 알 수 있는 개구멍을 만들어 두는 것임.

3. 감염확산, 정보 수집

A. 일단 한 대의 PC가 해커에 장악되면, 내부에 있는 다른 전산자원을 검색하여 취약점을 발견하여 하나하나 감염시켜 나간다.

B. 전산관리자나 회사 본부장급의 PC를 감염시켜 서버의 접속정보나 인사, 영업, 회계, 연구결과 등의 고급정보를 수집한다.

이선응 차장/김영준 과장
아이크래프트㈜ SNT본부 기술1팀

4. 중요 정보 유출, 전산인프라 공격수행

A. 수집된 정보를 해커가 준비한 서버로 야간이나 휴일 등 감시가 느슨한 시간을 이용하여 크기를 작게 분할하여 외부로 유출시킴

B. 수집가능한 정보를 모두 탈취한 후에도 오랜 시간(1년 이상) 잠복해 지속적으로 자료를 유출함

C. 필요에 따라서는 정치적, 사회경제적 필요성에 따라 D-Day를 지정하여, 조직업무를 마비시키기 위해 고개정보를 삭제하거나 서버를 다운시키거나 업무 PC를 포맷하는 등의 전산 인프라 공격을 수행함

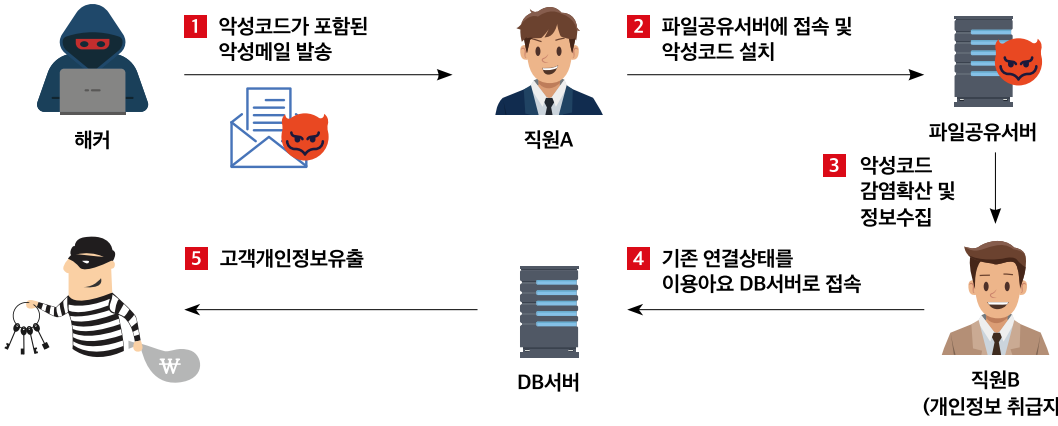

그림 3. APT 공격 수행 순서 / 출처 : 과학기술정보통신부

그럼 APT 공격에 대한 방어전략을 알아보자. 앞에서 DDoS와 APT 공격의 차이점에서 알 수 있듯이 APT 공격은 어떤 특정한 행위가 아닌 다양한 단계를 거쳐 이루어지므로, 이에 대응하기 위해서는 단계별로 세분화되어야 한다.

1. 정찰, 유인 단계

A. **개인정보 노출 차단** - 홈페이지 등의 노출된 게시판에 전산관리자나 관리자급의 E-Mail 주소 및 조직원에 대한 정보노출을 자제

B. **임직원 보안교육 실시** - 전 임직원을 대상으로 정기적인 보안교육을 실시하여, 출처가 불분명한 이메일의 첨부파일과 링크 클릭을 방지하고 주기적인 모의침투 훈련으로 경각심을 고취시킴

2. 감염, 내부 유입단계

A. **메일보안장비, 악성코드 탐지장비 도입** - 대부분의 공격이 메일을 통해 시작되므로, 악성코드가 첨부된 메일을 탐지하여 사내 PC에 다운로드 되는 것을 차단함

B. **사내 인터넷사용 제한** - 사내 PC에서 인터넷 접속 시 악성사이트에 방문하지 못하도록 URL 차단 기능을 동작시킴

C. **PC 보안 강화** - 업무 PC 및 사내 서버의 백신프로그램을 정기적으로 업데이트하고 탐지설정 상태를 점검하고 윈도우 업데이트 패치를 주기적으로 수행

3. 확산 단계

A. **내부 트래픽 모니터링 시스템 도입** - 감염된 PC가 내부자원을 대상으로 수행하는 다양한 공격행위 및 해커의 원격접속 트래픽을 탐지할 수 있도록 사내에서 발생되는 모든 트래픽에 대한 모니터링을 하여 감염된 PC 및 서버를 탐지 후 제거

B. **2, 3차 방화벽 도입** - 중요서버 앞에 별도의 방화벽을 설치하여, 사내 PC에서 중요서버에 접속을 못 하게 차단하고, 서버접속은 별도의 지정된 안전하게 관리되는 PC에서만 접속이 가능하게 통제

4. 정보유출 단계

A. **DB 방화벽 도입** - DB 접속을 위한 별도의 인증단계를 두어 서버관리자 권한으로 데이터 조회를 차단하고, 자료 열람 이력을 남겨, 비정상적인 조회 내역을 추적하여 감염 PC를 식별하고 2차 사고를 방지

B. **DB 암호화 솔루션 도입** - 자료가 유출되더라도 별도의 암호화를 풀 수 있는 키(key)가 없으면 자료를 확인할 수 없도록 자료를 암호화

C. **인터넷방화벽 보안정책강화** - 사내에서 인터넷으로 나가는 통신에 대한 정책을 엄격하게 설정하여, 수집한 정보를 외부 서버로 유출시키는 것을 차단하기 위해 인터넷 사용 주소나 사용서비스(port)를 엄격하게 제한

APT 공격은 매우 은밀하게 이루어지는 공격이다 보니, 조직 내에 감염 PC가 얼마나 존재하는지 확인할 수 있는 방법이 매우 제한적이다. 대부분의 조직은 업무 PC와 사내 서버에 설치된 백신을 통합관리 하는 수준을 벗어나지 못하고 있다. 문제는 백신이 알려진 악성코드만 탐지가 가능하지, 신규로 만들어져서 아직 외부에 알려지지 않은 악성코드는 탐지가 힘들다는 것이다. 실력이 있는 해커집단이나 국가 단위의 조직의 경우 기존에 존재하는 악성코드를 재활용하지 않고, 기존 악성코드를 변형하거나 공격대상의 취약점을 파악하여 공격대상에 최적화된 악성코드를 맞춤 제작하여 활용하는 사례가 많기 때문에 기존 백신으로 탐지가 힘든 경우가 많다.

공격을 하는 집단과 공격을 방어해야 하는 집단이 있는 한 언제나 도전과 응전의 역사가 반복되었다. 공격자가 새로운 공격방식을 개발하면, 방어자는 이 공격을 무력화할 수 있는 방어 수단을 찾아내고, 공격자는 다시 이런 방어수단을 무력화할 수 있는 공격수단을 개발하는 무한반복의 과정이 지속되고 있다.
[그림 4]와 같이 탐지를 회피하기 위해 악성코드는 계속 진화하게 되면서, 악성코드 탐지기술도 거기에 대응하여 다양한 기술을 이용하여 코드를 악성여부를 진단한다. 단순한 파일패턴 이외에 해당 코드가 얼마나 많이 사용되고 있는지, 공격패턴과 100% 일치하지 않더라도 어느 정도 일치하는지, 실제 가상 PC에 악성코드를 설치하여 어떻게 동작하는지 검사하는 방법들이 개발되었다.
또한 탐지시스템의 부담이 증가하여 처리속도가 떨어지는 것을 보완하기 위해 성능이 좋은 외부시스템을 활용하여 대신 분석업무를 수행하는 클라우드 기반의 탐지기능을 활용하는 방법도 많이 사용되고 있다.

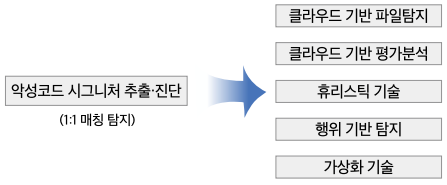

그림 4. 악성코드 탐지기술 / 출처 : 아이뉴스24

APT 공격 단계의 초기 단계인 감염단계를 차단하게 되면 이후 단계는 자연스럽게 차단되기 때문에 방어자의 입장에서는 이 초기 단계에 방어역량을 집중하는게 유리하다. 이메일에 첨부되거나 링크가 걸려 유입되는 악성코드를 정확히 탐지할수록 방어성공확률이 올라가기 때문에, 앞에서 설명한 것과 같이 기존에 알려진 공격에 대한 패턴 감시뿐만 아니라, 알려지지 않은 악성코드의 탐지를 위하여, 가상 PC 등을 이용하여 악성코드를 탐지하는 방법을 고안하였다.

이런 탐지방법의 확산으로 악성코드 감염성공률이 낮아지자 공격자는 다음과 같은 대응방법을 고안하게 되었다.

1. PC에 설치된 후 바로 동작하지 않고 일정 시간 잠복 상태로 숨어서 탐지를 회피
2. 가상의 PC의 OS이름, 키보드, 마우스 입력을 확인하여 가상 PC로 판단되면, 공격 동작을 수행하지 않고 정상코드로 위장하여 탐지를 회피

이런 방식을 적용하자 다시 악성코드를 PC 감염시키는 성공률이 올라가게 되자 방어자는 다시 탐지방법을 추가하였다.

1. 가상 PC의 시스템시간을 빨리 가게 만들어, 악성코드의 시간 확인기능을 속임
2. 가상 PC로 탐지되지 않기 위해 OS 이름을 바꾸고, 가상의 키보드, 마우스 입력신호를 추가하여 정상 PC로 위장
3. 악성코드의 일반적인 트래픽을 발생시키거나 파일을 저장하는 동작상태만 모니터링하는 것이 아니라, CPU로 보내는 명령전달상태를 모니터링하여 악성코드를 탐지

필자가 알고 있는 상황은 이 정도까지이나, 공격자와 방어자는 이후에도 계속 새로운 탐지 우회방안과 공격 탐지방안을 개발하며, ICT가 사용되고 있는 한 끝없는 싸움을 반복할 것으로 예상된다.

다음 시간에는 디지털 방송시스템에서의 네트워크 보안적용방안과 최신 정보보호 기술동향, 국내 정보보안 관리의 현실에 대해 설명하는 것으로 마무리하겠다.