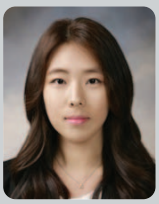
새롭게 진화하는 위협의 패러다임 – 지능형 지속 위협(APT)


유 홍 렬
연세대학교


정 성 미
연세대학교


권 태 경
연세대학교

Ⅰ. 서 론

1. 모든 것이 연결되는 세상

세상의 모든 사물들이 유·무선 네트워크를 통해 상호 연결되는 사물인터넷(IoT : Internet of Things)은 최근 IT 업계에서 화두가 되고 있는 개념이다. 이미 일상생활 속에서 널리 적용되어 있는 사물인터넷의 응용은 우리 삶의 모습을 크게 변화시켰다. 사물 간 결합이 활성화되려면 사물인터넷 및 통신 기술의 표준화가 필요한데 이미 국내·외 여러 단체에서 다양한 표준화 노력을 진행하고 있다. 〈표 1〉은 사물인터넷과 관련된 표준화 추진 단체를 나열하고 주요내용에 대하여 간략하게 기술한 것이다.

이제는 사물인터넷을 뛰어 넘어 모든 만물이 소통하는 만물인터넷(IoE : Internet of Everything)이 주목받는 개념으로 부상 하면서 상상 속에서나 가능했던 부분들이 현실 속에서 가능하게 되었다. 사물인터넷 또는 만물인터넷을 통한 사물-기기, 기기-기기, 사람-기기간의 결합은 기존에 없던 새로운 가치를 만들어내고 있다.

〈표 1〉 사물인터넷 관련 표준화 동향[1]

표준화 기관	주요 내용
IETFIoT	모든 사물을 IP기반으로 연결하고 다양한 서비스를 제공하는데 필요한 기술적 요구사항에 대한 표준화 (6LoWPAN WG, ROLL WG, Core WG, Lwig WG 등)
ITU-T IoT-GSI	IoT 시스템 기술의 표준화 (IoT 정의, 범위, 응용/서비스, 네트워크와 디바이스, 보안 등)
ITU-TJCA-IoT	Generic reference model architecture, IOT standards roadmap, NID(Network ID System) 및 USN terms and definitions 정의
ISO/IECJTC 1	IoT 관련 시장 요구사항과 표준간의 Gap 분석을 통한 효율적인 정보 기술의 표준화

오늘날 다양한 스마트 기기들은 사물인터넷과 밀접한 관련이 있다. 기기 간 네트워크 기술의 발전은 TV, 냉장고, 세탁기, 에어컨, 청소기 등 각종 가전기기들을 스마트 가전으로 변화시켰다. 이와 더불어 스마트폰, 클라우드 서비스 등 다양한 기술 및 서비스와의 결합을 시도하고 있다. 이것은 가전 뿐 아니라 스마트 그리드, 스마트 오피스 등 산업을 불문하고 모든 영역에서 진행되고 있다.

2. 연결 복잡도에 따라 증가하는 취약점들

IT기술간 융합과 결합으로 인하여 스마트 기기의 물리적인 복잡도는 기하급수적으로 증가하고 있다. 두 개체를 연결하거나 결합하기 위해서는 기본적으로 입/출력 인터페이스(interface)와 전달 매체(medium), 프로토콜(protocol)이 필요하다. 연결되는 개체가 많아질수록 인터페이스, 매체의 개수, 사용되는 프로토콜의 수는 증가한다. 이때 이 시스템의 취약점은 연결되는 수만큼 증가할 수 있다.

보호해야 할 시스템은 갈수록 복잡해지고, 시스템을 침해하기 위한 공격기법은 꾸준히 진화하거나 새롭게 개발되고 있어

일반적으로 컴퓨터 네트워크에서 그물형 토폴로지(mesh topology)는 가용성 측면에서 안전성이 높다고 평가되어 있다. 한 링크가 고장 나더라도 전체 시스템의 가용성에는 큰 문제가 되지 않기 때문이다. 또한 두 개체간의 데이터는 전용선으로 보내지기 때문에 비밀성과 보안성을 갖고 있다. 마지막으로 모든 노드는 표준화된 프로토콜을 사용할 수 있다.

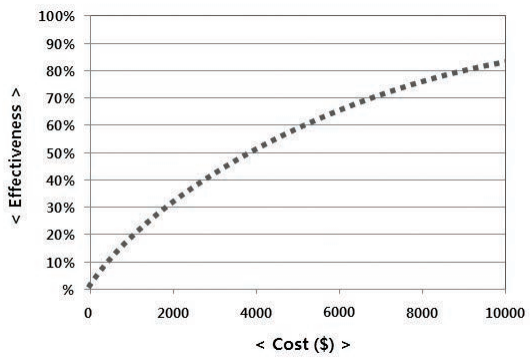
하지만 전통적인 전자기기들이 디지털화 된 후 다양한 기기들과 결합되는 오늘날 사물인터넷 환경에서는 단일화된 프로토콜이 존재하지 않는다. 따라서 각각의 인터페이스와 각각의 매체, 각각의 프로토콜에 대한 보안성이 모두 고려되어야 한다.

이것이 중요한 이유는 오늘날의 스마트 기기들은 실질적으로 우리의 일상생활에 잠재적으로 큰 위협이 될 수 있기 때문이다. 가전제품이나 산업시스템을 망라하고 많은 스마트 기기들은 개인 및 산업정보 등과 같은 데이터를 끊임없이 생성하고 저장하며, 전달한다. 또한 기기 간 통제를 위한 명령의 전달은 디지털화 된 데이터를 통해 이루어진다. 오늘날 해커들은 이러한 데이터를 공격함으로서 개인정보, 산업기밀을 유출하거나 기기 자체의 오작동을 유발한다. 이러한 공격의 새로운 패러다임 중 하나는 '지능형 지속 위협(APT : Advanced Persistent Threats)'이다.

본 고의 순서로는 II장에 변화하는 위협에 대해서 살펴보고, III장에서는 지능형 지속 위협의 정의, 특징, 공격 단계 및 사이클과 주요 사례에 대해 설명한 뒤, IV장에서 결론 및 대응방안에 대해서 기술한다.

Ⅱ. 변화하는 위협

보안은 투자수익(ROI : Return on Investment) 측정이 쉽지 않아 투자보다 비용이라는 인식이 강하다. 시스템의 복잡도가 낮고 구성이 단순했던 과거에는 컴퓨터 바이러스, 소프트웨어 크래킹 등 시스템을 침해하기 위한 공격 기법들이 단순했고 그 종류가 많지 않았다. 따라서 보안에 돈을 투자하면 어느 정도 침해를 방지할 수 있었고 보호수준은 증가하였다. 하지만 과거와 달리 오늘날에는 〈그림 1〉에서 볼 수 있는 것처럼, 보안에 투자하는 금액이 증가할수록 보호수준은 낮은 증가율을 보인다. 또한 투자 금액이 어느 정도의 임계점에 도달하면 증가하는 보호 효과는 거의 미비하다.



〈그림 1〉 시스템패치에 투자하는 비용대비 보호 효과[2]

우리가 보호해야 할 시스템은 갈수록 복잡해지고 있다. 서버, 운영체제, 메모리, 입/출력 인터페이스, 네트워크, 소프트웨어, 스토리지 등 보호해야 할 영역은 늘어만 가고 있다. 한편, 시스템을 침해하기 위한 공격기법은 꾸준히 진화하거나 새롭게 개발되고 있다. 트로이 목마(trojan horse), 논리 폭탄(logic bomb), 시한폭탄(time bomb), 트랩도어(trapdoor), 백도어(backdoor), 웜(worm), 래빗(rabbit), 서비스 거부 공격(DoS : Denial of Service), 제로데이 공격(zero-day attack) 등 공격의 유형과 기법들이 무수히 많아 분류할 수도 없을 정도이다. 공격자들은 이러한 기법들을 독립적으로 사용되기보다 서로 결합하여 사용한다. 이 말은 그만큼 우리가 보호해야 할 시스템의 많은 영역이 존재하며, 각 영역별로 방어해야만 하는 공격기법은 더욱 많다는 것이다.

시스템의 구성이 복잡할수록 한 시스템의 모든 영역을 보호하는 데 많은 비용이 필요하다. 하지만 많은 비용을 투자하더라도 그 효과가 증가하지 않는 다양한 원인이 있는데, 위협의 진화 속도는 매우 빠른 반면 대응기법은 빠르게 진화하지 못하고 있는 것이 그 중 하나이다. 보안을 그렇게 강조를 해도 침해사고가 끊이질 않는 이유이다. 더 이상 시그니처 기반의 백신, 규칙기반의 IDS(Intrusion Detection System), IPS(Intrusion Prevention System) 등 전통적인 방어기법으로는 끊임없이 진화하는 지능형 지속 위협에 대응할 수 없다.

위협의 진화 속도는 매우 빠른 반면, 대응 기법은 빠르게 진화하지 못하고 있어

최근 발생하는 많은 침해 사례들은 개인, 산업, 정부의 정보를 탈취하여 기밀성을 해치는 정보 유출의 위협과 오작동, 파괴 등 무결성과 가용성을 해치는 물리적 위협으로 크게 나누어 볼 수 있다.

1. 정보 유출의 위협

인터넷, 모바일과 같은 정보기술의 발달은 정보의 탈물질화를 야기하였다. 이미 많은 개인정보가 온라인에서 활용되고 있으며 이것은 비단 신상에 관한 정보뿐만이 아니다. 취미, 생각, 인간관계, 위치정보 정보 등이 차곡차곡 SNS에 쌓이고 있다. 기업에서는 ERP와 같은 다양한 경영정보시스템을 통해 영업 및 기술 정보를 디지털 형태로 보관, 활용하고 있으며 CRM과 같은 시스템을 통해 개인정보를 영업정보와 결합하려는 노력을 기울이고 있다.

특히 센서와 모바일 관련 기술이 발달하고, 분야와 산업을 망라한 다양한 것들이 융합 및 결합하면서 가히 빅데이터라 불릴 만큼 무수한 데이터들이 발생하고 있다. 이러한 데이터는 데이터마이닝을 통해 새로운 가치를 창출할 수 있는 만큼 공격자들이 노리는 대상이 될 수 있으며 그만큼 보호 가치가 크다고 할 수 있다.

2. 물리적인 통제의 위협

주로 물리계층에서 전기적 신호를 통해 제어가 이루어졌던 전통적인 전자기기와 달리, 오늘날 스마트 기기는 스스로 데이터를 생성하고, 저장하고, 결합하여 새로운 정보를 만든 후, 그 정보를 근거로 다른 기기를 제어한다. 이때 제어는 물리적인 신호가 아니라 논리적이며, 디지털화된 데이터를 통해 이루어진다. 이것의 장점은 이질적인 기종간에도 표준화된 인터페이스와 프로토콜을 사용할 수 있다는 것이고, 먼 거리에서도 원격으로 제어를 할 수 있다.

특히 모바일 환경이 진화하면서 많은 스마트 기기들이 등장했는데, 이제는 한걸음 더 나아가 사람-기기, 기기-기기, 사물-기기 간의 다양한 제어가 시도되고 있다. 스마트 홈, 스마트 카, 전자결제 등이 대표적인 예라고 할 수 있다. 컴퓨터로 TV를 통제하고 자동차 문을 열 수 있으며 조명을 끌 수 있다.

하지만 냉장고, 난방기, 청소기, 변기 등 기존의 많은 전자기기들이 인터넷에 연결되면서 해커들에 의한 위협 역시 증가하고 있다. 오늘날 스마트 기기들은 GPS, 카메라, 지문인식과 같은 센서를 내장하여 스스로 데이터를 수집하며, 수집된 데이터를 저장하는 스토리지를 갖는다. 저장되어 있는 데이터를 계산하거나 가

공하여 사용자의 판단을 도울 CPU와 이 모든 것들을 통제하는 운영체제까지, 사실상 모든 것이 컴퓨터라고 볼 수 있다. 문제는 이와 같은 복잡한 시스템이 악의적인 해커들의 위협에 쉽게 노출되어 있어 오작동, 파괴와 같은 가용성이 침해될 수 있다는 점이다. 이미 스마트TV, 스마트 카 등에 대한 공격이 많은 정보보호 전문가들에 의해 시연된 바 있다.

3. 사례 분석–스마트 기기

3.1. 자동차 내부 네트워크 침입

최근의 일부 스마트 카는 엔진 출력, 엔진오일 잔여량, 연비, 주행거리, 잔고장 등을 스마트폰에서 직접 볼 수 있는 자동차 진단 앱을 제공하고 있다. 스마트폰에서 자동차 진단 앱을 실행하면 외부의 무선 네트워크와 자동차 내부의 CAN(Controller Area Network) 버스를 거쳐 ECU(Electronic Control Unit)로 직접 연결된다. 이러한 구조는 악의적인 공격자의 타겟이 될 수 있으며 ECU를 악의적으로 제어했을 경우 자동차의 오작동이 발생할 수 있다[3].

〈그림 2〉은 간단한 자동차 공격의 시나리오를 보여준다. 공격자는 자동차 관리 앱에 악성코드를 심어 앱 스토어에 배포한다. 만약 사용자가 악성 앱을 다운로드 받아 실행하면 해당 앱은 자동차의 ECU로 연결되며 사용자에게 자동차의 다양한 상태를 제공한다. 사용자는 자신이 악성 앱을 설치했다는 것과 악성코드에 감염되었다는 사실을 모르기 때문에 이러한 서비스가 정상적인 것처럼 보인다.

한편 해당 악성 앱은 사용자에게 보이지 않는 백그라운드에서 공격자가 미리 준비해 놓은 서버로 연결된다.

〈그림 2〉 자동차 내부 공격 시나리오[3]

사용자가 자동차 관리 앱을 실행했다는 것과 현재 ECU와 연결되어 있다는 사실을 알게 된 공격자는 사용자의 스마트폰을 통해 자동차를 원격으로 제어할 수 있게 된다. 즉, 사용자의 스마트폰이 좀비가 된 것이다.

이와 같은 공격으로 가속, 엔진 폐쇄, RPM 조작, 핸들 제어 등의 물리적인 통제가 가능할 수 있다. 자동차 해킹은 개인 프라이버시 침해뿐만 아니라 인명 피해로 이어질 수 있다는 점에서 치명적인 위협이 될 수 있다.

3.2. 스마트 냉장고 해킹

2013년 말부터 2014년 초까지 스마트TV와 냉장고 등 가전기기를 해킹하여 스팸 메일을 보낸 사례가 발견되었다. 약 75만 건의 피싱과 스팸 메일이 홈 네트워크 환경에 적용된 각종 기기의 보안 취약점을 이용하여 발송되었다. 미국의 보안업체인 Proofpoint는 악성 이메일 중 25%가 스마트 가전기기와 같이 사물인터넷 개념이 적용된 기기에서 발생했다는 것을 발견하였다[4]. 이러한 공격은 해당 스마트 기기들이 봇넷(botnet)의 역할을 함으로서 가능했다. 특히 사물인터넷 개념이 적용된 기기에서 발생하는 이러한 공격을 Proofpoint는 씽봇(thingbots)이라고 명명했다. 해킹에 이용된 스마트 가전기기들은 인터넷상에서 암호가 풀려있거나 비밀번호가 초기 값인 채 노출돼 있는 등의 보안 조치가 허술해 해커들의 많은 표적이 되고 있다. 〈그림 3〉는 스마트 냉장고를 이용하여 스팸메일을 발송하는 공격 시나리오를 보여주고 있다.

〈그림 3〉 스마트 냉장고 공격 과정 시나리오

〈그림 4〉 스마트TV를 이용한 홈쇼핑 공격

3.3. 스마트TV 피싱 공격

스마트TV도 위협에서 자유롭지 못하다. 시장조사업체인 DisplaySearch에 따르면 스마트TV는 2012년 6900만대, 2013년 1억800만대가 팔렸으며, 2016년에는 2013년도의 두 배에 육박하는 1억 9800만대가 팔릴 것으로 전망했다[5]. 이처럼 스마트TV는 스마트폰에 비해 보급률이 낮지만 보급이 확산됨에 따라 점차 많은 공격이 이루어질 것으로 예상된다.

이전 절에서 언급한 냉장고 봇넷은 스마트TV에서도 발견되었다. 또한 TV를 이용해서 Phishing과 같은 사회공학적 공격이 이루어지기도 했다. 이러한 공격을 Tvishing(TV + Phishing)이라고 부른다. 홈쇼핑 화면에 공격자의 계좌번호 혹은 전화번호를 바꿔치기해 사용자에게 입금을 유도함으로서 피해를 발생시킬 수 있다.

3.4. 로봇청소기 도청 및 감시

아직 로봇청소기의 공개된 취약점은 알려져 있지 않으나 현재의 시스템으로도 충분히 해킹이 가능하다고 보고 있다. 특히 로봇청소기는 센서를 부착하고 있으며 움직일 수 있는 특성이 있다. 따라서 해커가 원하는 곳으로 이동해 도촬을 하는 등의 공격을 수행할 수 있다. 2013년 말 오스트리아의 한 가정집에서는 로봇청소기가 갑자기 저절로 스위치가 켜진 채 전기열판 위로 올라가 그곳에서 소진된 사례가 있다[6]. 이것은 해킹 공격에 의한 것이 아니었다. 하지만 로봇청소기를 공격하여 원격으로 조정했을 때 화재 등 물리적인 공격이 가능하다는 것을 시사하고 있다.

〈그림 5〉 화재로 전소한 로봇청소기 (출처 : metro.co.uk)

앞서 본 다양한 사례처럼, 스마트라는 수식어가 붙은 모든 사물인터넷 기기들이 이와 같은 위협에 노출되어 있다. 과거, 전자기기의 위협이란 화재나 오작동으로 인명의 피해였다. 오늘날 전자기기의 위협은 정보 유출과, 데이터 무결성 파괴에 의한 물리적인 통제 위협이 포함된다.

이와 같이 공격의 유형과 방법은 끊임없이 변화하고 있다. 기기 간의 융합으로 인해 시스템의 복잡도가 높아질수록 전통적인 보안 요구사항은 적용되지 않는다. 모든 가능성을 열어두고 사물인터넷에 대한 보안 위협을 고려해야 한다. 이와 관련해서 지능형 지속 위협의 특징을 이해하는 것은 매우 중요하다. 갈수록 복잡해지는 시스템에서 위협이 어떻게 변화하고 있는지 우리에게 많은 시사점을 제공하기 때문이다.

Ⅲ. 지능형 지속 위협

1. 지능형 지속 위협의 정의

지능형 지속 위협의 어원은 미 공군에서 유래된 것으로 알려졌다. 2009년 7월, Mike Cloppert는 자신의 블로그에서 2006년 미 8공군(USAF, United States Air Force)에서 있었던 한 회의에서 지능형 지속 위협이라는 용어를 처음 들었다고 주장하면서, "장기간에 걸친 목표와 전략을 가지고 정보전에 참여하는 수준이 매우 높은 적"이라고 표현했다[7]. 이 표현에서 강조된 위협의 특징은 '장기간', '목표의식', '높은 수준' 이다.

지능형 지속 위협이 본격적인 화두로 등장한 것은

2010년 1월이다. 당시 구글은 중국 정부의 요청에 따라 이루어졌던 검색 결과 검열에 협조하지 않을 것이며 중국 정부가 이것을 수용하지 않으면 중국에서 철수하겠다고 선언했다. 하지만 그 이면에는 중국에서 조직적으로 이루어졌던 지메일(G-mail)에 대한 공격이 있었다. 'Operation Aurora'로 불리는 이 공격은 2009년 중반부터 그해 말까지 이루어졌으며 구글 뿐만이 아니라 시만텍, 어도비 시스템, 야후, 주니퍼 네트워크 등 다수의 미국 IT업체들이 공격의 대상이었다[8].

위 공격이 발생한 같은 달 말, 미국의 정보보안 업체인 Mandiant사는 'M-Trends : The Advanced Persistent Threat' 라는 보고서에서 지능형 지속 위협을 "미국 정부 및 민간 기업 컴퓨터 네트워크를 대상으로 체계적으로 공격하는 수준이 높고 목표의식을 가진 상호 협력하는 공격자들의 그룹"으로 정의했다[9]. 여기서 알 수 있는 특징은 공격의 대상이 체계적인 '조직'이라는 것이며, 공격의 대상이 '미국'이라는 것이다.

Mandiant사의 정의는 지금도 널리 인용되고 있다. 그러나 위협의 객체를 미국 정부와 방위산업, 민간업체로 한정했다. 또한 오래전부터 지능형 지속 위협의 주체로서 중국을 염두하고 보고서를 작성했다. Mandiant사는 지능형 지속 위협의 주체와 객체의 대상을 각각 특정 국가로 한정함으로서, 지능형 지속 위협이라는 용어가 일반화된 정의로 여겨지는 것을 거부했다. 즉, 특정한 공격의 한 고유명사로 사용되길 원하는 것으로 보인다. 실제로 2013년 초 Mandiant사는 지능형 지속 위협을 가하는 중국에 위치한 인민해방군의 한 부대를 'APT1'이라고 명명하기도 했다[10].

이후 많은 학자들은 Mandiant사에서 제시했던 정의를 참조하여 지능형 지속 위협의 일반적인 정의를 만들었다. Frankie Li 등은 "특정한 목표 컴퓨터나 전체 네트워크를 대상으로 정교하고 체계적으로 공격하는 목표의식을 가진, 상호 협력하는 그룹에 의해 실행되는 사이버 공격"이라고 정의했다[11]. 2011년 3월 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)는 지능형 지속 위협을 다음과 같이 정의했다. "고도의 전문 지식과 충분한 리소스를 가진 공격자가 복수의 공격 요소(사이버 공격, 물리적 공격, 사기 등)를 사용해서 목적 달성의 기회를 만들기 위한 공격이다. 통상 그 목적으로는 조직의 정보 기술 인프라 내에 침입하기 위한 발판을 구축하고 확대하여, 정보의 지속적인 도용, 조직의 중요한 업무 수행을 방해하거나, 미래에 그러한 위협 행위를 준비하는 일에 있다. 지능적 지속 위협은 장기간에 걸쳐서 반복적으로 표적을 쫓거나, 시스템 관리자의 방어 노력에 대응하거나 적응하고, 목적을 달성기 위해서 필요한 수준까지 지속적으로 상호작용을 유지한다[12]."

> **지능형 지속 위협이란 특정한 목표 컴퓨터나 전체 네트워크를 대상으로 정교하고 체계적으로 공격하는 목표의식을 가진, 상호 협력하는 그룹에 의해 실행되는 사이버 공격**

이후 많은 문헌에서 사용되는 지능형 지속 위협의 정의는 대체로 위에서 언급한 Mandiant, NIST, Frankie Li 등을 참조하고 있다.

2. 지능형 지속 위협의 특징

지금까지 나온 정의들을 보면 위협의 특징을 나열함으로서 구성되어 있기는 하나, 정의에 따른 명확한 위협 판별은 어려울 수 있다. 용어 자체가 추상적인 의미를 담고 있으며 다양한 특징들을 포함하고 있기 때문이다. 즉, 일종의 버즈워드인 셈이다. 그럼에도 불구하고 우리가 지능형 지속 위협에 주목해야 하는 이유는 전통적인 위협과 명확히 다른 특징들이 존재하며 오늘날, 위협이 어떠한 방식으로 진화하는지 분명하게 보여주는 동시 많은 시사점을 제공하기 때문이다.

지능형 지속 위협이 '지능적'이고, '지속적' 위협이라는 점은 많은 문헌에서의 공통된 시각이다. 그렇다면 지능적이라는 것은 무엇을 의미하는 것이며, 무엇이 지속된다는 것일까? 지능형 지속 위협을 설명하는 기존의 많은 문헌들이 위협을 '지능형(advanced)', '지속(persistent)', 위협(threat)'으로 나누어 설명하고 있다. 그 중에서 대표적인 두 개를 〈표 2〉에 나열하였고,

〈표 2〉 지능형 지속 위협의 특징

	Bejtlich[13]	Command Five[14]	위협을 나타내는 키워드
advanced	컴퓨터 침입의 모든 범위를 다룰 수 있는 적을 의미한다. 그들은 잘 알려진 공개적인 취약점을 이용할 수 있고, 혹은 새로운 취약점을 연구하고 표적에 맞춘 익스플로잇을 개발할 수 있다.	해커는 탐지를 회피할 수 있는 능력을 가진다. 또한 잘 보호된 네트워크에 엑세스하고 연결을 유지할 수 있다. 해커는 일반적으로 잘 적응한다.	알려진 취약점 사용 (well-known vulnerabilities) 알려지지 않은 취약점 사용 (research new vulnerabilities) 공격의 조합 (multiple attack methodologies)
persistent	그들은 미션을 완수하기 위하여 공식적으로 일이 맡겨진다. 우연한 기회를 틈타 침입하지 않는다. 그들은 정보부대와 같이 지시를 받고, 의뢰자를 만족시키기 위해 일한다.	해커는 우리의 컴퓨터 네트워크로 접근하려고 하나, 우리는 그것을 막으려 한다. 하지만 위협의 지속성은 그러한 노력을 어렵게 한다. 해커가 한번 접근에 성공하면 제거하기는 매우 어렵다.	의뢰인 (master) 기간 (period) 상호작용유지 (maintain the level of interaction)
threat	상대는 목적이 없는 단순 공격 코드 조각이 아니다. 상대는 위협이다. 조직적이고, 자금력이 있으며, 동기가 있다. 어떤 사람들은 일당으로 구성된 다양한 그룹이라고 말한다.	해커 위협은 하고자 하는 의도나 생각뿐만이 아니라 전자적으로 저장된 민감한 정보에 접근하여 얻는 능력까지 포함한다.	조직화 (organization) 목적 (goal) 위협대상 (target) 공격방법 (attack method)

위협의 정의와 설명에서 드러나는 공통된 특징을 키워드로 추출하였다.

2.1 지능형 (advanced)

공격 행위자의 능력으로 설명된다. 시스템의 모든 영역을 침입할 수 있는 능력에 해당되며, 공격 시 다양한 공격 방법들과 도구들을 필요에 의해 조합한다. 잘 알려진 공개적인 취약점을 이용할 수 있으나, 알려지지 않은 취약점을 연구하거나 표적에 맞춘 익스플로잇을 개발할 수 있다. 마지막으로 은밀한 공격을 위하여 탐지를 회피할 수 있는 능력이 있다.

1) 알려진 취약점 사용 (well-known vulnerabilities)

알려진 취약점은 백신이나 기타 다양한 방어 시스템으로 충분히 대응할 수 있을 것으로 생각하는 사람들이 많다. 하지만 알려진 모든 시스템이 모든 취약점에 저항력을 가지고 있지는 않다. 따라서 지능형 지속 위협은 기존에 알려진 취약점을 적극적으로 찾아 공격에 활용한다. 이 말은 우리의 시스템이 모든 취약점에 대응할 수 있어야 한다는 것을 의미한다.

2) 알려지지 않은 취약점 사용 (research new vulnerabilities)

제로데이 공격은 시스템의 취약점을 이용하여 공격하는 것을 말하는데, 특히 해당 취약점에 대한 패치가 공개되지 않은 취약점을 악용하는 기법이다. 취약점이 공개되면(혹은 공개되지 않을 수도 있다) 패치가 제공되기 까지 오랜 시간이 걸리는데 그 시간동안 시스템은 무방비에 놓이게 된다. 이러한 취약점들을 활용하면 시스템을 쉽게 침해할 수 있으며, 이것은 지능형 지속 위협에서 사용되는 전형적인 공격 기법 중 하나이다. 알지도 못하는 취약점에 대비하기란 현실적으로 쉬운 문제가 아니다.

2.2 지속 (persistent)

'지속(persistent)'은 목적을 달성하려는 경향으로 인해 성공할 때 까지 끊임없이 장기간에 걸쳐 은밀하게 이루어지는 것을 말한다. 마지막 공격이 이루어지기까지 목표 시스템과 지속적으로 상호작용을 유지한다.

1) 의뢰인 (master)

의뢰인은 자금력과 조직화를 담보할 수 있으며, 목적과 목표를 명확하게 해준다. 특히 공격의 목적과 자금력은 공격의 지속성을 담보한다. 오랜 기간 동안 치밀하게 준비할 수 있는 여건을 마련해줄 수 있는 것이다.

2) 기간 (period)

지능형 지속 위협을 사이버 공격의 암으로 비유하기도 한다. 암은 초기에 증상이 없고 오랜 잠복기간이 있다. 마찬가지로 지능형 지속 위협은 오랜 기간에 걸쳐 이루어지면서도 발견되지 않는 특징이 있다. 공격자들은 다양한 공격탐지시스템을 우회하거나 탐지시스템의 능력 이하에서 활동한다.

가령, 특정 데이터베이스에서 가입자의 개인정보를

통째로 유출하면 탐지시스템이 쉽게 발견할 수 있을지도 모른다. 하지만 하루에 4~5명씩 1년에 걸쳐 조금씩 개인정보를 수집한다면 탐지시스템이 정상적인 업무 행위로 판단할 가능성이 있다. 실제로 이와 같은 살라미 공격(salami attack)이 오늘날 국내에서도 많이 일어나는 것을 볼 수 있다.

지능형 지속 위협의 기간은 반드시 사이버 공간에서 이루어지는 행위만을 포함하는 것이 아니다. 공격을 시도하기 이전에 물리적 공간에서 이루어지는 탐색, 정보수집, 사회공학적 공격 등도 활동 기간에 포함된다.

3) 상호작용 (maintain the level of interaction)

전통적인 위협은 대부분 당장 필요한 이익에 의한 것이었다. 그러나 지능형 지속 위협은 당장의 이익과 장기간의 이익 모두에 관심이 있다. 전략적으로 목표를 정해놓고 미래에 새로운 정보가 필요해지면 미리 마련해둔 침투 경로에 접근해 다시 유출해내기만 하면 된다. 목표 시스템과의 지속적인 상호작용을 위한 교두보는 장기적인 정보유출의 목적만 있는 것이 아니다. 여러 단계의 시스템을 침투해야만 목표를 달성할 수 있는 경우, 다음 단계의 침투를 위한 정보수집의 목적으로 활용되기도 한다. 언제든지 시스템에 드나들 수 있는 교두보를 마련해 놓고 지속적인 상호작용을 하는데 많이 사용되는 방법은 C&C(Command and Control) 서버를 사용하는 것이다. 그리고 이것은 탐지되지 않는 수준으로 유지된다.

2.3 위협 (threat)

'위협(threat)'은 기존의 전통적인 위협과 다르게 동기나 공격을 통해 이루고자 하는 목적이 분명하고, 이로 인해 공격 대상도 명확하다. 위협 행위자는 하나의 혹은 그 이상의 조직적인 집단일 수 있다. 또한 이들은 공격을 수행할 수 있는 자금력이 충분할 수 있다. 공격의 대상은 과거와 다르게 대체로 정부, 방위산업, 민간으로 확대되고 있으며, 정치적, 경제적, 군사적인 목적뿐만이 아니라 정보나 지적재산권을 탈취하기 위한 목적도 많다.

1) 조직화 (organization)

지능형 지속 위협은 아마추어 수준의 해커 개인이 아니라 잘 투자되고 조직화된 전문가들에 의해 수행된다. 위협 행위자는 하나의 그룹 혹은 그 이상의 그룹일 수 있으며 고용되었을 가능성이 있다. 또한 막대한 자금력의 지원을 받고 있을 수 있다. 지능형 지속 위협의 발단이 된 것으로 추정되는 중국에서는 많은 공격들이 조직적인 형태를 갖추고 있다.

2) 목적 (goal)

과거의 해커들은 자신의 능력을 과시하거나 재미, 호기심에 의해 수행하는 경우가 많았다. 이들을 아마추어, 크래커라고 부른다. 오늘날 지능형 지속 위협은 그것을 통해 이루고자 하는 명확한 목적을 가지고 있으며 주로 정치적, 금전적 목적, 기술적, 군사적 목적이 있다고 알려졌다. 국내에서 잘 알려진 지능형 지속 위협의 많은 공격들은 개인정보를 탈취하려는 목적이었다. 그러나 해외에서는 군사기밀, 핵시설파괴 등의 목적으로 이용된 사례들을 많이 찾아 볼 수 있다.

3) 위협 대상 (target)

과거의 해커들은 웜을 사용해 시스템에 침투하는 몇몇의 방법을 시도했다. 성공하면 시스템을 침해할 수 있었고, 만약 성공하지 않았다면 또 다른 타겟 시스템을 찾아 떠났다. 하지만 지능형 지속 위협은 침해하고자 하는 목표 지점과 범위가 비교적 명확하다.

2.4 주체, 행위, 개체에 따른 위협의 특징

지금까지 언급된 특징들이 모두 만족되어야만 반드시 지능형 지속 위협으로 구분할 수 있는 것은 아니다. 여기서 '지능형'이라는 것은 고도화 되고 복잡하며 완전히 새로운 기법을 통해 시스템에 침입하는 것이 아니다. 지능형 지속 위협 공격에 사용되는 가장 보편적인 방법은 스피어 피싱 같은 사회공학적 기법이나 기존에 존재하는 단순한 공격들의 조합일 수 있다. 단순한 공격 기법의 조합이라고 생각될 수 있는 위협들도 충분히 시스템을 무력화 시킬 수 있다.

기존의 문헌들은 지능형 지속 위협을 '지능형', '지속', '위협' 3가지로 분류하여 설명하고 있는데, 이는

〈표 3〉 주체, 행위, 개체에 따른 특징적 분류

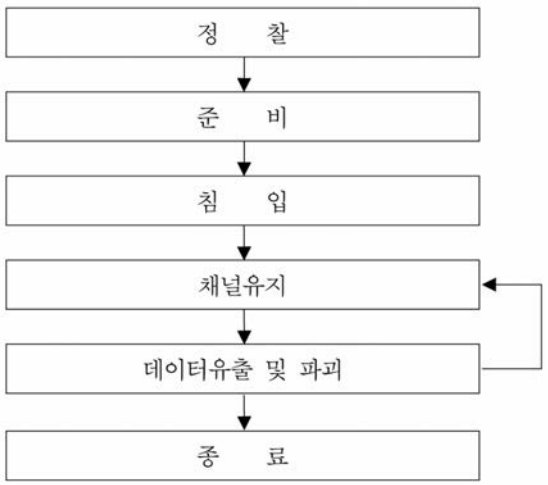
threat actor	조직화 (organization) 목적 (goal) 위협대상 (target) 의뢰인 (master)
threat activity	공격방법-알려진 취약점 사용 (well-known vulnerabilities) 공격방법-알려지지 않은 취약점 사용 (research new vulnerabilities) 공격의 조합 (combine multiple attack methodologies) 기간 (period) 상호작용 (maintain the level of interaction)
victim	피해자 (victim) 피해내용 (harm)

위협 자체가 가지는 다양한 변수와 복잡성을 쉽게 설명하는데 한계가 있었다. 따라서 본 논문은 〈표 3〉과 같이 '누가', '어떻게', '무엇을 공격하는지' 즉, 행위 개체에 따른 특징으로 분류하였다.

3. 지능형 지속 위협의 킬체인

지능형 지속 위협이 전통적인 위협과 크게 다른 점 중 하나는 공격을 위한 체계적인 단계가 존재한다는 것이다. 이러한 공격 체계는 기존의 발생했던 수많은 지능형 지속 위협 공격 사례 분석을 통해 도출한 것이다. 공격 단계는 사건에 따라 변형된 형태가 존재하며 문헌에 따라 약간의 차이가 있지만 공통적으로 〈그림 6〉과 같이 '정찰', '준비', '침입', '채널유지', '데이터유출 및 파괴', '종료'로 나눌 수 있다.

지능형 지속 위협은 전통적인 위협과는 달리 공격을 위한 체계적인 단계가 존재



〈그림 6〉 지능형 지속 위협의 킬체인인

3.1. 정찰

공격 대상에 대한 정보를 수집하는 것을 의미한다. 시스템의 운영체제, 네트워크 구성, 보안체계, 포트스캔 등 시스템 및 네트워크 자체에 대한 정보를 수집할 수 있다. 사실 이러한 활동들은 전통적인 공격에서도 이루어졌던 전형적인 정찰 활동이다. 그러나 오늘날 위협은 물리적인 시스템의 정보뿐만이 아니라, 그것을 운용하는 조직에 대한 정보와 관리자에 대한 개인정보까지 수집한다.

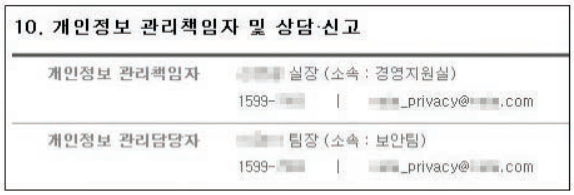
가령 자동차 시스템의 무결성을 해치고자 하는 공격자가 있다고 하자. 그는 자동차 모듈에 침투하기 위한 연구 시간을 줄이기 위해 자동차 회사 내 연구개발직 직원들에 대한 사회공학적 공격을 준비할지도 모른다. 자동차 회사 홈페이지에 들어가 조직도와 직원의 이메일 주소를 파악한 후 업무협조 이메일을 가장한 악성코드를 발송할 수 있다. 이러한 기법은 이미 수 많은 지능형 지속 위협에서 발견되고 있으며 이제는 전형적인 공격 기법이 되었다.

고위 임원들 역시 공격자들에게는 좋은 타겟이다. 고위 임원들은 온라인에 실무자보다 더 많이 노출되어 있으며 언론에 노출될 가능성도 있다. 임원들이 가진 회사 시스템 권한을 이용하면 내부 시스템에 쉽게 접근할 수 있으며, 직원들에게 정보유출을 유도하는 이메일을 보낼 수도 있다. 실제로 지능형 지속 위협에서 임원들을 타겟으로 한 공격이 증가하고 있다.

국내의 경우 정보통신망 이용촉진 및 정보보호 등에

〈표 4〉 사회공학적 공격을 위해 수집될 수 있는 인적 정보들

수집처	수집 가능한 내용들
회사 웹페이지	조직 구성, 직책, 담당자 이름, 근무처, 위치
직원 SNS	이메일 주소, 인간관계, 취미
언론	담당자 이름, 직책, 업무내용



〈그림 7〉 홈페이지에 안내된 개인정보 관리책임자 정보

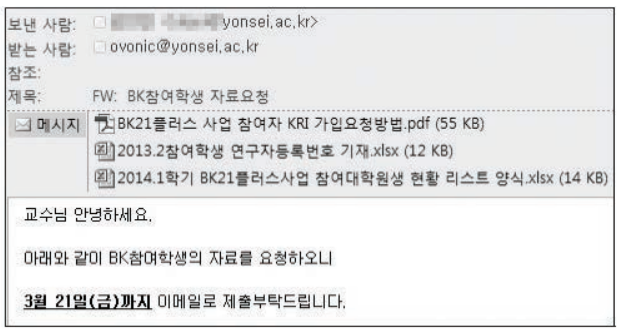
관한 법률에 따라 개인정보에 대한 관리책임자를 지정하도록 되어 있다. 많은 인터넷 사이트들이 〈그림 7〉처럼 개인정보 관리책임자를 홈페이지에 공개하고 있다. 이들은 회사 내 기술적 보안에도 많은 주의를 기울여야 하지만, SNS와 같은 사적 공간에서 자신들의 특징이 드러나는 것에도 주의를 기울여야 한다. 사회공학적 공격의 타겟이 될 수 있기 때문이다.

3.2. 준비

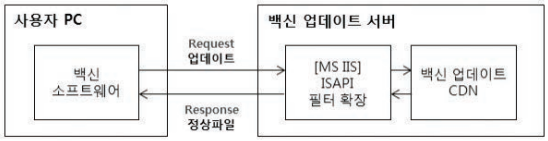
정찰을 통해 수집한 정보를 바탕으로 침입을 위한 적절한 공격지점을 찾고, 침입에 필요한 방법과 도구를 준비한다. 사회공학적 공격을 위해서 이메일을 작성하여 발송한다든지, 시스템에 침투하기 위한 맞춤형 악성코드를 직접 제작할 수도 있다. 〈그림 8〉와 같이 업무용 이메일을 가장하거나, 관혼상제, 사원모집, 인사장 등으로 위장할 수 있다.

3.3. 침입

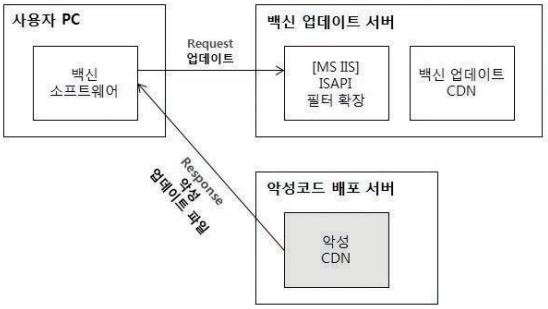
〈그림 8〉에 나타난 첨부파일 문서는 일상적인 업무와 관련된 것처럼 보이나 악성코드가 포함되어 있는 문서일 수 있다. 만약 그것이 악성코드라면 이메일 수신



〈그림 8〉 내용을 위장한 표적형 이메일



〈그림 9〉 정상적인 백신 업데이트 과정



〈그림 10〉 백신 업데이트 채널을 악용하는 공격자

자가 첨부파일을 여는 순간 PC는 악성코드에 감염된다. 하지만 문서는 정상적으로 열람할 수 있기에 사용자는 악성코드가 설치된지도 모른 채 PC를 사용할 것이다. 대개 사용자 몰래 설치된 악성코드는 공격자가 미리 준비해 둔 C&C(Command and Control)서버에 연결되어 공격자의 통제를 받으며, 공격자는 감염된 PC의 데이터를 열람할 수 있게 된다.

또 다른 방법으로는 운영체제의 취약점을 활용하여 원격에서 직접 시스템에 침입할 수도 있고, 정기적으로 다운로드 되는 백신의 엔진 업데이트나 소프트웨어 업데이트 채널을 활용하여 침입할 수도 있다. 백신 업데이트는 아무런 의심 없이 자동으로 설치되지만, 자동으로 다운로드 되는 채널 역시 공격자가 악용할 수 있음을 인지해야 한다. 따라서 가용한 모든 입/출력 인터페이스가 침입의 대상일 수 있음을 명심해야 한다.

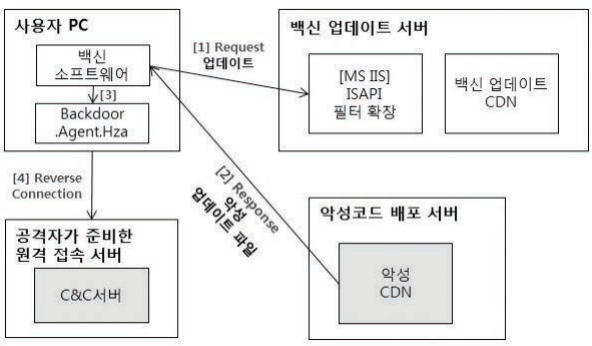
2011년, 국내의 대형 포털 사이트인 네이트 닷컴(nate.com)의 침해 사례에서, 공격자는 데이터베이스 관리 직원의 업무용 PC를 통해 가입자 데이터베이스에 접근하였다. 해당 직원 PC에 최초로 침투할 때 사용한 방법은 PC에 설치되어 있었던 백신 엔진 업데이트 채널을 악용한 것이었다. 해당 직원의 PC가 백신 엔진 업데이트를 자동으로 수행했을 때 악성코드는 설치되었다.

3.4. 채널유지

최초 침입이 성공하면 공격자는 침해된 시스템에 지속적으로 드나들 수 있는 원격 통로를 생성한다. 공격자들은 침해된 시스템을 장기적으로 접근하면서 내부의 네트워크를 파악하거나, 영업 기밀이 어느 서버에 있는지 파악하는 등 추가적인 정찰을 할 수 있다. 피해자가 입력하는 키보드 내용을 캡춰하여 아이디와 패스워드를 탈취할 수도 있다.

어찌되었든 공격자는 전체 네트워크를 제어하고 장기간 접속을 유지하는 경향이 있다. 이것은 최종 목적을 달성하기 위함이며 목적이 달성되면 연결의 흔적은 사라질 것이다. 이를 위해 관리자와 동등한 수준의 특수 권한을 획득하거나 크래킹 하이재킹과 같은 공격을 수행한다. 혹은 침해당한 시스템과 C&C통신을 수행하는 맞춤 제작된 툴이나 백도어를 설치함으로서 이러한 목표는 달성 가능하다.

최초 침입이 이루어지고 오랜 기간 채널이 유지되면서도 잘 탐지되지 않는 까닭은 공격자가 목표 시스템으로 접속하는 것이 아니라, 목표 시스템이 거꾸로 공격자가 준비해 놓은 C&C서버로 역접속(Reverse Connection)을 하기 때문이다. 사용자의 시스템이 악성코드에 감염되는 순간 해당 시스템은 외부에 있는 공격자의 C&C서버로 연결한다. 이것은 외부에서 내부로 들어오는 인바운드 트래픽 뿐만 아니라 아웃바운드 트래픽도 잘 탐지할 수 있어야 함을 의미한다.



〈그림 11〉 악성코드 감염 후 C&C서버로 역접속 하는 과정

3.5. 데이터 유출

시스템 안의 기밀 정보를 은밀하게 유출해 나간다. 이때 탐지를 피할 수 있는 수준으로 데이터를 유출하는 것이 중요하다. 이를 달성하기 위해서는 살라미 공격처럼 적은 양을 조금씩, 오랜 기간에 걸쳐 유출하기도 하며, 정상적인 트래픽으로 가장하기 위해 암호화와 데이터 마스킹 등의 기술을 사용하기도 한다.

지금까지 나열한 위협의 다섯 가지 단계는 지능형 지속 위협의 보편적인 프로세스를 기술한 것뿐이다. 모든 지능형 지속 위협은 고유의 특성을 지니며 변형된 형태도 많다. 따라서 반드시 위의 모든 단계를 포함하는 것이 아니다. 그리고 반드시 순서를 가지고 있지도 않다. 특정 단계는 목표 시스템의 복잡한 구조에 따라 반복 수행될 수 있고, 필요에 따라 생략될 수 있다.

Ⅳ. 대응전략 및 결론

지능형 지속 위협은 방지하는 것이 가장 이상적이나, 다루어야 할 보호 범위가 넓고 복잡한 문제로 인해 많은 어려움을 갖고 있다. 오늘날 그 어떠한 시스템도 다양한 위협으로부터 완벽하게 보호할 수 있다고 장담할 수 없다. 그렇다고 해서 예방책이 중요하지 않은 것은 아니다. 다만, 위협을 빠르게, 효과적으로 탐지할 수 있는 방법이 필요하다. 지능형 지속 위협의 많은 사례들은 최초 침입부터 공격이 수행되기 까지 짧게는 6개월부터 1년이 넘는 기간이 걸렸다. 정보를 수집하고 침입을 준비하기 위한 과정까지 포함하면 더 긴 시간이 필요했을 것이다. 이처럼 최근의 많은 공격은 그 목적과 목표가 명확하고 오랜 시간이 걸리더라도 반드시 성공하고자 하는 속성들을 가지고 있다. 은밀하게, 지능적으로, 지속적인 위협을 가하는 것이 지능형 지속 위협의 특징인 만큼 예방도 중요하나 빠른 탐지기능을 갖추는 것은 필수라고 할 수 있다.

은밀하게, 지능적으로, 지속적인 위협을 가하는 지능형 지속 위협의 특징을 고려할 때 예방도 중요하지만 빠른 탐지기능을 갖추는 것이 필수

1. 방지

방지의 목적은 공격을 막는 것이다. 피해가 발생하기 전에 공격을 막을 수 있다면 다행스러운 일이지만 모든 위협을 완벽하게 막는 것은 현실적으로 어려운 문제이다. 모든 방지책은 우회할 수 있는 길이 있다는 것을 명심하고 언제든지 침해받을 수 있음을 인식해야 한다.

보호하고자 하는 시스템의 모든 엔드 포인트 혹은 내부와 외부를 막론한 모든 입/출력 인터페이스가 침해받을 수 있으므로 이에 대한 대비책이 준비되어야 한다. 여기에는 사람에 대한 방지책까지 준비해야 한다. 시스템을 관리하고 이용하는 것은 결국 사람이다. 사람을 시스템의 한 구성요소로 본다면 내부자는 가장 중요한 공격 대상이다. 많은 침해 사례들이 내부자에 의해 발생했거나 내부자를 통로로 삼아 이루어졌다. 인적 취약점을 반드시 점검해야 한다. 인적자원과 같은 관리적 보안에 관해서는 ISO 27000 시리즈와 같은 정보보호 인증체계를 활용하여 점검을 해보는 것도 좋은 방법이다.

〈표 5〉 SANS에서 제시한 20가지 핵심 통제사항들[15]

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

또한 미국의 연구교육기관인 SANS는 효과적인 사이버 방어를 위한 핵심 보안 통제사항으로 20가지를 제시하고 있다. 이러한 항목들을 지표로 삼아 해당 시스템을 전반적으로 점검해 볼 필요가 있다.

2. 탐지

공격자는 얼마든지 우리의 방어수단을 우회할 수 있다. 때문에 우리는 시도되는 공격을 얼마나 빠르고, 효과적으로 탐지하는지가 중요하다. 그래야만 피해를 최소화할 수 있기 때문이다.

이를 위해 백신, 방화벽, IPS, IDS, DLP(Data Loss Prevention)와 같은 보안 시스템을 잘 이해하고 있어야만 한다. 이러한 것들은 룰(rules) 혹은 시그니처(signature) 기반으로 운영되며 한번 설정하면 이후 자동으로 탐지해준다. 만약 설정된 규칙이나 정책이 잘못되어 있거나, 미비한 것이라면 진화하는 지능형 지속 위협에는 효과적이지 못하다. 앞으로는 평판분석, 행위기반, 휴리스틱, 가상화 기술 등을 이용한 지능적인 탐지기법이 개발되어야 한다.

또한 지능형 지속 위협을 탐지하려면 인바운드 트래픽뿐만 아니라 아웃바운드 트래픽에도 집중해야 한다. 지능형 지속 위협의 많은 사례들이 C&C서버를 통해 제어하는 특징을 갖고 있기 때문이다. C&C서버는 공격자가 외부에서 내부로 연결을 시도하는 것이 아니라 내부에서 외부로 역접속한다. 이를 탐지하기 위해서는 목적지 IP주소와 도메인을 확인하거나, 커넥션의 길이가 과도하게 길지 않은지, 오랜 기간에 걸쳐 지속적으로 연결하고 있지 않은지를 모니터링 할 필요가 있다.

탐지가 시사하는 한가지 중요한 점이 있다. 탐지가 되었다는 것은 방지 대책이 성공적이지 못했다는 것을 의미한다. 따라서 예방을 위한 대책을 다시 마련하거나 개선점을 찾아보아야 함을 말해준다.

3. 결론

전자기기들은 위험 및 장애 발생으로 인한 안전사고

〈표 6〉 전자기기 강제인증제도

인증제도	인증종류	관련법령
전기용품 안전인증제도	안전인증 자율안전확인 공급자 적합성 확인	전기용품안전 관리법 (법률 제 11712호)
방송통신기자재 적합성평가	적합인증 적합등록 잠정인증	전파법 제5장 (법률 제 12304호)

를 방지하기 위하여 반드시 안전인증기관으로부터 인증 절차를 거쳐야한다. 또한 외부 전파에 의한 통신장애, 기기의 오작동으로 인한 인명 및 재산 피해 등 국내 전파환경을 보호하기 위한 인증을 받아야 한다. 전자기기 강제인증제도에는 전기용품 안전인증제도(KC)와 방송통신기자재 적합성평가(KCC)가 있다.

국내에서는 조직의 기밀정보유출 피해를 최소화하기 위해 체계적인 보안관리가 요구되면서 다양한 정보보호 및 개인정보보호관리체계 인증을 시행하고 있다. 이것은 대체로 ISO 27001과 유사하며 한국적인 실정에 맞춰 변형한 것이다. 정보보호관리체계는 효율적인 정보자산 관리에 있어 외부적인 위험요소뿐만 아니라 내부적인 위험요소를 미연에 방지하기 위한 적절한 표준을 제공한다. 〈표 7〉은 이에 적용된 국제표준 규격인 ISO 27001을 나타낸 것으로 14개의 보안 도메인과 114개의 보안 통제항목으로 구성된다.

〈표 7〉 ISO 27001:2013의 구성

보안 도메인	통제항목 수(개)
1. 정보보안 정책 (Information Security Policy)	2
2. 정보보안 조직 및 구성 (Organization of Information Security)	7
3. 인적 보안 (Human resources security)	6
4. 자산 관리 (Asset Management)	10
5. 접근통제 (Access Control)	14
6. 암호화 (Cryptography)	2
7. 물리적 & 환경적 보안 (Physical and environmental security)	15
8. 운영 보안 (Operations security)	14
9. 통신 보안 (Communication security)	7
10. 시스템 도입·개발·유지보수 (System acquisition, development and maintenance)	13
11. 공급 업체와의 관계 (Supplier relationships)	5
12. 침해사고 대응 관리 (Information Security incident management)	7
13. 사업 연속성 관리의 정보보안 측면 (Information security aspects of business continuity management)	4
14. 준거성 (Compliance)	8

전통적인 전자기기에서의 안전은 화재나 오작동을 야기하는 것을 방지하기 위한 전기적 안전이 핵심이었다. 이것은 전자기기 고유의 사용 목적을 방해하는 등 가용성을 해치는 것들로서 무결성, 기밀성을 해치는 것과는 거리가 멀었다. 하지만 전통적인 전가기기들이 스마트라는 수식어를 붙여 데이터를 저장하고, 전송하고, 결합하는 순간 기밀성을 고려해야만 한다. 또한 기기의 제어가 물리적인 전기적 신호의 차원이 아니라 논리적인 차원의 데이터로 제어될 때 우리는 무결성을 고려해야만 한다.

근본적으로 모든 데이터는 정보나 지식으로 변환될 수 있으며 이것은 많은 효용을 갖을 수 있다. 가치를 갖는 모든 데이터는 해커의 공격을 받을 수 있다. 또한 데이터가 통제의 도구로 사용될 때 해커에 의한 악의적인 오작동을 염려해야 한다. PC에 있는 데이터의 무결성이 침해되면 인간은 잠깐의 정신적 고통만 받을 뿐이지만, 스마트 카에 있는 제어 시스템의 무결성이 침해되면 인명 피해로 이어진다.

따라서 이제 전자기기들이 갖던 전통적인 '안전'의 개념을 컴퓨터 시스템에서 말하는 안전의 개념으로 확장해야 한다. 많은 기기들이 CPU와 메모리, OS를 갖고 컴퓨터화 되었기 때문이다. 컴퓨터 시스템에서 갖는 안전은 데이터의 무결성, 가용성, 기밀성을 보장하는 것이다. 하지만 이것을 보장하는 것은 매우 어렵다. 시스템이 복잡해질수록 위협은 더 많아졌고 지능형 지속위협처럼 끊임없이 진화하고 있기 때문이다.

이때 우리가 보호해야 할 대상과 시스템을 명확하게 이해하지 못한다면 공격으로부터 보호하고, 안전하게 지키고, 방어할 수 없다. 우리의 네트워크에 무엇이 연결되었는지, 전반적인 노출점이 무엇인지를 이해하기 위한 네트워크 구성도와 가시화 지도를 작성해야 한다. 완벽한 보안이라는 것은 존재하지 않는다. 현실적으로

모든 것을 방어하거나 탐지할 수 없기 때문이다. 따라서 디지털 자산에 대한 위험도 평가와 보호 대책에 대한 우선순위를 정해야 한다. 또한 빠른 탐지를 위해 효과적인 모니터링을 하는데 초점을 맞춰야 한다. 그래야만 피해를 최소화 할 수 있기 때문이다.

참 고 문 헌

[1] 홍용근, 신명기, 김형준, "사물인터넷(IoT/M2M) 표준화 동향," OSIA Standards & Technology Review, Vol. 26, No. 2, pp. 8-17, June 2013.

[2] Yue Chen, Barry Boehm, and Luke Sheppard, "Measuring Security Investment Benefit for COTS Based Systems - A Stakeholder Value Driven Approach," International Conference on Software Engineering, September 2006.

[3] 조아람, 조효진, 우사무엘, 손영돈, 이동훈, "CAN 버스 공격에 안전한 메시지 인증 및 키 분배 메커니즘," 정보보호학회 논문지, Vol. 22, No. 5, pp. 593-607, August 2013.

[4] Proofpoint, "Proofpoint Uncovers Internet of Things (IoT) Cyberattack," January 2014. Available from:http://www.proofpoint.com/about-us/press-releases/01162014.php

[5] NPD DisplaySearch, "Smart TV Surges in Popularity Worldwide," Quarterly Smart TV Shipment and Forecast Report, June 2012.

[6] Mark Molloy, "World's first robot suicide? Android 'rebels' against monotonous housework," Metro, November 2013. Available from:http://metro.co.uk/2013/11/12/worlds-first-robot-suicide-android-rebels-against-boring-housework-4183508/

[7] Mike Cloppert, "Security Intelligence: Introduction (pt 1)," SANS Computer Forensics Blog, July 2009. Available from:http://computer-forensics.sans.org/blog/2009/07/22/security-intelligence-introduction-pt-1.

[8] Beth E. Binde, Russ McRee, Terrence J. O'Connor, "Assessing Outbound Traffic to Uncover Advanced Persistent Threat," SANS Technology Institute, May 2011.

[9] Mandiant, "M-Trends, the Advanced Persistent Threat," Mandiant Reports, January 2010.

[10] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant Reports, 2013.

[11] Frankie Li et al., "Evidence of Advanced Persistent Threat: A case study of malware for political espionage," 2011 6th International Conference on Malicious and Unwanted Software, pp. 102-198, October 2011.

[12] "SP- 900-39 : Managing Information Security Risk: Organization, Mission, and Information System View," NIST, March 2011. Available from:http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[13] Richard Bejtlich, "What Is APT and What Does It Want?," TaoSecurity Blog, January 2010. Available from:http://taosecurity.blogspot.kr/2010/01/what-is-apt-and-what-does-it-want.html.

[14] "Advanced Persistent Threats: A Decade in Review," Command Five Pty Ltd, June 2011. Available from:http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf.

[15] SANS Institute, "Critical Security Controls for Effective Cyber Defense," Available from:http://www.sans.org/critical-security-controls.

유 홍 렬

2013년 2월 서울과학기술대학교 산업공학 학사
2013년~현재 연세대학교 정보대학원 석사과정

〈관심분야〉
Advanced Persistent Threat, HCI, Usable Security, Social Engineering, Human Factors

정 성 미

2012년 2월 강남대학교 미디어정보공학, 컴퓨터공학 학사
2013년 9월~현재 연세대학교 정보대학원 석사과정

〈관심분야〉
Social Engineering, Usable Security, HCI, Privacy

권 태 경

1992년 연세대학교 컴퓨터과학과 학사
1995년 연세대학교 컴퓨터과학과 석사
1999년 연세대학교 컴퓨터과학과 공학박사
1999년~2000년 U.C. Berkely Post-Doc.
2001년~2013년 8월 세종대학교 컴퓨터공학과 교수
2007년~2009년 Univ. Maryland at College Park 교환교수
2013년~현재 연세대학교 정보대학원 교수

〈관심분야〉
Information Security and Privacy, Applied Cryptography, Cryptographic Protocol, Network Protocol, Usable Security, and Human-omputer Interactions