이것만은 알아야 할 네트워크 보안 이야기
Part 8. APT 1. APT 공격의 방식과 사례

글. 이선응 아이크래프트 수석
ka3211a@gmail.com

이번 호에서는 APT 공격이 무엇인지 알아본 후, 공격이 진행되는 단계를 순차적으로 설명하고, 지금까지 발생한 대표적인 2가지 APT 공격사례를 소개하도록 하겠다.

연재 목차

APT는 Advanced Persistent Threat의 약자로 지능형 지속 공격이라고 해석할 수 있다. 일정한 절차나 특정 기술을 계속 반복해서 사용하는 공격이 아니고, 계속 신규로 개발되는 새로운 전술과 기술을 이용하여 다양하게 진화하는 공격으로, DDoS와 같이 단시간 내에 공격이 이루어지지 않고, 짧게는 수일에서 길게는 수년 단위로 공격이 지속하는 공격 유형을 말한다. 사실상 최근에 이루어지는 대부분의 공격이 이런 APT 공격의 특성을 가지고 있다.
지난 호에서 설명한 DDoS 공격 혹은 각종 홈페이지 해킹사고 등도 이런 APT 공격에서 특정 단계에 해당하는 공격으로 인터넷 초창기의 실력 좋은 해커 한 명이 취미로 하는 공격이 아니고, 자생적으로 조직된 해커집단이나 국가의 후원을 받는 조직이 금전적이나 정치적인 이유로 고도로 전문화된 방식을 사용하는 공격이 대부분이다.

[표 1]은 최근 APT 공격을 통해 공격자가 달성하려는 목적을 기술하였다. 이제 단순한 호기심 차원에서 개인적인 욕망이 아니라 특정한 목적을 설정하고 공격이 시작된다. DDoS 등을 통한 경쟁사나 협박 대상에 대한 서비스 방해일 수도

	방해	데이터 절도	사이버 범죄	핵티비즘	파괴적 공격
목표	접근 및 확산	경제적, 정치적 이익	금전적 이득	비방, 언론 및 정책	운영 방해
예시	봇넷 및 스팸	지능형 지속적 위협 그룹	신용카드 절도	웹사이트 훼손	데이터 삭제
표적	×	√	√	√	√
특성	보통 자동화	지속적	자주 기회주의적	과시	분쟁 주도

표 1. APT 공격을 통해 달성하려는 목적 / 출처 : FireEye

있고, 조직의 고객정보 등의 높은 가치를 가지는 데이터를 이용한 금전적인 수익이나 인터넷에 공개하는 행위일 수도 있으며, 정치적이거나 민족주의적 목적이나 국가적인 이익을 위해 특정 조직에 대한 테러행위 등 다양한 목적을 달성하기 위해 공격이 이루어진다. 특히 요즘의 코로나 사태에 따른 백신이나 치료제에 대한 연구내용은 현재 가장 가치가 높은 정보로 이런 연구를 수행하는 의약품 연구조직은 공격그룹이 우선하여 노리는 타겟이 될 수 있다.

이제 APT 공격이 이루어지는 방식을 설명해 보자. 다양한 벤더나 전문가들이 APT 공격에 대한 다양한 방법으로 공격 양상을 설명하고 있는데 필자는 파이어아이(FireEye)라는 APT 방어 장비 업체의 모델을 설명하도록 하겠다. [그림 1]과 같이 공격자는 타겟으로 설정한 조직에 대해 다양한 정보를 수집하여 침투방식을 결정하고, 조직구성원의 단말에 악성코드를 은밀하게 설치하여 거점을 확보하게 된다. 다음 단계로 이 거점에서 권한을 상승시켜 관리자 권한을 획득하여 해당 단말을 완전히 제어 가능하게 만든 다음 조직의 다양한 전산 자원에 대한 정보를 수집한다. 거점 주위의 다른 단말과 사내 서버까지 모두 접속 권한을 확보한 후에는, 지속적으로 접속 가능한 안전통로(backdoor)를 확보하여 언제나 접속이 가능하게 관리한다. 이후 오랜 시간 동안 조직의 정보를 탈취하거나, 정보를 암호화시켜 협박하거나, 혹은 특정한 D-Day를 설정하여 일시에 전산 자원을 파괴하는 등 임무를 완수하는 방식으로 공격이 이루어진다.

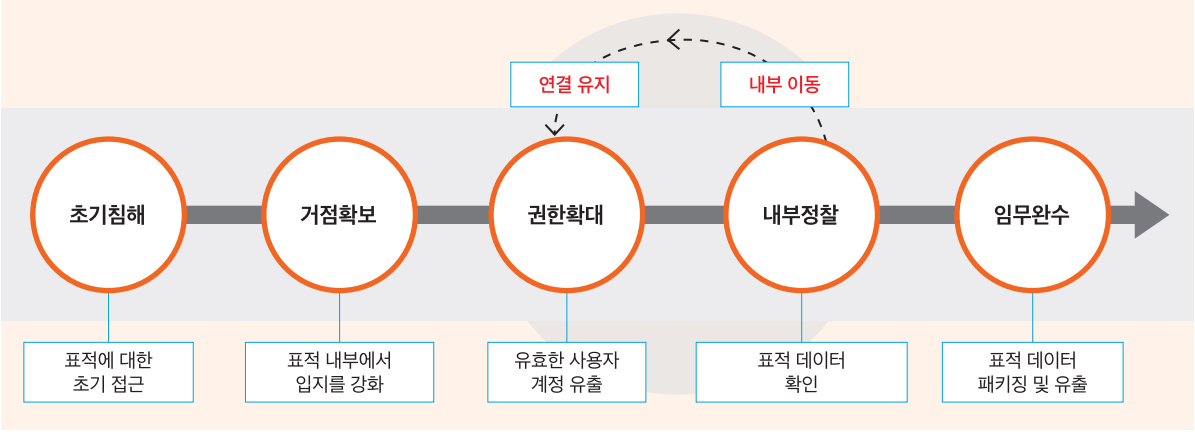

그림 1. APT 공격의 진행 단계 / 출처 : FireEye

단계별로 어떻게 공격이 이루어지는지 알아보자.

먼저 **초기침해단계**는 공격대상이 선정되면 해당 조직의 외부로 공개된 전산 자원과 구성원들의 연락처를 수집하는 것으로 시작된다. 운영 중인 홈페이지 서버의 취약점을 스캔해서 침투 가능성을 확인하거나, 재택근무나 출장자를 위한 VPN 접속서비스의 취약점 혹은 계정정보, 또는 구성원들의 이메일을 수집하여 악성코드가 숨겨진 파일을 이메일에 첨부하여 열어보게 유도하는 방법을 사용한다. 이 단계에서 가장 많이 사용되고 있는 기법은 워터링홀(Watering hole)과 스피어피싱(Spear phishing)이 있다.

먼저 워터링홀은 [그림 2]의 왼쪽 그림과 같이 초원의 물웅덩이에 사자가 숨어 있다가 물을 먹기 위해 접근하는 동물들을 공격하는 방식에서 유래된 것으로, 타겟으로 지정한 조직의 구성원들이 많이 방문하는 웹사이트를 해킹해서 악성코드를 숨겨 두었다가, 해당 웹에 접속하게 되면 악성코드에 감염되게 만드는 방식으로 내부에 침투하는 기법을 의미한다. 두 번째로는 작살로 고기를 잡는 것처럼 [그림 2]의 오른쪽 그림과 같이 무차별적으로 이메일을 보내 감염시키는 것이 아니라, 공격 대상 조직의 구성원 이메일을 입수하여 공격대상을 선별해서 수신자가 첨부파일을 열거나 메일

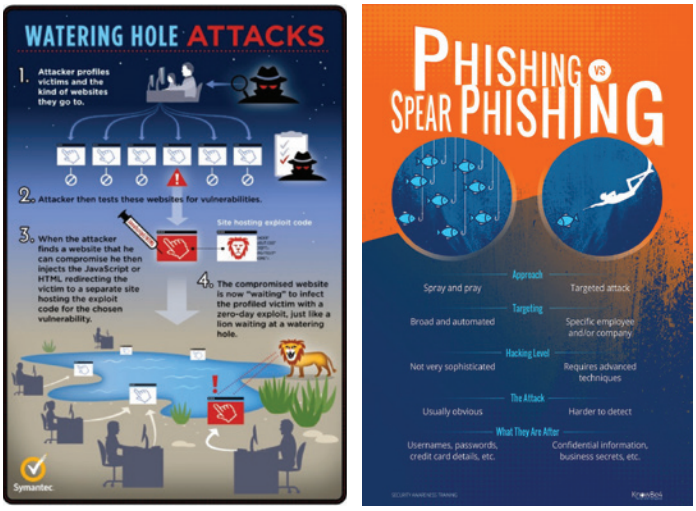

그림 2. 워터링홀(Watering hole)과 스피어피싱(Spear phishing) 공격

내의 URL을 클릭하게 유도하여 해당 PC를 감염시키는 방식인 스피어피싱이 사용된다.

스피어피싱에 사용되는 메일의 유형을 알아보자. [그림 3]와 같이 용량초과나 계정차단 등의 경고 관련 메일을 보내서 수신자의 흥미를 유도한 다음 의심 없이 첨부파일을 클릭하거나 본문에 있는 URL을 클릭하도록 유도하는 내용으로 구성되어 있다. 이때 첨부파일의 문서를 열거나 URL을 클릭하게 되면 해당 단말로 악성코드가 다운로드되어 감염되는 것이다.

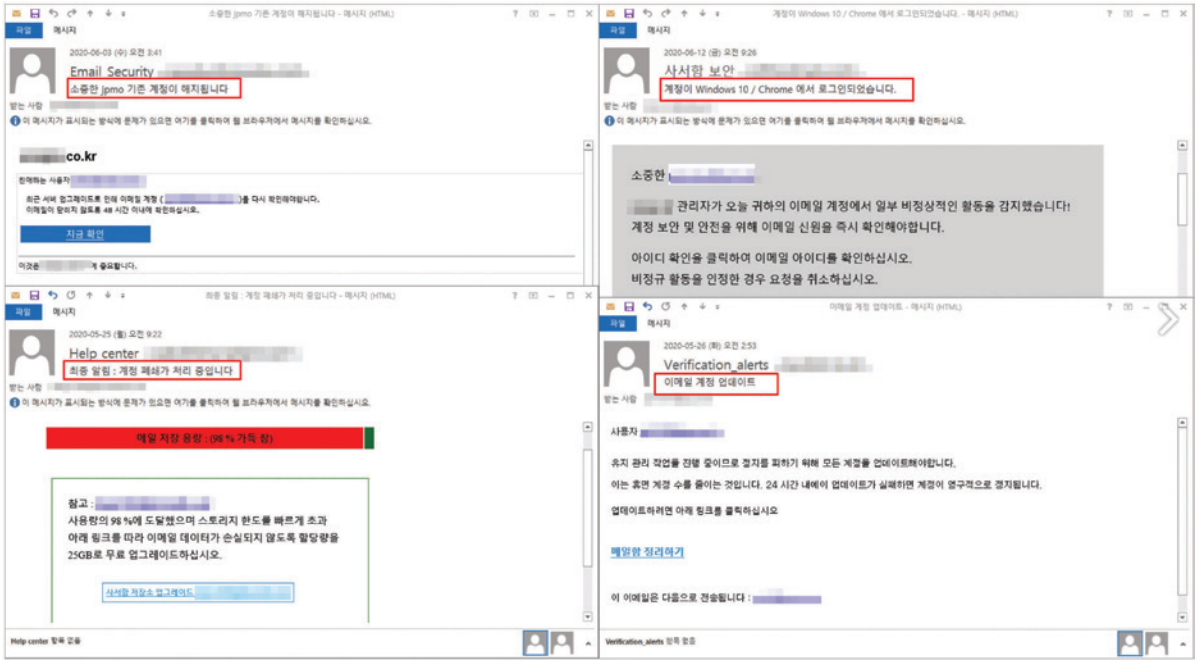

그림 3. 스피어피싱에 사용되는 이메일 유형 / 출처 : EST security

이러한 스피어피싱을 통한 악성코드 감염사고뿐만 아니라 랜섬웨어에 감염되어 단말에 저장된 모든 데이터가 암호화되어 공격자의 협박을 받는 사례가 빈번하게 발생하고 있다. 이에 정부기관인 한국인터넷진흥원(KISA)에서는 스피어피싱에 대한 경각심을 높이고, 침해사고를 방지하기 위해 다양한 홍보 활동을 하고 있는데, [그림 4]는 이러한 홍보 활동의 일환으로 전 국민이 알기 쉽게 만화형식으로 만든 보안교육 자료이니 참고하기 바란다. 이러한 스피어피싱 공격에 대응하기 위해서는 악성코드가 포함된 메일을 탐지하고 차단하는 시스템을 도입해야 하고, 단말에 설치된 바이러스 백신이 언제나 최신상태가 유지되게 관리해야 한다. 무엇보다 외부와의 직접적 접촉이 많아 메일이 홈페이지에 노출되어 있는 영업, 고객 관리 등의 팀원에 대한 정기적인 보안교육을 통해 출처가 의심되는 메일은 열어보지 말고 삭제할 수 있도록 하는 것이 최상의 방법이다.

그림 4. 스피어피싱으로 인한 침해사고방지 홍보 만화 / 출처 : 한국인터넷진흥원

두 번째 **거점확보단계**로 감염시킨 단말의 호스트 이름, 네트워크 정보, OS 버전 등의 단말 정보를 수집하고, 기능이 보강된 악성코드를 추가로 설치하여 다양한 데이터를 수집하여 원활하게 공격자의 저장장치로 전송하기 위한 디스크 연결설정을 하기도 한다.

세 번째 **권한확대단계**는 감염 단말의 계정 권한이 관리자 권한이 아닐 경우 권한 상승을 위해 해당 OS의 권한 상승 취약점을 유발하는 추가적인 악성코드를 설치하여 권한을 관리자 권한으로 상승시킨다. 또한 단말 내의 사용자 계정 패스워드를 알아내거나 추가적인 계정을 생성하여 향후 정상적인 접속에 사용한다.

네 번째 **내부정찰단계**는 단말이 속한 네트워크 구조를 파악하고 같은 네트워크 내에 있는 다양한 단말 혹은 서버를 탐색하기 시작한다. 이를 통해 단말의 취약점을 통해 추가로 감염시키거나 로그인 정보를 탈취하여 단말에 연결된 공유폴더 및 단말 내의 이메일, 문서 등 다양한 데이터를 열람하여 향후 공격 방향을 결정하는 데 사용한다.

다섯 번째 **내부이동단계**는 내부 정찰을 통해 확보된 네트워크 구성 및 서버, 단말 정보를 이용하여 서버 및 단말의 관리자 권한을 획득하여 목표조직의 전산 자원에 광범위하게 접근 권한을 획득하여 내부 기밀문서, 계정정보 등을 수집한다. 이때 백신 및 보안 장비의 탐지를 회피하기 위해 해킹목적으로 개발한 툴이 아닌 정상적인 프로그램을 사용하기도 한다. 해당 조직이 만약에 망 분리가 되어 있어 업무망 혹은 운영 망에 접근이 불가능한 경우 망간 접점이 되는 시

스템(망 연계 솔루션, 보안 USB 등)을 찾아서 해당 시스템의 취약점을 조사하여 침입을 시도하게 된다.

여섯 번째 **연결유지단계**는 감염 단말이 재부팅되거나 예상하지 못한 프로세스 충돌 등으로 악성코드가 종료되어 침입 경로를 잃을 수 있다. 이를 방지하기 위해서 악성코드가 재부팅 후에도 다시 실행될 수 있도록 서비스를 등록하고 시작 프로그램을 설정, 작업 스케줄러 등록, 웹쉘 삽입 등을 수행한다. 웹쉘(Web shell)이란 웹을 통해 브라우저에서 운영체제의 커널(핵심프로그램 : 시스템의 모든 것을 통제)과 연결하여 다양한 명령을 내릴 수 있도록 동작하는 스크립트의 일종이다. 이를 통해 일종의 개구멍(백도어 : Back door)을 만들어 두는 것으로 공격자가 원할 때 언제나 은밀하게 접근할 수 있게 한다. 앞에서 설명한 3~6번째 단계는 계속 반복되면서 조직 내의 전산 자원을 조금씩 확보해 나가게 된다. 이 기간이 며칠 단위가 될 수도 있고 탐지가 되지 않는다면 몇 년 단위도 될 수 있다. 이렇게 오랜 기간 지속해서 침입한 조직에 잠복하는 특성 때문에 지속 공격이라는 명칭이 붙게 되었다.

마지막 일곱 번째 **임무완수단계**는 조직 내의 다양한 정보를 수집하여 외부로 전송시키는 단계이다. 이때 보안 장비에서 탐지되는 것을 회피하기 위해 수집한 정보를 암호화시키거나 데이터를 한 번에 전송하지 않고 100KB 정도의 적은 양으로 쪼개서 보내는 방법을 사용한다. 만약에 침투한 조직의 전산 자원이 더 이상 활용할 필요가 없어지게 되면 마지막 단계로 특정한 D-Day를 지정하여 내부 전산 자원을 파괴하는 등의 행위를 하는 경우도 있다.

앞에서 설명한 APT 공격의 각 단계가 [그림 5]에 정리되어 표시되어 있다. 최초 직원1이 악성코드에 감염된 웹사이트를 방문하여 악성코드에 감염이 된다. 감염된 직원1 PC를 통해 인터넷PC 관리솔루션 서버에 웹쉘이 업로드하여 이를 통해 인터넷망에 있는 모든 PC가 모두 악성코드에 감염된다. 인터넷망의 PC가 장악되고 정찰을 통해 내부망에 접근할 수 있는 통로인 망 연계 장비를 발견 후 취약점을 확인하여 침투하게 되고 내부망의 중앙관리솔루션을 장악하여 내부망의 PC까지 모두 악성코드에 감염시켜서 조직의 전산 자원을 완전히 장악하는 단계로 완성된다.

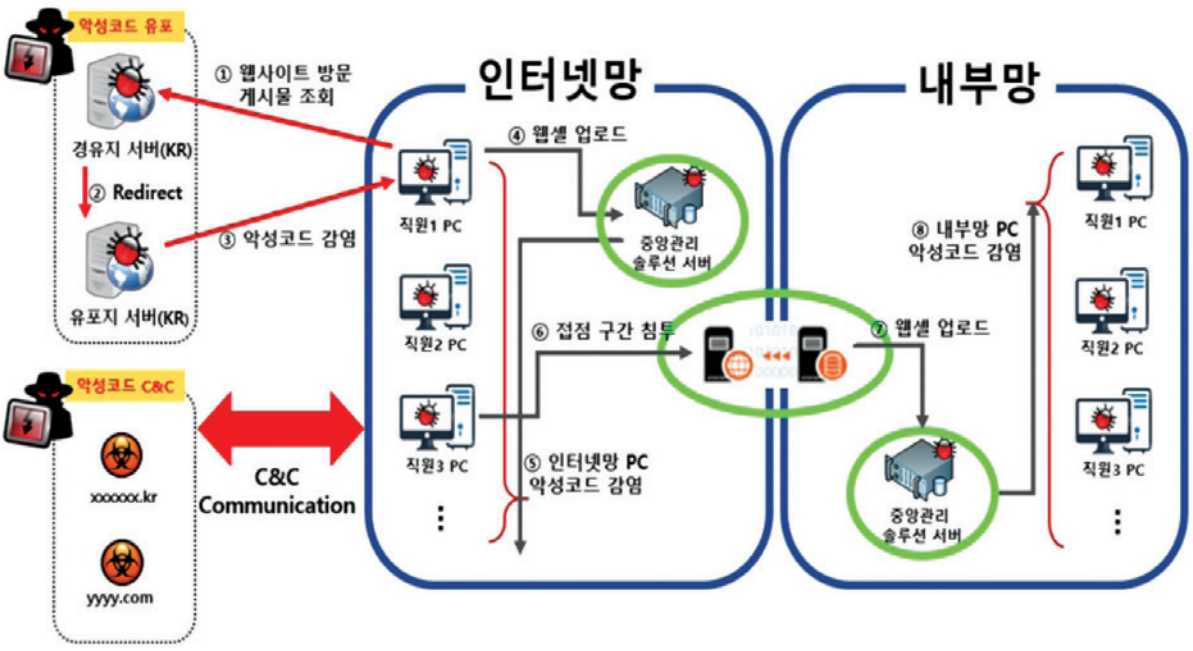

그림 5. APT 공격의 진행 순서

다음으로 이러한 공격기법을 통해 공격사례를 살펴보자. 일명 '320 전산 대란'으로 알려진 침해사고도 전형적인 APT 공격의 일종이다. 2013년 3월 20일 'KBS, MBC, YTN' 등 주요 방송사와 은행, 카드 회사 등의 전산망이 마비되었던 사건이다. 3월 20일 오후 2시 10분경부터 주요 방송사들의 컴퓨터가 일제히 작동을 멈췄다. 직원들의 PC는 정상작동 중에 재시작이 필요하다는 안내로 재부팅을 요구하거나 갑자기 자동으로 재시작이 되었으며 이후에 부팅이 안 되거나 작동이 멈춘 채 재부팅하라는 메시지만 띄우는 상황이 발생하였다. 비슷한 시간, 신한은행의 창구거래, ATM 거래가 모두 중단되었다. '우리은행'의 경우 DDoS 공격을 받았으나 보안 장비를 통해 방어해 냈다. 'LG유플러스'의 그룹웨어도 해킹당했다는 소식이 알려졌다. 이런 현상들이 동시다발적으로 이루어졌다는 점에서 고의적인 공격일 가능성이 거의 확실시 되었으며, 보안업체에서는 MBC.EXE, KBS.EXE라는 파일이 돌아다녔다고 확인하는 것으로 보아 계획된 공격의 정황이 농후해졌다.

사고가 발생한 이후 피해를 본 6개 기관의 컴퓨터 32,000대가 모두 동일한 해킹그룹(후이즈팀)의 이름이 들어간 악성코드가 발견되어 이 팀의 정체가 무엇인지, 북한과의 연계 가능성이 있는지 등을 조사하였다. 악성코드는 PC 부팅에 관여하는 MBR(마스터 부트 레코더) 영역뿐만 아니라 C 드라이브 영역을 모두 더미값(숫자 0이 반복되는 값)으로 여러 번 반복해서 덮어쓰기하여 PC가 부팅하지 못하고 부팅이 되더라도 데이터 복구가 불가능하게 만드는 방법을 사용한 것으로 확인되었다. 사건 발생 하루가 지난 상황에서 방송통신위원회는 방송국에서 사용 중인 하우리의 '바이로봇', 안랩의 'V3' 등의 바이러스 백신 업데이트 서버를 통한 악성코드가 유포된 것이 직원 PC의 작동 불능 원인으로 지목했다. 백신 업데이트 서버는 모든 PC가 신뢰하여 의심 없이 파일을 받아서 설치하는 것을 악용하여 전체 PC를 손쉽게 감염시킨 것이다. PC를 사용할 수 없는 기간 동안 'MBC 라디오'는 실시간 사연을 팩스와 휴대전화로 받았고, 'KBS'는 PC 스크린에 대본을 띄우지 못해 DJ 옆에 작가들이 붙어 앉아 실시간으로 대본을 써서 방송을 했다고 전해진다.

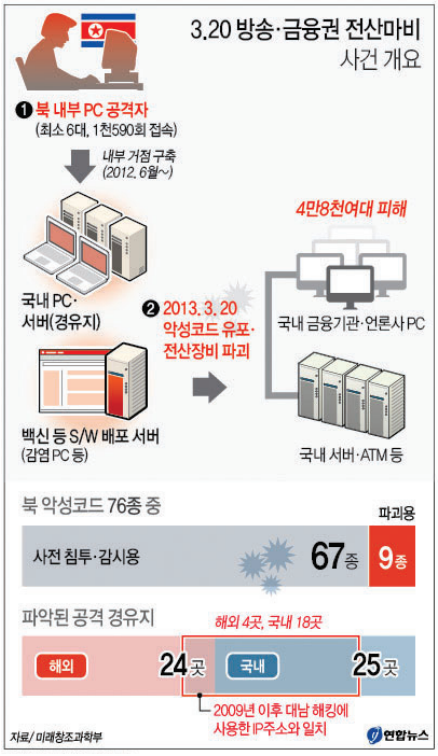

그림 6. 320 방송·금융권 전산 마비 개요 / 출처 : 연합뉴스

[그림 6]과 같이 민관군 합동대응팀의 분석결과 8개월 전부터 북한정찰총국이 국내에 내부거점을 구축한 이후 다양한 악성코드를 활용하여 방송국의 백신 배포 서버에 침투하여 공격을 수행한 것으로 결론 내렸다. 이 해킹그룹은 오랫동안 조직의 정보를 탈취하는 것보다 전산 자원을 파괴하여 공격능력을 과시하는 것이 최종 목표였던 것이다. 사건 발생 이후 재발 방지를 위해 다양한 PC 관리 서버의 취약점을 개선하고, 개선된 백신을 사용하여 악성코드의 탐지능력을 높이고 업무자료의 주기적인 백업을 통해 PC에 문제가 있더라도 이른 시일 안에 복구가 가능하게 하는 등 많은 개선을 이루어졌다.

다음으로 살펴볼 공격사례는 '평창 동계올림픽 개막식 공격'이다. 평창 이전의 올림픽 기간에도 DDoS 공격은 발생한 적이 있지만 평창올림픽은 2018년 2월 9일 오후 8시 개막식 시작에 맞추어 악성코드를 통해 올림픽운영에 필요한 핵심서버 50여 대가 파괴되었다. 이로 인해 올림픽 관련 웹사이트 마비, 올림픽 현장 와이파이 서비스 중단, 미디어센터 IPTV가 중단되고, 8시 이후에 개막식 티켓 발행이 중단되어 일부 좌석이 비어 있는 채로 개막식이 진행되었다. 다행인 것은 운영망과 방송망이 분리되어 있어 개막식 중계방송에는 문제가 없었다는 점이다. 여기에 사용된 악성코드를 분석해 보니 초기에는 북한과 연관된 것으로 보여, 북한이 이번 공격의 배후로 지목되었다. 그러나 미국 정보당국에서는 러시아 해외정찰국이 실제 공격의 배후로 결론 내렸

다. 러시아가 북한이 공격한 것으로 위장한 '위장전술작전'을 수행한 것이라고 밝혔다. 러시아가 평창올림픽을 대상을 사이버 공격을 벌일 만한 동기는 충분했다. 이전 하계올림픽에서 러시아당국이 선수들에게 조직적으로 금지약물을 복용시킨 것이 확인되어 평창올림픽에는 러시아 국적으로 경기에 출전할 수 없도록 제한한 것이 이번 공격의 동기로 추정되었다.

공격을 분석한 결과 [그림 7]와 같이 개막식 1개월 전인 1월에 올림픽 운영전산실과 연결된 라우터를 해킹한 이후에 이를 통해 내부 PC 300여 대를 감염시키고 내부에서 사용하는 44개의 계정정보를 탈취하여 서버접근 권한을 획득하고 개막식 시작 시각에 맞추어 서버 내의 데이터를 복구 불가능하게 지워버린 후 부팅이 불가능하게 파괴한 것으로 확인되었다.

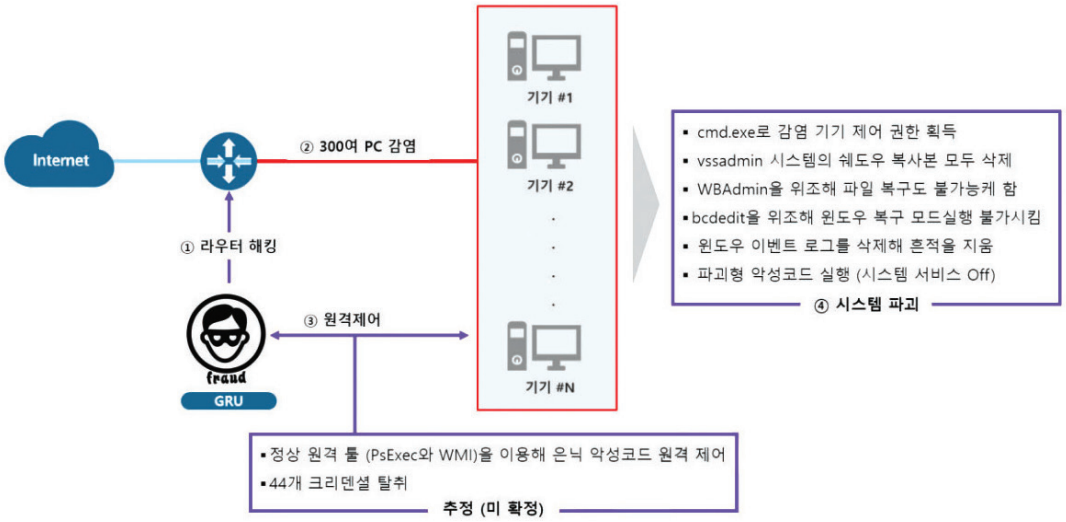

그림 7. 평창 동계올림픽 개막식 사이버 공격 순서 / 출처 : 수산INT

다행스러운 점은 올림픽운영팀이 이런 경우를 대비하여 데이터를 사전에 백업하고 재해복구훈련을 여러 차례 실시하면서 비상상황에 대비한 점이다. 공격 발생 이후 다음날 경기 시작 전인 오전 8시까지 파괴된 모든 시스템을 복구하였다. 그리고 시스템의 모든 계정정보를 바꾸고, 발견된 악성코드를 탐지하고 제거할 수 있는 백신을 긴급하게 제작하여 시스템에 적용하였다. 320 전산 대란 때 복구에 9일이 걸린 것에 비해 이번 공격은 12시간 만에 복구된 것은 올림픽조직위원회의 철저한 사전대비가 있었기에 가능한 것이었다.

마지막으로 이러한 APT 공격이 어떤 산업별로 얼마나 빈번하고 오랫동안 이루어지는지 알아보자. [표 2]는 APT 방어 장비 벤더에서 전 세계에 설치된 자사 장비에서 탐지하는 APT 공격 경보를 바탕으로 작성한 자료이다. 침해 통지 항목에서 '외부'는 조직이 APT 공격을 당한 사실을 외부 기관에서 통보받은 경우를 의미하고, '내부'는 조직이 공격을 당한 사실을 독자적으로 탐지한 경우를 의미한다. 2011년 내부에서 직접 탐지한 경우가 6% 정도였으나 2019년 47%까지 개선된 것을 확인할 수 있다. 그동안 여러 다양한 APT 공격 탐지 장비 도입과 강화된 보안 규정을 준수하고 보안 조직을 보강한 것이 내부탐지역량이 강화된 결과로 나타난 것으로 볼 수 있다.

침해 통지	2011년	2012년	2013년	2014년	2015년	2016년	2017년	2018년	2019년
외부	94%	63%	67%	69%	53%	47%	38%	41%	53%
내부	6%	37%	33%	31%	47%	53%	62%	59%	47%

표 2. APT 공격의 내부, 외부별 탐지 건수 / 출처 : FireEye M-Trend 2020

[표 3]은 APT 공격이 최초로 침입한 이후 탐지될 때까지 얼마나 소요되었는지를 나타내는 표이다. 항목의 숫자는 공격이 얼마나 지속하였는지를 평균값으로 나타낸 것이다. 2011년 평균 416일 동안 공격이 지속하였지만, 2019년에는 평균 56일 만에 공격이 탐지되었다. 내부에서 탐지된 시간은 평균 30일이 걸렸으나, 외부에서 탐지된 경우는 141일이 소요되었다. 외부에서 탐지하는 경우는 공격을 시작하는 거점이나 경유지, C&C 서버가 발각되어 조사하는 중에 공격 목표가 확인되는 경우가 많아 더 많은 시간이 소요되는 것으로 생각된다.

침해 통지	2011년	2012년	2013년	2014년	2015년	2016년	2017년	2018년	2019년
전체	416	243	229	205	146	99	101	78	56
외부	-	-	-	-	56	80	57.5	50.5	30
내부	-	-	-	-	320	107	186	184	141

표 3. APT 공격의 내부, 외부별 탐지에 걸린 시간 / 출처 : FireEye M-Trend 2020

[그림 8]은 특정 산업을 표적으로 한 APT 공격이 얼마나 탐지되었는지를 나타내는 그림이다. 탐지가 많이 된다는 의미는 그만큼 가치가 있는 데이터를 많이 생산한다는 의미일 수도 있고 APT 방어 장비 등 보안 인프라가 비교적 체계적으로 갖추어져 있다고도 볼 수 있다. 엔터테인먼트/미디어 산업의 경우 2015년 3위에서 2019년 1위까지 계속 TOP 5 안에 포함되는 산업군으로 APT 공격자 입장에서는 선호되는 목표이기 때문에 해당 산업군의 보안담당자는 좀 더 APT 공격에 대한 강화된 대처 방안을 마련해야 할 것으로 생각된다.

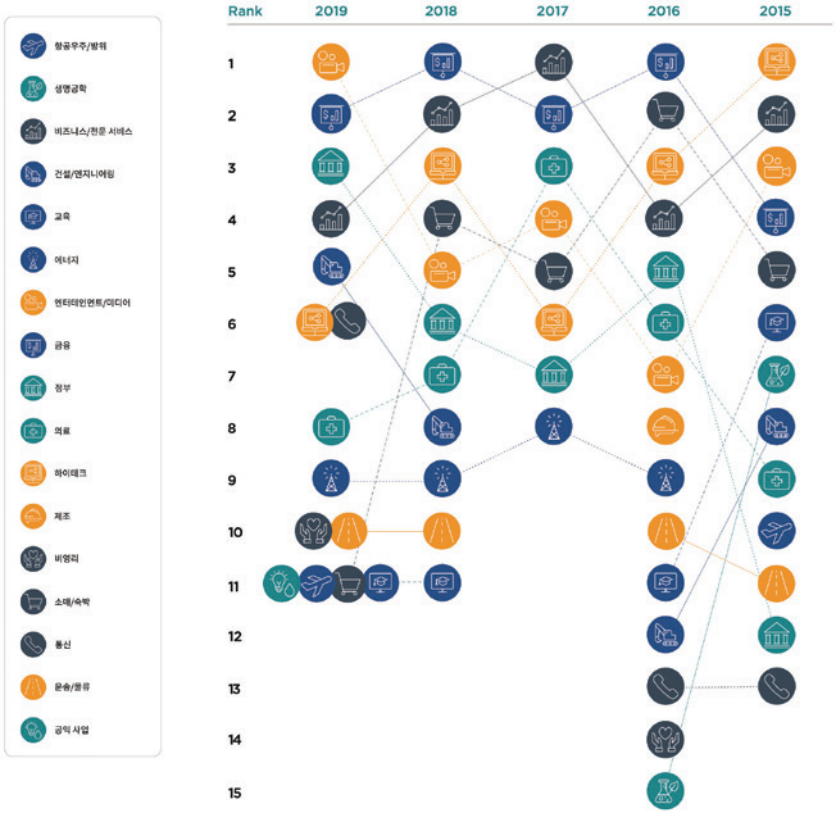

그림 8. APT 공격대상에 대한 산업별 통계정보 / 출처 : FireEye M-Trend 2020

다음 호에서는 이러한 APT 공격을 조사하는 과정에서 밝혀진 공격그룹의 실체와 공격의 주요 도구인 악성코드에 대해서 알아보고, APT 공격을 탐지하고 차단하기 위한 대응 방안에 대해서 설명하도록 하겠다.