이것만은 알아야 할 네트워크 보안 이야기
Part 9. APT 2. APT 공격그룹과 악성코드(Malware)

글. 이선응 아이크래프트 수석
Ka3211a@gmail.com

이번 호에서는 다양하게 발생하고 있는 APT 공격을 수행하는 공격그룹과 공격의 주요 도구인 악성코드를 통해 어떻게 공격이 이루어지는지 알아보도록 하겠다.

연재 목차

공격자의 입장에서는 공격을 수행하면서 이용하는 다양한 공격 인프라(공격을 하기 위해 이용하는 해킹한 서버, 경유지로 활용되는 해킹된 단말 PC, 사용한 악성코드)를 확보하여 공격을 시작한다. 이런 공격 인프라를 식별하기 위해서 공인 IP, 도메인, 호스트네임, URL, 공격에 사용한 악성코드 정보 등을 일정한 포맷으로 정리해 놓은 것을 공격침해지표, IOC(Indicators of compromise)라고 부른다. 이런 침해지표를 이용하여 방화벽의 보안정책과 IPS 등의 룰에 추가하여, 또 다른 대상을 향한 공격에 재활용되는 것을 막기 위해 많은 보안 벤더에서 해당 정보를 공유하여 방어에 활용된다. 그런데 이러한 공격 인프라는 쉽게 확보하고, 필요가 없어지면 쉽게 교체가 가능하기에 침해지표의 유효기간은 짧으며 계속된 활용이 불가능하고, 공격집단을 식별하기에는 한계가 있다.

그래서 보안전문가들은 공격집단을 좀 더 정확하고 긴 시간 동안 추적하기 위한 새로운 지표를 개발하였다. 그것은 공격자가 쉽게 바꾸기 힘든 기술 요소를 확인하여 공격그룹을 구분하는 것이다. APT 공격의 각 단계를 수행하기 위해서는 다양한 공격 전술(Tactic)과 기법(Technique), 절차(Procedure)들이 사용되고 있는데 이 세 가지 공격수단의 각 앞글자를 따서 TTP라고 부른다. 공격이 탐지된 이후에, 공격당한 시스템을 조사하다 보면, 단계별로 어떠한 TTP가 사용되었는지 확인할 수 있다. 공격 중 사용되는 다양한 TTP의 경우 공격을 준비하면서 타켓의 특성에 맞추어 오랜 시간 동안 학습하고 숙달하기 위해 자체 테스트환경에서 연습을 수행하며, 필요하면 새로운 공격툴을 직접 개발하기도 한다. 그래서 이런 공격을 추적하는 입장에서는 침투방식, 악성코드 유형, 공격망 구성방식 등의 전술 및 사용된 기술, 절차 등은 공격그룹들이 쉽게 바꾸지 못하고 계속 사용하려는 특성을 이용하여 그룹의 특성을 나타내는 TTP들을 파악하여 공격그룹을 구분할 수 있게 되었다.

인터넷 초창기의 공격자는 개인이나 2~3명의 그룹이 단순한 호기심이나 기술을 과시하는 아마추어적인 목적으로 해킹이 이루어졌다면, 현재의 환경은 거의 모든 사회 인프라가 인터넷을 통해 연결되어 있고 컴퓨터를 통해 대부분의 업무가 이루어져 사회의 필수인프라에 접근하여 조작/파괴하거나 높은 가치의 정보를 해킹을 통해 취득할 수 있는 환경이 되었다. 금전적인 이익을 추구하거나 국가의 후원을 받는 조직이 적성국가(적으로 간주되는 국가)나 경쟁국가를 공격하여 국가 단위의 이익을 추구하는 방식으로 공격의 목적이 다양해지고 규모가 확장된 것이다.

침해 조사단계에서 TTP 정보를 통해 확인되는 특정 그룹은 임시(TEMP) 그룹으로 분류하고 있다가 다른 침해조사에서 같은 특성이 반복되어 나타날 경우, 식별된 그룹으로 격상된다. TEMP 그룹에 대한 정보가 충분히 확보되면, 공격의 성격에 업무용 이메일 사기나 자금 탈취행위 등 고도의 금융 범죄를 일으키는 범죄 그룹은 FIN으로 분류하고, 국가의 후원을 받아 스파이 활동에 주력하는 그룹은 APT라는 이름을 부여한다. [그림 1]은 APT 공격을 탐지하여 침해조사 중에 사용한 다양한 TTP 정보의 특성을 바탕으로 식별된 APT 그룹을 국가별로 구분하여 표시한 내용이다. 중국을 시작으로, 이란, 북한, 러시아, 미국, 우즈베키스탄, 베트남 등 다양한 국가의 후원을 받는 것으로 추측되는 공격그룹이 나열되어 있다.

China [edit]

Further information: Chinese espionage in the United States

- PLA Unit 61398 (also known as APT1)
- PLA Unit 61486 (also known as APT2)
- Buckeye (also known as APT3)[33]
- Red Apollo (also known as APT10)
- Codoso Team (also known as APT19)
- Wocao (also known as APT20)[34][35]
- PLA Unit 78020 (also known as APT30 and Naikon)
- Periscope Group (also known as APT40)
- Double Dragon (also known as APT41)[36]
- Tropic Trooper[37][38]
- Winnti Group[39][40]

Iran [edit]

- Elfin Team (also known as APT33)
- Helix Kitten (also known as APT34)
- Charming Kitten (also known as APT35)
- APT39

North Korea [edit]

- Ricochet Chollima (also known as APT37)
- Lazarus Group (also known as APT38)

Russia [edit]

- Fancy Bear (also known as APT28)
- Cozy Bear (also known as APT29)
- Voodoo Bear
- Venomous Bear

United States [edit]

- Equation Group[41]

Uzbekistan [edit]

- SandCat (associated with the National Security Service (Uzbekistan))[42]

Vietnam [edit]

- OceanLotus (also known as APT32)[43]

그림 1. 공격침입조사 중 TTP 특성을 통해 식별된 APT 공격그룹 / 출처 : 위키피디아

여기서 북한과 중국의 공격그룹을 소개하도록 하겠다. 먼저 북한의 APT38 그룹으로 2014년 이후 13개국 이상에서 은행, 금융기관을 공격하여 자금 탈취를 주목적으로 활동하고, 파괴적인 악성코드를 이용하여 금융기관에서 수억 달러의 자금을 탈취하려는 시도를 하였다. 주로 은행을 대상으로 정교한 공격을 펼치는데, 장기적인 계획하에 자금 탈취를 시도하기 전에 피해 환경에 장기간 숨어 있으면서, 맞춤형 개발도구를 사용하며, 침해시스템을 파괴하려는 의도가 있는 것으로 알려져 있다. 북한 정권에 대한 강화된 경제 제재로 인한 어려움을 금융시스템 공격을 통해 만회하려는 충분한 동기가 있는 것으로 파악된다.

[그림 2]는 APT38 그룹을 조사하면서 공격단계별로 사용한 TTP를 표시한 목록이다. 단계별로 사용 가능한 기술과 절차는 굉장히 다양하지만 한 그룹이 사용하는 기술과 절차는 한정적이다. 그래서 각 단계에서 사용한 기술과 절차를 통해 공격그룹의 구분이 가능한데, 이런 특성을 통해 공격그룹을 특정하고 추적이 가능한 것이다.

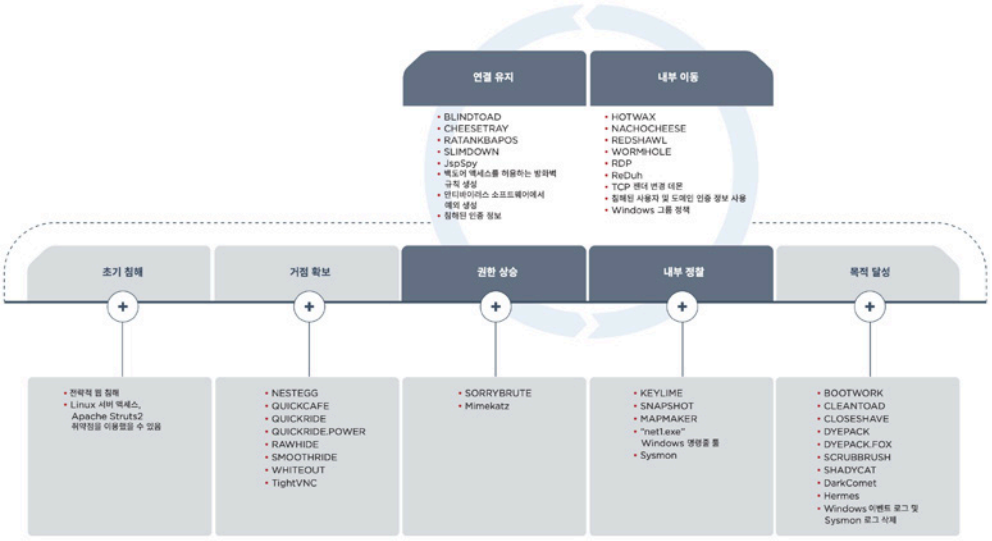

그림 2. APT38 그룹의 공격단계별 사용된 TTP 목록 / 출처 : 파이어아이 M-Trend 2019

다음으로 중국 정부의 후원을 받는 것으로 추정되는 APT41 그룹이다. 이 그룹은 중국 정부의 지원을 받으며 스파이 활동을 벌이고 금전적 목적을 위해 활동하는 공격그룹으로, 정부의 지원을 받기 전까지 비디오 게임 산업을 표적으로 활동한 그룹이었다. 이 그룹은 소프트웨어개발사를 공격하여 정식으로 출시되는 정상적인 프로그램의 파일에 악성코드를 심는 방식으로 공격을 진행하였고 금전적 이익을 목적으로 하는 영리 추구가 주목적이었다. 식별된 초기에는 전문 컨설팅, 통신, 뉴스, 미디어 조직을 대상으로 공격하는 정부 후원그룹과는 구분되었으나, 최근 정부 후원 그룹과 비슷한 목적으로 스파이 활동을 주목적으로 하는 그룹으로 성격이 바뀌면서, 기존의 독립적인 그룹이 정부의 후원을 받

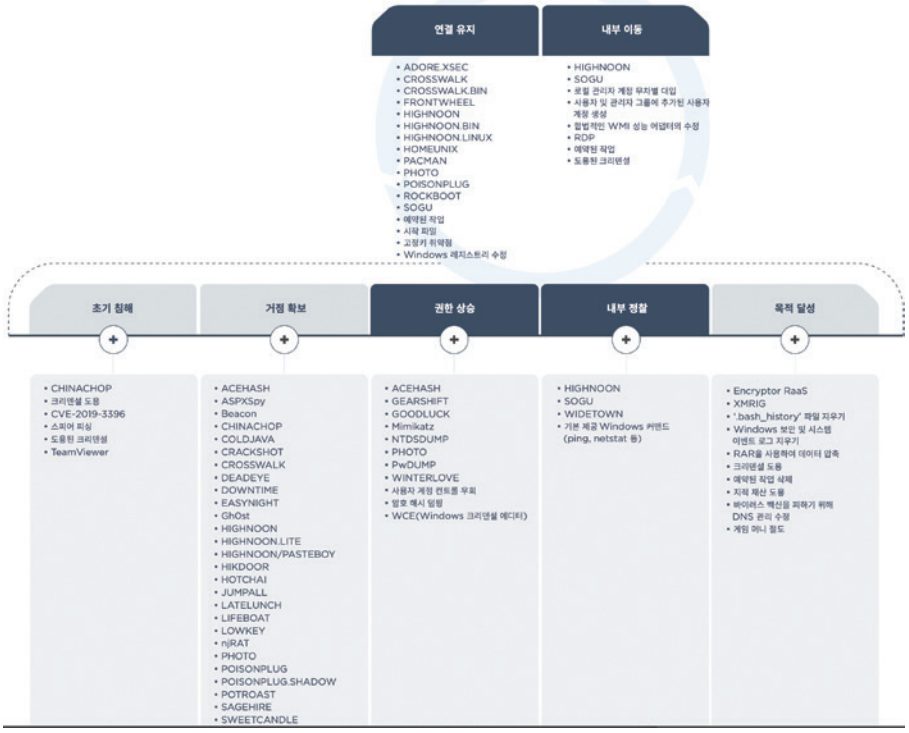

그림 3. APT41 그룹의 공격단계별 사용된 TTP 목록 / 출처 : 파이어아이 M-Trend 2020

기 시작한 것으로 추정된다. 이 그룹이 사용하는 TTP 내역을 [그림 3]과 같이 기술하였다. 2012년 최초로 식별된 이후로 다양한 기술과 절차를 사용하여 공격한 것을 확인할 수 있다.

이 외에도 러시아, 이란 등의 후원을 받는 것으로 의심되는 공격그룹이 다수 식별되었다. 러시아의 경우 NATO, 동유럽, 우크라이나 및 에너지 부분에 대한 공격을 지속하였다. 또한 미국과 프랑스 선거를 표적으로 하고, 평창 동계올림픽에 대한 공격으로 능력을 과시하였다. 러시아 APT 그룹에 대한 공개적인 노출과 법적인 기소에도 불구하고, 러시아의 전략적 이익에 따라 정치, 국제기관을 대상으로 전 세계적인 사이버 공격을 지속해서 수행하고 있다.

이란의 경우 자국의 핵발전소가 이스라엘의 사이버 공격으로 파괴되는 공격을 받은 이후 방어적 성격으로 2011년 국가 사이버사령부를 창설하였다. 비대칭 전력으로 미국의 제재에 대한 보복 및 전쟁 억제, 정치적 영향력 및 경쟁력 확보 등을 목적으로 활동하였다. 이후 미 방위산업 관련 조직에 대한 정부수집 활동 등 다양한 공격그룹(APT33, 34, 35, 39)을 양성하여 수동적인 공격에서 능동적이며 공세적인 공격 수준으로 비약적으로 발전하였다.

마지막으로 소개할 그룹은 한국을 주요 공격목표로 하는 북한의 공격그룹으로 추정되는 김수키(Kimsuky)라는 그룹이다. 국내에는 10,799명의 개인정보와 원자력발전 제어프로그램 자료, 원전설계도 등이 유출된 2014년 한수원 해킹 공격을 주도하였다. 사회공격기법의 공격방식을 사용하고, 다양한 국내/외 사회적 이슈 및 북한 관련 이슈들을 이용하여 활발한 공격을 진행하고 있다. [그림 4]와 같이 최근에는 코로나19 관련 문서로 사칭한 워드 매크로 악성코드를 첨부하여 '코로나 바이러스 관련 이사장님 지시사항'이라는 제목으로 악성메일을 유포한 바 있다. 또한 21대 국회의원 선거문서로 사칭한 '21대 국회의원 선거관련.docx', '외교문서 관련(이재춘국장).docx' 파일 등으로 위장하거나 한국과 미국의 대북 관련 분야에 종사하는 인물을 대상으로 파일을 열어볼 경우 정보 유출이 이루어지는 공격이 발견되는 등 정보 탈취를 주목적으로 하는 그룹이다.

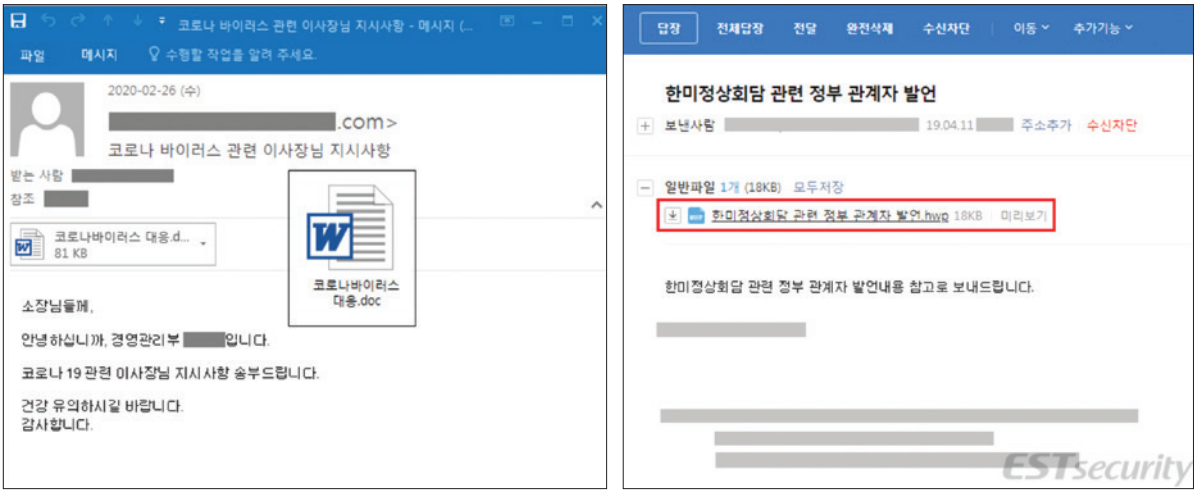

그림 4. 김수키(Kimsuky) 그룹이 발송한 스피어피싱 메일 / 출처 : ESTsecurity

다음으로 다양한 APT 공격을 하기 위한 도구로 이용되는 멀웨어(Malware)에 대해서 알아보자. 악성코드(Malicious Code)라고도 불리며, 정상적인 기능을 위해 만들어진 것이 아니라, 사용자에게 해악을 끼치는 악의적인 목적으로 만들어진 모든 코드의 총칭이다.

구현 방법으로 컴퓨터 바이러스, 트로이목마, 웜 등이 존재한다. 요즘은 악성코드 유포 사유가 점점 더 금품을 요구하는 목적으로 변하였으며, 랜섬웨어처럼 사용자의 데이터를 인질로 하여 협박, 갈취하는 방식으로 발전하여 굉장히 활성화되어 있는 공격방식으로 발전하였다. 기능에 따라 분류해보면 사용자의 동의 없이 개인정보를 빼가는 '스파이웨어', 시스템에 대한 정상적인 절차를 거치지 않고 시스템에 접근을 가능하게 하는 '백도어', 컴퓨터의 관리자 레벨의 권한으로 접근을 가능하게 해주는 '루트킷', 사용자의 키보드 입력정보를 텍스트 파일로 저장하는 '키로그', 컴퓨터 내의 데이터에 접근할 수 없게 암호화하여, 데이터를 인질로 금품을 요구하는 랜섬웨어(Ransom(인질)+Ware), 사용자의 동의 없이 광고를 강제로 보여주는 '애드웨어' 등이 모두 멀웨어 범주에 속한다.

여기서 APT 공격에 활용되는 것은 스파이웨어, 백도어, 루트킷, 키로그 등이 기능이 활용되고 있는데 최초 이러한 악성코드를 컴퓨터에 감염시키기 위해서는 악성코드가 공격대상 조직의 컴퓨터에서 실행되게 만들기 위해 웹브라우저를 통한 '워터링홀' 공격방식이나 사용자에게 이메일을 보내 공격하는 '스피어피싱' 공격을 이용한다고 이전 호에서 설명하였다. 이런 악성코드가 컴퓨터에서 실행된다고 모든 컴퓨터가 감염되는 것은 아니고, 해당 컴퓨터의 OS 혹은 프로그램의 취약점이 있고, 그 취약점을 악용할 경우에만 악성코드에 감염된다. 여기서 취약점이란 쉽게 말해 버그(bug)인데 이 버그를 악용하면 특정한 명령을 임의로 실행하게 만들거나, 임의로 파일을 생성하거나 파일을 업로드한 후 실행시켜 최종적으로 시스템의 관리자 권한을 획득하게 만들 수 있는, 말 그대로 취약점이다. 통상 보안취약점은 CVE(Common Vulnerabilities and Exposures)로 불린다. [그림 5]는 국내에서 개발되어 사용 중인 소프트웨어에서 발견되어 신고된 취약점 리스트를 캡처한 내용이다. 여기서 각 취약점의 ID는 발견된 년도와 일련번호를 표시한 것이다. CVE-2020-7814이란 2020년도에 발견된 7814번째 취약점이란 뜻이다. 이러한 취약점은 컴퓨터뿐만 아니라 휴대폰, 네트워크 장비, 보안장비, 서버, 집에서 사용하는 공유기, 가전제품 등 소프트웨어를 사용하는 모든 시스템에서 발견되는 것으로, 이런 취약점을 보완하지 않으면 언제든지 공격자를 통해 해당 시스템이 공격당할 위험이 지속할 수밖에 없다.

번호	제목	조회수	첨부	게시일
45	CVE-2020-7814 | 라온위즈 KUpload 파일 다운로드 및 실행 취약점 NEW	501		2020.07.03
44	CVE-2020-7820, CVE-2020-7821 | 투비소프트 NEXACRO14/17 ExtCommonApiV13 임의 코드 실행 취약점 NEW	378		2020.07.01
43	CVE-2020-7816 | DaView Indy, DaVa+. DaOffice 스택 오버플로우 취약점 NEW	518		2020.06.30
42	CVE-2019-19161 | 투비소프트社 MIPLATFORM CyMiInstaller322 ActiveX에 존재하는 파일교체 가능 취약점 NEW	528		2020.06.29
41	CVE-2019-19163 | 코맥스 월패드 코드 실행 취약점 NEW	443		2020.06.29
40	CVE-2019-19160 | Cabsof의 Reportexpress ProPlus ActiveX 원격 명령 실행 취약점 NEW	415		2020.06.29
39	CVE-2020-7812, CVE-2020-7813 | 가온아이 ezHTTPTrans Active-X 파일 다운로드 및 실행 취약점	2,080		2020.05.21
38	CVE-2020-7808 | 라온위즈社 K Upload 제품에서 발생하는 무결성 검사 미흡으로 인한 코드 수정 가능 취약점	2,620		2020.05.19
37	CVE-2020-7809 | 이스트소프트 알송 DOM-Based XSS 취약점	2,566		2020.05.14
36	CVE-2019-19162 | 투비소프트 XPLATFORM Use After Free 취약점	2,866		2020.05.11

그림 5. 국내에서 개발된 소프트웨어의 보안취약점 리스트 / 출처 : 한국인터넷진흥원

이러한 취약점은 사용자가 우연히 발견할 수도 있고, 제품을 개발한 제조사, 전문 테스트 기관에서 발견하여 개발사에 신고를 통해 알려지기도 한다. 신고를 접수한 개발사는 최대한 빠른 시간에 해당 취약점을 제거한 수정 버전을 내놓아 사용자들이 취약점을 제거할 수 있도록 하고 있다. 우리가 컴퓨터를 사용할 때 Windows OS를 사용하다 보면 윈도우

업데이트가 된다는 메시지를 자주 접하게 된다. 마이크로소프트사에서 개발한 윈도우 OS에 있는 보안취약점을 자체적으로나 혹은 외부에서 확인되어 취약점을 제거할 수 있는 수정 파일을 다운로드받아 컴퓨터에 적용하는 과정이다.

또한, 취약점을 발견한 개인이나 단체가 이 취약점을 개발사에 알리지 않고 공격에 악용할 수도 있는데 이런 알려지지 않은 취약점을 이용하는 공격을 제로데이(Zero-Day) 공격이라고 불린다. 즉, 취약점이 알려지지 않았거나, 아직 취약점을 제거할 수 있는 패치가 나오지 않은 상태로 제로데이라는 뜻은 해당 취약점이 알려지거나 발견된 날을 뜻하며, 개발사가 취약점을 제거할 수 있는 수정본을 개발하기에는 얼마간의 시간이 필요한데, 아직 패치가 나오기 전의 상태를 말한다. 즉 해당 취약점에 대한 대책이 아직 없기에 해당 취약점을 이용한 공격을 막을 수 없어서 어떤 컴퓨터라도 해당 취약점을 가지고 있는 소프트웨어를 쓰고 있다면 공격에 무방비로 노출될 수밖에 없는 상태에 놓여 있는 것을 뜻한다.

이런 특징으로 인해 제로데이 취약점은 공격자들에겐 만능 무기를 소유하고 있는 것으로 간주되며, 모든 공격자가 취약점을 찾는 데 혈안이 되어 있다. 설령 취약점을 찾는다고 해도 함부로 사용하지 않고, 결정적인 타켓이나 중요한 동기가 생겼을 때 사용하기 위해 아껴 두게 된다. 본인이 이용할 동기가 없다고 하면 이런 취약점을 공격자끼리 혹은 소프트웨어 개발사와 거래하는 경우도 있다. [그림 6]은 이렇게 발견한 취약점의 종류에 따라 책정된 가격 리스트이다. 발견된 취약점을 적용할 수 있는 OS가 얼마나 많이 사용되는지, 얼마나 쉽게 적용할 수 있는지, 얼마나 광범위하게 영향을 미칠 수 있는지에 따라 가격을 책정해서 거래가 이루어지는 금액을 표시한 것이다. 그림에서 오른쪽 제일 상단 박스의 경우 윈도우 OS를 사용하기만 하면 적용할 수 있고 사용자가 별다른 동작(클릭)이 없더라도 자동으로 원격에서 공격자가 원하는 악성코드를 실행해서 컴퓨터를 장악할 수 있는 취약점이 발견된다면 최대 백만 달러까지 가격이 책정되어 있는 것을 확인할 수 있다.

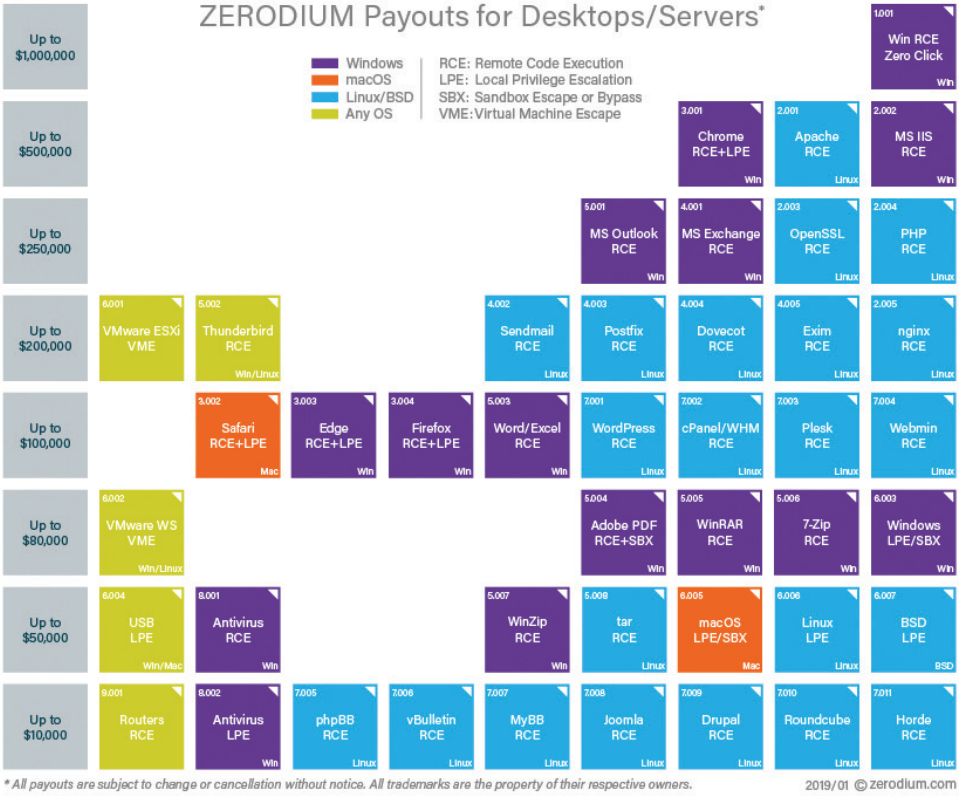

그림 6. 발견된 취약점의 종류에 따라 책정된 가격정보 / 출처 : Zerodium

이러한 취약점이 발견된 후 취약점을 제거할 수 있는 업데이트 혹은 패치를 적용하지 않게 되면 이를 이용하여 시스템에 침입할 수 있는 수단으로 활용될 수 있다. 이렇게 취약점을 이용한 공격을 익스플로잇(exploit)이라고 한다. 발견된 보안 취약점을 이용하여 공격자의 의도된 동작을 수행하도록 만들어진 절차 혹은 명령, 스크립트, 프로그램을 뜻한다. 국가의 후원을 받는 APT 공격그룹의 경우 이러한 제로데이 익스플로잇(알려지지 않은 취약점 공격)을 보유하고 있다가 대규모 공격에 활용된 경우가 많다. 예를 들면 CVE-2015-6585 취약점의 경우 한컴오피스 2014에서 발견된 취약점으로 이를 주로 사용하는 공공기관과 교육기관을 타켓으로 북한의 공격그룹이 공격에 활용한 경우가 있었다.

익스플로잇이 성공하게 되면 공격자는 실제 악성 행위를 수행하는 악성코드를 감염시스템에 설치하게 되는데 이때 사용되는 프로그램이 드로퍼(Dropper)이다. 드로퍼가 사용되는 이유는 악성코드를 압축해서 시스템에 설치된 백신 등의 보안프로그램 탐지를 회피하고 필요 시에 압축을 해제하여 메모리에 올려서 동작이 가능한 상태로 만드는 역할을 수행한다. 드로퍼에 의해 악성코드가 정상적으로 작동을 시작하면, 감염시킨 시스템에 대한 정보를 사전에 설정된 외부 서버(C&C 서버)로 전송한 후 추가적인 악성코드나 공격자의 명령을 수행하게 되는데 이런 동작을 콜백(Callback)이라고 한다. 앞에서 설명한 세 가지 단계를 통해서 공격자는 시스템감염을 완성하게 되는데 [그림 7]을 통해 이 단계를 정리해 보았다. APT 공격은 아래 세 가지 단계를 통해 시스템을 감염시켜야 공격이 시작될 수 있다. 방어자의 입장에서는 감염된 이후에 공격을 탐지하는 것보다는 시스템을 감염시키는 초기 단계를 탐지해서 차단하는 것이 더 효율적인 방어라고 할 수 있다. 그래서 많은 APT 탐지 장비들이 이 단계를 집중해서 공격을 탐지하려고 한다. 좀 더 자세한 사항은 APT 공격방어장비를 소개할 때 설명해 드리도록 하겠다.

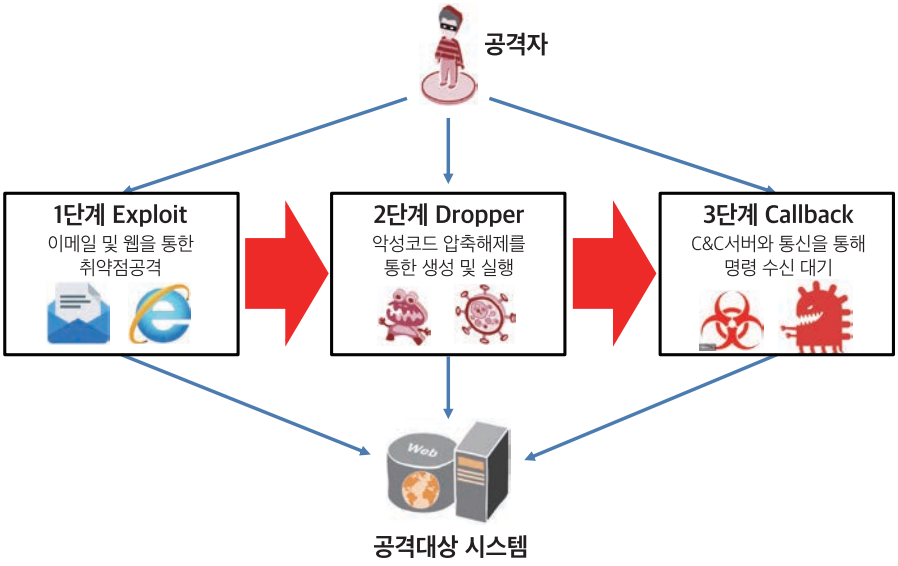

그림 7. APT 공격 초기 시스템감염 순서

악성코드에 의한 침해사고가 빈번해 지면서 여기에 대응하기 위한 방어기술이 발전하고 방어체계가 발달하면서, 점점 악성코드를 통한 공격 성공률이 떨어지게 되었다. 이에 대응하는 공격자의 전략도 발전하게 되는데 악성코드가 컴퓨터에 감염되는 것을 차단하는 백신의 탐지 성공률이 증가하게 되자 탐지를 회피하기 위해 다양한 멀웨어 변종의 출현이 증가하게 되었다. 변종 멀웨어의 증가에 대응하기 위해 가상환경에서 멀웨어가 동작하는 행위를 모니터링하여 악성 여부를 판단하는 기술이 발전하면서 다시 악성코드 탐지율이 증가하자, 이에 대응하여 가상환경에서의 탐지를 우회하는 기술이 개발되어 발달하게 된다. 창과 방패의 경쟁이 무한 반복되고 있는 것이다. 그럼 하나씩 자세히 알아보자.

악성코드의 사용이 활성화되면서 처음부터 전부를 개발하는 것이 아니고 최초로 만들어진 멀웨어의 원형을 참고해서 변형시키거나 멀웨어 생성툴을 통해 손쉽게 새로운 멀웨어 변종을 개발하여 공격에 이용되는 경우가 흔해졌다. 그 이유는 취약점이 발견되면, 취약점을 악용하여 멀웨어가 개발된 후, 이를 이용하여 실제 공격이 발각되면 침해사고분석을 통해 사용된 멀웨어가 분석되어 사용한 정황이 노출되기 때문이다. 이렇게 노출된 멀웨어는 패턴이 추출되어 바이러스 백신에 등록되어 이후 공격에서는 백신에 의해 쉽게 탐지가 되기 때문에 동일한 멀웨어를 통한 공격 성공률은 떨어질 수밖에 없다. 한 백신 업체의 보고서에 의하면 평균 4초마다 새로운 변종이 1개씩 생성된다고 한다. 대략 6개월만에 410만 개, 1년 사이에 600만 개의 멀웨어 변종이 등장하기 때문에 모든 변종의 패턴을 백신에 업데이트하는 것은 불가능한 점을 이용하여 물량 공세를 통해 공격 성공률을 높이는 전략을 사용한다.

멀웨어를 탐지하는 방식에는 크게 정적 분석과 동적 분석이라는 두 가지 방식이 있다. 정적 분석은 멀웨어를 실행하지 않고 그 파일 자체가 가지고 있는 내용을 통해 멀웨어 여부를 판단하는 것이다. 비교적 쉽고 빠르게 높은 기술 수준 없이 수행 가능한 장점이 있지만, 요즘같이 변종을 쉽게 만들 수 있는 환경에서는 공격 탐지가 점점 어려워지고 있다. 동적 분석은 의심되는 파일을 가상화 시스템에서 실제 실행을 시켜 생성되는 프로세스 및 파일을 모니터링하고 외부 서버와 통신 여부를 확인하여 악성 여부를 판별하기 때문에 정적 분석에 비해서는 좀 더 정확하게 악성 여부를 판단할 수 있다. 그러나 분석에 시간이 비교적 많이(1~5분 정도) 소요되고, 여러 개의 가상환경을 동시에 이용하고 관리하기 위해 고성능의 하드웨어가 필요한 점이 단점이라고 할 수 있다.

동적 분석을 통한 멀웨어 탐지 장비의 보급이 활성화되면서 공격 성공률이 떨어지자 멀웨어 제작자들은 가상환경을 탐지할 수 있는 기능을 추가하여 탐지를 회피할 수 있는 능력을 추가하였다. 멀웨어가 실행되는 환경이 실제 컴퓨터인지 가상환경인지 구분하여 실제 컴퓨터이면 악성 행위를 시작하고, 가상환경으로 판단되면 악성 행위를 하지 않고 탐지를 회피하는 전술을 사용하기 시작한 것이다. 이 전술은 동적 분석 장비를 개발하는 보안벤더가 가상화 환경을 다양한 사용자의 실제 환경을 똑같이 모사할 수 없어서 규격화된 몇 개(5~10개)의 가상환경만을 이용하여 탐지할 수밖에 없는 빈틈을 이용한다. 가상환경인지 여부를 판단하기 위해서 아래와 같은 다양한 방식을 사용한다.

1. 사람의 개입을 통한 마우스 포인트의 움직임, 클릭 동작, 스크롤 동작이 있는지 확인
2. 사용자의 응답을 요구하는 대화상자를 표시하여 응답 여부를 확인
3. 멀웨어가 설치되면 바로 동작하지 않고 일정 시간 대기하거나 특정 시간에만 동작하게 설정
4. 많이 사용하는 가상화 소프트웨어의 특정 요소의 값과 버전을 파악하여 일치하는지 여부 확인
5. 멀웨어가 설치되면 재부팅되기 전까지 악성 행위를 하지 않고 대기

물론, 멀웨어 탐지장비를 개발하는 벤더에서도 이런 탐지우회전술을 감안하여 새로운 탐지방식을 개발하여 적용하지만 이러한 공격자와 방어자 간의 도전과 응전은 반복될 수밖에 없다.

다음 시간에는 APT 공격의 증가로 인한 기존 보안모델의 문제점을 해결하기 위해 각광받고 있는 Zero Trust 보안모델을 알아보고, AI(인공지능)를 공격 탐지에 활용하는 방안과 인공지능의 공격 탐지 정확도를 높이기 위한 빅데이터의 중요성에 대해 알아보도록 하겠다.