https://doi.org/10.33778/kcsa.2024.24.3.153

한국어 기반 APT 그룹의 공격사례 및 인텔리전스 활용 방안★

이 정 훈*, 최 윤 성**

요 약

IT 기술이 발전하고 많은 기업들이 보안 솔루션을 채택함에 따라 해킹 위협과 보안 위협이 증가하고 있음에도 불구하고 사이버 공격과 위협은 여전히 수년간 지속되고 있다. APT 공격은 특정 대상을 선택하여 지속적으로 공격하는 기법으로 지능적이고 지속적인 공격을 의미한다. APT 공격의 위협은 수년간 APT를 수행하기 위해 전자 네트워크를 통해 가능한 모든 수단을 사용한다. 제로데이 공격, 악성코드 유포, 사회공학적 기법 등이 수행되며 일부는 직접 기업에 침입하기도 한다. 이러한 기법들은 이미 2000년부터 시행되고 있으며 특히 사회공학적 기법의 경우 보이스피싱에서도 유사하게 사용되고 있다. 따라서 APT 공격에 대한 대응방안 연구가 필요하다. 본 연구는 한국을 대상으로 한국어 기반의 APT 그룹들의 공격사례들을 분석하고 APT 공격그룹을 분석하기 위한 올바른 인텔리전스 사용 방법을 제시한다.

How to use attack cases and intelligence of Korean-based APT groups

Lee Jung Hun*, Choi Youn Sung**

ABSTRACT

Despite the increasing hacking threats and security threats as IT technology advances and many companies adopt security solutions, cyberattacks and threats still persist for years. APT attack is a technique of selecting a specific target and continuing to attack. The threat of an APT attack uses all possible means through the electronic network to perform APT for years. Zero-day attacks, malicious code distribution, and social engineering techniques are performed, and some of them directly invade companies. These techniques have been in effect since 2000, and are similarly used in voice phishing, especially for social engineering techniques. Therefore, it is necessary to study countermeasures against APT attacks. This study analyzes the attack cases of Korean-based APT groups in Korea and suggests the correct method of using intelligence to analyze APT attack groups.

Key words : APT attack, Cyber Security, Advanced Persistent Threat, Threat Intelligence, Korean Based APT

접수일(2024년 08월 06일), 수정일(1차: 2024년 09월 10일), 게재확정일(2024년 09월 19일)

★ 본 논문은 2023학년도 인제대학교 학술연구조성비 보조에 의한 것임 (This work supported by grant from Inje University, 2023)

* 인제대학교 컴퓨터공학부 학사과정(주저자)

** 인제대학교 AI빅데이터학부 조교수 (교신저자)

1. 서 론

APT 공격의 위협은 수년간 APT를 수행하기 위해 전자 네트워크를 통하여 가능한 수단과 방법을 가리지 않는다. 제로데이 공격을 포함한 악성코드 유포, 및 사회공학적 기법 등 다양한 종류의 최신 해킹기법이 APT 공격에 활용되고 있으며, 특정 회사에 직접적으로 침입하여 심각한 문제를 발생시키기도 한다. 해당 방법이 2000년 이전부터 이미 수행되고 있었고, 특히 사회공학적 기법의 경우에는 보이스피싱에도 적용되고 있다. [1]

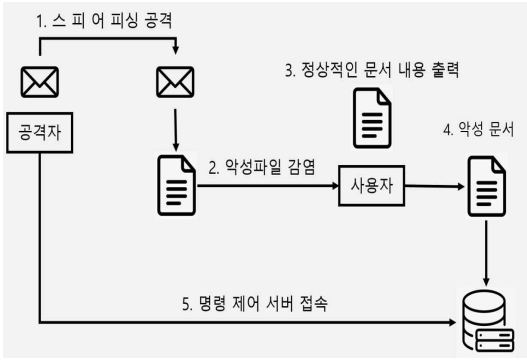
보안 기업들이 APT 공격을 막기 어려운 이유는 여러 가지가 있는데, 전통적인 정보보안은 한 분야에 집중되어 있다. 예를 들어 방화벽, 백신, 보안 관제 등 분야별로 나누어져 있으며, APT 공격은 정보보안의 빈틈과 취약한 사각지대를 공격하기 때문에 감지하는데 어려움이 존재한다. 따라서 보안 기업에서 시행하는 보안 정책은 부분적인 방어이며 APT는 종합적인 공격이라고 할 수 있고, APT 공격은 공격자가 주도권을 가진다. [2]

공격자는 보안 기업의 취약점을 알고 있으면서, 보안 기업은 공격자를 감지하기 힘들다. 특히 APT 공격은 공격의 규모도 작은데다 정밀해서 감지하기 힘들고, 해커는 적당한 시점이 되기까지 매우 길게 대기할 수 있으며, 사회공학적 기법까지 동원하고 있다. 즉, 인간의 허점을 노리고 있는데 보안을 운영하는 회사의 주체도 결국 사람이기 때문에 언젠가는 실수를 저지르게 되어있다. 해커가 이 허점을 이용하여 공격을 시도하면 시스템이 붕괴할 수 있다. 특히, 내부 직원이 기업에 앙심을 품거나 직원 하나하나가 다 빈틈인 경우는 매우 심각한 위험의 원인이 될 수 있으며, 실제로 대다수의 APT는 보이스피싱과 비슷하게 인간의 욕심을 실수로 가장하여 정보를 스스로 유출하도록 유도하고 있다. 이메일을 기반으로 하여 각종 최신 기법과 바이러스를 동원한 APT 공격이 점차 증가하고 있다. 따라서 APT 공격에 대한 올바른 인텔리전스의 사용으로 APT 공격을 최소화하고 대응하기 위한 연구가 필요하다. 본 논문에서는 APT 공격의 시나리오 및 공격 유형의 기본적인 형태를 알아보고 한국어를 사용하는 APT 공격그룹별 특징과 공격 벡터 및 공격 유형 그리고 공격 대상에 대한 전반적인 개요와 공격에 사용된 기법들을 분석하여 각각의 공통점과 차이점을 알아본 후 한국어 기반 APT 공격으로부터 피해를 최소화하기 위한 올바른 인텔리전스 사용법을 제시하는 것으로 결론을 맺는다.

2. APT 공격의 정의와 형태

2.1 APT 공격의 정의

APT(Advanced Persistent Threat)는 (그림 1)과 같이 개인 및 기관 또는 기업을 상대로 지속적인 해킹 공격 시도를 통해 개인정보나 중요한 데이터를 유출하는 형태의 공격을 의미한다. 해커가 특정 목표를 정해두고 계획적으로 접근 후 일정 시간 감시하다가 보안이 취약한 시점에 모든 데이터를 탈취한다. [1-4][7-9]



(그림 1) APT 공격 시나리오

대부분의 개인이나 기업에서 APT 공격의 피해를 보는 경우, 공격의 초기부터 정밀하게 계획한 후 접근하여 취약한 곳을 감시하다가 공격하기 때문에 언제 어떠한 경로로 악성코드가 침투하고 동작했는지 파악하는 것은 쉽지 않다. 또한 내부 직원이 개입되어 있다면 피해를 방지하는 것이 더욱 어려워진다. 국내도 내부 직원을 통하여 APT 공격 피해사례는 여러 차례 보도된 바 있으며, 문제가 발생했음에도 보안을 방치하는 기업은 여전히

존재한다. 대표적인 APT 공격의 내부자 피해사례로는 2009년 7월 7일에 발생한 디도스 사태와 3월 4일에 발생한 디도스 사태, 2011년에 일어난 '은행 전산망 마비 사태'가 있다. APT 공격의 또 다른 형태인 랜섬웨어(Wanna Cry)가 크게 이슈화되기도 했다.

(그림 2) Wanna Cry 랜섬웨어

해당 랜섬웨어는 데이터를 탈취하려는 목적보다 데이터를 빌미로 금전적인 목적을 요구하는 악성코드지만, APT 형태의 공격으로 특정 기업을 목표로 하여 악성코드를 배포하고 감염된 대상자가 기업인 경우, 업무가 마비되는 정도의 치명적인 문제가 발생하기도 하였다.

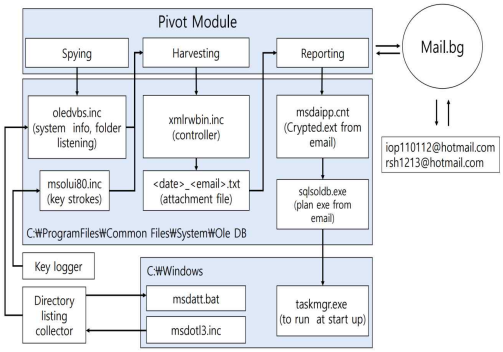
<표 1> APT 공격과 기타 사이버 공격의 차이점

	APT 공격	기타 사이버 공격
대상	대상과 표적 특정	불특정 다수
목표	정부기관, 공공기관	대부분 금전적인 목적
범위	조직화 된 공격	조직화 되어있지 않음
빈도	지속적	일시적
탐지	비교적 어려움	비교적 쉬움

국내에서 APT 공격 악성코드 유형으로 랜섬웨어는 개인이 감염되는 것보다 기업이 감염되었을 때, 중요한 문서 데이터가 암호화되어 사용 불가능해지거나 사용자에게 제공되는 서비스 전체에 피해가 발생하게 되면서 직접적으로 감염되지 않았던 사용자도 피해를 받는다. [2][3]

3. 한국어 기반 APT 공격그룹

3.1 Kimsuky Group



(그림 4) 2013년 Kimsuky 그룹의 APT 공격

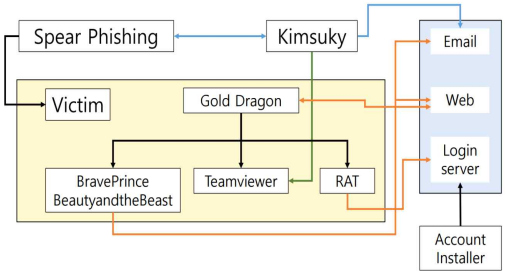
2013년에 처음 발견되었으며, 가장 대표적인 공격사례로는 2014년 한국 수자력 원전 도면 유출사건의 배후로 지목된 바 있다. 주로 국가나 정부의 외교 관련 인텔리전스를 이용하여 대부분 외교 관련 기자나 탈북자들을 대상으로 공격을 진행하고 있다. 최근에는 가상화폐를 이용하여 공격을 시도하는 정황도 확인되었으며, 대한민국을 대상으로 주로 공격을 시도하고 있으므로 한글(hwp)나 워드프로세스의 취약점을 주로 사용하고 있으며 이를 통해 1,400명의 이메일을 탈취한 바 있다. [3][13]

(그림 4)와 같이 Kimsuky 그룹의 주요 특징은 모듈들을 크게 3가지로 나눈다. Spying 모듈과 Harvesting 모듈과 Reporting 모듈로 나뉘는데 이 3가지의 모듈들이 서로 유기적으로 동작한다. 이러한 구조는 현재까지도 사용하고 있으며 (그림 5)와 같이 2013년 발견 당시와 2018년에 평창동계올림픽 이슈를 목적으로 사용된 공격 프로세스의 구조 또한 매우 유사하다.[3][4]

3.1.1 Kimsuky Group의 공격 특징

(그림 4)와 (그림 5)에서 확인할 수 있듯이 Kimsuky 그룹은 여러 가지 도구들을 활용하고 있으며, 공격의 구조는 크게 변화되지 않고 있다. 대표적으로 변조된 웹서버를 활용하여 명령을 제어하기 위한 서버인 C&C(Command & Control)나 C2 서버로 활

용하여 유로 호스팅 서비스를 사용하여 결제 수단을 가상화폐를 사용해 등록자의 익명성을 보장하고 있기 때문으로 알려졌다.



(그림 5) Gold Dragon APT 공격 프로세스

Kimsuky 그룹은 이 중에서도 <표 1>, <표 2>와 같이 한국의 이메일 서비스를 자신들의 C&C 서버로 활용하여 사용하는 것으로 밝혀졌다. 따라서 Kimsuky 그룹은 국내의 이메일 서비스에 대해서 능숙하게 활용할 수 있는 그룹이다.

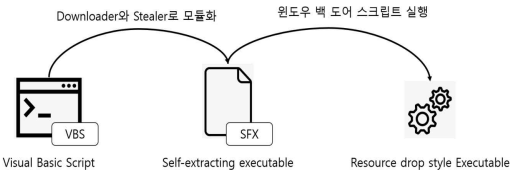
<표 1> 공격자 이메일 정보

이메일 주소	비밀번호
k1-tome@daum.net	c$#*****fzF (특정 문자열***처리)

<표 2> 스레드 별 프로토콜 사용유형

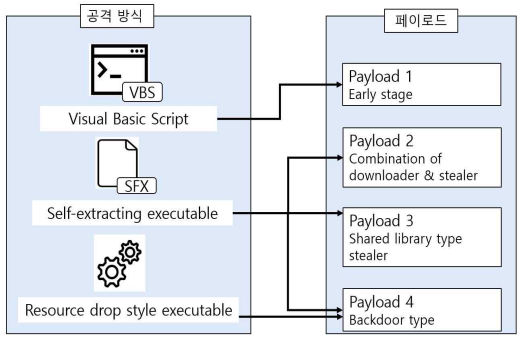
이메일 주소	관련 스레드
smtps://smtp.daum.[.]net:465	ping 스레드
imaps://imap.daum[.]net:993	command 스레드

Kimsuky 그룹의 공격의 원리와 절차를 살펴보면 해당 호스트를 감염시키기 위해서 처음에는 감염시키기 위한 목적으로 Visual Basic Script를 활용하였다. 또한. SFX(Self-Extracting Executable)이라는 실행파일을 사용하기도 하며, 본래의 윈도우 실행파일이지만 추가적으로 내장된 악성코드들을 사용하여 새로운 악성코드들을 추가 생성하는 방법도 활용하였다. 해당 공격의 특이점은 Visual Basic Script를 활용과 SFX파일의 활용, 윈도우 실행파일을 활용한 방법을 시도하였는데 여기서 (그림 6)과 같이 점점 모듈화가 되어 발전된 형태라고 할 수 있다. [7]



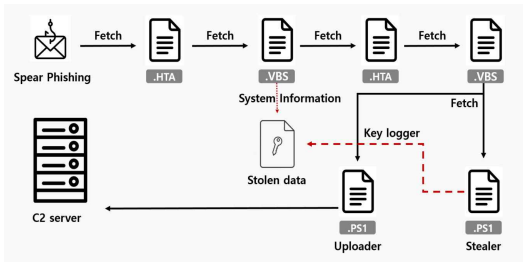
(그림 6) Kimsuky 그룹의 공격 절차 및 원리

(그림 6)과 같이 공격이 진행되는데 최종적으로 감염된 호스트에서 확인할 수 있는 Payload는 크게 4가지가 있으며, (그림 7)과 같이 악성행위를 하는 Early stage와 악성코드를 다운로드하고 내부의 정보를 탈취하기 위한 downloader와 stealer 및 공유된 라이브러리를 사용하여 stealer에 필요한 모듈을 가져와서 유기적으로 활용하고 마지막으로 백도어에서 실행하기 위한 Payload로 구성되어 있다.



(그림 7) Kimsuky 그룹의 APT 공격에서 확인할 수 있는 공격 방식과 4가지 Payload

이 외에도 Kimsuky 그룹은 (그림 8)과 같이 2019년 이후로 스피어피싱도 자주 활용하고 있다.

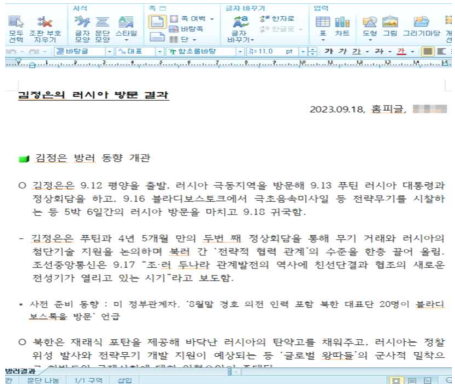


(그림 8) 스피어피싱을 활용한 공격

처음에 HTA (HTML Applicaiton)파일이 생성되는데, 사용자가 HTML 파일을 사용하기위한 포맷이다. HTA 파일을 실행하게 되면 추가적으로 악성코드를 받아오게 되며, 해당 악성코드는 Visual Basic Script 파일로 .vbs 확장자를 가진다. .vbs 파일이 실행되면 시스템 내부의 기본적인 정보를 특정파일로 저장하게 된다. 이후, 다른 HTA 파일을 받아오게 되고 받아온 HTA 파일은 또 다른 .vbs 파일을 실행시키면서 동작한다. 최종적으로 실행을 마치면 2개의 윈도우 Powershell 파일이 생성되는데, 생성된 2개의 Powershell 파일은 공격자의 서버에 바로 등록되지 않고 필요한 정보인지 검증 후 공격자의 서버에 등록되게 된다. 불필요한 탐지를 줄이고 발견 가능성을 감소하기 위한 목적으로 판단할 수 있다. 일반적으로 윈도우 환경의 실행파일은 이미 연구된 사례가 많아 식별하는 것은 상대적으로 식별하기 쉬운 편에 속하고 있으나 (그림 8)에서 진행된 공격 과정에서는 윈도우 실행파일이 아닌 스크립트 형식의 문서 형태로 이루어진 파일들이기 때문에 탐지하는 과정에 많은 어려움이 따른다. 따라서 공격자는 이러한 과정에서 이미 취약한 부분을 숙지한 상태에서 APT 공격을 수행하였다는 사실을 확인할 수 있다. [8][9]

3.2 Dark Hotel Group

2014년에 처음 발견되었으며, 외교와 관련된 고위 담당자들 및 해외에서 거주하고 있는 북한의 외교 담당자들을 대상으로 공격을 수행하였다.


김정은식 러시아 방문 결과

2023.09.18. 홈피글,

김정은 방러 동향 개관

○ 김정은은 9.12 평양을 출발, 러시아 극동지역을 방문해 9.13 푸틴 러시아 대통령과 정상회담을 하고, 9.16 블라디보스토크에서 극초음속미사일 등 전략무기를 시찰하는 등 5박 6일간의 러시아 방문을 마치고 9.18 귀국함.

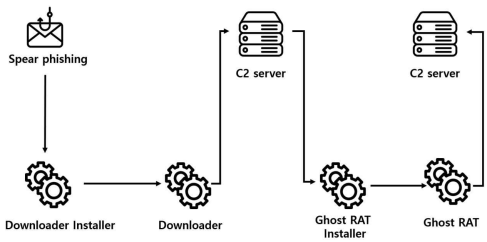
- 김정은은 푸틴과 4년 5개월 만의 두번 째 정상회담을 통해 무기 거래와 러시아의 첨단기술 지원을 논의하며 복러 간 '전략적 협력 관계'의 수준을 한층 끌어 올림. 조선중앙통신은 9.17 '조·러 두나라 관계발전의 역사에 친선단결과 협조의 새로운 전성기가 열리고 있는 시기'라고 보도함.

• 사전 준비 동향 : 미 정부관계자, '8월말 경호 의전 인력 포함 북한 대표단 20명이 블라디보스톡을 방문' 언급

○ 북한은 재래식 포탄을 제공해 바닥난 러시아의 탄약고를 채워주고, 러시아는 정찰위성 발사와 전략무기 개발 지원이 예상되는 등 '글로벌 왕따들'의 군사적 밀착으

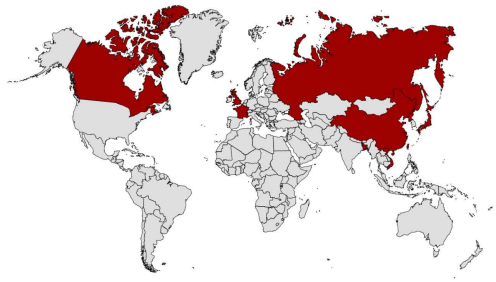
(그림 9) 외교 관련 악성 문서파일

주로 해외의 호텔 무선 네트워크에 침투하여 객실 번호를 기준으로 특정한 호텔 투숙객을 대상으로 지정하여 명명되었다.



(그림 10) dark hotel 그룹의 공격 프로세스

감염의 절차는 (그림 10)과 같이 메일을 확인하고 문서파일을 실행하게 되면 내부적으로 다운로더가 설치된다. 이후 다운로더가 다운받은 데이터를 공격자의 서버와 통신하여 공격자의 서버에서 정보의 가치와 중요도를 파악하여 필요한 정보로 판단되면 원격제어 악성코드인 Ghost RAT를 설치 및 실행하여 필요한 정보를 탈취할 수 있게 된다. 해당 악성코드는 오픈소스로 공개되었지만, 자신들의 공격할 대상의 특성에 맞게 제작한 뒤 공격을 수행하였다. (그림 11)과 같이 전 세계적으로 APT 공격을 수행하였고, 주로 외교 관련 인텔리전스나 해외에서 거주 중인 북한사람들 및 인권 단체, 북한과 연결된 기업들을 대상으로 수행하였다. [10]



(그림 11) Dark Hotel 그룹의 공격 대상 국가

3.2.1 Dark Hotel Group의 공격 특징

Dark Hotel 그룹의 공격 중 가장 큰 특징은 분석가들이 공격의 배후를 쉽게 특정하지 못하도록 가짜

플래그(False Flag)를 사용한다는 점이다. (그림 12)와 같이 Ghost RAT를 분석해보면 사용자를 나타내는 값의 마지막에 'kp'라는 문자열을 확인할 수 있다. 'kp' 는 전 세계의 나라와 그 부속된 영토와 구성된 단위의 명칭에 고유한 부호가 부여된 국제 표준을 뜻하는 ISO 3166의 표준형식 중 두 자리 국가코드를 나타내고 있는 ISO 3166 alpha-2 표준에서 북한에게 부여된 국가코드이다.

```
strcpy(Mozilla_5.0_(Ma,"Mozilla/5.0 (Macintosh; U; Intel Mac OS X OLEZA; kp)");
strcpy(&Version_5.1, "Version/5.1");
```

(그림 12) Ghost RAT에서 확인된 kp 문자열

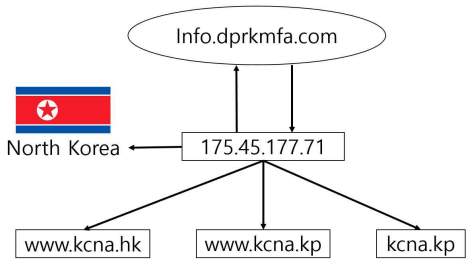
또한 사용된 악성 문서 중에서 한가지는 (그림 13)과 같이 특정 어플리케이션을 설치하기 위한 설치 매뉴얼의 내용의 문서가 사용되었는데 해당 악성 문서를 분석해본 결과 북한에서 주로 사용하는 글꼴인 '천리마체'를 사용하였고, (그림 14)에서 보는 바와 같이 (그림 13)에서 사용한 글꼴과 (그림 14)의 글꼴이 동일한 것을 알 수 있다. [7][8]

(그림 13) 천리마체를 사용하는 악성 문서

다람쥐 헌 쳇바퀴에 타고파.
1234567890

(그림 14) 북한에서 사용하는 천리마체

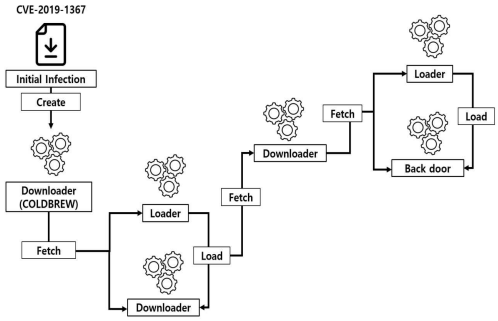
해당 악성 문서를 실행하게 되면 Ghost RAT 가 실행되고 공격자의 서버와 통신하는 과정에서 백도어에 해당 서버의 ip 주소가 175.45.177.41로 설정되어 있었으며 해당 ip는 조선중앙텔레비전의 웹서버 ip 주소를 의미한다. 해외에서도 잘 알려진 북한의 기관의 ip 주소를 서버로 사용한다면 분석을 하는 분석가의 입장에서 공격자를 특정하기 쉬울 것이다. 따라서 해당 웹서버의 ip 주소를 사용했다는 것은 공격을 수행하기 위해서가 아닌 Ghost RAT 가 C&C 서버와 통신이 잘 되는지의 여부와 APT 공격의 배후로 적발되지 않기 위한 가짜 플래그로 사용했다는 것을 알 수 있다. [9]



(그림 15) False Flag로 사용된 C&C 서버

3.2.2 Cold Brew APT 공격

해당 공격은 (그림 16)과 같이 cve-2019-1367 취약점을 사용하여 메모리의 처리하는 방식에 있어 원격코드를 실행하는 취약점을 활용하였다. [3][4][9]



(그림 16) Cold Brew APT 공격 프로세스

(그림 17) Cold Brew 공격에서 사용된 파일

먼저 공격 대상자가 (그림 17)과 같은 파일을 실행하게 되면 다운로더가 <표 3>에서 표시한 경로에 생성된다. 이때 공격에 사용된 다운로더 이름이 '콜드브루(Cold Brew)'였기 때문에 Cold Brew 공격이라고 명명되었다.

<표 3> 다운로더 생성 경로

downloader 생성 경로
Y:₩src₩NVCtrl₩Install₩ColdBrew64₩x64₩Relaese₩COLDBREW64.pdb

이후 다운로더(COLDBREW64.pdb)가 로더를 불러오게 되고 다운받은 로더가 이전과는 다른 다운로더를 다시 불러오게 되고 불러온 다운로더는 다시 새로운 형태의 다운로드를 불러오게 된다. 가장 최근에 생성된 새로운 형태의 다운로더는 다시 로더를 생성하여 백도어 프로그램을 다운로드하여 백도어에서 실행되게 하였다. 따라서 악성코드가 또 다른 악성코드를 받아오는 과정도 여러 단계로 체계화하여 공격 탐지율을 회피하려는 것을 확인할 수 있다. [4][9][10]

3.3 Blue Noroff Group

해당 그룹은 2017년에 처음 발견되었으며, 발견 당시에 사용했던 파일명이 Noroff 였던 점과 해당 그룹의 특징 중의 하나인 윈도우 Powershell을 잘 활용했다는 점을 활용하여 현재의 Blue Noroff 그룹이라고 명명되었다. 해당 그룹은 주로 금전적인 이득을 목적으로 금융기관 및 가상화폐 거래소를 대상으로 공격을 수행하였고 공격 대상이 된 국가는 (그림 18)과 같다. [10][13]

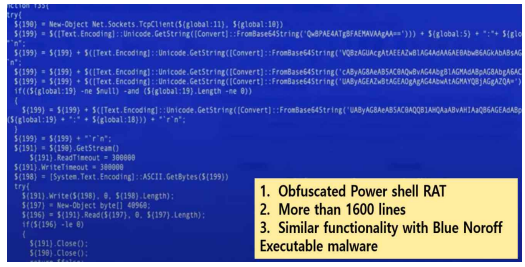
(그림 18) Blue Noroff 그룹의 공격 대상 국가

3.3.1 Blue Noroff Group의 공격 특징

해당 그룹은 가상화폐 거래소를 대상으로 공격을 진행하였는데, 특정 애플리케이션을 제작하여 공격을 수행하였다. (그림 19)를 보면 공격에 사용된 가상화폐 솔루션을 제작한 뒤, 대상자에게 광고 및 홍보를 목적으로 전송한 다음 공격의 대상자가 해당 솔루션을 구입하거나 사용하게 되면 감염되는 형식으로 공격이 수행되었다.

(그림 19) APT 공격에 사용된 가상화폐 솔루션

공격에 사용된 가상화폐 솔루션 프로그램은 실제로 솔루션이 동작하도록 설계되었으며, 공격자로 하여금 대상자의 운영체제에 제한을 받지 않기 위하여 여러 운영체제의 제한을 받지 않는 멀티 플랫폼 형태로 제작되었다. 그리고 해당 솔루션을 구입하여 특정한 사용자의 정보를 입력하면 해당 정보를 받아 악성행위가 진행되었다. 해당 솔루션을 실행하게 되면 윈도우 Powershell 파일이 실행되는데 (그림 20)과 같다.



(그림 20) 솔루션 동작 후 Powershell 파일 실행

솔루션이 실행되면 Powershell 파일이 다운로드되고 해당 Powershell 파일은 난독화가 되어있었으며, 약 1,600줄의 코드를 사용하였다. 그리고 기존의 Blue Noroff 그룹이 윈도우에서 사용하던 기능들을 전부 윈도우 Powershell로 구현하였다. 이를 바탕으로 해당 그룹은 가상화폐 거래소의 솔루션을 제공하는 형태로 공격을 수행하였고, Powershell을 적극적

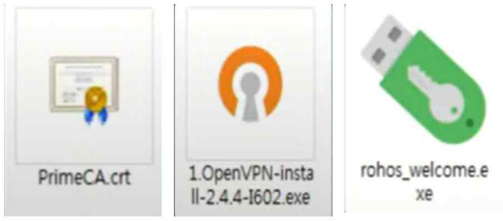
으로 활용하였다는 것을 확인할 수 있다. 또한 가상화폐 거래 및 국내외 송금 시스템에 대해서 숙지하고 있으며, Powershell을 활용한 것으로 보아 프로그램 및 소프트웨어의 설계 및 제작 능력도 보유하고 있을 것으로 파악할 수 있다. [3-5][7-10][13]

3.4 Lazarus Group

'라자루스(Lazarus)' 그룹은 2014년 한 보안 회사인 '노베타(Novetta)'에 의해서 처음 발견되었으며, 공격 대상은 금전적인 이득의 목적과 사이버 첩보활동의 목적으로 크게 2가지로 분류된다. 금전적인 이득을 목적으로 가상화폐 거래소를 공격하였는데 <표 4>와 같다. [7-9]

<표 4> 라자루스 그룹의 공격에 사용된 파일

공격 대상	위장된 어플	파일명
홍콩	Wechat messenger	wechat.exe
홍콩	OpenVPN client	1.OpenVPN-install-2.4.4-1602.exe
대한민국	Rohos Logon Key	rohos_welcome.exe

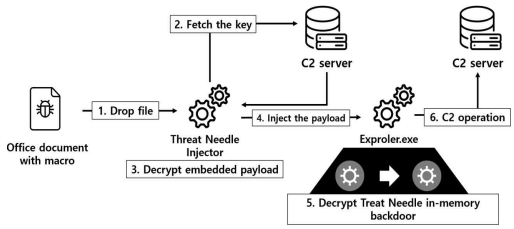


(그림 21) 위장된 어플리케이션

(그림 21)을 보면 홍콩의 경우 특정 메신저 어플을 사용하여 공격을 수행하였고 대한민국의 경우 메신저 어플은 아니지만 실제로 금융권에서 사용자를 인증하기 위한 인증서 프로그램으로 위장하여 해당 프로그램을 실행시키면 공격이 수행되는 형태로 공격을 수행하였다. (그림 21)에서 확인할 수 있는 프로그램들은 해당 거래소에서 실제로 사용중인 어플리케이션이었으며, 라자루스 그룹이 이러한 점을 사전에 숙지하여 대상에 맞게 APT 공격을 수행했다는 사실을 확인할 수 있다. [4-9]

3.4.1 Lazarus Group의 공격 특징

라자루스 그룹은 ThreatNeedle이라는 이름의 악성코드를 사용한 방식으로 공격을 수행하였는데 공격과정은 (그림 22)와 같으며, 공격과정에서 가장 큰 특징은 최종적으로 생성된 악성코드는 디스크 상에서 생성되지 않고 메모리에서만 동작하기 때문에 여러 백신 프로그램에서도 탐지가 어려우며 분석가의 입장에서도 많은 어려운 점이 존재한다. [10]



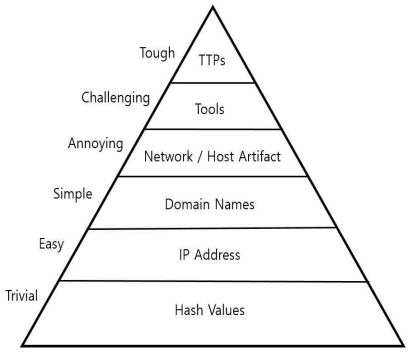
(그림 22) Threat Needle APT 공격 프로세스

공격을 수행할 때 첫 번째로 악성 오피스 문서를 제작을 하는데 주로 공격 대상이되는 기업의 인사 담당자에게 입사 지원서나 이력서의 내용으로 위장된 오피스 문서를 전송한다. 이후 공격 대상이 되는 기업의 인사 담당자가 해당 파일을 실행하게 되면 Threat Needle injector라는 악성코드가 생성된다. 이러한 과정으로 생성된 injector 악성코드는 공격자의 서비인 C&C 서버로 감염된 대상의 정보를 보낸다. 또한 감염된 대상의 정보가치가 높다고 판단되면 특정한 키 값을 C&C 서버로부터 수신하고 수신된 키의 값을 가지고 실제로 사용되는 악성코드를 사용해서 정상적인 파일(explorer.exe)로 위장한다. 위장된 exproler.exe는 다시 내부적으로 자신의 코드를 재실행하여 메모리에서 백도어 형태로 동작하는 Threat Needle이라는 이름의 악성코드를 생성 및 실행한다. 이러한 프로세스를 활용하여 윈도우 뿐만 아니라 (그림 21)과 같이 모바일 어플리케이션으로도 변조하여 공격을 수행하였다. [4][5][13]

4. 정확한 인텔리전스 사용

4.1 APT 공격 행위 기반 분석의 필요성

보안 담당자의 입장에서 대응하기 위한 난이도를 나타내보면 (그림 23)과 같다. 상위로 올라갈수록 대응 방법의 난이도가 높은 것을 나타낸다. [11]

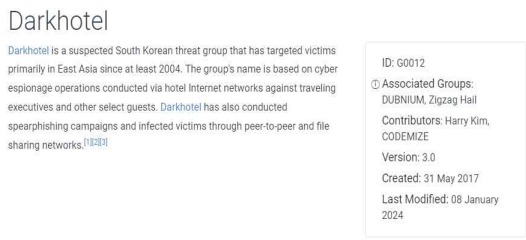


(그림 23) 공격 대응 난이도 도식화

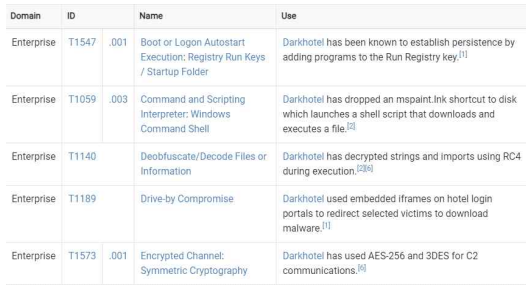
보안 담당자는 공격자들의 Tool이나 공격자의 공격 행위가 각 APT 그룹들의 목적이 다르기 때문에 이러한 공격 행위들을 전부 이해하고 대응하기는 쉽지 않다. 따라서 이러한 부분들을 공격자의 입장에서 생각한다면 해시값이나 ip 및 도메인들을 변경하는 것은 어렵지 않을 것이다. [19] 하지만 보안 담당자가 네트워크 대역이나 공격자의 공격 대상이되는 호스트의 정보나 흔적을 변경한다면 공격자는 악성코드의 동작 방식을 변경해야하기 때문에 제약이 발생할 수 있을 가능성이 존재한다. 또한 보안 담당자가 Tool을 이용해서 대응을 한다면 공격자는 해당 Tool에 대한 정보들을 숙지해야 할 것이고 보안 담당자가 공격 행위에 대한 대응방법으로 사용하는 Tool에 맞게 다시 악성코드를 설계해야 할 것이다. 마지막으로 공격 행위를 기반으로 대응한다면 공격자는 APT 공격 프로세스를 재설계 해야하는 상황이 발생하여 공격의 확률을 줄이고 위협의 가능성을 감소시킬 수 있다. [15-18]

4.2 MITRE ATT&CK의 활용 방안

MITRE ATT&CK은 실제 사이버 공격 사례를 식별한 이후 공격자가 사용했던 공격의 방법과 기술들의 관점에서 분석하여 공격 기법 및 기술적인 정보들을 분류하여 목록화가 되어있는 표준적인 데이터이며 실제 공격자의 공격 전술과 공격 기술 및 다양한 공격 정보들을 확인하고 이를 활용하여 대응 방안을 모색할 수 있다. [13-18]

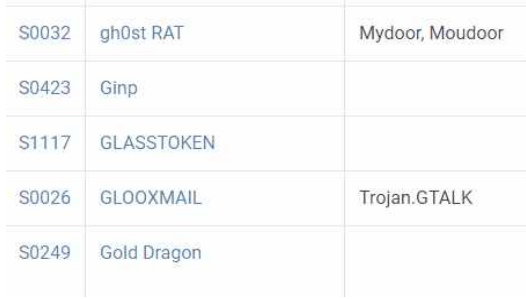


(그림 24) Dark Hotel APT 그룹의 정보



Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Darkhotel has been known to establish persistence by adding programs to the Run Registry key.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Darkhotel has dropped an mspaint.lnk shortcut to disk which launches a shell script that downloads and executes a file.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Darkhotel has decrypted strings and imports using RC4 during execution.[2][6]
Enterprise	T1189		Drive-by Compromise	Darkhotel used embedded iframes on hotel login portals to redirect selected victims to download malware.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Darkhotel has used AES-256 and 3DES for C2 communications.[6]

(그림 25) Dark Hotel의 APT 공격에 사용된 기술정보



S0032	gh0st RAT	Mydoor, Moudoor
S0423	Ginp	
S1117	GLASSTOKEN	
S0026	GLOOXMAIL	Trojan.GTALK
S0249	Gold Dragon	

(그림 26) Kimsuky와 Dark Hotel 그룹에서 사용되었던 도구(Ghost RAT, Gold Dragon)의 정보

5. 결 론

APT 공격의 배후를 특정하여 추가적인 예측을 하기 위한 용도로 사용하는 것은 유용한 방법이지만 APT 공격을 수행한 공격의 주체와 공격의 대상 및 공격 방법과 절차를 밝혀내는 것이 더욱 중요한 과제라고 할 수 있을 것이다. 이전의 다크호텔 사례를 통해서 false flag를 잘 사용하기 때문에 이러한 기술적인 데이터가 없으면 함정에 빠질 수 있다는 점을 보아 공격의 주체를 특정하고 파악하기 위해서는 기본적으로 충분한 기술적인 요소들의 이해도와 올바른 인텔리전스 사용이 필요하다. 따라서 이러한 APT 공격의 위협을 줄이기 위해서는 기업과 기관에서 현재 중요한 정보의 자산이 무엇인지와 취약한 부분이 어디에 있는지를 특정하고 우선순위를 두어 파악하는 것과 꾸준한 보안 점검을 통해서 관리하는 것이 필요하다. 그리고 기관과 기업을 대상으로 공격하는 APT 그룹들은 어떠한 그룹들인지 사전에 MITRE ATT&CK를 통해 사전에 위협 요소들을 파악한다면 올바른 인텔리전스를 사용하여 사전에 공격 요소들을 파악하고 APT 공격 위협을 최소화할 수 있을 것이다.

참고문헌

[1] M. Khosravi and B. T. Ladani, "Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection", IEEE, Vol. 8, pp.162642-162656, 2020.

[2] K. G. Lee, J. H. Lee and K. B. Yim "Classification and Analysis of Malicious Code Detection Techniques Based on the APT Attack", Applied Science, Vol. 13, No. 5, pp.1-32. 2023.

[3] 최창희, 신찬호, 신성욱 "MITRE ATT&CK 모델을 이용한 사이버 공격 그룹 분류", 한국 인터넷정보학회 논문지, 제23권, 제6호, pp. 1-13, 2022.

[4] Y. H. Kim, W. H. Park, "A study on cyber threat prediction based on intrusion detection event for APT attack detection", Multimedia Tools and Applications, Vol. 71, pp. 685-698, 2014.

[5] T. Jabar, M. M. Singh, "Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework", Sensors, Vol. 22, No. 13, pp. 1-38, 2022.

[6] A. A. Al-Kadhimi, M. M. Singh and M. N. Akmal Khalid, "A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques", Vol. 13, No. 14, pp. 1-47, 2023.

[7] S. Singh, P. K. Sharma, S. Y. Moon, D. S, Moon, J. H. Park, "A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions", J Supercomputing, Vol. 75, pp. 4543-4574, 2019.

[8] Marc R. DeVore and Sangho Lee, "APT(ADVANCED PERSISTENT THREAT)S AND INFLUENCE: CYBER WEAPONS AND THE CHANGING CALCULUS OF CONFLICT", East Asian Affairs, Vol. 31, No. 1, pp. 39-64, 2017.

[9] L. Burita, D. T. Le, "Cyber Security and APT Groups", IEEE, pp. 1-7, 2021.

[10] J. H. Lee, J. H. Jeon, C. Y. Lee, J. B. Lee, J. B. Cho, K. H. Lee, "A Study on Efficient Log Visualization Using D3 Component against APT: How to Visualize Security Logs Efficiently", IEEE, pp.1-6, 2016.

[11] Y. S. Shin, K. M. Kim, J. J. Lee, K. H. Lee, "ART:Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity" IEEE, pp. 15-20, 2021

[12] R C. Veena, S H. Brahmananda, "A Significant Detection of APT using MD5 Hash Signature and Machine Learning Approach", International Journal of Engineering Trends and Technology, Vol. 70, No. 4, pp. 95-106, 2022.

[13] Y. K. Kim, J. J. Lee, M. H. Go, K. H. Lee,"Analysis of the Asymmetrical Relationships between State Actors and APT Threat Groups" IEEE, pp. 695-700, 2020.

[14] Y. Mei, W. Han, S. Li, X. Wu, K. Lin, Y. Qi,

"A Review of Attribution Technical for APT Attacks", IEEE, pp. 512-518, 2022.

[15] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping", IEEE, pp. 106-112, 2020.

[16] A. Georgiadou, S. Mouzakitis and D. Askounis, "Accesing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework", Sensors, Vol. 21, No. 9, pp. 1-14, 2021.

[17] N. Naik, P. Jenkins, P. Grace, and J. Song, "Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain MITRE ATT&CK Framework and Diamond Model" IEEE, pp. 1-7, 2022.

[18] Y. H. Jo, O. G. Choi, J. W. You, Y. K. Cha and D. H. Lee, "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework" Sensors, Vol. 22, No. 5, pp. 1-18, 2022.

〔저자소개〕

이 정 훈 (Jung-Hun Lee)

2019년 03월~현재 인제대학교 재학
email : newpaper841@gmail.com

최 윤 성 (Youn-sung Choi)
2006년 2월 성균관대학교 정보통신공학부 학사
2007년 8월 성균관대학교 전자전기컴퓨터공학부 석사
2015년 8월 성균관대학교 전자전기컴퓨터공학부 박사
2016년 3월 ~ 2020년 2월 호원대학교 사이버보안학과 조교수
2020년 3월 ~ 현재 인제대학교 AI융합대학 AI소프트웨어학부 조교수
email : cys2020@inje.ac.kr