국내·외 리서쳐 공격에 사용된 라자루스 그룹의 최신 0day 취약점 및 관련 악성코드 분석

S2W BVT x ENKI

K-CTI 2021

2021 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

2021. 3. 9

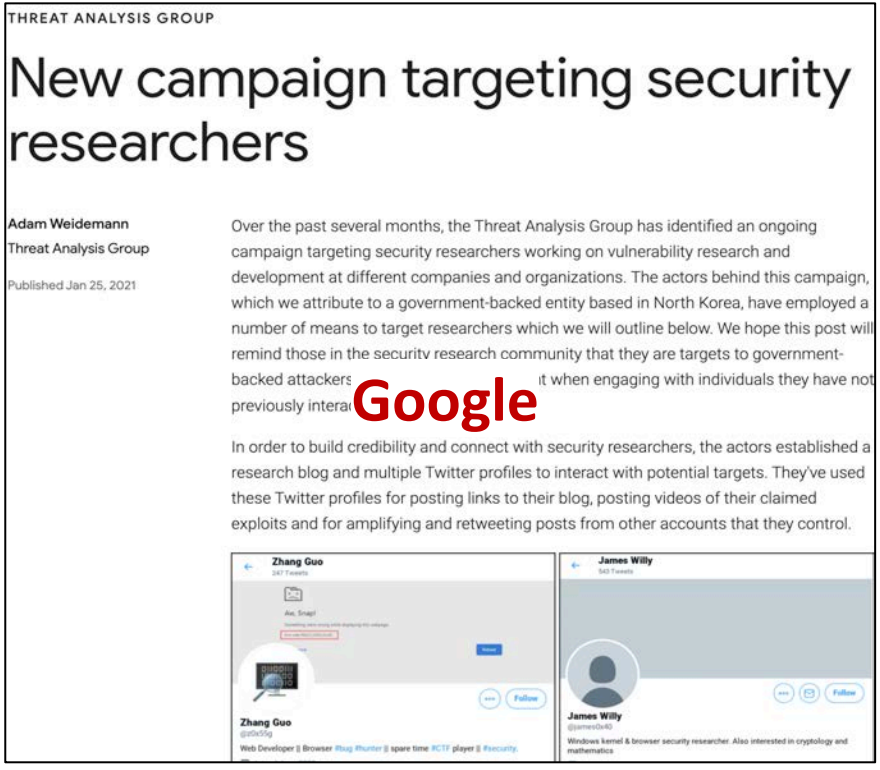
ENKI 박세한 대표 & S2W LAB 류소준 책임

소개

- 사건 개요
- 공격 시도
- 취약점 분석
- 악성코드 분석
- 과거 사례 비교
- 결론

사건 개요

- 지난 1월 보안 연구자 대상 해킹 공격 관련 보고서 공개
- 공격의 배후로 북한의 해킹 그룹 라자루스를 지목 됨



THREAT ANALYSIS GROUP

New campaign targeting security researchers

Adam Weidemann
Threat Analysis Group

Published Jan 25, 2021

Over the past several months, the Threat Analysis Group has identified an ongoing campaign targeting security researchers working on vulnerability research and development at different companies and organizations. The actors behind this campaign, which we attribute to a government-backed entity based in North Korea, have employed a number of means to target researchers which we will outline below. We hope this post will remind those in the security research community that they are targets to government-backed attackers [illegible] when engaging with individuals they have not previously interac[illegible]

Google

In order to build credibility and connect with security researchers, the actors established a research blog and multiple Twitter profiles to interact with potential targets. They've used these Twitter profiles for posting links to their blog, posting videos of their claimed exploits and for amplifying and retweeting posts from other accounts that they control.

January 28, 2021

ZINC attacks against security researchers

Microsoft Threat Intelligence Center (MSTIC)
Microsoft 365 Defender Threat Intelligence Team

Share

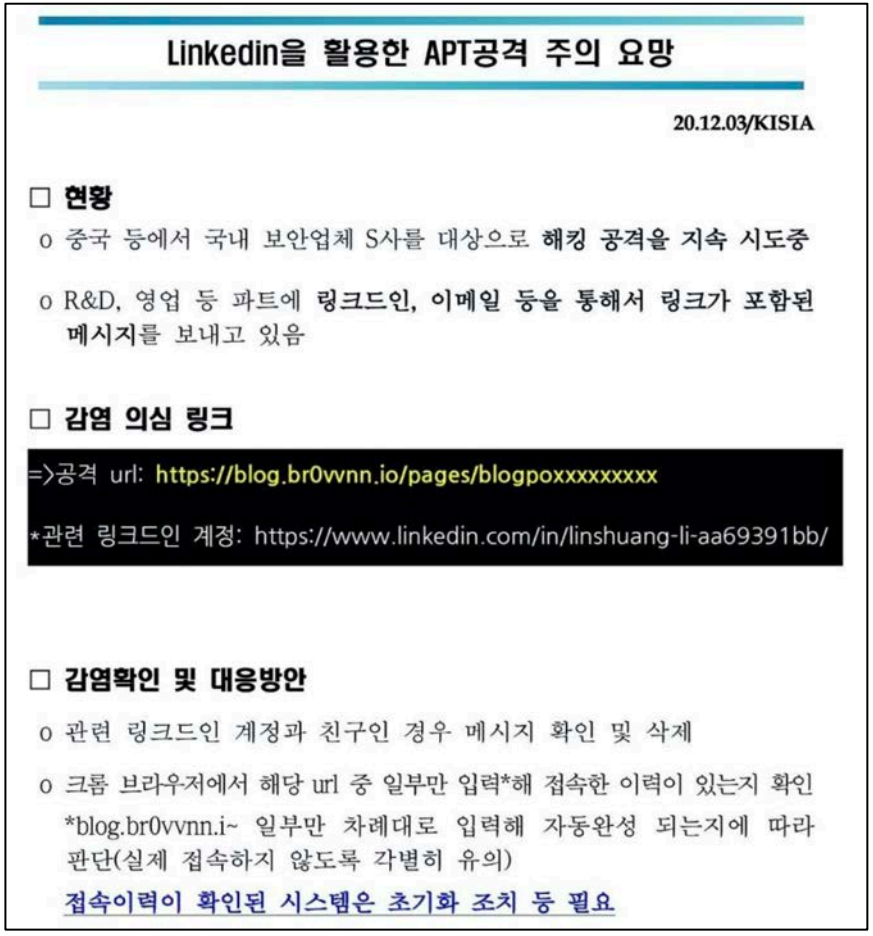
Microsoft

In recent months, Microsoft has detected cyberattacks targeting security researchers by an actor we track as ZINC. The campaign originally came to our attention after Microsoft Defender for Endpoint detected an attack in progress. Observed targeting includes pen testers, private offensive security researchers, and employees at security and tech companies. Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to ZINC, a DPRK-affiliated and state-sponsored group, based on observed tradecraft, infrastructure, malware patterns, and account affiliations.

This ongoing campaign was reported by Google's Threat Analysis Group (TAG) earlier this week, capturing the browser-facing impact of this attack. By sharing additional details of the attack, we hope to raise awareness in the cybersecurity community about additional techniques used in this campaign and serve as a reminder to security professionals that they are high-value targets for attackers.

사건 개요

- 위협 정보가 공개되기 이전 지난 해 11월, 국내를 대상으로 활발한 공격이 이뤄짐
- 알려진 주요 공격 대상은 국내 보안업체 S사, T사, ENKI 등이 있음
- 공격 대상은 오펜시브 시큐리티 보안 회사로 취약점 연구를 진행하는 공통점이 존재
- 링크드인, 트위터 등 SNS를 활용해 타겟과 1:1 접촉을 시도
- 공격 파급력이 큰 브라우저(Chrome, IE)의 0day 취약점을 활용한 고도의 공격 기술 사용



Linkedin을 활용한 APT공격 주의 요망

20.12.03/KISIA

□ 현황

o 중국 등에서 국내 보안업체 S사를 대상으로 해킹 공격을 지속 시도중

o R&D, 영업 등 파트에 링크드인, 이메일 등을 통해서 링크가 포함된 메시지를 보내고 있음

□ 감염 의심 링크

=>공격 url: https://blog.br0vvnn.io/pages/blogpoxxxxxxxxx

*관련 링크드인 계정: https://www.linkedin.com/in/linshuang-li-aa69391bb/

□ 감염확인 및 대응방안

o 관련 링크드인 계정과 친구인 경우 메시지 확인 및 삭제

o 크롬 브라우저에서 해당 url 중 일부만 입력*해 접속한 이력이 있는지 확인

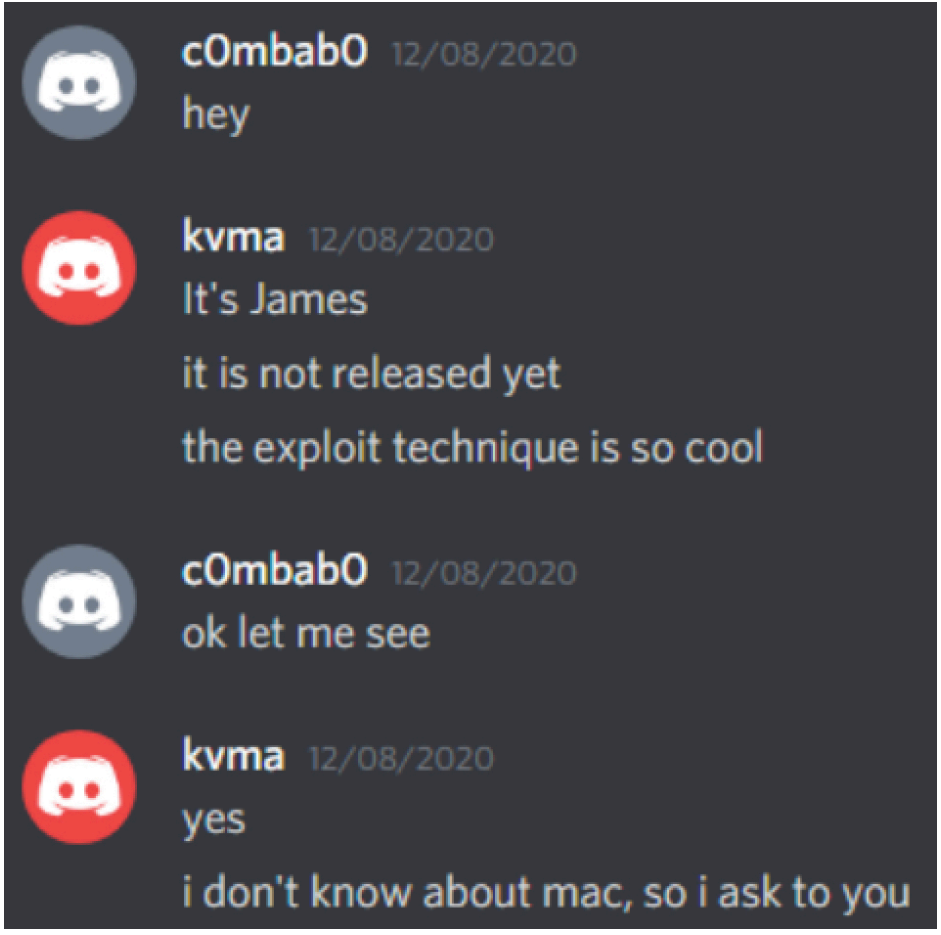
*blog.br0vvnn.i~ 일부만 차례대로 입력해 자동완성 되는지에 따라 판단(실제 접속하지 않도록 각별히 유의)

접속이력이 확인된 시스템은 초기화 조치 등 필요

공격 시도

- 공격자는 보안 취약점 블로그를 운영하며 0day 연구자로 가장한 SNS 계정을 활용
- 트위터를 이용해 초기 접근 후 텔레그램, 디스코드 등으로 대화 채널을 변경 시도 함
- 취약점 익스플로잇 코드 개발에 협업을 요청하며 대상 별로 준비된 공격 코드를 전달

* 윈도우 취약점 연구 경험자
  Visual Studio 프로젝트 전달
* 브라우저 취약점 연구 경험자
  크롬 브라우저 기술 문서 (MHT 파일)
* 대화 중 공격자 소유의 블로그 링크를 통해 크롬 브라우저 0day 공격 시도



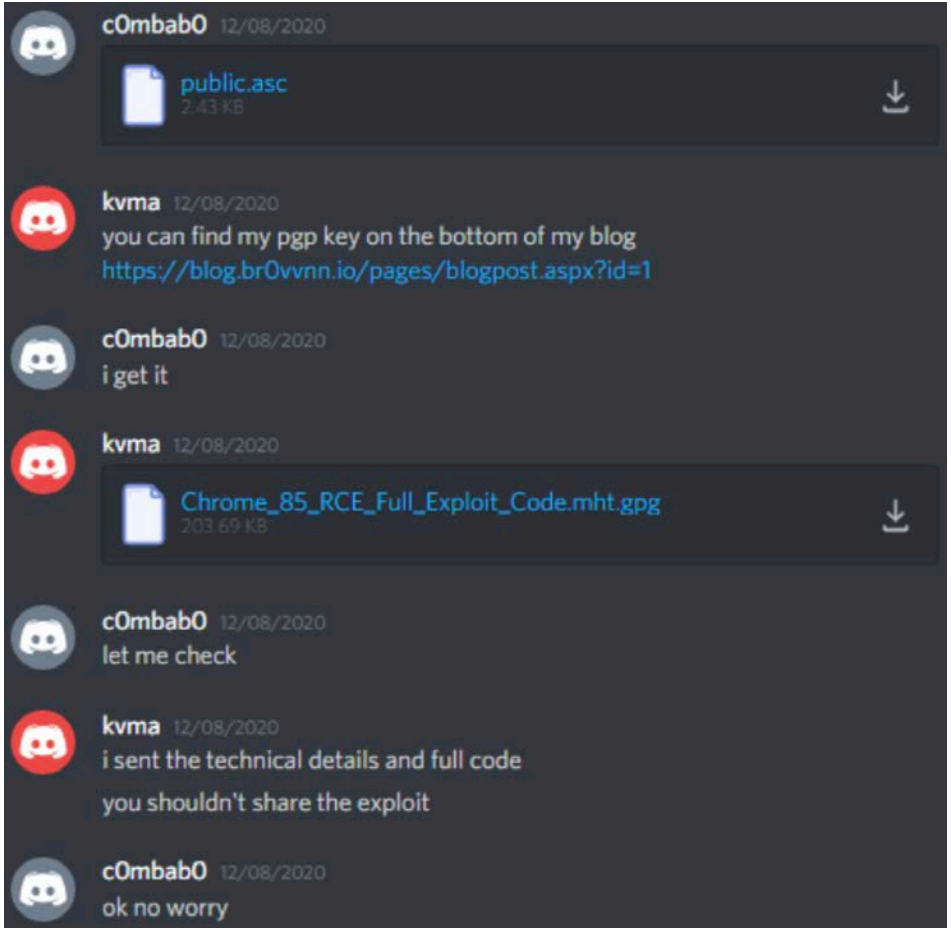
공격 시도

- 공격자는 보안 취약점 블로그를 운영하며 0day 연구자로 가장한 SNS 계정을 활용
- 트위터를 이용해 초기 접근 후 텔레그램, 디스코드 등으로 대화 채널을 변경 시도 함
- 취약점 익스플로잇 코드 개발에 협업을 요청하며 대상 별로 준비된 공격 코드를 전달

* 윈도우 취약점 연구 경험자
Visual Studio 프로젝트 전달

* 브라우저 취약점 연구 경험자
크롬 브라우저 기술 문서 (MHT 파일)

* 대화 중 공격자 소유의 블로그 링크를 통해 크롬 브라우저 0day 공격 시도



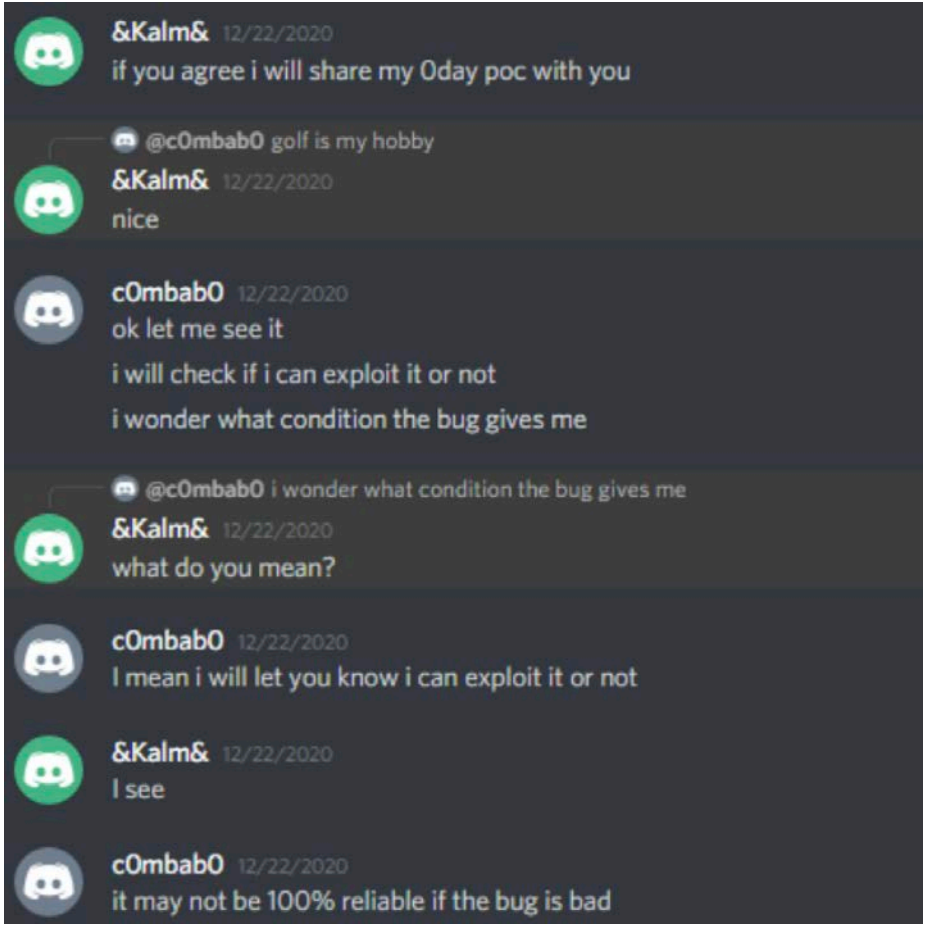
공격 시도

- 공격자는 보안 취약점 블로그를 운영하며 0day 연구자로 가장한 SNS 계정을 활용
- 트위터를 이용해 초기 접근 후 텔레그램, 디스코드 등으로 대화 채널을 변경 시도 함
- 취약점 익스플로잇 코드 개발에 협업을 요청하며 대상 별로 준비된 공격 코드를 전달

* 윈도우 취약점 연구 경험자
Visual Studio 프로젝트 전달

* 브라우저 취약점 연구 경험자
크롬 브라우저 기술 문서 (MHT 파일)

* 대화 중 공격자 소유의 블로그 링크를 통해 크롬 브라우저 0day 공격 시도



취약점 분석

- MHTML 확장자 파일 실행 시 윈도우 기본 설정 상 Internet Explorer 가 실행
- HTML로 작성된 기술 문서로 중요 코드 확인을 위해 스크립트 기능 허용이 필요
- 스크립트는 원격지 codevexillium[.]org 에서 최신 버전의 Internet Explorer 브라우저 0day 공격 코드 다운로드 및 실행
- 공격 코드는 특정 시기 이후 동작하지 않도록 설정
  2020/12/13 11:13:36 GMT+0900
- 0day 공격 코드는 고도로 무기화 됨
  * 99% Reliable
  * Process Continuation
  * New exploit technique for windows

취약점 분석

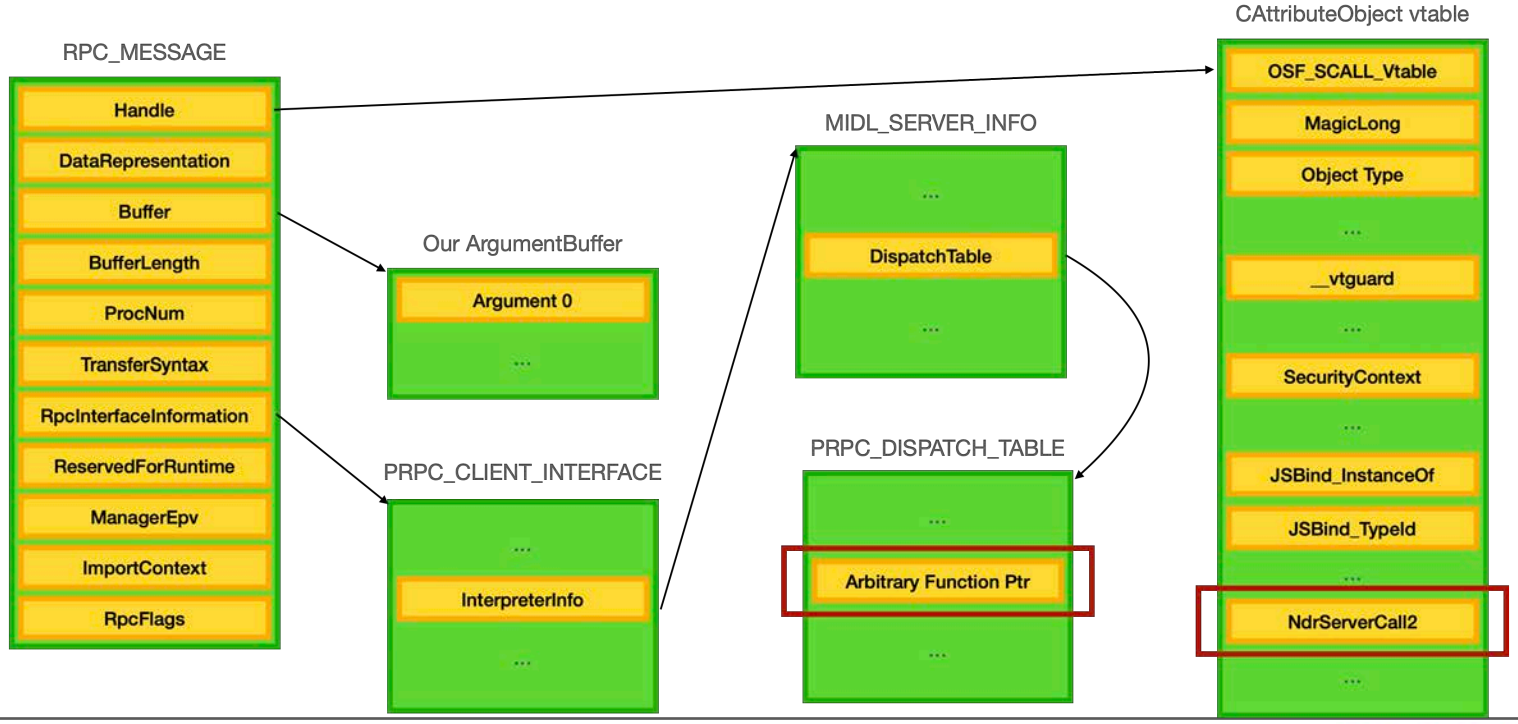
- 주요 브라우저 및 Flash Player 빈번하게 발생 했던 메모리 오염 버그
- MS Edge 출시 후 버그 공격의 효과적인 방어 기법인 MemGC 보호 기법의 영향을 받지 않음
- 2009년 중국 정부 지원을 받는 해커가 동일 유형의 버그를 이용해 구글을 해킹한 이력이 있음

```
1   var ele = document.createElement('element')
2   var att = document.createAttribute('attribute')
3   att.nodeValue = { // [1] typeof(att.nodeValue) == Object
4       valueOf: function() {
5           ele.clearAttributes() // [2] Free all attributes for 'ele'
6       }
7   }
8   ele.setAttributeNode(att)
9   ele.removeAttributeNode(att) // [3] Trigger att.valueOf
10                               // [4] Free 'att'
11  // [5] Double Free Bug
```

* https://en.wikipedia.org/wiki/Operation_Aurora
* https://fortune.com/2017/06/23/google-project-zero-hacker-swat-team

취약점 분석

- 공격 코드는 최신 버전의 윈도우 10 에서도 성공적으로 동작하도록 설계 됨
- 최종 악성코드 실행 이전 임의 코드 실행(Arbitrary code execution) 조건을 만족하기 위해 윈도우 소프트웨어에 범용적으로 적용 가능한 공격 기법이 사용 되었음



악성코드 분석

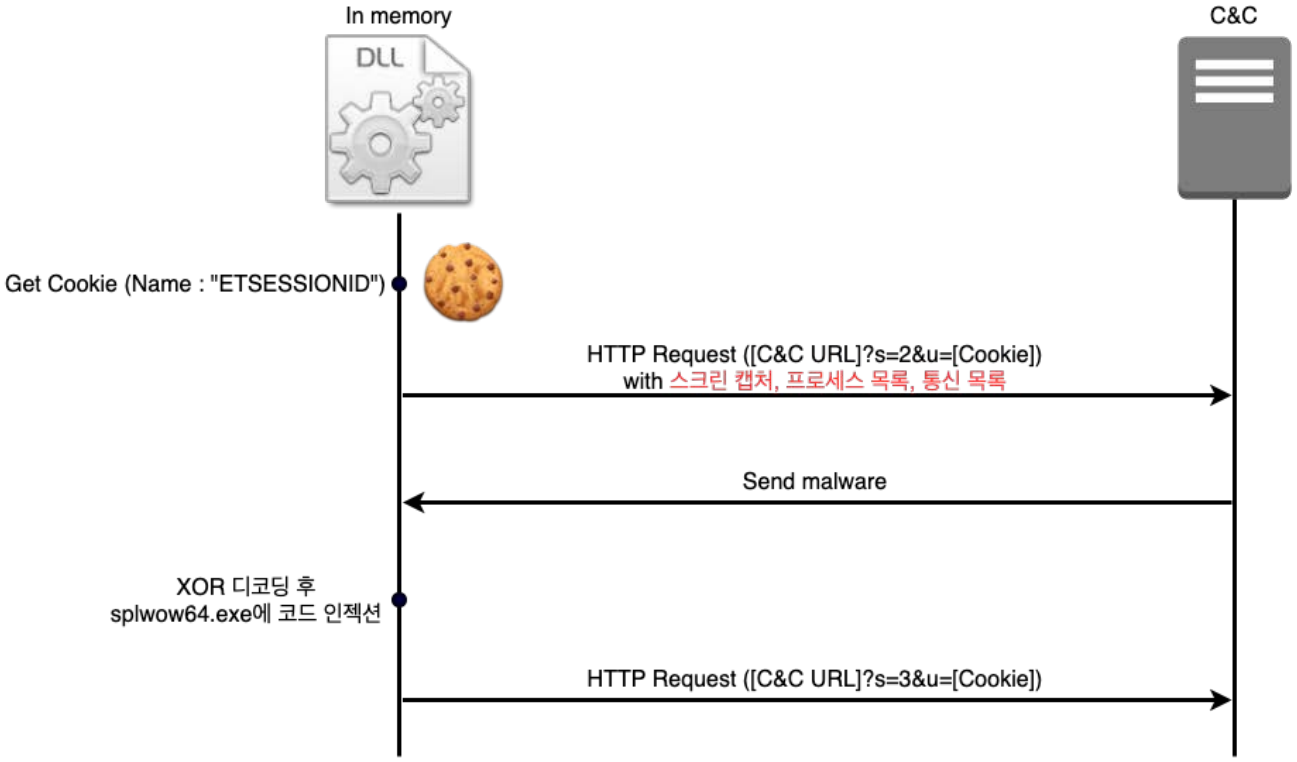
IE, Chrome, VisualStudio

MHTML

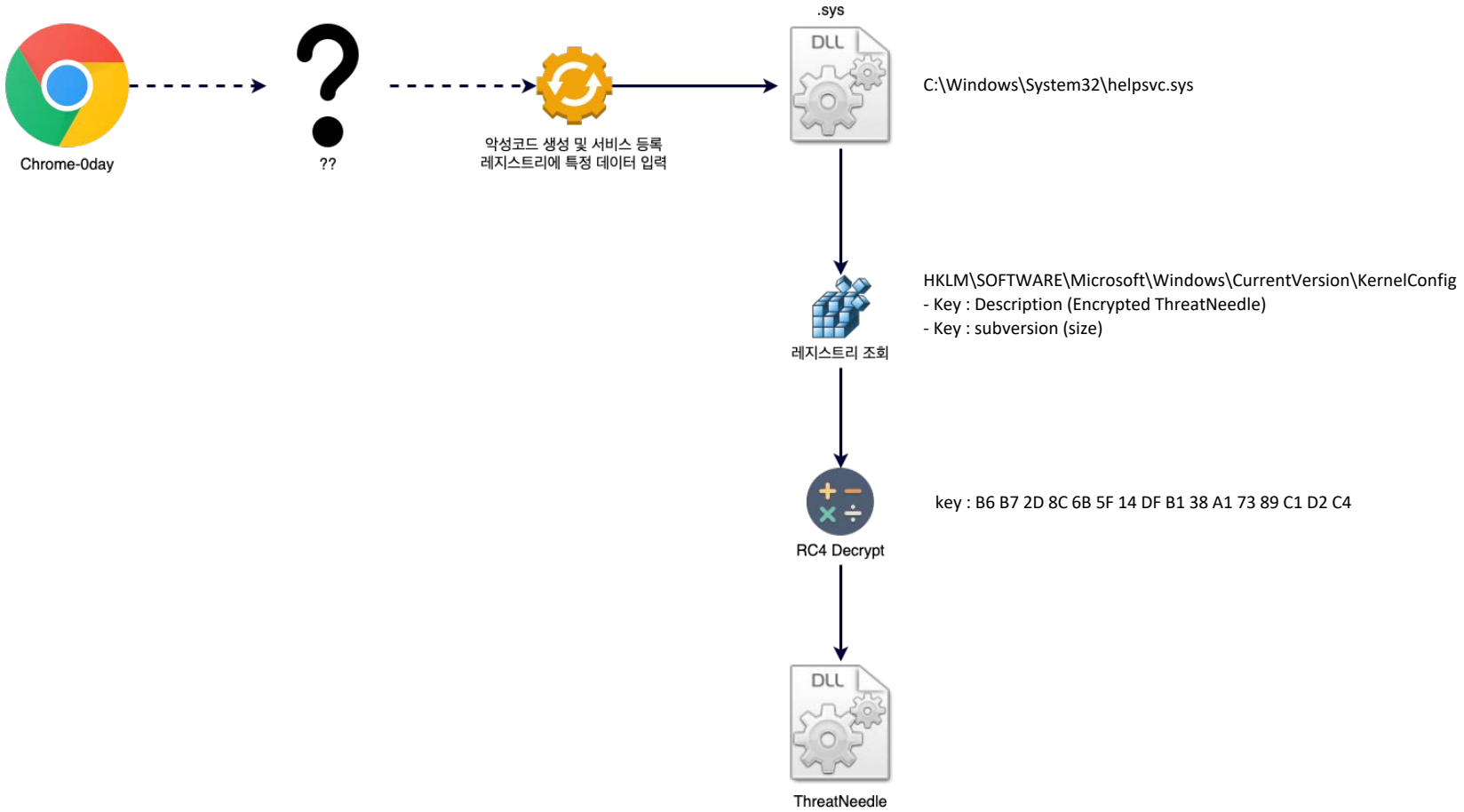
블로그 접속

VisualStudio

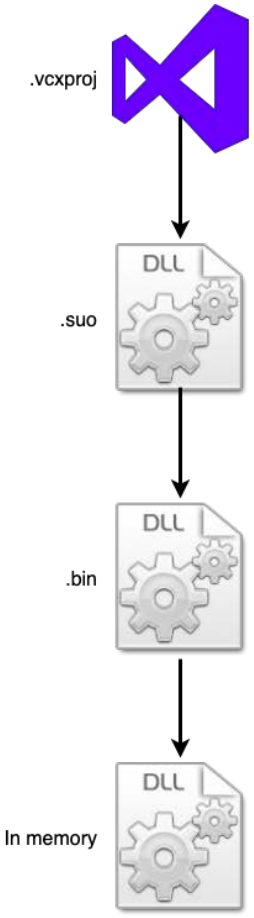
악성코드 분석 - IE


In memory
DLL
C&C
Get Cookie (Name : "ETSESSIONID")
HTTP Request ([C&C URL]?s=2&u=[Cookie])
with 스크린 캡처, 프로세스 목록, 통신 목록
Send malware
XOR 디코딩 후
splwow64.exe에 코드 인젝션
HTTP Request ([C&C URL]?s=3&u=[Cookie])

악성코드 분석 - 블로그 유도



악성코드 분석 - VisualStudio



- PreBuildEvent의 Command 태그로 인해 빌드 시 powershell 코드 실행

- Execute : rundll32 **vcxproj.suo**

- Parameter : **CMS_dataFinal**, **Bx9yb37GEcJNK6bt**, **4901**

- 카스퍼스키(avp.exe), 어베스트(avastui.exe) 프로세스 검사
- C:\ProgramData\vmware 폴더 생성 후 vmnet-update.bin 파일 생성
- 자동 실행 레지스트리에 하위 DLL 등록
  - path : SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Key : Onedrive_update
  - Value : C:\Windows\System32\rundll32.exe
    C:\ProgramData\VMware\vmnat-update.bin,OCSP_resp_find IxUi5CZ0IV45j89Y 4901

- 파라미터 검사 및 뮤텍스 생성 (**IxUi5CZ0IV45j89Y**)

- 파일 내 특정 bytes를 decrypt하여 메모리에 로드 (파라미터 : **4901**)
  - Case 1 : RC4 알고리즘 (key :62 AA A2 B2 C9 F4 F0 C6 62 B1 F2 E3 16 AE 6F 9C)
  - Case 2 : 커스텀 알고리즘 (key : tav!}C.mLq?d8a^$hCn/_A6US/5%#<=j)

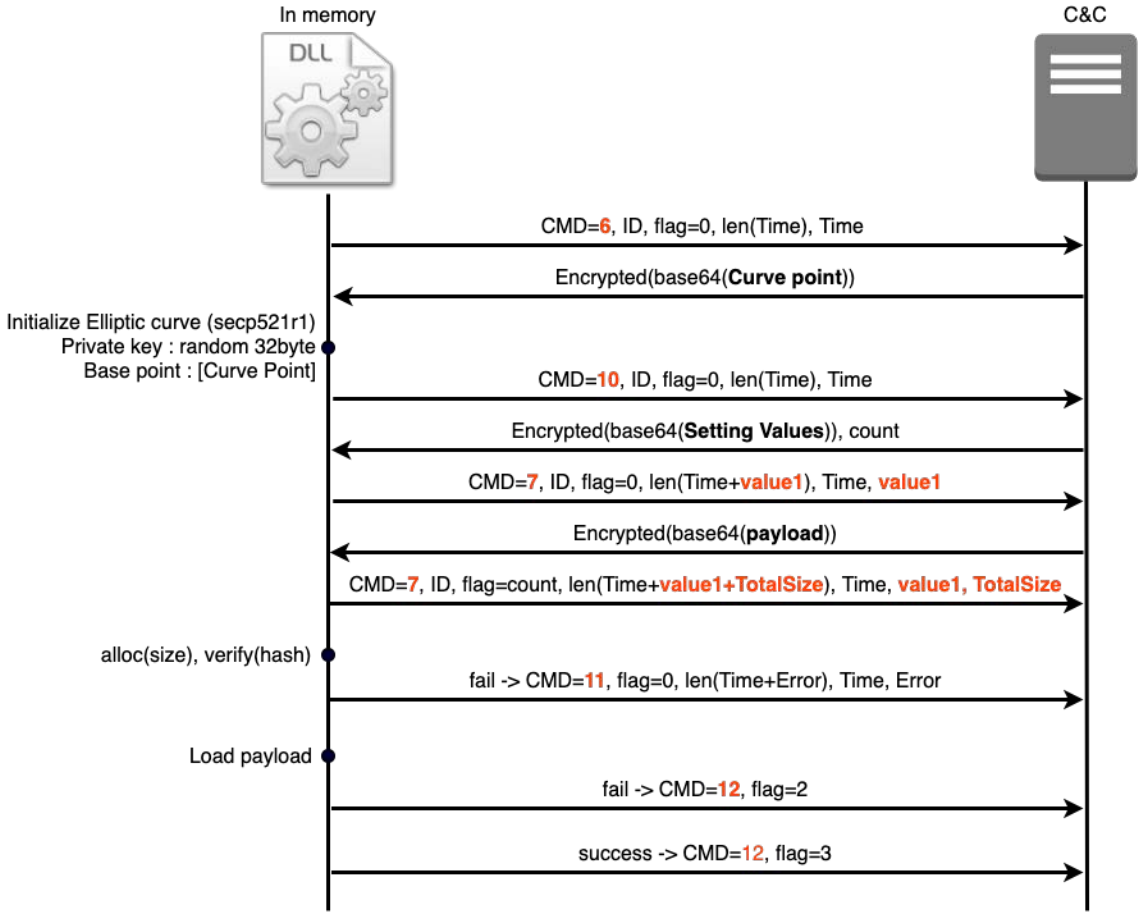
- 파라미터가 **4자리 숫자**인지 검사

- 파라미터 + 12자리 랜덤 알파벳 또는 숫자로 이루어진 16자리 식별 값 생성

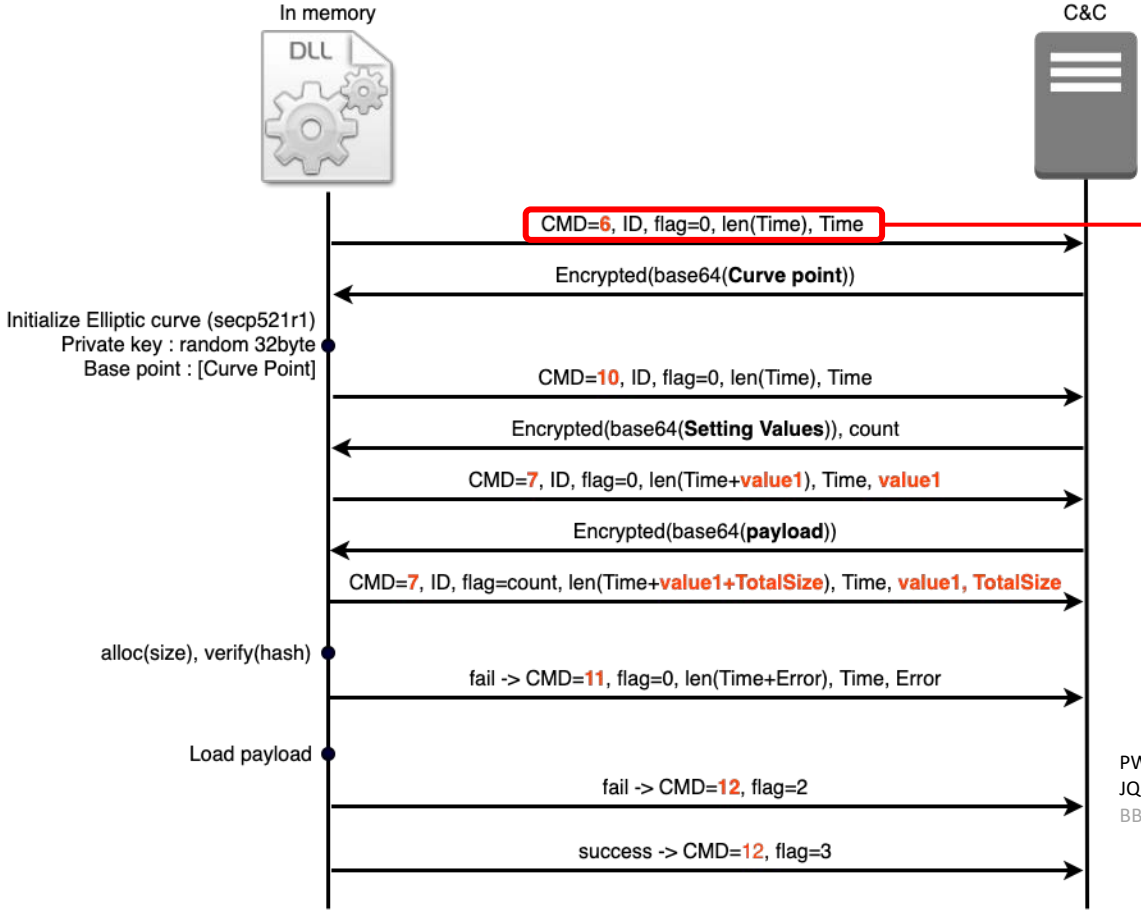
- AES256으로 C&C 서버 주소 추출

- HTTP 통신으로 C&C 서버와 연결

악성코드 분석 - VisualStudio



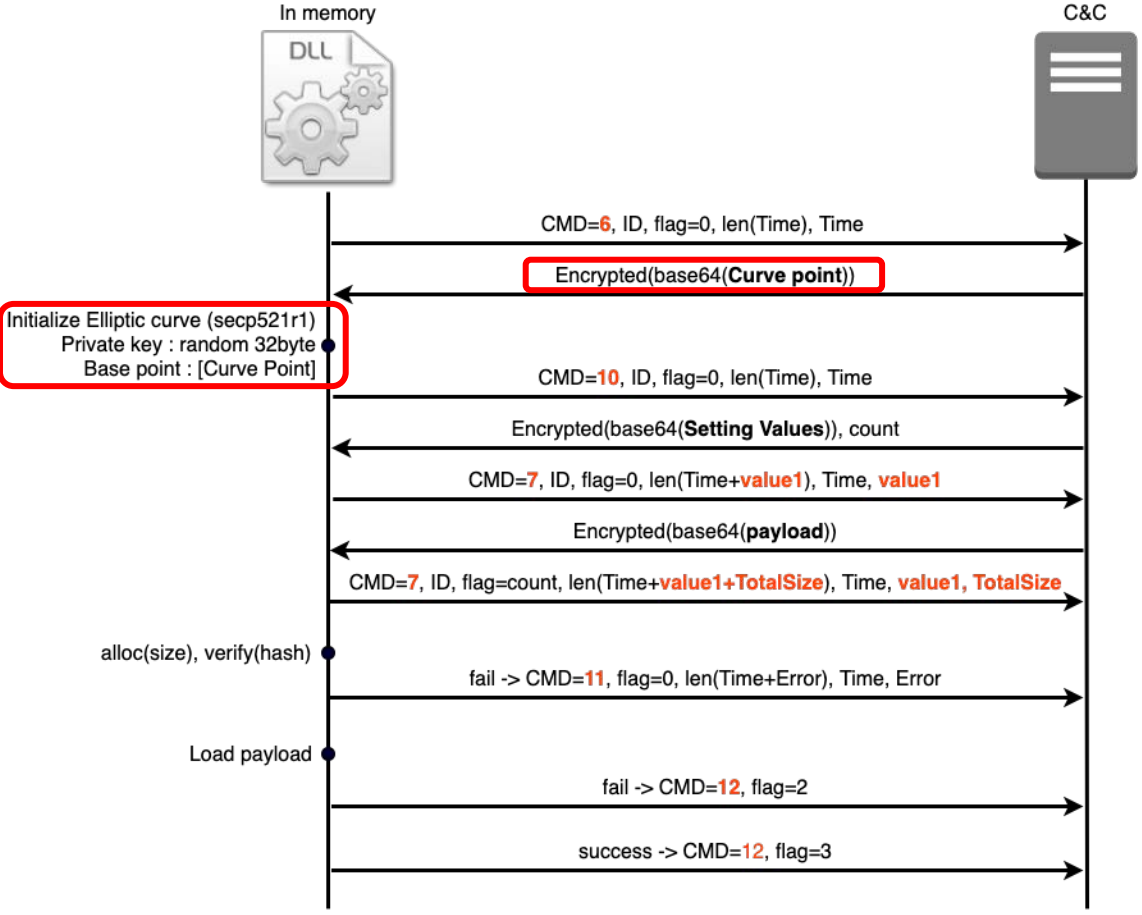
악성코드 분석 - VisualStudio



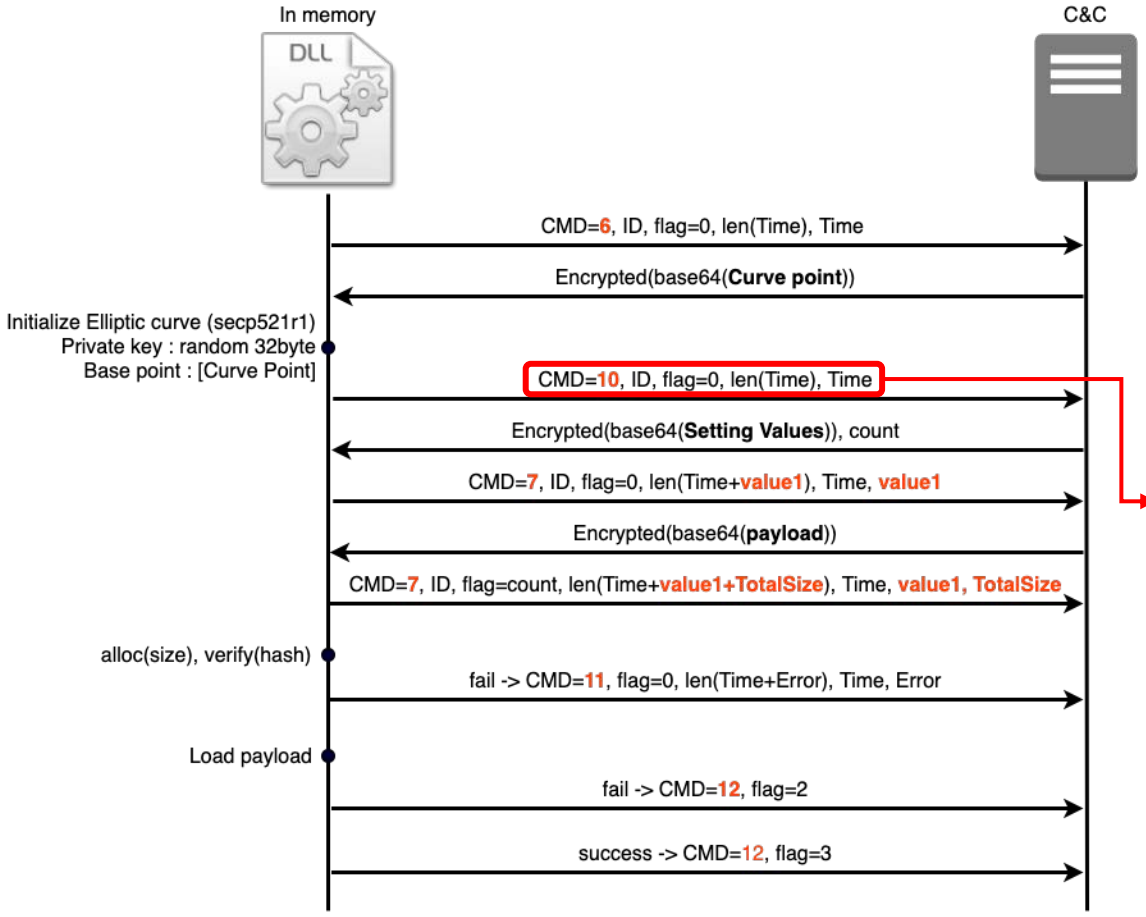
Num	필드 길이	데이터
1	2	랜덤{6}
2	5	base64(ID)
3	4	사용 X
4	6	Flag=0
5	6	len(시간)
6	6	base64(시간)
7~9	1~10	1~20개 랜덤 문자열 (무의미)

PW=GQWLXM&DTUXG=**YWJjZFpUd3dPYzBoQ05iTg==**&HDFV=&XPTERQ=**0**&EVYNQM=**52**&
JQRMAQ=**MgAwADIAMQAtADAAMQAtADIANwAgADEANQA6ADEAOAA6ADMAOQA=**&
BBYXCYGNER=LBBONCVIQHJUYC&RXBVB=QOZUYRDUX

악성코드 분석 - VisualStudio

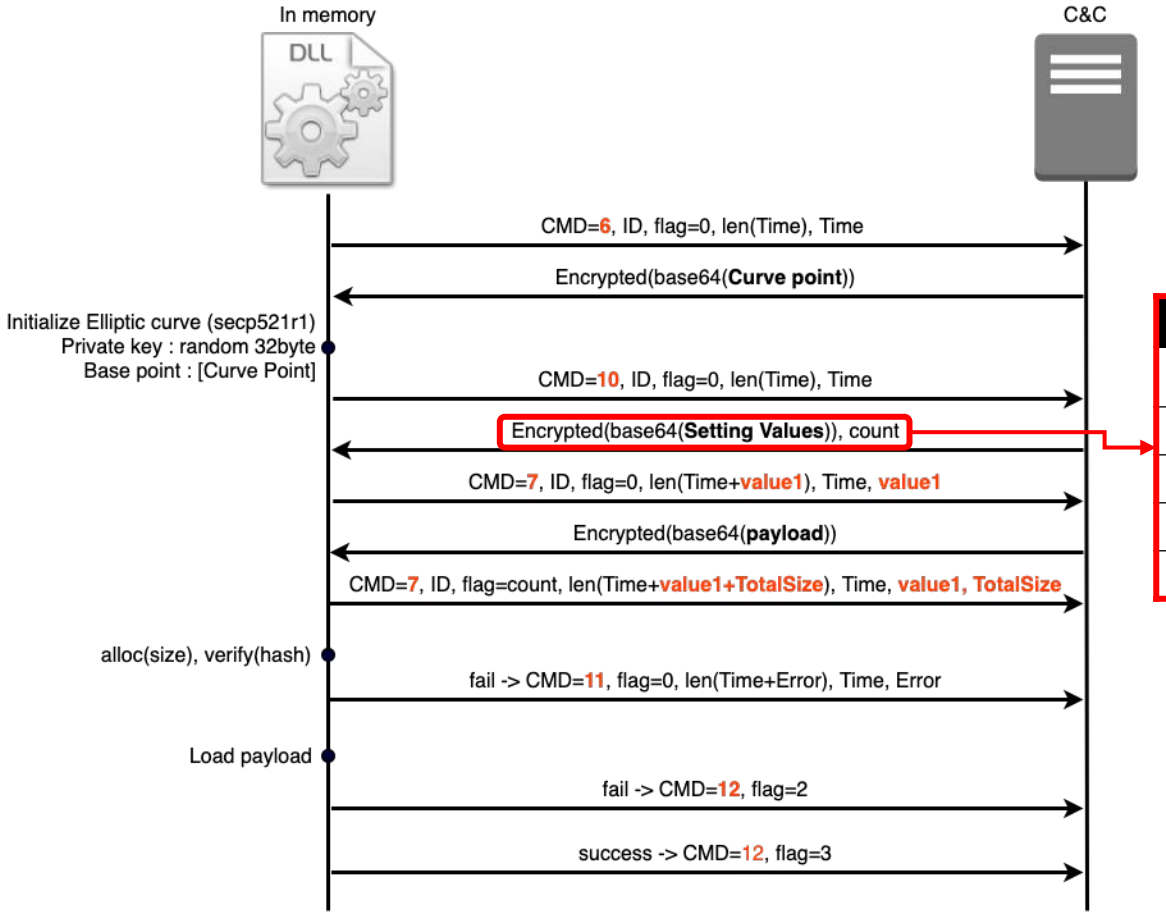


악성코드 분석 - VisualStudio



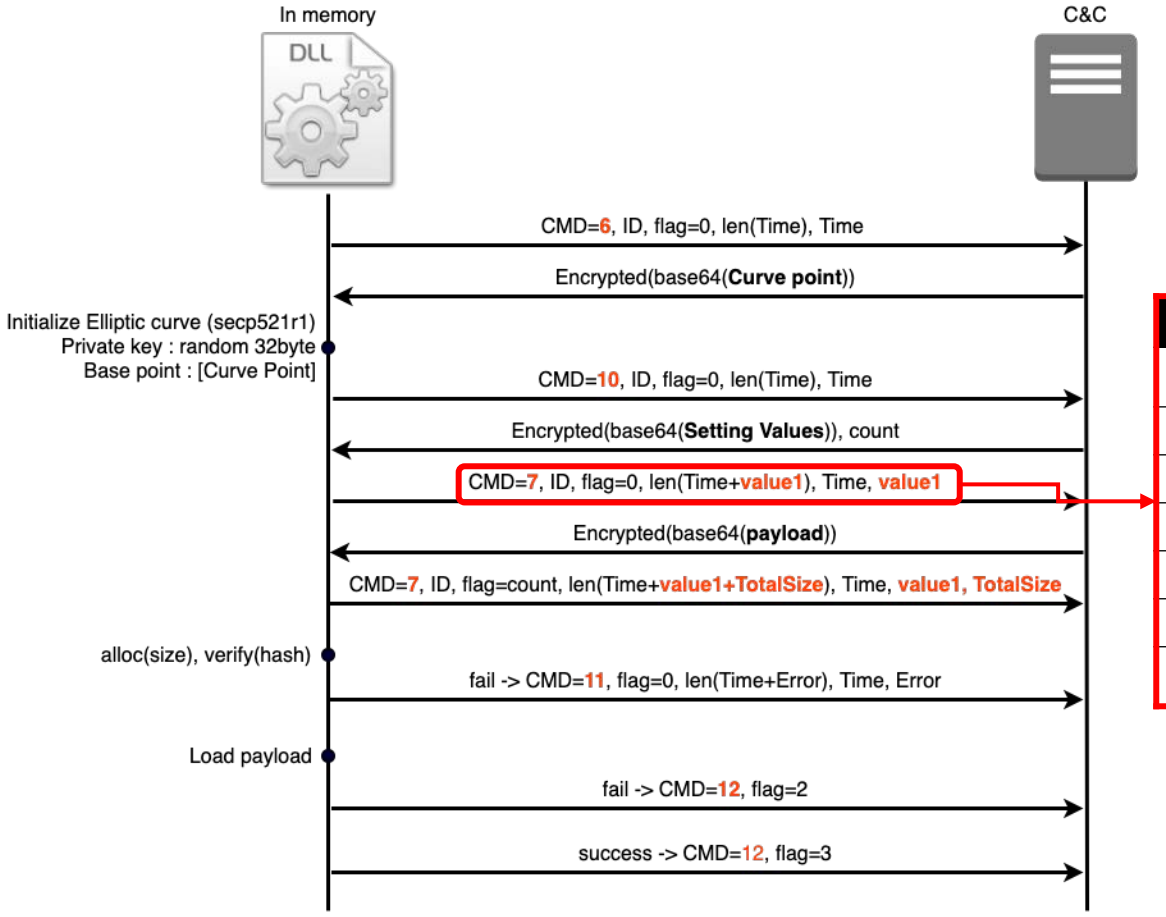
Num	필드 길이	데이터
1	2	랜덤{10}
2	5	base64(ID)
3	4	사용 X
4	6	Flag=0
5	6	len(시간)
6	6	base64(시간)
7~9	1~10	1~20개 랜덤 문자열 (무의미)

악성코드 분석 - VisualStudio



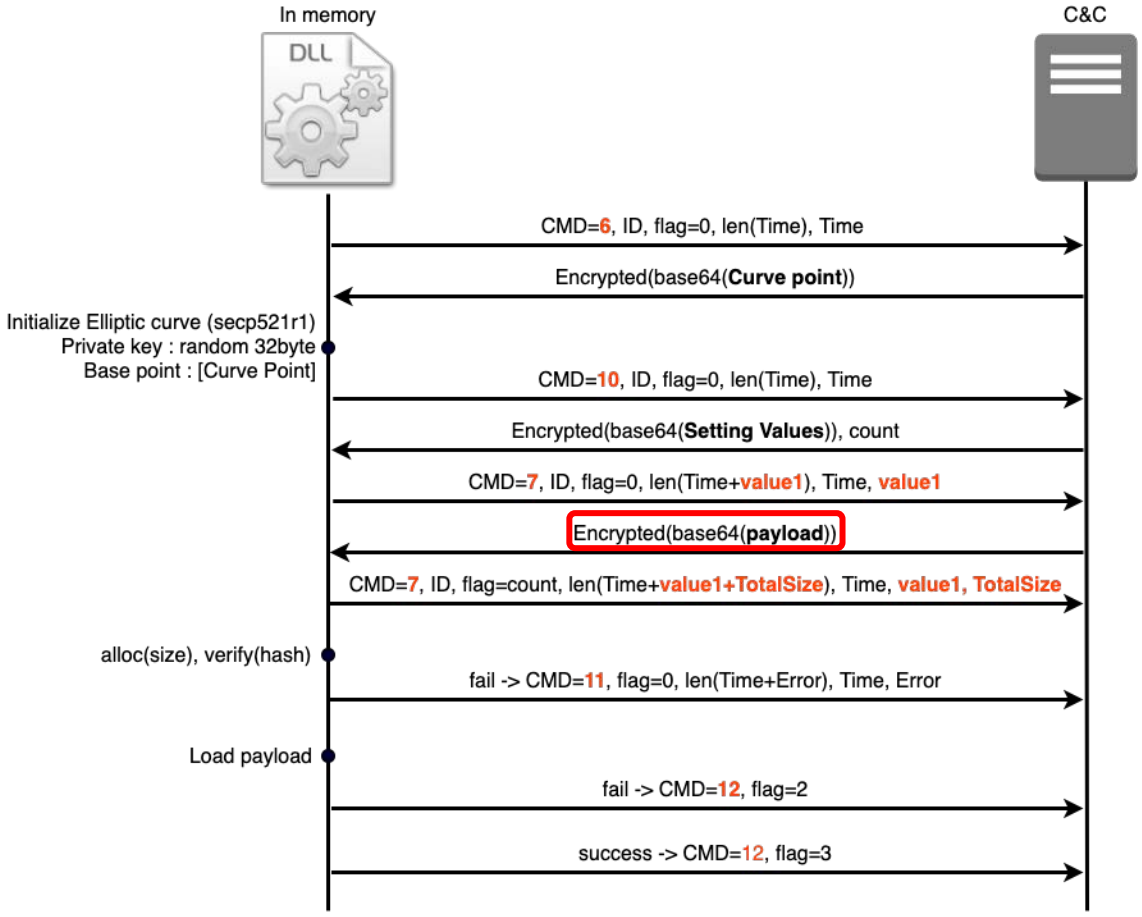
Num	데이터
value1	이후 발신 데이터 크기
value2	추가 payload 크기
value3	추가 payload export 함수 명
value4	Export 함수 실행 시 파라미터
value5	추가 payload HASH

악성코드 분석 - VisualStudio

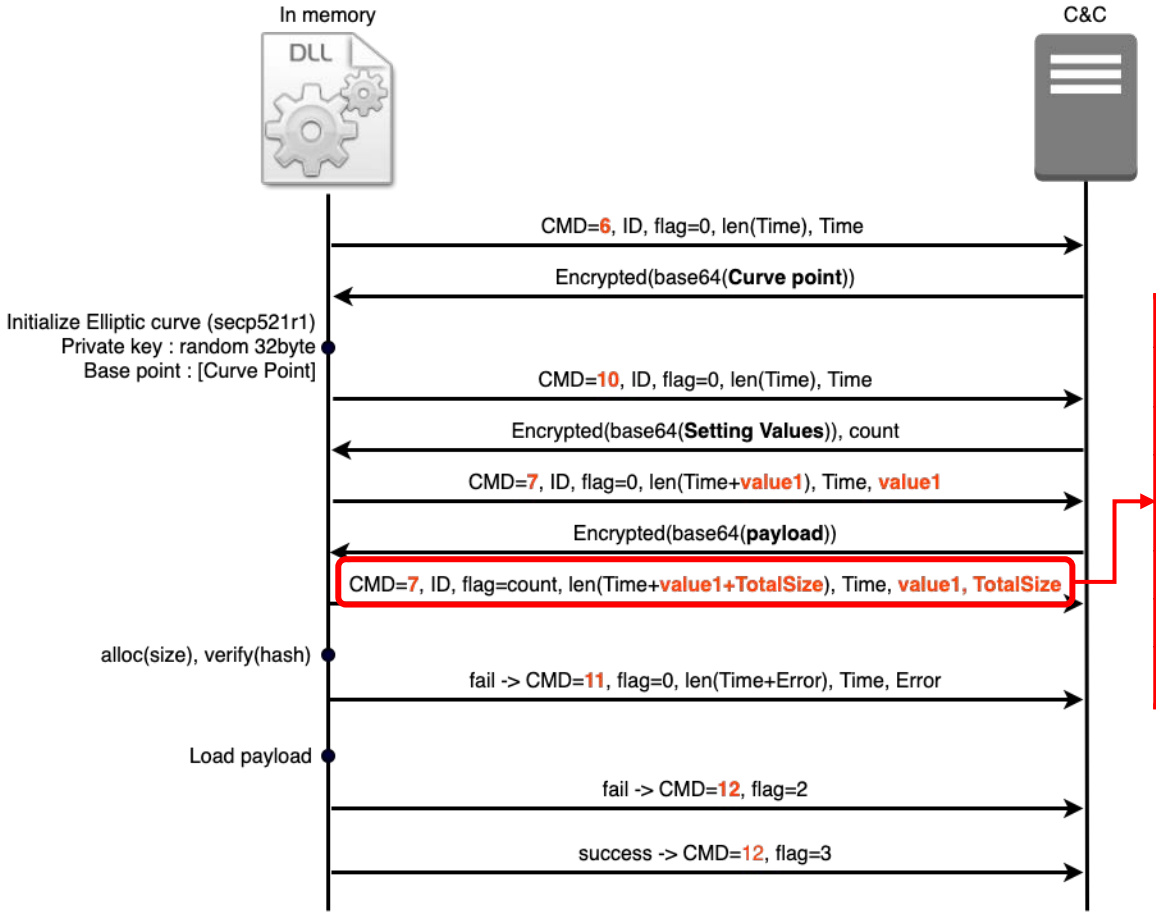


Num	필드 길이	데이터
1	2	랜덤{7}
2	5	base64(ID)
3	4	사용 X
4	6	Flag=0
5	6	len(시간+value1)
6	6	base64(시간, value1)
7~9	1~10	1~20개 랜덤 문자열 (무의미)

악성코드 분석 - VisualStudio

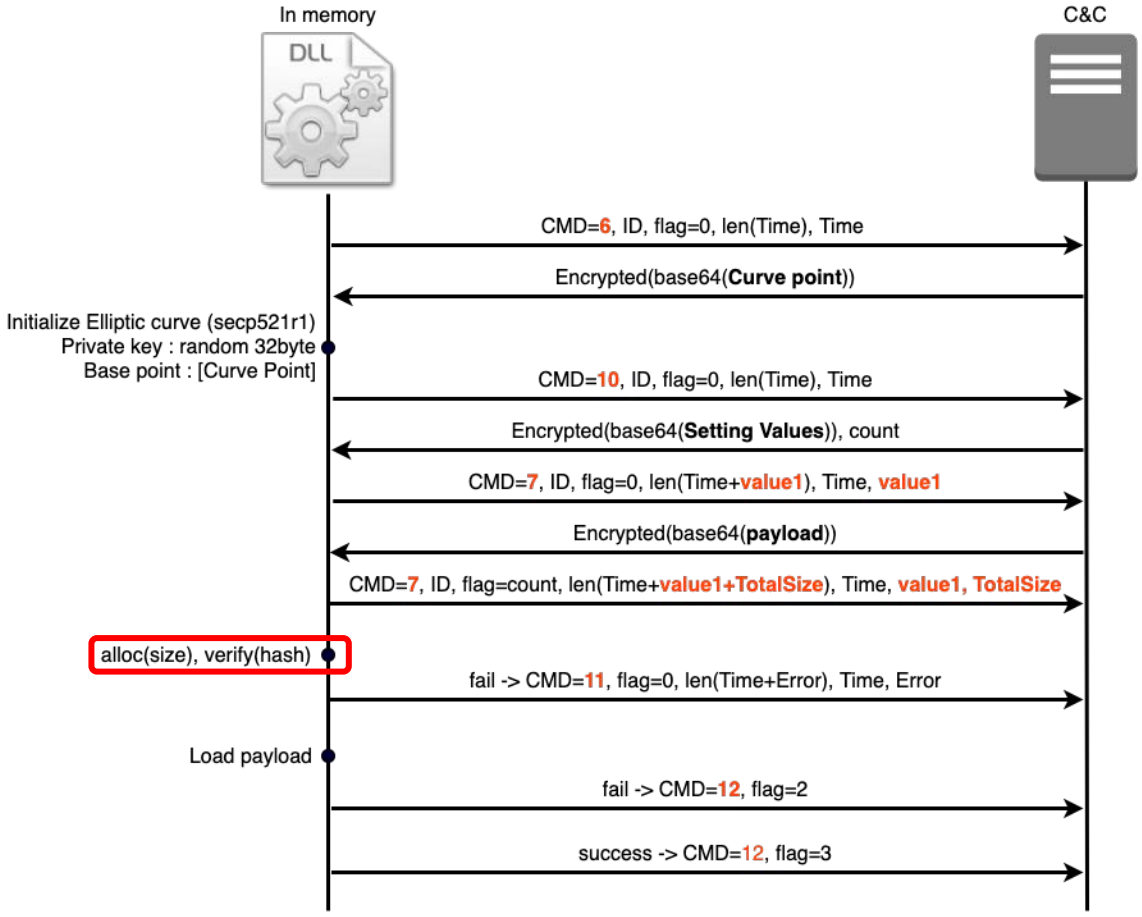


악성코드 분석 - VisualStudio



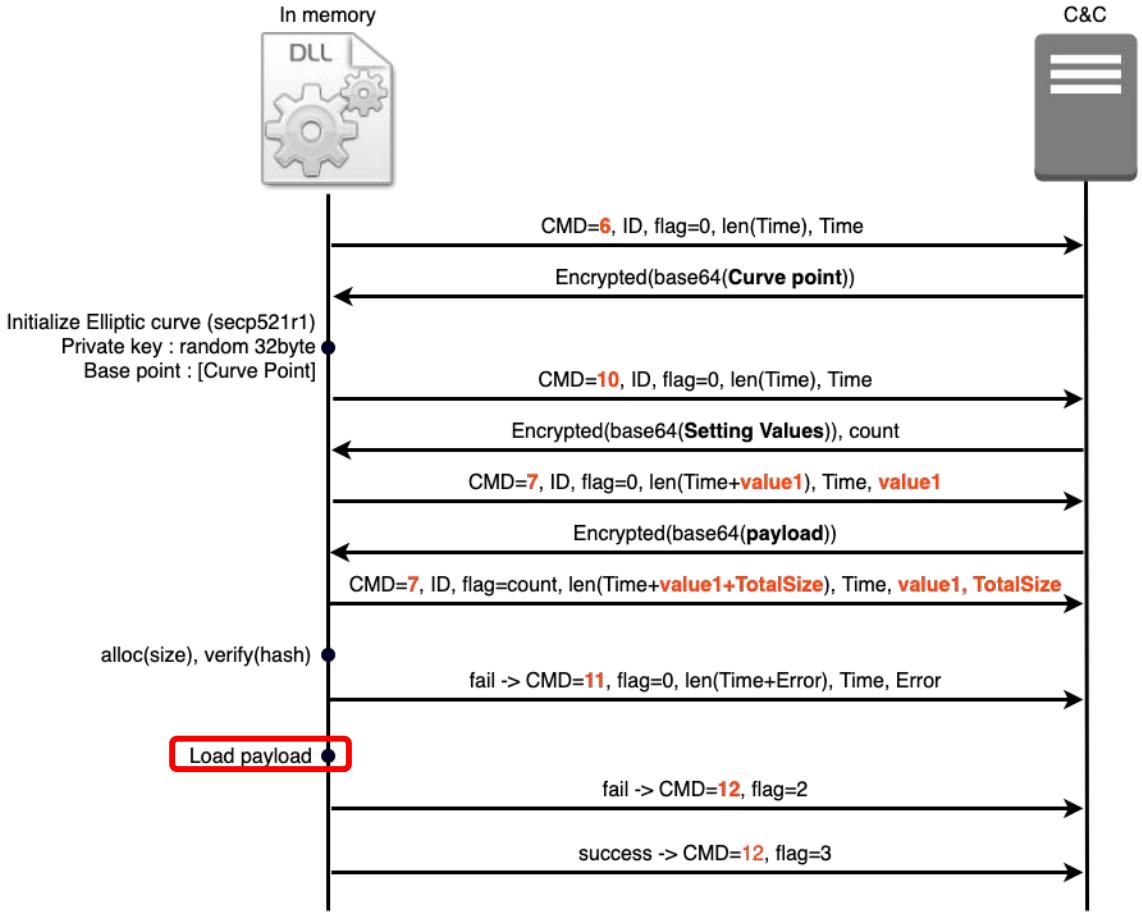
Num	필드 길이	데이터
1	2	랜덤{7}
2	5	base64(ID)
3	4	사용 X
4	6	Flag=count
5	6	len(시간+value1+total size)
6	6	base64(시간, value1, total size)
7~9	1~10	1~20개 랜덤 문자열 (무의미)

악성코드 분석 - VisualStudio



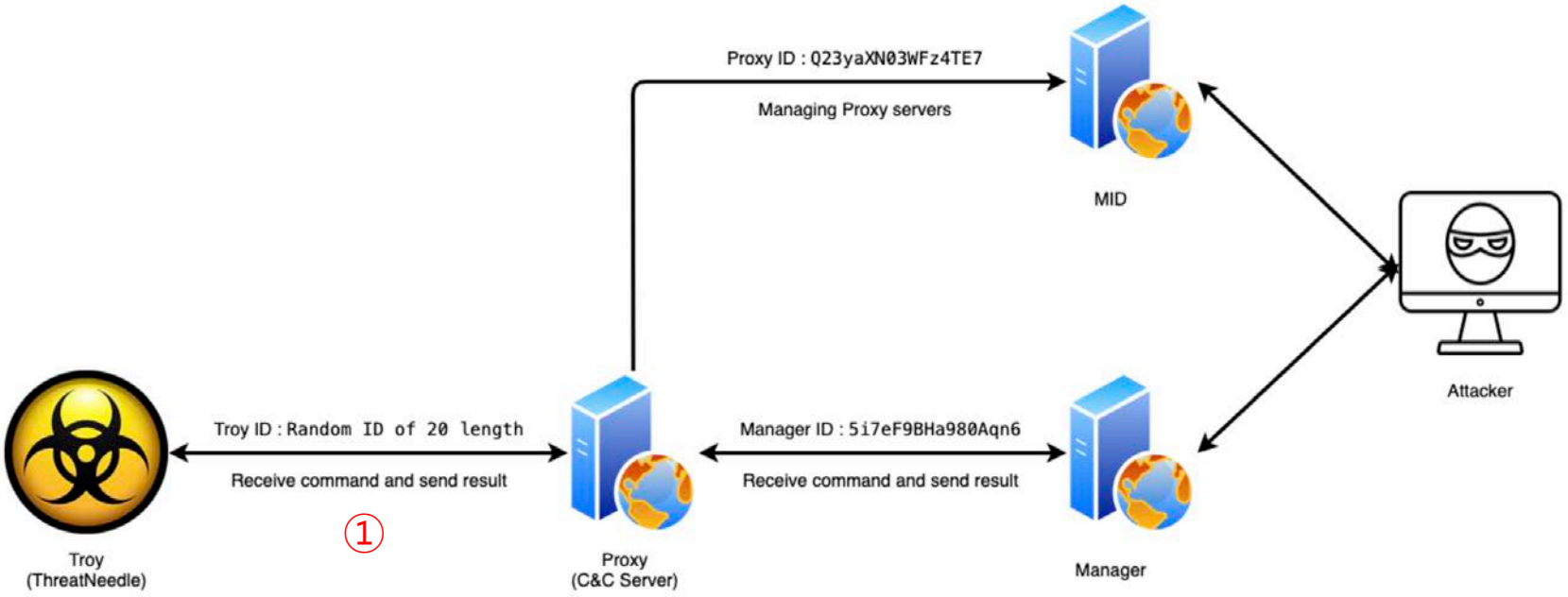
Num	데이터
value1	이후 발신 데이터 크기
value2	추가 payload 크기
value3	추가 payload export 함수 명
value4	Export 함수 실행 시 파라미터
value5	추가 payload HASH

악성코드 분석 - VisualStudio

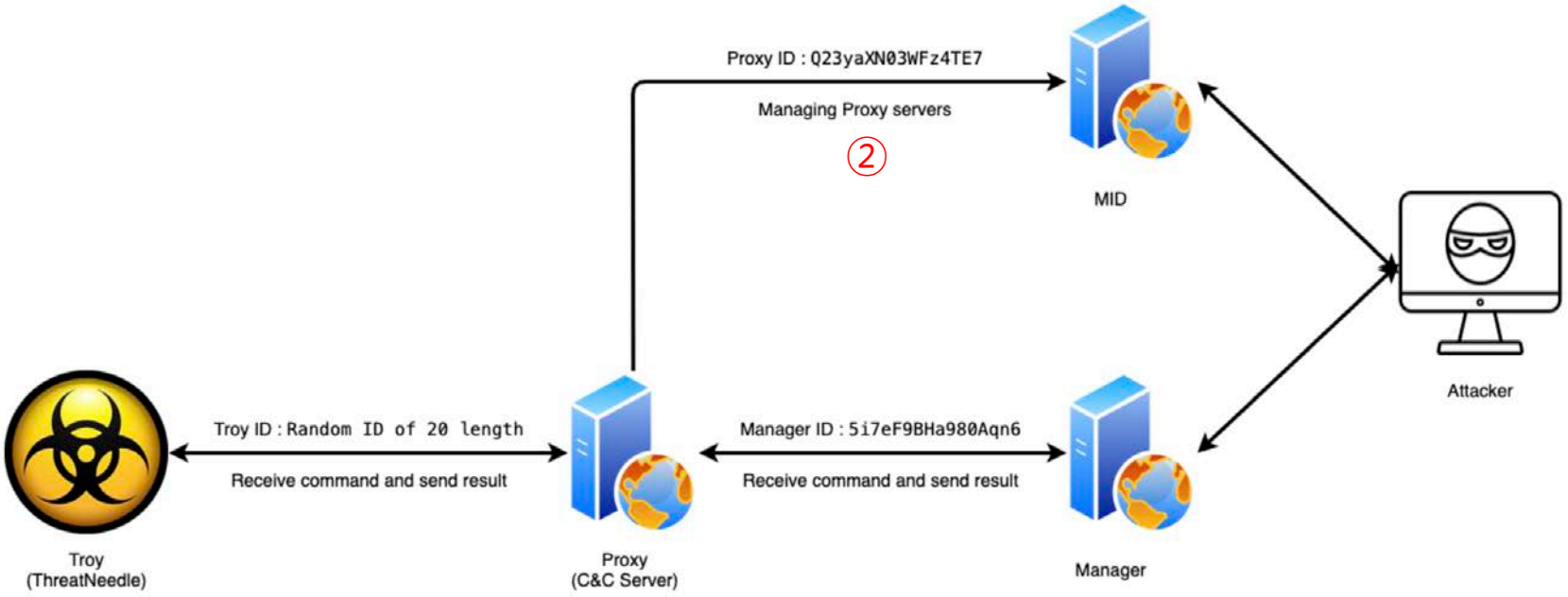


Num	데이터
value1	이후 발신 데이터 크기
value2	추가 payload 크기
value3	추가 payload export 함수 명
value4	Export 함수 실행 시 파라미터
value5	추가 payload HASH

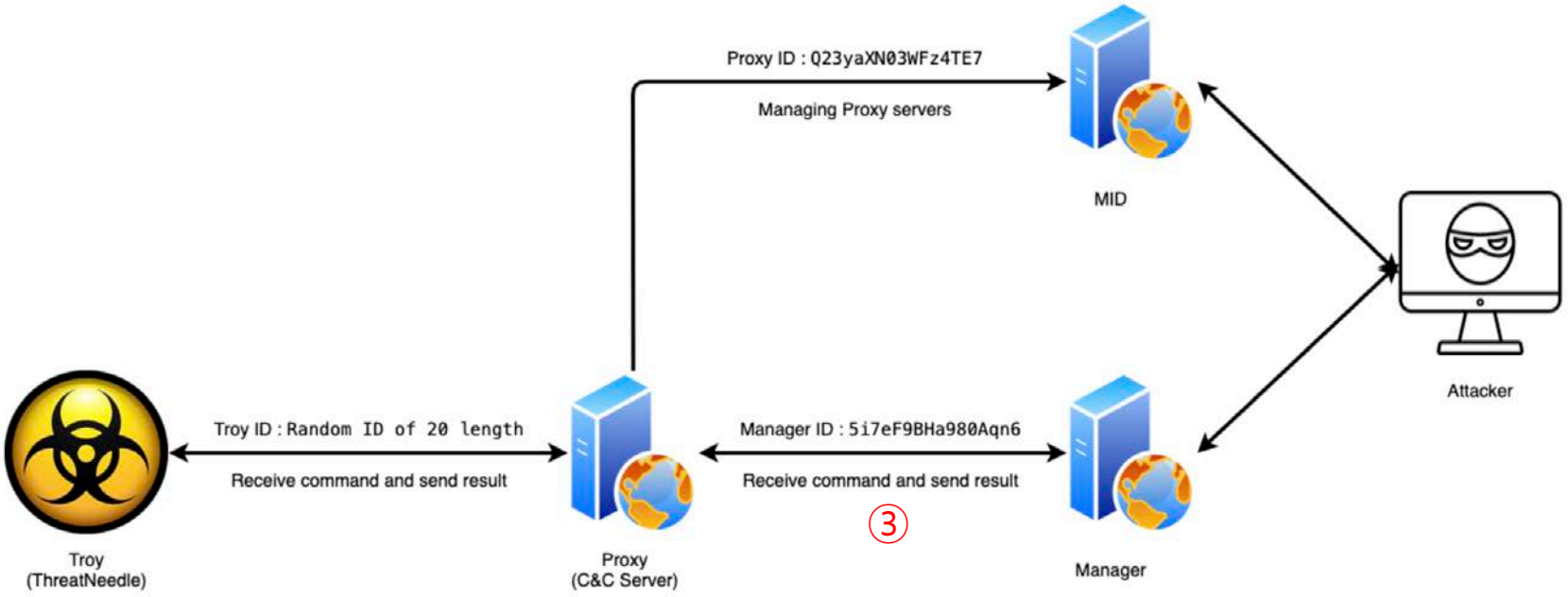
최종 원격제어 악성코드 - ThreatNeedle



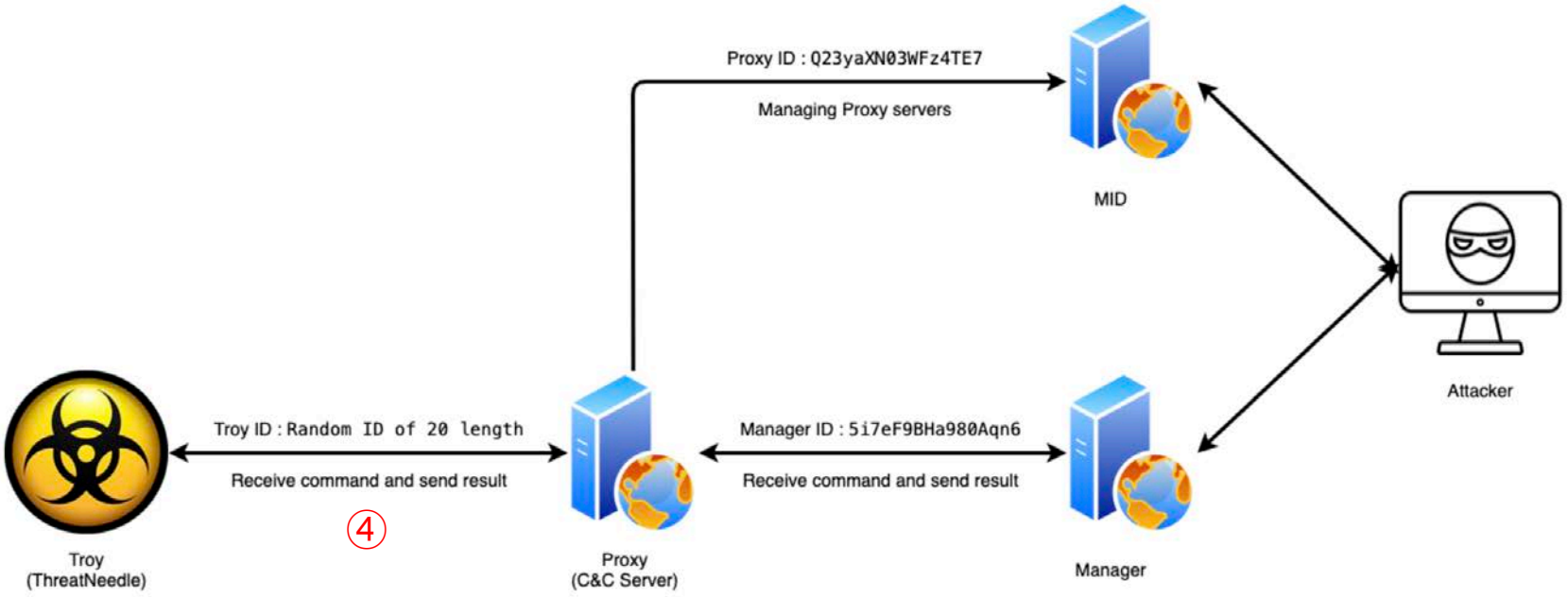
최종 원격제어 악성코드 - ThreatNeedle



최종 원격제어 악성코드 - ThreatNeedle



최종 원격제어 악성코드 - ThreatNeedle



국내 공격

[긴급] 베라포트 악용한 공급망 공격 발견! 북한 해킹조직

좋아요 116개 | 입력 : 2020-11-16 22:13

#공급망 공격 #라자루스 #이셋 #ESET

美보안업체 "유빗 해킹 배후, 북한 연계 라자루스 유력"

입력 2018.01.17 (11:33) | 수정 2018.01.17 (11:36)

한국 가상화폐 거래소 유빗에 대한 해킹 사건은 북한과 연계된 조직 라자루스의 소행일 가능성이 유력하다고 월 스트리트 저널이 16일 보도했다.

"빗썸 350억 해킹, 北 '라자루스' 소행인 듯"

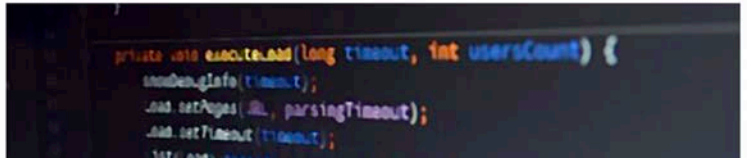
박서준 | 입력 2018.06.28 15:14 | 댓글 0

"이메일 분석 결과 과거 라자루스 공격 방식과 비슷"
美보안업체 에일리언볼트, 빗썸 해킹 배후로 北지목

구글플레이에 국내 군사기밀 노린 악성 앱 유포됐었다

지난해 8월 삭제...해커, 정상적인 앱에 악성코드 심어

임민철 기자 | 입력 :2019/02/11 17:16 -- 수정: 2019/02/12 08:55 | 컴퓨팅



주요 악성코드

北 해킹그룹 라자루스, 방산업체 타깃 새로운 사이버 공격 시도

ThreatNeedle/
Manuscrypt

WannaCry ransomware has links to North Korea, cybersecurity experts say

Similarities spotted between details of last week's massive cyber-attack and code used by a prolific cybergang with links to North Korean government

[긴급] 인도 핵발전소 공격 악성코드, 라자루스 공격코드?

입력 : 2019-10-31 10:44

#인도 #쿠단 쿨람 핵발전소 #KKNPP #해킹 #악성코드 #7·7 디도스 #유사점 #라자루스 #Lazarus

MATA: Multi-platform targeted malware framework

APT REPORTS 22 JUL 2020 7 minute read

넹코드 유사점 발견돼

가동이 중단된 가운데, 공격

사점이 발견돼 충격을 주고 있

Operation AppleJeus Sequel

APT REPORTS 08 JAN 2020 8 minute read

Lazarus supply-chain attack in South Korea

ESET researchers uncover a nove

ZVERA VeraPort software

Anton Cherepanov

16 Nov 2020 - 11:30AM

Share

ESET telemetry data recently led our researchers to discover attempts to deploy Lazarus malware via a supply-chain attack in South Korea. In order to deliver its malware, the attackers used an unusual supply-chain mechanism, abusing legitimate South Korean security software and digital certificates stolen from two different companies.

// AUTHORS

GREAT

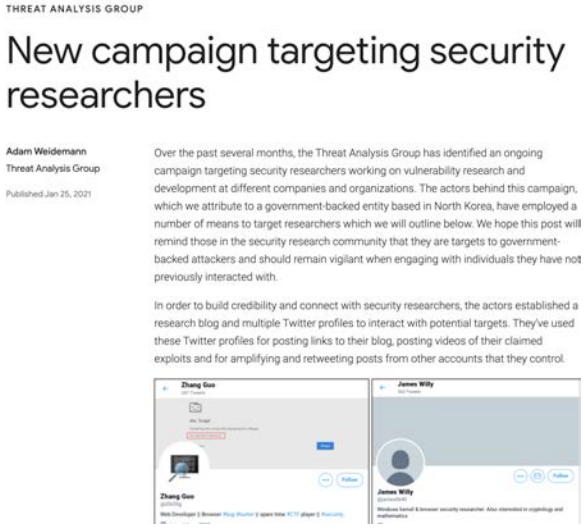
The Lazarus group is currently one of the most active and prolific APT actors. In 2018, Kaspersky

개인을 직접 노리는 라자루스 캠페인

CLEARSKY Cyber Security

Operation 'Dream Job'

Widespread North Korean Espionage Campaign



Malbus
(2017년 중순~)

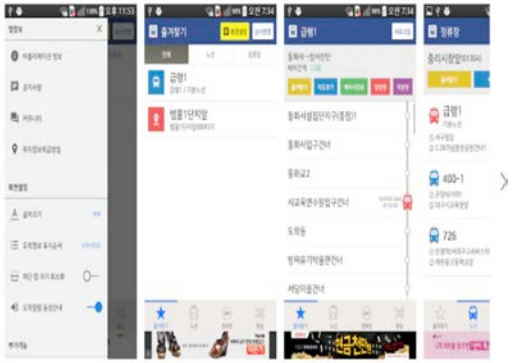
Dreab job
(2019년~)

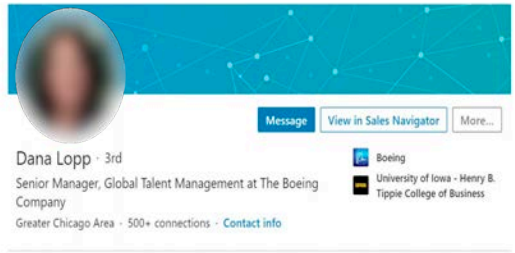
Targeting security researchers
(2020년 하순~)

점점 과감해지는 침투 시도

앱 (일상) -> Linkedin (구직)

-> Twitter, Telegram, KeyBase, LinkedIn, Discord, Email (소셜)





2. The fake profile that apparently was deleted after the attackers finished the impersonation

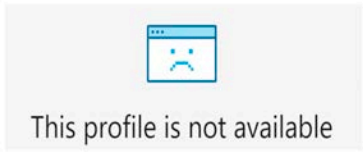
Fake: https://www.linkedin.com/in/dana-lopp-4132121b0

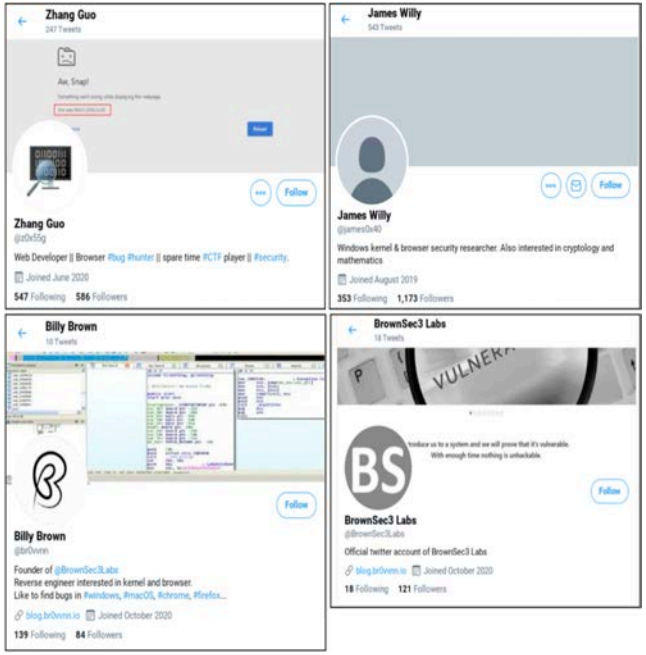
www.linkedin.com › dana-lopp-4132121b0

Dana Lopp - Senior Manager, Global Talent Planning ...

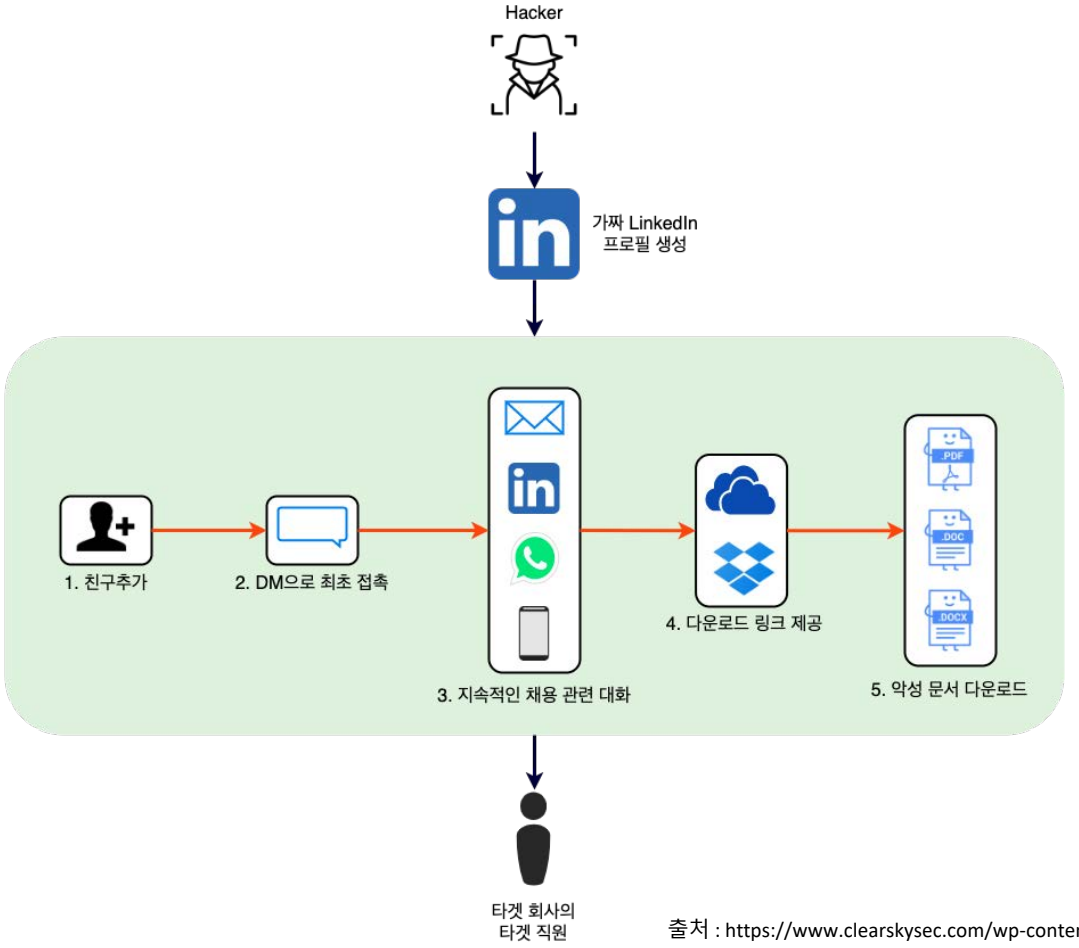
Manage the client facing HR Client Services team for Boeing Global Services with responsibility for integrated solutions around Talent Management, People ...

Greater Chicago Area - Senior Manager, Global Talent Planning & Acquisition - Boeing





Operation Dream Job



출처 : https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

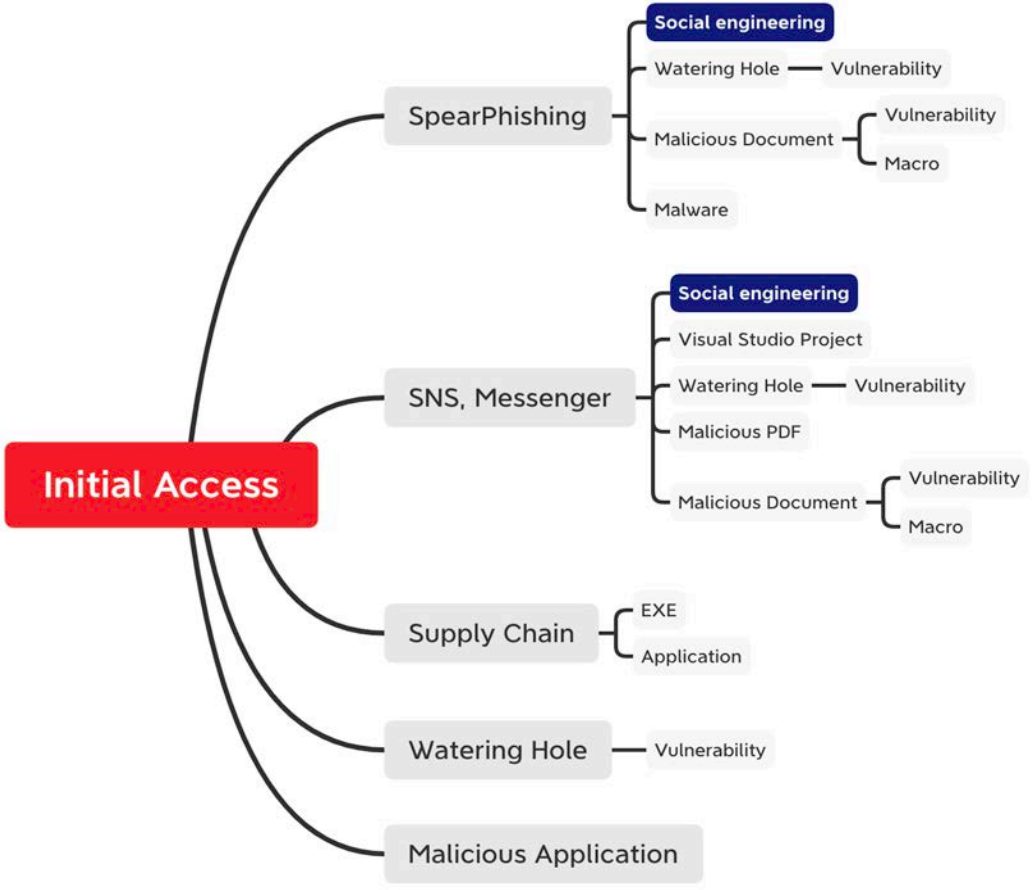
Operation Dream Job

1. Sumatra 변조 (Open-source PDF reader)
2. 악성 DOC 파일 (악성 매크로 포함)
3. 악성 DOCX 파일 (악성 매크로가 포함된 DOTM 파일 다운로드)

각 Operation 비교

	Malbus	Dream Job	Targeting Security researchers
시기	2017년 중순~	2019년~	2020년 하순~
타겟	국내 / 앱 개발자	해외 / 국방, 정부 기업, 방위, 항공 우주 기업 직원	국내 및 해외 / 보안 취약점 리서처
최종 타겟	앱 사용자 중 국방 관련 종사자	국방, 정부 기업, 방위, 항공 우주 기업	?
최초 접촉	개발자 : 스피어 피싱	LinkedIn	Twitter, Telegram, KeyBase, LinkedIn, Discord, Email
접촉 내용	개발자 : 개발 외주	채용	같이 연구, 조언 등
악성코드 전달	개발자 : 메일 내 첨부파일 타겟 : 앱 업데이트 or 다운로드	Onedrive / Drobox 링크 전송	압축 파일 전송, 블로그 유도, MHTML 열람 유도
로더	개발자 : 악성 한글파일 타겟 : 악성 앱	악성 PDF, 악성 DOC, 악성 DOCX	악성 VisualStudio 프로젝트, Zero-day 취약점
최종 악성코드	ThreatNeedle	DeathNote, ThreatNeedle	ThreatNeedle

점점 다양해지는 Initial Access



결론 1

- LinkedIn, Twitter 등의 SNS를 활용하면 타겟에 대한 정보를 보다 쉽게 수집할 수 있음
- 같은 분야 종사자 또는 채용 담당자로 사칭하여 신뢰관계 형성
  - 기밀 보장
  - 행위 유도
  - 지속 가능

  -> 코로나로 인한 재택근무 증가로 보다 더 쉬운 접근 가능
- 라자루스는 점점 더 과감하게 다양한 매체를 통해 개인에게 직접 접근하고 있음
  - 정확한 목표로 정확한 타겟을 설정하여 특화된 공격을 시도
- 개인의 경우 기업보다 방어 체계 구축이 미흡하기 때문에 대응 및 탐지가 어려움
- 보안 리서처들은 업데이트를 잘 수행하지만, 이 점이 오히려 독이 되었음
  - 설마 나에게 크롬, IE 제로데이를 ?

결론 2

- 공격자들이 열심히 하는 만큼 방어자들도 열심히 대비해야한다.
  - 메이저 Zero-day, 화술, 전략, 일일이 직접 컨택하는 노력..

- 매우 실력있는 리서처의 개인PC 감염 사례

결론 3

출처 : https://twitter.com/ifsecure/status/1354023914721210368?s=21

THANK YOU

ENKI 박세한 : shpark@enki.co.kr

S2W LAB 류소준 : hypen@s2wlab.com