

효율적인 APT 시뮬레이터 프레임워크 제안

An Efficient APT Simulator Framework

허남정¹, 최상훈^{2,*}, 박기웅^{2,†}

세종대학교 시스템보안연구실 (지능형드론 융합전공) 석사과정¹

세종대학교 시스템보안연구실 (연구교수)^{2,*}

세종대학교 정보보호학과 (교수)^{2,†}

목차

I. 서론

II. 선행 연구 및 프로그램

III. 효율적인 APT 프레임워크 제안

IV. APT 프레임워크 : 에이전트 및 C2 Server 통신 과정

V. 구현 코드

VI. 결론

[참고 문헌]

- 최근 사이버 보안 분야에서 **APT 공격이 기업의 자원을 탈취하고 인프라를 망가뜨리고 있음 [1].**
- APT 공격은 증가하고 있는 추세이며, **APT 공격에 대응하기 위한 수단이 필요함 [1].**
- 백신/모니터링 시스템
 - 기업의 네트워크에 대한 지속적으로 감시하고 및 탐지하여 실시간으로 대응함.
- **APT 시뮬레이터**
 - 실제 APT 공격 사항을 재현하여 조직 내 보안 취약점을 탐지하고 개선 방안을 도출함 [2].



심각해지고 있는 APT 공격 1 : 중국 해킹 단체

□ 많은 중국의 해킹단체들이 APT 공격으로 국내 기업의 인프라에 상당한 피해를 입히고 있음.

중국의 APT 단체 벨벳앤티, 대기업을 3년이나 몰래 염탐해 왔다

입력 : 2024-06-25 18:03



고급 기술을 총동원한 중국의 APT 조직이 3년이나 한 기업을 염탐해 왔다는 사실이 드러났다. 정상적인 도구와 장비들을 한껏 활용했고, 덕분에 들켜지 않을 수 있었다. 이러한 공격은 조만간 보편화될 것으로 예상된다.

[보안뉴스 문정후 기자] 중국의 APT 공격 단체 하나가 F5의 네트워크 장비를 활용해 한 피해 기업의 네트워크에서 지속적인 공격을 실시할 수 있었던 것으로 밝혀졌다. 공격자들은 3년 동안이나 몰래 피해 조직에 침투한 상태로 여러 가지 정보를 입수한 것으로 분석되고 있다. 보안 업체 (Sygnia)가 이와 관련된 내용들을 조사해 발표했다. 피해 기업에 대해서는 정확한 내용이 공개되지 않았다. 다만 규모가 꽤 큰 조직이라고만 시그니아가 밝혔다.

중국의 해킹 단체 윈티, 한국의 게임사 그래비티 공격

입력 : 2020-04-22 00:31



아마도 여러 APT 단체의 연합인 윈티그룹, 다양한 공격 기술 발휘 가능해
드로퍼 샘플 분석했더니 최근 한국의 게임사 그래비티 공격했다는 흔적 나와

[보안뉴스 문가용 기자] 중국의 APT 공격 단체인 윈티그룹(Winnti Group)이 한국의 비디오 게임 회사인 그래비티(Gravity)를 공격했다고 보안 업체 블랙베리(BlackBerry)가 발표했다. 윈티 그룹은 2009년부터 액시엄(Axiom), 바륨(Barium), 블랙플라이(Blackfly) 등의 조직들과 한 목적으로 활동해 왔으며, 주로 항공, 게임, 제약, 기술, 통신, 소프트웨어 산업을 노려왔다.

심각해지고 있는 APT 공격 2 : 북한 해킹 단체

□ 북한의 많은 해킹 단체들은 한국 정부 기관을 대상으로 APT 공격을 시도하고 있음.

北 김수키 해커그룹, ‘블루샤크’ 전술로 APT 공격 감행

입력 : 2024-10-05 20:20



LNK, ISO, MSC, HWP 등 다양한 유형의 악성파일 사용
인터뷰, 특강, 강연 의뢰로 위장해 접근 시도
원드라이브, 프로톤 드라이브 등 클라우드 통해 악성파일

[보안뉴스 김경애 기자] 2024년 상반기 동안 한국을 주요
협) 공격이 관찰된 가운데, 북한의 해커조직 김수키(Kimsu
로 APT 공격을 펼친 것으로 드러났다.

공식 거지 인증하는 북한의 APT 조직, 이제 랜섬웨어 공격까지

입력 : 2024-07-26 17:37



요약 : 보안 외신 해커뉴스에 의하면 북한의 APT 공격자들이 랜섬웨어 공격을 시작했다고 한다. 보안 업체 맨디언트(Mandiant)는 APT45라고 알려진 북한의 해킹 조직이, 기존 APT 조직들이 정부 조직이나 주요 외교 첩보들을 훔쳐내는 것에 집중하는 것과 달리 돈을 벌기 위해 랜섬웨어를 활용하여 한국, 일본, 미국의 여러 단체들을 공격하는 중이라고 발표했다. 북한 정권의 APT 운용은 다른 나라의 그것과 비교해 사뭇 다른데, 가장 큰 차이가 바로 '돈을 벌기 위해 움직인다'는 것이다. 현재 APT45는 셰터드글래스(ShatteredGlass)와 마우이(Maui)라는 랜섬웨어를 주로 활용하는 중이라고 한다.

가장 많이 본 기사 [4

- 1 [긴급] 레디스
- 2 [단독] 랜섬웨
- 3 지코스모, 카사
- 4 북한 IT노동자
- 5 업무 관련 메일
- 6 제140차 CISC
- 7 MS의 로우코
- 8 연말시즌, 해커

심각해지고 있는 APT 공격 3 : 클라우드 환경

□ 클라우드 환경을 이용한 APT 공격이 이루어지고 있음.

클라우드 스토리지 활용한 APT 공격... 경찰청부터 전세계약서까지 사칭

입력: 2024-07-25 14:13

구글 드라이브, 원드라이브, 드롭박스 활용해 악성코드 유포
 다양한 파일 포맷과 주제를 활용한 디코이 문서로 악성코드 감염 숨겨
 파일 실행 전, 파일 확장자와 포맷이 일치하는지 확인 필요

[보안뉴스 박은주 기자] 최근 구글 드라이브(Google Drive), 원드라이브(OneDrive)와 같은 클라우드 서비스를 활용한 APT 공격이 활개 치고 있다. 공격 배후가 유력하다. 정보 유출, 추가 악성코드 다운로드뿐만 아니라 감염 시스템 제어가 벌어질 수 있어 각별한 주의가 요구된다.

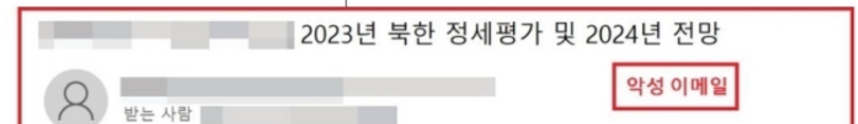
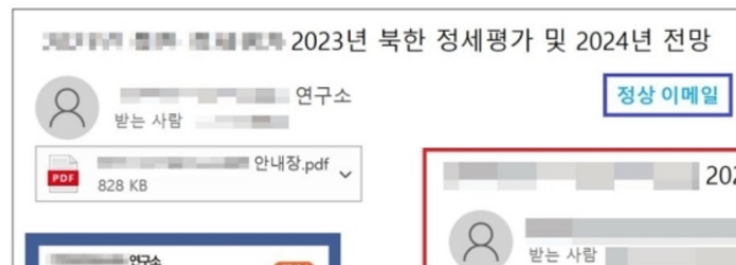
‘웨비나’ 행사 안내장 사칭 APT 공격 포착... ROKRAT 변종형 악성 파일

2024-02-06 00



전형적인 스피어 피싱 공격 기법 사용...시즌 상관없이 진행되는 일상 위협 캠페인
 바로가기(LNK) ‘파일 압축형 공격’, ‘LNK’, ‘CHM’ 등 파일 확장자 및 ‘화살표’ 포함 여부 확인

[보안뉴스 이소미 기자] ‘2023년 북한 정세 평가 및 2024년 전망’ 행사 안내장을 사칭해 문서처럼 속여 해킹 공격을 수행한 징후가 포착됐다. 공격자들은 성공률을 높이기 위해 해당 행사가 진행되기 전인 지난해 12월 28일 다음과 같이 ‘신뢰 기반 접근 전략’ 공격을 수행했다.



효율적인 APT 시뮬레이터 프레임워크 제안

An Efficient APT Simulator Framework



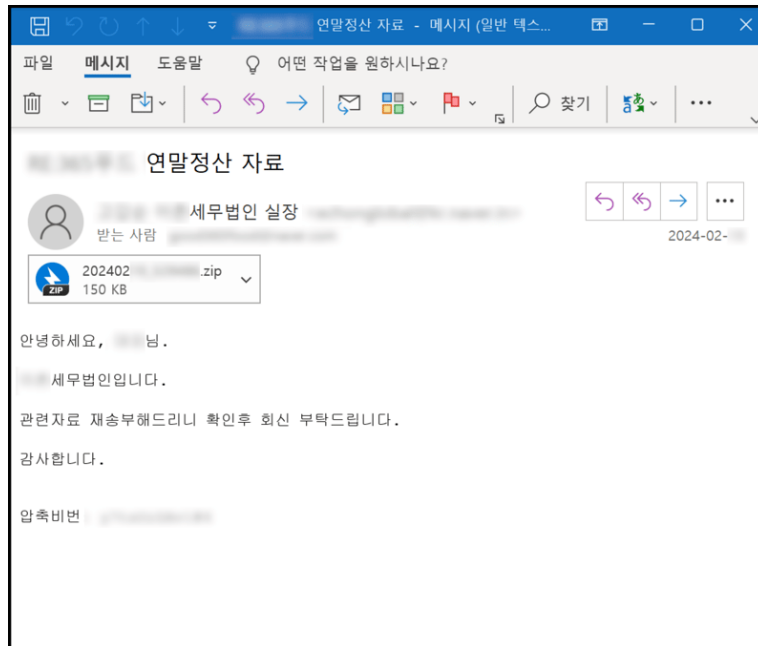
APT 시뮬레이터

서론 : 일반적인 APT 공격 과정

❑ MITRE ATT&CK 테크닉 ID

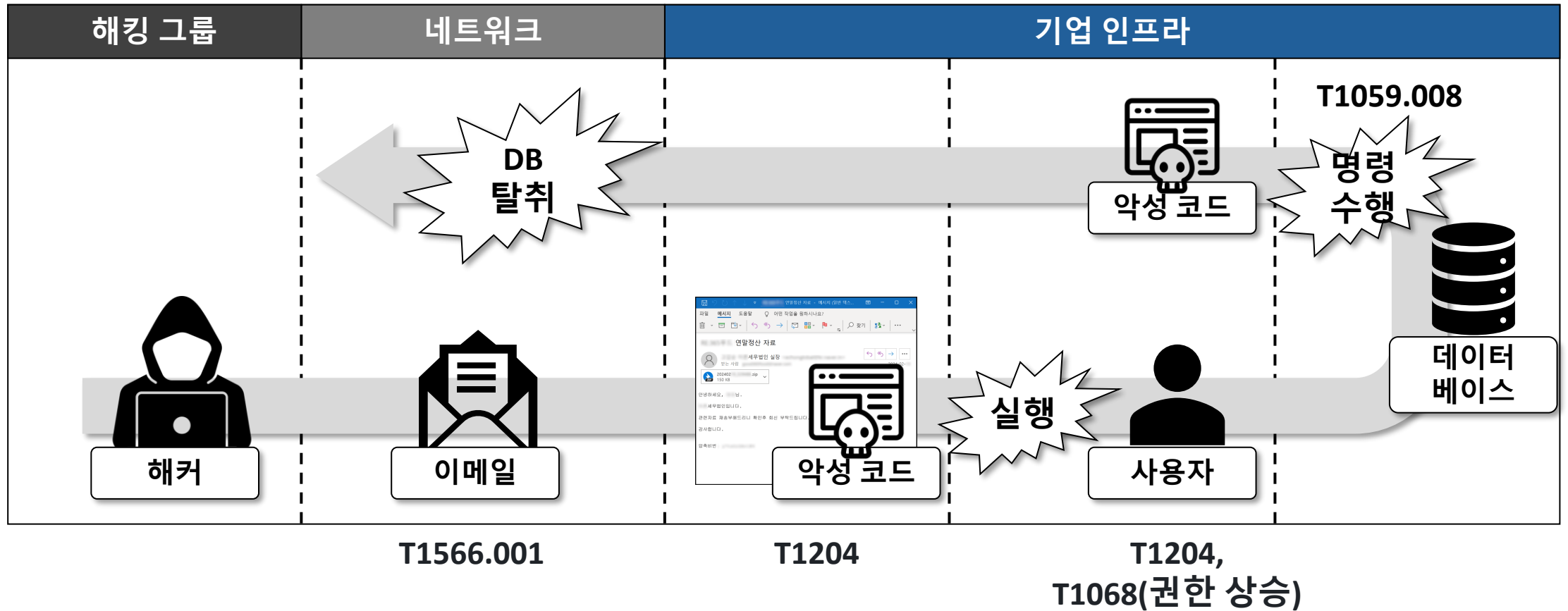
❑ T1566.001

- ❑ 공격자는 피해자 시스템에 접근 권한을 얻기 위해 악성 첨부 파일이 포함된 피싱 이메일을 보낼 수 있음.
- ❑ 첨부 파일에는 ZIP, PDF, 실행 파일 등이 포함될 수 있으며, 이를 열면 공격자가 시스템 취약점을 악용하여 시스템 권한을 획득함.



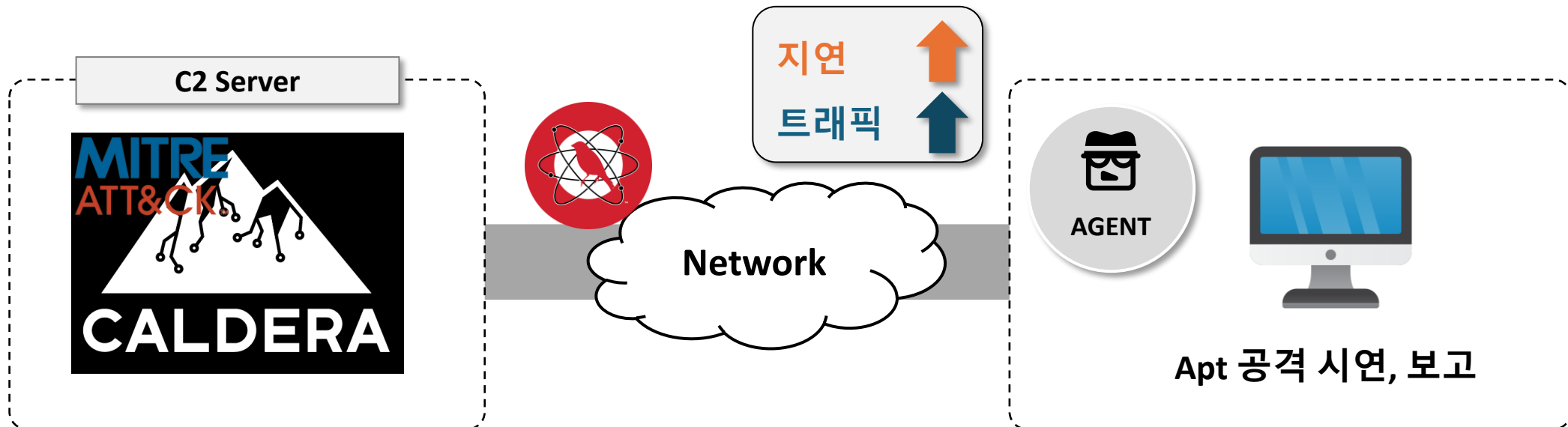
Apt 공격 시연, 보고

서론 : 일반적인 APT 공격 과정



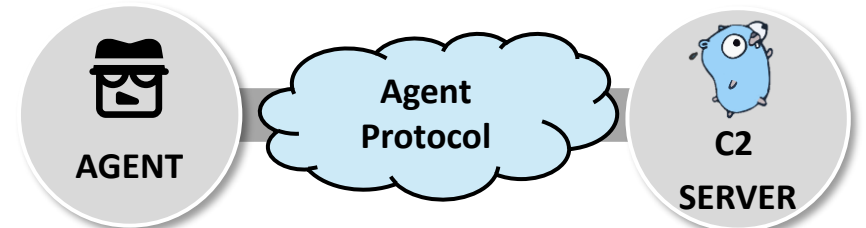
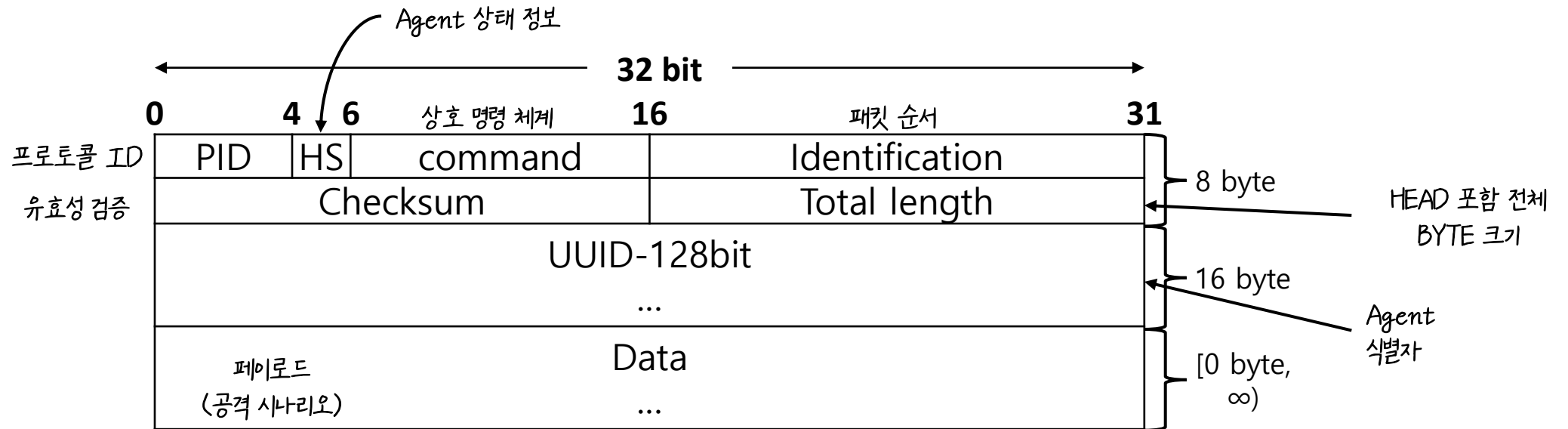
❑ CALDERA

- ❑ MITRE에서 만든 도구로, 실제 대상 PC에 설치되어 APT 공격 상황을 재현하고 조직 내 보안 취약점을 탐지하며 개선 방안을 도출함 [3].
- ❑ Atomic Red Team은 공격 시나리오를 오픈소스로 공개하며, CALDERA는 이를 사용해 대상 시스템에서 APT 공격을 재현함 [4].



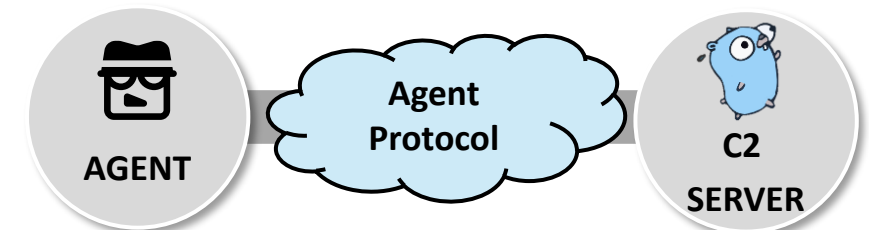
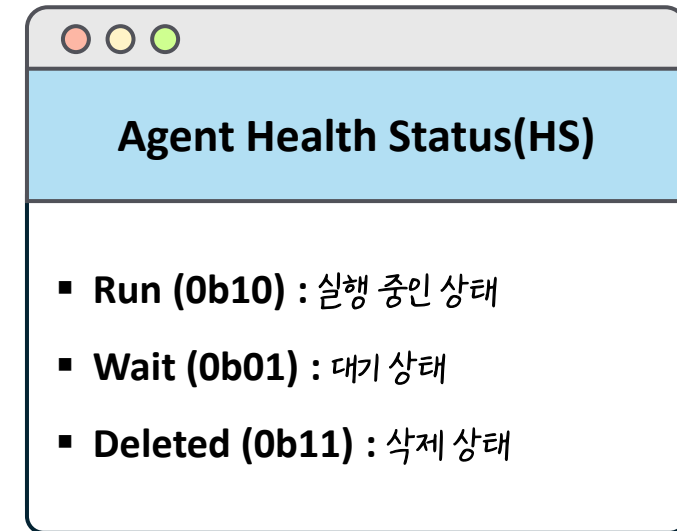
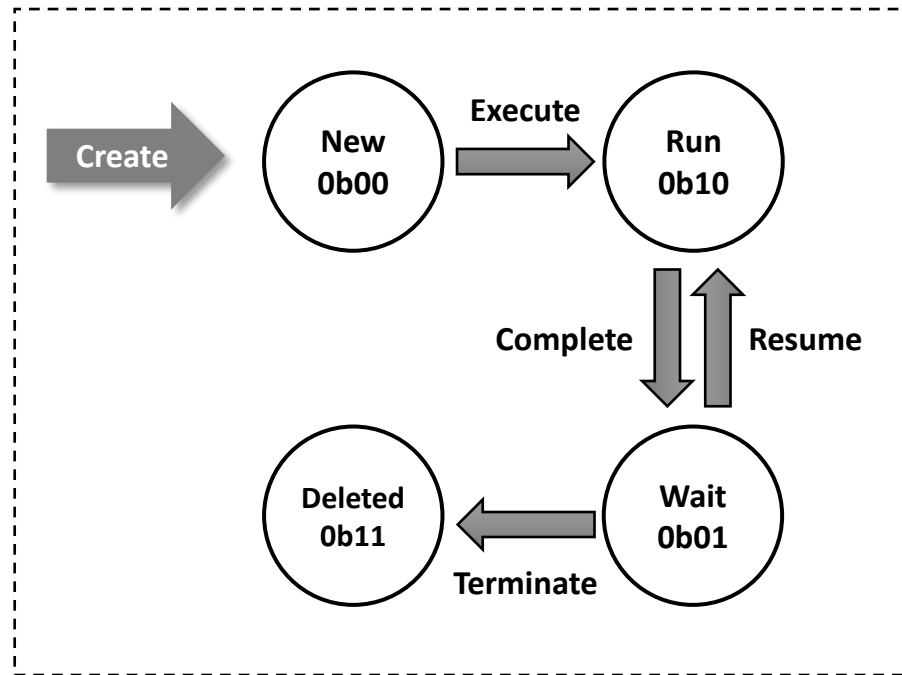
효율적인 APT 프레임워크 제안 : 프로토콜

- 새로운 APT 프레임워크와 에이전트가 소통할 수 있는 통신 언어를 제안함.
- 기존 JSON, YAML 같은 데이터 표준 포맷을 사용할 때보다 더욱 가볍고 효율적인 통신 구조를 제공함.

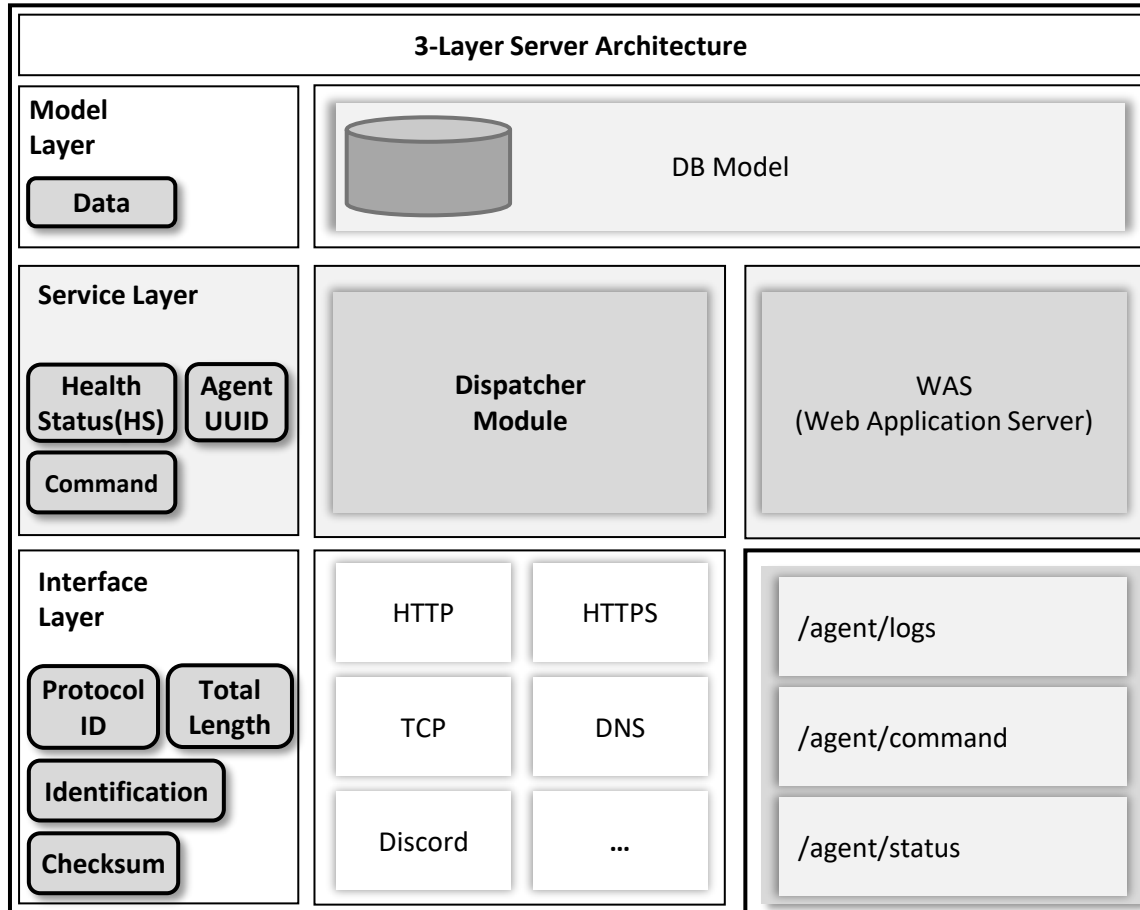


효율적인 APT 프레임워크 제안 : 프로토콜

- HS 필드는 2비트로 구성되어 있으며, 에이전트의 상태를 C2 서버에 보고함.
- 에이전트가 처음 시작될 때는 **New(0b00)** 상태로 설정됨.



효율적인 APT 프레임워크 제안 : C2 Server 아키텍처



❑ 각 레이어(Layer)에서 사용되는 필드를 기준으로 레이어를 구분함.

❑ Interface Layer

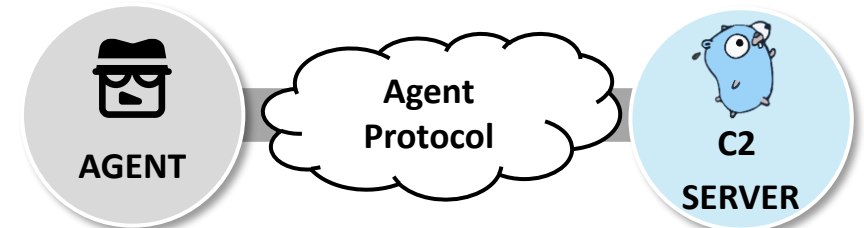
- ❑ **Protocol ID(PID)**: 통신 프로토콜을 식별.
- ❑ **Checksum**: 데이터의 무결성을 검증.
- ❑ **Identification**: 패킷의 병합 및 순서 보장.
- ❑ **TotalLength**: 헤더와 데이터를 분리 및 가공에 사용.

❑ Service Layer

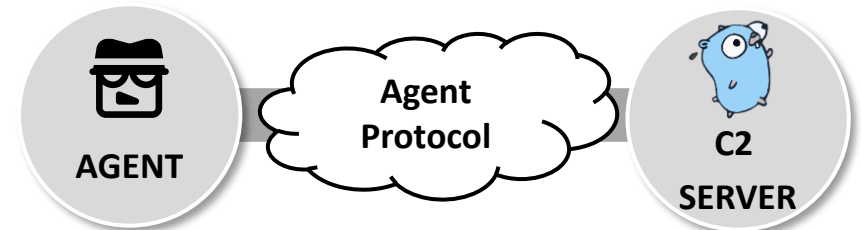
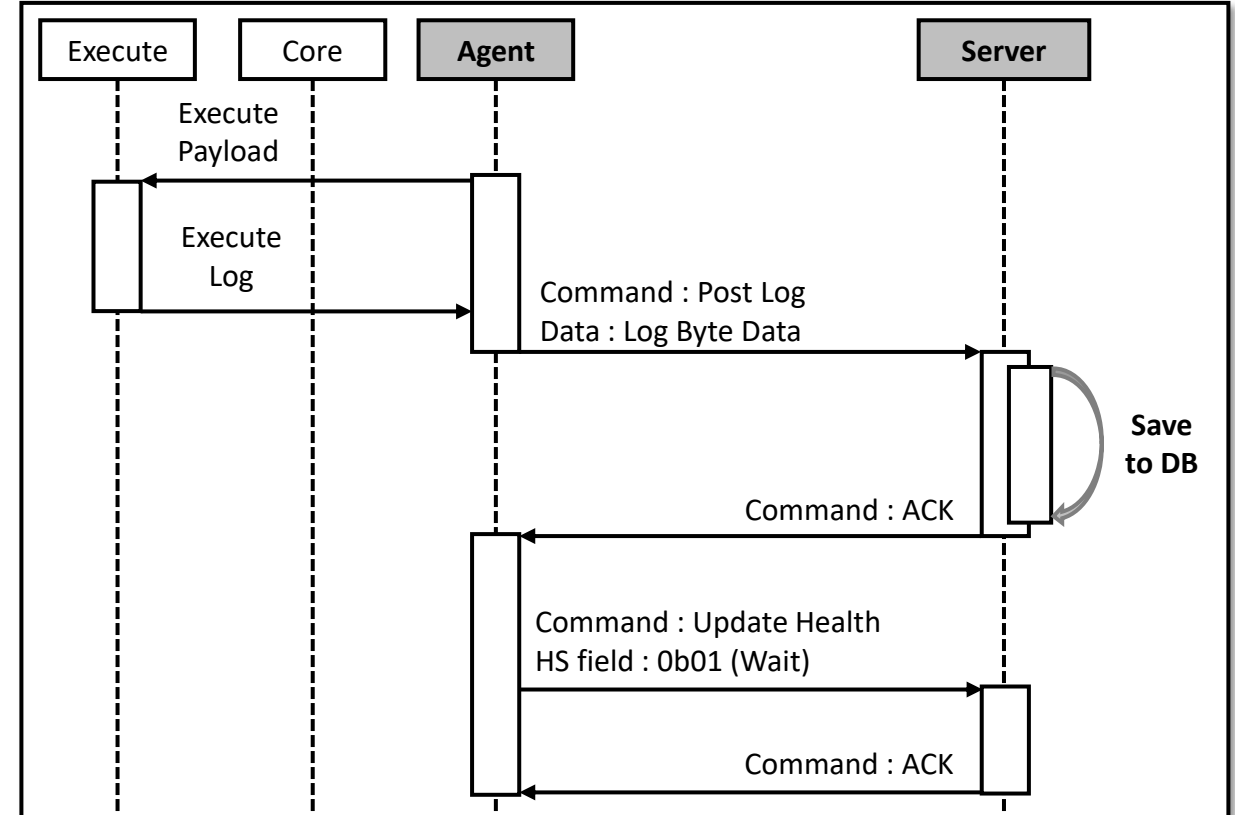
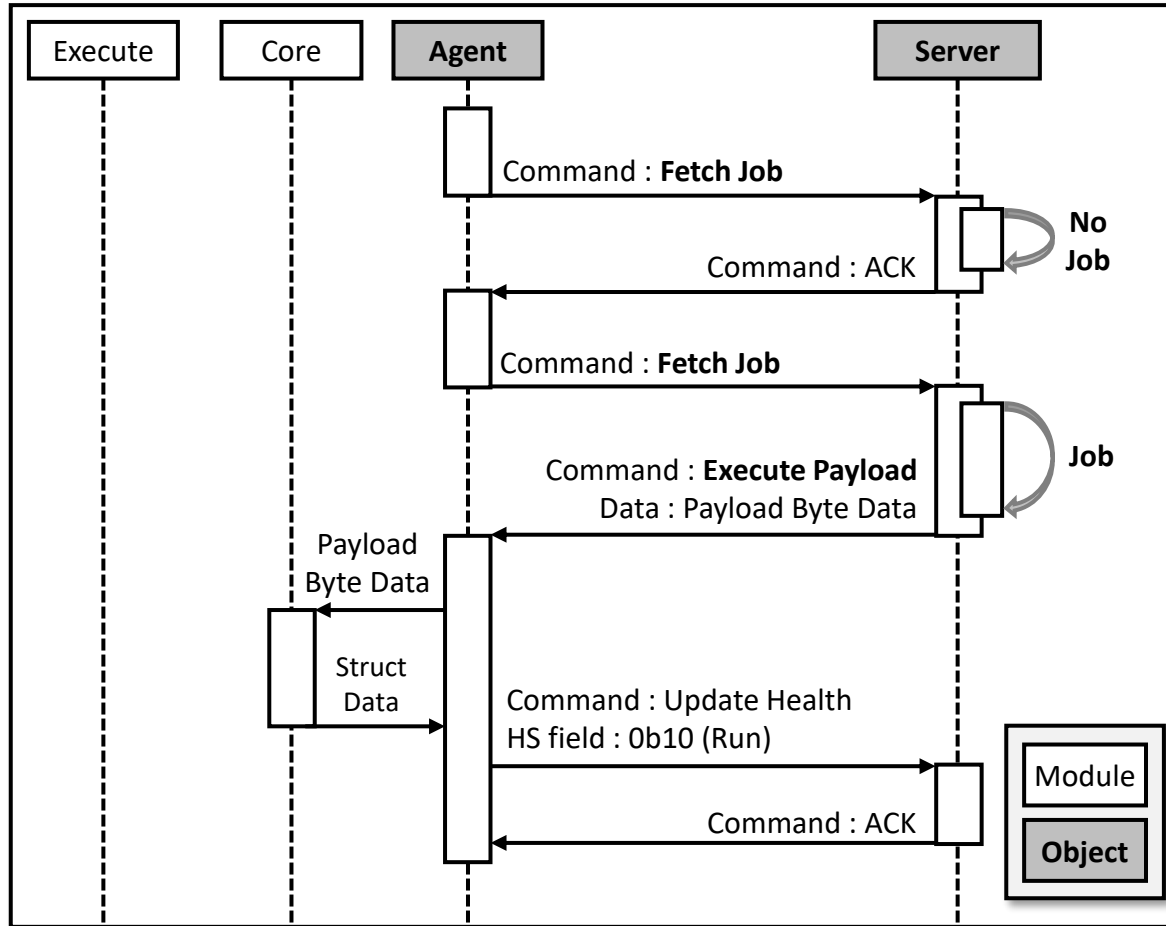
- ❑ **Agent UUID** : Agent를 식별하는데 사용.
- ❑ **Command** : 에이전트와 c2 서버 간의 상호 작용에 사용.

❑ Model Layer

- ❑ **Data 필드**: 데이터를 저장하고 처리하는데 사용.



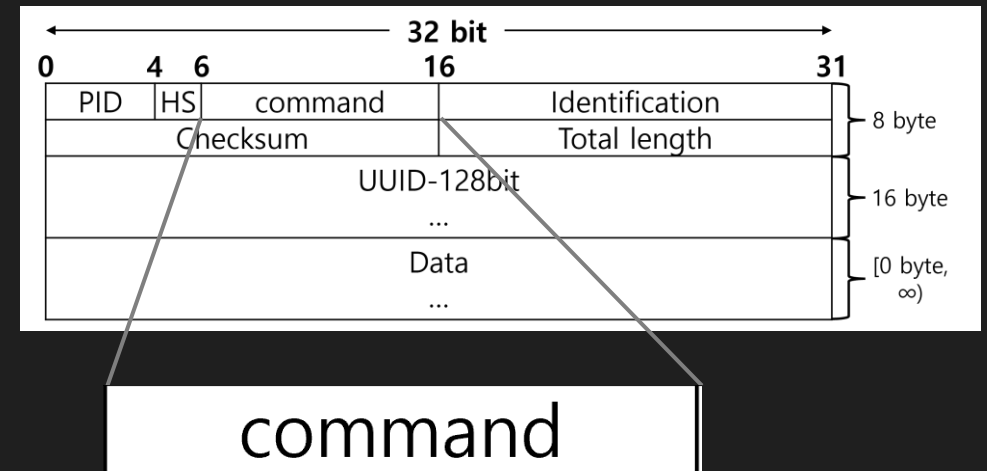
APT 프레임워크 : 에이전트 및 C2 Server 통신 과정



효율적인 APT 프레임워크 제안 : 프로토콜

Protocol Command

```
const (
    ACK COMMANDTYPE = 0b0000000000 // 0
    UPDATE_AGENT_PROTOCOL COMMANDTYPE = 0b0000000001 // 1
    UPDATE_AGENT_STATUS COMMANDTYPE = 0b0000000010 // 2
    SEND_AGENT_SYS_INFO COMMANDTYPE = 0b0000000011 // 3
    ERROR_ACK COMMANDTYPE = 0b0000000100 // 4
    SEND_AGENT_APP_INFO COMMANDTYPE = 0b0000000101 // 5
    FETCH_INSTRUCTION COMMANDTYPE = 0b0000000110 // 6
    SEND_PROCEDURE_LOG COMMANDTYPE = 0b0000000111 // 7
    GET_APPLICATION COMMANDTYPE = 0b0000001000 // 8
    GET_SYSTEMINFO COMMANDTYPE = 0b0000001001 // 9
    EXECUTE_PAYLOAD COMMANDTYPE = 0b0000001010 // 10
    EXECUTE_CLEANUP COMMANDTYPE = 0b0000001011 // 11
)
```

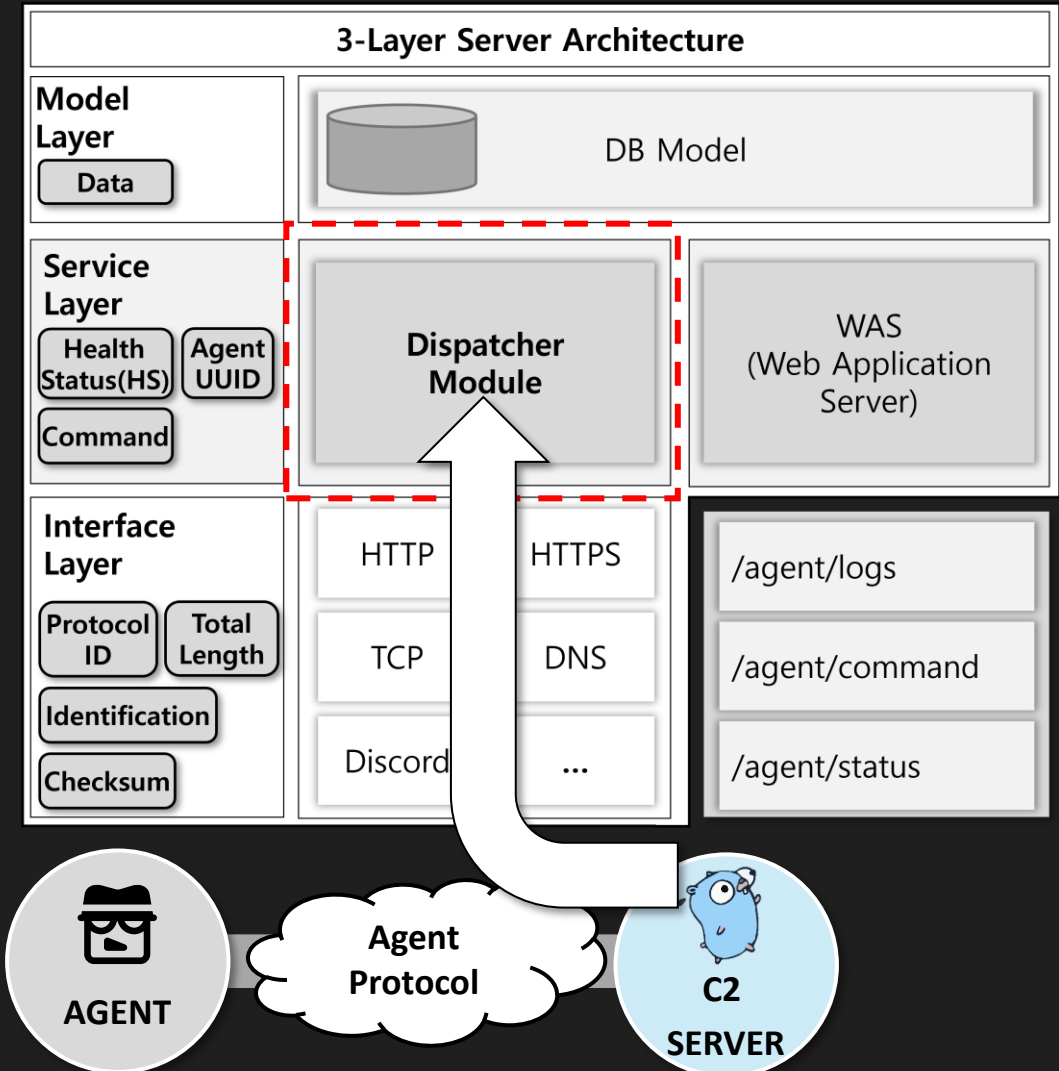


효율적인 APT 프레임워크 제안 : C2 Server 아키텍처

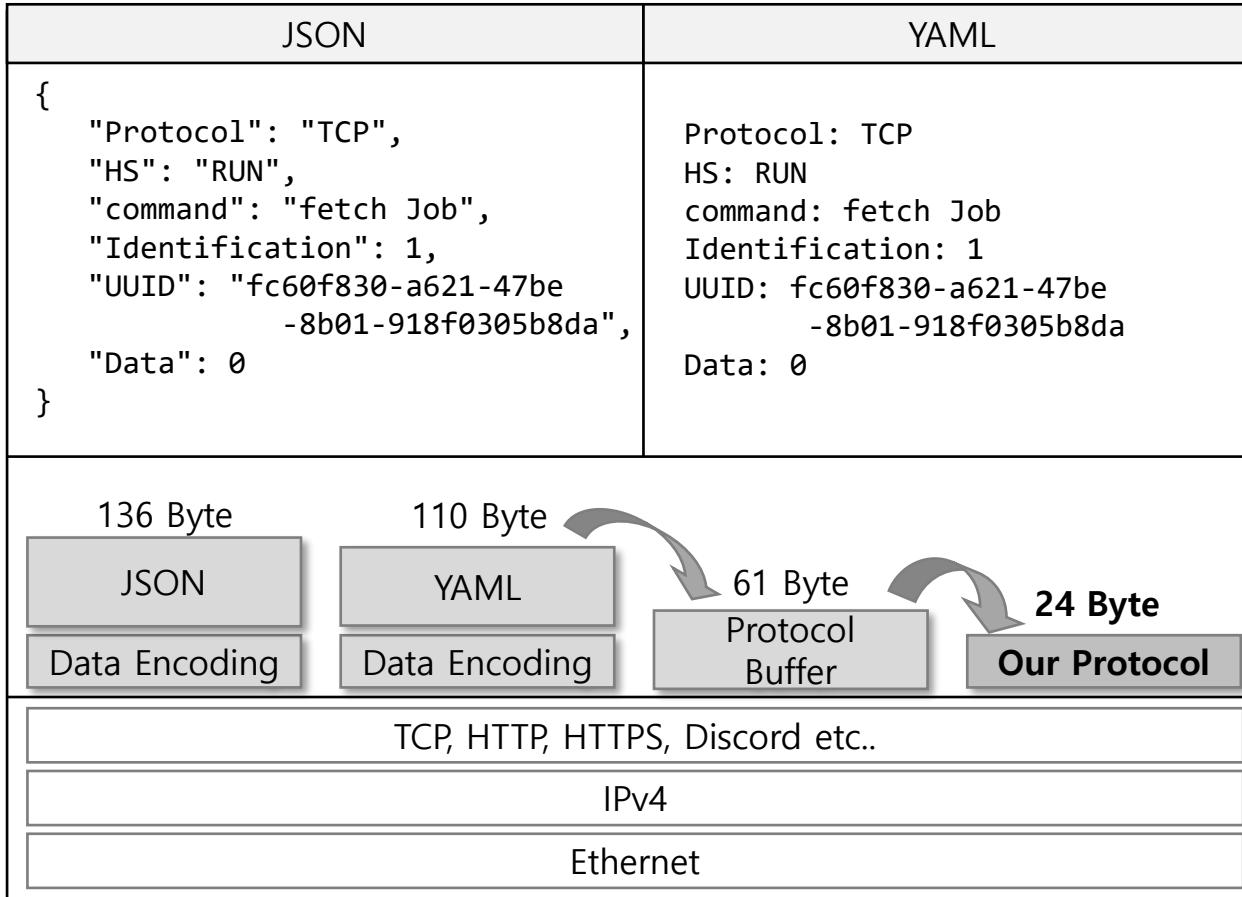
```
func (cd *CommandDispatcher) Action(hs
*HSProtocol.HS)
    (*HSProtocol.HS, error) {
    switch hs.Command {
    case HSProtocol.UPDATE_AGENT_PROTOCOL:
        return UPDATE_AGENT_PROTOCOL(hs)
    case HSProtocol.UPDATE_AGENT_STATUS:
        return UPDATE_AGENT_STATUS(hs)
    case HSProtocol.SEND_AGENT_SYS_INFO:
        return SEND_AGENT_SYS_INFO(hs)
    case HSProtocol.ERROR_ACK:
        break // 예약
    case HSProtocol.SEND_AGENT_APP_INFO:
        return SEND_AGENT_APP_INFO(hs)
    case HSProtocol.FETCH_INSTRUCTION:
        return FETCH_INSTRUCTION(hs)
    case HSProtocol.SEND_PROCEDURE_LOG:
        return SEND_PROCEDURE_LOG(hs)
    }

    return nil, fmt.Errorf("Invalid Command")
}
```

Service
Layer :
Dispatcher
Module



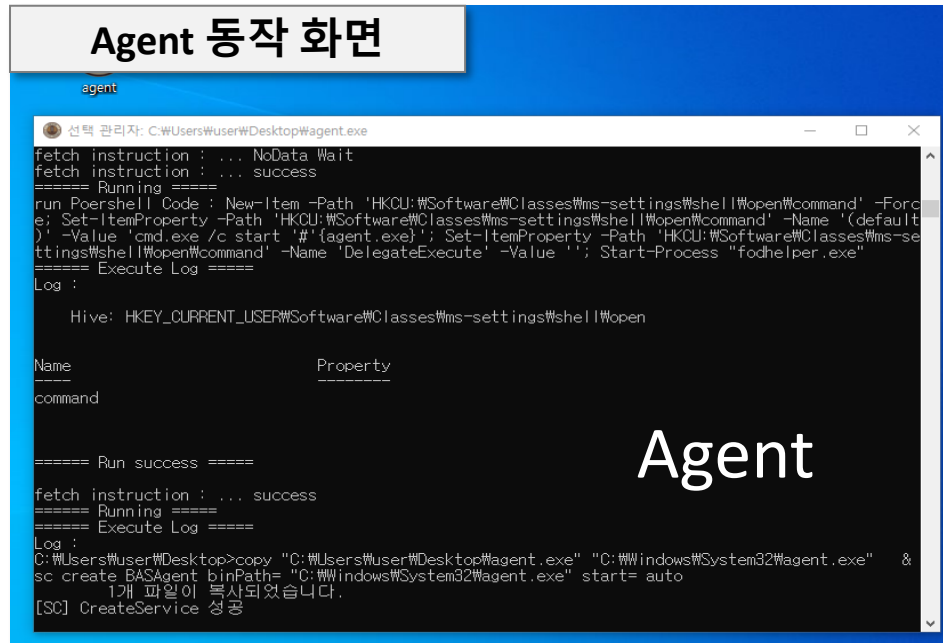
효율적인 APT 프레임워크 제안



- 제안된 Agent 프로토콜은 다른 데이터 표준 포맷과 비교했을 때 더 높은 데이터 전송 효율을 보여줌.
- Agent와 C2 서버 간 통신에 필요한 필수 요소만 포함하여 데이터 교환을 효율적으로 설계함.
- 이를 통해 더욱 낮은 데이터 크기로 통신이 가능함.

- 제안된 Agent 프로토콜은 다른 데이터 표준 포맷과 비교했을 때 더 높은 데이터 전송 효율을 제공함.
- Agent와 C2 서버 간 통신에 필요한 필수 요소만 포함하여 설계되었으며, 이를 통해 데이터 크기를 최소화하고 통신을 더욱 효율적으로 수행할 수 있음.

Agent 동작 화면



```
agent
선택 관리자: C:\Users\user\Desktop\agent.exe
fetch instruction : ... NoData Wait
fetch instruction : ... success
===== Running =====
run Powershell Code : New-Item -Path 'HKCU:\Software\Classes\ms-settings\shell\open\command' -Force; Set-ItemProperty -Path 'HKCU:\Software\Classes\ms-settings\shell\open\command' -Name '(default)' -Value 'cmd.exe /c start "#\{agent.exe}"; Set-ItemProperty -Path 'HKCU:\Software\Classes\ms-settings\shell\open\command' -Name 'DelegateExecute' -Value ''; Start-Process "fodhelper.exe"
===== Execute Log =====
Log :
Hive: HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open

Name      Property
-----
command

===== Run success =====
fetch instruction : ... success
===== Running =====
===== Execute Log =====
Log :
C:\Users\user\Desktop>copy "C:\Users\user\Desktop\agent.exe" "C:\Windows\System32\agent.exe" &
sc create BASAgent binPath= "C:\Windows\System32\agent.exe" start= auto
1개 파일이 복사되었습니다.
[SC] CreateService 성공
```

QnA

- [1] 장성우, 인용준, APT(Advanced Persistent Threat) 공격 시나리오 검증 시스템 연구, 한국산학기술학회, Apr, 2023.
- [2] A. Dabit, O. A. Al-Haija, M. Al-Fayoumi, Identifying Weaknesses: A Guide to Conducting an Vulnerability Effective Network Assessment, International Arab Conference on Technology (ACIT), Dec, 2023.
- [3] Information N. Mohamed, Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework, Sep, 2022.
- [4] M. Okuma et al., Automated Mapping Method for Sysmon Logs to ATT&CK Techniques by Leveraging Atomic Red Team, International Conference on Signal Processing and Information Security (ICSPIS), pp.104-109, Nov, 2023.
- [5] A. Dorri, S. S. Kanhere and R. Jurdak, Multi-Agent Systems: A Survey, IEEE Access, vol.6, pp.28573-28593, Apr, 2018.
- [6] D. C. Castillo, J. Rosales and G.-A. T. Balnco, Optimizing Binary Serialization with an Independent Data Definition Format, International Journal of Computer Applications, vol.180, no.28, Mar, 2018.
- [7] A. Sidhardhan, S. Keerthana and J.-M. Kannimoola, Weaponizing Real-world Applications Control), as C2 (Command and International Innovative Data Conference on Communication Technologies and Application (ICIDCA), pp.458-463, Mar, 2023.
- [8] M. Suliman and B. Alluhaybi, Protecting Mobile Agent against Man-In-TheMiddle Attack: The Dummy Agent Model, The International Journal of Advanced Networking and Applications (IJANA), vol.13, no.04, pp.5024-5028, Mar, 2022.