타겟형 워터링홀 공격, 그리고

KISA의 사이버 위협 헌팅

K-CTI 2022
2022 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

AGENDA

1. Target watering hole attack
    - Analysis of target watering hole attack.
    - Attribution

2. Cyber Threat Hunting
    - Threat Hunting

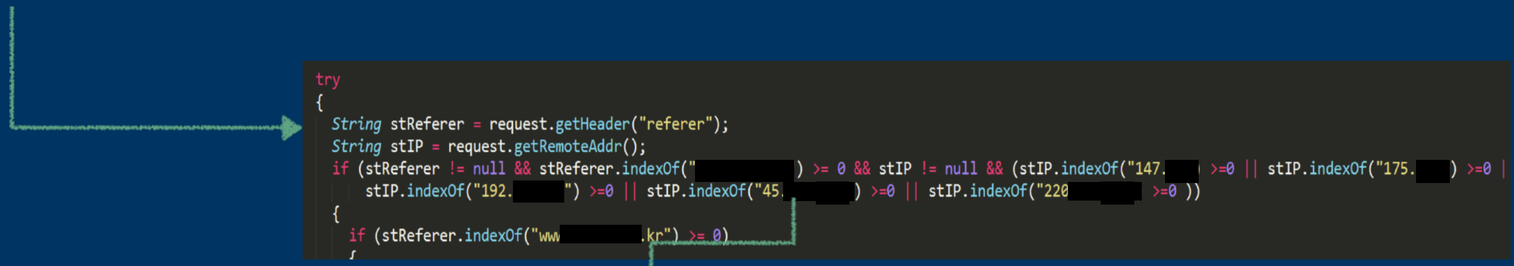
ANALYSIS OF TARGET WATERING HOLE ATTACK

Web Site

국내 특정 사이트 방문시 다른 사이트로 연결 되도록 악성 스크립트 삽입 확인

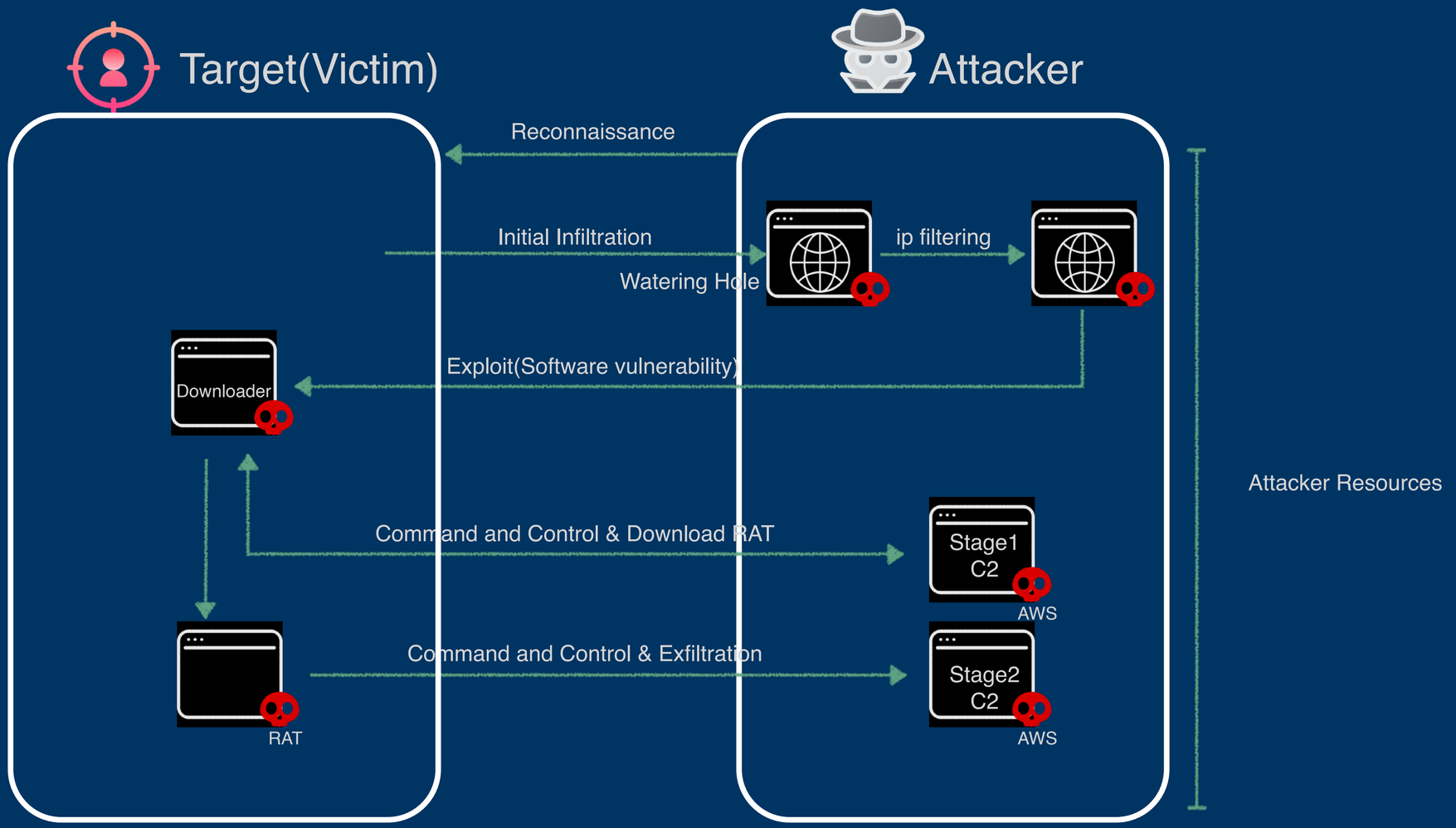
연결된 사이트에서 아이피 필터링 후 추가 페이지로 연결

취약점을 통한 악성코드 다운로드(감염) 및 실행



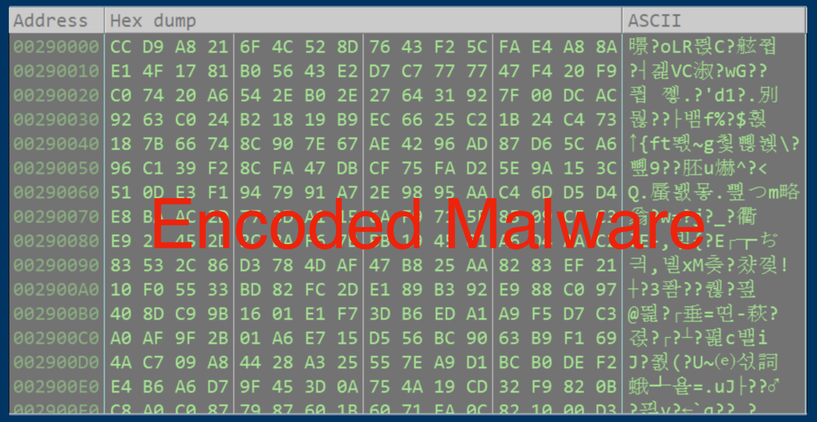
공격 대상 기업

ANALYSIS OF TARGET WATERING HOLE ATTACK

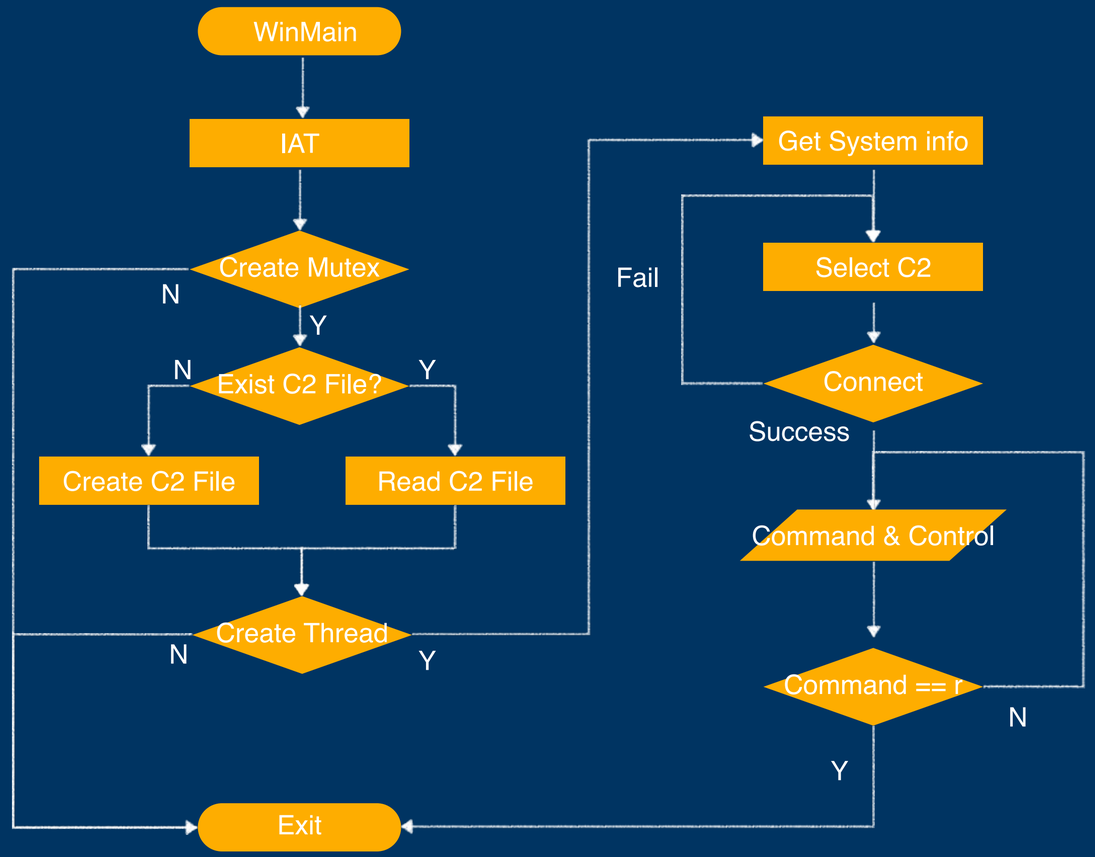


ANALYSIS OF TARGET WATERING HOLE ATTACK

Path : C:\users\public\iexplore.exe



ANALYSIS OF TARGET WATERING HOLE ATTACK

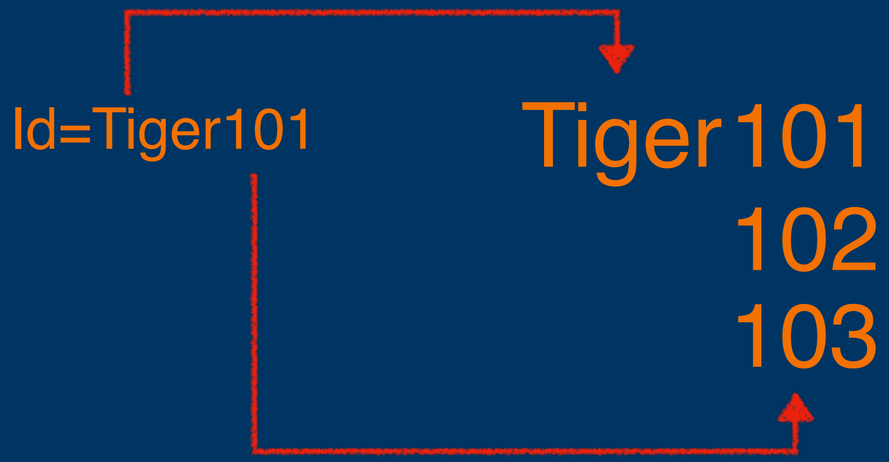


C2 File	lnk{22A98A71-67ED-40BB-A5F4-8CCAF6BFA6EB}.tmp
IAT, String	Base64 : A-Za-z0-9+/= + RC4 Algorithm(key : 0123456789ABCEDF)
C2 Communicate	Base64 : A-Za-z0-9#$=

Command & Control

Command	Description	Request ID
o	Cmd Command	Tiger102
p	Upload File	Tiger102, Tiger103
q	Download File	Tiger102
r	Terminate Thread	Tiger102
s	Update C2	Tiger102

ANALYSIS OF TARGET WATERING HOLE ATTACK



Send System info

Command Result (OK , Error…)

File Upload

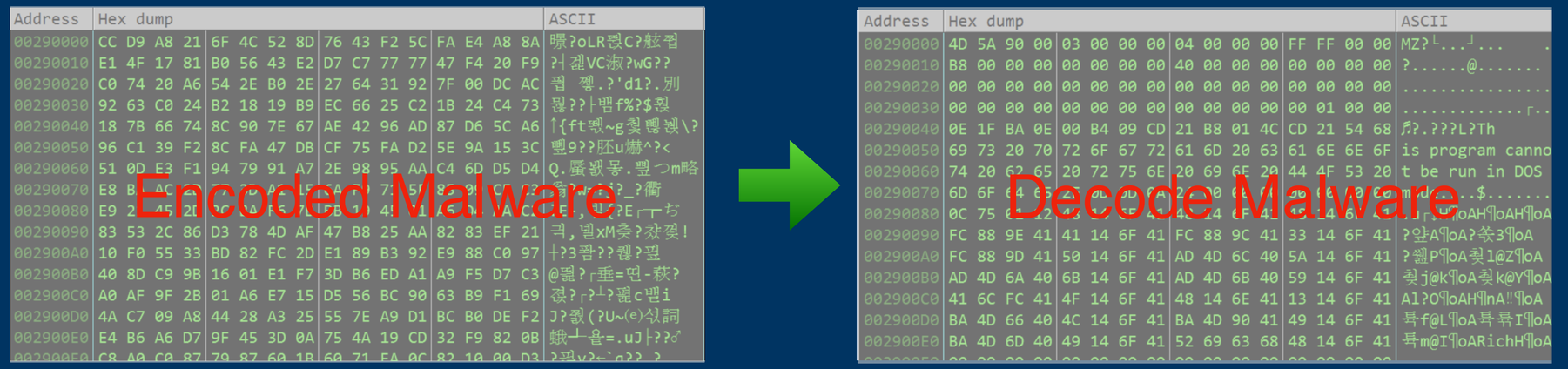
ANALYSIS OF TARGET WATERING HOLE ATTACK

Operation ByteTiger

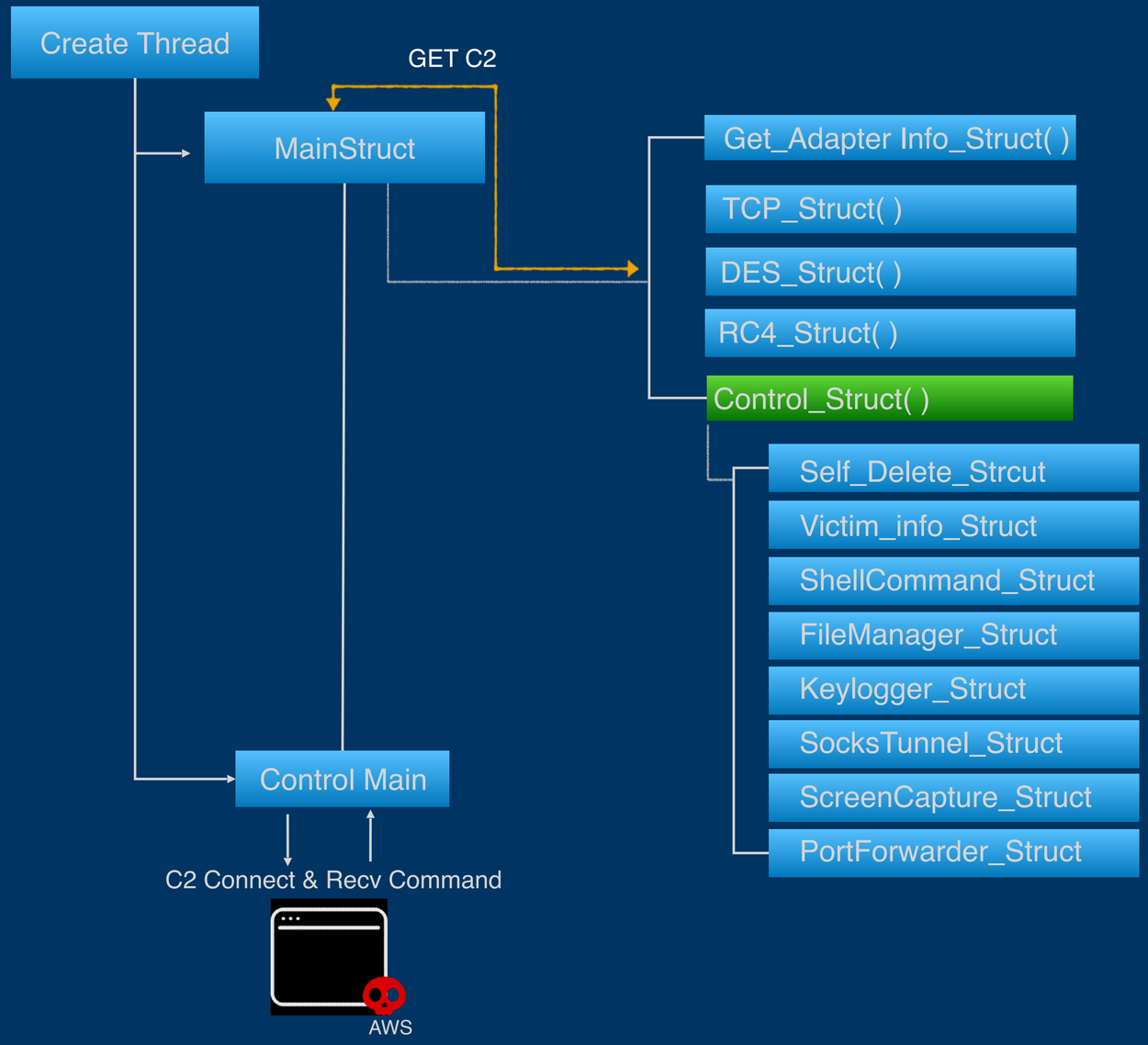
Id=Tiger101 Tiger101 Send System info

ANALYSIS OF TARGET WATERING HOLE ATTACK

TigerRAT - ASDCli.exe



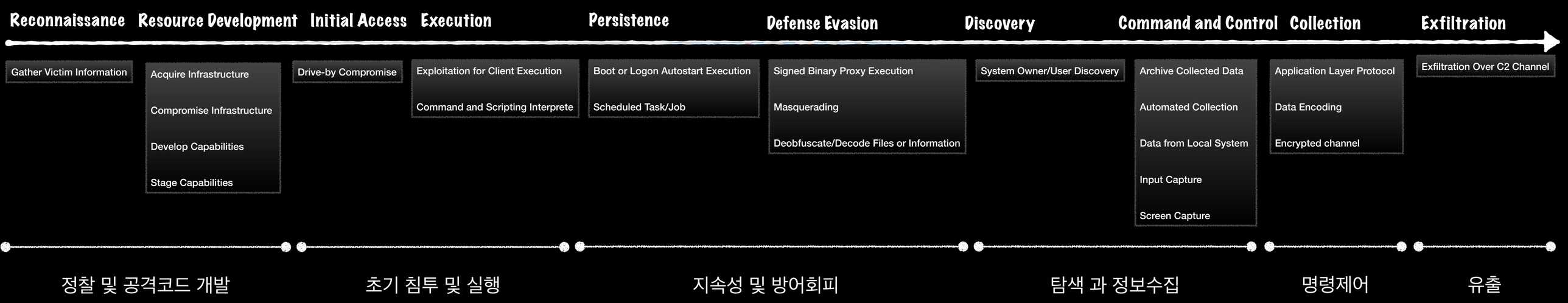
ANALYSIS OF TARGET WATERING HOLE ATTACK



CYBER THREAT HUNTING

THREAT HUNTING BEFORE RISK

CYBER THREAT HUNTING



정찰 및 공격코드 개발 | 초기 침투 및 실행 | 지속성 및 방어회피 | 탐색 과 정보수집 | 명령제어 | 유출

CYBER THREAT HUNTING

THANK YOU

Taewoo lee / KrCert