

# 타겟형 워터링홀 공격, 그리고

KISA의 사이버 위협 헌팅

# 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

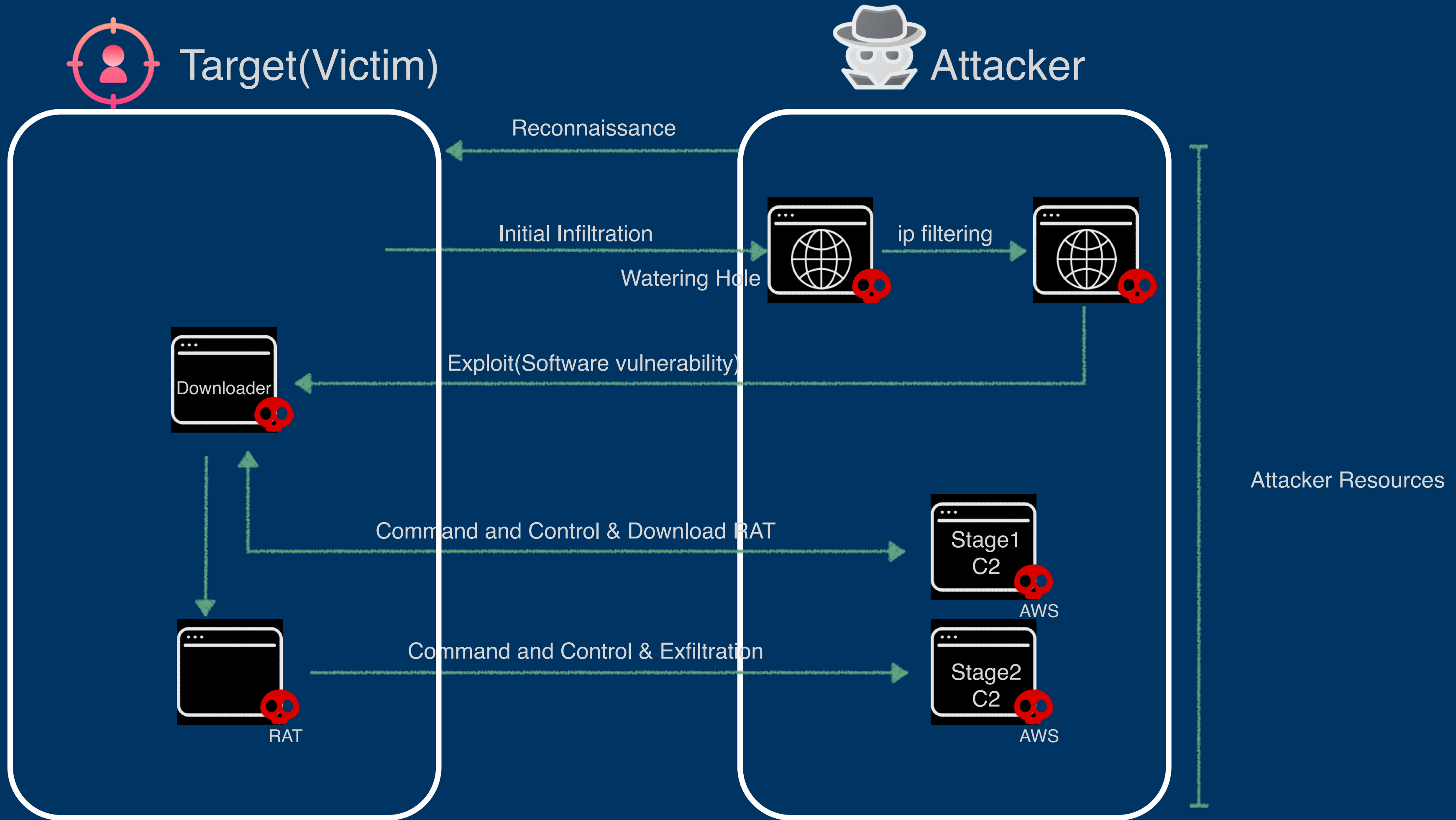
연결된 사이트에서 아이피 필터링 후 추가 페이지로 연결

취약점을 통한 악성코드 다운로드(감염) 및 실행

```
try
{
String stReferer = request.getHeader("referer");
String stIP = request.getRemoteAddr();
if (stReferer != null && stReferer.indexOf(" ") >= 0 && stIP != null && (stIP.indexOf("147. ") >= 0 || stIP.indexOf("175. ") >= 0 |
stIP.indexOf("192. ") >= 0 || stIP.indexOf("45. ") >= 0 || stIP.indexOf("220 ") >= 0 ))
{
if (stReferer.indexOf("www. ".kr") >= 0)
{
```

공격 대상 기업

# ANALYSIS OF TARGET WATERING HOLE ATTACK

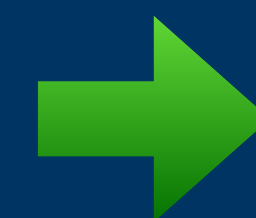


# ANALYSIS OF TARGET WATERING HOLE ATTACK

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

Address	Hex dump	ASCII
00290000	CC D9 A8 21 6F 4C 52 8D 76 43 F2 5C FA E4 A8 8A	暻?oLR뵡C?絃뵡
00290010	E1 4F 17 81 B0 56 43 E2 D7 C7 77 77 47 F4 20 F9	? 뵡VC淑?wG??
00290020	C0 74 20 A6 54 2E B0 2E 27 64 31 92 7F 00 DC AC	뵡 뵡.'d1?.別
00290030	92 63 C0 24 B2 18 19 B9 EC 66 25 C2 1B 24 C4 73	뵡??+뵡f%?\$뵡
00290040	18 7B 66 74 8C 90 7E 67 AE 42 96 AD 87 D6 5C A6	↑{ft뵡~g뵡뵡뵡\?
00290050	96 C1 39 F2 8C FA 47 DB CF 75 FA D2 5E 9A 15 3C	뵡9??胚u뵡^?<
00290060	51 0D E3 F1 94 79 91 A7 2E 98 95 AA C4 6D D5 D4	Q.뵡뵡뵡.뵡뵡뵡m略
00290070	E8 B1 AC 21 7D A2 1F 5A 71 71 57 87 01 C1 72	뵡뵡뵡뵡?_뵡
00290080	E9 21 45 21 2C 0A F5 7E FB 11 41 11 A5 01 A C	뵡뵡,뵡?E 뵡뵡
00290090	83 53 2C 86 D3 78 4D AF 47 B8 25 AA 82 83 EF 21	크,뵡xM뵡?뵡뵡!
002900A0	10 F0 55 33 BD 82 FC 2D E1 89 B3 92 E9 88 C0 97	+??뵡뵡?뵡?뵡
002900B0	40 8D C9 9B 16 01 E1 F7 3D B6 ED A1 A9 F5 D7 C3	@뵡?r垂=뵡-萩?
002900C0	A0 AF 9F 2B 01 A6 E7 15 D5 56 BC 90 63 B9 F1 69	뵡?r?+?뵡c뵡뵡i
002900D0	4A C7 09 A8 44 28 A3 25 55 7E A9 D1 BC B0 DE F2	J?뵡(?U~(e)뵡뵡詞
002900E0	E4 B6 A6 D7 9F 45 3D 0A 75 4A 19 CD 32 F9 82 0B	蛾-뵡=뵡.uJ ??뵡
002900E8	C8 A0 C0 87 79 87 60 1B 60 71 EA 0C 82 10 00 D3	?뵡v?뵡=뵡?? ?

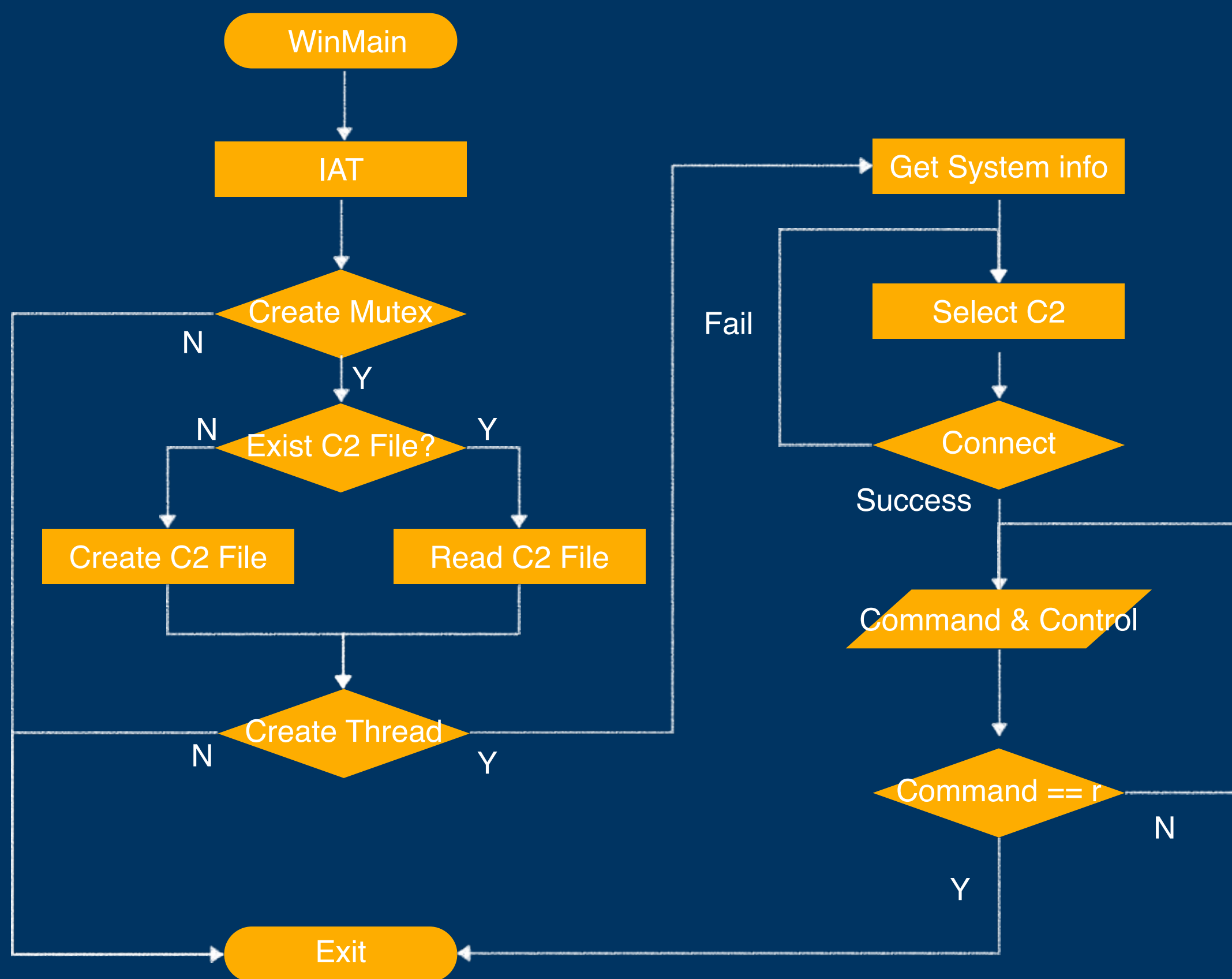
Encoded Malware



Address	Hex dump	ASCII
00290000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?L...J... .
00290010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....
00290020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00290030	00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00	.....r..
00290040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	뵡?.???L?Th
00290050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00290060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00290070	6D 6F 64 65 20 2D 0D 0A 20 00 00 00 00 00 00 00	Command...\$.....
00290080	0C 75 01 12 03 00 00 00 00 00 00 00 00 00 00 00	뵡뵡뵡뵡oAH뵡oAH뵡oA
00290090	FC 88 9E 41 41 14 6F 41 FC 88 9C 41 33 14 6F 41	?뵡A뵡oA?뵡3뵡oA
002900A0	FC 88 9D 41 50 14 6F 41 AD 4D 6C 40 5A 14 6F 41	?뵡뵡P뵡oA뵡1@Z뵡oA
002900B0	AD 4D 6A 40 6B 14 6F 41 AD 4D 6B 40 59 14 6F 41	뵡j@k뵡oA뵡k@Y뵡oA
002900C0	41 6C FC 41 4F 14 6F 41 48 14 6E 41 13 14 6F 41	A1?O뵡oAH뵡nA!!뵡oA
002900D0	BA 4D 66 40 4C 14 6F 41 BA 4D 90 41 49 14 6F 41	뵡f@L뵡oA뵡뵡I뵡oA
002900E0	BA 4D 6D 40 49 14 6F 41 52 69 63 68 48 14 6F 41	뵡m@I뵡oARichH뵡oA
002900E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Decode Malware

# ANALYSIS OF TARGET WATERING HOLE ATTACK



C2 File

Ink{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



# ANALYSIS OF TARGET WATERING HOLE ATTACK

## Operation ByteTiger

Id=Tiger101

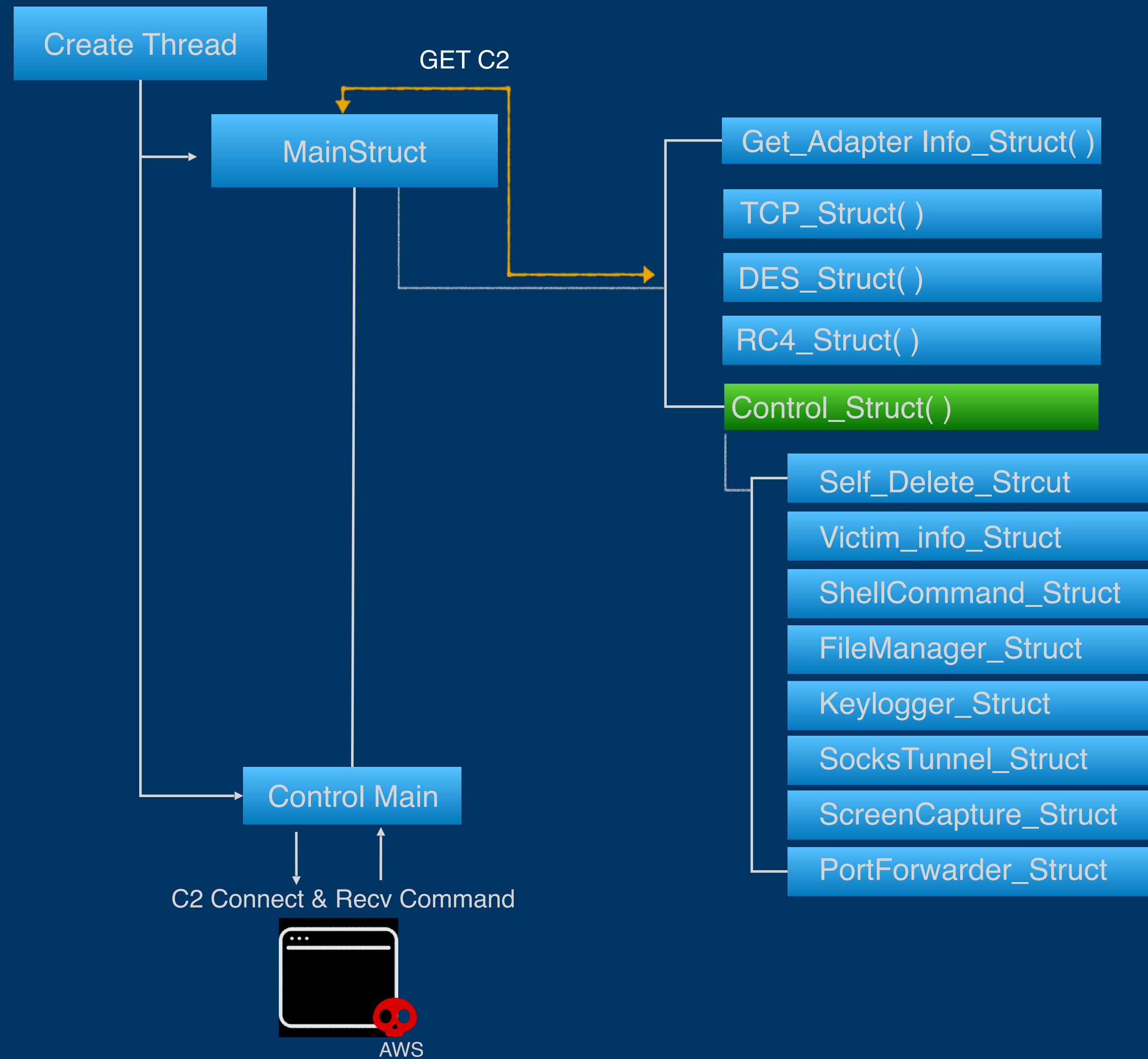
Tiger101

Send System info





# ANALYSIS OF TARGET WATERING HOLE ATTACK



# **CYBER THREAT HUNTING**

**CYBER THREAT HUNTING**

**THREAT HUNTING BEFORE RISK**

# CYBER THREAT HUNTING



# CYBER THREAT HUNTING

Result



Hunting

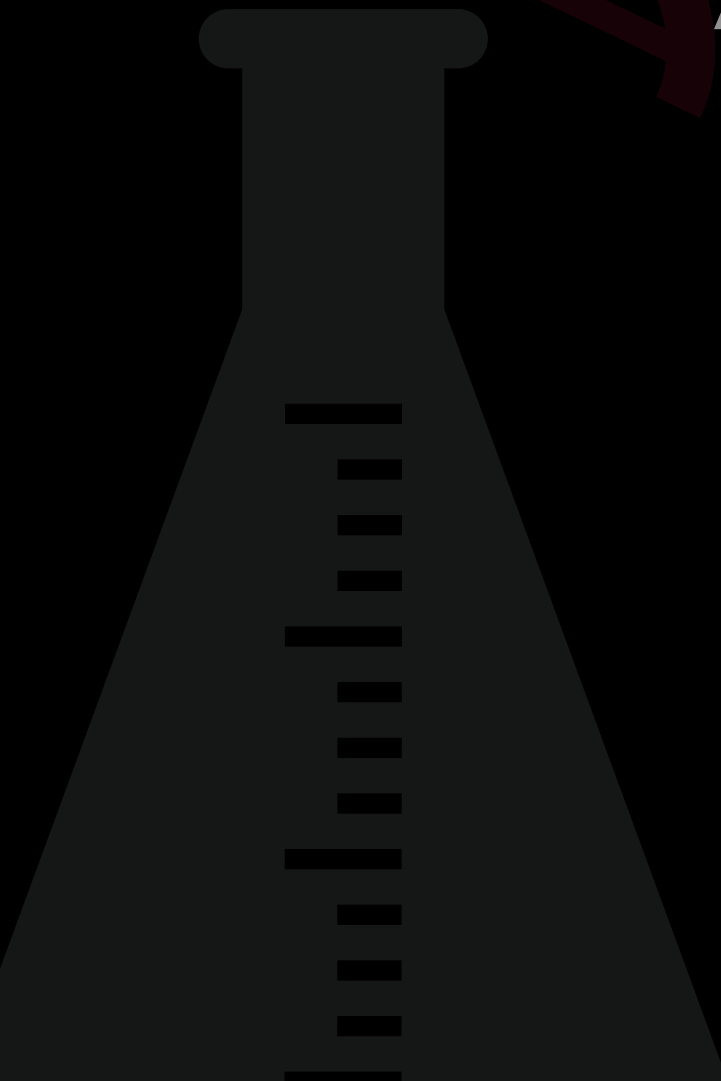
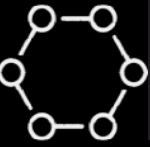


THREAT HUNTING

Analyzing ( Analyst)



Analyzing ( System)



**THANK YOU**

Tâewoo lee / KrCert