RANSOMWARE

- scp겨울 프로젝트 1차 중간발표 -

2주간 나는

프로젝트 진행도

중부대 정보보호학과 | 91913622 송태현

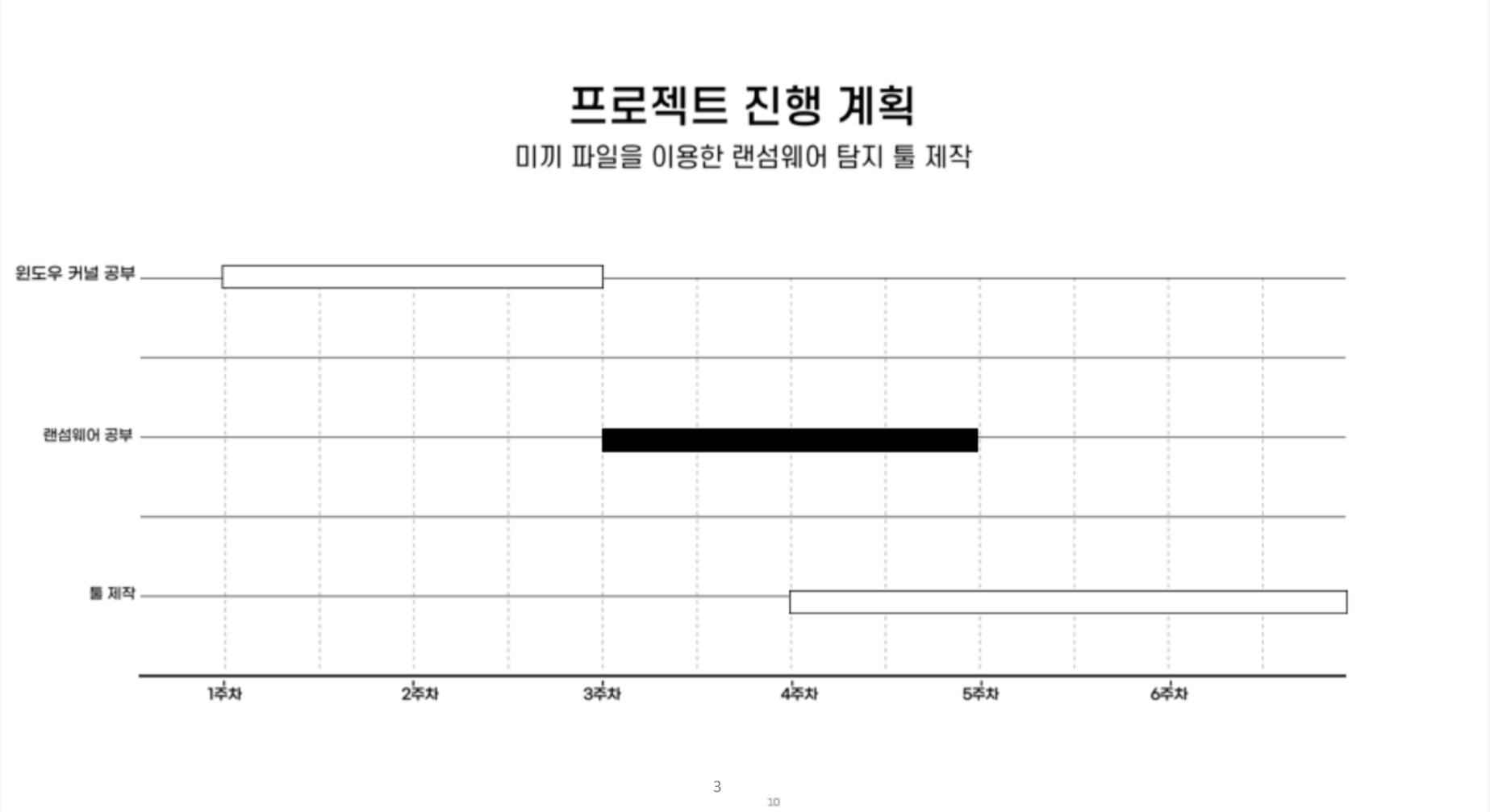
RANSOMWARE

CONTENTS

01

전체 구상도

저번주에 잠시 보여드렸던 프로젝트의 큰 그림입니다.



Q

그렇다면 2주가
지난 우리 팀은 어떻게
진행을 했을까
?

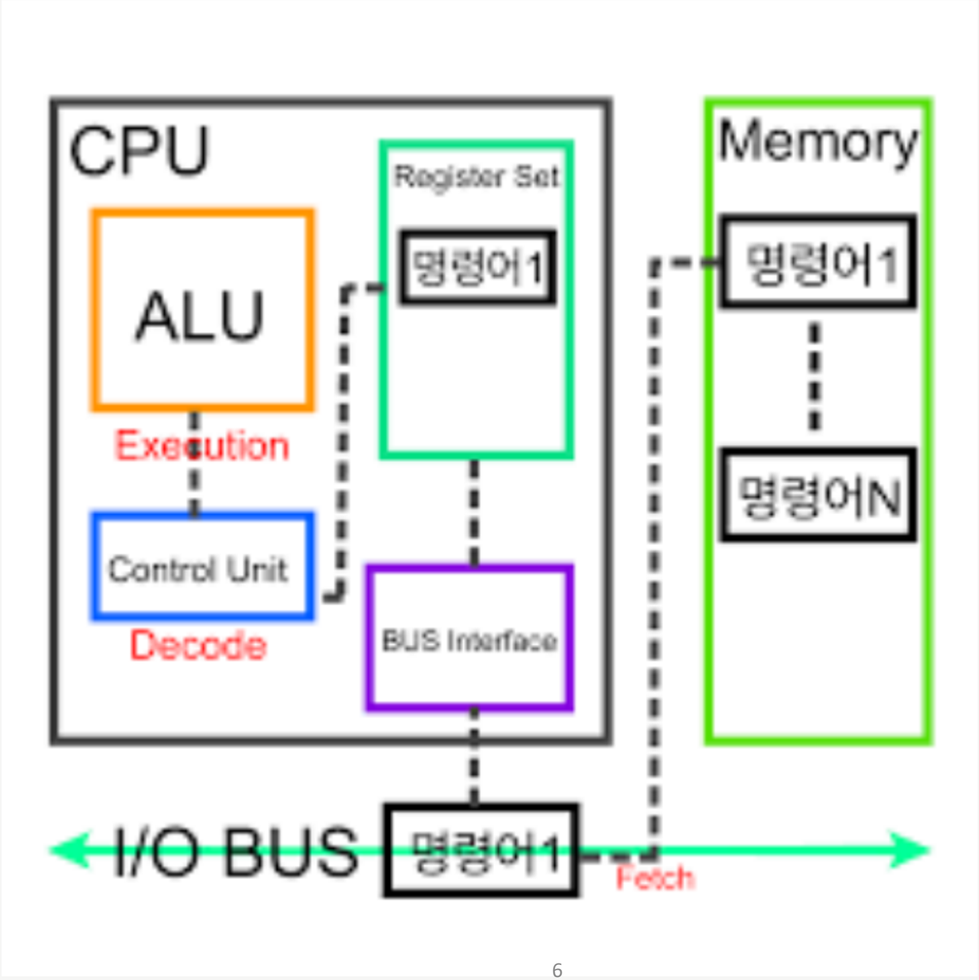
02

현재 진행도

- 윈도우 시스템 프로그래밍으로 기초 적인 컴퓨터 구조 공부
- 윈도우10 , 각종 툴들과 같은 기본 실습환경 구축

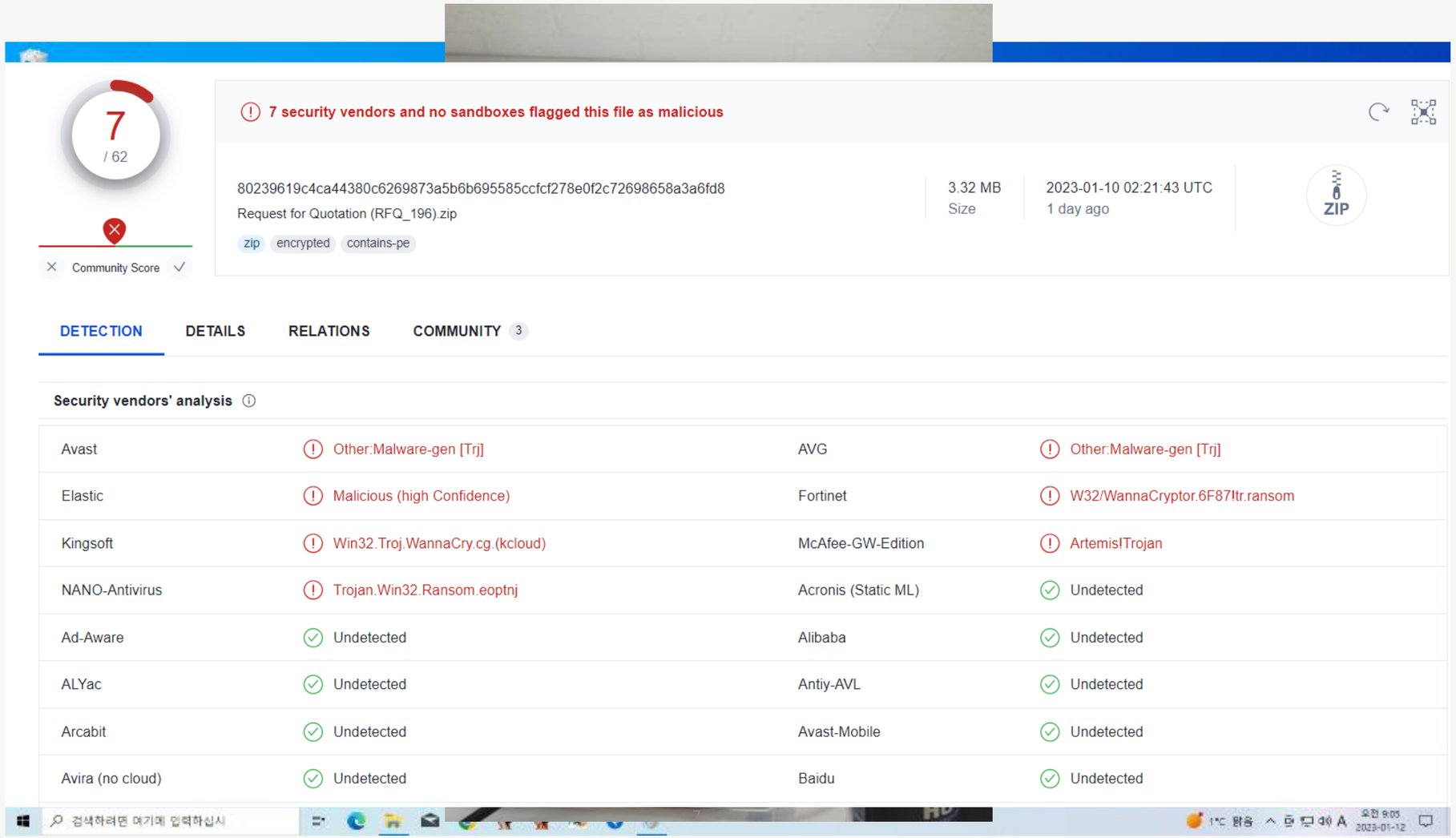
02

현재 진행도


CPU
ALU
Execution
Control Unit
Decode
Register Set
명령어1
BUS Interface
Memory
명령어1
명령어N
I/O BUS
명령어1
Fetch

02

현재 진행도


7
/ 62
Community Score
7 security vendors and no sandboxes flagged this file as malicious
80239619c4ca44380c6269873a5b6b695585ccfcf278e0f2c72698658a3a6fd8
Request for Quotation (RFQ_196).zip
zip
encrypted
contains-pe
3.32 MB
Size
2023-01-10 02:21:43 UTC
1 day ago
ZIP
DETECTION
DETAILS
RELATIONS
COMMUNITY 3
Security vendors' analysis
Avast
Other:Malware-gen [Trj]
AVG
Other:Malware-gen [Trj]
Elastic
Malicious (high Confidence)
Fortinet
W32/WannaCryptor.6F87!tr.ransom
Kingsoft
Win32.Troj.WannaCry.cg.(kcloud)
McAfee-GW-Edition
ArtemisTrojan
NANO-Antivirus
Trojan.Win32.Ransom.eoptnj
Acronis (Static ML)
Undetected
Ad-Aware
Undetected
Alibaba
Undetected
ALYac
Undetected
Antiy-AVL
Undetected
Arcabit
Undetected
Avast-Mobile
Undetected
Avira (no cloud)
Undetected
Baidu
Undetected
검색하려면 여기에 입력하십시


Q
2주뒤에는
뭘 보여 줄건데?

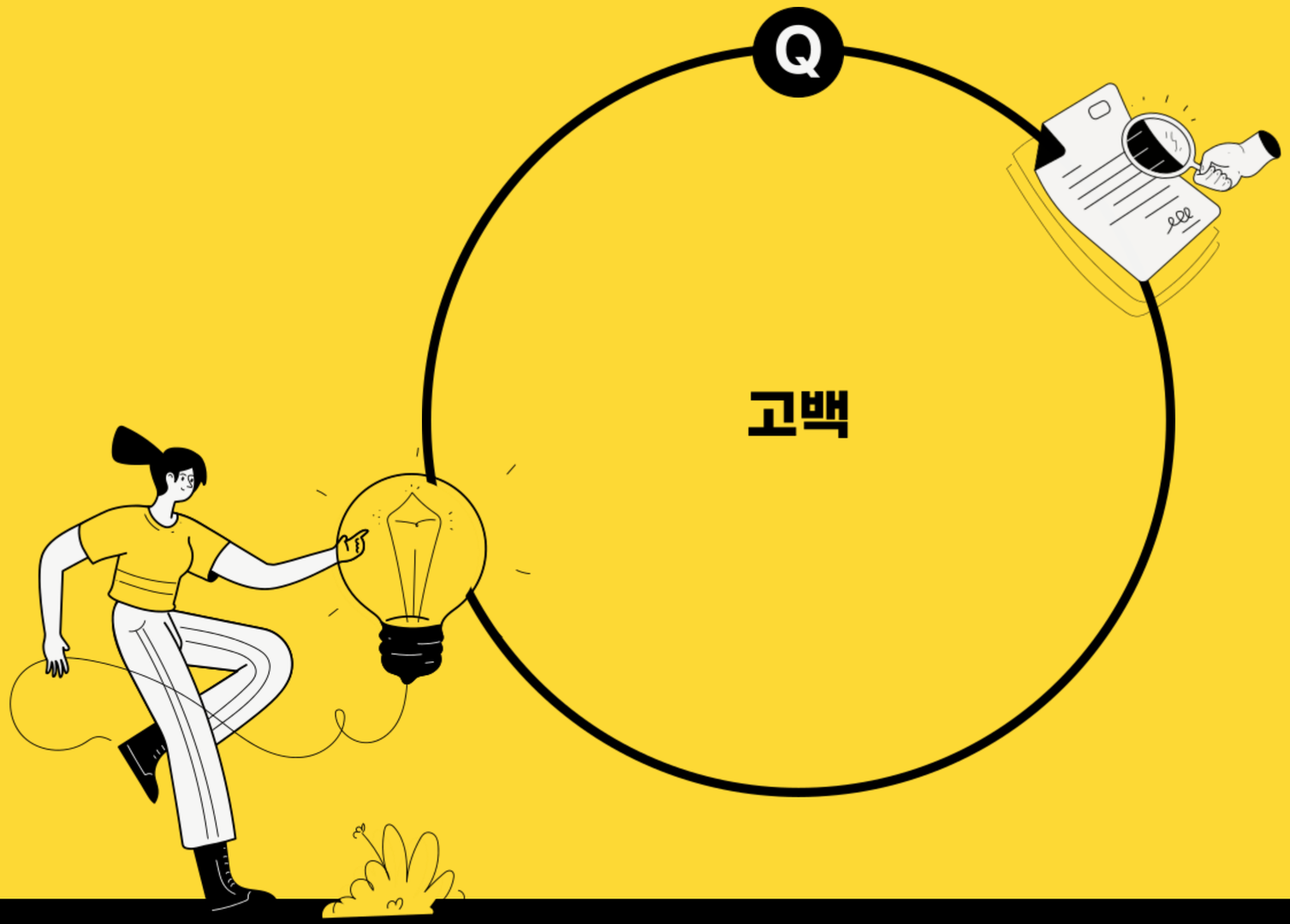
미래 계획

rust기반 Black Cat 분석

- rust로 컴파일된 랜섬웨어인 Black Cat 분석
- 초기에는 분석 보고서를 바탕으로 분석을 할예정
- 후에 시간이 남으면 조치 방법을 강구

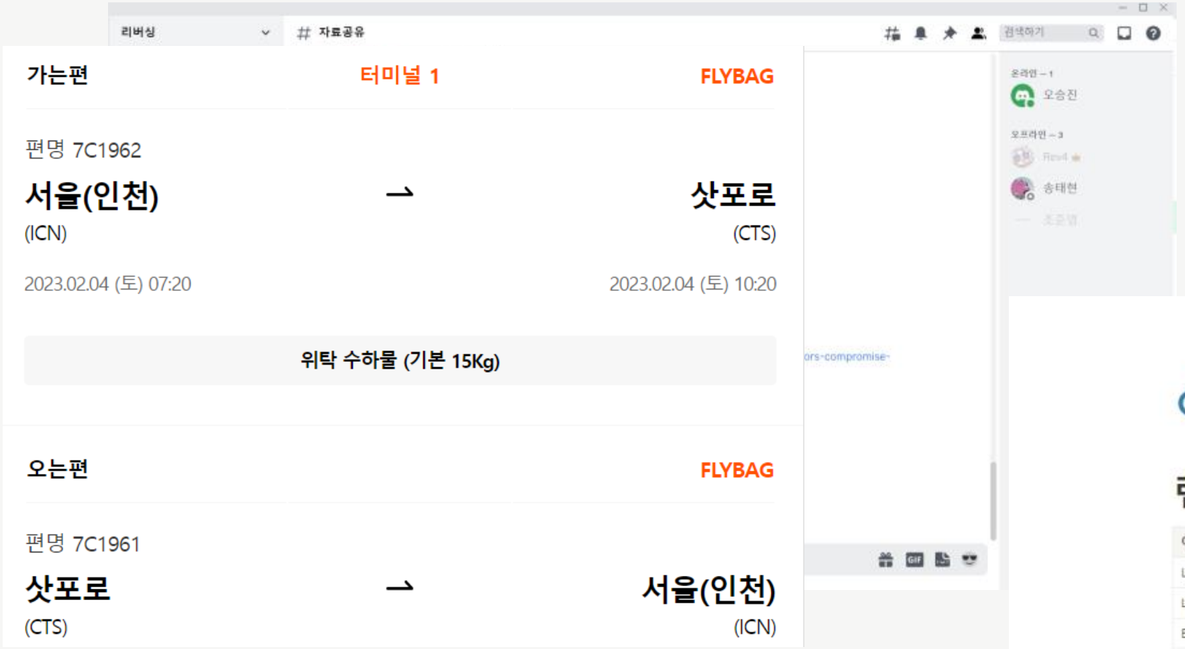
'?' 랜섬웨어 분석

- 2022년에 Hot 했던 랜섬웨어중 하나로 진행 예정


Q
고백

04

고백



랜섬웨어(Windows)

이름	비밀번호	URL
LockBit 3.0 Builder		Github
Lockbit 3.0	infected	Bazaar
BlackCat	infected	Bazaar
Sugar	infected	Bazaar
Conti	infected	Bazaar
Pandora	infected	Bazaar
DarkSide	infected	Bazaar
AvosLocker	infected	Bazaar
RagnarLocker	infected	Bazaar
BlackMatter	infected	Bazaar
Cuba	infected	Bazaar

- Q&A -

THANK YOU

감사합니다.