차세대 보안리더
양성 프로그램

BoB 팀 프로젝트 최종 보고 : Power IR

Incident Response Service Based on Artifacts

[Mentor / PL] Nikolay, 김종현, 정승기

[Mentee] 진필근, 한채민, 김동현, 김형규, 정동호

“하나의 목표를 향한 완벽한 조합”

멘토단 / PL

주 멘토 : Nikolay

부 멘토 : 김 종 현

PL: 정 승 기

정보보호특기병 트랙

진 필 근

프로젝트 총괄 및 Web 개발

보안 컨설팅 트랙

한 채 민

대외 협력 및 산출물 관리

디지털 포렌식 트랙

김 동 현

김 형 규

정 동 호

Artifact 조사 및 Malware 분석 / Client, Script 개발 및 알고리즘 고안

KITRI BoB 팀 프로젝트 최종 보고 : Power IR

1. 프로젝트 이해
2. 프로젝트 수행
3. 프로젝트 결론

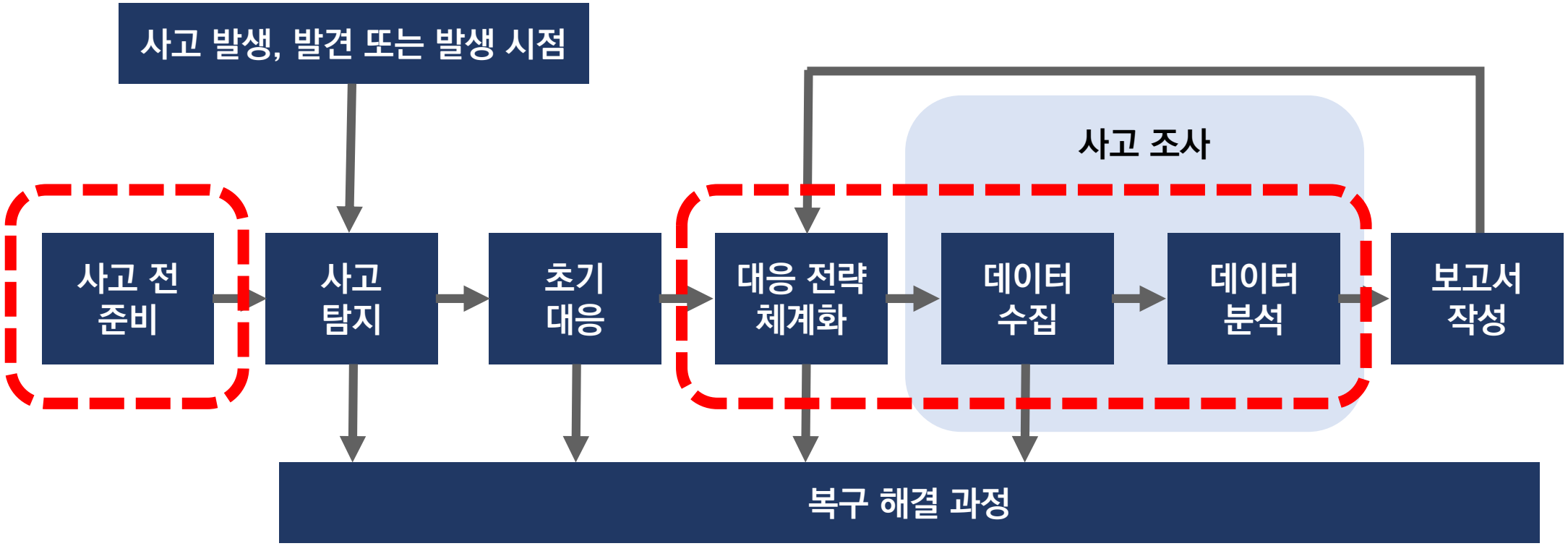
1. 프로젝트 이해

A. 프로젝트 목적

B. 프로젝트 범위

“침해사고의 전체적인 스케치 가시화를 통한 신속한 대응”

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

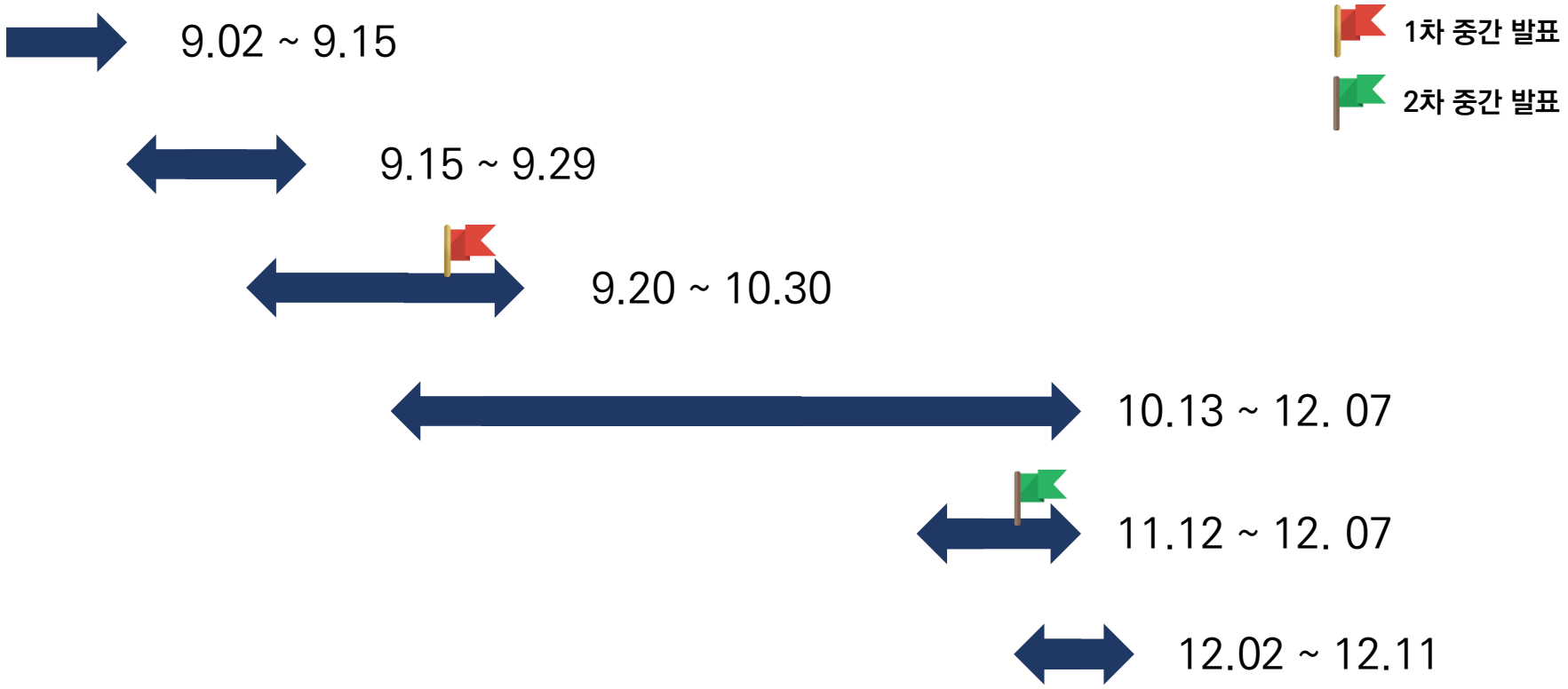


2. 프로젝트 수행

A. 프로젝트 일정

B. 개발 수행 내역

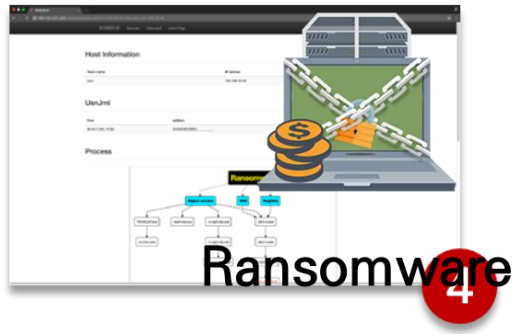
“프로젝트 계획에 따라 100% 진행, 총 1038 페이지의 산출물”



- WBS
- 프로젝트 계획서
- 시장 조사 보고서
- 기술 조사 보고서
- 요구 사항 명세서
- 테스트 결과 보고서
- 클라이언트 프로그램
- 웹 사이트 및 서버
- Power IR 사고 대응 매뉴얼
- 프로젝트 기술 관련 논문

관리자 클라이언트

알고리즘



웹 페이지

사용자 매뉴얼

강화 스크립트

“기존 제품의 방식에 변화를 주다”

취약점 발생 가능성

시스템 자원 소모

Windows PowerShell

원격 연결

모듈 기능

범용성

권한 관리

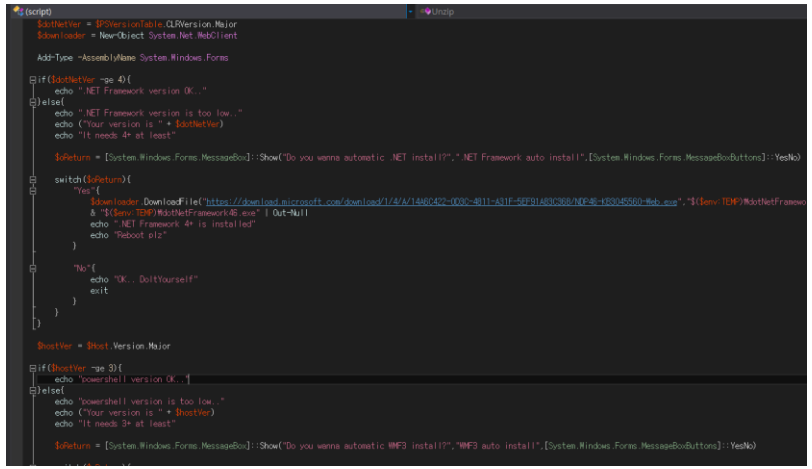
“효율적인 아티팩트 수집을 위한 포렌식 준비”

(KDFS2014) 정보 유출 사고와 포렌식 준비도

1. 클라이언트 설정을 강화하자!!

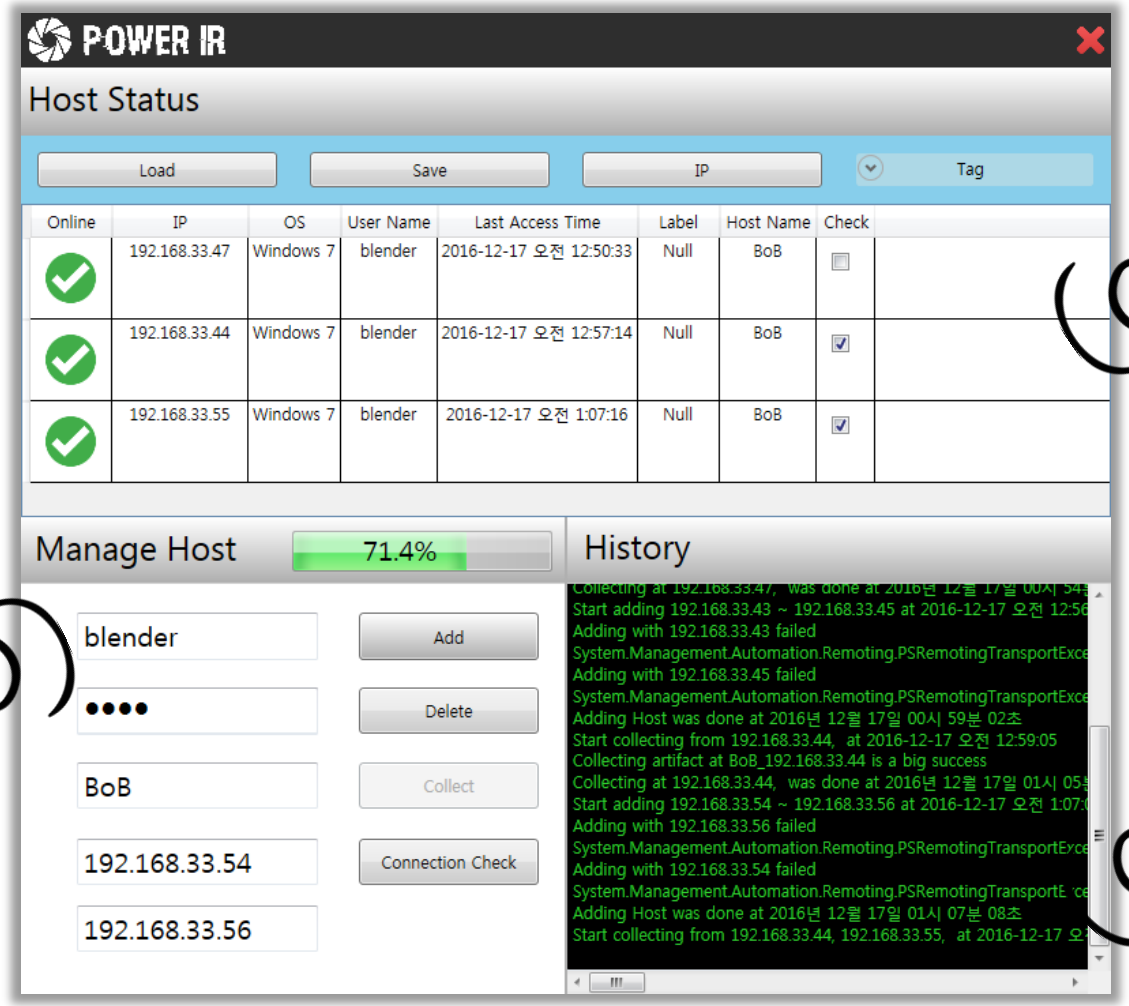
11 이벤트 로그 크기

- 이벤트 로그 크기를 증가시켜 효율적인 시스템 및 사용자 이벤트 추적



- .NET Framework 설치
- WMF 설치
- PowerForensics 모듈 적용
- 개체 액세스 감사
- 이벤트 로그 강화

“다량의 호스트를 관리하기 좋은 클라이언트”



연결 호스트 목록화

호스트 계정 정보 입력

호스트 연결 상태
및 에러 출력

“대상 선정을 위한 사전 인터뷰”

SAINT SECURITY
GLOBAL SECURITY SOLUTION PROVIDER

악성코드 분석팀 김승언 팀장님

“프로젝트의 대상을 고려해본다면 **최근에 기업에서 주목**하고 있는

악성코드인 Ransomware나 KeyLogger를 대상으로 진행을 해보면 좋을 것이다.”

AhnLab

ASEC 차민석 책임 연구원님

“파괴나 은닉과 관련한 악성코드는 백신도 해결하기 힘든 부분이다,

앞서 제시한 악성코드만 집중하더라도 **충분한 가치가 있다고 생각**한다.”

“알고리즘 설계를 위한 특징 파악”

랜섬웨어

파일의 암호화 과정

많은 양의 파일 변경

“최적의 결과를 위한 지속적인 연구”

파일 변화량 중점 알고리즘

랜섬웨어 선호 확장자 필터링

랜섬웨어 비선호 확장자 제외 필터링

윈도우 업데이트 및 파일 설치에 대한 오진

특정 파일 한정 업데이트에 대한 오진

“지속적인 연구의 결과”

암호화 패턴 유사도

비교 알고리즘

추가 아티팩트 연계를 통한

프로세스 추적

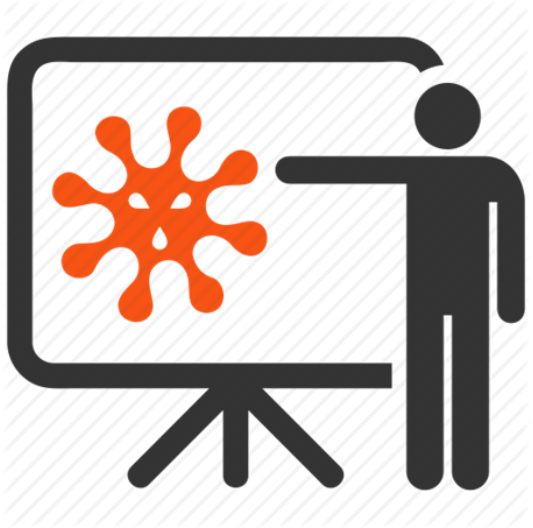
```
for i in s:
    q += [i.split('\t')[2]]
    if len(q) > 20: del q[0]
    if (is_sublist(['DATA_OVERWRITE', 'DATA_OVERWRITE, DATA_EXTEND', 'DATA_OVERWRITE, DATA_EXTEND, CLOSE',
                    'RENAME_OLD_NAME', 'RENAME_NEW_NAME', 'RENAME_NEW_NAME, CLOSE']*2,q))\
    or (is_sublist(['DATA_OVERWRITE', 'DATA_OVERWRITE, DATA_EXTEND', 'DATA_OVERWRITE, DATA_EXTEND, CLOSE']*3,q)):
```

```
['FCDEFCDEFCOBNHBNHOFLO','FCDEFCDEFCFLO','DVDVDEDVDEORPARWARWAO','DTDEDTDVDEDTDVDEDTBNHDVDEDTBNHO',
 'RPARWADVRWADVDERWADVDERWABNHDVDERWABNHO','BNHBNHORPARWADVRWADVDERWADVDERWABNHDVDERWABNHO']
```

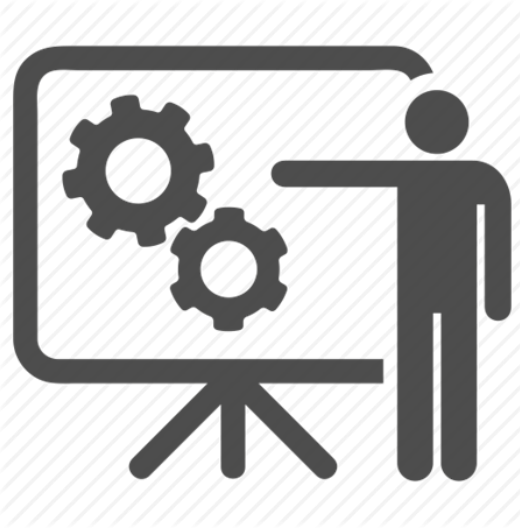
```
# Check all gene patterns.
for j in range(len(genes)):
    curPatIdx = curPat.find(genes[j][:3]) # Find the right location.
    if(curPatIdx > 3 or curPatIdx == -1): continue

    # We use the levenshtein distance algorithm to measure the similarity between the pattern and the current usn.
    score = jellyfish.levenshtein_distance(curPat[curPatIdx:curPatIdx+genes_len[j]],genes[j])
    row = i.split('\t')
```

오진 사항 개선 및 정확도 향상

“Ransomware 테스트 결과”



2차 중간 발표 이전 : 20개



2차 중간 발표 이후

최근 발생 Ransomware 31개 추가

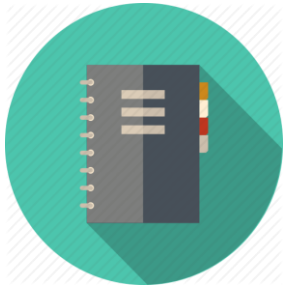
총 51개 중

48개 탐지

“알고리즘 설계를 위한 특징 파악”

키로거

키로깅을 위한 지속적인 파일 접근



파일을 생성해서 기록하는 키로거

“최적의 결과를 위한 지속적인 연구”

키 입력에 따른 파일 접근량 계산 알고리즘

꾸준한 접근 기록을 남기는 로그 및 아티팩트와 관련한 오진

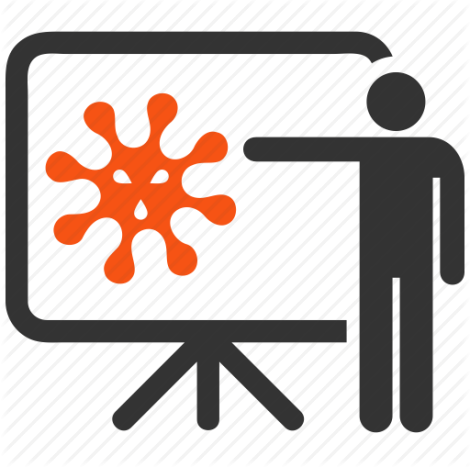
접근 시간차의 평균을 통한 계산 알고리즘

일반적인 정상 파일이 소수 탐지됨

일반인의 타이핑 속도에 기반한 시간차 알고리즘

수집한 키로거 한정 모두 잡아냄

“Key Logger 테스트 결과”



해외 유명 키로거

6개 샘플 수집

총 6개 중

6개 탐지

추가적인 샘플 테스트

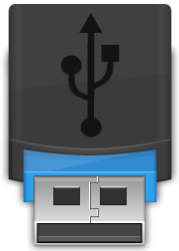
알고리즘 고도화 필요

“일반적인 유입 경로에 대한 탐색”

E-Mail & 파일 다운로드

크롬 History DB에 SELECT 쿼리 요청 → 다운로드 내역 중 ‘의심 파일 이름 ’ 을 포함하는 레코드 나열 → 다운로드 위치 / 다운로드 일자 / 다운로드 사이트

외부 장치 연결



추정 프로세스 파일의 생성 시각 탐지 → 프로세스가 돌아간 최초의 시간 획득 / 파일 생성 시간 획득 → EVENT 1008, 2003을 통한 외부 장치 연결 및 제거 시간 통해 입력되어 있던 장치 스캔

“논문 발표와 인터뷰를 통한 알고리즘 검증”

2016 KDFS 동계 워크숍 통과 및 발표

Artifact 기반 Key Logger 탐지*

김 형 규[1] 김 동 현[1] 정 동 호[1] 진 필 근[1] 한 채 민[1]
[1]KITRI BoB

Key Logger Detection based on Artifact

Hyeong-Gyu Kim[1] Dong-Hyun Kim[1] Dong-Ho Jung[1] Phil-Geun Jin[1] Chae-Min Han[1]
[1]KITRI BoB

요 약

본 논문은 개인정보 유출에 사용되는 일부 유형의 Key Logger에 대해 컴퓨터에 기록되는 File System Artifact를 중심으로 Key Logging 활동이 발생했는지 여부를 탐지하고 예상되는 프로세스를 검출하는 것을 목적으로 한다. 기존 접근 방식과는 다르게 Key Logging에 따른 흔적을 조합하여 행위 발생 여부를 파악할 수 있다는 점에서 충분한 연구가치가 있다고 판단하여 진행하였다. 본 연구에서의 연구대상 범위에는 사용자의 키 입력을 지속적으로 기록하는 파일을 생성하는 Key Logger로 한정하였다. 향후 추가적인 Key Logger 유형의 행동에 따라 기록되는 Artifact를 분석한 후 이를 패턴화하여 연구의 범용성을 늘려나가고자 한다. 또한, 추가적인 연구를 통하여 패턴을 추가한다면 다양한 종류의 Key Logger의 활동 여부를 판단할 수 있을 것이다. 주 분석 Artifact는 $UsnJrnl과 강화된 Windows Event Log를 중심으로 실제 호스트에서 악성 행위에 대한 분석을 진행하였다. 본 연구에서는 기본적으로 Logging이 이루어지는 Artifact만으로 Key Logging 행위 발생 여부를 판단할 수 있다는 단서를 제공하고자 한다.

Session 3	디지털 포렌식 기술 I	좌장 : 최종현
15:45~16:45	ZIP파일 복구 도구의 성능한계와 개선방안	정병준 (고려대)
	Themida API 난독화 해제방안	이재휘 (고려대)
	Artifact 기반 Key Logger 탐지	김형규 (BoB)

HAURI

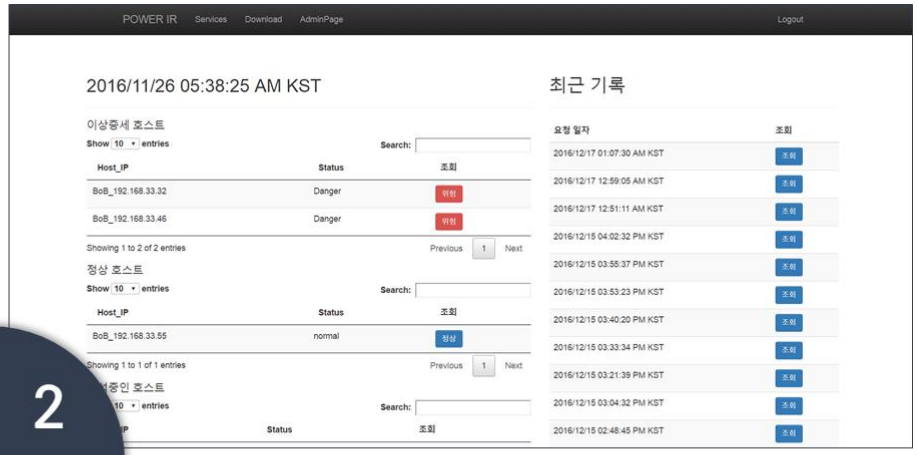
하우리 연구원 및 임직원

“해당 프로젝트에서 각각의 악성코드들을
구분해내는 알고리즘과
노이즈 제거를 위한 접근방법은
충분히 적절하다고 판단한다.”

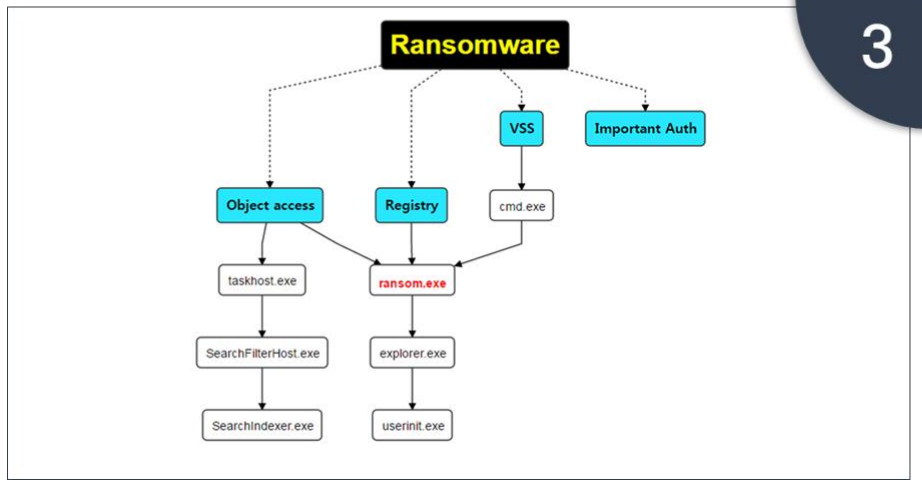
국제사이버범죄 연구센터
신지호 연구원

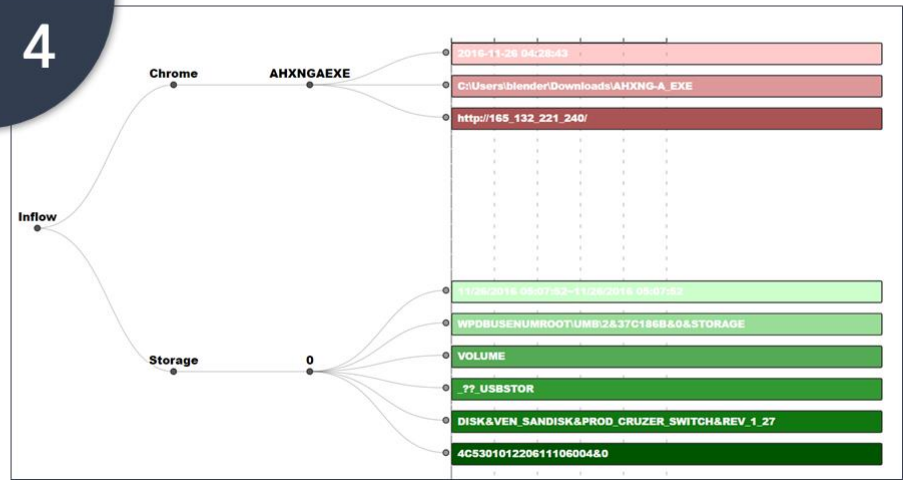
“악성코드들과 유입 경로 파악을 위한
접근 방식과 설계된 알고리즘,
이를 구현한 코드가
잘 구현되고 있다고 생각한다.”

“기록 관리 및 침해 사고에 대한 스케치 제공”

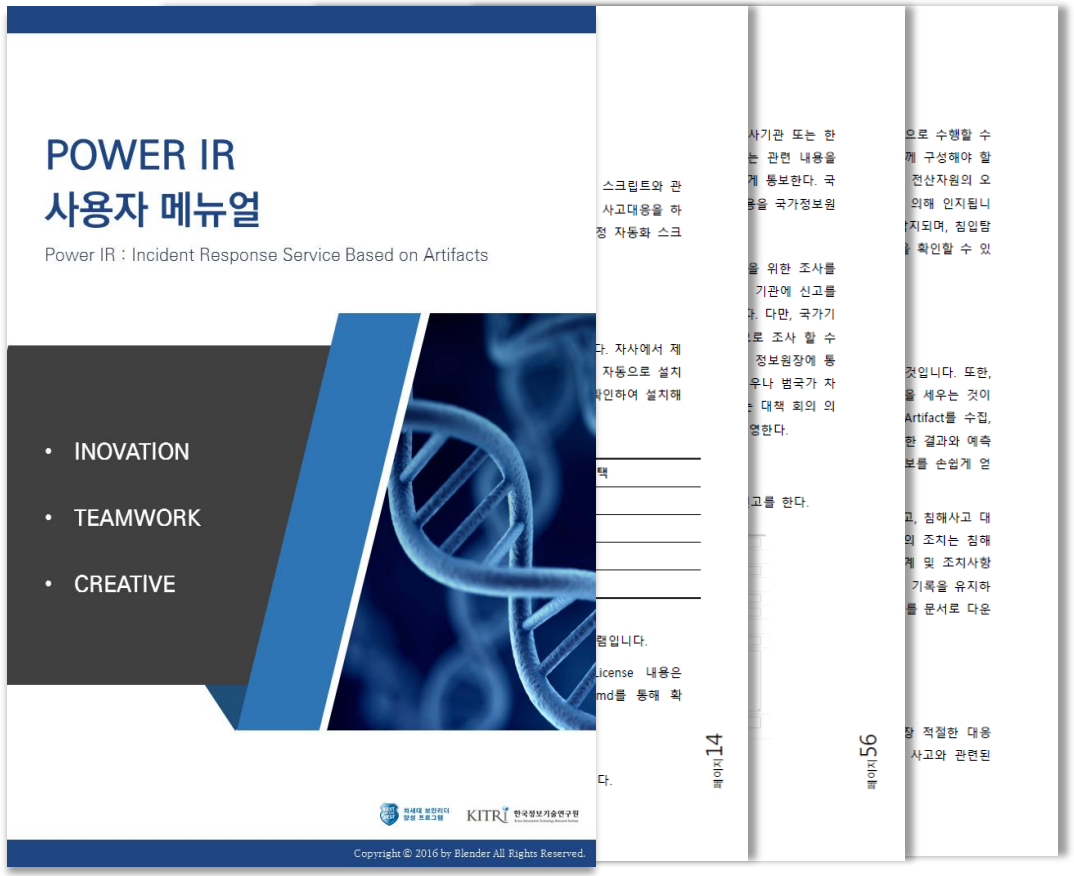


1 2
3 4





“효율적인 활용을 위한 자체 매뉴얼 제공”



- POWER IR 사용 가이드
- 단계별 침해사고 분석 절차
- 시나리오 별 사고 대응 방법
  - ✓ Ransomware
  - ✓ Key Logger
- 부록 : 침해사고 대응 신고 절차

3. 프로젝트 결론

A. 프로젝트 검증

B. 프로젝트 성과

C. 프로젝트 고도화

“PCA 3단계 인터뷰를 통한 프로젝트 검증”

한국 IT 서비스 학회

“논문에 제시한 내용을 토대로 구현이 되었다는 것을 고려해본다면 해당 도구가 **현업의 문제점을 해결하고 큰 수익을 낼 수 있을 것이라 생각한다.**”

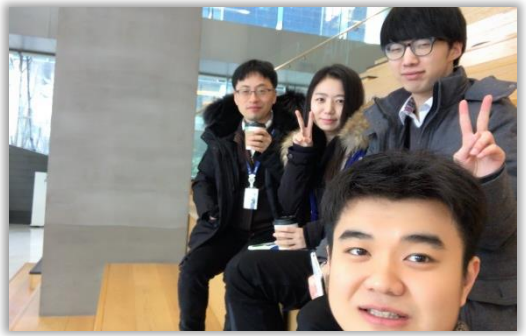
국제 사이버범죄 연구센터

신지호 연구원님

“상당히 인상적이며 상용화되면 괜찮을 것 같다고 생각한다. **경찰 내부 시스템에 잘 녹여내도 큰 효과가 있을 것이며 시각화 부문에서도 좋은 점수를 주고 싶다.**”

하우리 연구원 및 임직원

“감염 경로 확인과 더불어 포렌식 작업에 필요한 여러 요소를 종합해본다면 **큰 그림을 그려주는 POWER IR은 많은 도움이 될 수 있다고 본다**.”



안랩 차민석 책임 연구원님

“아티팩트의 수집만으로 여러 호스트의 악성코드 감염 경로나 프로세스에 대한 정보를 보여준다는 점에서 **분석관들이 많은 도움을 받을 수 있을 것 같다**. 또한 독특한 **알고리즘을 자체적으로 활용하며 오진을 줄여 나갔다는 점이 상당히 인상적이다**.”

세인트 시큐리티 김승언 팀장님

“대량의 호스트를 검사 할 수 있고, 실제 악성 코드들에 대해 커버가 된다는 점에서 **현업 사용 가능성이 충분하다**. 또한 **B2B에서 큰 이슈로 다뤄지는 악성코드에 대해 구현**이 되어 있는 만큼 **사업성 또한 충분히 가지고 있다.**”

기업 및 전문가와의 인터뷰를 통해 피드백 반영

프로젝트의 “가치” 및 “활용 가능성” 검증

“논문 투고 4건, 논문 및 대외 발표 6회, 세미나 참석 2회”

한국IT서비스학회 Korea Society of IT Services

한국정보보호학회 Korea Institute of Information Security & Cryptology

CARBON BLACK ARM YOUR ENDPOINTS

KUCIS 대학정보보호동아리연합회

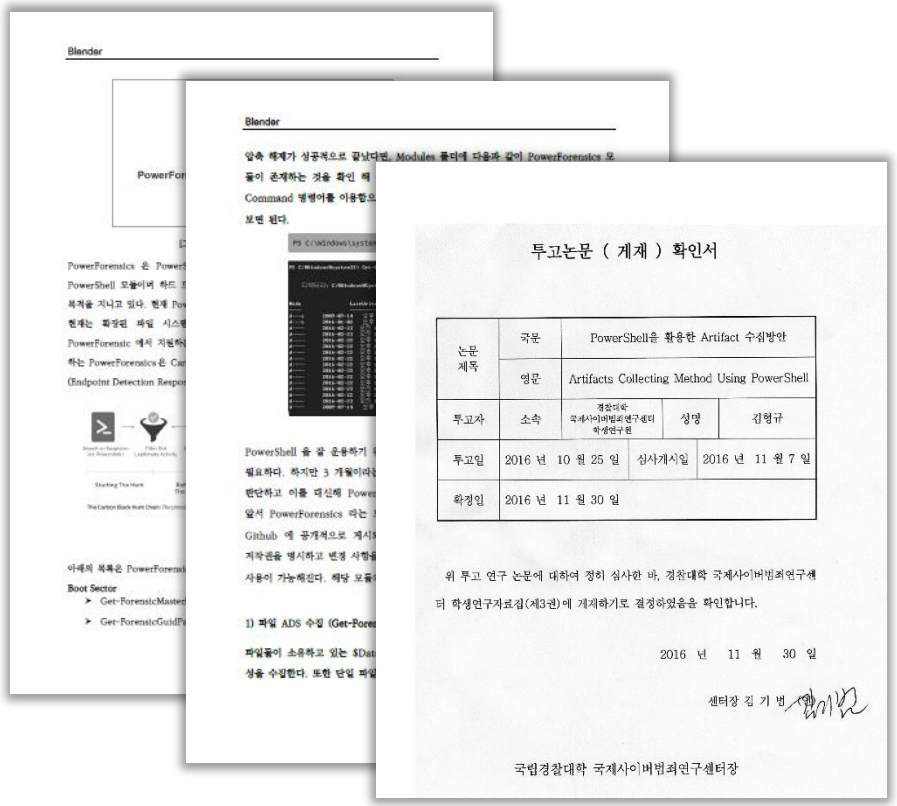
한국법과학회 KOREAN SOCIETY OF FORENSIC SCIENCES

(사) 한국디지털포렌식학회 http://kdfs.or.kr

KOREA UNIVERSITY

서울여자대학교 SEOUL WOMEN'S UNIVERSITY

“PowerShell을 활용한 아티팩트 수집 방안, 경찰 대내 자료집(ICRC) 게재”



투고논문 (게재) 확인서

논문 제목	국문	PowerShell을 활용한 Artifact 수집방안		
	영문	Artifacts Collecting Method Using PowerShell		
투고자	소속	경찰대학 국제사이버범죄연구센터 학생연구원	성명	김형규
투고일	2016 년 10 월 25 일	심사개시일	2016 년 11 월 7 일	
확정일	2016 년 11 월 30 일			

위 투고 연구 논문에 대하여 정히 심사한 바, 경찰대학 국제사이버범죄연구센터 학생연구자료집(제3권)에 게재하기로 결정하였음을 확인합니다.

2016 년 11 월 30 일

센터장 김 기 범

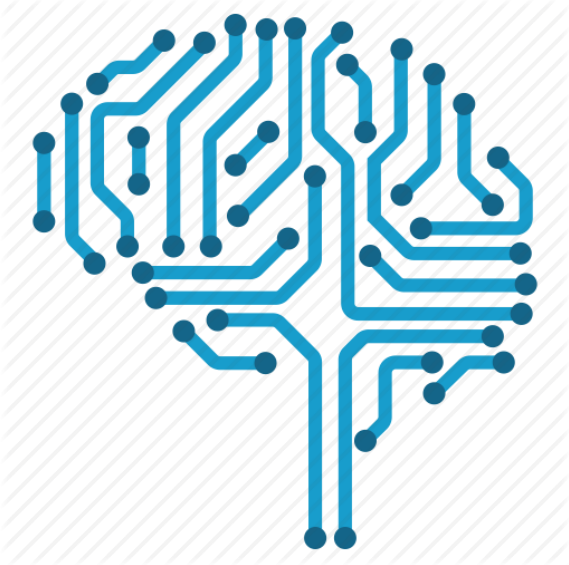
국립경찰대학 국제사이버범죄연구센터장

프로젝트를 통해

습득한 지식을

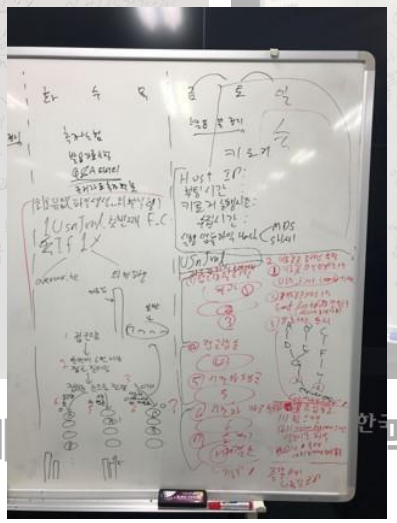
사회에 환원 함으로써

“지식의 나눔”을 실천

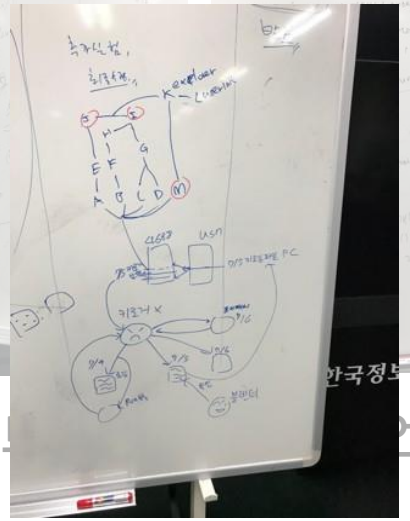


“프로젝트를 진행하며 저희는 한 층 더 성장 할 수 있었습니다”

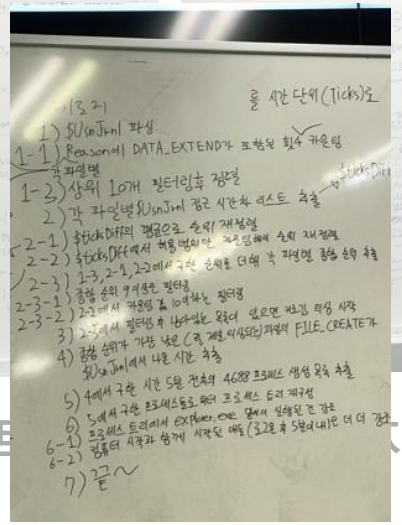
매 번 서로의 지식과 생각을 공유해가며 난관을 해쳐 나갔습니다.



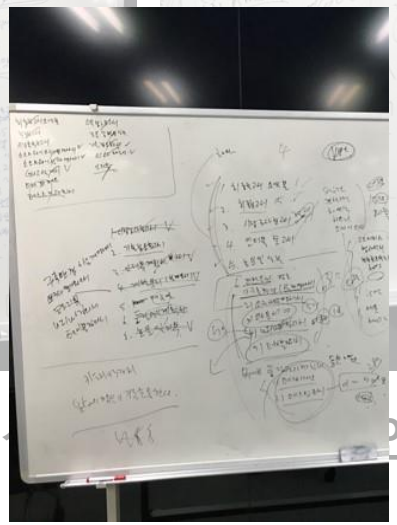
랜섬웨어 알고리즘



키로거 알고리즘



피드백 반영

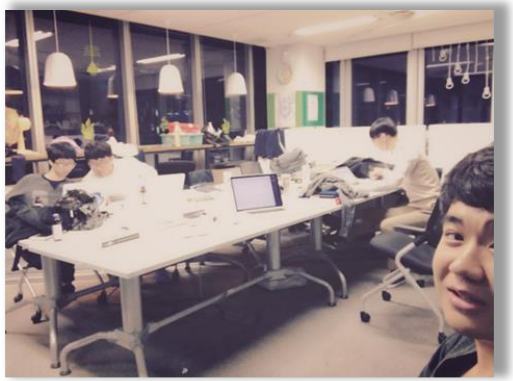


매뉴얼 기획

“무엇보다 중요하였던 것 은 서로 간의 믿음”

멘토님께 가르침을 받고, 함께 노력을 해 왔기에 여기까지 올 수 있었습니다.








KITRI BoB 팀 프로젝트 최종 보고 : Power IR

Thank You!

Q&A

KITRI 한국정보기술연구원
Korea Information Technology Research Institute