

# “위협 차단에서 위험 관리로의 전환”

부제 : 새로운 맞대응이 필요한 시대

PASCON 2020

# “위협 종합분석과 T.T.P 보고서”

부제 : 우리는 잘 준비되어져 가고 있는가?

Indicator of Compromise

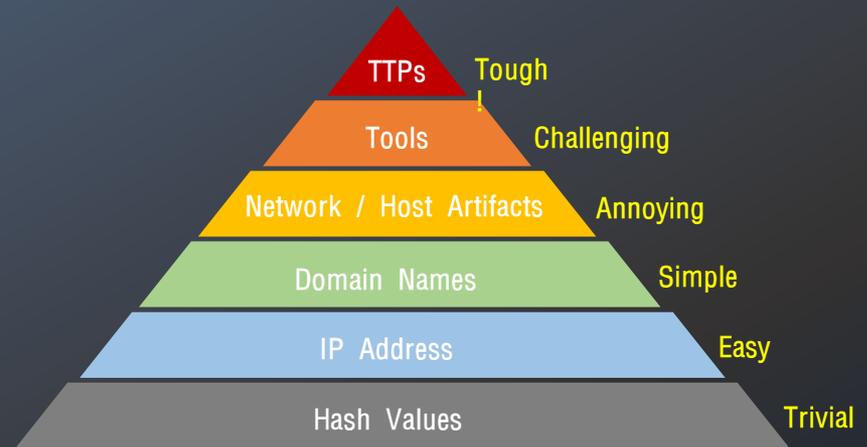
# IoC

이미 발생된 피해

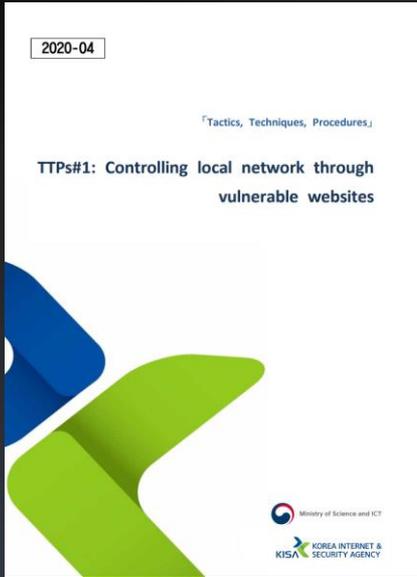
Indicator of Attack

# IoA

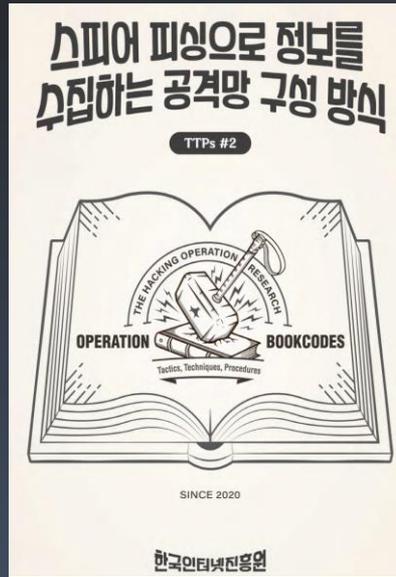
활동중인 공격



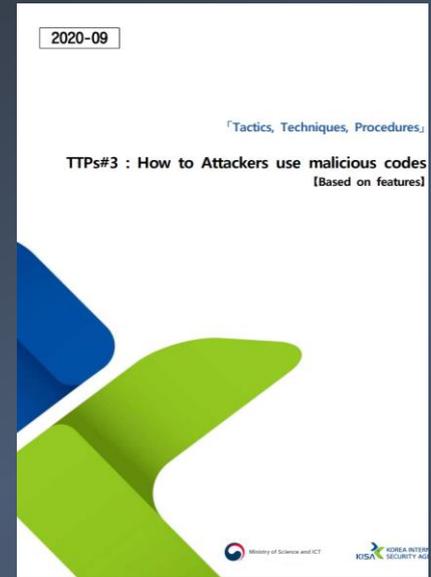
TTPs#1



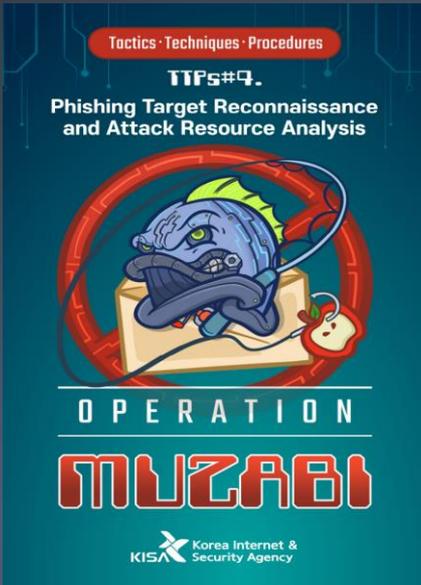
TTPs#2



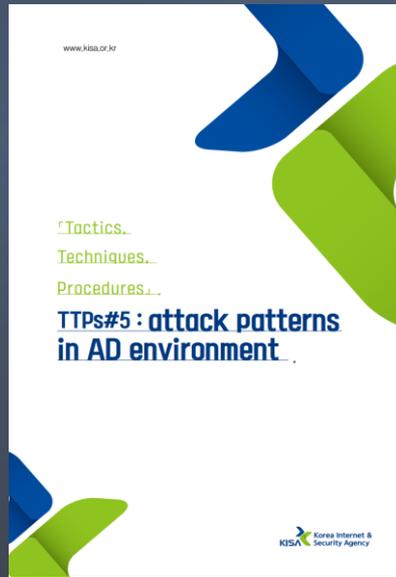
TTPs#3



TTPs#4



TTPs#5



TTPs#6



기업 & KrCERT

**Threat** Shut Down?

**Risk** Management..

# 사이버 위험 관리

사이버상에서

각종 위협으로 인해 발생할 수 있는

기업의 잠재적 손실을 최소화하는

효율적인 방법을 찾고 실제로 구현하는 것

질문 1

**이벤트 로그 삭제 시 알 수 있는가?**

## 질문 2



이벤트 로그 삭제



팀뷰어 채널 존재



비정상 계정 생성



다수의 접근실패 이력 존재



AD 비정상 파일배포 이력 존재



중요 관리자PC 백신탐지 이력 존재

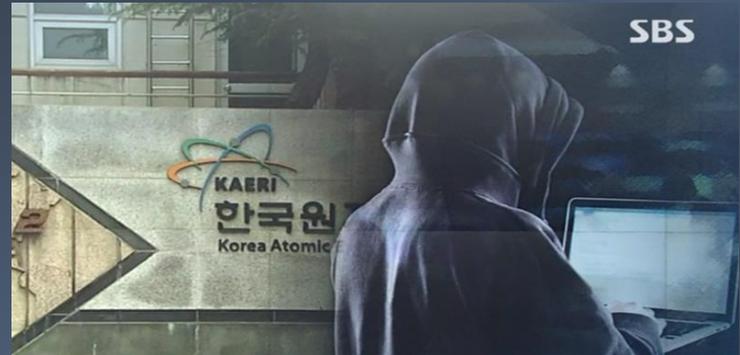
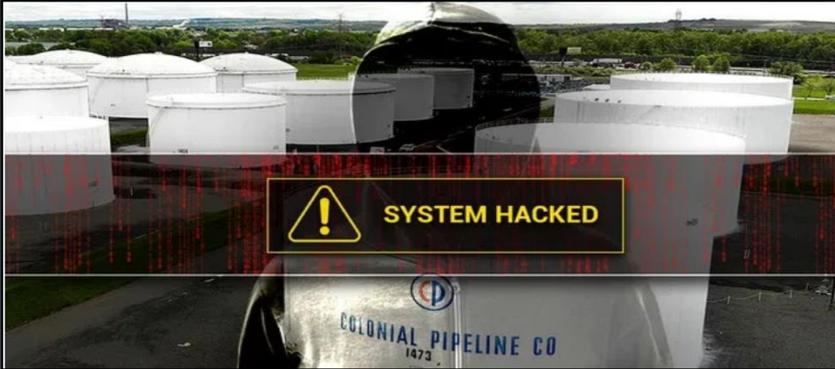


웹서버 웹셸 탐지

**위험 관리를 위해 필요했던**

**2가지 질문**

**On the face of Threat**



일반파일 1개 (27.2KB) 모두저장

[설문지] 2021 데이터기반 미래전망 연구(평화안보).doc (27.2KB)

**(1차)정상문서**

이와 관련하여, 각 정책 분야별로 2021년의 핵심 아젠다를 선정하여 지속가능성을 평가하여 정부의 2021년 정책 운용에 대한 함의...

본 조사에서는 각 정책 분야별 핵심 아젠다에 대한 각 아젠다별 현 대한 각 분야 전문가들의 의견을 듣고자 합니다.

응답 요청 정책 분야는 평화안보, 이와 관련된 아젠다의 평가 부

응답 내용은 철저하게 비밀이 보장되며, 연구목적 외의 다른 용도

설문에 응해주신 전문가에게는 소정의 사례(20만원)를 드리고자 하

참가신청서양식.doc [호환 모드] - Word

**(2차)악성문서**

Microsoft Office와 관련이 없는 응용 프로그램을 사용하여 작성된 문서

문서를 보시려면 도구바의 "콘텐츠 사용"을 클릭하세요

**랜섬웨어가 위협일까? 과연??**



- ☞ VPN
- ☞ NAC
- ☞ 그룹웨어



- ☞ 클라우드 서비스 운영업체



- ☞ VDI 환경



- ☞ 무차별적



Zero-day Exploit

- ☞ 최초 침투, 거점 구축
- ☞ 정보 유출



Watering hole

- ☞ 문서편집 프로그램 취약점
- ☞ 관리자 권한 탈취



Dark Web

- ☞ VDI 계정 구입
- ☞ AD환경 장악



Spear Phishing

- ☞ [vpn-alert.pe.hu](http://vpn-alert.pe.hu)
- ☞ [gvpn.kro.kr](http://gvpn.kro.kr)
- ☞ [estsft.autoupdate.kro.kr](http://estsft.autoupdate.kro.kr)
- ☞ [emailsecurity.ahn-lab-kro.kr](http://emailsecurity.ahn-lab-kro.kr)

맞대응 할 수 있는 지점인가?

# Beyond Incidents

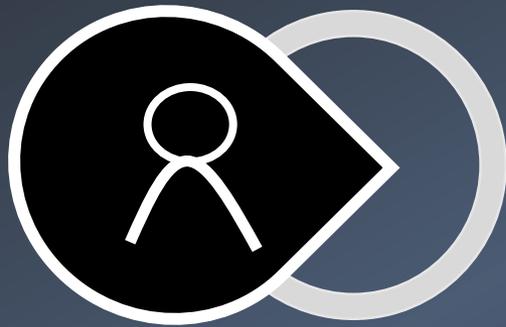
시간적 Term이 존재하고

공간적 제약이 너무 크다.

전략의 유연성에 있어서

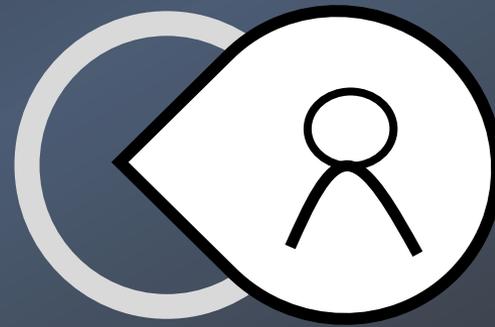
공격자들은 늘 우위에 있다.

# 새로운 맞대응



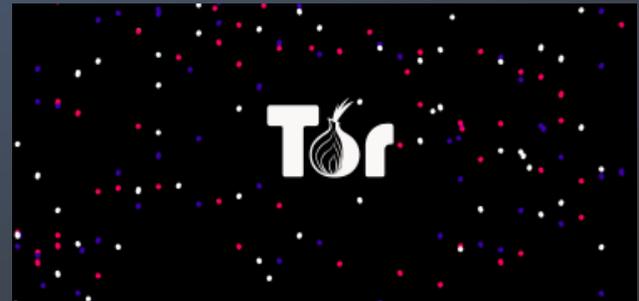
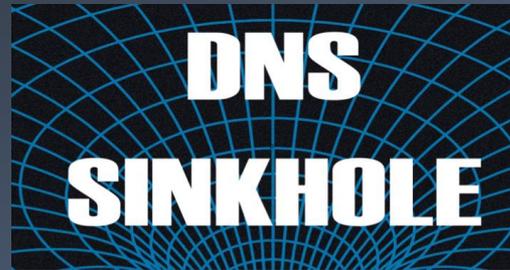
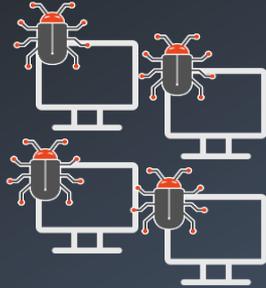
Attacker

versus



Defender  
(기업 & KrCERT)

# 맞대응의 변화



# 맞대응의 변화

Tactics · Techniques · Procedures

TTPs#9.

## Phishing Target Reconnaissance and Attack Resource Analysis



OPERATION

MUZABI

KISA Korea Internet &  
Security Agency

### [긴급] 개인정보 유출사건 관련 중요 알림

안녕하십니까. 한국인터넷진흥원입니다.

최근 웹메일 로그인 관련 취약점에 의한 개인정보 유출사건이 대대적으로 발생하고 있습니다.  
회원님의 메일계정 [tvcho829@gmail.com](mailto:tvcho829@gmail.com) 에서도 해당 취약점에 의한 해킹 흔적이 발견되었습니다.

o 세부정보

- 취약점: CVE-2021-0419235
- 적용플랫폼: Android 8, 9, 10, 11

안전한 웹메일 이용을 위하여 즉시 한국인터넷진흥원에서 제공하는 비정상적인 쿠키 삭제봉사를  
이용하세요.

[비정상적인 쿠키 모두삭제 >](#)

비정상적인 쿠키를 삭제하지 않을 경우 회원님의 개인정보가 지속적으로 유출될 수 있습니다.

기타문의사항은 [kisa.security@gmail.com](mailto:kisa.security@gmail.com) 로 연락바랍니다.

우리에게 필요한 새로운 맞대응

**Threat** Shut Down



**Risk** Management

# 사이버 위험 관리

사이버상에서

각종 위협으로 인해 발생할 수 있는

기업의 잠재적 손실을 최소화하는

효율적인 방법을 찾고 실제로 구현하는 것

# 기업

희망.. 단서..

21. 10. 12. 오후 5:50



An official website of the United States government



# Conti Ransomware Alert(AA21-265A)

- ✓ Use multi-factor authentication
- ✓ Implement network segmentation and filter traffic
- ✓ Scan for vulnerabilities and keep software updated
- ✓ Remove unnecessary applications and apply controls
- ✓ Implement endpoint and detection response tools
- ✓ Limit access to resources over the network, especially by restricting RDP
- ✓ Secure user accounts

## Mitigations

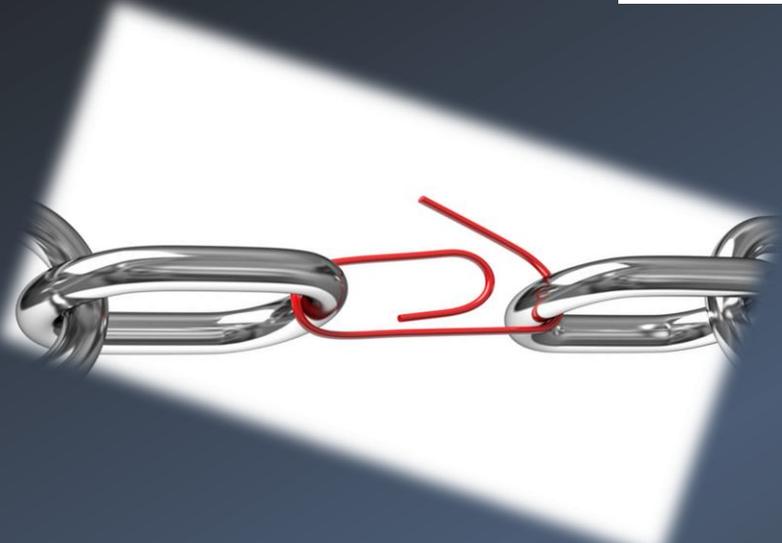
기업

현재의 공격은

개시되는 지점이 다를 뿐이지

진행되는 과정은 동일하다.

# 기업



디자인 되지 않은 보안의 영역



# KrCERT

희망.. 단서..

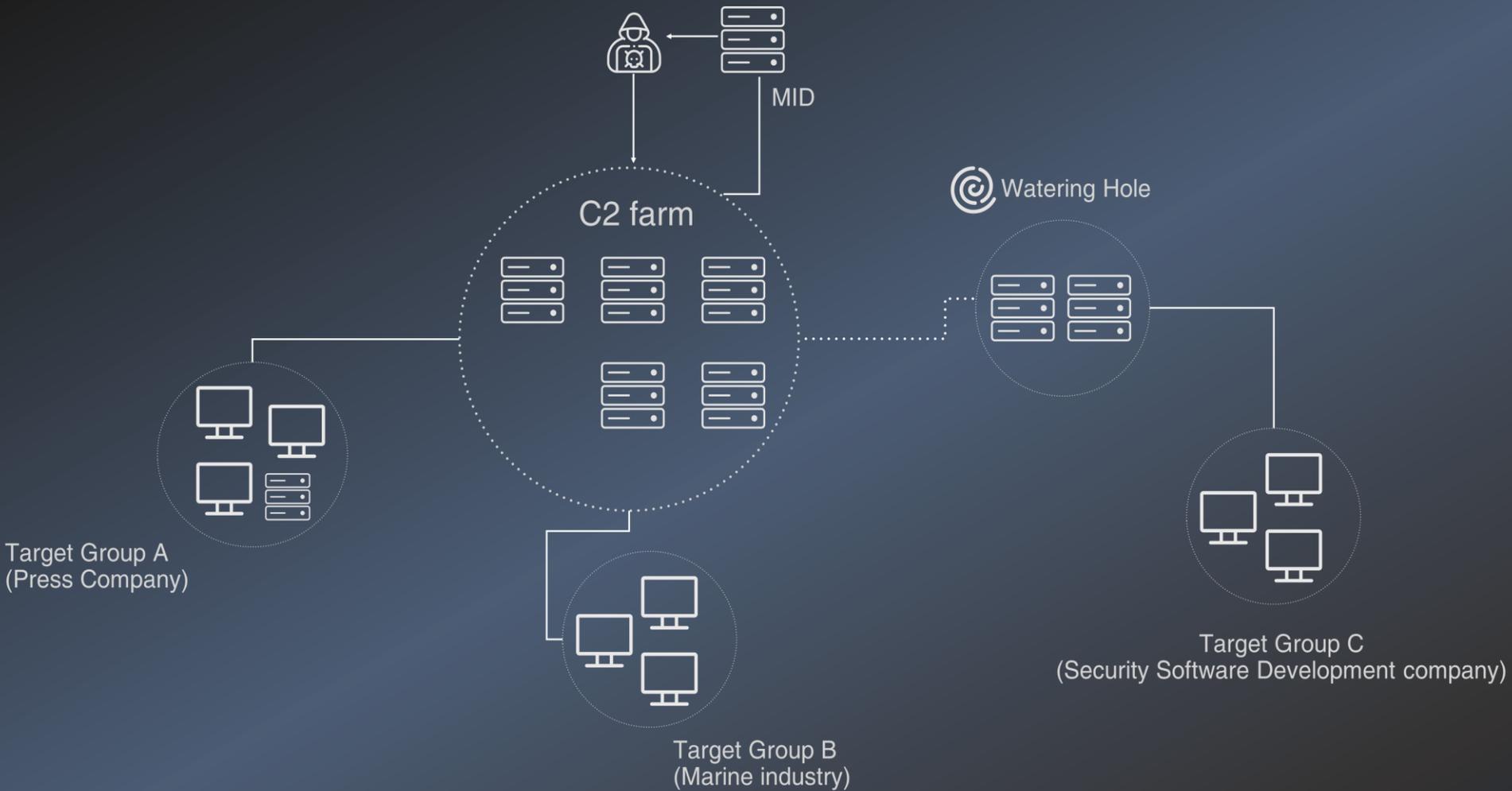
# KrCERT

공격 전에는 인프라가 만들어지고

만들어진 인프라는

관리되기 위해 반드시 묶인다.

# KrCERT



이벤트 로그 삭제 시 알 수 있는가?

감사합니다.

leejk@kisa.or.kr