PASCON 2020

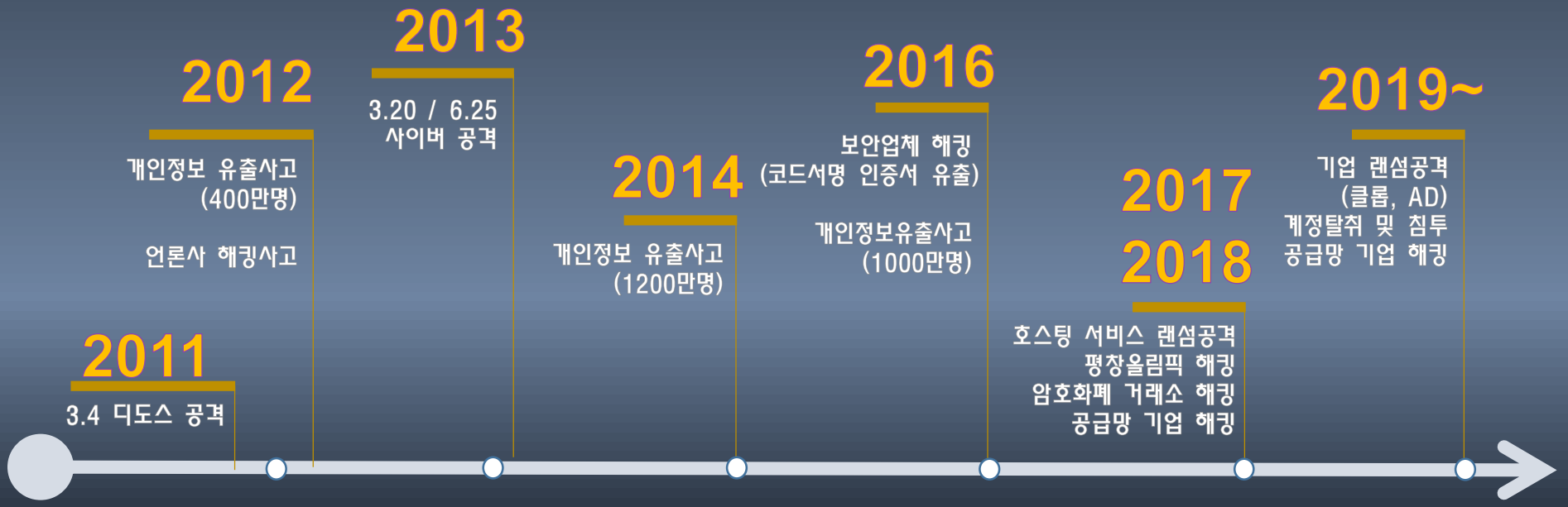
“위협 종합분석과 T.T.P 보고서”

부제 : 우리는 잘 준비되어져 가고 있는가?

KISA 종합분석팀 이재광

leejk@kisa.or.kr

10 Years

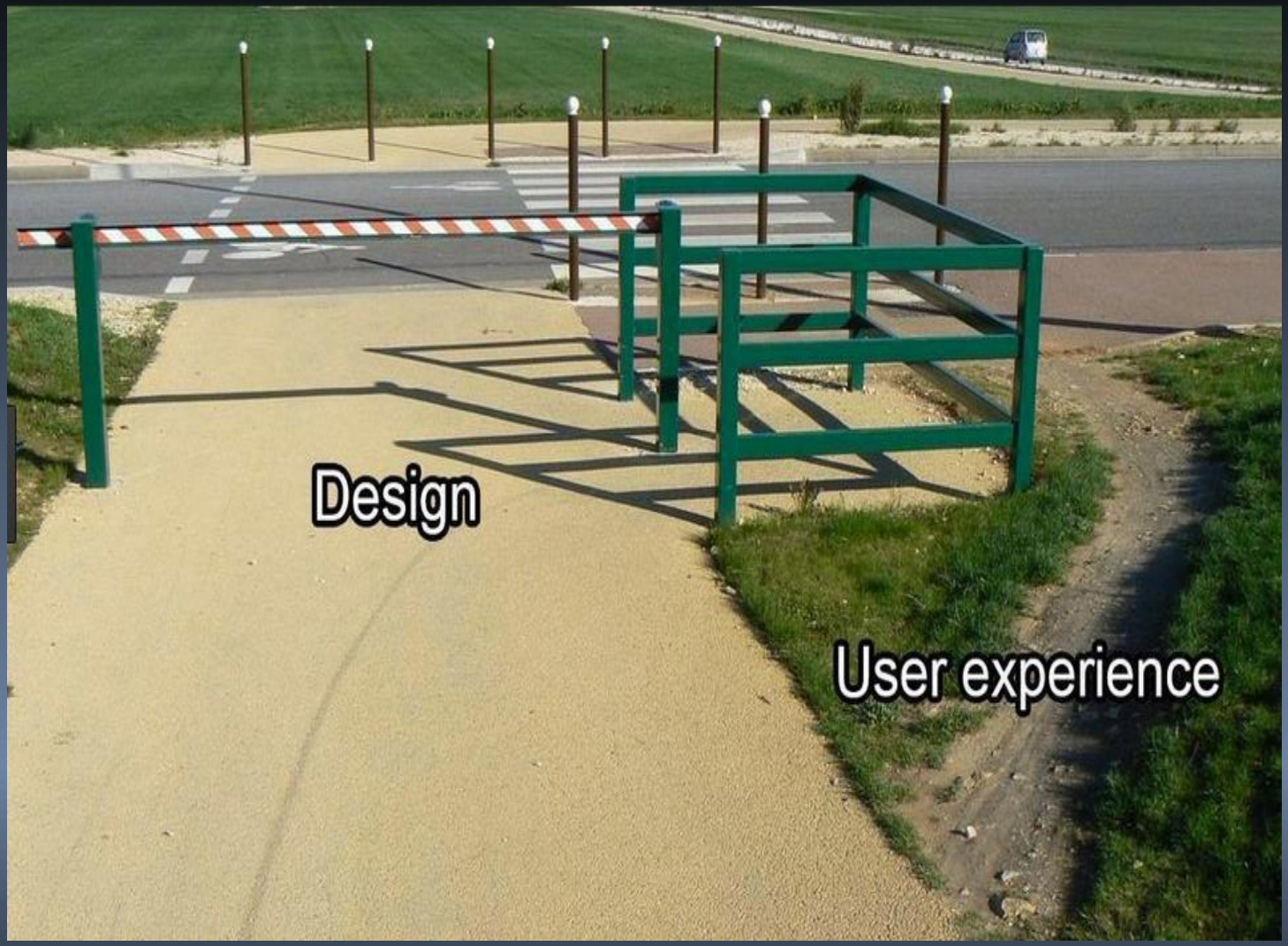

2011
3.4 디도스 공격
2012
개인정보 유출사고
(400만명)
언론사 해킹사고
2013
3.20 / 6.25
사이버 공격
2014
개인정보 유출사고
(1200만명)
2016
보안업체 해킹
(코드서명 인증서 유출)
개인정보유출사고
(1000만명)
2017
2018
호스팅 서비스 랜섬공격
평창올림픽 해킹
암호화폐 거래소 해킹
공급망 기업 해킹
2019~
기업 랜섬공격
(클롭, AD)
계정탈취 및 침투
공급망 기업 해킹

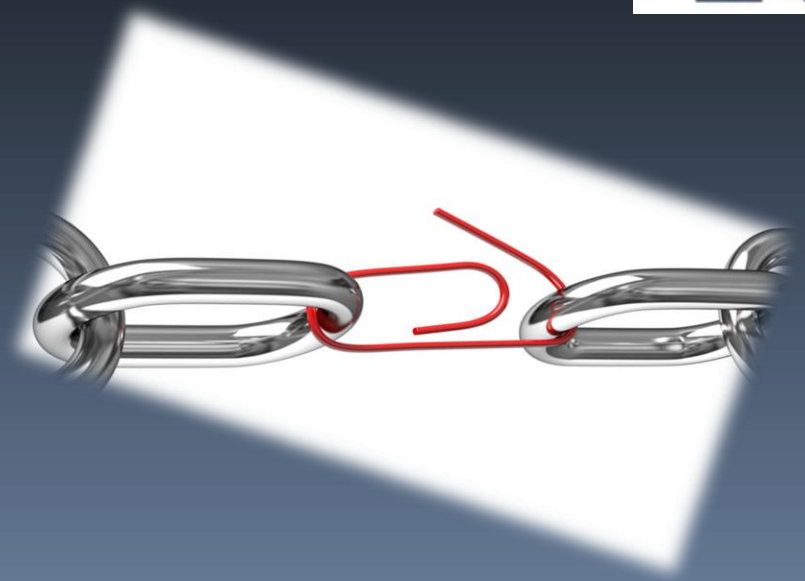
IoC 확대

방어 영역 확장

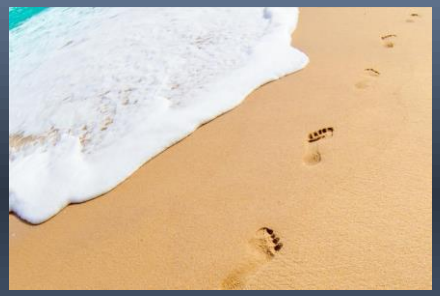
탐지 기술의 발전

많은 사고 사례의 간접 경험


Design
User experience



디자인 되지 않은 보안의 영역



방어자 환경에는 디자인 될 수 없는 영역이 항상 존재한다

특히, 공급망 이라는 공간은 더 넓어지고 있다

Kr/CERT, 가시성 확보 방법에 대한 새로운 접근 필요

보안 투자 기업, 피해 예방이 가능하고 공격자에게 큰 손실을 입힌다

그렇지 않는 기업, 공격에 쉽게 허물어지고,
사고 이후 디자인을 고민하는 것을 매우 어려워한다.

여전히 많은 사고들이 진행되고 있다

우리는 과거 보다 더욱

잘 준비되어 있는가?

최근 침해사고 사례

공격자의 움직임과 방어자의 고민

'2017년 국내 사이버 침해사고 분석 및 2018년 사이버위협 전망'

부제 : 변화의 흐름 속에서 우리는 안전한가?

은밀하게 위대하게

부제 : 해커의 전략과 흔적들

"2019 주요 침해사고 사례와 전망"

부제 : 방어자가 공격에 개입하는 것이 *왜* 어려운가?

사고분석

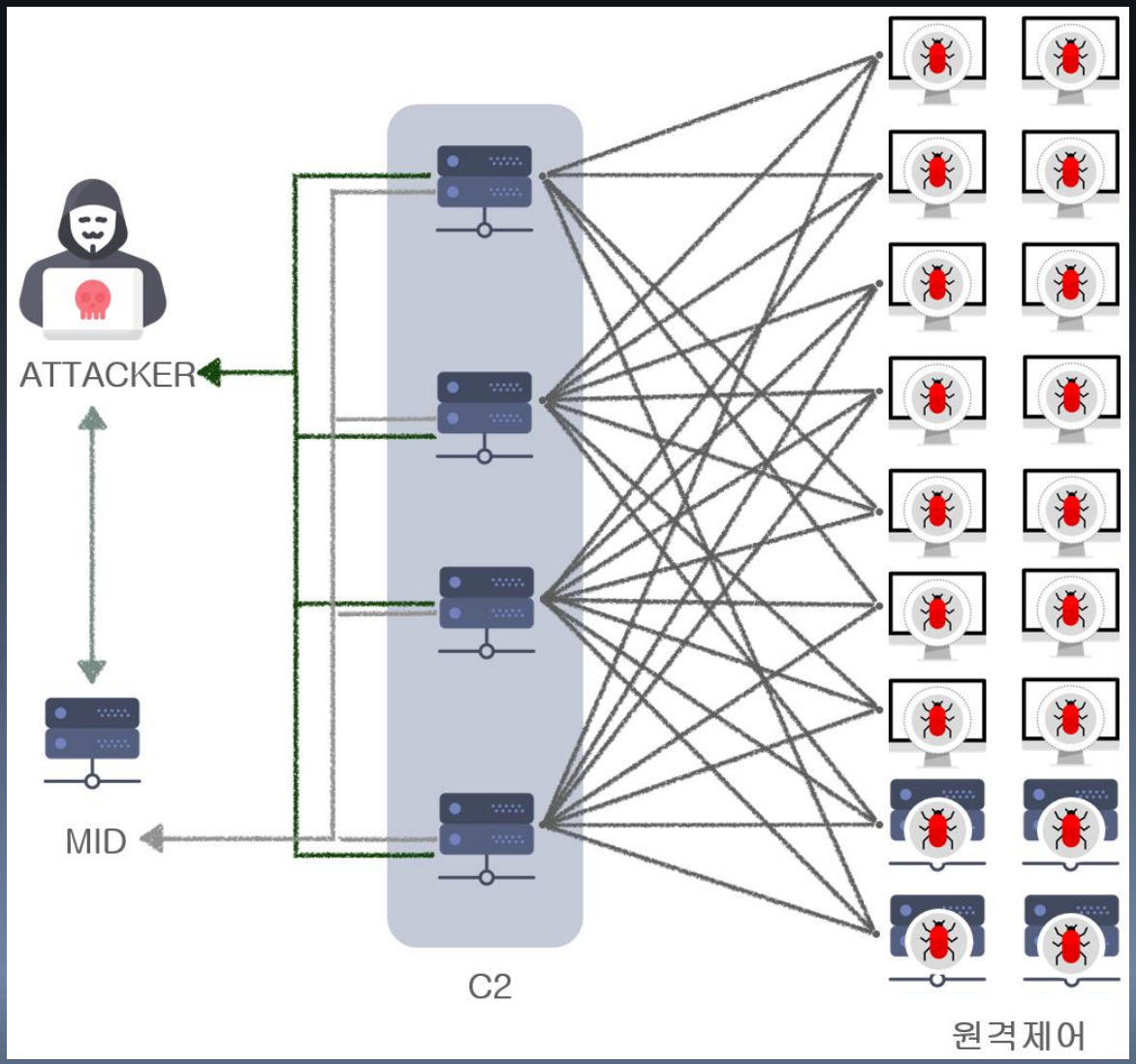
이미 발생된 피해

종합분석

활동중인 공격

IoC

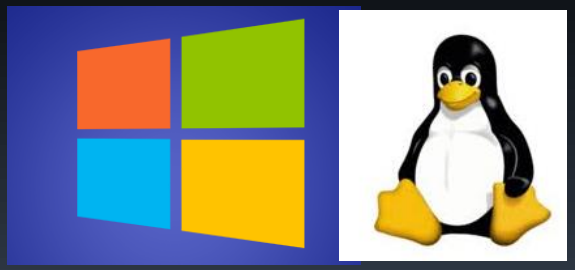
Indicator of Compromise



Malware

한번 노출된 C2는 재사용 하지 않는다

악성코드는 C2 변경이 용이하게 제작되고 있으며, C2 업데이트가 빈번히 발생

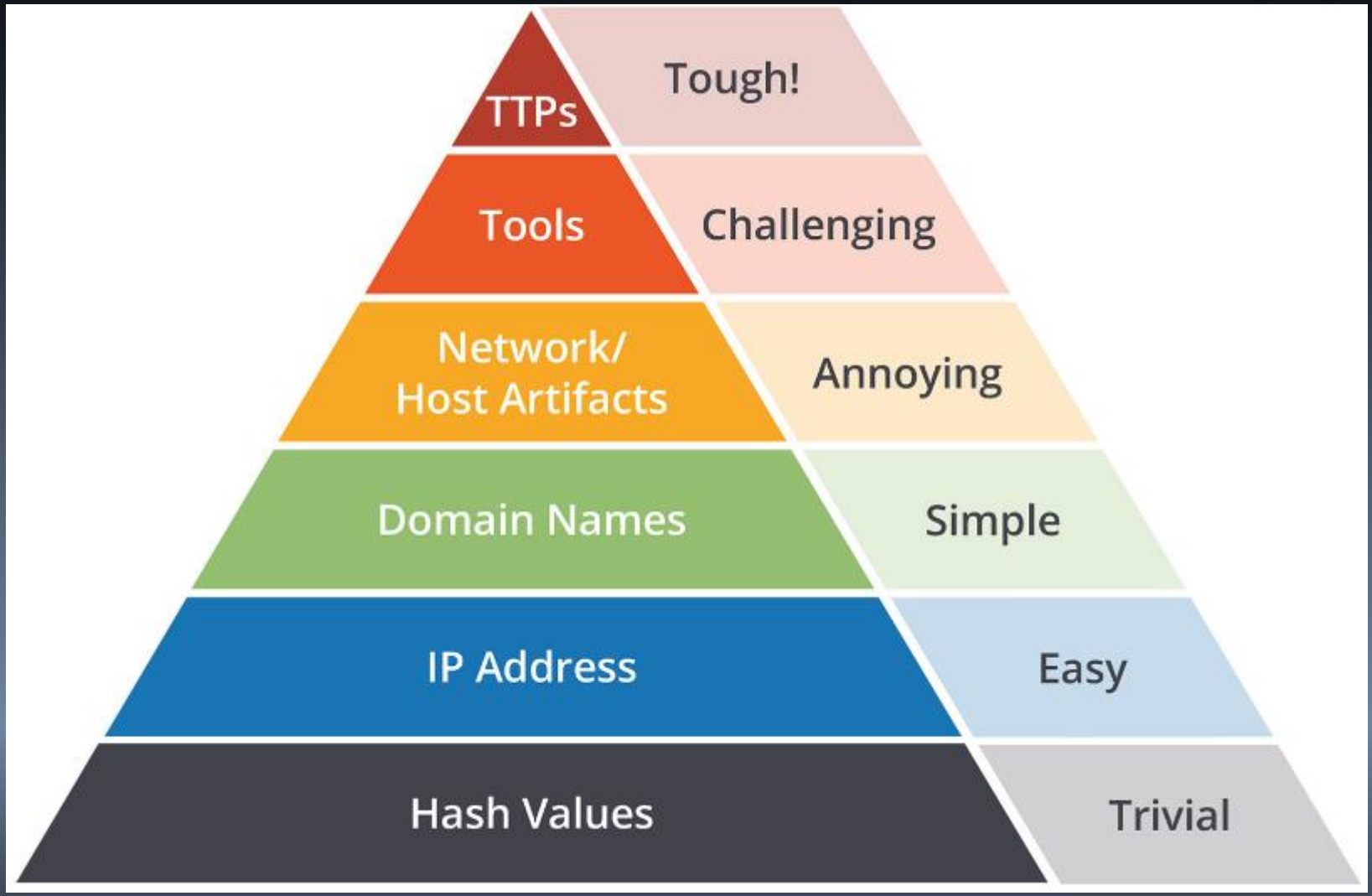


Exploit

SECURITY APPLIANCE

Attacker

어떻게?


TTPs
Tough!
Tools
Challenging
Network/
Host Artifacts
Annoying
Domain Names
Simple
IP Address
Easy
Hash Values
Trivial

IoC

Indicator of Compromise

IoA

Indicator of Attacks

공격의 효율성을 떨어뜨리고 피해를 최소화하기 위해

방어자가 개입할 수 있는 공간(방법론)을 제시하는 것이 목적

철학

✓사이버 공격은 단일한 행위가 아닌 여러 과정의 집합체

✓공격의 시작부터 완성까지 프로세스적인 성격을 보인다

✓공격이 시작되면 초기 단계와 진행단계, 심화되어져 가는 단계들이 존재하며

✓특정 공격 단계의 시행에 방어자가 개입하여 일부를 무력화 또는 지연시킨다면

✓공격의 효율성은 급격히 떨어지고 피해를 최소화 할 수 있다

Kill Chain

Intrusion Kill Chain

Cyber Kill Chain

ATT&CK

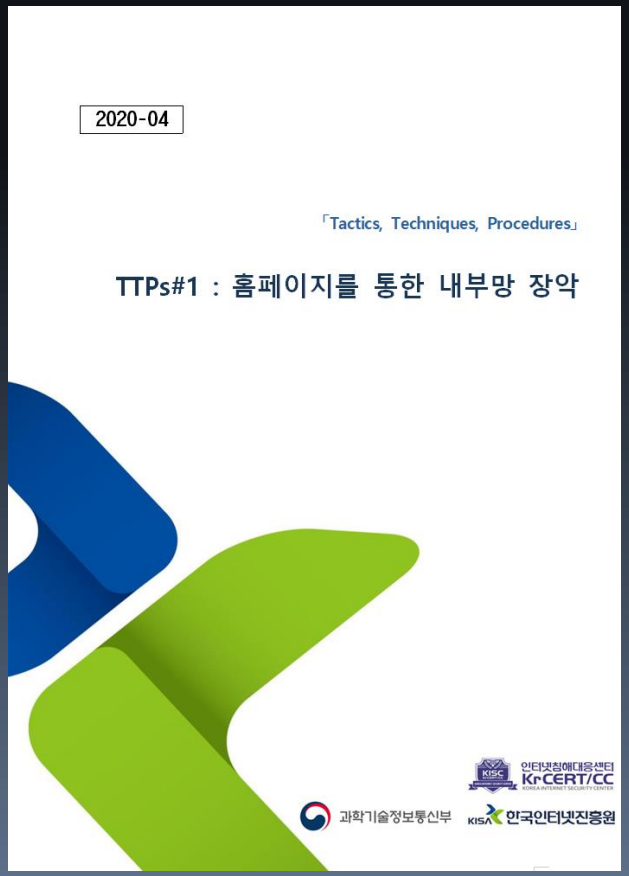
Adversarial Tactics, Techniques, &nd Common Knowledge

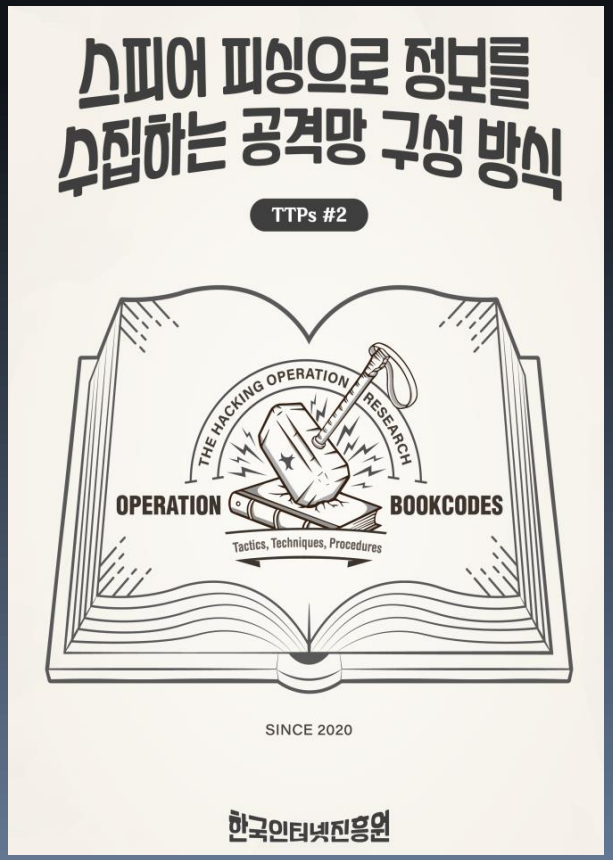
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
9 techniques	10 techniques	17 techniques	12 techniques	32 techniques	13 techniques

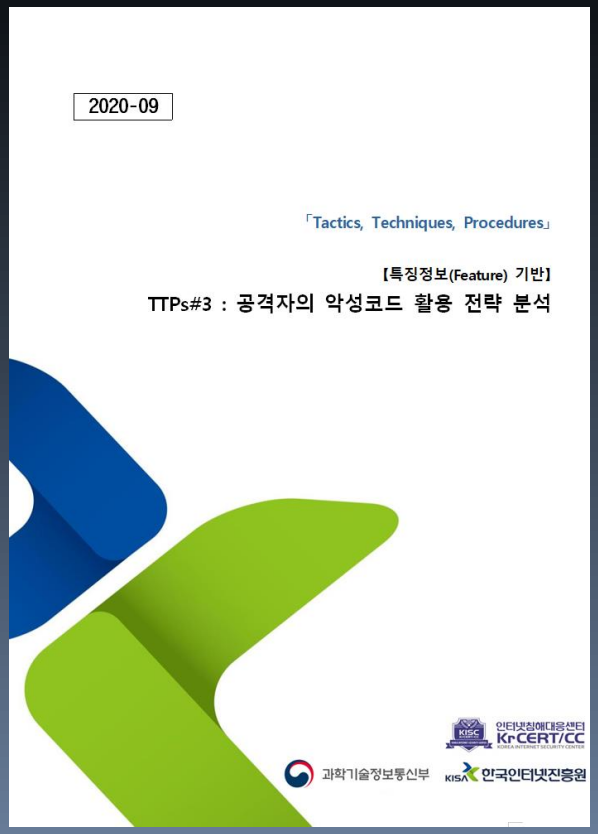
Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
22 techniques	9 techniques	15 techniques	16 techniques	8 techniques	13 techniques

TTPs

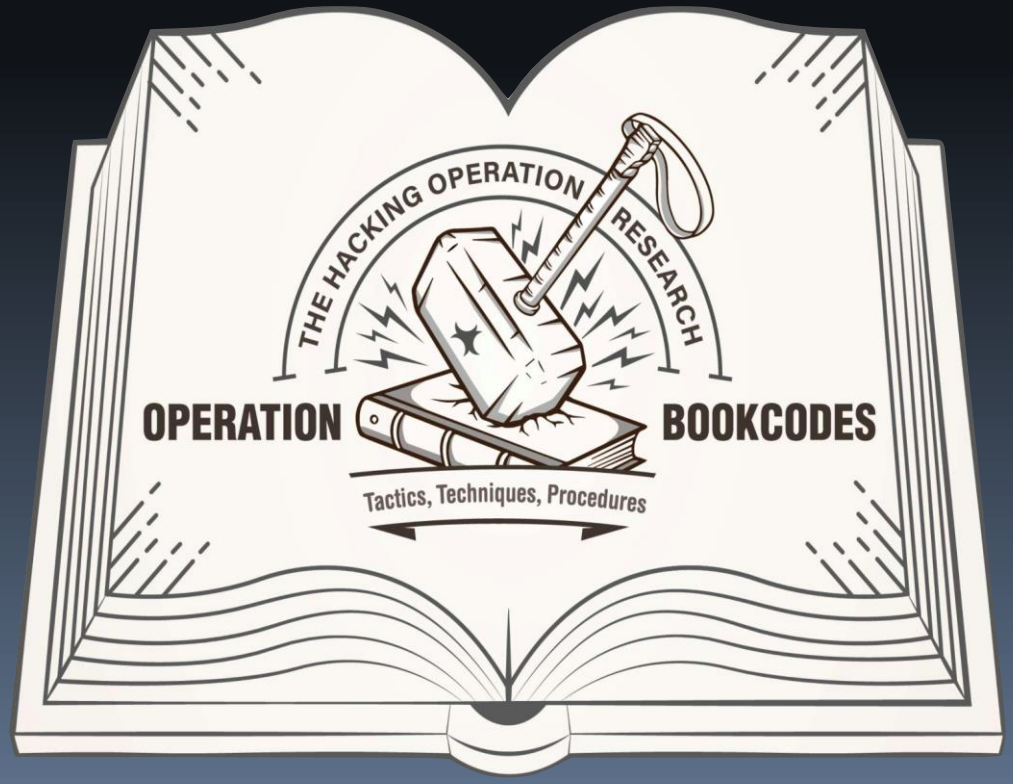
Tactics, Techniques, Procedure


2020-04
「Tactics, Techniques, Procedures」
TTPs#1 : 홈페이지를 통한 내부망 장악
과학기술정보통신부
KISA 한국인터넷진흥원


스피어 피싱으로 정보를
수집하는 공격망 구성 방식
TTPs #2
THE HACKING OPERATION RESEARCH
OPERATION BOOKCODES
Tactics, Techniques, Procedures
SINCE 2020
한국인터넷진흥원


2020-09
「Tactics, Techniques, Procedures」
【특징정보(Feature) 기반】
TTPs#3 : 공격자의 악성코드 활용 전략 분석
과학기술정보통신부
KISA 한국인터넷진흥원

TTPs #4

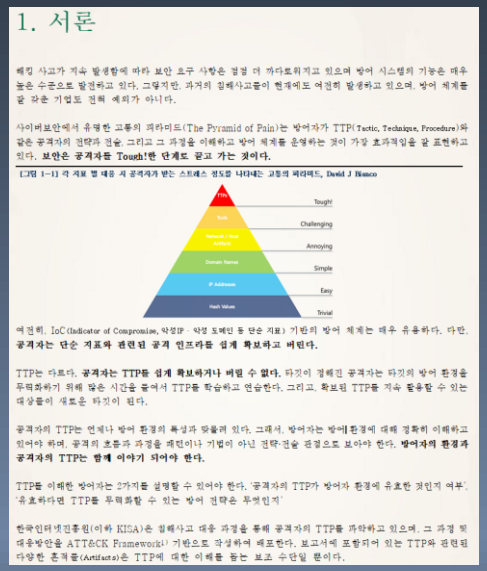


내부 보안 점검 및 강화

리눅스 환경

IoC?

Study Hard?



1. 서론

해킹 사고가 지속 발생함에 따라 보안 요구 사항은 점점 더 까다로워지고 있으며 방어 시스템의 기능은 매우 높은 수준으로 발전하고 있다. 그럼에도 불구하고 과거의 침해사고들이 현재에도 여전히 발생하고 있으며, 방어 체계를 뚫는 기법도 진화 예외가 아니다.

사이버보안에서 유명한 고통의 피라미드(The Pyramid of Pain)는 방어자가 TTP(Tactic, Technique, Procedure)와 같은 공격자의 전략과 전술, 그리고 그 과정을 이해하고 방어 체계를 운영하는 것이 가장 효과적임을 잘 표현하고 있다. **보안은 공격자를 Touch!한 단계도 묻고 가는 것이다.**

[그림 1-1] 각 지표 별 대응 시 공격자가 받는 스트레스 정도를 나타내는 고통의 피라미드, David J Bianco

여전히, IoC(Indicator of Compromise, 악성IP · 악성 도메인 등 단순 지표) 기반의 방어 체계는 매우 유용하다. 다만, **공격자는 단순 지표와 관련된 공격 인프라를 쉽게 확보하고 버린다.**

TTP는 다르다. **공격자는 TTP를 쉽게 확보하거나 버릴 수 없다.** 타깃이 정해진 공격자는 타깃의 방어 환경을 투력화하기 위해 많은 시간을 들여서 TTP를 학습하고 연습한다. 그리고, 확보된 TTP를 지속 활용할 수 있는 대상물이 새로운 타깃이 된다.

공격자의 TTP는 언제나 방어 환경의 특성과 맞물려 있다. 그래서, 방어자는 방어환경에 대해 정확히 이해하고 있어야 하며, 공격의 흐름과 과정을 패턴이나 기법이 아닌 전략·전술 관점으로 보아야 한다. **방어자의 환경과 공격자의 TTP는 함께 이야기 되어야 한다.**

TTP를 이해한 방어자는 2가지를 설명할 수 있어야 한다. '공격자의 TTP가 방어자 환경에 유효한 것인지 여부', '유효하다면 TTP를 투력화할 수 있는 방어 전략은 무엇인지'

한국인터넷진흥원(이하 KISA)은 침해사고 대응 과정을 통해 공격자의 TTP를 파악하고 있으며, 그 과정 및 대응방안을 ATT&CK Framework[1] 기반으로 작성하여 배포한다. 보고서에 포함되어 있는 TTP와 관련된 다양한 흔적물(Artifacts)은 TTP에 대한 이해를 돕는 보조 수단일 뿐이다.

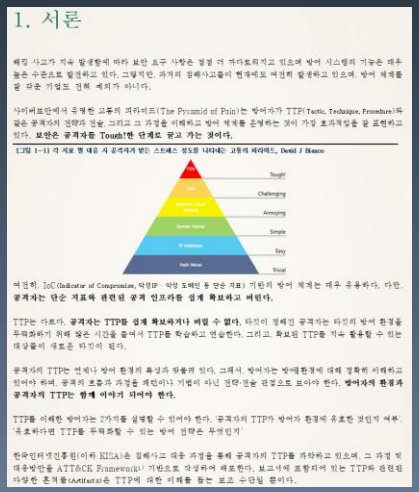
공격자의 TTP는 언제나 방어 환경의 특성과 맞물려 있다.

So What?

방어자는 방어 환경에 대해 정확히 이해하고 있어야 한다.

방어자는 공격의 흐름과 과정을 패턴이나 기법이 아닌
전략과 전술 관점으로 보아야 한다.

방어자의 환경과 공격자의 TTP는 함께 이야기 되어야 한다.



1. 서론

해킹 사고가 지속 발생함에 따라 보안 요구 사항은 점점 더 까다로워지고 있으며 방어 시스템의 기능은 매우 높은 수준으로 발전하고 있다. 그럼에도 불구하고 해킹사고들이 현재에도 여전히 발생하고 있으며, 방어 체계를 갖춘 기업도 안전 지대가 아니다.

사이버보안에서 유명한 고통의 피라미드(The Pyramid of Pain)는 방어자가 TTP(Tactic, Technique, Procedure)와 같은 공격자의 전략과 절술, 그리고 그 과정을 이해하고 방어 체계를 운영하는 것이 가장 효과적임을 잘 표현하고 있다. **보안은 공격자를 Touch!한 단계로 묻고 가는 것이다.**

[그림 1-1] 각 지표 별 대응 시 공격자가 받는 스트레스 정도를 나타내는 고통의 피라미드, David J Bianco

Tough
Challenging
Annoying
Simple
Easy
Trivial

여전히, IoC(Indicator of Compromise, 악성IP, 악성 도메인 등 단순 지표) 기반의 방어 체계는 매우 유용하다. 다만, **공격자는 단순 지표와 관련된 공격 인프라를 쉽게 확보하고 버린다.**

TTP는 다르다. **공격자는 TTP를 쉽게 확보하거나 버릴 수 없다.** 타깃이 정해진 공격자는 타깃의 방어 환경을 무력화하기 위해 많은 시간을 들여서 TTP를 학습하고 연습한다. 그리고, 확보된 TTP를 지속 활용할 수 있는 대상들이 새로운 타깃이 된다.

공격자의 TTP는 전체나 방어 환경의 특성과 맞물려 있다. 그래서, 방어자는 방어환경에 대해 정확히 이해하고 있어야 하며, 공격의 흐름과 과정을 파편이나 기법이 아닌 전략·절술 관점으로 보아야 한다. **방어자의 환경과 공격자의 TTP는 함께 이야기 되어야 한다.**

TTP를 이해한 방어자는 2가지를 설명할 수 있어야 한다. '공격자의 TTP가 방어자 환경에 유효한 것인지 여부', '유효하다면 TTP를 무력화할 수 있는 방어 전략은 무엇인지'

한국인터넷진흥원(이하 KISA)은 침해사고 대응 과정을 통해 공격자의 TTP를 파악하고 있으며, 그 과정 및 대응방안을 ATT&CK Framework[1] 기반으로 작성하여 배포한다. 보고서에 포함되어 있는 TTP와 관련된 다양한 흔적들(Artifacts)은 TTP에 대한 이해를 돕는 보조 수단일 뿐이다.

TTP를 이해한 방어자는 2가지를 설명할 수 있어야 한다.

1) 공격자의 TTP가 방어자의 환경에 유효한 것인지 여부

2) 유효하다면 TTP를 무력화 할 수 있는 방어 전략은?

보고서에 포함되어 있는 TTP와 관련된 다양한 흔적들(Artifacts)은 단지 TTP에 대한 이해를 돕는 보조 수단

우리는

잘 준비되어져 가고 있는가?

감사합니다.