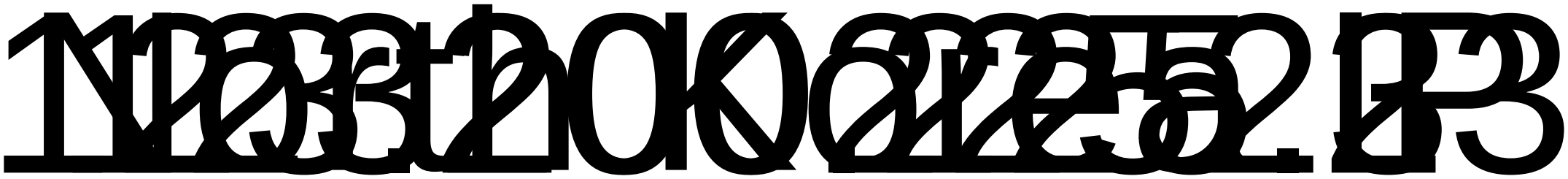
INTELLIGENCE LED SECURITY

김현준 상무 / 기술 지원 총괄

FireEye
SECURITY REIMAGINED

THREAT INTELLIGENCE 의 정의



Actionable
Forward Looking
Prioritizes Alert and Actions

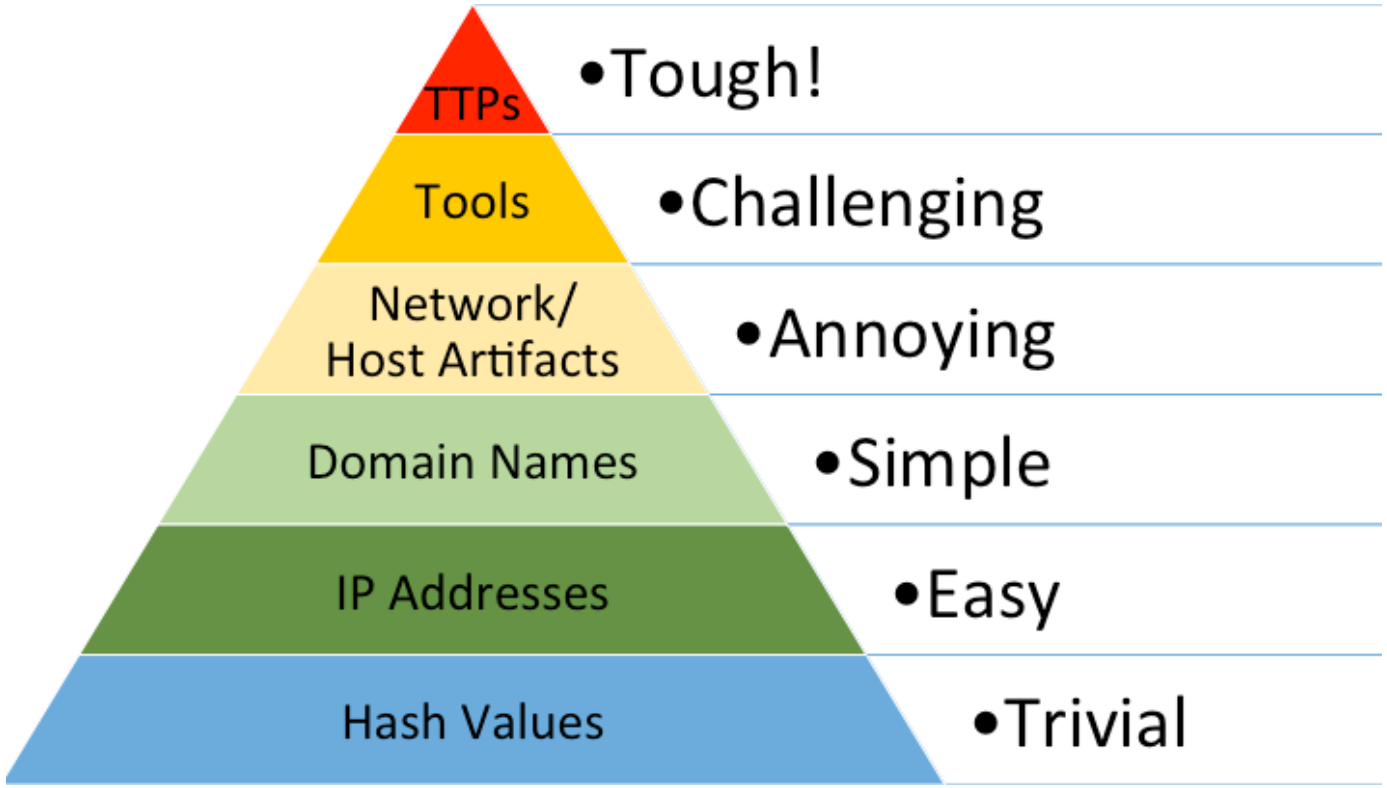
FireEye

Information vs Intelligence

INFORMATION	INTELLIGENCE
가공/정제 되지 않은 데이터	분류 되고 정제된 정보
평가 되지 않은 정보	분석 전문가에 의해 평가가 완료된 정보
가능한 모든 source 로 부터의 데이터 취합	신뢰할만한 source 로 부터의 데이터 취합 및 정확성을 위한 상호 분석
정확할 수도 있고, 틀릴 수도 있고, 잘못된 이해, 불완전한, 관계 있을 수도 있고 관계 없을 수도 있음	정확하고, 신속하고, 관계가 있으며 분석이 완료된 정보

Or as the FBI put it: *"simply defined, intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions – specifically, decisions about potential threats to our national security."*

Intelligence 의 종류



- MD5 hash / IP address /Domain 은 공격자가 쉽게 변경 가능
- Network/host artifact 는 분석이 어려움
- TTP 가 가장 확보 하기 어려우나 가장 유용

현재 보안 현실

보안 전문가 부족

너무 많은 이벤트

엔드포인트 가시성 부족

FireEye

사이버 위협에 대한 이해

공격의 실체는 악성 코드가 아니라 사람

공격의 배후에는 사람이 존재

정상 윈도우 툴 이용

공격자의 습성 파악이 중요

체계적으로 전문화되고 금전적 후원을 받는 조직

고도의 전략을 구사

목적 달성을 위해 치밀 하게 준비

공격 방법을 변경 후 지속적인 공격 시도

특정 목적 존재

목적을 이루기 전에는 공격을 멈추지 않음

지속적인 공격 시도

최근 사이버 위협 – 방글라데시 은행 해킹

- 2월초 81M (약 1,000 억원)이 해킹으로 인해 도난됨
- 자금 인출 몇 주전 부터 악성코드 (RAT)를 통해 내부 시스템 관찰 – SWIFT code 유출
- zero day exploit 및 custom 악성 코드 사용
- Mandiant 에서 침해 조사 중

http://fortune.com/2016/03/12/malware-bangladesh-bank-heist/

Malware Suspected in Bangladesh Bank Heist

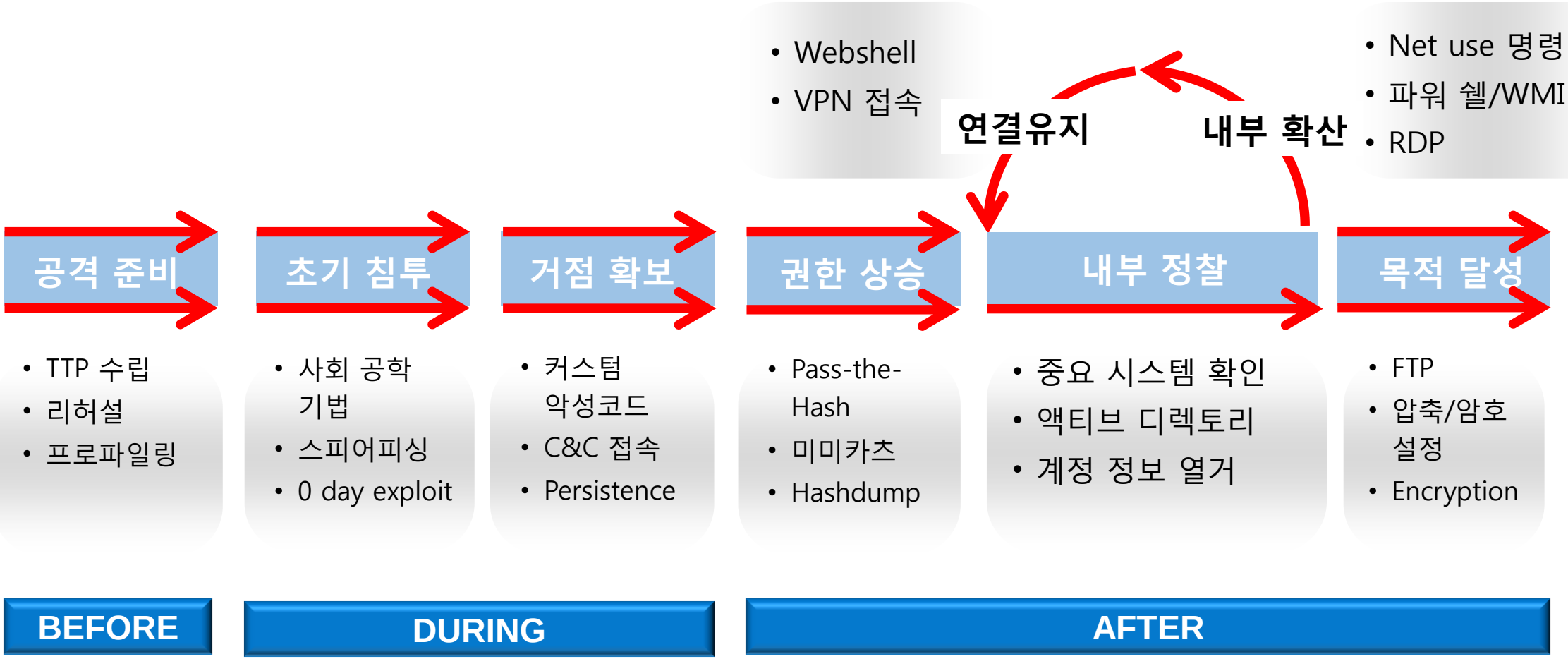
by Reuters MARCH 12, 2016, 12:02 PM EDT

Malware gave hackers an inside look at the bank's systems.

Commuters pass by the front of the Bangladesh central bank building in Dhaka March 8, 2016. REUTERS/Ashikur Rahman

FireEye

사이버 위협의 전개 과정



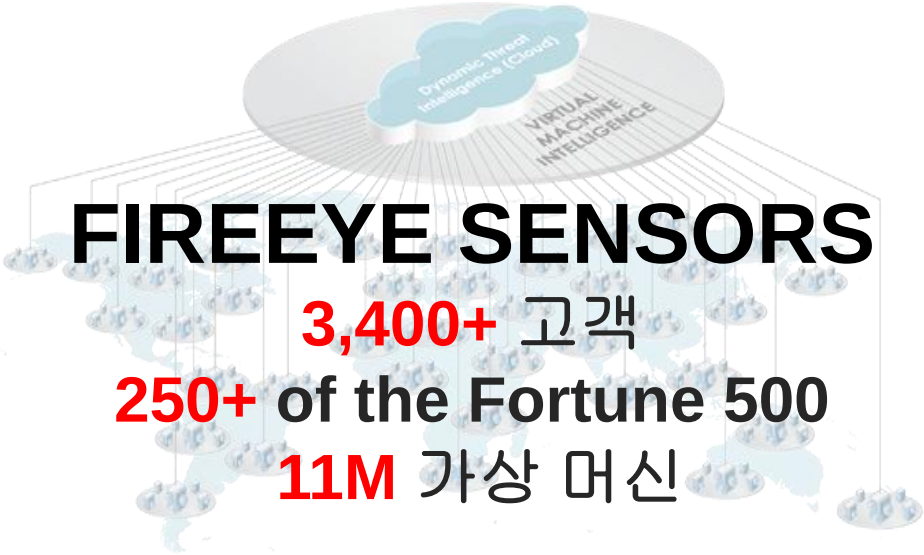
FireEye Intelligence Coverage

BEFORE

iSIGHT

20 locations worldwide
29 languages
18 countries
300 experts

DURING



FIREEYE SENSORS

3,400+ 고객
250+ of the Fortune 500
11M 가상 머신

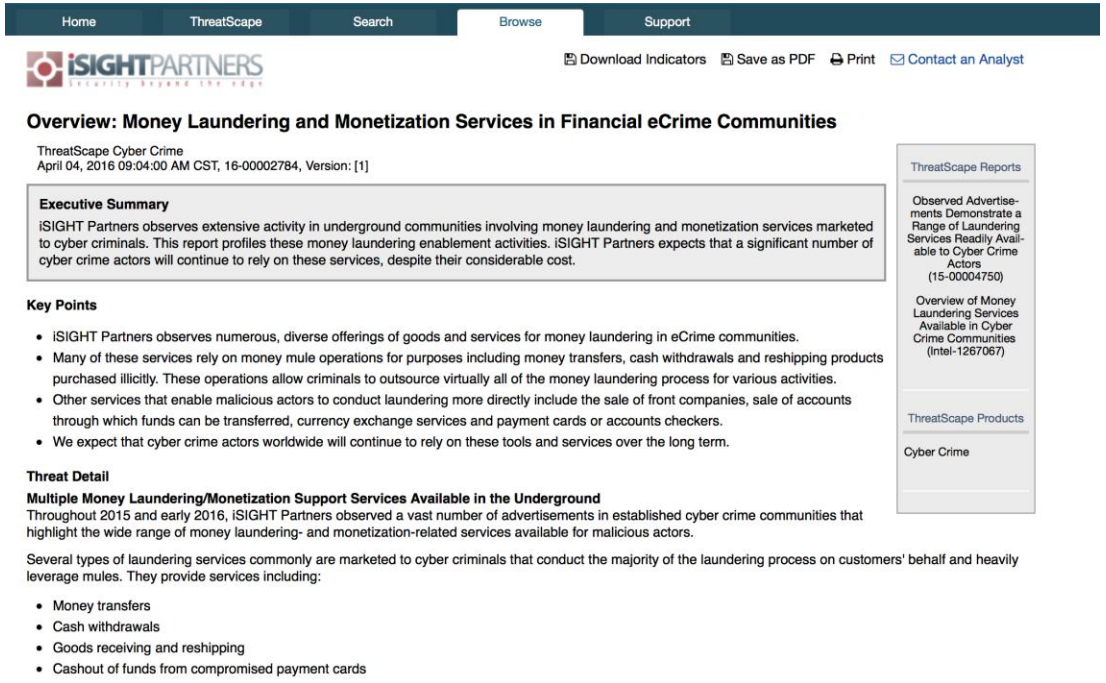
MANDIANT

AFTER

1,200+ 고객
200+ of the Fortune 500
200 건 이상의 침해 대응

iSIGHT Intelligence

- Human intelligence
- 2007년 부터 Threat intelligence 제공
- 공격자의 TTP 및 context 제공
- 16,000 공격 그룹 추적
- API/SDK 지원
- Clint Engagement Manager

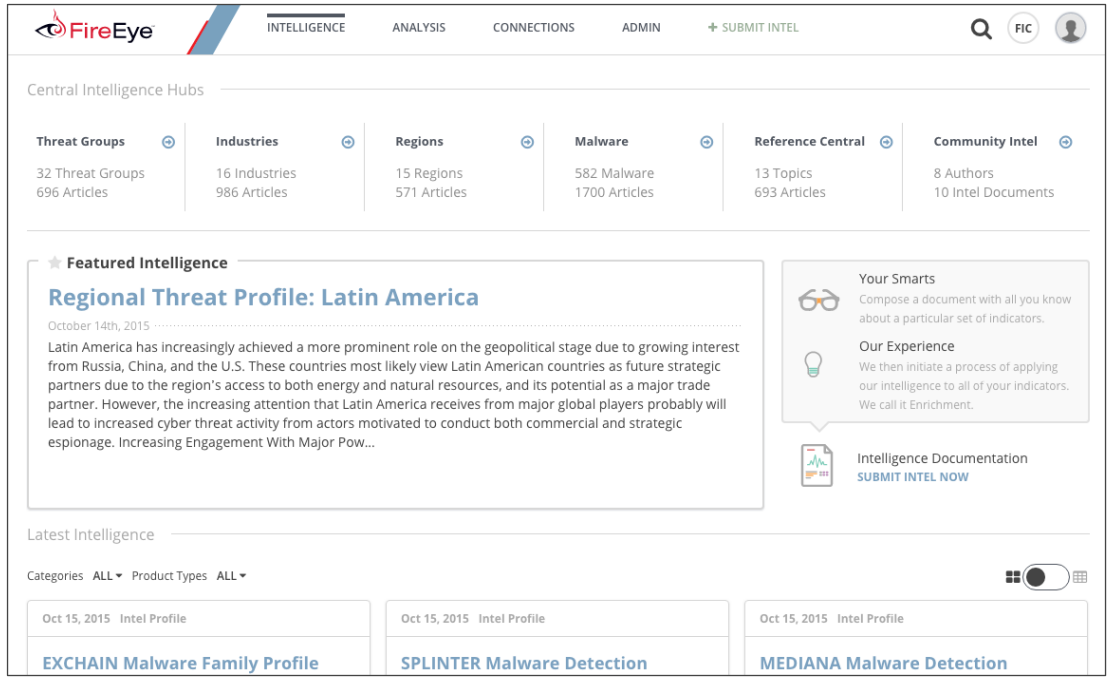


FireEye intelligence

- Machine intelligence
- 11M 의 가상머신이 분석 결과 공유
  - 매일 50조 이상의 VM 분석
  - 매일 40만개의 새로운 샘플 분석
  - 매일 1조 5천억개의 URL 분석
- 최근 40개의 zero day exploit 중 22개를 최초 발견

Mandiant intelligence – FIC

- 300여개의 nation state 공격 그룹 추적
- 공격 그룹별/산업군별/지역별/악성코드별 intelligence 제공
- 공격자의 TTP 및 공격의 context 제공
- 매년 200 건 이상의 침해 조사를 통해 intelligence 수집



THANK YOU

FireEye