CIO Summit 2012

CIO Summit 2012

창조적 혁신으로 새로운 가치를 창출하라!

IT Creative Innovation for New Value!

전자신문 CIO BIZ 한국CIO포럼 FORUM

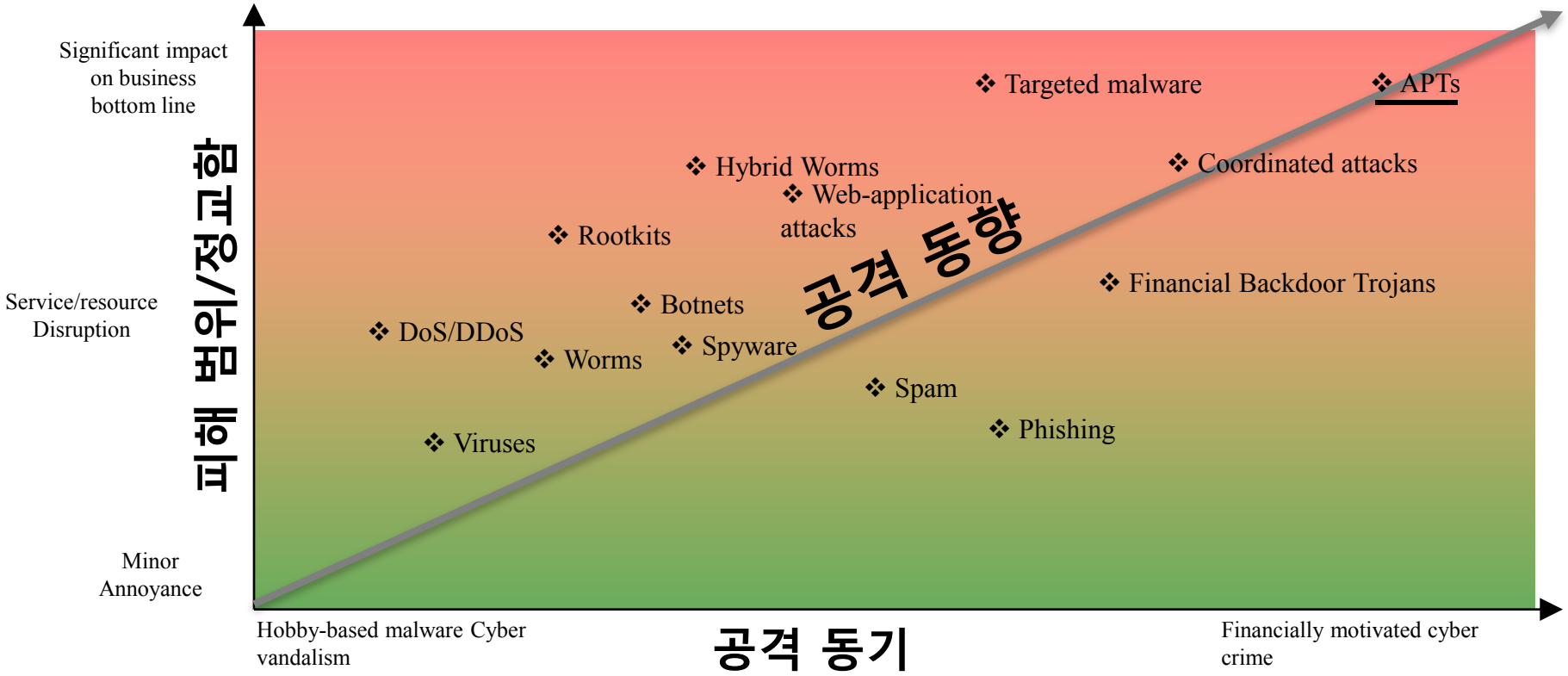
APT 공격에 따른 대응 전략

조남용 | 차장
EMC

지능형 지속 공격
(Advanced Persistent Threat : APT)

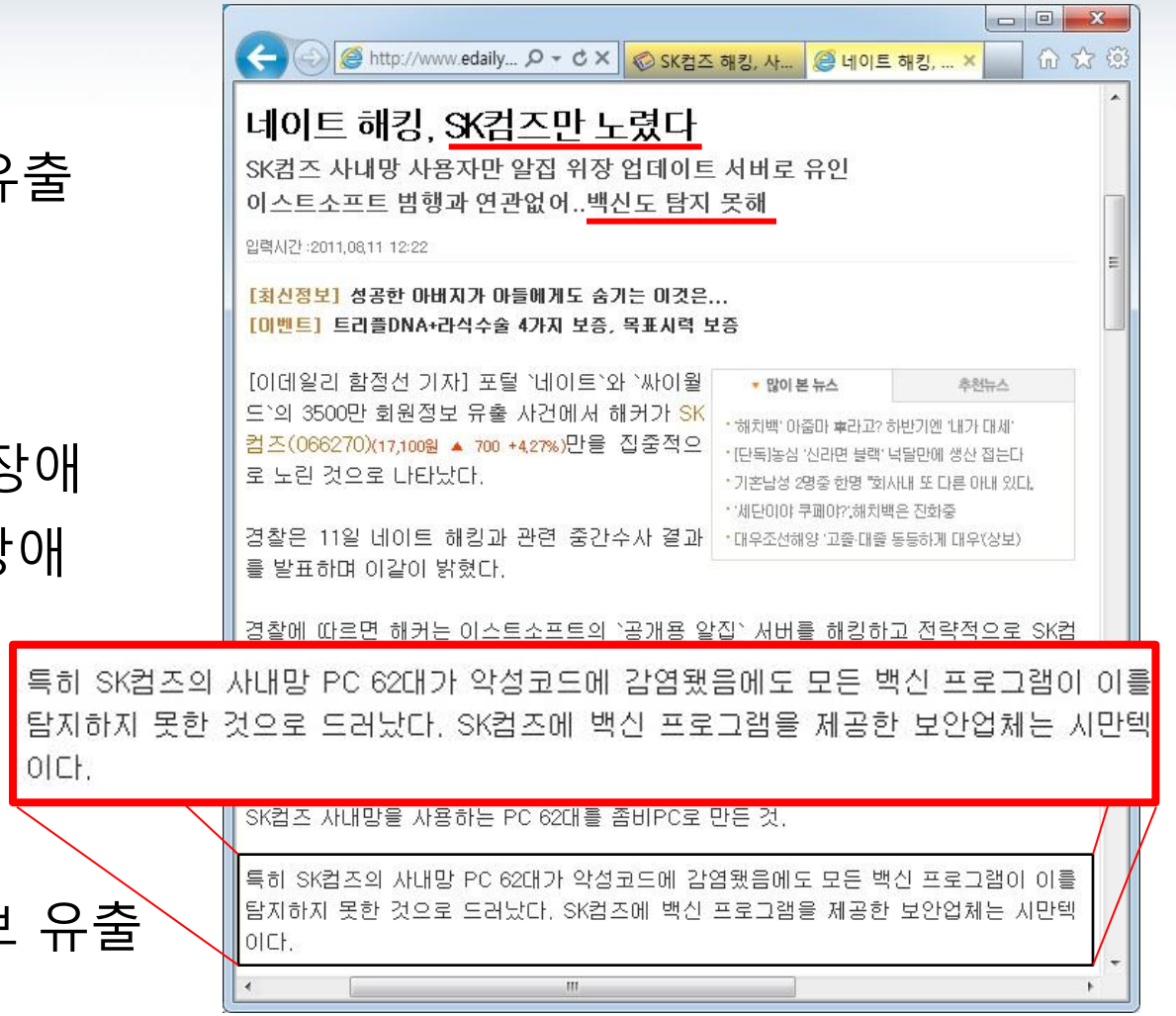
Changing Threat Environment

- 금전적 이득을 위한 사이버 범죄
- 비즈니스 기반에 막대한 위협 초래
- 정교함 / 피해범위 / 공격의 속도가 급격히 증가
- Advanced Persistent Threats (APTs)



지능형 지속 공격(APT) 사례

- 현대캐피탈
  - 고객 43만 명 정보 유출
- 농협
  - 운영 서버 200여대 장애
  - 은행 및 카드 업무 장애
  - 원장 데이터 손실
- SK컴즈
  - 회원 3,500만 명 정보 유출

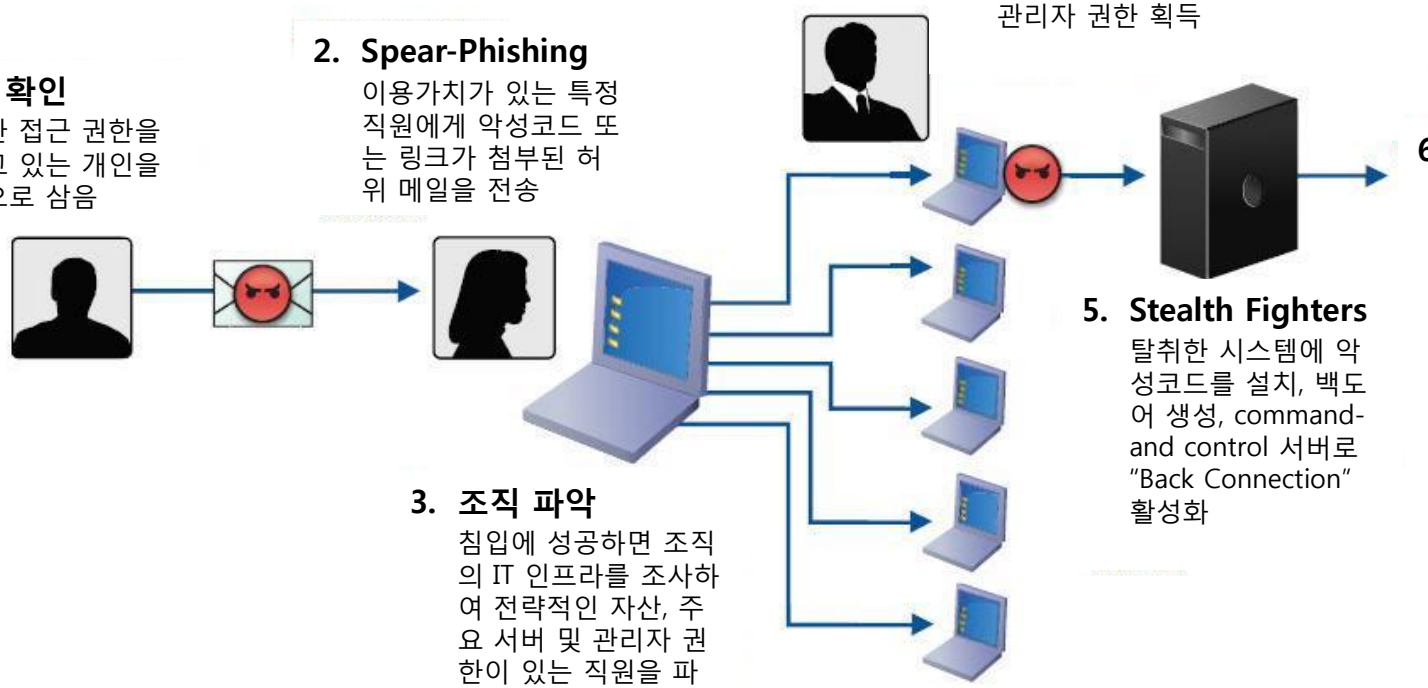


지능형 지속 공격(APT)

- 지능형 지속 공격 (APT)
  - 공격자가 특징 기업 혹은 조직의 기밀 정보를 획득하기 위해 장기간 동안 은밀하게 진행하는 공격 형태
- 주요 특징
  - 특정 조직에 최적화된 공격 수행
  - 충분한 시간과 비용을 투자
  - 조직 및 구성원 개인에 대한 충분한 정보 수집
    (사회공학적인 방법 이용)
  - 탐지 회피
    - low and slow 전략
    - 알려지지 않은 악성코드(Zero-Day Attack) 사용
    - 이상징후를 파악하지 못하도록 장기간에 걸쳐 은밀히 활동
  - 다양한 방향으로 공격, 사용자 및 Endpoint에 집중

지능형 지속 공격(APT)

일반적인 공격 단계



1. 표적 확인
필요한 접근 권한을 가지고 있는 개인을 표적으로 삼음

2. Spear-Phishing
이용가치가 있는 특정 직원에게 악성코드 또는 링크가 첨부된 허위 메일을 전송

3. 조직 파악
침입에 성공하면 조직의 IT 인프라를 조사하여 전략적인 자산, 주요 서버 및 관리자 권한이 있는 직원을 파악

4. 권한 상승
추가적인 Spear-Phishing 또는 권리자 계정 탈취를 통해 관리자 권한 획득

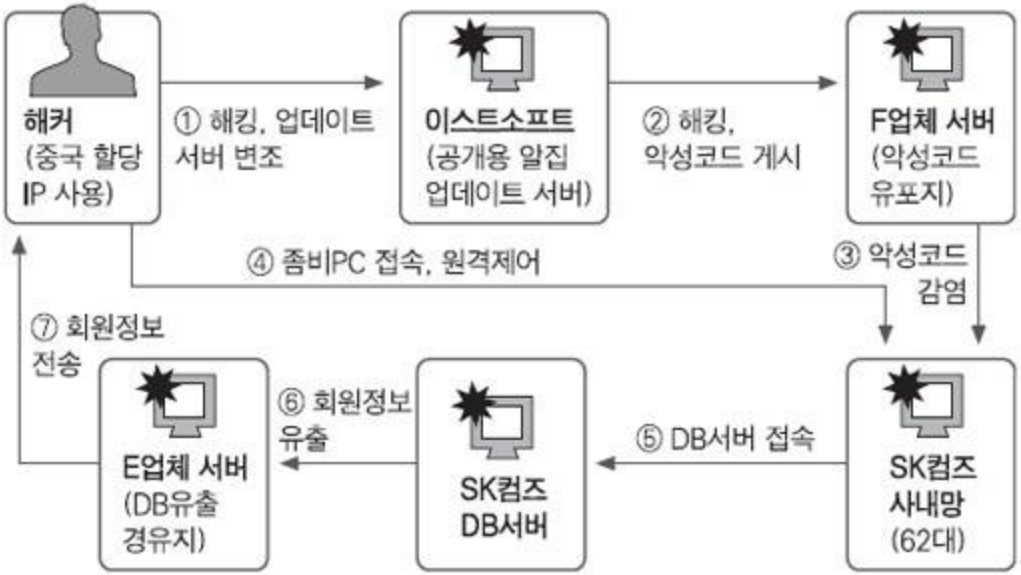
5. Stealth Fighters
탈취한 시스템에 악성코드를 설치, 백도어 생성, command-and control 서버로 "Back Connection" 활성화

6. D-day
Command-and-control 인프라를 활성화하여 탈취한 정보를 압축/암호화하여 전송

지능형 지속 공격(APT)

국내 공격 사례

SK컴즈 회원정보 유출 상황



출처:한국일보

SK컴즈의 3500만 개인정보 유출 개념도

출처:디지털타임스

지능형 지속 공격(APT)

기존 보안 시스템 우회

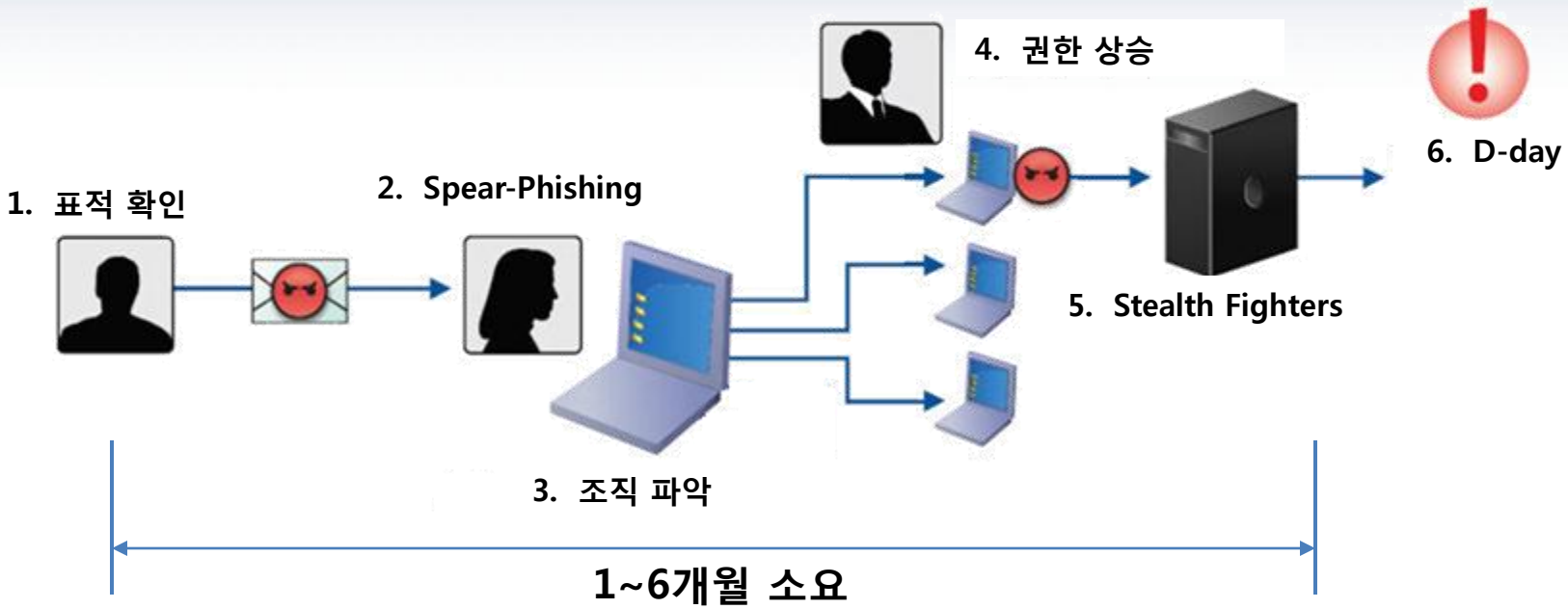
- Firewall
  - 대부분의 Firewall은 외부에서 내부로의 접속을 제어
  - 내부에서 외부로의 연결이 허용된 포트 사용
    - 일반적으로 HTTP (80)포트를 사용하여 내부에서 외부에 있는 원격 조종 서버로 연결

- IDS/IPS 및 Anti-Virus
  - IDS/IPS 및 Anti-Virus는 알려진 악성코드에 대한 Signature 기반 탐지
  - 지능형 지속공격(APT)에서는 알려지지 않은 신종/변종 악성코드 사용

- 보안 관제
  - 원하는 정보를 얻기까지 장기간에 걸친 은밀한 활동
  - 일반적인 Worm 및 공격 탐지 패턴에 발각되지 않음

지능형 지속 공격(APT) 대응 방안

지능형 지속 공격(APT) 대응 방안



- 공격자가 원하는 정보에 접근하기 까지 소요 시간 지연
  - 네트워크 분리 (망 분리)
  - 내부 시스템 인증 강화
- 공격자가 원하는 정보에 접근하기 이전 단계에서 탐지 / 제거
  - 알려지지 않은 악성코드(Zero-Day Attack) 탐지 / 제거
  - 악성코드 / bot-net / Command & Control 지점 접근 트래픽 탐지 / 차단

지능형 지속 공격(APT) 대응 방안

공격자의 공격 소요 시간 지연

- 공격자가 원하는 정보를 획득하기까지의 시간 지연
  - 조직의 보안 체계가 일정 수준 이상 갖추어져 있을 경우 공격자는 최초 잠임 후 원하는 정보에 도달하기 까지 1개월~6개월 정도의 시간이 필요
  - APTs 공격 소요 시간 지연을 위한 주요 보안 조치
    - 시스템 패치 관리
      - 악성코드 공격의 성공률을 낮추어 내부 시스템을 점령에 많은 시간 필요
    - 내부 인증 강화
      - OTP, Smart Card 등을 이용한 인증 내부 시스템 인증 강화는 악성코드를 이용한 계정 탈취를 어렵게 함
    - 망 분리
      - 업무 망과 주요 시스템 운영 망을 분리하여 업무 망에 악성 코드가 감염되더라도 주요 시스템에 접근을 어렵게 함
    - 중요 정보 확산 방지 및 암호화
      - 주요 기밀 정보에 대한 보호 등급 설정 및 주기적 검색을 통한 정보 확산 방지
      - 주요 기밀 정보에 대한 암호화 적용 및 암호화 키 관리

지능형 지속 공격(APT) 대응 방안

공격에 대한 탐지 / 제거

알려지지 않은 악성코드(Zero-Day Attack) 탐지

- 외부로부터 유입되는 모든 실행파일에 대한 전수조사 실시
- 비 정상적인 실행 파일 분석을 통해 Zero-Day Attack이 의심되는 파일 탐지
- SandBox에서 실행파일을 실행시켜 행위를 모니터링하여 악성코드와 흡사한 행위를 하는지 분석
  - SandBox : 테스트를 목적으로 구현된 독립된 실행 환경으로 주로 검증되지 않은 코드를 실행하여 행위 모니터링에 사용됨

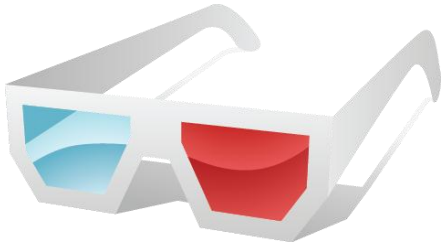
모든 네트워크 트래픽 저장 및 모니터링

- 비 정상적인 경로를 통한 실행파일 유입 탐지
  - 브라우저 취약점 이용
  - 실시간 Botnet, 악성코드 배포지점 정보를 이용한 의심스러운 파일 다운로드 탐지
- 외부로 연결이 허용된 트래픽(80, 443 port 등) 모니터링으로 외부 공격자로의 접속을 탐지
  - 접속 Port 와 실제 프로토콜의 일치여부 확인 (예: HTTP 프로토콜을 사용하지 않는 80 port 트래픽)
  - 의심가는 IP 로의 접속 내용 확인 (실시간 Botnet, Command&Control 지점 정보 이용)

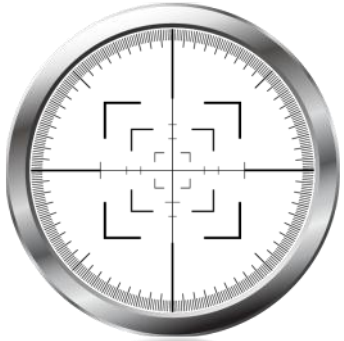
NetWitness 개요

NetWitness Is …

혁신적인
네트워크 모니터링
솔루션



네트워크
행위 및 내용에 대한
광범위한 가시성



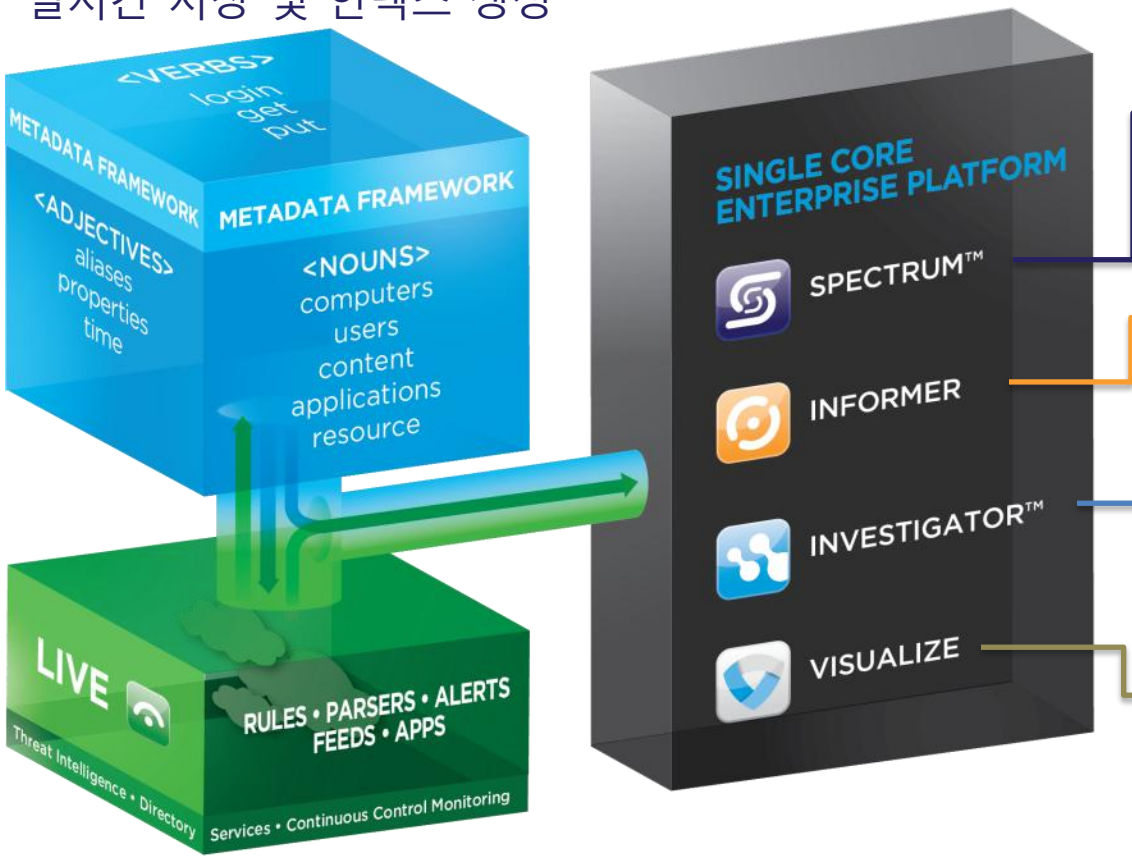
정확하고
실효적인 대응체계
제공

Know Everything. Answer Anything.

NetWitness

Network Security Analysis Platform

모든 네트워크 트레픽의
실시간 저장 및 인덱스 생성



자동화된 악성코드 분석 및 위험도 평가

자동화된 위협 보고서 및 경보

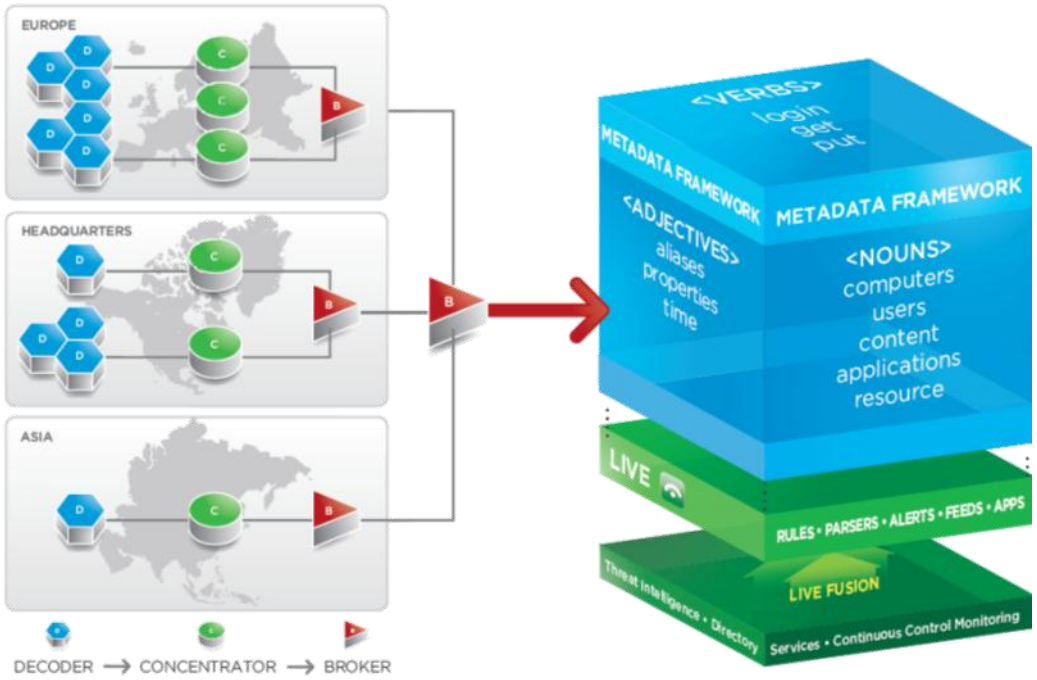
즉각적인 원인 파악 및 분석

혁명적인 가시화를 통한 신속한 Content 리뷰

NetWitness 주요 기능

NetWitness NextGen Platform

Session 기반 네트워크 분석 플랫폼



- NextGen Platform
  - 네트워크상의 모든 트래픽 저장
  - 네트워크 트래픽을 세션단위로 인덱스
    - Source IP / Port,
      Destination IP / Port
    - Protocol
      (HTTP/MSN IM/POP3/SSH)
    - Action (login/get/sendto/attach)
    - File Type (exe/pdf/jpg)
    - Etc
  - 실시간 인덱스 생성
  - 인덱스 기반 고속 검색
  - 네트워크 트래픽 정보를 이용한
    상세 내용 조회
  - NextGen 플랫폼에 다양한 어플리케이션 구현
    - Spectrum/Informer/Investigator/Visualize

NetWitness Investigator

Network Session 기반 대화형 분석 솔루션

Investigator

- Layer 2-7 컨텐츠에 대해 세션기반 대화형 분석 방식 제공
- Port에 독립적인 세션 기반 분석 (특허기술/수상경력)
- 사용자 친화적인 데이터 표현

  (Web, Voice, Files, Emails, Chats, etc.)
- 대용량 데이터 고속 검색
  - 수 테라 바이트 데이터를 인덱스 기반 고속 검색
  - 신속한 분석
- 전세계 50,000 이상의 보안 전문가들이 Freeware 사용 중

NetWitness Spectrum

Signature-free 악성코드 탐지 솔루션

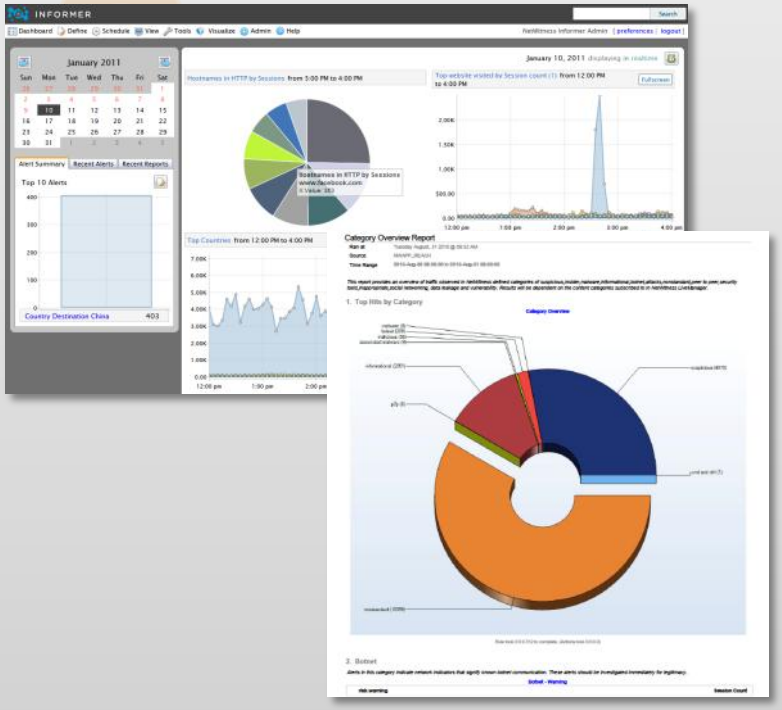
Spectrum

- 알려지지 않은 악성코드(Zero-Day Attack) 탐지
- 네트워크 상의 모든 실행파일에 대해 다양한 관점에서 악성코드 여부 분석
  - File
    - 파일의 고유 속성 / 파일 헤더 정보를 분석하여 변조된 실행파일 탐지
  - NextGen
    - 파일 출처에 대한 네트워크 정보를 확인하여 비 정상적인 유입경로 확인
  - Community
    - 해당 파일의 Signature에 대해 Online Community에 질의
  - SandBox
    - 실행파일을 테스트 환경에서 실제 실행하여 악성코드 행위 탐지

NetWitness Informer

Monitoring & Alerting

Informer



- 위협 상황을 종합적으로 인지할 수 있는 유연한 대시보드 제공
- 다양한 부서에서 사용
  - 네트워크 보안
  - 내부 보안 / 인사관리
  - 법무 / R&D / 감사
  - I/T 운영
- HTML, PDF 등 다양한 리포트 제공
- SIEM과 완벽한 연동을 위해 다양한 로그 전송 방식 제공
  - CEF, SNMP, syslog, SMTP

NetWitness Visualize

네트워크 컨텐츠의 혁신적인 가시화

Visualize

- 네트워크 컨텐츠의 가시성을 제공하는 혁신적인 인터페이스
  - 네트워크 트래픽에서 모든 이미지, 파일, 객체, 오디오, 음성 등을 추출하여 대화형 인터페이스로 표현
  - 멀티터치, 드릴다운, 타임라인 및 자동 재생 기능 제공
  - 네트워크 컨텐츠의 신속한 리뷰

NetWitness Live

최신 탐지 정책 실시간 업데이트

- NetWitness community로부터 분석 방식 자동 업데이트
  - Global threat intelligence
  - Solutions to problem-sets:
  - Advanced threats
  - Malware
  - BOTNets
  - Policy/Audit
  - Enterprise Monitoring
  - Fraud
  - User Attribution
  - Risk prioritization

Use Case

NetWitness를 이용한 APTs 탐지

APTs 탐지 시나리오

- 악성코드 유입 탐지
  - 알려진 악성코드
  - 알려지지 않은 악성 코드
- 악성 코드 유입 경로 확인
  - Browser 취약점
  - 이 메일 첨부파일
  - 파일 공유 사이트
- 악성 코드 감염 시스템의 네트워크 접속 내역 추적
  - 감염된 시스템의 모든 트래픽 내용
  - 이상 트래픽의 목적지 IP 주소 추적

알려지지 않은 악성코드(Zero-Day Attack) 탐지

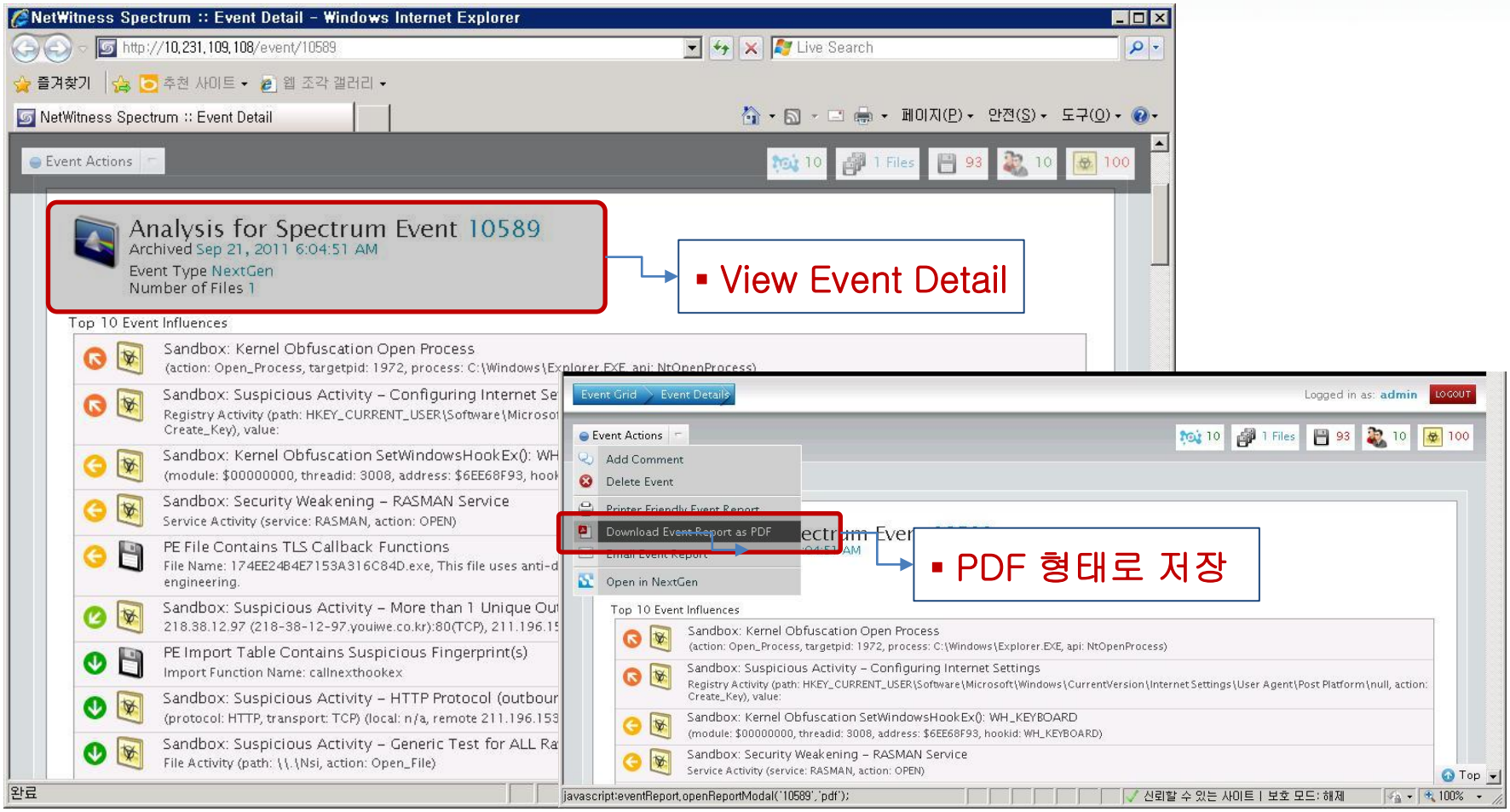
알려진 악성코드
현재 사용중인 Anti-Virus에서 탐지됨

알려지지 않은 악성코드 의심파일 (Suspicious Zero-Day)
Anti-Virus 및 Community 정보에는 탐지되지 않지만 파일 속성 및 유입경로가 악성코드 특성을 가짐

알려진 않은 악성코드
현재 사용중인 Anti-Virus에서 탐지 못함
타사 AntiVirus에서 탐지

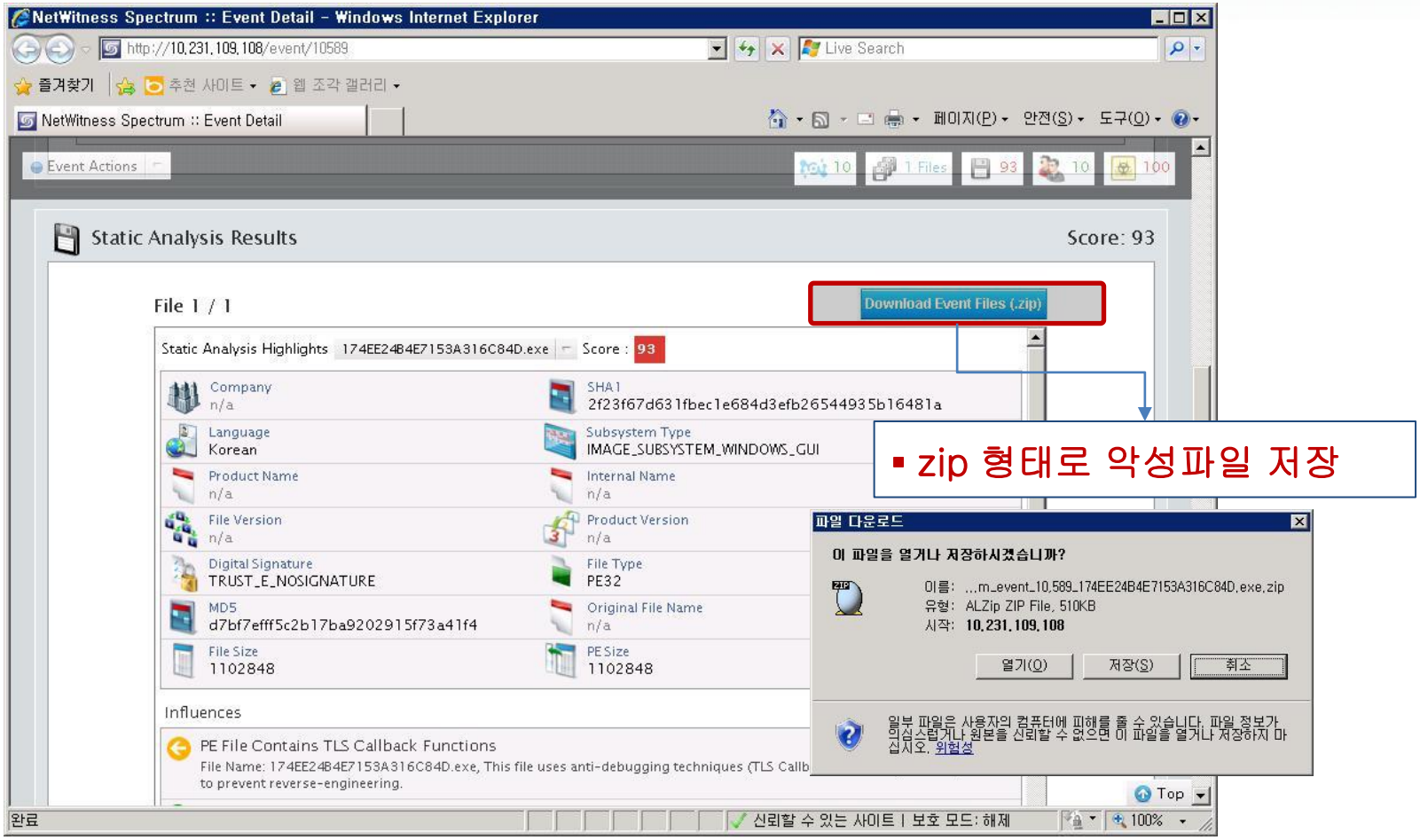
악성코드 유입 경로 분석

악성코드 탐지 근거 상세 내용 및 보고서 생성



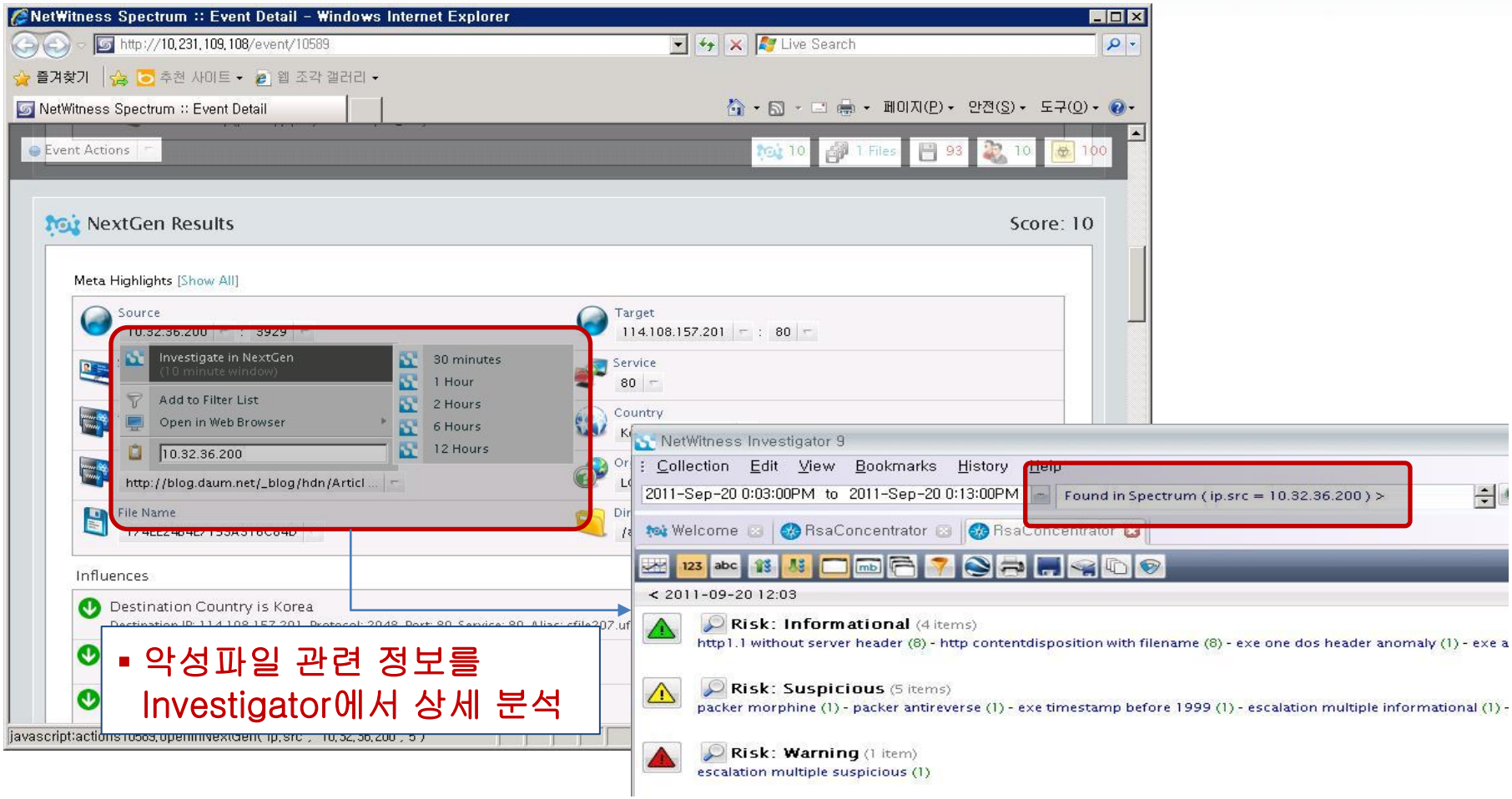
악성코드 유입 경로 분석

악성코드 파일 추출



악성코드 유입 경로 분석

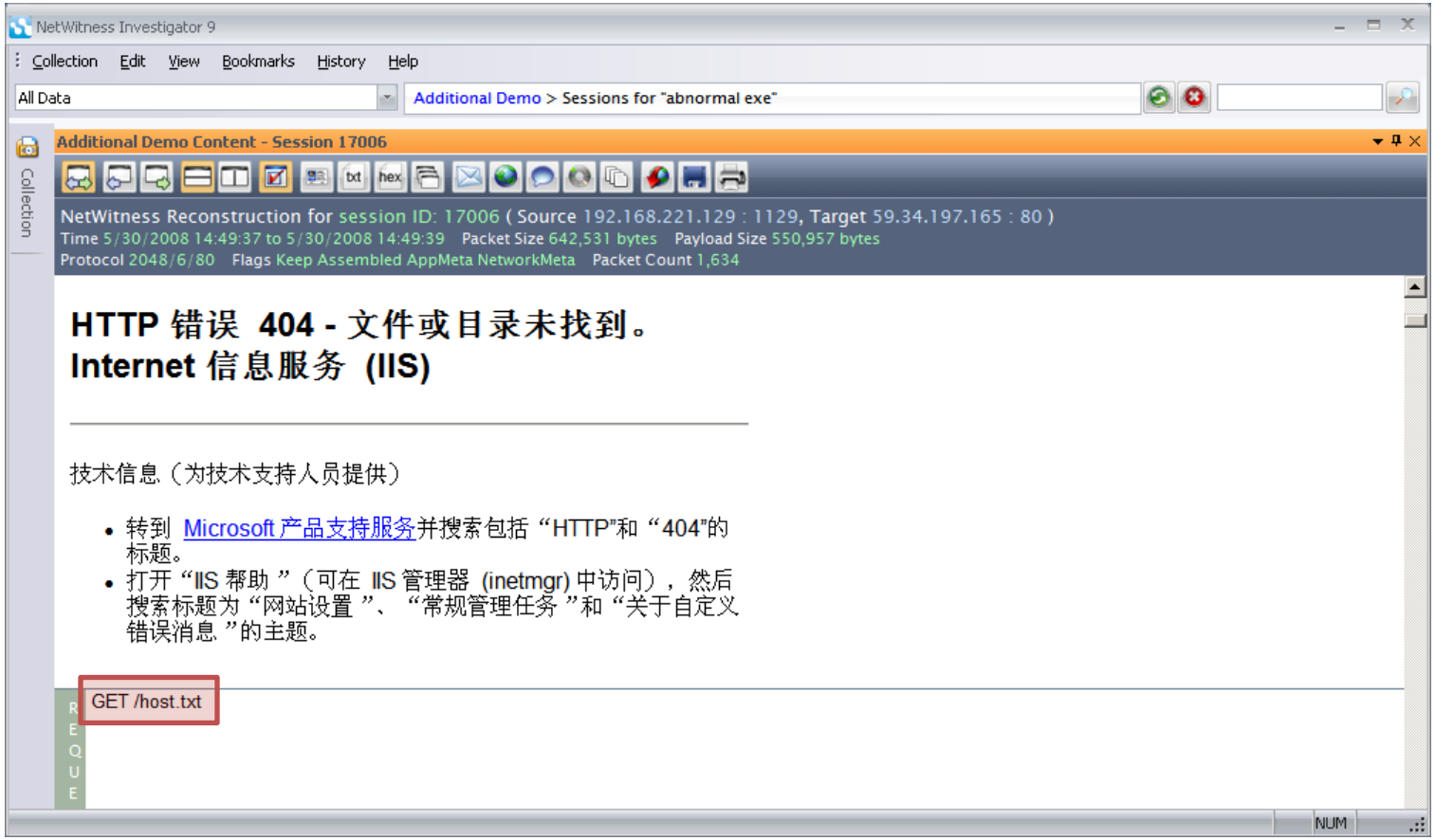
악성코드와 관련된 상세 트래픽 내용 조회



- 악성파일 관련 정보를 Investigator에서 상세 분석

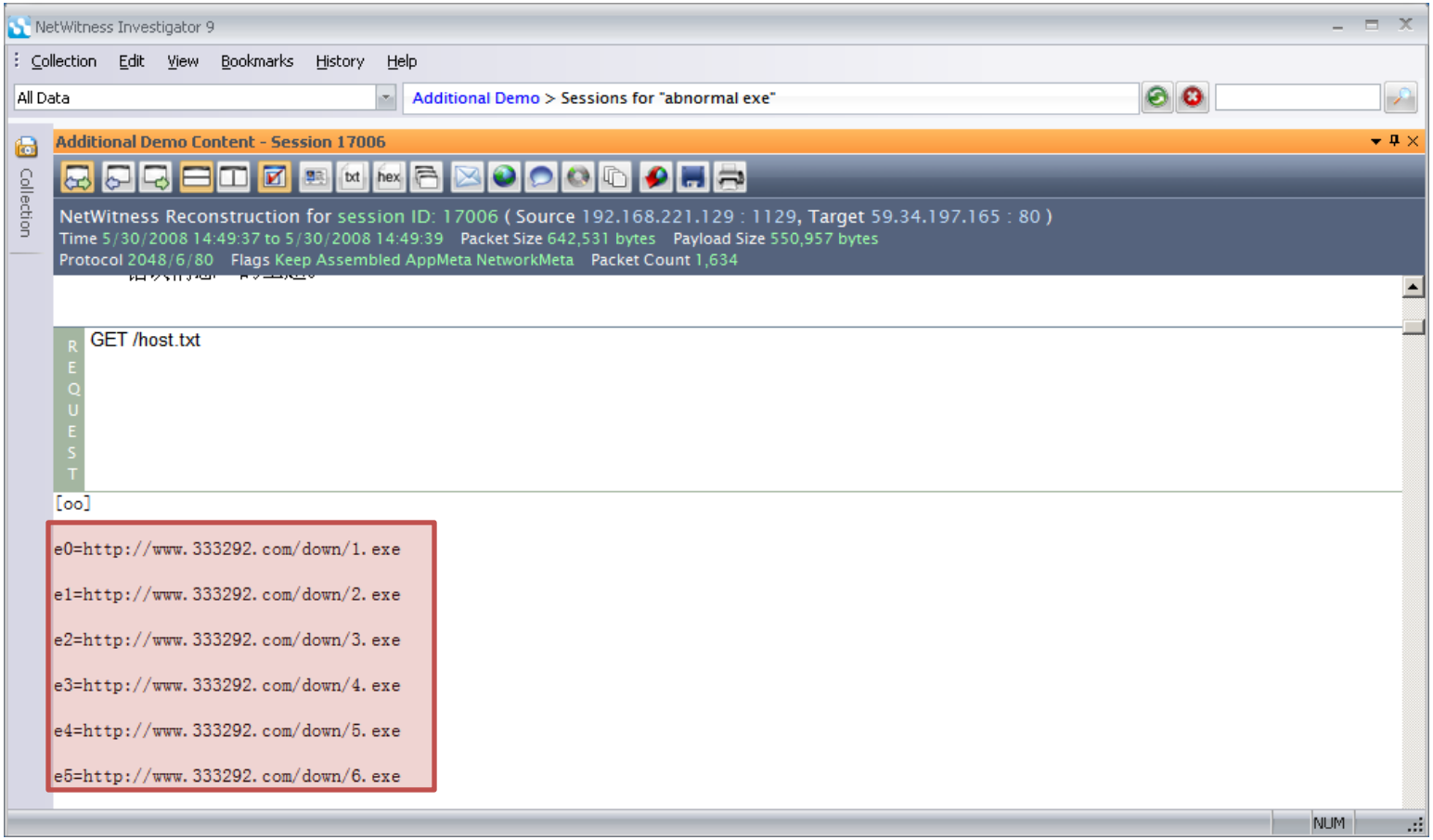
악성코드 유입 경로 분석

Session 세션 상세 내용 – 404 Not Found 표시 이후 특정 파일 다운로드



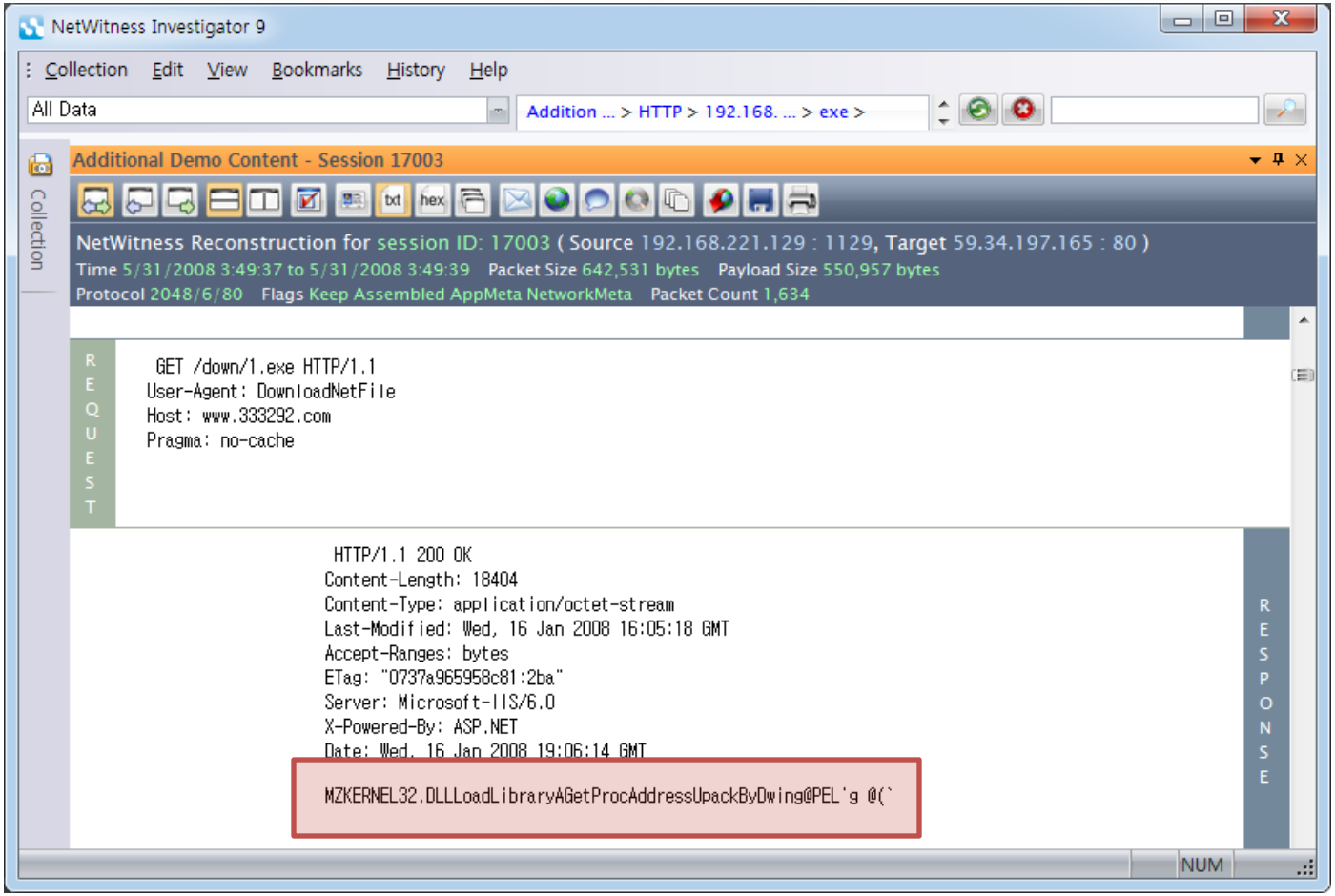
악성코드 유입 경로 분석

Session 세션 상세 내용 – 특정 사이트로 이동, 파일 다운로드



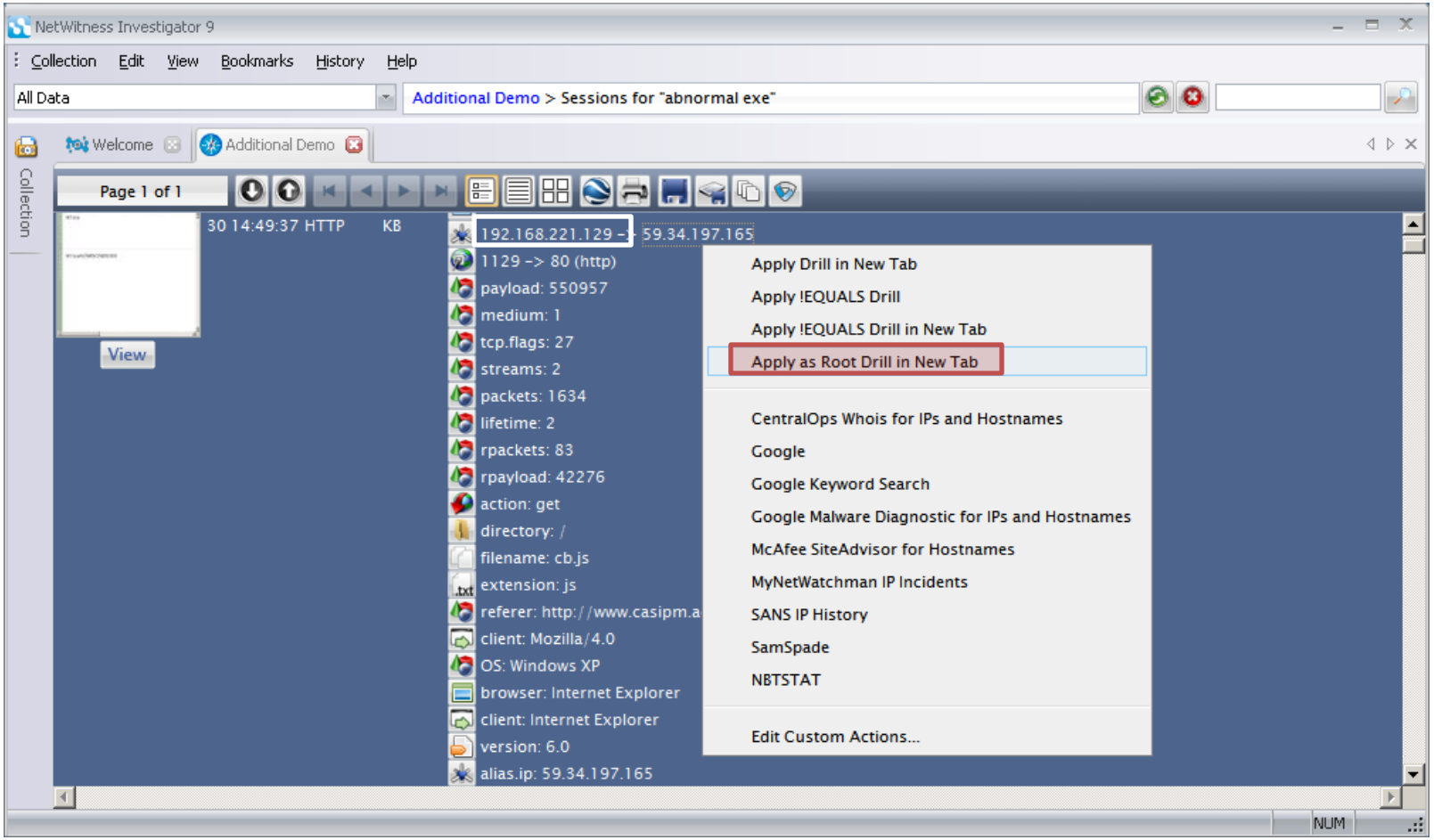
악성코드 유입 경로 분석

악성코드 다운로드 내용 확인



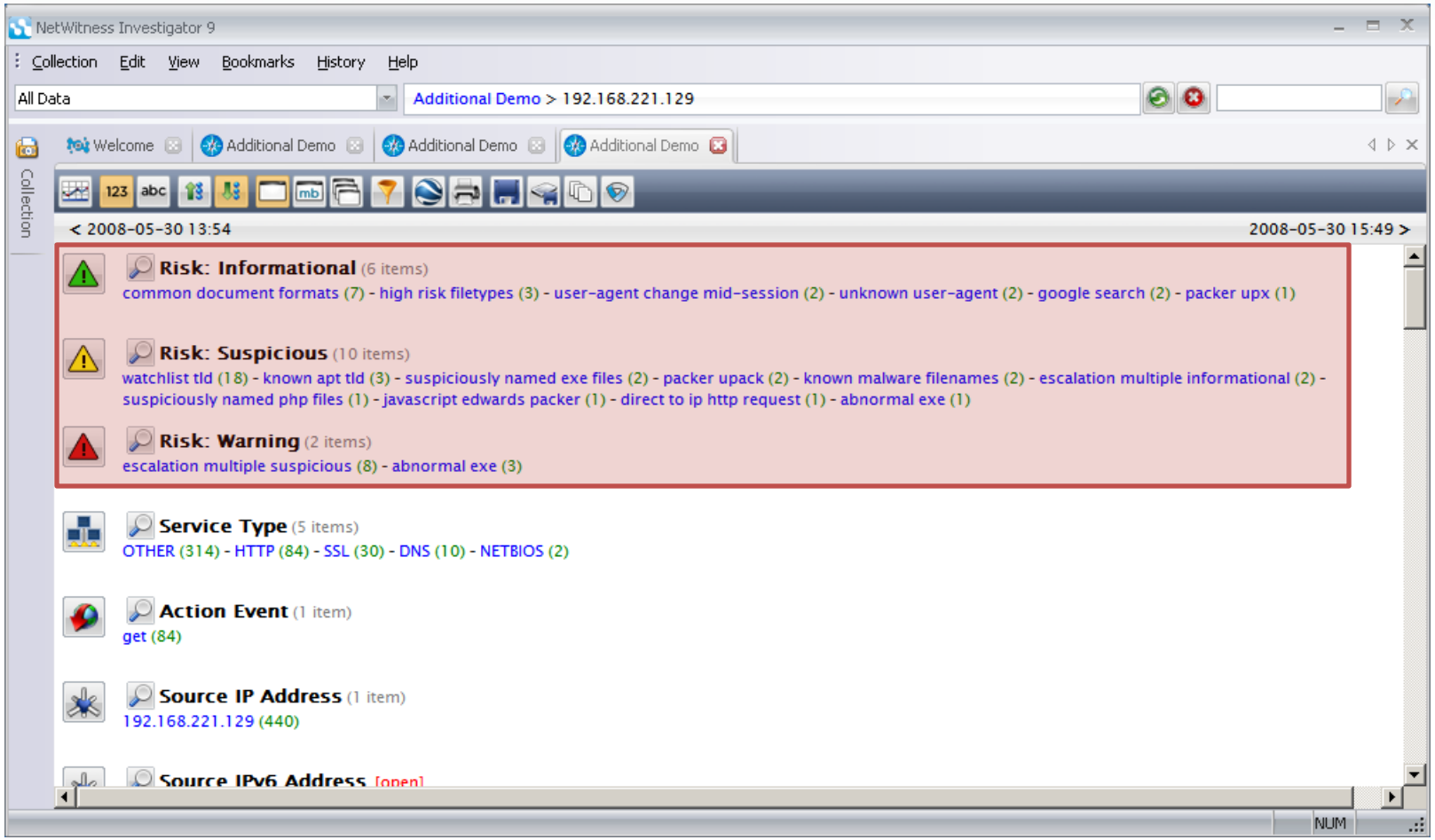
감염된 시스템 트래픽 분석

감염된 시스템의 트래픽 내역 확인



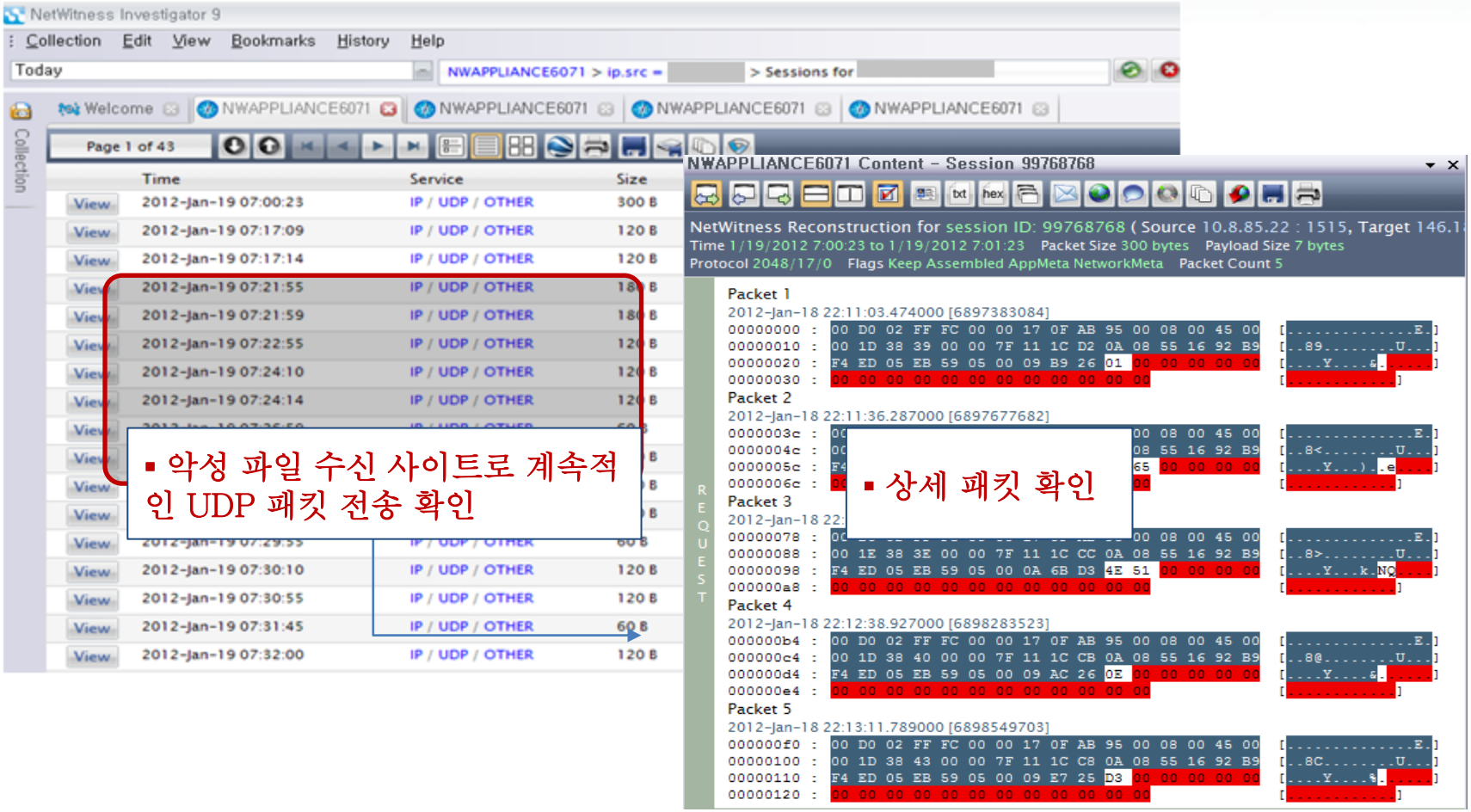
감염된 시스템 트래픽 분석

감염된 시스템의 이상 트래픽 내역 분석



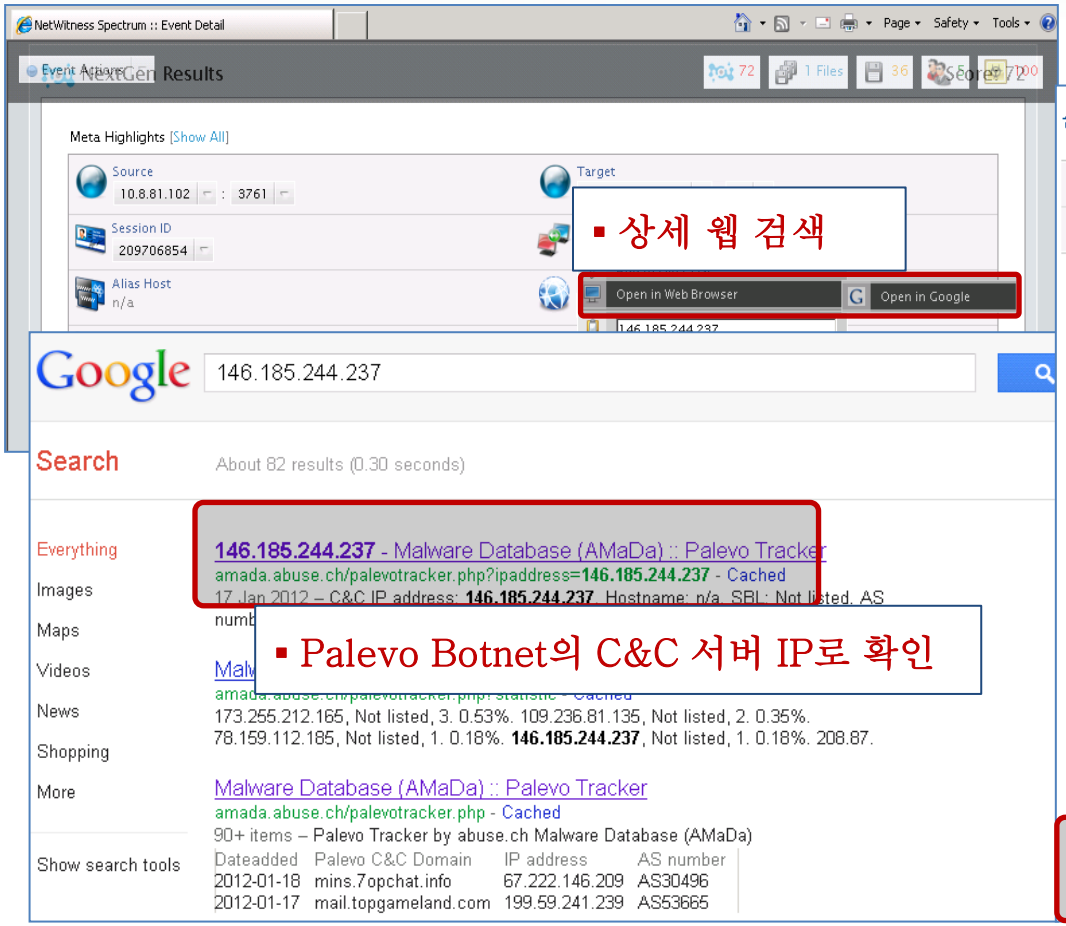
감염된 시스템 트래픽 분석

악성 파일 전송 후 추가 행위 분석



감염된 시스템 트래픽 분석

Web 검색을 통한 내역 확인



결언

전체 트래픽 분석의 필요성

- **악성코드 대응 체계 강화**
  - 악성코드 유입 및 행위에 대한 능동적 대응 체계 확보
  - AV 미탐지 악성코드 및 알려지지 않은 악성 코드 탐지
  - 악성코드 유입 경로에 대한 지속적 차단 및 악성코드 행위 차단

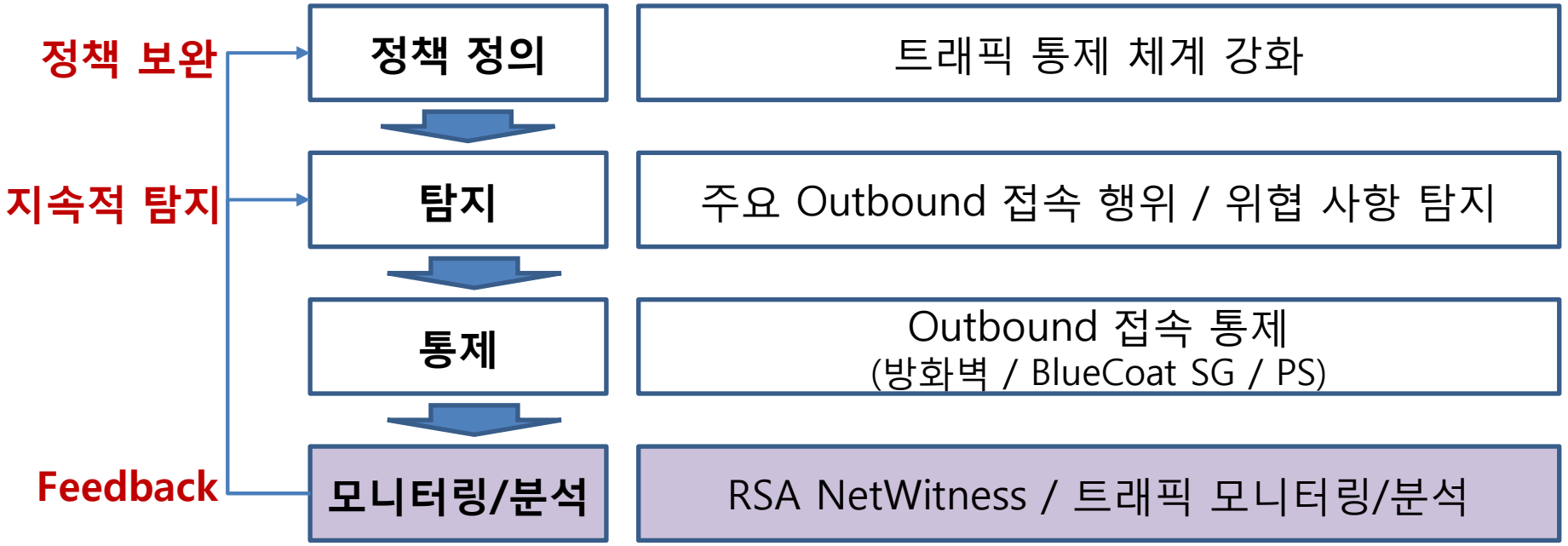
- **주요 위협 탐지 / 대응 방안 제시**
  - 알려지지 않은 신규 공격 행위 파악 및 대응
  - 탐지를 회피하는 정교한 공격 탐지 / 제거
    - Zero-Day Malware, Botnet , C&C 서버 접근
  - 위협이 되는 사이트 접근 행위 탐지 및 통제

- **내부 직원의 행동 유형 분석**
  - 조직에 위협이 될 수 있는 업무 관행 파악 및 개선
  - Outbound 트래픽 통제 시에 기존 업무 영향도 분석

트래픽 통제 체계 강화 방안

지속적인 보완/최적화 Cycle

- **RSA NetWitness를 이용한 통제 체계의 지속적 보완/강화**
  - 주요 위협 모니터링 및 상세 분석 결과를 Feedback으로 이용
  - 기존 정책의 지속적 보완
  - OutBound 접속 통제 항목의 지속적 보완



Q & A

Thank you