

# CIO Summit 2012

창조적 혁신으로 새로운 가치를 창출하라!

IT Creative Innovation for

**New Value!**



# APT 공격에 따른 대응 전략

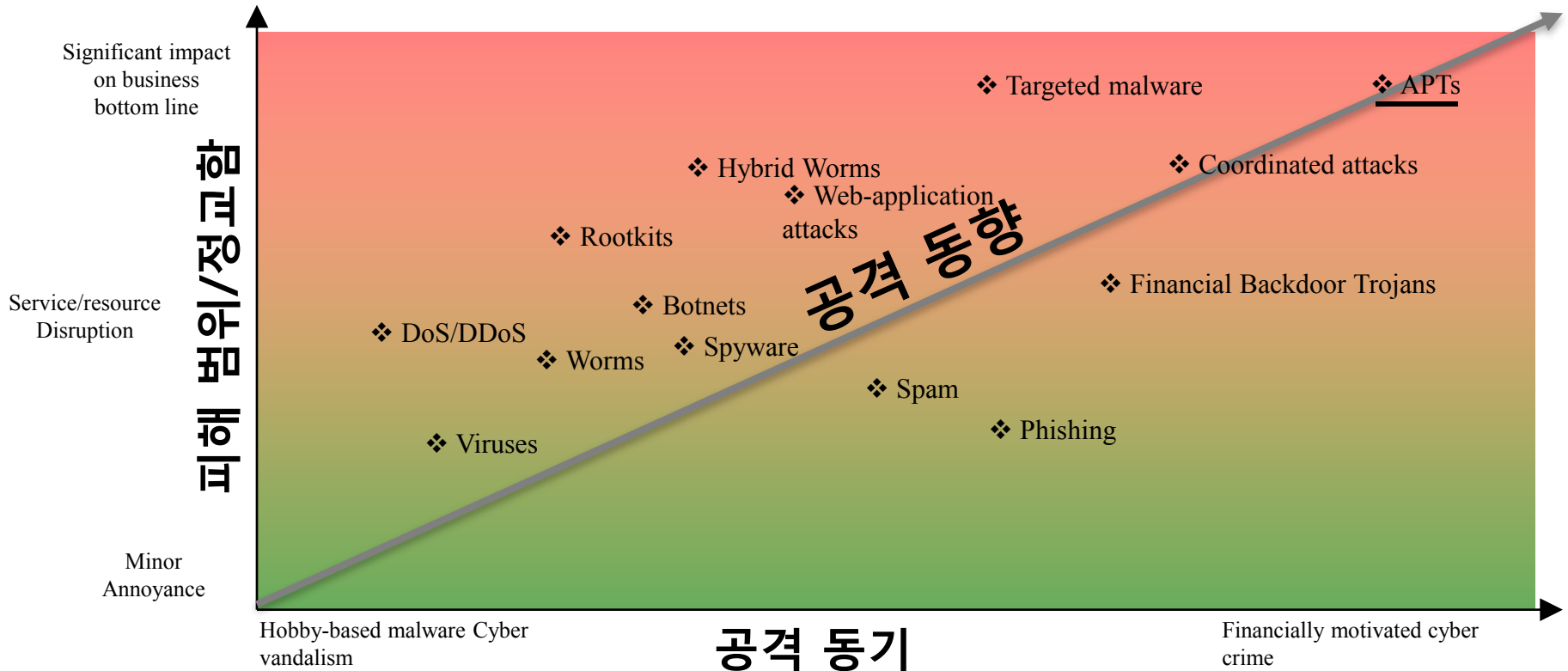
조남용 | 차장  
EMC

# 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

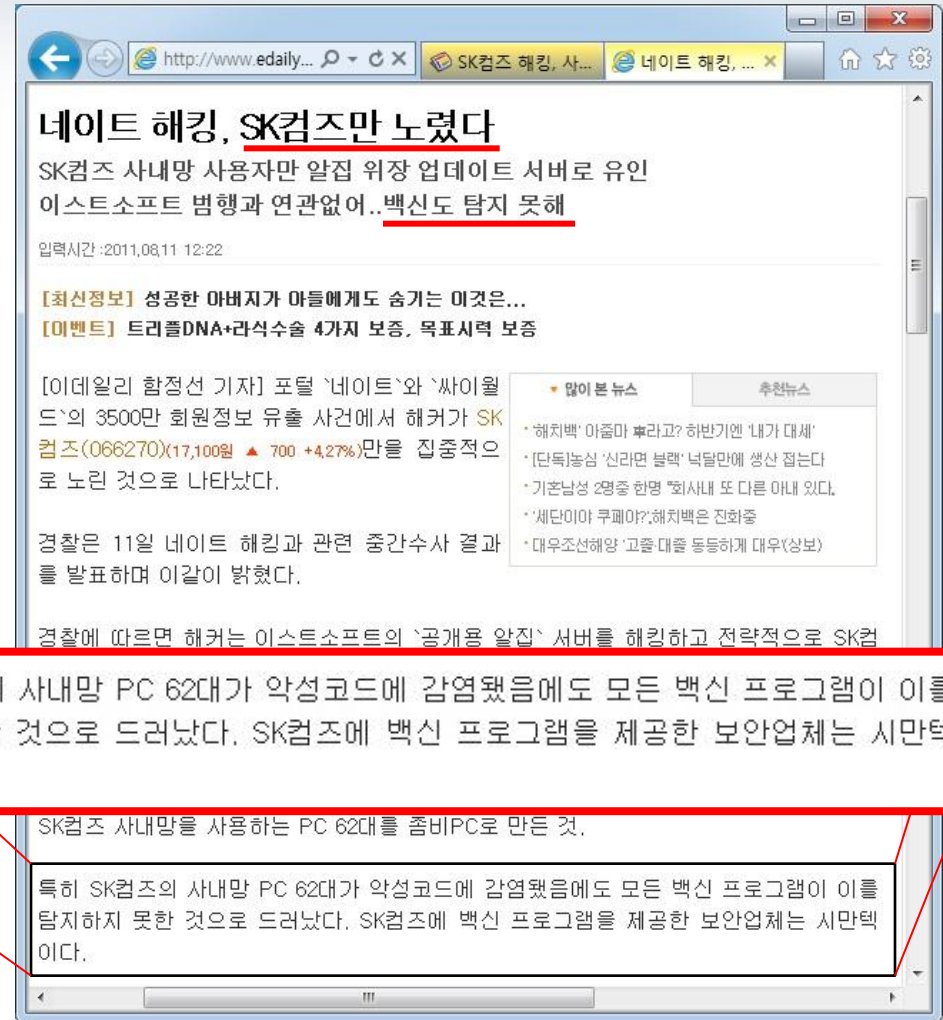
- 고객 43만 명 정보 유출

## ■ 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)

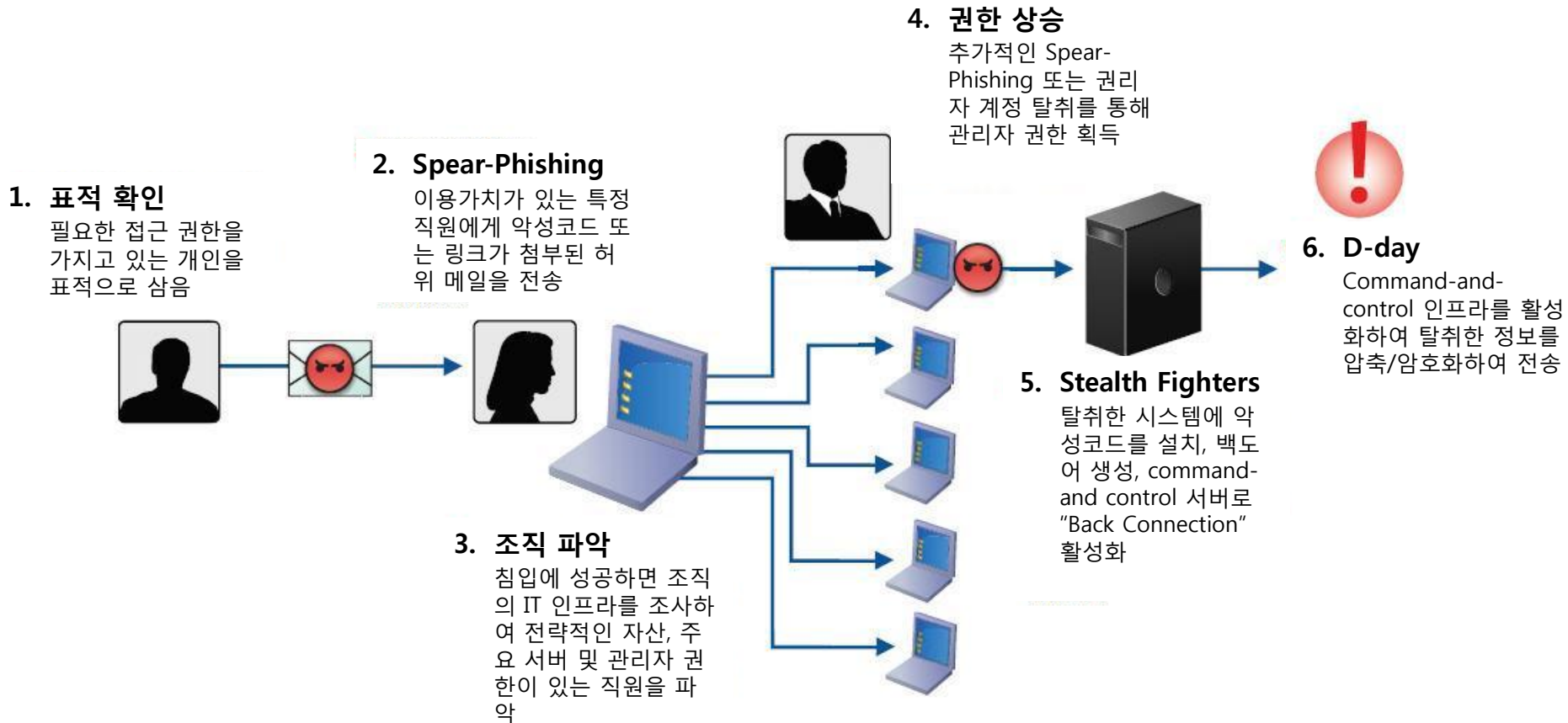
- 공격자가 특정 기업 혹은 조직의 기밀 정보를 획득하기 위해 장기간 동안 은밀하게 진행하는 공격 형태

## ■ 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)

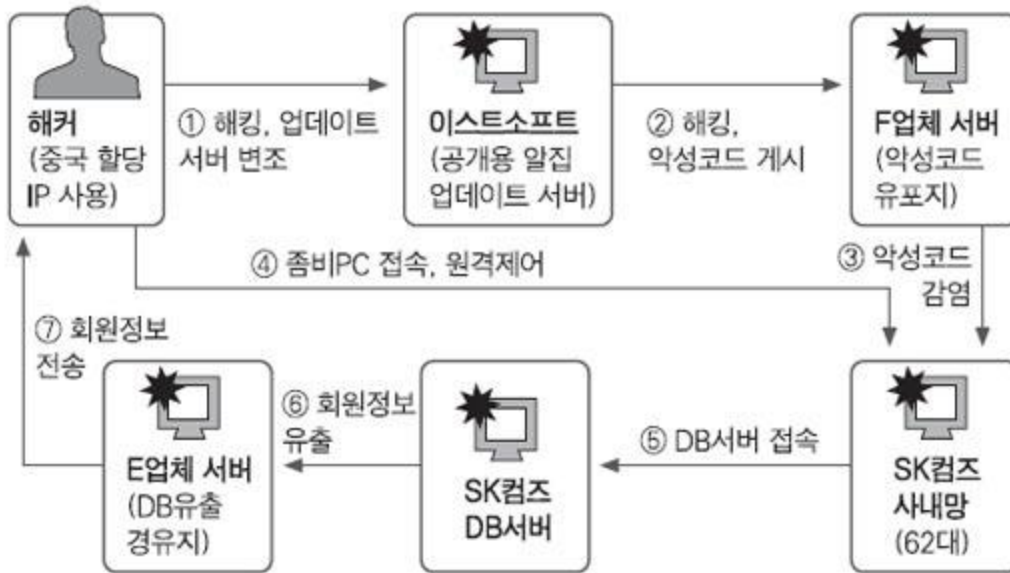
## 일반적인 공격 단계



# 지능형 지속 공격(APT)

## 국내 공격 사례

### SK컴즈 회원정보 유출 상황



출처:한국일보

### SK컴즈의 3500만 개인정보 유출 개념도

해커, 이스트소프트 알집 업데이트 서버를 해킹해 악성코드화

SK컴즈 서버 공격

SK컴즈 사내망 PC 62대 좀비PC화

데이터베이스 서버망 접근 가능한 관리자 아이디와 비밀번호 수집

좀비PC 원격 조종해 DB서버에 접속

3500만여명 회원 정보 중국에 할당된 IP로 유출

출처:디지털타임스



# 지능형 지속 공격(APT)

## 기존 보안 시스템 우회

### ■ Firewall

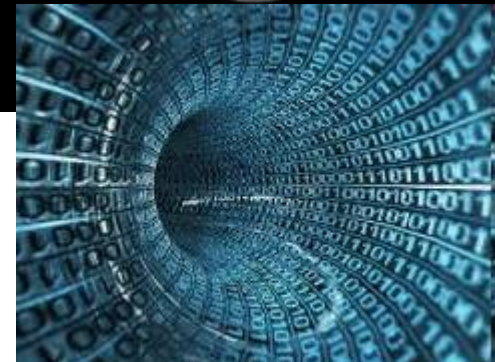
- 대부분의 Firewall은 외부에서 내부로의 접속을 제어
- 내부에서 외부로의 연결이 허용된 포트 사용
  - 일반적으로 HTTP (80)포트를 사용하여 내부에서 외부에 있는 원격 조종 서버로 연결

### ■ 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

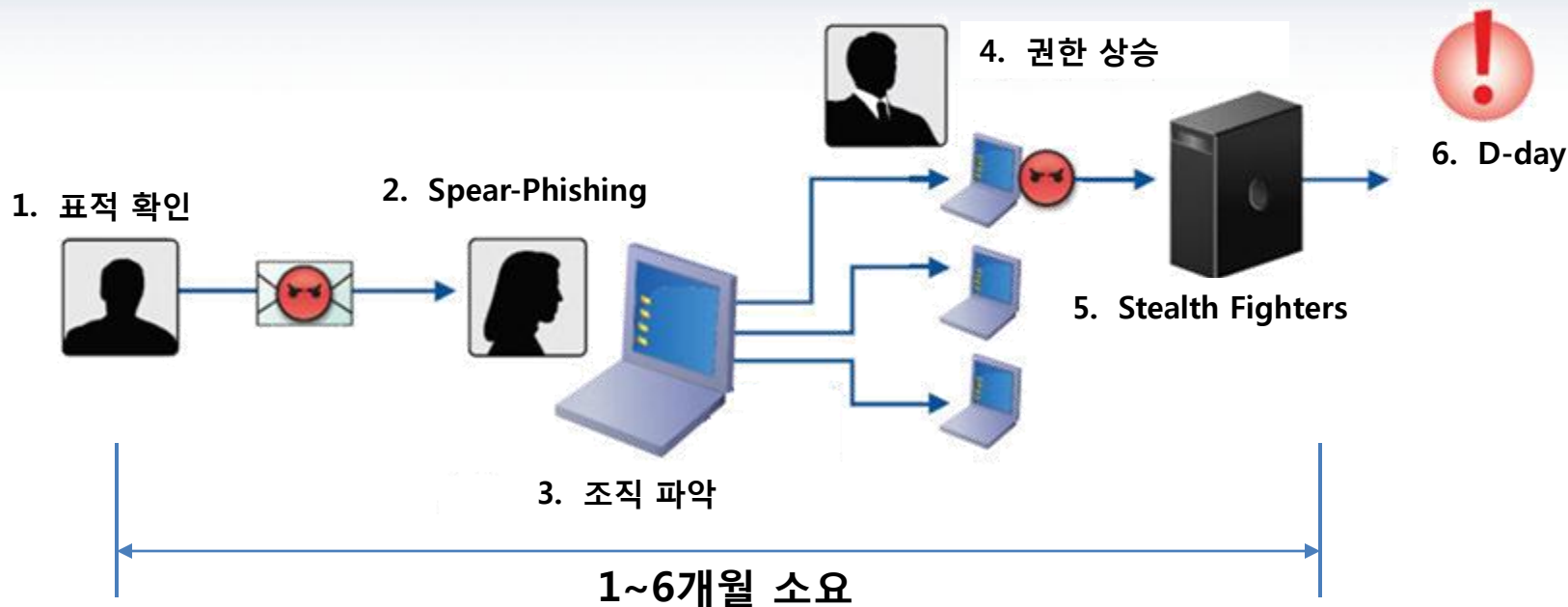
### ■ 보안 관제

- 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 잠입 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

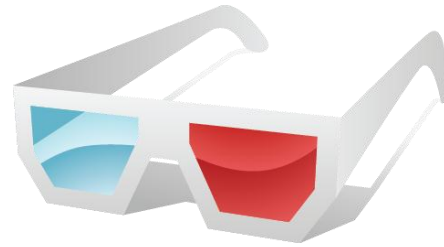
- 비 정상적인 경로를 통한 실행파일 유입 탐지
  - 브라우저 취약점 이용
  - 실시간 Botnet, 악성코드 배포지점 정보를 이용한 의심스러운 파일 다운로드 탐지
- 외부로 연결이 허용된 트래픽(80, 443 port 등) 모니터링으로 외부 공격자로의 접속을 탐지
  - 접속 Port 와 실제 프로토콜의 일치여부 확인 (예: HTTP 프로토콜을 사용하지 않는 80 port 트래픽)
  - 의심가는 IP 로의 접속 내용 확인 (실시간 Botnet, Command&Control 지점 정보 이용)

# NetWitness 개요

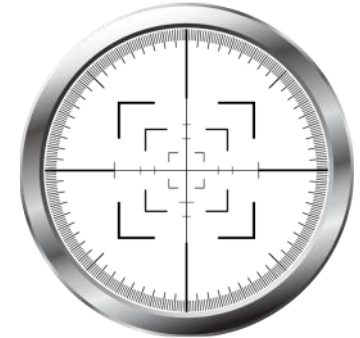
# NetWitness Is ...



혁신적인  
네트워크 모니터링  
솔루션



네트워크  
행위 및 내용에 대한  
광범위한 가시성



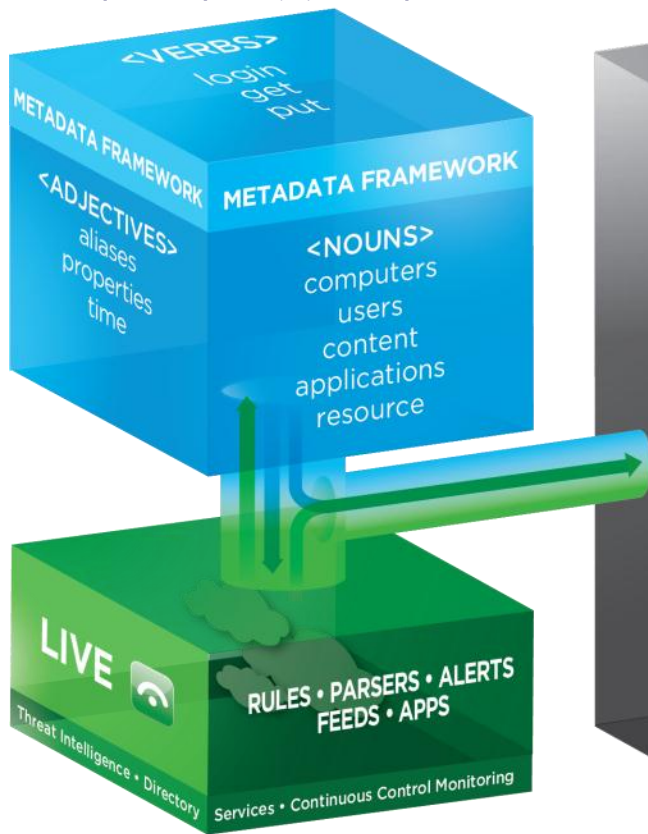
정확하고  
실효적인 대응체계  
제공

**Know Everything. Answer Anything.**

# NetWitness

## Network Security Analysis Platform

모든 네트워크 트래픽의  
실시간 저장 및 인덱스 생성



자동화된 악성코드 분석 및  
위험도 평가

자동화된 위협 보고서 및 경  
보

즉각적인 원인 파악 및 분석

혁명적인 가시화를 통한 신  
속한 Content 리뷰



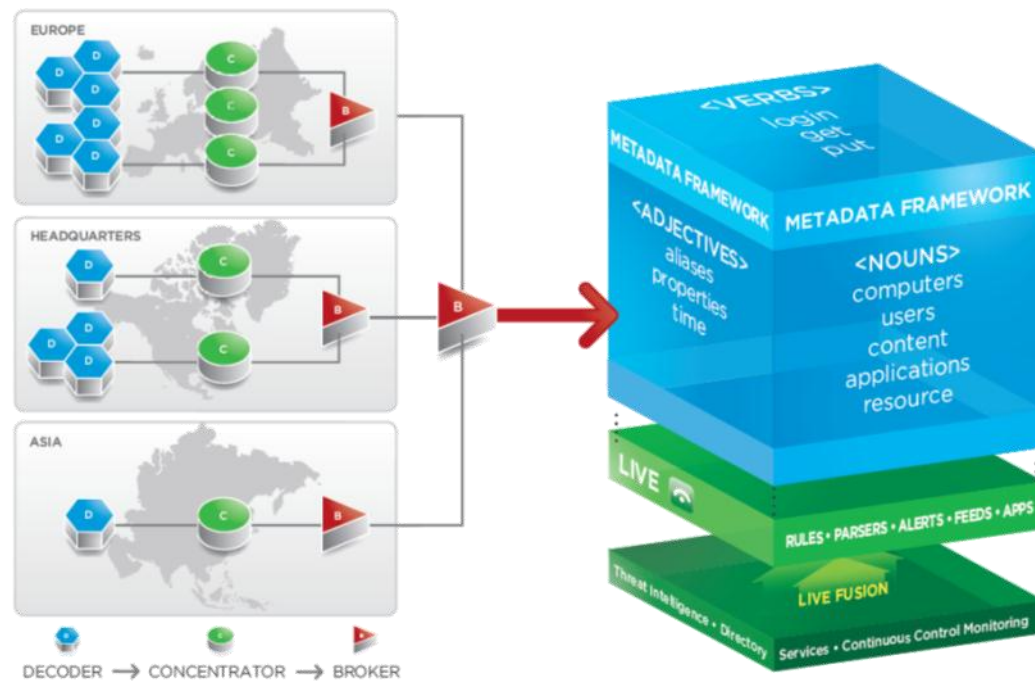
# NetWitness 주요 기능

# 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 콘텐츠에 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



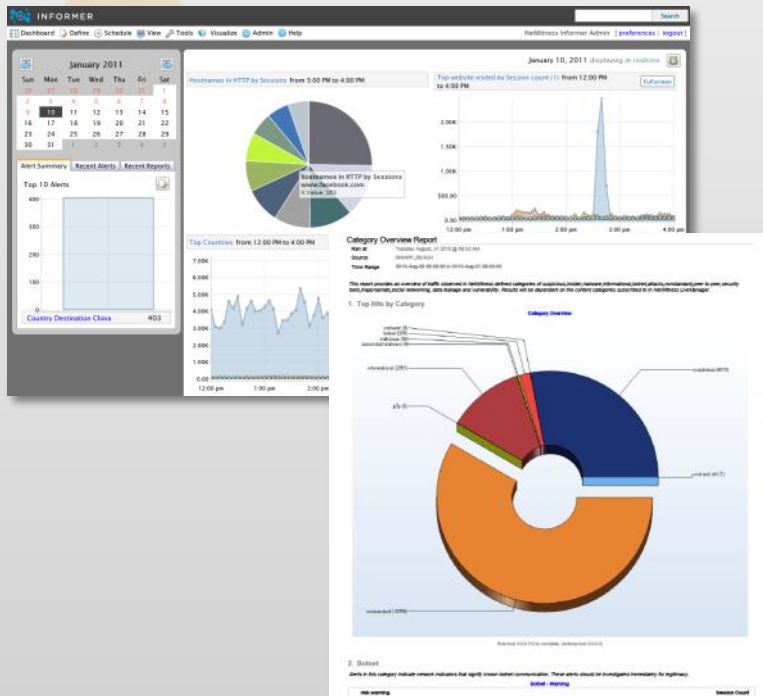
- 알려지지 않은 악성코드(Zero-Day Attack) 탐지
- 네트워크 상의 모든 실행파일에 대해 다양한 관점에서 악성코드 여부 분석
  - File
    - 파일의 고유 속성 / 파일 헤더 정보를 분석하여 변조된 실행파일 탐지
  - NextGen
    - 파일 출처에 대한 네트워크 정보를 확인하여 비 정상적인 유입경로 확인
  - Community
    - 해당 파일의 Signature에 대해 Online Community에 질의
  - SandBox
    - 실행파일을 테스트 환경에서 실제 실행하여 악성코드 행위 탐지

# 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 콘텐츠의 혁신적인 가시화



Visualize



- 네트워크 콘텐츠의 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 콘텐츠의 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



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

알려진 악성코드 현재 사용중인 Anti-Virus에서 탐지됨

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

# 악성코드 유입 경로 분석

악성코드 탐지 근거 상세 내용 및 보고서 생성

The screenshot displays the NetWitness Spectrum interface. At the top, the browser address bar shows the URL `http://10.231.109.108/event/10589`. The main content area features a summary card for "Analysis for Spectrum Event 10589", which is highlighted with a red box. This card includes the event type "NextGen" and the number of files "1". A blue arrow points from this card to a red box containing the text "View Event Detail".

Below the summary card, a list of "Top 10 Event Influences" is visible, detailing various system activities such as "Sandbox: Kernel Obfuscation Open Process" and "Sandbox: Suspicious Activity - Configuring Internet Settings".

An "Event Actions" menu is open, showing several options. The option "Download Event Report as PDF" is highlighted with a red box. A blue arrow points from this option to another red box containing the text "PDF 형태로 저장" (Save as PDF).

The interface also shows a top navigation bar with icons for "10" items, "1 Files", "93" items, "10" items, and "100" items. The bottom status bar indicates the user is logged in as "admin" and provides a "LOGOUT" button.

# 악성코드 유입 경로 분석

## 악성코드 파일 추출

NetWitness Spectrum :: Event Detail - Windows Internet Explorer

http://10.231.109.108/event/10589

Static Analysis Results Score: 93

File 1 / 1

Download Event Files (.zip)

Static Analysis Highlights 174EE24B4E7153A316C84D.exe Score: 93

Company n/a	SHA1 2f23f67d631fbec1e684d3efb26544935b16481a
Language Korean	Subsystem Type IMAGE_SUBSYSTEM_WINDOWS_GUI
Product Name n/a	Internal Name n/a
File Version n/a	Product Version n/a
Digital Signature TRUST_E_NOSIGNATURE	File Type PE32
MD5 d7bf7efff5c2b17ba9202915f73a41f4	Original File Name n/a
File Size 1102848	PE Size 1102848

Influences

- PE File Contains TLS Callback Functions  
File Name: 174EE24B4E7153A316C84D.exe, This file uses anti-debugging techniques (TLS Callb to prevent reverse-engineering.

파일 다운로드

이 파일을 열거나 저장하시겠습니까?

이름: ...m\_event\_10.589\_174EE24B4E7153A316C84D.exe.zip  
 유형: ALZip ZIP File, 510KB  
 시작: 10.231.109.108

열기(O) 저장(S) 취소

일부 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 파일 정보가 의심스럽거나 원본을 신뢰할 수 없으면 이 파일을 열거나 저장하지 마십시오. [위험성](#)

완료

신뢰할 수 있는 사이트 | 보호 모드: 해제

■ zip 형태로 악성파일 저장

# 악성코드 유입 경로 분석

## 악성코드와 관련된 상세 트래픽 내용 조회

The image shows a screenshot of a Windows Internet Explorer browser displaying the NetWitness Spectrum Event Detail page. The browser address bar shows the URL `http://10.231.109.108/event/10589`. The page content includes a 'NextGen Results' section with a score of 10. Under 'Meta Highlights', there is a table with columns for Source, Target, Service, and Country. A red box highlights the 'Investigate in NextGen' button and a dropdown menu with options: 30 minutes, 1 Hour, 2 Hours, 6 Hours, and 12 Hours. Below this, there is a search bar with the text 'Found in Spectrum (ip.src = 10.32.36.200) >'. In the bottom right, the NetWitness Investigator 9 interface is visible, showing a list of risk items: 'Risk: Informational (4 items)', 'Risk: Suspicious (5 items)', and 'Risk: Warning (1 item)'. A red box highlights the search bar in Investigator 9. A blue arrow points from the 'Investigate in NextGen' button to the search bar in Investigator 9. A text box in the bottom left contains the text: '악성파일 관련 정보를 Investigator에서 상세 분석'.

NetWitness Spectrum :: Event Detail - Windows Internet Explorer

http://10.231.109.108/event/10589

NextGen Results Score: 10

Meta Highlights [Show All]

Source	Target	Service	Country
10.32.36.200	114.108.157.201	80	Korea

Investigate in NextGen (10 minute window)

- 30 minutes
- 1 Hour
- 2 Hours
- 6 Hours
- 12 Hours

Found in Spectrum (ip.src = 10.32.36.200) >

NetWitness Investigator 9

2011-Sep-20 0:03:00PM to 2011-Sep-20 0:13:00PM

Risk: Informational (4 items)  
http 1.1 without server header (8) - http contentdisposition with filename (8) - exe one dos header anomaly (1) - exe a

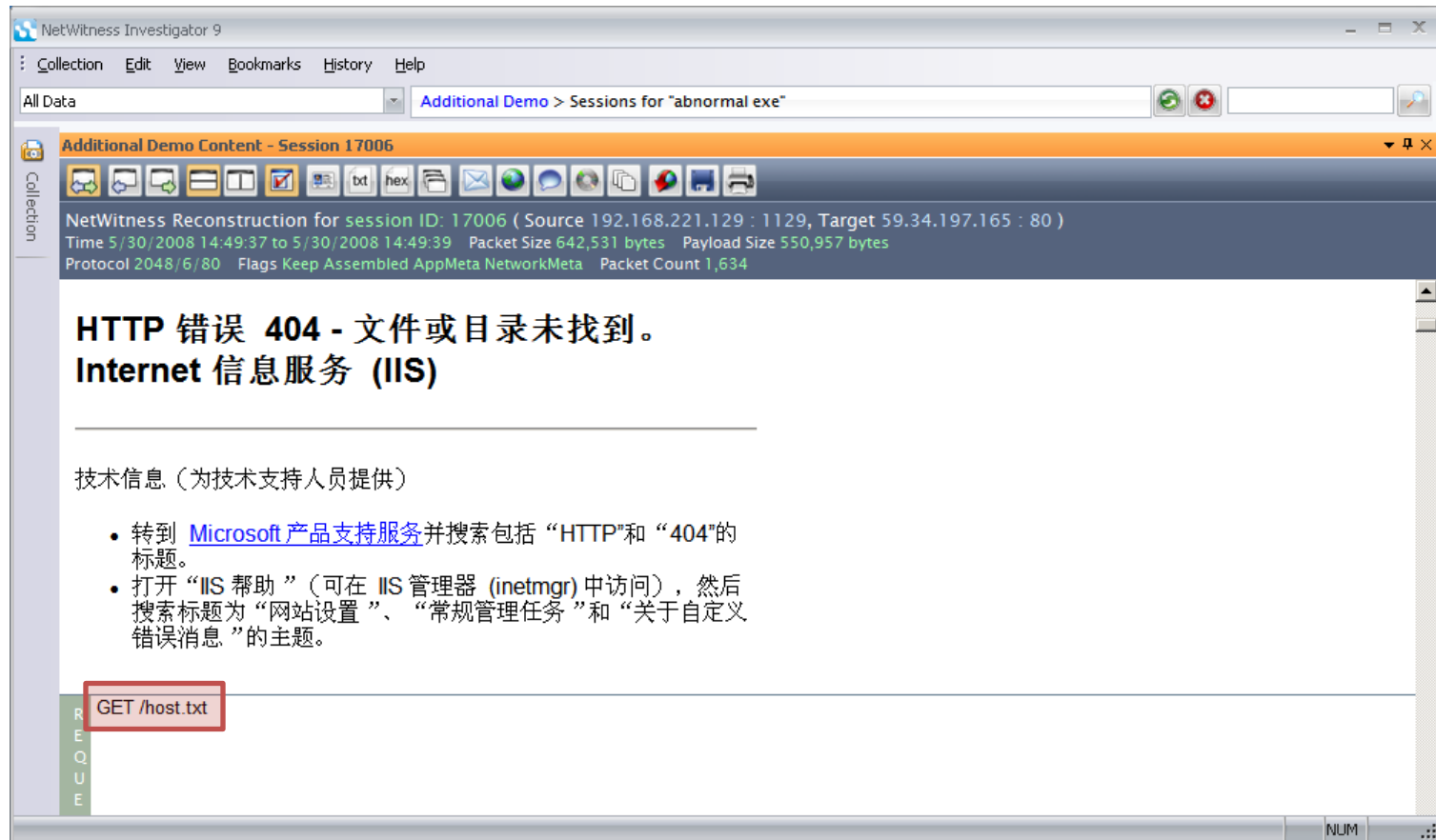
Risk: Suspicious (5 items)  
packer morphine (1) - packer antireverse (1) - exe timestamp before 1999 (1) - escalation multiple informational (1) -

Risk: Warning (1 item)  
escalation multiple suspicious (1)

악성파일 관련 정보를 Investigator에서 상세 분석

# 악성코드 유입 경로 분석

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



NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data Additional Demo > Sessions for "abnormal exe"

Additional Demo Content - Session 17006

NetWitness Reconstruction for session ID: 17006 ( Source 192.168.221.129 : 1129, Target 59.34.197.165 : 80 )  
Time 5/30/2008 14:49:37 to 5/30/2008 14:49:39 Packet Size 642,531 bytes Payload Size 550,957 bytes  
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,634

**HTTP 错误 404 - 文件或目录未找到。**  
**Internet 信息服务 (IIS)**

技术信息 (为技术支持人员提供)

- 转到 [Microsoft 产品支持服务](#) 并搜索包括 "HTTP" 和 "404" 的标题。
- 打开 "IIS 帮助" (可在 IIS 管理器 (inetmgr) 中访问), 然后搜索标题为 "网站设置"、"常规管理任务" 和 "关于自定义错误消息" 的主题。

REQUEST

GET /host.txt

NUM

# 악성코드 유입 경로 분석

Session 세션 상세 내용 - 특정 사이트로 이동, 파일 다운로드

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data Additional Demo > Sessions for "abnormal exe"

Additional Demo Content - Session 17006

NetWitness Reconstruction for session ID: 17006 ( Source 192.168.221.129 : 1129, Target 59.34.197.165 : 80 )  
Time 5/30/2008 14:49:37 to 5/30/2008 14:49:39 Packet Size 642,531 bytes Payload Size 550,957 bytes  
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,634

R  
E  
Q  
U  
E  
S  
T

GET /host.txt

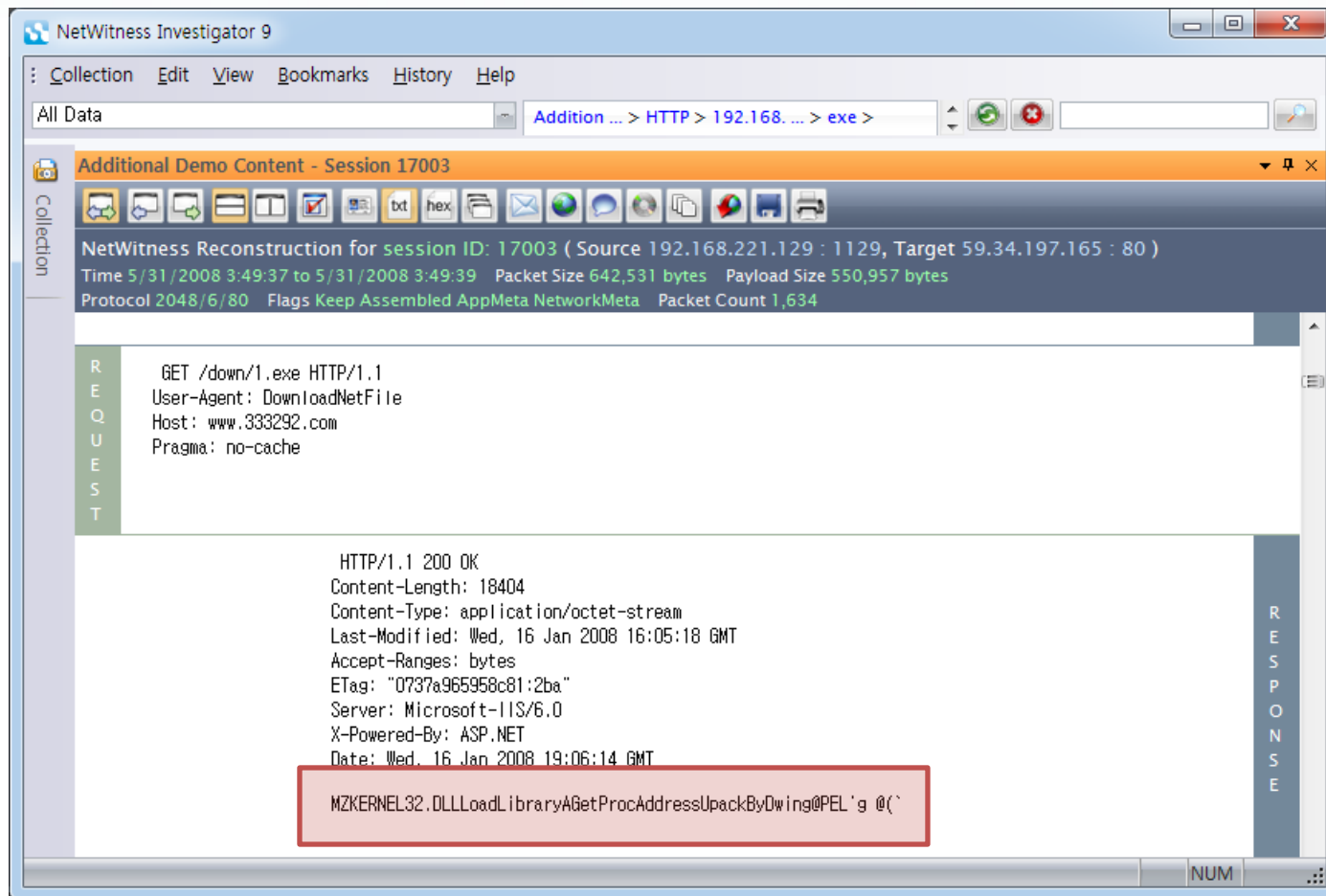
[oo]

e0=http://www.333292.com/download/1.exe  
e1=http://www.333292.com/download/2.exe  
e2=http://www.333292.com/download/3.exe  
e3=http://www.333292.com/download/4.exe  
e4=http://www.333292.com/download/5.exe  
e5=http://www.333292.com/download/6.exe

NUM

# 악성코드 유입 경로 분석

## 악성코드 다운로드 내용 확인



NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data Addition ... > HTTP > 192.168. ... > exe >

Additional Demo Content - Session 17003

NetWitness Reconstruction for session ID: 17003 ( Source 192.168.221.129 : 1129, Target 59.34.197.165 : 80 )  
Time 5/31/2008 3:49:37 to 5/31/2008 3:49:39 Packet Size 642,531 bytes Payload Size 550,957 bytes  
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 1,634

REQUEST

```
GET /down/1.exe HTTP/1.1
User-Agent: DownloadNetFile
Host: www.333292.com
Pragma: no-cache
```

RESPONSE

```
HTTP/1.1 200 OK
Content-Length: 18404
Content-Type: application/octet-stream
Last-Modified: Wed, 16 Jan 2008 16:05:18 GMT
Accept-Ranges: bytes
ETag: "0737a965958c81:2ba"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 16 Jan 2008 19:06:14 GMT
```

MZKERNEL32.DLLLoadLibraryAGetProcAddressUpackByDwing@PEL'g @(`

NUM



# 감염된 시스템 트래픽 분석

## 감염된 시스템의 트래픽 내역 확인

The screenshot displays the NetWitness Investigator 9 interface. The main window shows a traffic analysis session for 'abnormal.exe'. The left pane shows a collection of traffic, and the right pane shows a detailed view of a specific session. The session details include:

- Time: 30 14:49:37
- Protocol: HTTP
- Size: KB
- Source IP: 192.168.221.129
- Destination IP: 59.34.197.165
- Destination Port: 80 (http)
- Payload: 550957
- Medium: 1
- TCP Flags: 27
- Streams: 2
- Packets: 1634
- Lifetime: 2
- Rpackets: 83
- Rpayload: 42276
- Action: get
- Directory: /
- Filename: cb.js
- Extension: .js
- Referer: http://www.casipm.a
- Client: Mozilla/4.0
- OS: Windows XP
- Browser: Internet Explorer
- Client: Internet Explorer
- Version: 6.0
- Alias IP: 59.34.197.165

A context menu is open over the source IP address, showing various actions:

- Apply Drill in New Tab
- Apply IEQUALS Drill
- Apply IEQUALS Drill in New Tab
- Apply as Root Drill in New Tab
- CentralOps Whois for IPs and Hostnames
- Google
- Google Keyword Search
- Google Malware Diagnostic for IPs and Hostnames
- McAfee SiteAdvisor for Hostnames
- MyNetWatchman IP Incidents
- SANS IP History
- SamSpade
- NBTSTAT
- Edit Custom Actions...

# 감염된 시스템 트래픽 분석

## 감염된 시스템의 이상 트래픽 내역 분석

NetWitness Investigator 9

Collection Edit View Bookmarks History Help

All Data Additional Demo > 192.168.221.129

Collection

< 2008-05-30 13:54 2008-05-30 15:49 >

- Risk: Informational** (6 items)
  - common document formats (7) - high risk filetypes (3) - user-agent change mid-session (2) - unknown user-agent (2) - google search (2) - packer upx (1)
- Risk: Suspicious** (10 items)
  - watchlist tld (18) - known apt tld (3) - suspiciously named exe files (2) - packer upack (2) - known malware filenames (2) - escalation multiple informational (2) - suspiciously named php files (1) - javascript edwards packer (1) - direct to ip http request (1) - abnormal exe (1)
- Risk: Warning** (2 items)
  - escalation multiple suspicious (8) - abnormal exe (3)
- Service Type** (5 items)
  - OTHER (314) - HTTP (84) - SSL (30) - DNS (10) - NETBIOS (2)
- Action Event** (1 item)
  - get (84)
- Source IP Address** (1 item)
  - 192.168.221.129 (440)
- Source IPv6 Address** [open]

NUM



# 감염된 시스템 트래픽 분석

## Web 검색을 통한 내역 확인

**상세 웹 검색**

**Palevo Botnet의 C&C 서버 IP로 확인**

146.185.244.237 - Malware Database (AMaDa) :: Palevo Tracker  
 amada.abuse.ch/palevotracker.php?ipaddress=146.185.244.237 - Cached  
 17 Jan 2012 - C&C IP address: 146.185.244.237 Hostname: n/a SBL: Not listed AS

Dateadded	Palevo C&C Domain	IP address	AS number
2012-01-18	mins.7opchat.info	67.222.146.209	AS30496
2012-01-17	mail.topgameland.com	199.59.241.239	AS53665

### 신종 웜과 트로이목마 주의!

입력날짜 : 2012-01-24 01:04

스크랩 프린트하기 목록

Tweet Like 4

Twitter Facebook LinkedIn YouTube

### 최신 바이러스 백신으로 엔진 업데이트 필요

[보안뉴스 권 준] 웜의 일종인 'Win32/Palevo.worm.52736.E'와 트로이목마의 한 종류인 'Win-Trojan/Autorun.232105'가 최근 발견돼 주의가 요망된다고 안철수연구소의 보안대응조직인 ASEC은 밝혔다.



'Win32/Palevo.worm.52736.E'는 자기 자신을 휴지통 폴더에 복사하고 자동실행 되도록 Desktop.ini 스크립트 파일을 같은 폴더에 생성한다.

이 웜은 자  
일을 다른  
으로 보인

**UDP 패킷의 용도가 키보드 입력값 전송인 것으로 추측됨**

등에서 실행 파  
서 설치하는 것

특히, 해당 사이트로 사용자의 개인정보를 전송하거나 사용자가 입력하는 키보드 입력 값을 가로채 전송하는 것은 물론 다양한 악의적인 스크립트를 실행하는 경우도 있으므로 주의가 요구된다는 것.

# 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

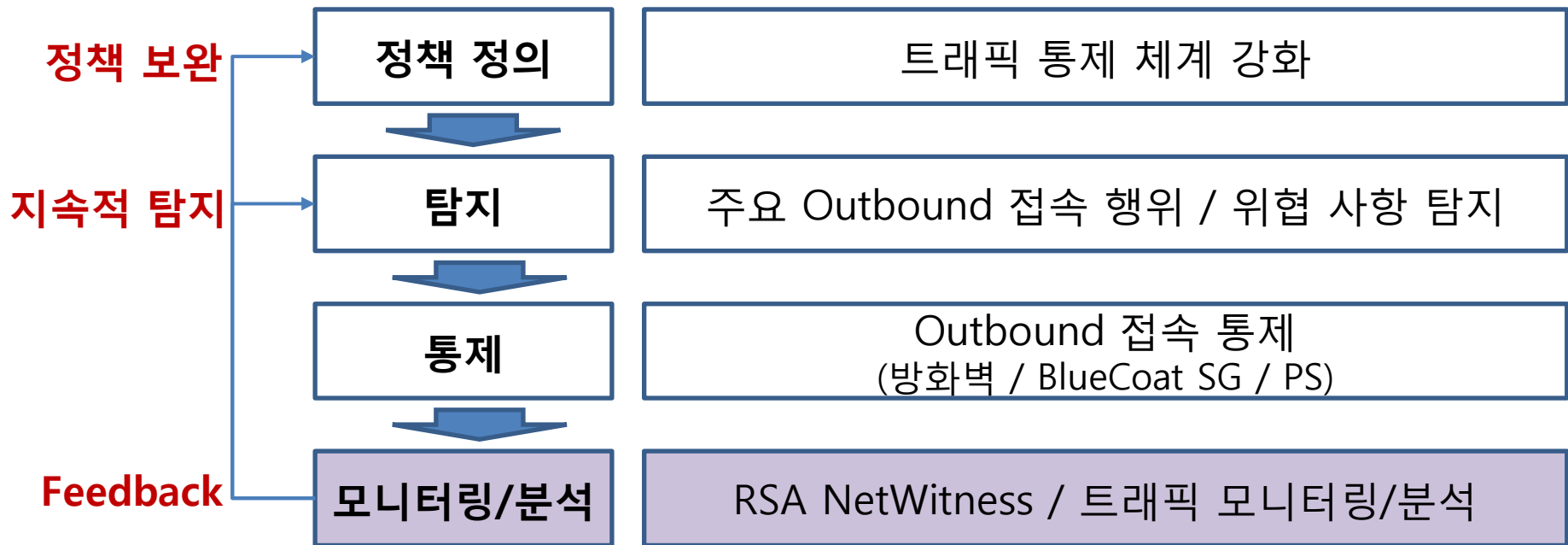
- 조직에 위협이 될 수 있는 업무 관행 파악 및 개선
- Outbound 트래픽 통제 시에 기존 업무 영향도 분석

# 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***