지능형 지속 위협(APT)의 최근 경향과 효과적인 대응 방안

한국트렌드마이크로
최영삼 실장
sam_choi@trendmicro.co.kr

Agenda

- 최근 APT 동향
- APT 탐지 이슈
- 대응 기술 소개
- 대응 사례

최근 APT 동향

2014년 동향

Scale of Impact and Losses Due to Cyber Attacks Intensified

2014 Was the "Year of PoS RAM Scrapers"

Heartbleed and Shellshock Proved That No Application Was Invulnerable

Online and Mobile Banking Faced Bigger Security Challenges

TREND MICRO

최근 사례 – Sony, 한수원

12월 24일 한국수력원자력 MBR 파괴 악성코드 공격받아

2014년 12월 24일 | by Trend Micro

최근 국내 주요 원전시설을 운영하는 한국수력원자력(이하 한수원)이 마스터 부트 레코드(이하 MBR)를 삭제하도록 설계된 악성코드에 감염되어 사회적 이슈가 되고 있습니다. 악성코드는 한글 워드 프로세서(HWP) 취약점을 통해 감염되었으며, 한수원 임직원들이 악성 첨부파일을 실행하도록 하기 위한 다양한 사회공학적 공격 기법이 사용되었습니다. 아래 그림과 같이 공격은 임직원들에게 전송된 스피어피싱 이메일에서부터 시작되었으며 첨부파일 실행시 2가지 악성코드를 설치하는 방식으로 진행되었습니다.

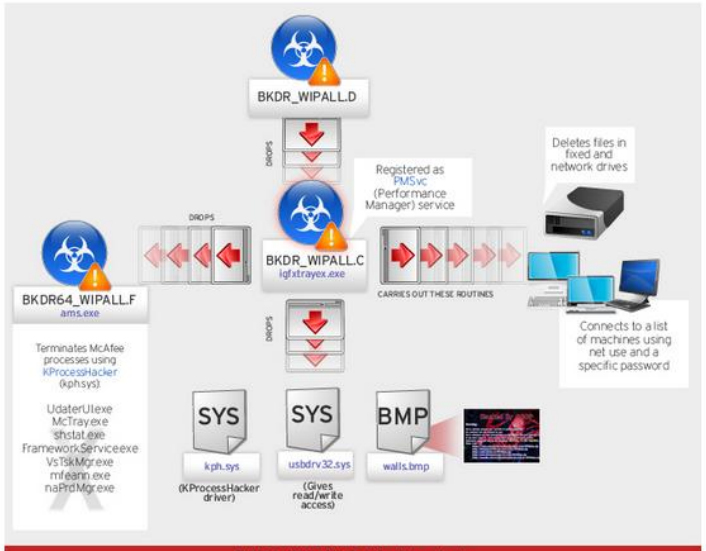
Infection Chain for MBR Wiper Attack

출처 : 트렌드마이크로 블로그

12월 8일 소니 픽처스 해킹 GOP 경고문과 관련된 WIPALL 악성코드 분석

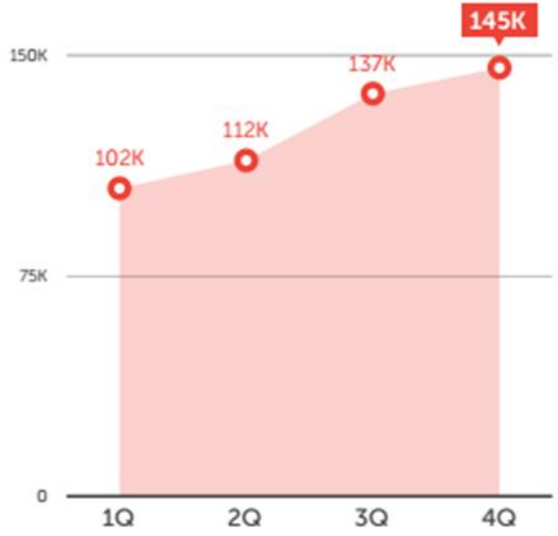
2014년 12월 8일 | by Trend Micro

이전 블로그에서는 소니 픽처스 해킹에 사용된 WIPALL 악성코드에 대한 분석과 이와 관련된 FBI 보안 조언에 대해 다루었습니다. 이번에는 다른 WIPALL 악성코드 변종들과 소니 픽처스 직원들의 감염된 컴퓨터에 나타난 GOP 경고문에 링크된 경로에 대해 자세히 알아보도록 하겠습니다. 다음은 이번 게시글에서 다루게 될 감염 경로 및 연관성에 대한 개요입니다.

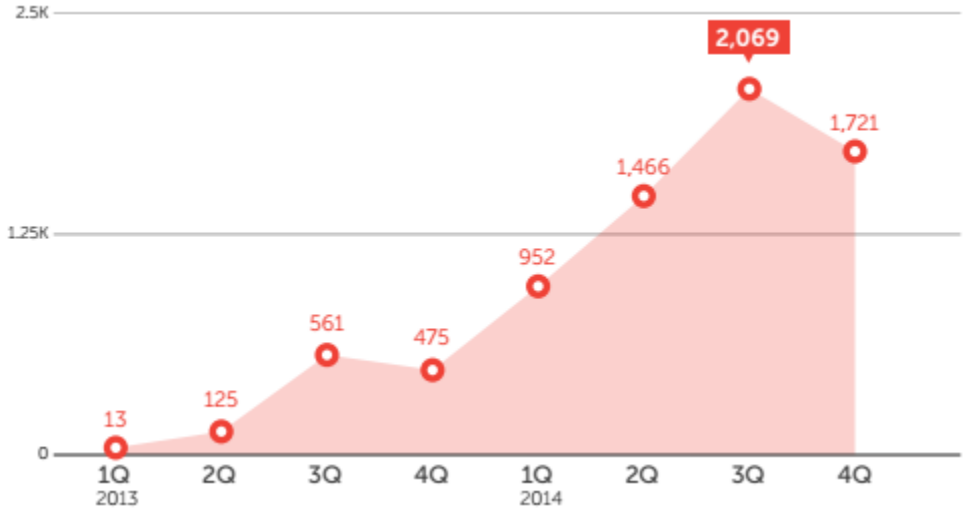


BKDR_WIPALL.D infection chain

Banking Malware

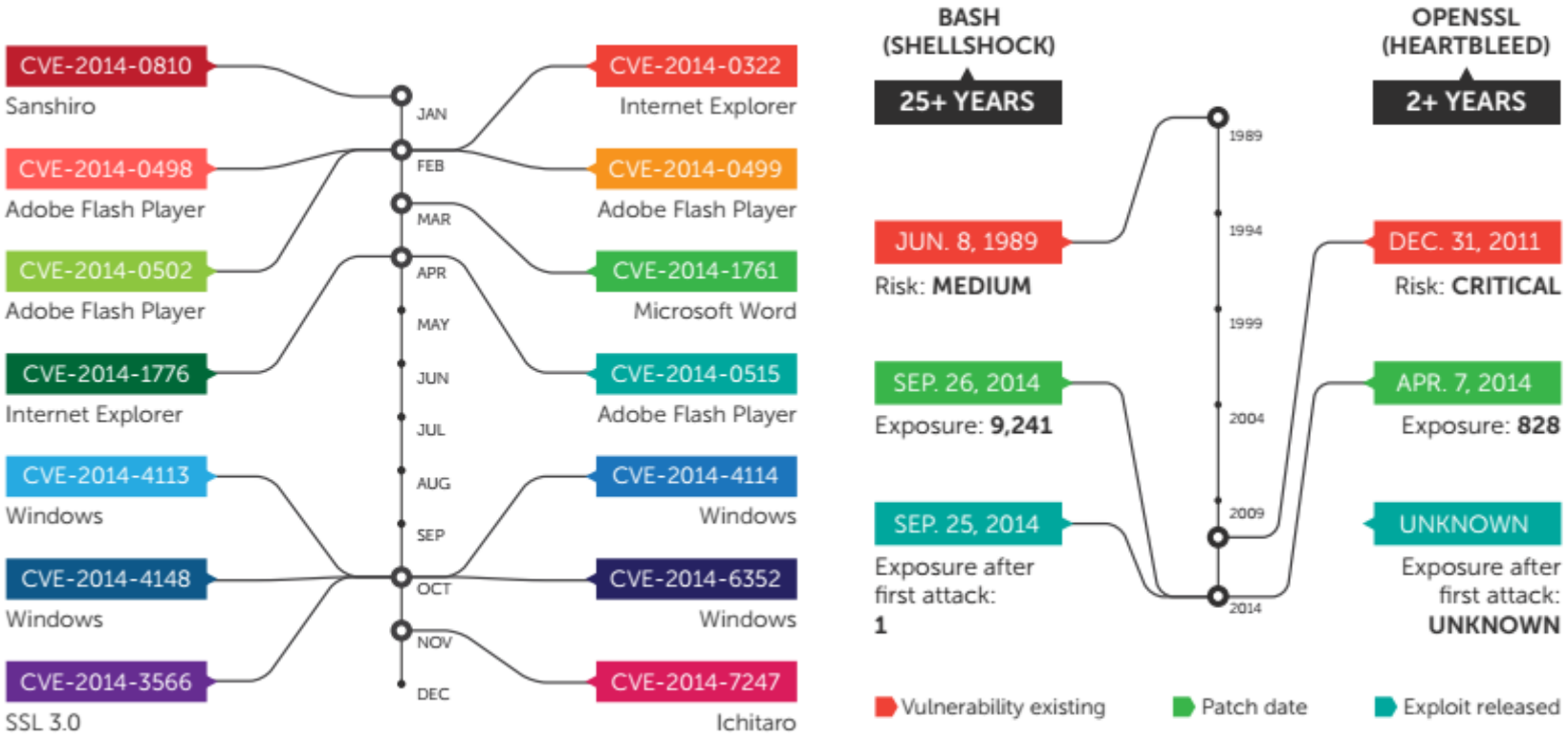


2014 Online Banking Malware가 발견된 PC 대수



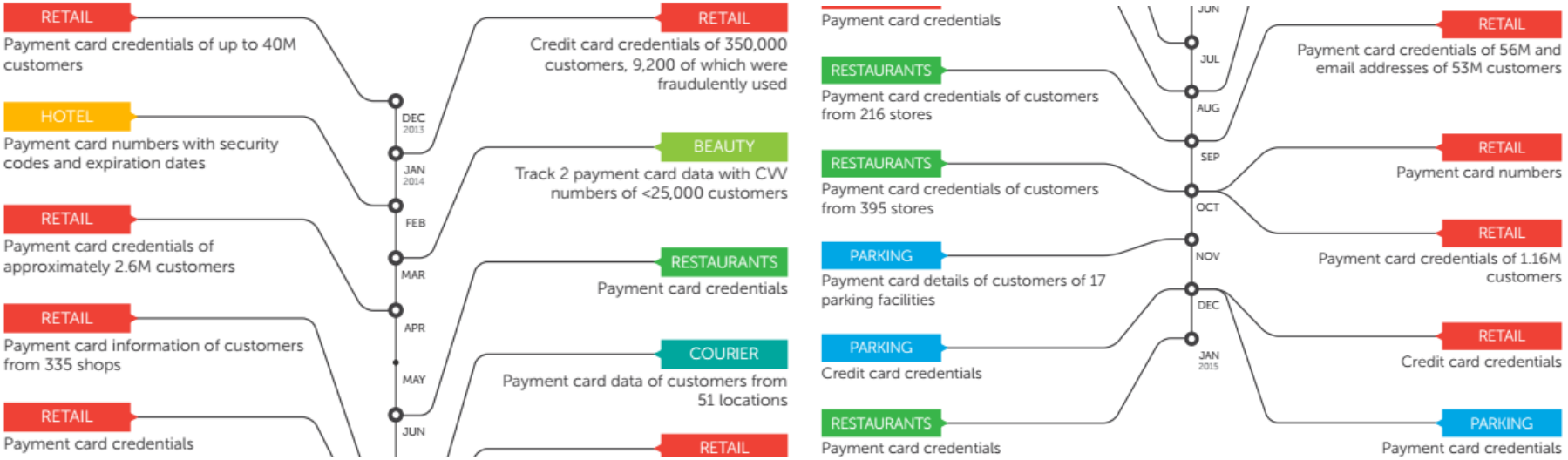
모바일 뱅킹/금융 Malware 개수

Zero-Day 취약점



주요 Zero-Day 취약점의 타임라인 (2014)

PoS-RAM-Scraping



PoS-RAM-Scraping 사고 타임라인 (2014)

APT 탐지 이슈

APT 탐지 어려움

- 기존 백신 및 전통적인 보안 솔루션에서 탐지 못함

  Anti-Virus

  Intrusion Prevention System / Next Generation Firewall

- 다양한 탐지 회피 기법

  Packing, Obfuscation, Anti-VM 등

TREND MICRO

APT 솔루션 이란?

가장 중요한 2가지 기능

- Unknown Malware 탐지
- C&C Communication 탐지

APT 솔루션 이란?

APT 기반 솔루션

- Mirror Traffic Detection, Email Gateway + Sandbox
- IPS, Next-Gen F/W + Sandbox
- Web Gateway, Web Filter, Anti-Spam + Sandbox

"Sandbox는 APT 탐지를 위해 필수적인 구성요소임 "

TREND MICRO

Sandbox 이슈

- 다양한 Sandbox 우회 기법
- Sandbox 분석 환경의 정형화로 인한 탐지 한계
- 오탐

"공격자는 Sandbox 우회 집중"

" Sandbox 분석 기능에 너무 의존하는 기술은 한계가 있을 수 밖에 없음"

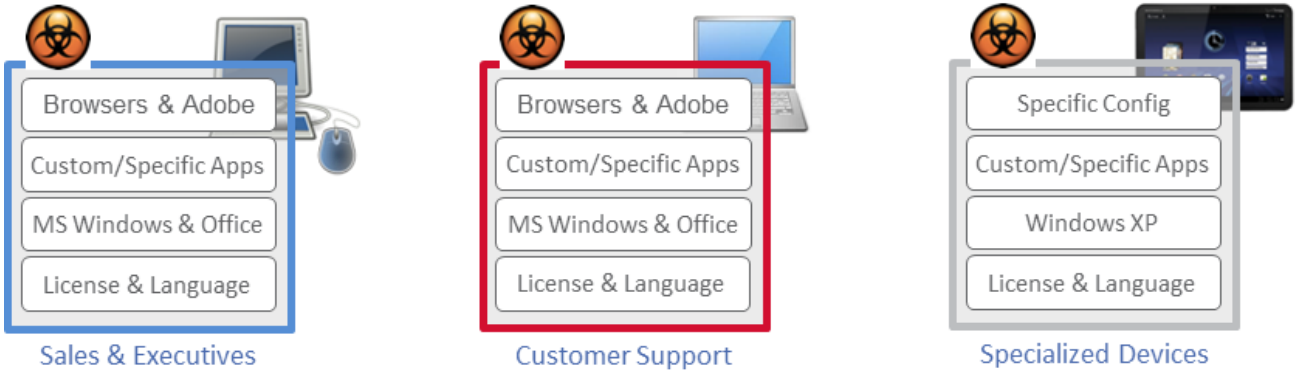
TREND MICRO

APT 대응 기술

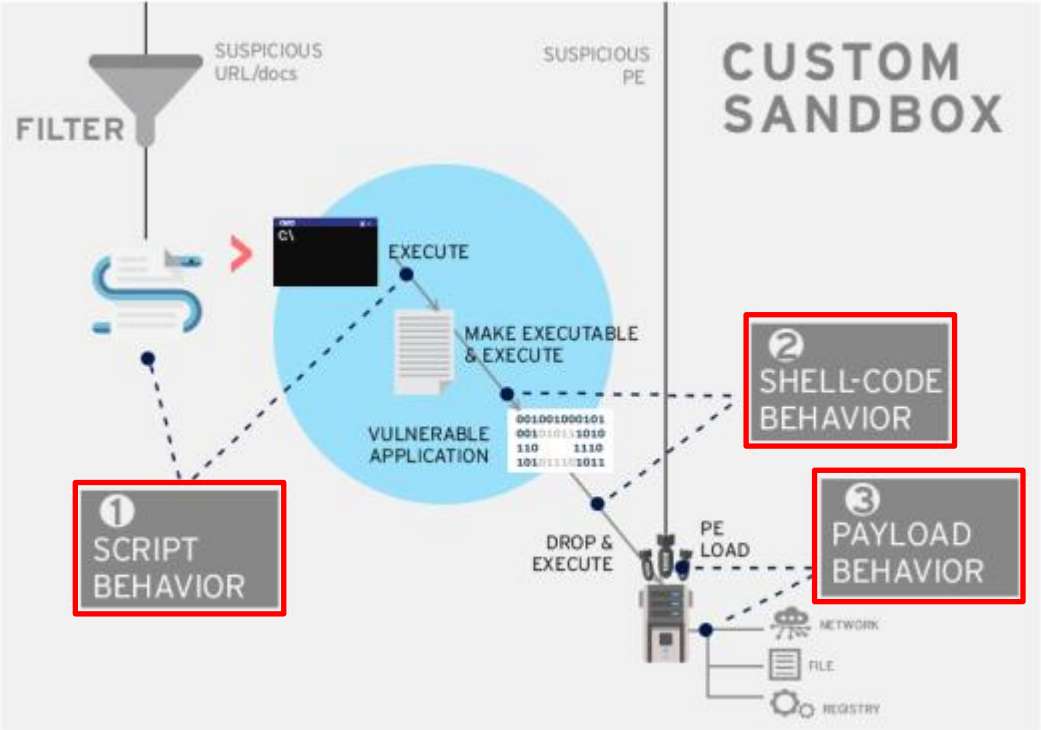
Custom Smart Sandbox

- 사용자 환경과 동일한 OS 및 Application 버전으로 구성

1) 사용자 조직을 타깃으로 하는 공격에 대한 정확한 탐지
2) 사용자 환경에서 실행되는 malware 분류
3) 시스템 구성 정보를 기반으로 하는 회피 기법 무력화



Custom Smart Sandbox



맞춤형 스마트 Sandbox 구조

Script Behavior

Exploit의 변칙적 개체 활용, 함수 호출 및 Heap-Spray를 알려줌

Shell-Code Behavior

ROP/Shell-Code 실행을 통해 이루어지는 Exploit의 스택 및 힙 사용과 어플리케이션 프로세스의 변칙적 파일/레지스트리 활동 탐지

Payload Behavior

생성된 자동 실행 루틴, 드롭된 파일, C&C 서버 접속 등과 같이 시스템에 미치는 영향을 밝혀낼 수 있음

Custom Smart Sandbox - Anti-Evasion

Malware에서 가상(Sandbox)환경 체크 항목

- Hypervisor Detection
- Virtual Device Detection
- Network Address Detection
- BIOS/Activation code Detection
- Virtual Driver Detection
- CPUID Detection
- Human Interaction Detection
- Timer Evasion

등등…

Custom Smart Sandbox

	HTTP Trunk	HTML Evasion	Java Pack200	SWF DoSWF	PE Evasion
FlashPack EK	✔	✔	✗	✔	✗
Rig EK	✗	✔	N/A	✗	✔
Magnitude EK	✔	✔	N/A	✔	✔
Nuclear EK	✗	✔	✗	✗	✔
Fiesta EK	✔	✔	✗	✗	✔
Angler EK	✔	✔	✔	✗	✔
Sweet Orange EK	✔	✔	N/A	✗	✗
Styx EK	✗	✔	N/A	✗	✗

Exploit Kit이 사용하는 정적 검사 회피 기법

정적 검사로 탐지할 수 없는 Exploit Kit은 맞춤형 스마트 Sandbox로 분석/탐지

ActionScript
Flash Exploit을 위한 맞춤 기능

Emulator
가상시스템 역할

Script Engine
Java, Java Script, VBScript를 실행

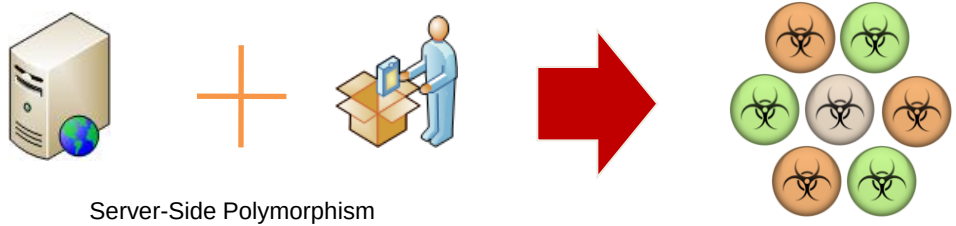
-> Sandbox 내에서 테스트되는 모든 코드에 대한 정보를 더 효과적으로 수집

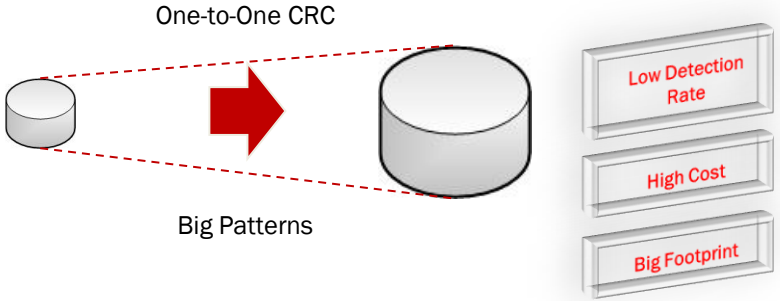
TREND MICRO

Custom Smart Sandbox - Zero-Day Exploit

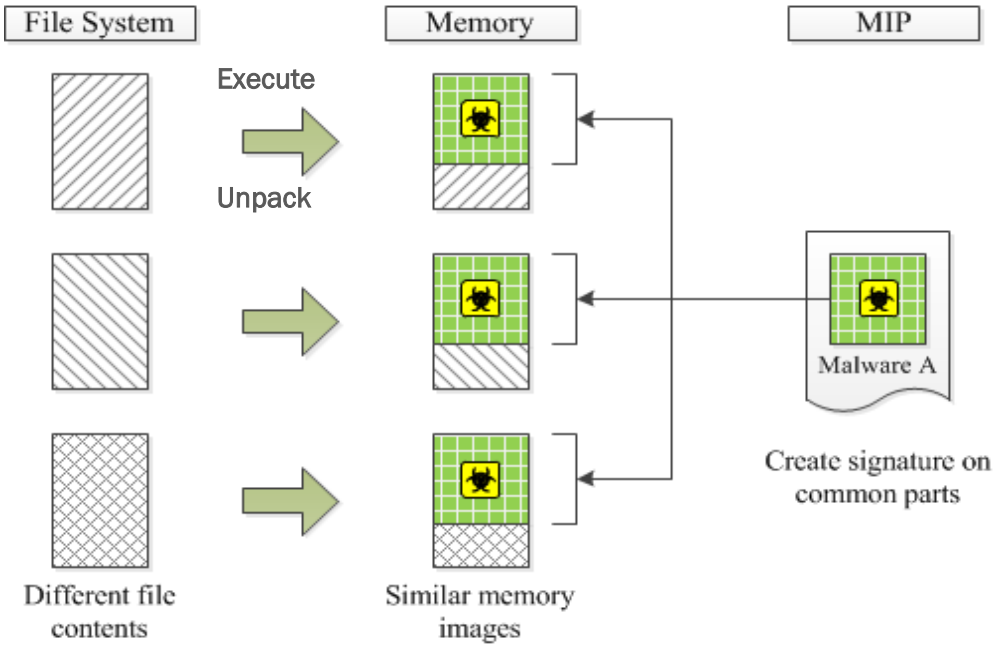
- Browser Emulation
  > exploit behavior, fingerprint of exploit page & CVE
- Browser Hook
  > browser behavior monitoring
- System Hook
  > Drop file, New process/registry/service
  > System file injection

Custom Smart Sandbox - Memory Scan





Custom Smart Sandbox - Memory Scan



C&C 통신 탐지

- 알려진 C&C 정보 (IP address, Domain, URL)
- Fingerprint of Payload
- URL Sandboxing

Global Threat Intelligence

TREND MICRO | Threat Connect

Copy Shortcut

188.124.15.228

Overview | Connection Details

Summary

Rating:	Dangerous
Category:	C&C Server
Last server location:	Bursa, Turkey
First monitored:	2013-11-08
Last activity:	2014-12-29

30-Day Connection Statistics

Trend	
Total	1775 connections
Peak	2014-12-13 (168 connections)
Trough	2014-12-27 (0 connections)
Average	60 connections

Related Malware Family - Trojan

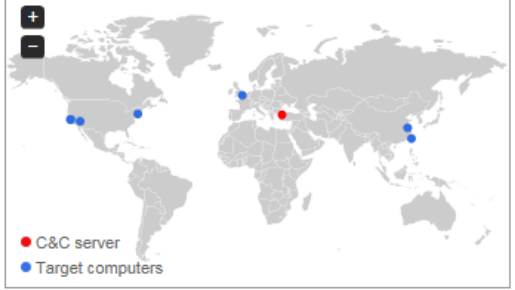
Damage potential	medium
Distribution potential	medium

A Trojan horse program is a malware that is not capable of automatically spreading to other systems. Trojans are usually downloaded from the Internet and installed by unsuspecting users.

Trojans, as the term implies, may come in *disguise* when in your system. It can:

Be disguised as a legitimate software component

Distribution



Country Impact

Taiwan	99%
United States	1%
Japan	<1%
China	<1%
United Kingdom	<1%

Sightings

Common
1001 - 10000 Sightings

View full report

ack address

ver
CK_GENERIC.WRS
rkey

3-11-08
4-12-28

4-12-13 (168 connections)
wan, United States, Japan

TREND MICRO

다양한 탐지 기법과 다중 검사 필요

- Known Malware 탐지
- C&C 통신 탐지
- Sandbox 분석 (Unknown Malware & C&C)
  - > Anti-Evasion
  - > Zero-Day Exploit 탐지(Script Analyzer)
  - > Memory Scan
- Global Threat Intelligence

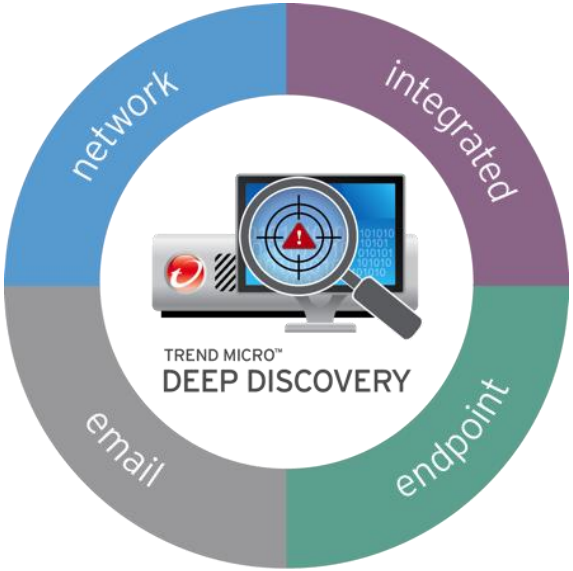
APT 대응 사례

Deep Discovery Products

Network-wide attack detection

APT 탐지

트래픽 분석을 통해 악성 사이트 접속, 악성코드 다운로드, C&C 통신 및 악성 행위 탐지



Integrated sandboxing

APT 분석

알려지지 않은 신종/변종 악성코드에 대한 행위 분석 (Sandbox 분석)

Email attack protection

Email APT 차단

이메일에 첨부된 악성 첨부파일과 URL을 탐지, 분석, 차단하는 Email APT 전용 솔루션

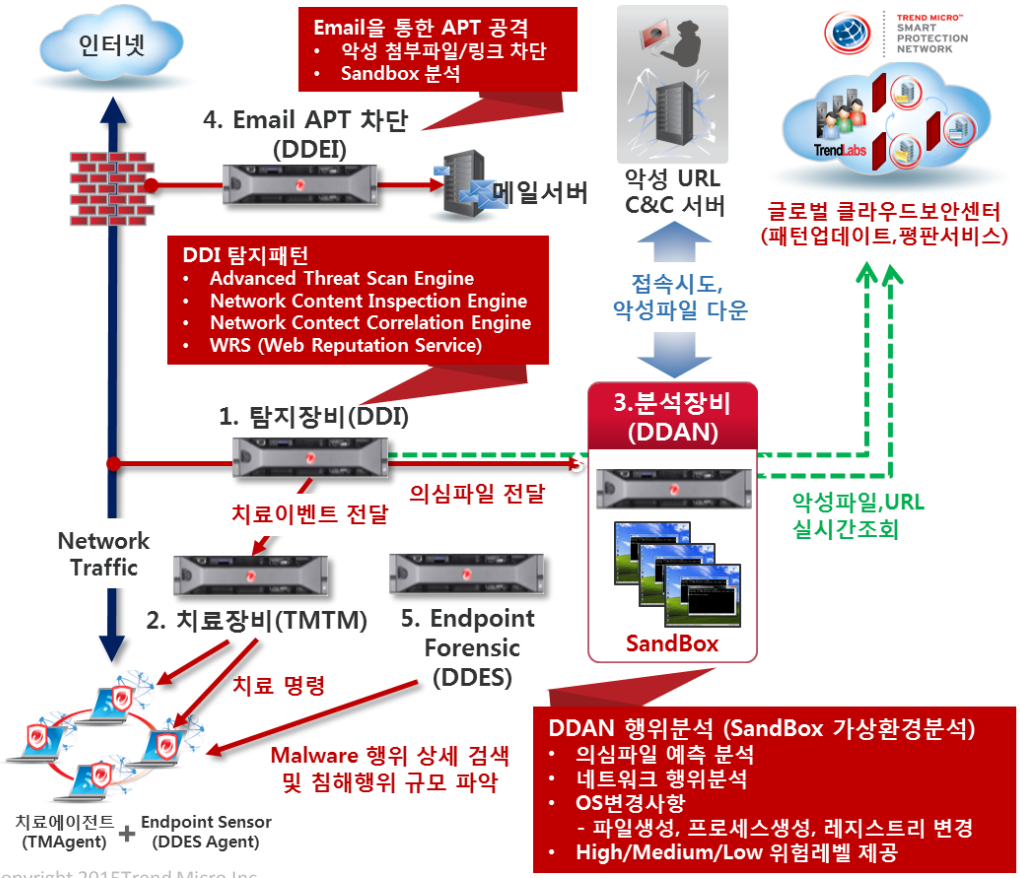
Endpoint Investigation

Endpoint Malware Forensic

Endpoint 에서의 Malware 행위/결과 분석 및 대응

TREND MICRO

Workflow



1. APT 탐지장비 (Inspector)

- ✓ SMTP, POP, HTTP, FTP, P2P 등 80여개의 프로토콜과 어플리케이션 탐지
- ✓ 실행파일, 문서파일, 압축파일 등 수집 및 탐지
- ✓ 알려진 악성코드 탐지 및 치료이벤트 발생
- ✓ 웹평판서비스 –Black List Domain (WRS - Web Reputation Service)
- ✓ 알려진 C&C 접속 탐지 및 치료이벤트 발생
- ✓ 알려지지 않은 악성코드 탐지 및 분석장비로 전송

2. APT 분석장비(Analyzer)

- ✓ 의심파일 예측분석
- ✓ 악성코드 네트워크 행위 분석
- ✓ PCAP생성 및 제공
- ✓ 추가 다운로드 파일 분석
- ✓ OS 변경사항 분석
- ✓ High/Medium/Low 위험레벨 제공
- ✓ 악성의심파일 수동 업로드 분석

3. Email APT 차단 솔루션(Email Inspector)

- ✓ Email에 첨부된 악성 파일 탐지/차단
- ✓ Email에 포함된 악성 링크 탐지/차단
- ✓ 샌드박스 분석
- ✓ WRS(웹평판서비스) 조회

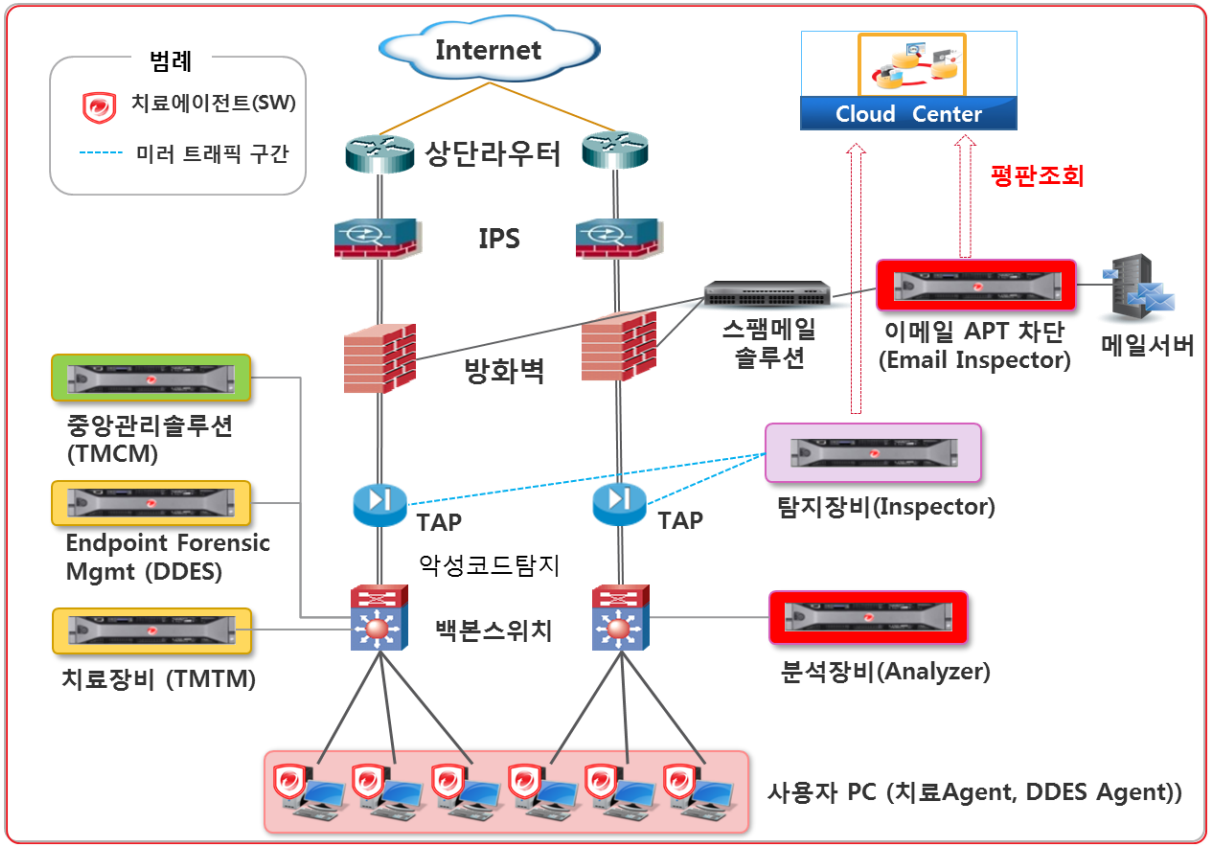
4. Endpoint Forensic(Endpoint Sensor)

- ✓ Endpoint에서의 Malware 행위 및 결과 분석
- ✓ Malware에 의한 침해행위 전후 관계,시간, 규모 파악을 통해 신속한 확산 방지

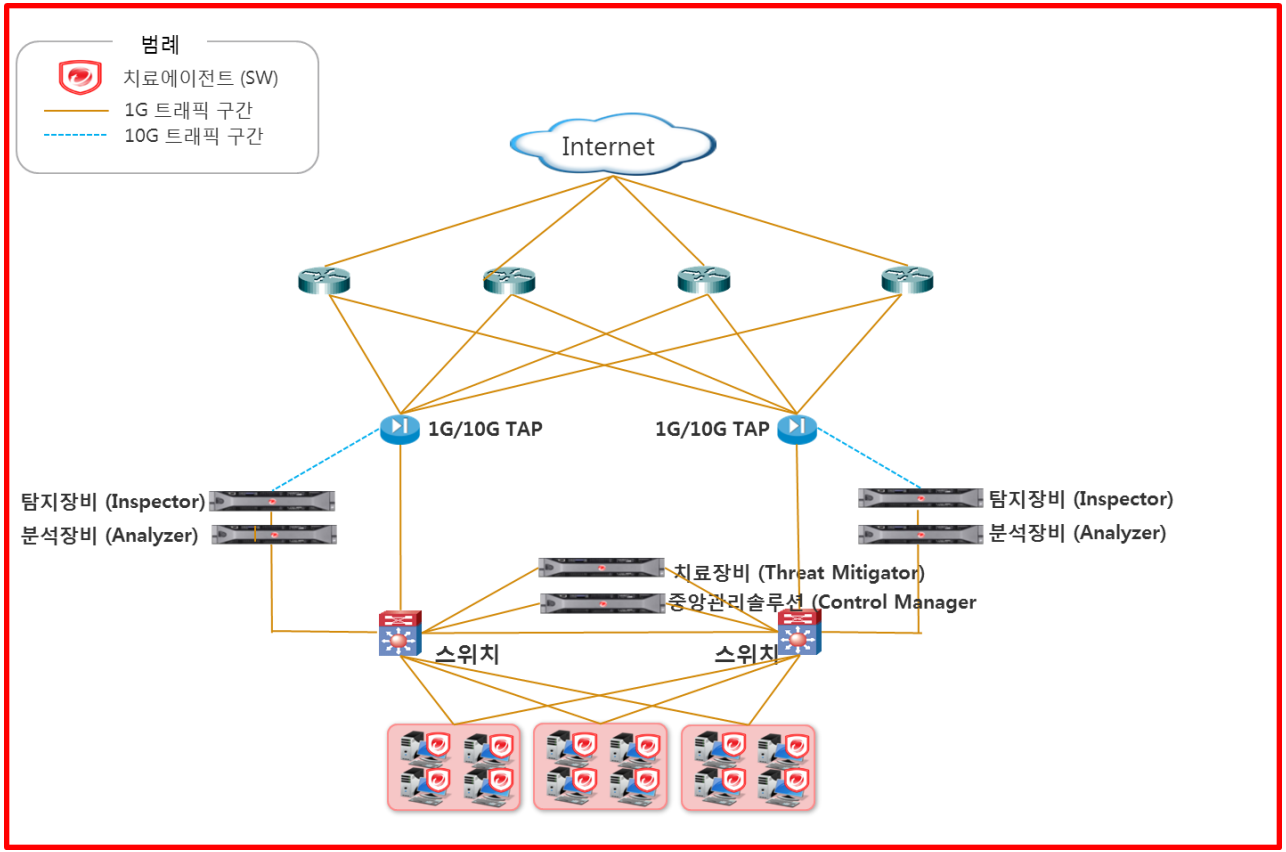
5. 치료장비(Threat Mitigator)

- ✓ 에이전트관리
- ✓ 치료명령전달
- ✓ 치료결과로그관리

APT 대응 사례 – A카드사



APT 대응 사례 – A미디어사



Thank You