실행파일에서 악성 코드의 행동을 정적으로 검출하기

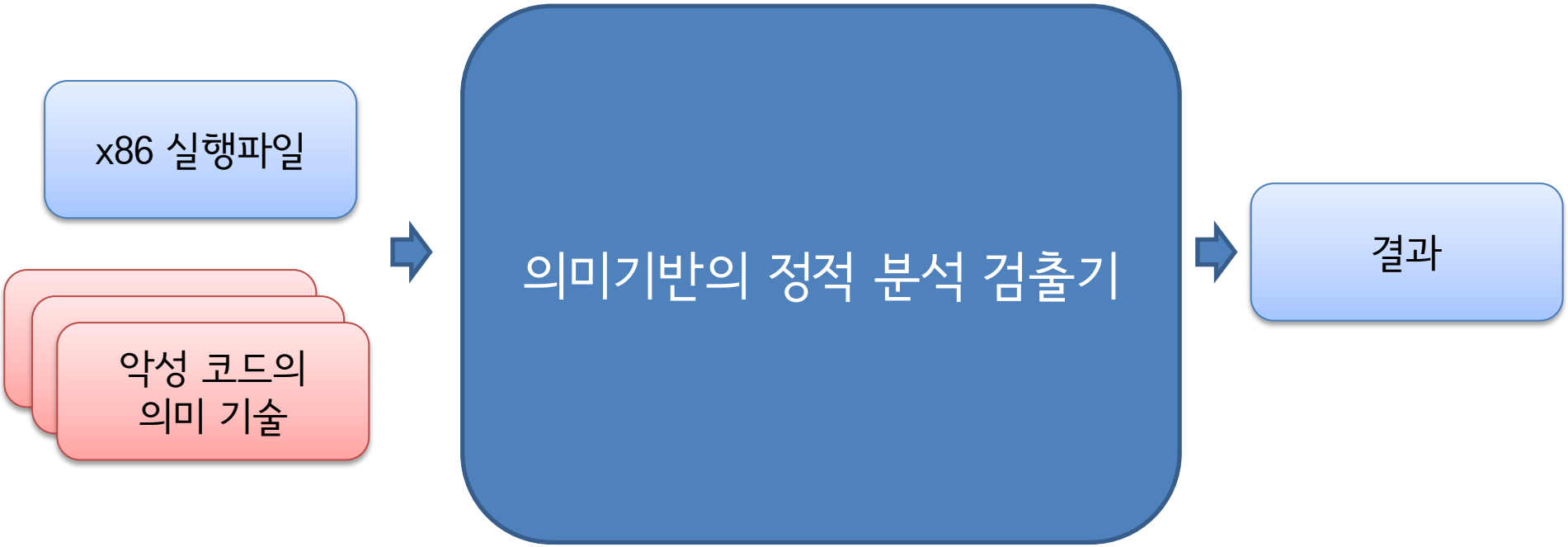
이승중

2012.07.26

서울대학교 프로그래밍 연구실

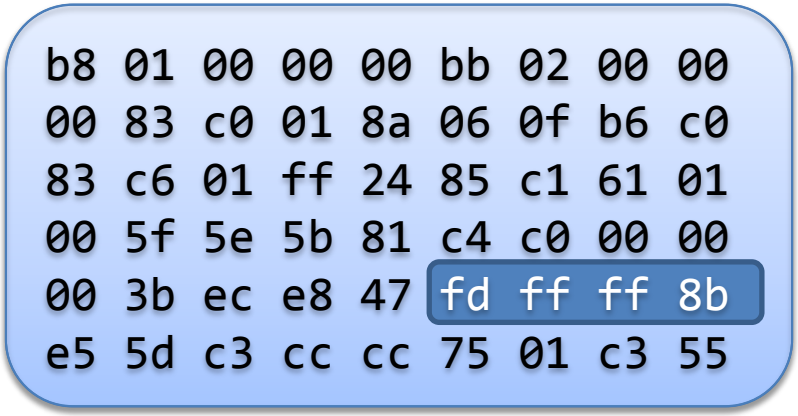
목표

x86 실행파일이
악성코드의 행동을 하는지 여부를
의미 기반의 **정적 분석**으로 찾아내기



기존의 방식 vs 의미 기반의 분석

- 기존의 방식
  - 프로그램 특정 부분의 모양이
    악성 코드의 생김새와 같은지 검사

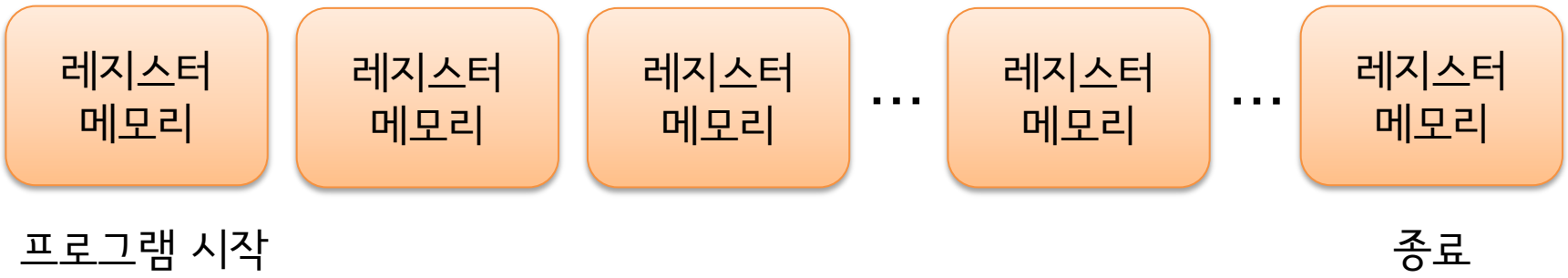


x86 프로그램

악성 코드 패턴

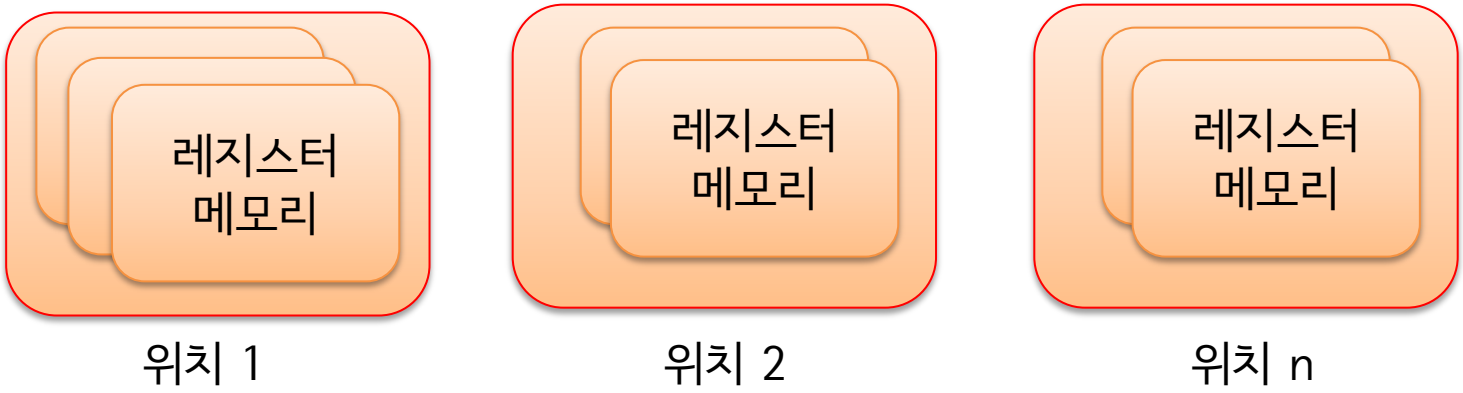
기존의 방식 vs 의미 기반의 분석

- 의미 기반의 분석
  - 프로그램의 실행 의미 사용
  - x86 프로그램의 실행 의미
    - 머신 상태(레지스터와 메모리)의 변화 과정

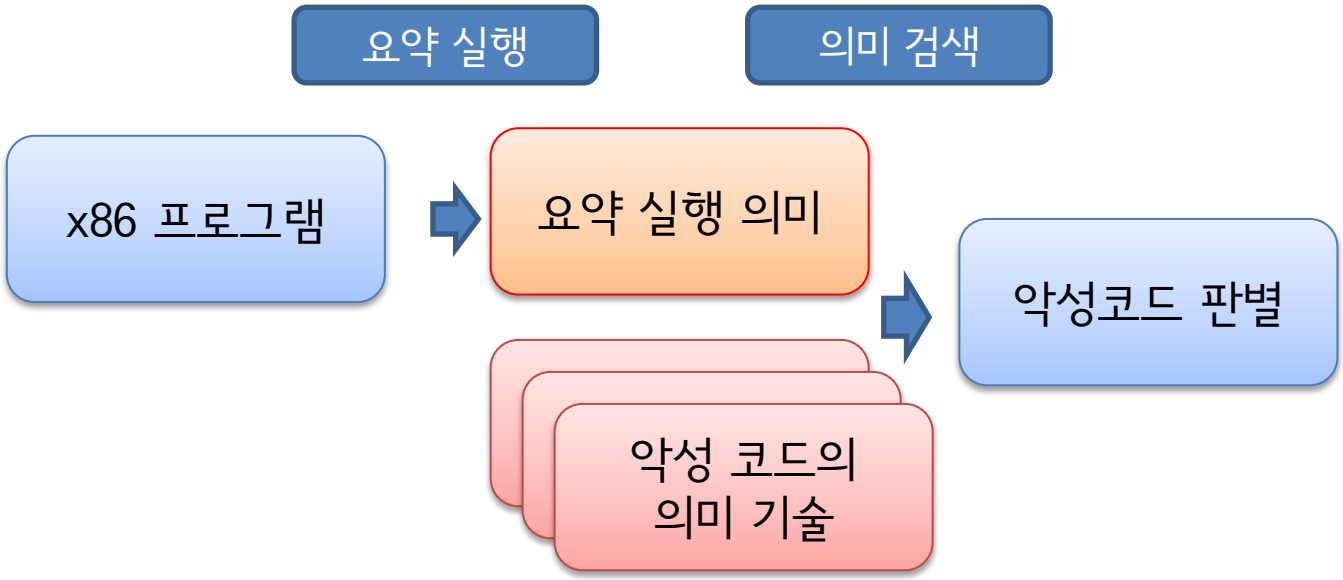


기존의 방식 vs 의미 기반의 분석

- 의미 기반의 분석
  - 모든 정보를 다 알 필요가 없으므로 요약
  - x86 프로그램의 요약 실행 의미
    - 프로그램 카운터(PC) 위치 별로 가능한 모든 레지스터와 메모리의 상태를 포괄하는 요약 상태들



실행 의미 기반 악성 코드 검출



악성 코드의
의미 기술

악성 코드의 행동을 표현

- 행동 기술 언어 정의

$$
\begin{array}{lcll}
c & := & b & \\
 & | & b \wedge b & \\
 & & & \\
b & := & \mathit{InsideCodeSection}(e) & \text{address belongs to code section} \\
 & | & \{e\ (e^*)\} & \text{function call is in the code} \\
 & | & \{e := e\} & \text{assignment is in the code} \\
 & | & \{\mathit{x86\_instruction}\} & \text{x86 instruction is in the code} \\
 & | & \{\mathit{x86\_instruction}\} \text{ with } c & \text{x86 instruction is in the code with given condition} \\
 & | & e = e & \text{values of two expressions are equal} \\
 & | & \neg b & \\
 & | & b \vee b &
\end{array}
$$

- 많은 악성 코드 행동을 잘 표현
  - 시스템 행동 가로채기 등

virustotal

SHA256: 2794c8ff69463d21ba689bcd5e14526c28dc82ac2cf7ab47e15aa746ec7d4b86

File name: 5A17B4874AE37462794DBA537EBBB27F

Detection ratio: 34 / 42

Analysis date: 2011-08-27 05:41:23 UTC (9개월, 1주 ago)

More details

Antivirus	Result	Update
AhnLab-V3	-	20110826
AntiVir	TR/Rootkit.Gen	20110826
Antiy-AVL	-	20110827
Avast	Win32:Agent-LWA [Rtk]	20110826
Avast5	Win32:Agent-LWA [Rtk]	20110826
AVG	BackDoor.Generic13.ALJF	20110826
BitDefender	Trojan.Rootkit.Agent.BX	20110827
ByteHero	-	20110822
CAT-QuickHeal	Rootkit.Agent.bx	20110827
ClamAV	BC.Heuristics.Rootkit.B-11.SDT	20110827

virustotal

SHA256: ff3273ea6a09c644e3e8fc18f25a2f015707a7a9854bd0017e9f2307a5ee0786

File name: hideprocess.sys

Detection ratio: 5 / 42

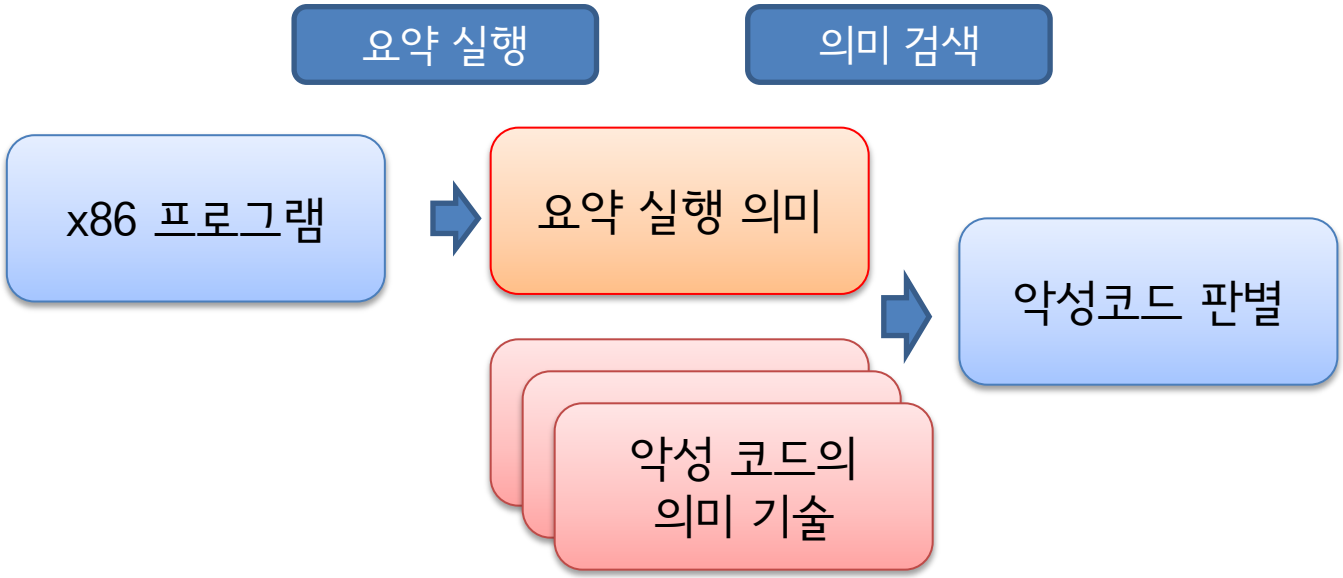
Analysis date: 2012-06-03 21:05:08 UTC (0분 ago)

More details

Antivirus	Result	Update
AhnLab-V3	-	20120603
AntiVir	TR/Rootkit.Gen	20120603
Antiy-AVL	-	20120603
Avast	-	20120603
AVG	-	20120603
BitDefender	-	20120603
ByteHero	-	20120531
CAT-QuickHeal	-	20120603
ClamAV	-	20120602
Commtouch	-	20120603

포스터

- x86 실행파일이 악성코드의 행동을 하는지 여부를 **의미 기반**의 **정적 분석**으로 찾아내기



- x86 핵심 언어 의미 구조
- 악성코드의 의미 기술 예
- 의미를 검색하는 방법