TREND MICRO

Security
TRENDS 2018

데이터센터(리눅스 서버)를 위한 통합서버보안 적용방안

Trend Micro
김석주 부장

리눅스 서버 위협 요소

리눅스 기반 시스템 보안의 필요성

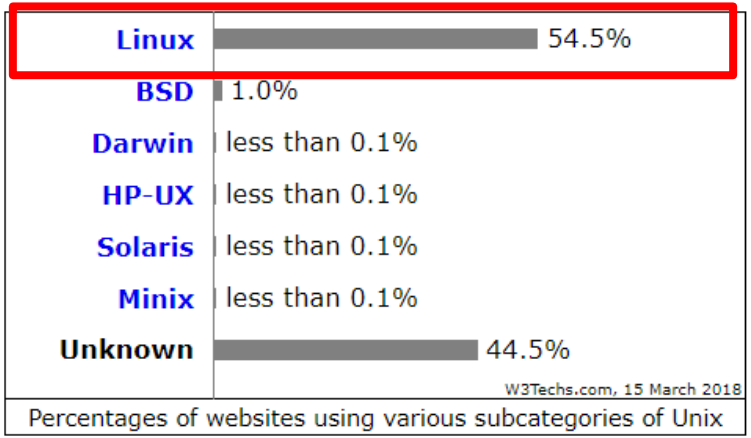
- 67.1%의 웹 서버가 유닉스/리눅스 서버(2018년 2월 1일 by W3Techs)
- 전체 유닉스 계열 서버중 리눅스 서버가 절반 이상(2018년 2월 1일 by W3Techs)

Operating Systems

Most popular operating systems

© W3Techs.com	usage	change since 1 February 2018
1. Unix	67.1%	+0.3%
2. Windows	33.0%	-0.2%

percentages of sites



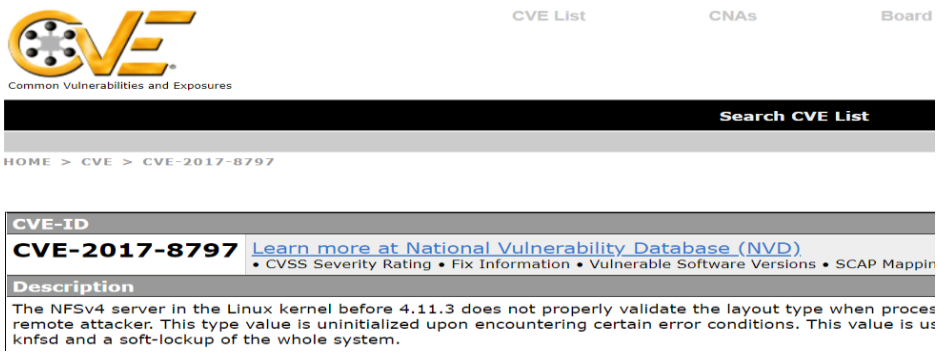
Percentages of websites using various subcategories of Unix

리눅스 시스템 대상 최근 위협 사례

Linux Kernel NFSv4 nfsd PNFS Denial Of Service Vulnerability (CVE-2017-8797)

- Linux Kernel의 NFSv4 컴포넌트에 대한 DoS 취약점
- 원격 공격자는 취약점을 가진 리눅스 시스템에 제작된 패킷을 보냄으로써 이 취약점을 악용
- NFS4.11.3이하 버전에서는 외부에서 들어오는 GETDEVICEINFO / LAYOUTGET의 UDP 패킷을 인증없이 처리

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8797



리눅스 시스템 대상 최근 위협 사례

TREND MICRO | Security TRENDS 2018

TREND MICRO 보안 블로그

리눅스 서비스 중단 (Denial of Service) 을 야기시키는 systemd 취약점 발견

게시일: 2017-12-15 | 작성자: Trend Micro

많은 리눅스 배포판이 최근 systemd 에서 발견된 결함으로 위험에 노출되어 있다는 사실이 밝혀졌습니다. DNS Resolver 의 결함은 취약한 시스템에 대한 DoS (Denial-of-service) 서비스 거부 공격을 유발할 수 있습니다. 이 취약점은 취약한 시스템이 공격자가 제어하는 DNS 서버에 DNS 쿼리를 전송함으로써 악용됩니다. 그런 다음 DNS 서버는 조작된 쿼리를 다시 돌려보내어 systemd 를 무한루프로 실행되도록 하여 시스템의 CPU 사용량이 100% 가 되도록 만듭니다. 해당 취약점은 CVE-2017-15908 입니다.

사용자가 공격자의 제어 하에 DNS 서버를 쿼리하도록 하는 방법은 여러 가지가 있지만, 멀웨어 또는 소셜 엔지니어링을 사용하여 사용자 시스템이 공격자가 제어하는 도메인을 방문하도록 하는 것이 가장 쉬운 방법입니다.

- 취약점 분석:

RFC 4034에 정의된 NSEC (Next Secure) 레코드는 DNS Security Extensions (DNSSEC) 에 추가된 새로운 유형의 리소스 레코드 중 하나인데, NSEC bitmap에서 pseudo-type을 표현하는 비트를 처리하는 과정에서 발생

- 대응 방안:

들어오는 DNS 응답 트래픽을 모니터링하고 응답 섹션의 DNS RR 에 DNS 및 NSEC RR 을 정의하는 RFC 4034 Section 4에 지정된 타입의 레코드가 포함되어 있는지 검색.
첨부된 bitmap 이 처리되고 pseudo-types 가 포함되어 있다면 차단

리눅스 시스템 대상 최근 위협 사례

TREND MICRO | Security TRENDS 2018

Cryptocurrency Miner Distributed via PHP Weathermap Vulnerability, Targets Linux Servers

'합법적 대규모 암호 화폐 채굴 운영업체는 악용 여부 구분없이 채굴에 사용되는 전자기기에 투자'

'Cacti's Network Weathermap plug-in의 오래된 PHP 취약점인 CVE-2013-2618을 이용해 Linux Web Server 대상으로 Shell 스크립트 다운로드 및 실행하여 몰래 채굴'

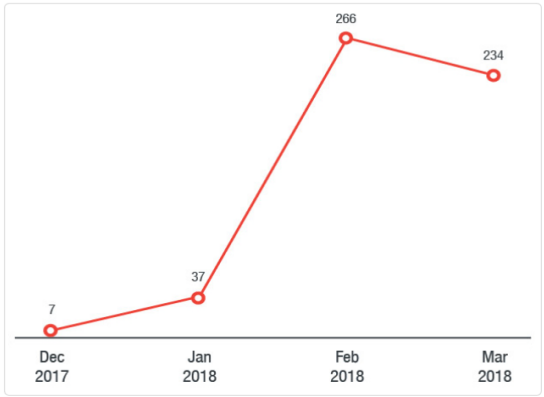


Figure 1. Network intrusion attempts observed from the cryptocurrency-mining campaign (December 2017 to mid-March 2018)

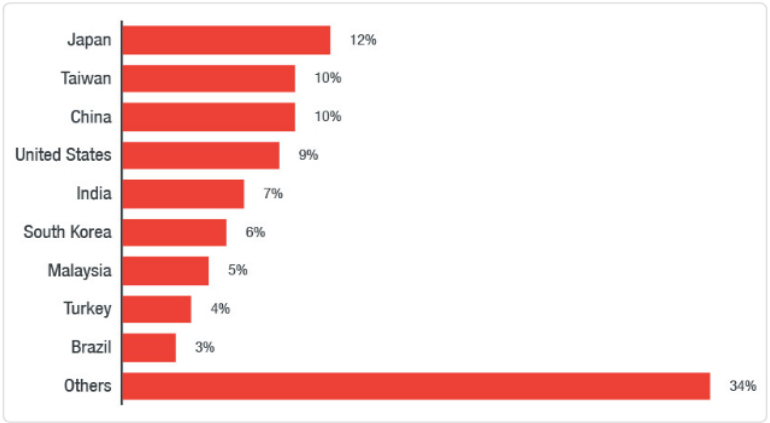


Figure 2. Country distribution of the malicious cryptocurrency-mining campaign

2017’ Major Player (랜섬웨어)

WannaCry

- 약 US$4 billion 피해

Petya

- 약 US$300 million 피해

Bad Rabbit

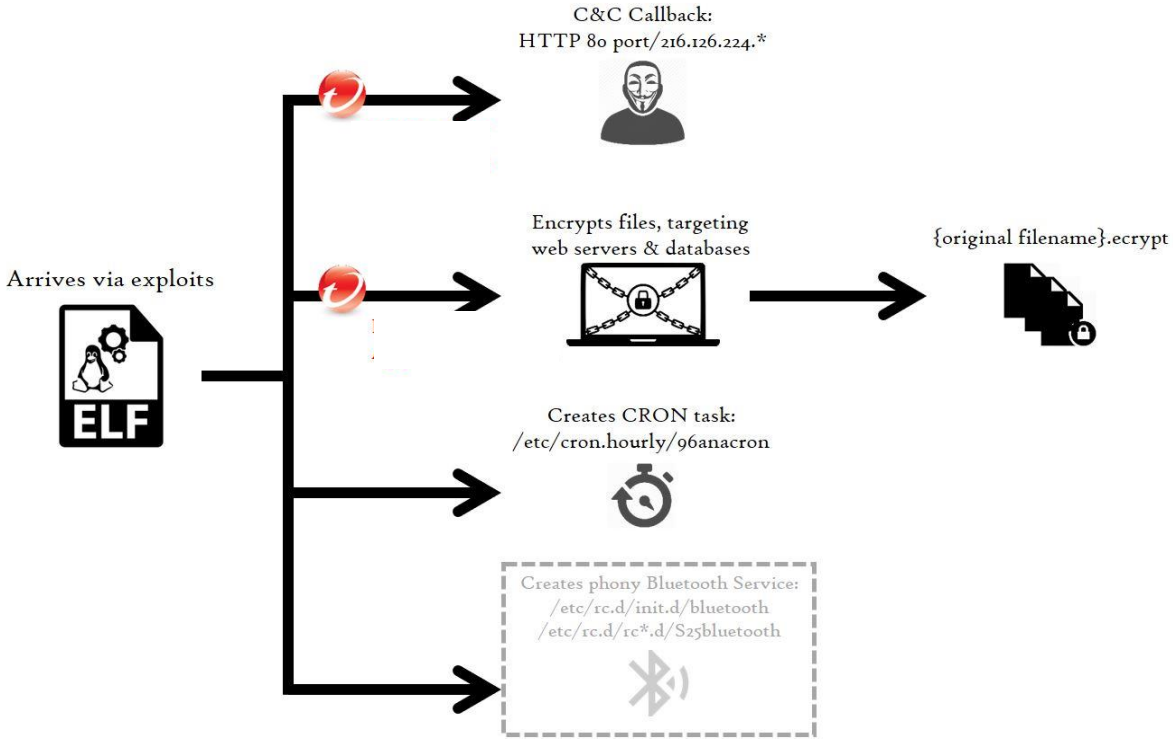
- 러시아 및 동유럽의 미디어 기업들과 인프라 서비스 중단 피해

2017’ 피해의 배경이 된 주요 취약점 (랜섬웨어)

TREND MICRO | Security TRENDS 2018

MARCH	Microsoft는 Windows SMB 원격코드 실행 취약점(CVE-2017-0144와 CVE-2017-0145)에 대한 보안 패치 릴리즈
APRIL	해커 그룹 Shadow Broker **EternalBlue** exploit 공개
MAY	**EternalBlue** exploit을 이용한 WannaCry 확산
JUNE	**EternalBlue** exploit을 이용한 Petya 확산
OCTOBER	**EternalRomance** exploit을 이용한 Bad Rabbit 발견

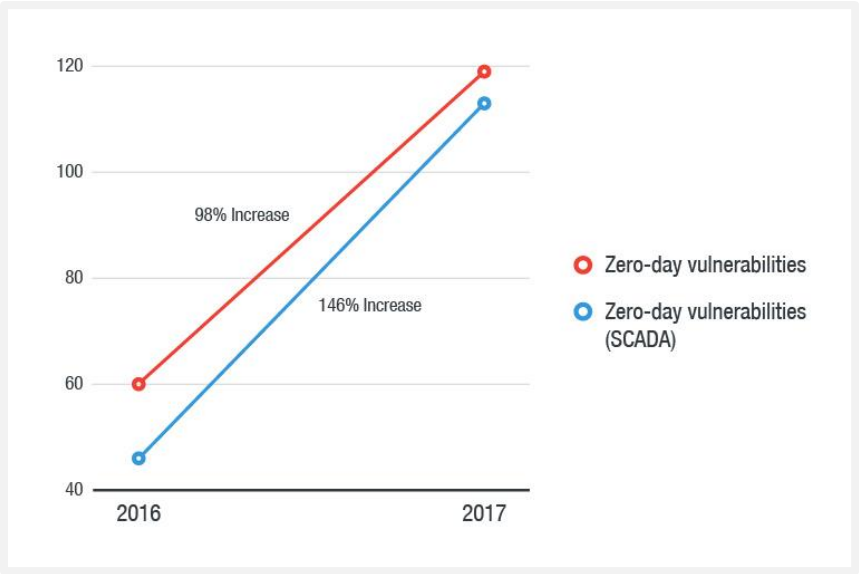
2017' EREBUS 랜섬웨어 위협 사례



SCADA 관련 Zero-Day 취약점 증가

TREND MICRO | Security TRENDS 2018

	2016	2017
Zero-Day Vulnerabilities	60	119
Zero-Day Vulnerabilities (SCADA)	46	113



리눅스 서버 보안 가이드

리눅스 서버 레벨 보안

TREND MICRO | Security TRENDS 2018

호스트 네트워크 트래픽 분석


Intrusion Prevention


Firewall


Vulnerability Scanning

Stop network attacks, shield vulnerable applications & servers

시스템 프로세스/파일/로그 검사


Application Control


Integrity Monitoring


Log Inspection

Lock down systems & detect suspicious activity

파일 기반 멀웨어 탐지


Anti-Malware


Behavioral Analysis & Machine Learning


Sandbox Analysis

Stop malware & targeted attacks

vmware | Microsoft Hyper-V | openstack CLOUD SOFTWARE | amazon web services | Google Cloud Platform | docker

NUTANIX | VCE | SAP | Microsoft Azure | IBM

네트워크 트래픽 분석

침입방지

네트워크와
어플리케이션에
대한 위협 방어

방화벽

측면 이동 공격 차단
및 서버 공격 포인트
감소

취약점 스캔

자동화된 취약점 감사
및 방어 룰 적용

OS와 어플리케이션에 대한 취약점 방어
(ex: Struts 2, Shellshock)

랜섬웨어 탐지 및 차단 (ex: WCRY)

긴급 패치에 대한 요구 감소

EOS 시스템과 어플리케이션 방어

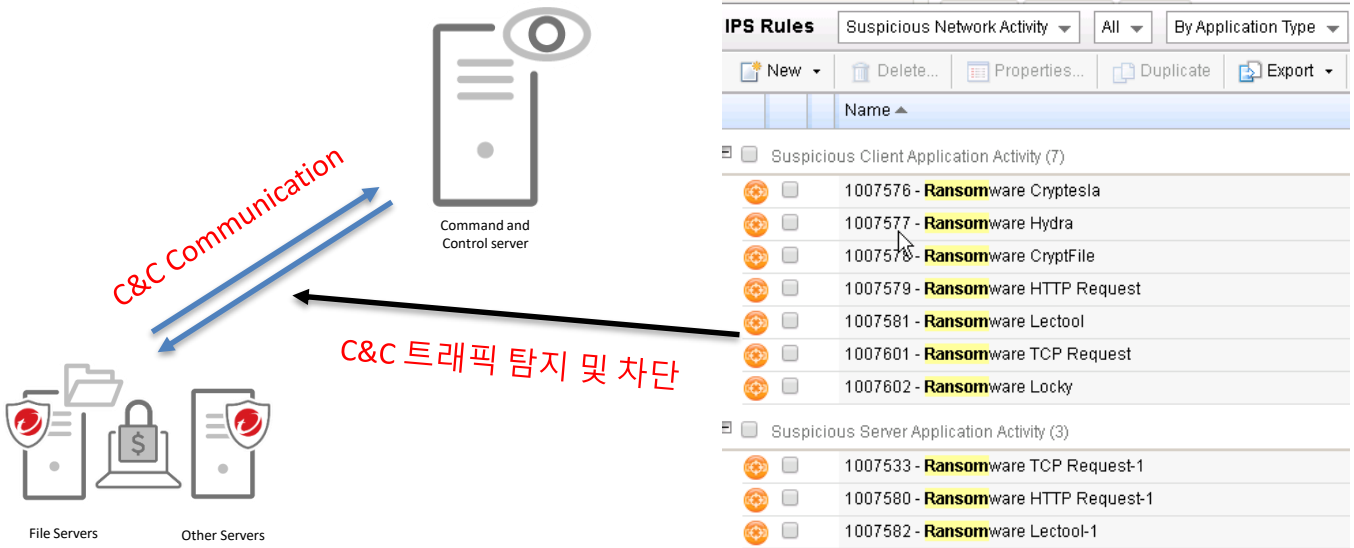
가상 패치(Virtual Patching)

	Vulnerabilities Covered in and after 2014 (approx.)	Before 2014 (approx.)	Total
Non-Windows OS and Core Services	80	230	310
Web Servers	114	472	586
Application Servers	255	319	574
Web Console/Management Interfaces	113	453	566
Database Servers	10	218	228
DHCP, FTP, DNS servers	9	82	91

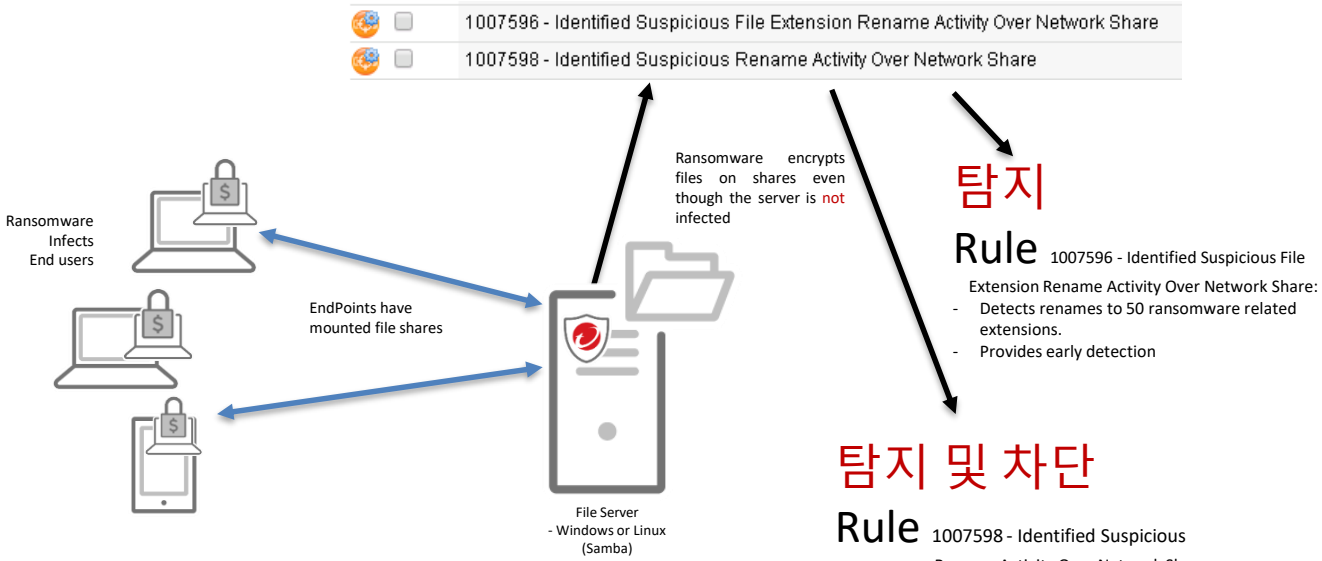
Deep Security 취약점 대응
(CVE기준)

NFS Server (1)			
1008802 - Linux Kernel NFSv4 nfsd PNFS Denial Of Service Vulnerability (CVE-2017-87...	February 14, 2018	CVE-2017-8797	High
Web Client Common (2)			
1003186 - Adobe Flash Player For Linux ActionScript ASnative Command Execution	August 26, 2015	CVE-2008-5499	Critical
1008139 - Linux Kernel Use After Free Remote Code Execution Vulnerability (CVE-2016-...	February 8, 2017	CVE-2016-7117	Critical
Web Server Apache (4)			
1005492 - Identified Suspicious Apache Linux/Cdorked HTTP Request Cookie Header	August 1, 2013	N/A	Critical
1005464 - Debian Linux Httpd Vulnerability	August 14, 2013	CVE-1999-0678	Medium
1005642 - Red Hat Linux Apache Remote Username Enumeration Vulnerability	August 28, 2013	CVE-2001-1013	Medium
1000618 - Apache Linux Slapper Worm (.A variant) Probe	February 28, 2018	N/A	Medium

랜섬웨어 C&C 트래픽 탐지 차단



파일서버 랜섬웨어 조기 탐지 차단



탐지

Rule 1007596 - Identified Suspicious File Extension Rename Activity Over Network Share:

- Detects renames to 50 ransomware related extensions.
- Provides early detection

탐지 및 차단

Rule 1007598 - Identified Suspicious Rename Activity Over Network Share :

- Rule to prevent renames *after* N renames in T1 seconds *for* T2 seconds.
- E.g. if Deep Security Detects 10 renames in 60 seconds stop any rename activity for, say, 24 hrs

시스템 프로세스/파일/로그 검사

어플리케이션 컨트롤

서버에서의 변경 방지 및 Lock down (whitelisting)

무결성 모니터링

의심스럽거나 인가되지 않은 변경 탐지 – 파일, 포트, 레지스트리 등

로그감사

시스템 전반의 로그 정보 통합 및 보고

랜섬웨어와 같은 악성 공격 차단

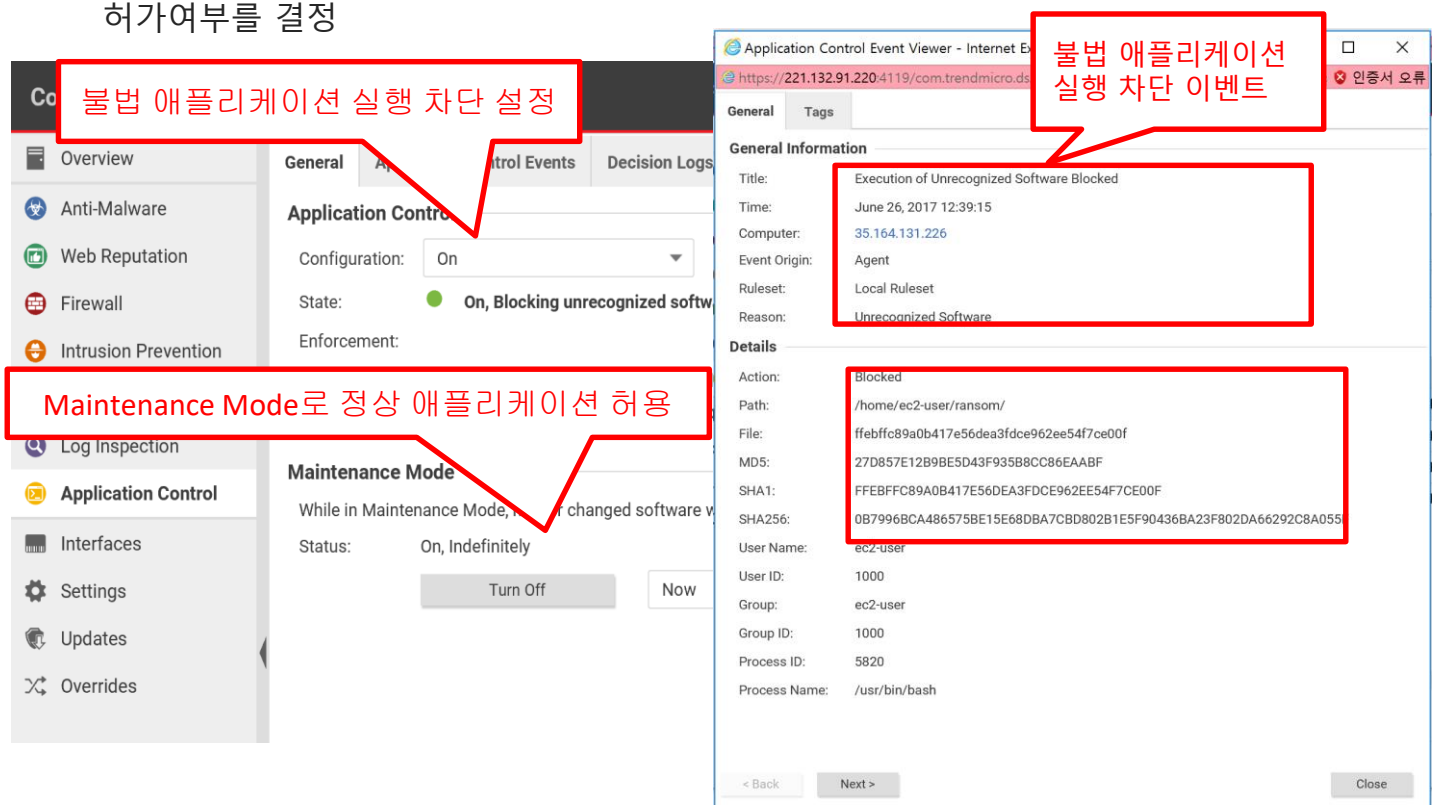
DevOps 와 CI/CD Pipeline 연계

공격 포인트 감소

IOCs (indicators of compromise) 탐지 및 알림

어플리케이션 컨트롤

- 인가되지 않은 어플리케이션 실행을 차단(Default)하고 이벤트를 발생하여 허가여부를 결정

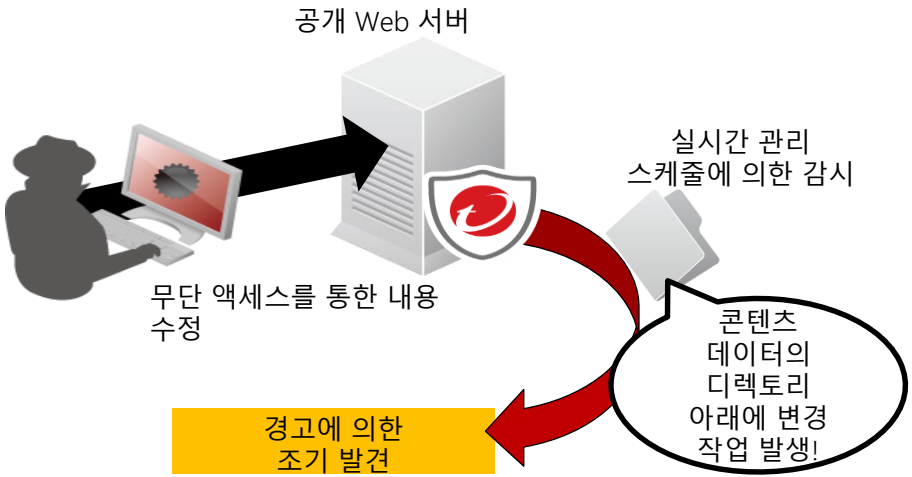


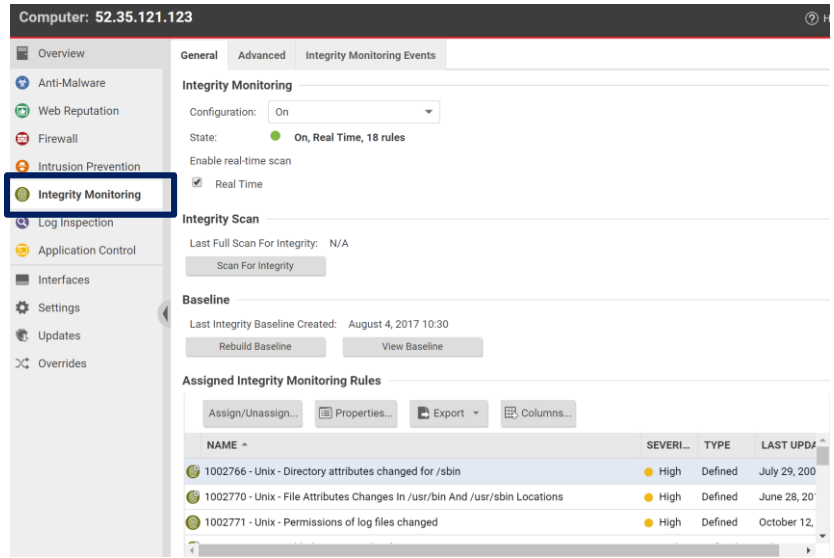
시스템 무결성 검사

TREND MICRO | Security TRENDS 2018

- 파일 (파일 속성 포함), 디렉토리, 레지스트리,프로세스 등의 변화를 감지

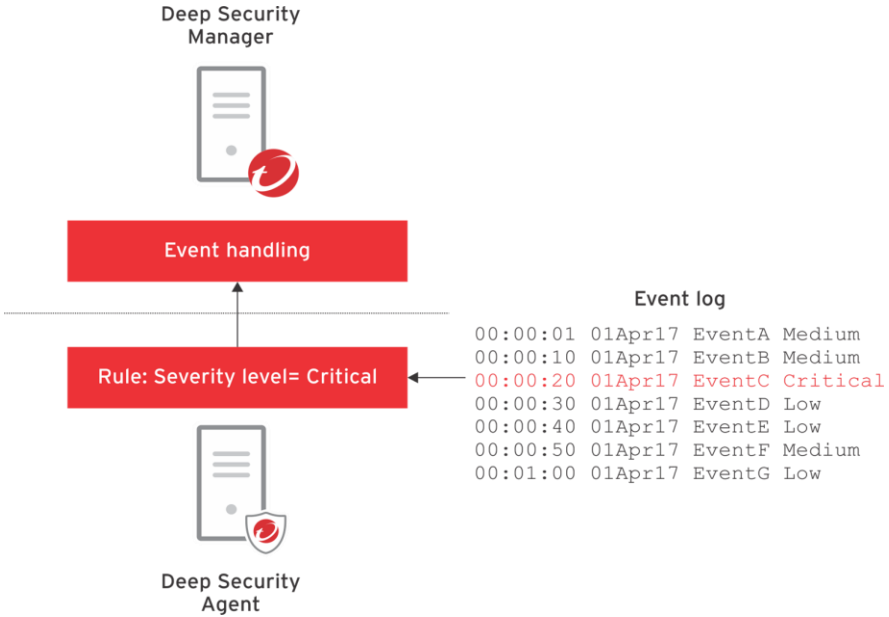
무결성 모니터링 (예)





시스템 로그 검사

- 시스템/App 로그를 모니터링 하여 서버에 접근한 의심스러운 공격에 대해 모니터링 제공



파일 기반 멀웨어 탐지

안티멀웨어 &
컨텐츠필터링

알려진 멀웨어
탐지 및 차단

멀웨어와 표적 공격 차단

행위분석 머신러닝

의심스러운 파일 및
행위 탐지

랜섬웨어 탐지 및 차단(ex: WCRY)

zero-day 공격 방어

샌드박스 분석

의심스로운 파일을
커스텀 샌드박스로
분석 요청

알려지지 않은 위협을 분석하고 보안 장비와 공유

리눅스 서버용 안티멀웨어

- 가장 높은 탐지율과 다양한 리눅스 OS 종류를 지원

Platforms

- Windows (10.3 Agents)
- Red Hat Enterprise Linux (10.3 Agents)
- CentOS (10.3 Agents)
- Oracle Linux (10.3 Agents)
- SUSE Linux (10.3 Agents)
- Ubuntu (10.3 Agent)
- Debian (10.3 Agent)
- Cloud Linux (10.3 Agent)
- Amazon (10.3 Agents)
- Azure (10.3 Agents)
- Agentless (NSX) (10.3 Agents)

Anti-Malware Enabled

PLATFORM	STATUS	POLICY							
Ubuntu Linux 16 (64 bit)	Managed (Online)	None	●	●	○	○	●	●	○
Ubuntu Linux 16 (64 bit)	Managed (Online)	None	●	●	○	○	●	●	○
Ubuntu Linux 16 (64 bit)	Managed (Online)	None	●	●	○	○	●	●	●
Red Hat Enterprise 7 (64 bit)	Managed (Online)	None	●	●	○	○	●	●	●
Ubuntu Linux 16 (64 bit)	Managed (Online)	None	●	●	●	○	●	○	○
Red Hat Enterprise 6 (64 bit)	Managed (Online)	None	●	●	○	○	●	○	○

https://help.deepsecurity.trendmicro.com/supported-features-by-platform.html

TrendLabs: Security Intelligence Blog

- https://blog.trendmicro.com/trendlabs-security-intelligence/

TREND MICRO

Security
TRENDS 2018

THANK YOU

Trend Micro
김석주 부장