

Carbon Black Enterprise

제품 소개 자료



ENTERPRISE
RESPONSE



ENTERPRISE
PROTECTION

2016

(주)인섹시큐리티

● 최근 악성코드 동향

➔ TeslaCrypt 변종 – 파일 확장자를 ‘mp3’ 로 바꾸는 랜섬웨어

파일 확장자 `mp3`로 바꾸는 랜섬웨어 등장... 이중 프로세스로 탐지 우회

[AD] [3/23] 지능형 서비스로봇 기술,시장 최신분석 및 적용사례와 상용화 세미나

파일 확장자를 ‘.mp3’로 바꾸는 랜섬웨어가 국내에 등장했다. 지난해 유포돼 확장자를 ‘.micro’로 변경하는 테슬라크립트(TeslaCrypt) 변종이다. 이중 프로세스로 동작으로 보안제품에 적용된 행위기반 탐지 일부 기능을 회피한다. 올 들어 랜섬웨어 피해가 다소 줄었지만 다양한 변종이 등장해 주의가 요구된다.



<파일 확장자를 ‘.mp3’로 바꾸는 랜섬웨어가 등장했다.©게티이미지뱅크>

보안 업계에 따르면 확장자를 mp3로 바꾸는 랜섬웨어는 설 연휴 직후인 지난 11일경부터 국내피해사례가 보고됐다. 온라인 커뮤니티와 네이버 지식인 서비스 등에도 관련 문의가 올라왔다.

● 최근 악성코드 동향

- ➔ KeRanger – 3일 동안 잠복 후 데이터를 암호화하여 금전을 요구하는 랜섬웨어



● 최근 악성코드 동향

➔ Locky - 기본적으로 파일을 암호화하고, 네트워크에 공유된 데이터까지 암호화를 수행하는 랜섬웨어

또 새 랜섬웨어! 단일 시스템뿐 아니라 네트워크도 침입

입력날짜 : 2016-02-19 11:55 스크랩 프린트하기 목록

좋아요 63 트윗 

최근 랜섬웨어의 트렌드 : 파일을 바꾸기, 네트워크 넘나들기
랜섬웨어 해커들에 돈을 주는 건 공격자들을 후원하는 꼴

[보안뉴스 문가용] 이제 귀에 못이 박힐 정도로 지겨울 수 있지만, 어쩔 수 없다. 새로운 랜섬웨어가 또 다시 등장했다. 이번에 등장한 랜섬웨어의 이름은 록키(Locky)로 이를 처음 발견한 건 영국의 보안 전문가인 케빈 뷰몬트(Kevin Beaumont)다. 그에 따르면 록키 랜섬웨어는 1시간의 4000대의 기기를 감염시키는 속도로 퍼져가는 중이라고 한다.



▲ 말 그대로 우후죽순 피어나는 랜섬웨어들

● Carbon Black Enterprise Response

➔ 최신 사이버 위협 및 악성코드 탐지 / 실시간 침해사고 대응 솔루션

Carbon Black은 Carbon Black 전용 에이전트를 통하여 엔드포인트에서 일어나는 모든 프로세스의 행위를 모니터링 및 추적하여 사이버 위협 또는 악성코드를 실시간으로 탐지하고, 신속하게 대응 가능한 솔루션입니다.

탐지

DESCRIPTION	ACTIVITY	ALERT DATA	ACTION
6C0952FD081F50E9F56267F0B16C02AC BIT9 mysinglemessenger.exe (2 more)	about 5 days Unsigned	6C0952FD081F50E9F56267F0B16C02AC Alliance: VirusTotal Score > 3 My Watchlists	51 feed rating report score confidence criticality
98EFC5726B2A6024F59240F14DAC47 BIT9 keygen.exe	about 5 days Unsigned	98EFC5726B2A6024F59240F14DAC47 Alliance: VirusTotal Score > 3 My Watchlists	51 feed rating report score confidence criticality
6ED168BEFBEE60DC3CE3F25CF116C0F0 BIT9 keygen.exe	about 5 days Unsigned	6ED168BEFBEE60DC3CE3F25CF116C0F0 Alliance: VirusTotal Score > 3 My Watchlists	51 feed rating report score confidence criticality
9E97011C50DB3F6B06A4B21BE5197A1E GHOSTLIKE-PC kmservice.exe	about 7 days Unsigned	9E97011C50DB3F6B06A4B21BE5197A1E Alliance: VirusTotal Score > 3 My Watchlists	51 feed rating report score confidence criticality

Current Server License will expire in 17 days

행위

Time	Process Name	Action
2016-01-27 09:25:14.350 GMT	childproc	d)
2016-01-27 09:25:09.128 GMT	modload	Loaded c:\windows\system32\apphelp.dll Signed (863793d15b4026b1a5fdeca873d4d84)
2016-01-27 09:25:09.128 GMT	modload	Loaded c:\program files\samsungscan and fax manager 2\scanmgr2.exe Explicit Distrust (7a5a67207d054a513211ea65f1c6f67d)
2016-01-27 09:25:09.126 GMT	childproc	PID 4328 started c:\program files\samsungscan and fax manager 2\scanmgr2.exe Explicit Distrust (7a5a67207d054a513211ea65f1c6f67d)
2016-01-27 09:25:09.90 GMT	modload	Loaded c:\windows\system32\profapi.dll Signed (c733d233b622b7f9ce5031e4b756ee26)
2016-01-27 09:25:08.984 GMT	modload	Loaded c:\program files\common files\common desktop agent\cdasrvps.dll Explicit Distrust (373f28044c-d61423799d9c60b6f1c15)
2016-01-27 09:25:08.969 GMT	modload	Loaded c:\program files\samsungscan and fax manager 2\cdas2pc\astyle\cstyles Unsigned (469534a090b37247ab2d6237c00a242)
2016-01-27 09:25:08.969 GMT	modload	Loaded c:\windows\system32\psapi.dll Signed (a543ac1f7138376d778d630a35fcb4c)
2016-01-27 09:25:08.968 GMT	modload	Loaded c:\windows\system32\midimap.dll Signed (5a12c364ad144cc0ad0e56dbbc34462)
2016-01-27 09:25:08.967 GMT	modload	Loaded c:\windows\system32\msacm32.dll Signed (85683df1f917e407f6be1a04986bf1c8)
2016-01-27 09:25:08.966 GMT	modload	Loaded c:\windows\system32\msacm32.drv Signed (07393a09c46083508e751b63b03c8301)
2016-01-27 09:25:08.959 GMT	modload	Loaded c:\windows\system32\audioses.dll Signed (50b8937a81360d16a5c772302bd32cfe)
2016-01-27 09:25:08.954 GMT	modload	Loaded c:\windows\system32\devobj.dll Signed (cc4e8bba7800dcab217e014c3291a7)
2016-01-27 09:25:08.953 GMT	modload	Loaded c:\windows\system32\cfmgmg32.dll Signed (3faaa12666e655f51b2fca674f543)
2016-01-27 09:25:08.953 GMT	modload	Loaded c:\windows\system32\setupapi.dll Signed (10fb1650afda6d44588f3c445dc273)

Current Server License will expire in 17 days

● Why you need Carbon Black ?

➔ 최근 보안 동향은 사이버 위협 및 악성코드 사전 차단과 사후 분석/탐지

Carbon Black은 실시간으로 발생하는 사이버 위협과 악성코드를 탐지하고 차단이 가능합니다.



Real Time

다양한 운영체제의 프로세스를 실시간으로 모니터링 및 추적, 기록
(Windows, Linux, Mac 지원)



Containment

악성 프로세스 탐지 시 버튼 하나로 확산 방지를 위해 위협 탐지 호스트 네트워크 차단



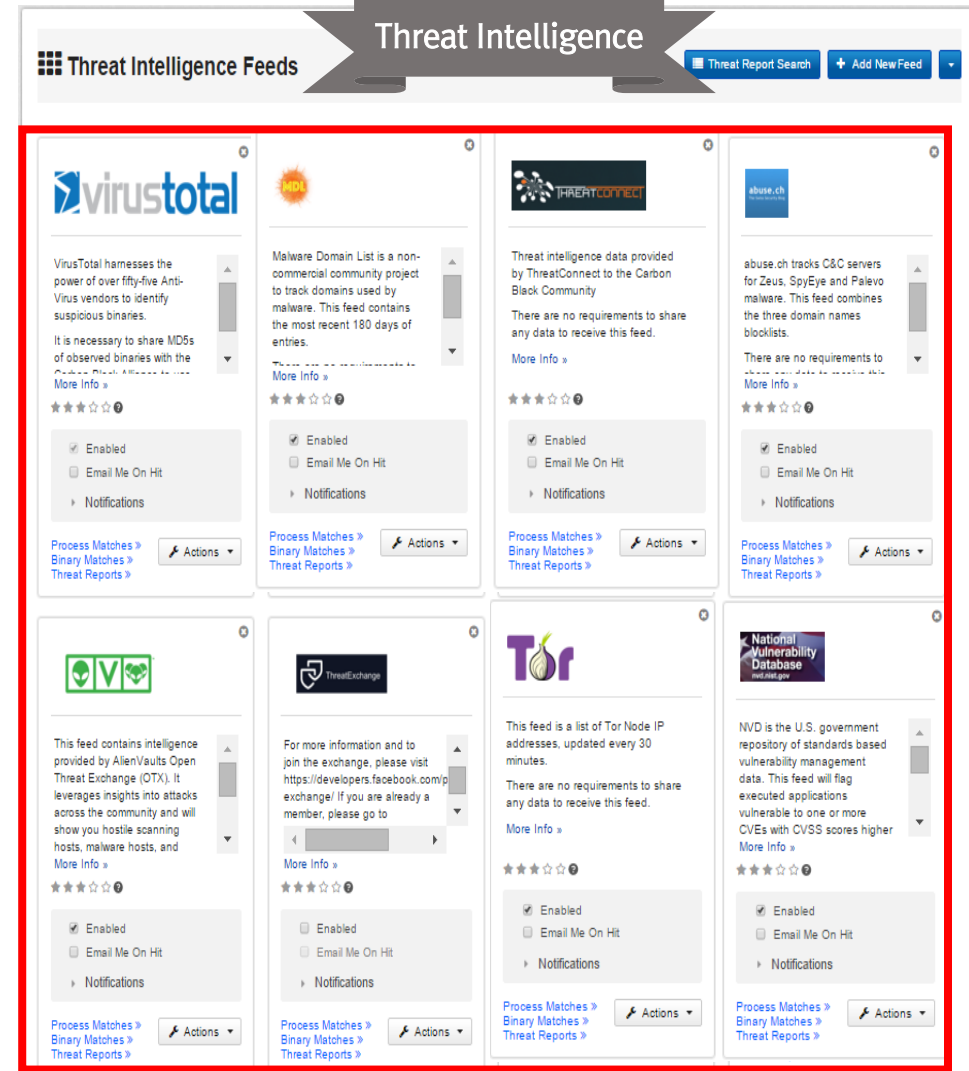
Alliance

다양한 글로벌 보안 업체와 위협 정보 공유 체계를 구축하여 Threat Intelligence 제공

● Threat Intelligence

Carbon Black에서 제공하는 악성코드 및
사이버 위협 정보 공유 연합

Carbon Black은 글로벌 보안업체들과 전략적 파트너십을 체결하여
최신 악성코드 및 위협들을 탐지하고 차단하는데 필요한
Threat Intelligence 서비스를 제공하고 있습니다.



Threat Intelligence Feeds

Threat Report Search + Add New Feed

- VirusTotal**: VirusTotal harnesses the power of over fifty-five Anti-Virus vendors to identify suspicious binaries. It is necessary to share MD5s of observed binaries with the community.
 - Enabled
 - Email Me On Hit
 - Notifications
- MDL**: Malware Domain List is a non-commercial community project to track domains used by malware. This feed contains the most recent 180 days of entries.
 - Enabled
 - Email Me On Hit
 - Notifications
- THREATCONNECT**: Threat intelligence data provided by ThreatConnect to the Carbon Black Community. There are no requirements to share any data to receive this feed.
 - Enabled
 - Email Me On Hit
 - Notifications
- abuse.ch**: abuse.ch tracks C&C servers for Zeus, SpyEye and Palevo malware. This feed combines the three domain names blocklists. There are no requirements to share any data to receive this feed.
 - Enabled
 - Email Me On Hit
 - Notifications
- AlienVaults**: This feed contains intelligence provided by AlienVaults Open Threat Exchange (OTX). It leverages insights into attacks across the community and will show you hostile scanning hosts, malware hosts, and more.
 - Enabled
 - Email Me On Hit
 - Notifications
- ThreatExchange**: For more information and to join the exchange, please visit https://developers.facebook.com/page/threatexchange/. If you are already a member, please go to [link].
 - Enabled
 - Email Me On Hit
 - Notifications
- Tor**: This feed is a list of Tor Node IP addresses, updated every 30 minutes. There are no requirements to share any data to receive this feed.
 - Enabled
 - Email Me On Hit
 - Notifications
- National Vulnerability Database**: NVD is the U.S. government repository of standards based vulnerability management data. This feed will flag executed applications vulnerable to one or more CVEs with CVSS scores higher than [value].
 - Enabled
 - Email Me On Hit
 - Notifications

● 주요 Alliance 구성원

VirusTotal, MDL, THREATCONNECT, abuse.ch,
AlienVaults, ThreatExchange, Tor, NVD 등

Endpoint Monitoring

➔ 지속적으로 모니터링하고 행위를 기록하여 침해사고 분석 시 필요한 아티팩트 정보를 제공합니다

Process Search

The Process Search interface displays search filters for Hostname (19) and Parent Process (5). Below the filters are four charts: Host Type (workstation 100%), Hour of Day, Day of Week, and Process Start Times. A table of related events is shown below, with the following data:

Process Name	Age	Host	Regmod	Filemod	Modload	Netconn	Proc
beats updater.exe	about 8 days	INSEX-PC	regmod 15	filemod 0	modload 0	netconn 3	proc 0
qtask.exe	about 7 days	INSEX-PC	regmod 0	filemod 0	modload 19	netconn 0	proc 0
sublime_text.exe	about 5 days	INSEX-PC	regmod 0	filemod 0	modload 41	netconn 0	proc 0
beats updater.exe	about 7 days	INSEX-PC	regmod 51	filemod 0	modload 51	netconn 4	proc 0
wooribankseclog...	about 6 days	INSEX-PC	regmod 0	filemod 0	modload 42	netconn 0	proc 0

Binary Search

The Binary Search interface displays search filters for Digital Signature (1), Publisher (2), Company Name (200), and Product Name (200). Below the filters are four charts: Sign Time, Host Count, First Seen, and Cb Alliance: VirusTotal Hit Counts. A table of related metadata is shown below, with the following data:

Signature	Company	Seen as	Size
13/1D2953/D51A83F-B090803F-26284E3D	Gretech Corporation	uninstall.exe about 11 days	101.89 KB
B2/C395E2169F-0C06268/369/05A8A69	daumiesetting.exe	about 11 days	57 KB
B1-CB/ZD/F-9F-C1CEB0C0ADEBBF-ACE/F1...	logmanager.exe	about 11 days	230.5 KB
2958B4F-60F-42CF-B446F-C330AC35AE2D...	settime.exe	about 11 days	59.5 KB

● Process Analysis

- 프로세스 트리 및 동작 흐름 확인

프로세스 트리로는 부모 프로세스와 자식 프로세스를 확인 할 수 있으며, 해당 프로세스의 Threat Intelligence와의 Match를 통해 악성 프로세스 정보 확인 가능

● 프로세스 활동 로그

Filemod, Regmod, Modload, netconn, block 등 다양한 기준으로 활동 로그를 분류하여 상세한 프로세스 활동 기록 분석 가능

각 활동 로그 및 프로세스를 위협 정보 공유 연합인 Threat Intelligence의 정보와의 Match를 통해 악성 행위 판별 가능

Process Analysis

chrome.exe on SUNGMIN-PC by Sungmin-PC\Sungmin - running
Command line: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"

Isolate host Go Live Actions

Process Analysis

Process: chrome.exe

PID: 2596

OS Type: windows

Path: c:\program files (x86)\google\chrome\application\chro...

Username: Sungmin-PC\Sungmin

MD5: 23294e80af8a4c6853522d12a391933a1

Start Time: 2012-01-25T15:51:22.557Z

Interface IP: 192.168.0.36

Server Comms IP: 192.168.0.36

chrome.exe: Signed by Google Inc

Alliance Feeds 1 hit(s) in 1 report(s)

On Demand Feeds 4 hit(s) in 2 report(s)

Type	Dir	Invest	Threat	Terms	Feeds	Sig	Pub	File Action	File Type	Domain	IP	Reg Action	Reg Hive	Child Path
Child MD5														
Type	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q
filemod (277)	c:\windows\syswow64	Untagged (488)	Known Good (95)	SRSTrust (0)										
modload (130)	c:\users\sungmin\app		Known Bad (1)	VirusTotal (1)										
childproc (22)	c:\users\sungmin\app			Bit9+CBThreatInte (4)										
regmod (18)	c:\users\sungmin\app			None (481)										
netconn (18)	c:\users\sungmin\app													
processmon (11)	c:\users\sungmin\app													

Time	Type	Description
2018-01-26 19:40:55.146 GMT	filemod	First wrote to c:\users\sungmin\appdata\local\google\chrome\user data\default\network action predictor
2018-01-26 18:53:12.373 GMT	filemod	First wrote to c:\users\sungmin\appdata\local\google\chrome\user data\safe browsing cookies
2018-01-26 18:50:45.392 GMT	filemod	First wrote to c:\users\sungmin\appdata\local\google\chrome\user data\default\favicons

● Easy Hash Ban

➡ Hash 차단 기능으로 동일 Hash값을 가진 프로세스를 모든 호스트에서 실행 차단합니다

Hash Ban

Confirm **Banned Hashes**

Use the checkboxes to remove hashes or click the hash to edit. x

KNOWN HASHES

The following hashes are recognized by Carbon Black:

<input type="checkbox"/> 9166C1276B296BC78FA816CD8448CD32	1 computers have seen this md5 in 1 processes.
---	--

Banning the hashes listed above will prevent them from executing.

Bit9+ CARBON BLACK
5.1.0 Patch 3 Copyright © 2013-2016 Bit9, Inc. All rights reserved.

Manage Hash

View All Banned Previously Banned

Sort By MD5
Asc Desc
Search for MD5

BANNED HASH	NOTES	MOST RECENT BLOCK	TOTAL BLOCKS	HOSTS W/ AT LEAST ONE BLOCK	BAN
e6bb53d93618c372a852e984153b954		N/A	0		<input type="checkbox"/>
c6a0e0bc8c8fc199db1a358c0c64b442	Ban Test for Samsa	N/A	0		<input checked="" type="checkbox"/>
c355d12fa264b22ba44fc67323e8e819	Ban Test for Sungmin	about 7 days	12	SUNGMIN-PC	<input checked="" type="checkbox"/>
a44d3a17d461e01627d0c58f9fe5258		N/A	0		<input type="checkbox"/>
91a4136d5db828478100f5aa2ed8d96b	Ban Test for Samsa	N/A	0		<input checked="" type="checkbox"/>
8e45adb3d38c21e3d0706f796fd7696		about 1 day	1	CARBONBLACKTEST	<input checked="" type="checkbox"/>
880415c853f2172bdc94b402ae4eb395	Ban Test for Samsa	about 8 days	1	INSECSECU-PC	<input checked="" type="checkbox"/>
7467d903ceda2f8693c169eb544216b0	Ban Test for Samsa	N/A	0		<input checked="" type="checkbox"/>

BUT,
사전 차단 어려움

● 화이트리스트(WhiteList) 란?

- ➔ 화이트 리스트(WhiteList)란 리스트에 등록된 프로세스들만 동작하도록 하고 리스트에 없는 프로그램은 실행을 거부하는 방식을 말합니다.



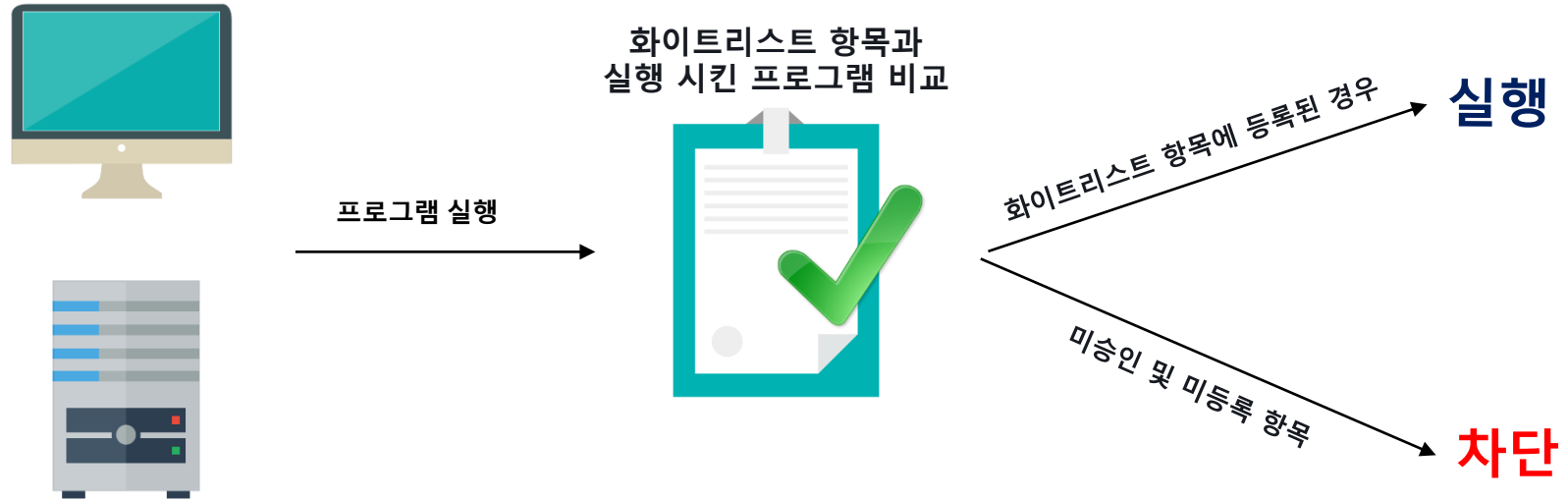
● CarbonBlack Enterprise Protection 소개

- ➔ 사용자의 PC, 서버 등에서 실행되는 응용프로그램 및 운영체제의 파일의 Hash 값을 화이트리스트 목록으로 생성한 뒤, 목록에 없는 파일의 실행을 차단합니다.



● 화이트리스트(WhiteList) 기반의 보안 솔루션

- ➔ 화이트 리스트란 등록 된 프로세스들만 실행을 허용하고 리스트에 없는 프로그램은 실행을 거부하는 방식을 말합니다.



● WhiteList 방식의 필요성

- ➔ 현재 전 세계 유포 된 악성코드 누적 양은 5억 개 정도이며 매달 새로운 악성코드가 약 1000 만개 이상 유포되고 있습니다.

Total Malware



New Malware



● WhiteList VS BlackList

➔ Protection 같은 경우는 화이트리스트 방식, 일반적으로 알고 있는 AV 엔진들이 블랙리스트 방식입니다.

WhiteList 방식과 BlackList 방식의 비교표

WhiteList	구분	BlackList
사전 예방	처리 방식	사후처리
허용된 프로세스만 사용	실행 범위	모든 프로그램 허용
제한적 환경	편의성	범용적 환경
변경 없음	엔진 사이즈	지속적인 증가
낮음	리소스 점유율	높음
높음	보안 수준	낮음
필요없음	업데이트/패치	주기적 필요

● WhiteList 방식의 필요성

➔ WhiteList 방식의 CarbonBlack Enterprise Protection을 사용하면 랜섬웨어를 예방할 수 있습니다.

파일 확장자 '.mp3'로 바꾸는 랜섬웨어 등장... 이중 프로세스로 탐지 우회

[AD1][3/23] 지능형 서비스로봇 기술, 시의 적절한 위협사태와 상용화 세미나

파일 확장자를 '.mp3'로 바꾸는 랜섬웨어가 등장했다. 이 랜섬웨어는 파일 확장자를 '.micro'로 변경하는 테슬라크립트(TeslaCrypt) 변형 랜섬웨어와 유사한 행위기반 탐지 일부 기능을 회피한다. 둘 들어 랜섬웨어 탐지 기술의 진화가 요구된다.



<파일 확장자 '.mp3'로 바꾸는 랜섬웨어가 등장했다.>[게티이미지뱅크]

보안 업계에 따르면 확장자 mp3로 바꾸는 랜섬웨어는 실 연초 직후인 지난 11일부터 국내 피해사례가 보고됐다. 온라인 커뮤니케이션 데이터 지적인 서비스 등에도 관련 문의가 올라왔다.

HOME > News > 컴퓨터/인터넷 보안 > 일반

애플 맥 OS에서 최초로 랜섬웨어 피해사례 발견

유은정 | 승인 2016.03.08 | 수정 2016.03.09 10:20



또 새 랜섬웨어! 단일 시스템뿐 아니라 네트워크도 침입

실력남파 | 2016-02-19 11:55

공유

최근 랜섬웨어 트랜스락(TransLocker)은 공격자들을 후원하는 랜섬웨어 해커들에게

[보안뉴스 특가] 랜섬웨어 공격이 더욱 심각해지고 있다. 새로운 랜섬웨어가 또 등장했다. 이번에 등장한 랜섬웨어는 기존 랜섬웨어와 다른 점을 처음 발견한 건 영국의 보안 업체인 케빈 뷰먼드(Kevin Beaumont)다. 랜섬웨어는 1시간의 잠복기를 거친 뒤 공격을 감행한다. 랜섬웨어는 공격을 감행하는 1시간의 잠복기를 거친 뒤 공격을 감행한다.

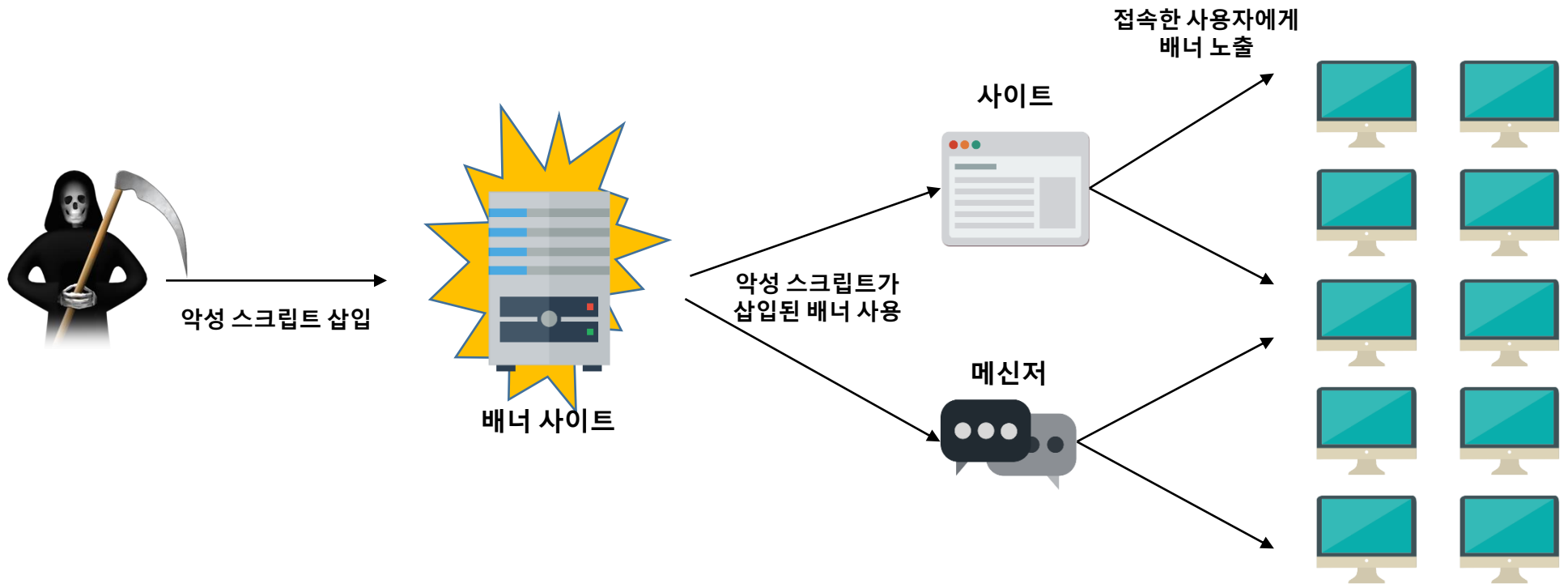


▲ 알 그레로 우후죽순 피어난 랜섬웨어

사전에 랜섬웨어 실행을 차단함으로써 감염으로부터 예방할 수 있습니다.

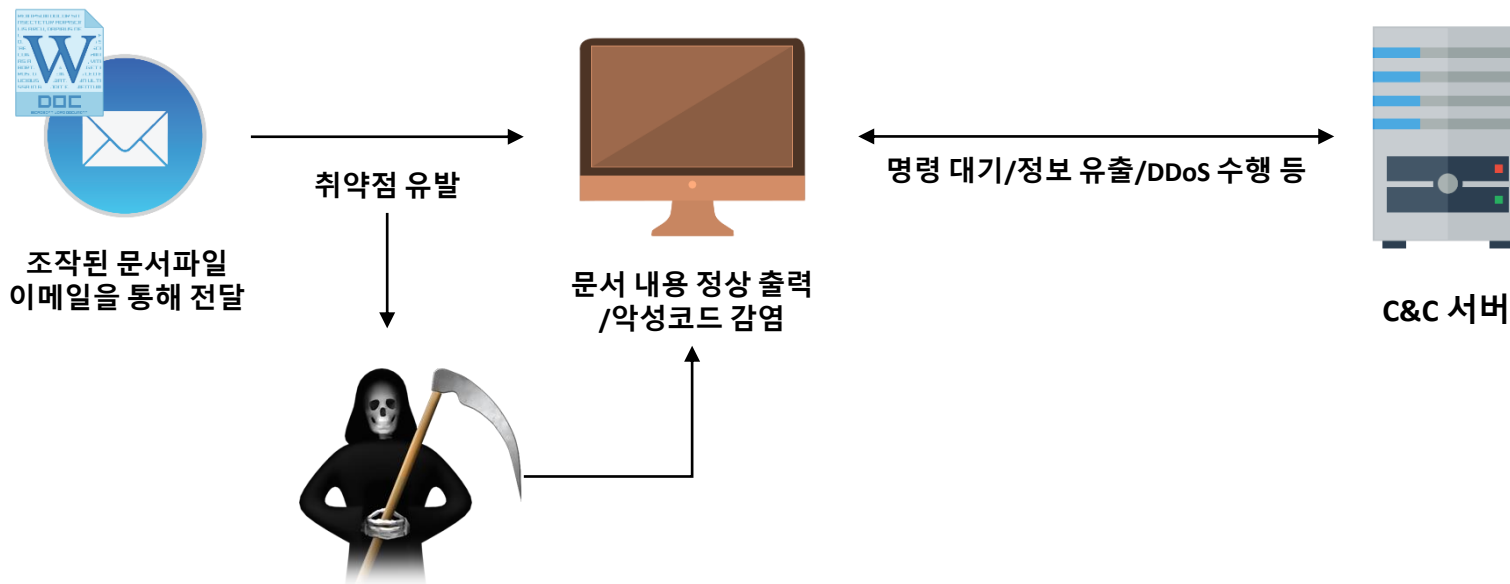
● WhiteList 방식의 필요성

➔ 웹 사이트를 통한 악성코드 경유 및 유포 감염



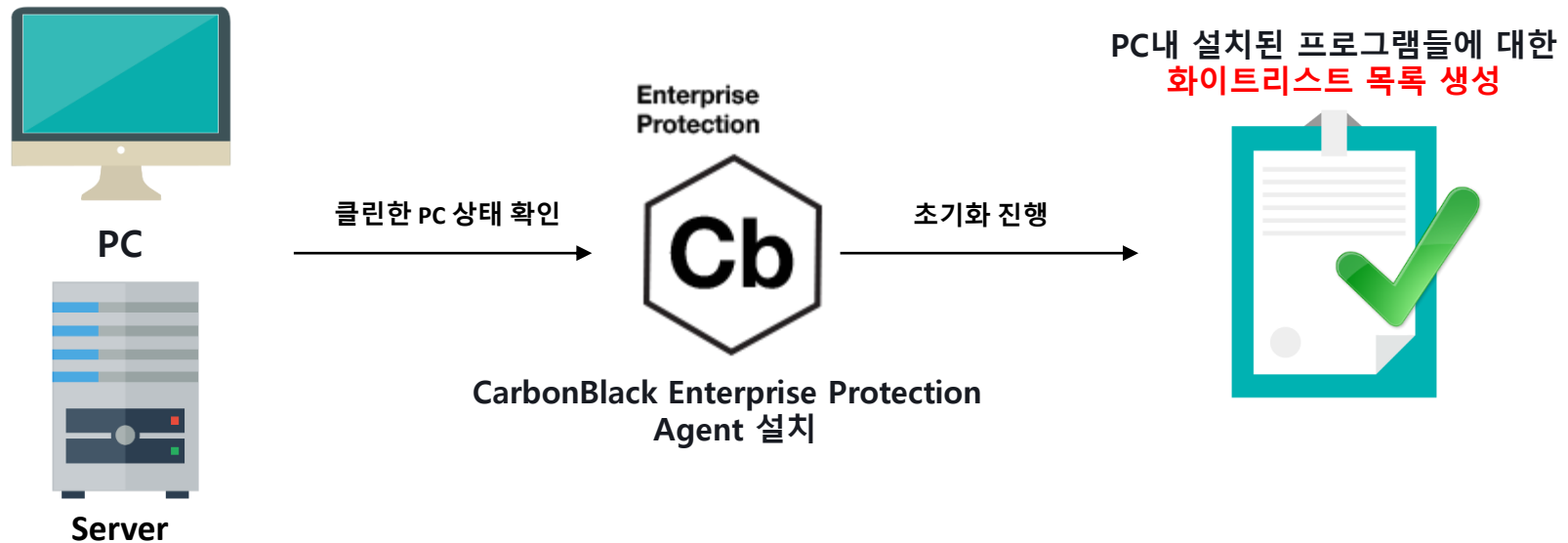
● WhiteList 방식의 필요성

➔ 이메일 전파를 통한 악성코드 감염



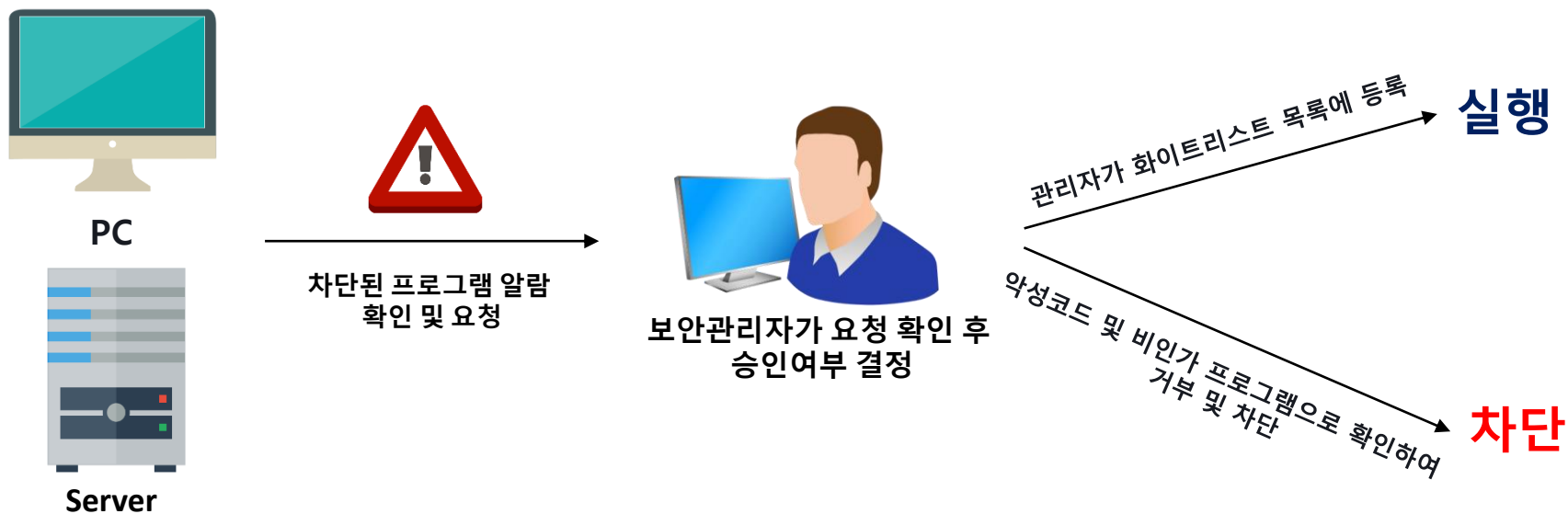
● CarbonBlack Enterprise Protection 동작방식

- ➔ 사용자 PC를 신뢰할 수 있는 상태로 만든 뒤, Protection Agent를 설치합니다.
이후 초기화 과정을 통해 설치 된 프로그램 및 정책을 포함하여 화이트리스트로 생성합니다.

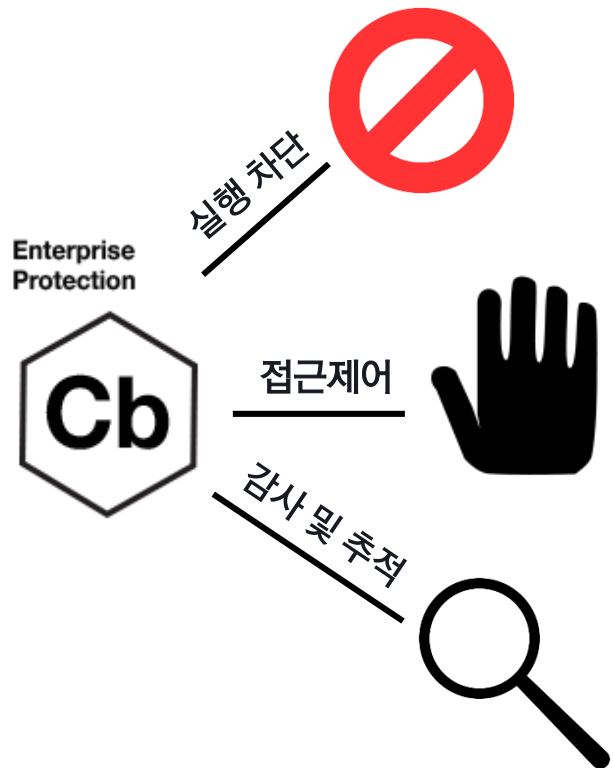


● CarbonBlack Enterprise Protection 동작방식

- ➔ Protection에 의해 차단된 항목에 대해서 관리자에게 요청하게 되면 요청 내역이 관리자에게 전달이 되고 관리자는 해당 내역을 확인하여 승인/차단을 결정할 수 있습니다.



● CarbonBlack Enterprise Protection 동작방식



회사 정책에 따른 **승인된 소프트웨어만 허용 함**으로서
최신 APT 공격, 스피어 피싱, Zero-day 공격을 차단

레지스트리, 프로세스, 시스템 파일 등에 대한 불법적인 **접근을 막기 위한 실시간 모니터링 및 제어, 통제**

Parity Knowledge 서비스를 이용 **소프트웨어의 위험성을 식별**하
고, 개인저장 장치에 **내부 데이터 접근 내역 추적 가능**

● CarbonBlack Enterprise Protection 의 특징


1. 화이트리스트 방식으로 운영됩니다.
2. 등록된 자산들의 모든 행위에 대해서 모니터링이 가능합니다.
3. 정책을 레벨을 설정하고, 설정된 정책을 그룹별, 개인별로 구분하여 적용할 수 있습니다.
4. 인터넷이 단절된 상태에서도 오프라인 정책을 적용할 수 있습니다
5. 엔드포인트에서 설치 된 에이전트를 강제로 삭제할 수 없습니다.
6. 이동형 저장매체에 대해서 접근 제한 및 차단할 수 있습니다.
7. 뛰어난 확장성을 바탕으로 타 AV 엔진들과 연동하여 사용할 수 있습니다.
8. 정책을 설정할 때 로컬, 글로벌 단위로 구분하여 적용할 수 있습니다.
9. 적은 리소스 소요로 에이전트로 설치된 자산들이 운영 되는데 있어서 영향이 전혀 없습니다.

● 다양한 보안 솔루션 연동 및 확장 가능한 제품























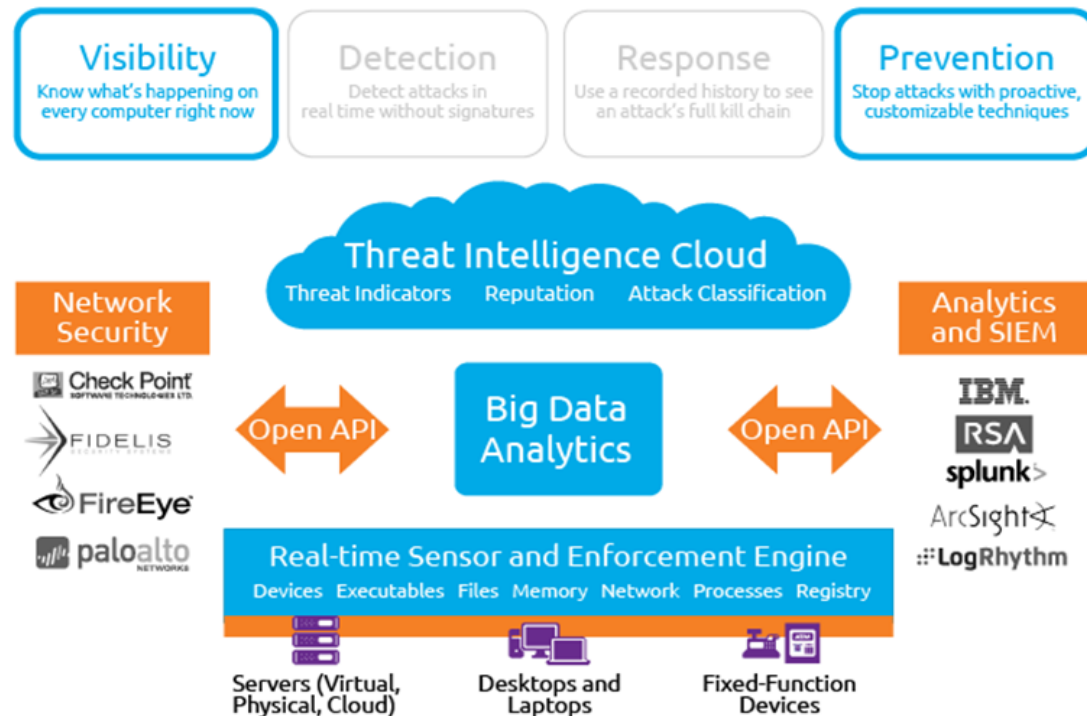
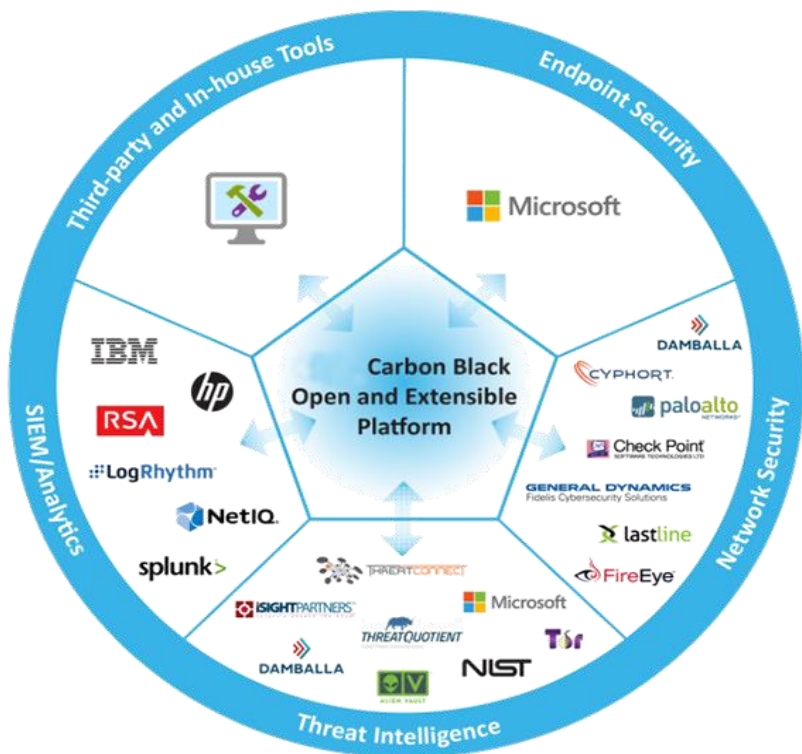






● 다양한 보안 솔루션 연동 및 확장 가능한 제품

- ➔ Carbon Black은 아래와 같은 솔루션(Network Security, Endpoint Security, SIEM / Analytics, Threat Intelligence, Third-party and In-house Tool)과 연동을 할 수 있습니다.



27

CARBON
BLACK
ARM YOUR ENDPOINTS

Reseller



INSEC Security

Solution Business Department, INSEC Security
[Education & Products Sales]

www.bit9korea.co.kr / www.totalsecurity.com

서울시 금천구 가산디지털1로 128 STX-V-TOWER 5층 505호

Tel : + 82-2-863-5687 | Fax : + 82-2-862-5687 |

Contact

Sales Director, INSEC Security, 신영섭 이사 | kidari@insec.co.kr | Tel : 010-4145-6800

Technical Engineer, INSEC Security, 채준혁 대리 | david@insec.co.kr | Tel : 010-2031-4456