

A blue-tinted background image showing a business handshake over a laptop. A white square frame is centered over the handshake. The text '보안이벤트 추적·대응 시스템' is overlaid in white.

보안이벤트 추적·대응 시스템

CONTENTS

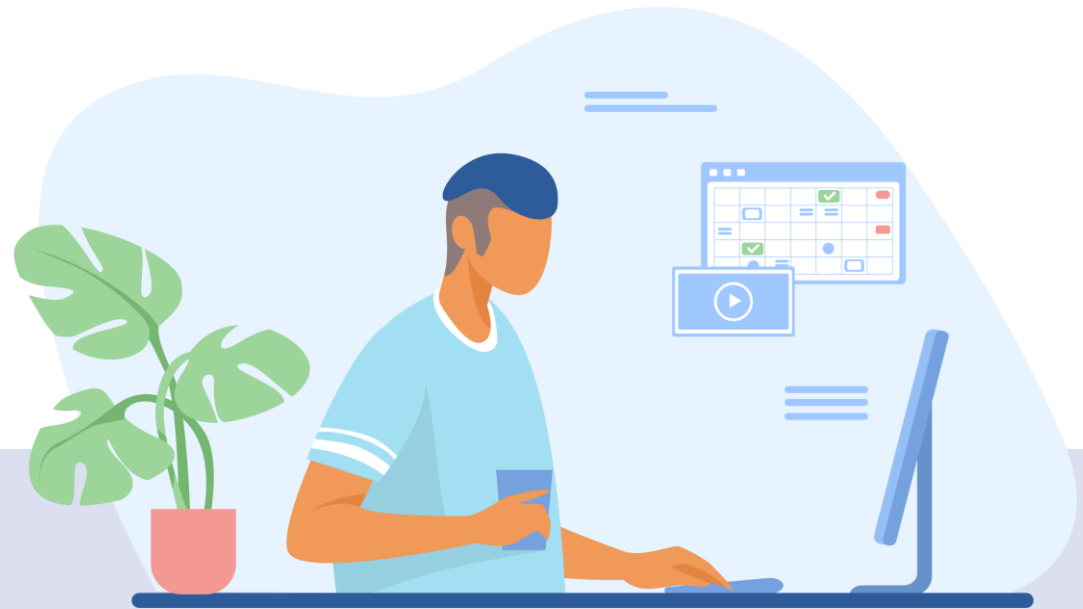
- 01 시스템 구성
- 02 항목별 탐지 방식
- 03 멀웨어 탐지 결과
- 04 도입효과



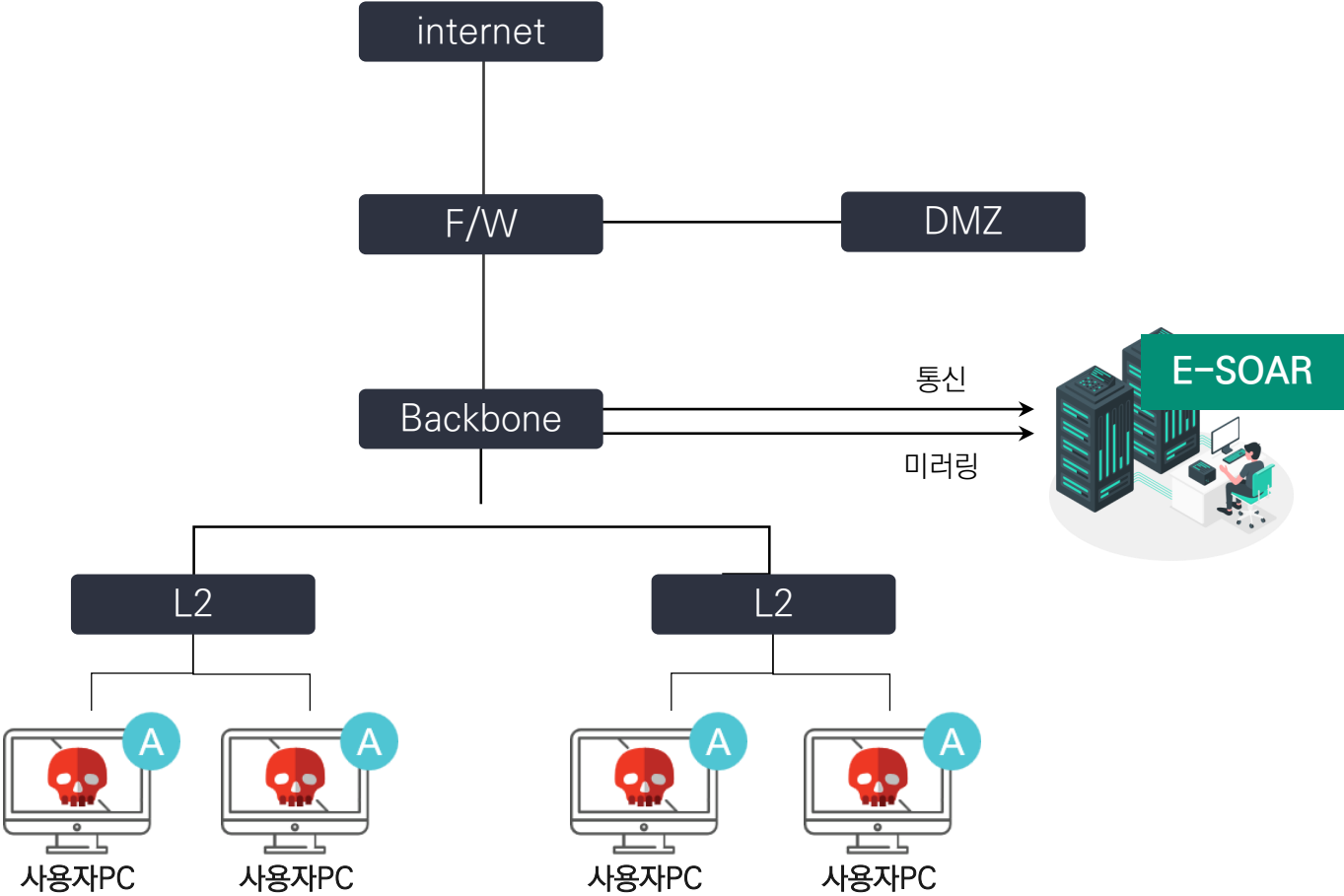
시스템 구성

개요

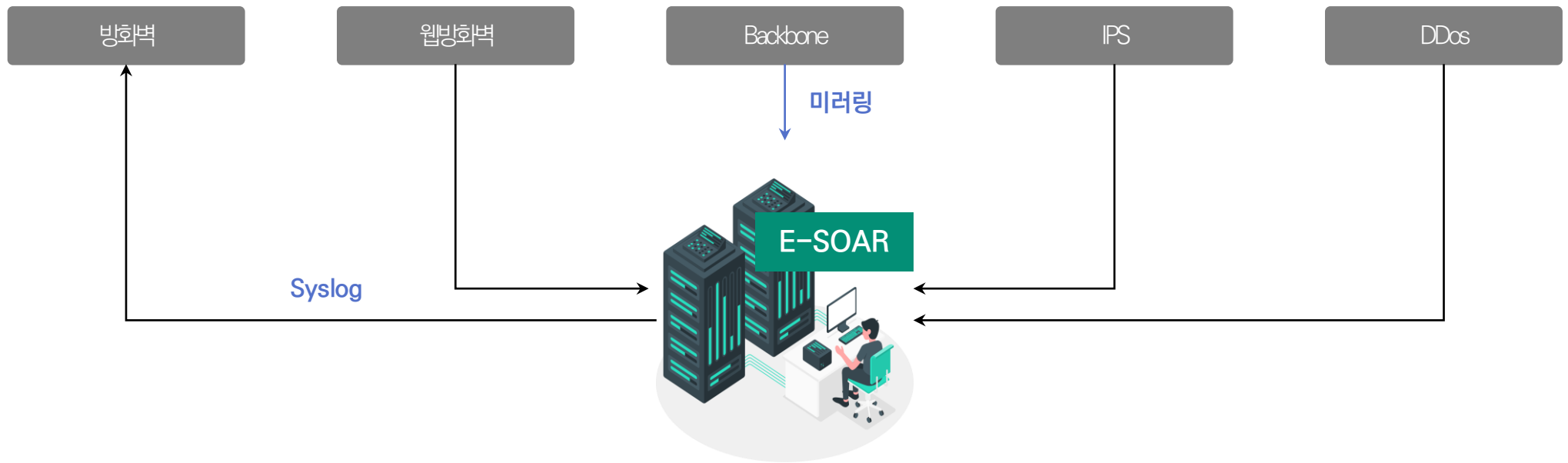
각종 보안장비, 미러링, 통합보안관리솔루션에서 탐지되는 이벤트를 보안이벤트 추적·대응시스템과 연계하여 엔드포인트(사용자PC 등)의 비정상 행위를 실시간 탐지/추적/분석 후 즉시 대응하고 증거 자료를 보관함으로써 조직의 보안 수준을 이전보다 높여주는 시스템



설치 구성도



보안장비 및 네트워크장비 연동 현황



연동별 감시항목

백본 미러링을 통한 이벤트 수집

- ✓ Black IP 접근 현황 감지
- ✓ 내부 사용자 중요서버 접근 현황 감지

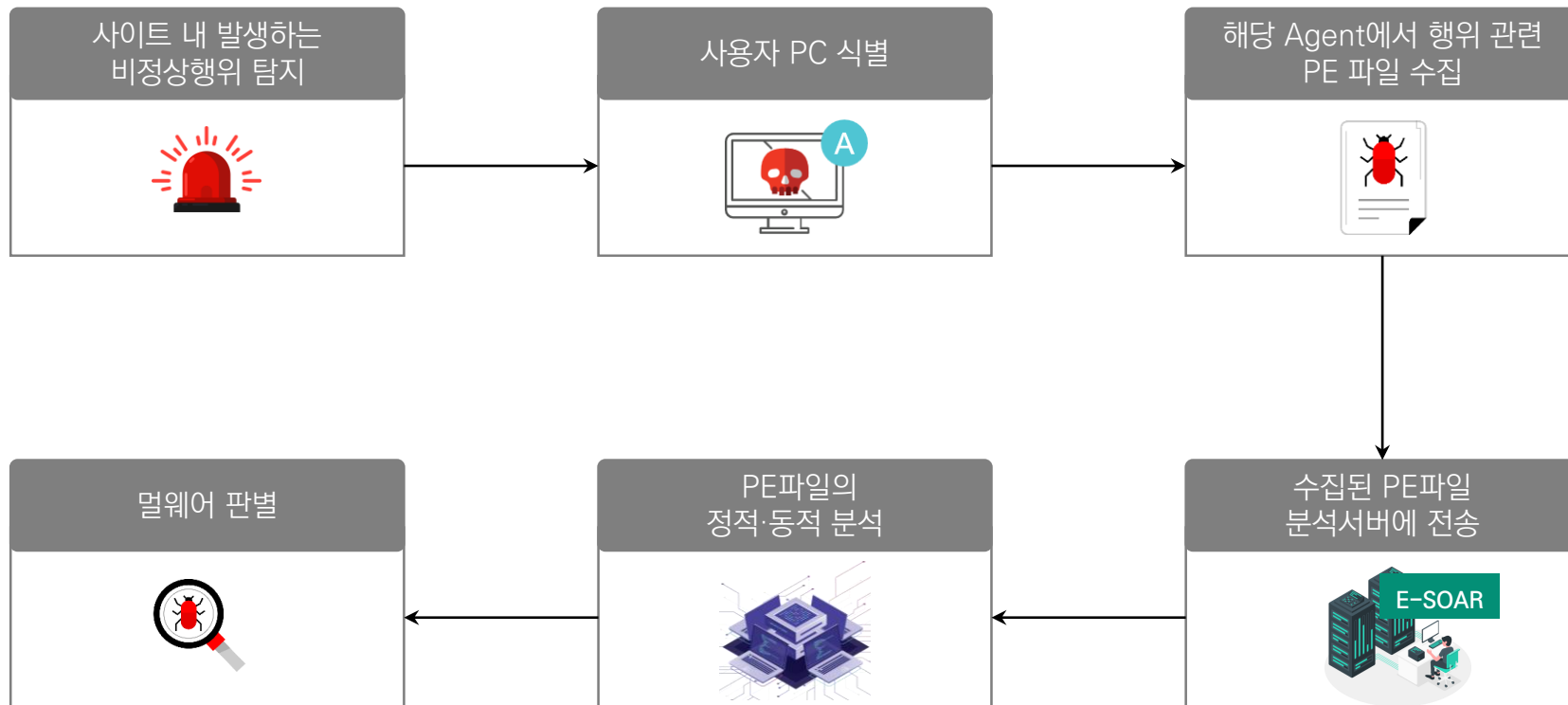
SysLog 전송을 통한 이벤트 수집

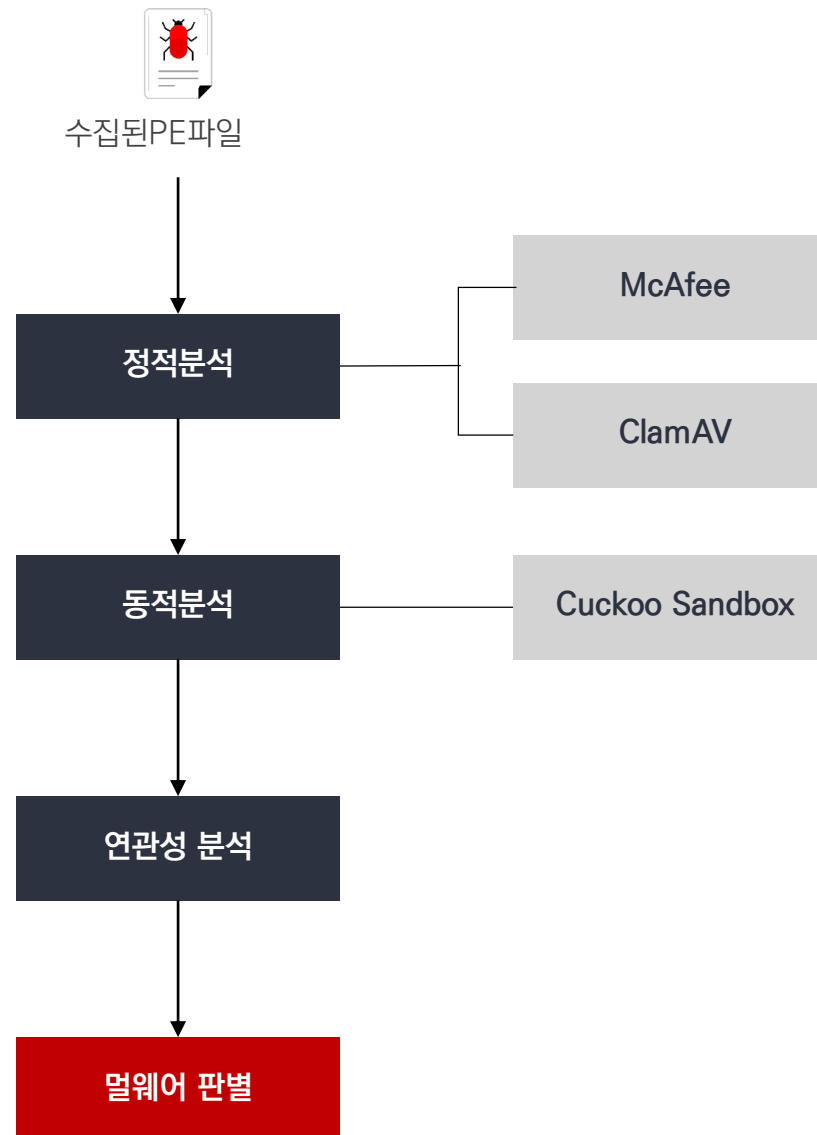
- ✓ IPS 차단/탐지 로그 감시
- ✓ WAF 차단/탐지 로그 감시
- ✓ DDos 차단/탐지 로그 감시
- ✓ 사용자 PC의 방화벽 차단 로그 현황 감시

Agent 모니터링을 통한 이벤트 탐지

- ✓ 사용자 PC에서 접근성이 용이한 주변 IT기기와 장비들의 접근 시도 감시
- ✓ 외부에서의 접근 시도 감시

보안이벤트 추적·대응시스템 흐름도

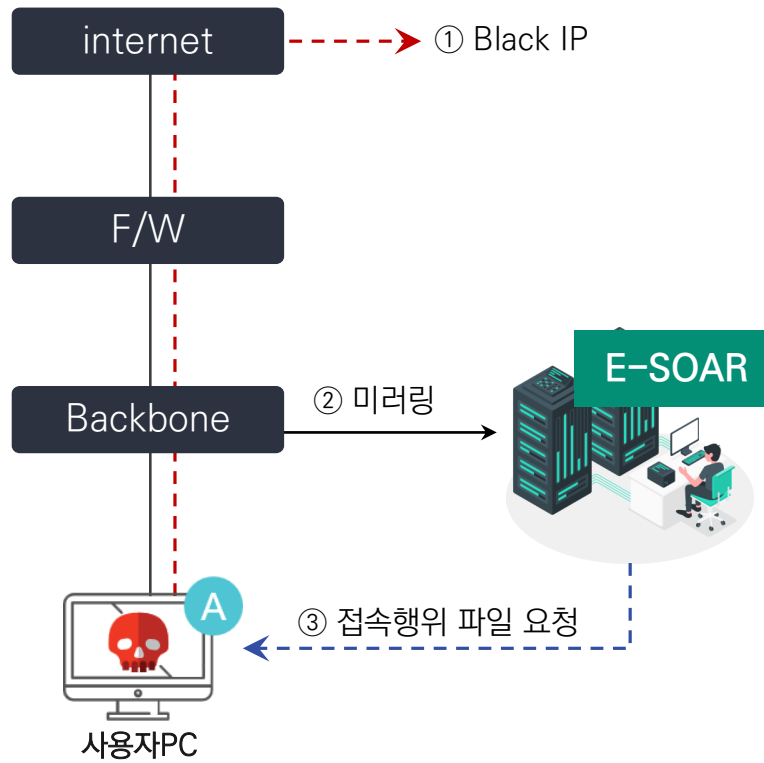














항목별 탐지 방식

BlackIP 탐지



BlackIP 탐지 현황



사용자로그정보모니터링분석결과정책설정시스템관리

yyyu

Black IP 탐지

모니터링 > Black IP 탐지

PDF출력

엑셀출력

경신주기 정지 새로고침

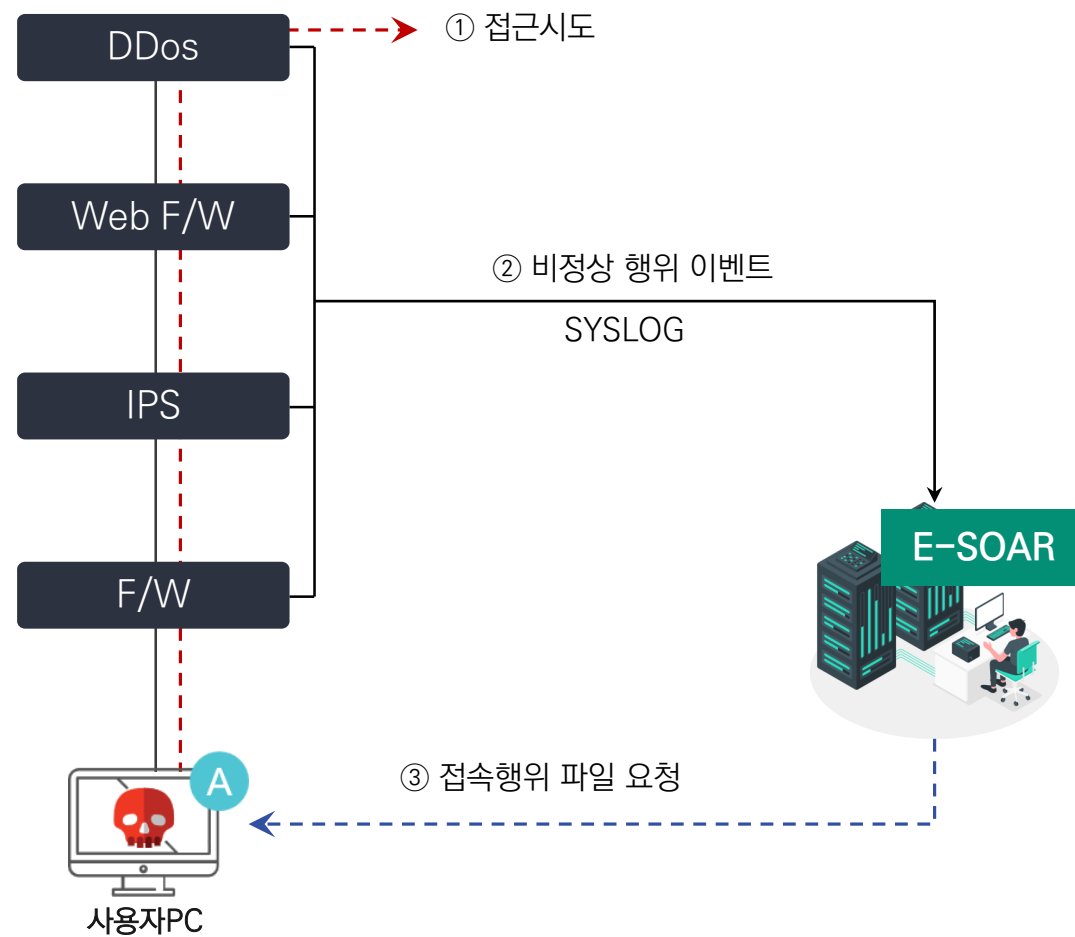
2021-07-12 ~ 2021-07-12 통합검색

검색









Total 48,178

NO	탐지번호	탐지일자	사용자 정보	접근정보	프로세스명	사용비율	서명	다운로드	분석결과
1	20227378	2021-07-12 14:47:57			chrome.exe	55.03%	○	⚠	
2	20227358	2021-07-12 14:47:56			msedge.exe	11.18%	○	⚠	
3	20227365	2021-07-12 14:47:56			chrome.exe	55.03%	○	⬇	
4	20227354	2021-07-12 14:47:55			msedge.exe	11.18%	○	⬇	1.2 / 6.6
5	20227342	2021-07-12 14:47:53			msedge.exe	11.18%	○	⚠	
6	20227340	2021-07-12 14:47:53			msedge.exe	11.18%	○	⬇	1.2 / 6.6
7	20227330	2021-07-12 14:47:52			msedge.exe	11.18%	○	⬇	1.2 / 6.6
8	20227320	2021-07-12 14:47:51			smartscreen.exe	79.02%	✖	⬇	1.4 / 6.6
9	20227318	2021-07-12 14:47:51			svchost.exe	89.57%	○	⬇	1.2 / 6.6
10	20227315	2021-07-12 14:47:50			chrome.exe	55.03%	○	⬇	6.2 / 7.0
11	20227304	2021-07-12 14:47:48			svchost.exe	89.57%	○	⬇	1.2 / 6.6
12	20227286	2021-07-12 14:47:47			kakaotalk.exe	26.57%	○	⬇	0 / 14.0
13	20227282	2021-07-12 14:47:46			powerpnt.exe	22.86%	○	⬇	0 / 6.6
14	20227280	2021-07-12 14:47:46			msedge.exe	11.18%	○	⬇	1.2 / 6.6
15	20227279	2021-07-12 14:47:45			msedge.exe	11.18%	○	⬇	1.2 / 6.6
16	20227273	2021-07-12 14:47:45			chrome.exe	55.03%	○	⬇	6.2 / 7.0
17	20227275	2021-07-12 14:47:45			svchost.exe	89.57%	○	⬇	1.2 / 6.6
18	20227269	2021-07-12 14:47:44			chrome.exe	55.03%	○	⬇	6.2 / 7.0
19	20227259	2021-07-12 14:47:42			remoting_host.exe	3.27%	○	⬇	5.8 / 7.4
20	20227248	2021-07-12 14:47:41			chrome.exe	55.03%	○	⬇	6.2 / 7.0
21	20227241	2021-07-12 14:47:40			msedge.exe	11.18%	○	⬇	1.2 / 6.6

프로세스동계



IPS 탐지 현황






사용자로그정보모니터링분석결과정책설정시스템관리

yyu

IPS 탐지

모니터링 > IPS 탐지

 PDF출력  엑셀출력

☒ 분류 














☒ DDoS ☒ IPS ☒ WebFW ☒ FW

경신주기: 정지 새로고침

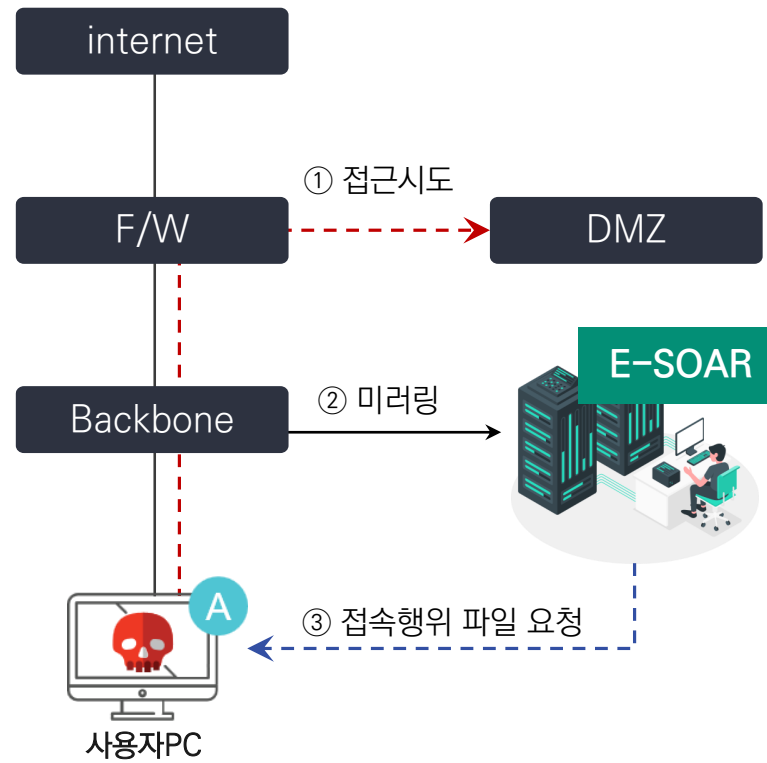
2021-07-12 ~ 2021-07-12 통합검색

검색


Total 948

NO	탐지번호	탐지일자	IPS장비 IP	사용자정보	검근정보	탐지명	프로세스명	사용비율	서명	다운로드	분석결과
1	34959679	2021-07-12 15:37:32	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
2	34959428	2021-07-12 15:36:12	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
3	34959342	2021-07-12 15:35:41	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
4	34959235	2021-07-12 15:35:07	203.250.2.17			(0075)HTTPD Overflow	msedge.exe	11.18%	○		1.2 / 6.6
5	34959223	2021-07-12 15:35:02	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
6	34959056	2021-07-12 15:34:13	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
7	34959025	2021-07-12 15:34:02	203.250.2.17			(0075)HTTPD Overflow	chrome.exe	55.03%	○		6.2 / 7.0
8	34959024	2021-07-12 15:34:02	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
9	34958910	2021-07-12 15:33:35	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
10	34958858	2021-07-12 15:33:24	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
11	34958824	2021-07-12 15:33:06	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
12	34958778	2021-07-12 15:32:58	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6
13	34958748	2021-07-12 15:32:49	203.250.2.17			(0104)HTTP Login Brute Force	asdsvc.exe	61.06%	○		0.8 / 6.6

프로세스 상세



중요서버 탐지 현황



사용자로그정보모니터링분석결과정책설정시스템관리

YJW

중요서버 탐지




모니터링 > 중요서버 탐지

PDF출력엑셀출력


경신주기탐지새로고침

2021-01-012021-07-12통합검색

Total 3

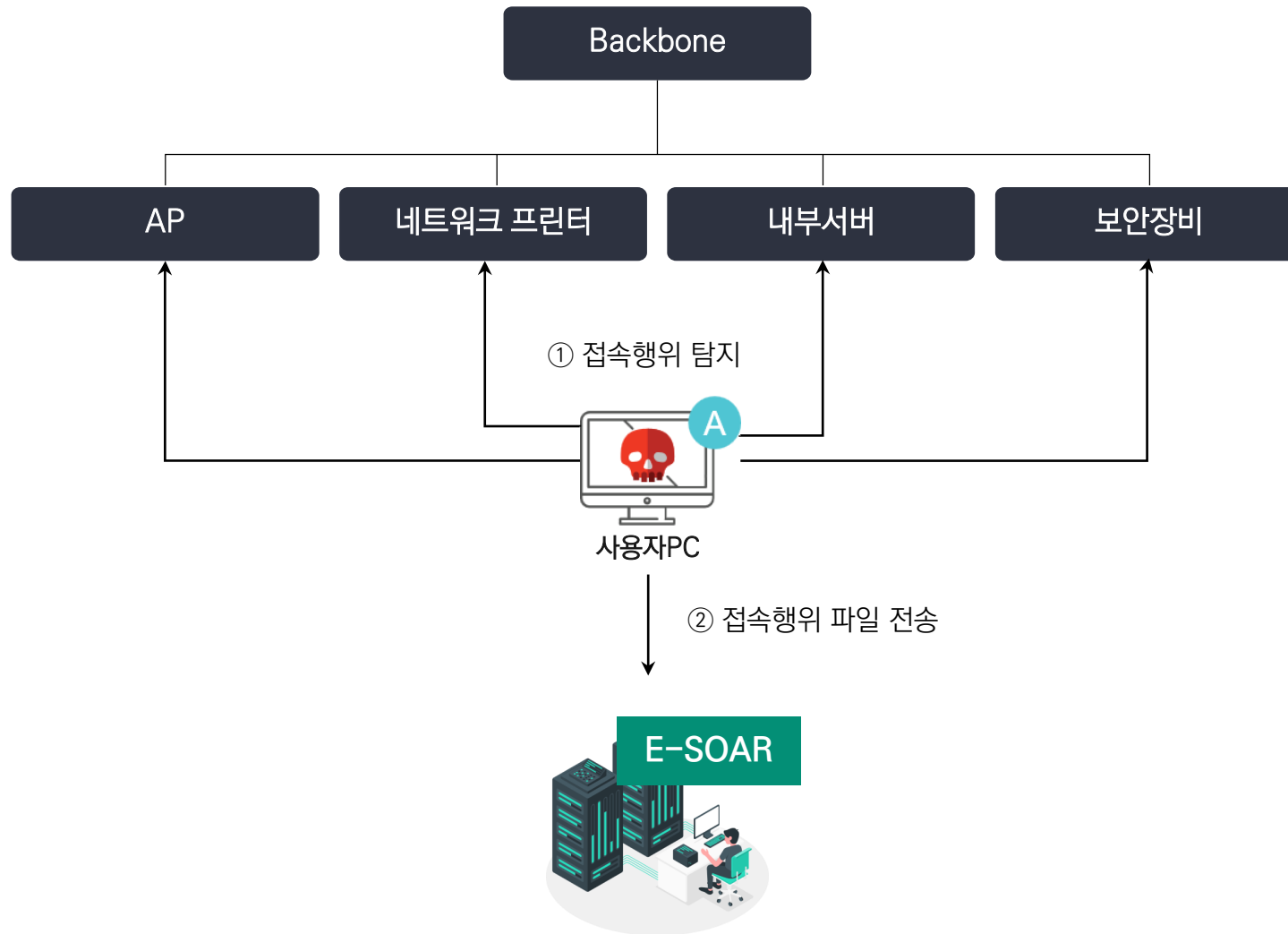
NO	탐지번호	탐지일자	사용자정보	접근정보	프로세스명	사용비율	서명	다운로드	분석결과
1	27	2021-02-03 14:42:20			editplus.exe	0.31%	○		0 / 9.2
2	20	2021-02-03 14:37:20			editplus.exe	0.31%	○		0 / 9.2
3	4	2021-02-03 14:21:03			putty.exe	0.06%	✕		

1


0 / 9.2

프로세스동계

네트워크 장비 탐지



네트워크 장비 탐지 현황


사용자
로그정보
모니터링
분석결과
정책설정
시스템
관리

yyyu

네트워크장비 탐지

홈 > 모니터링 > 네트워크장비 탐지

PDF출력 엑셀출력

갱신주기 정지 새로고침

2021-07-12 ~ 2021-07-12

통합검색

검색

Total 15

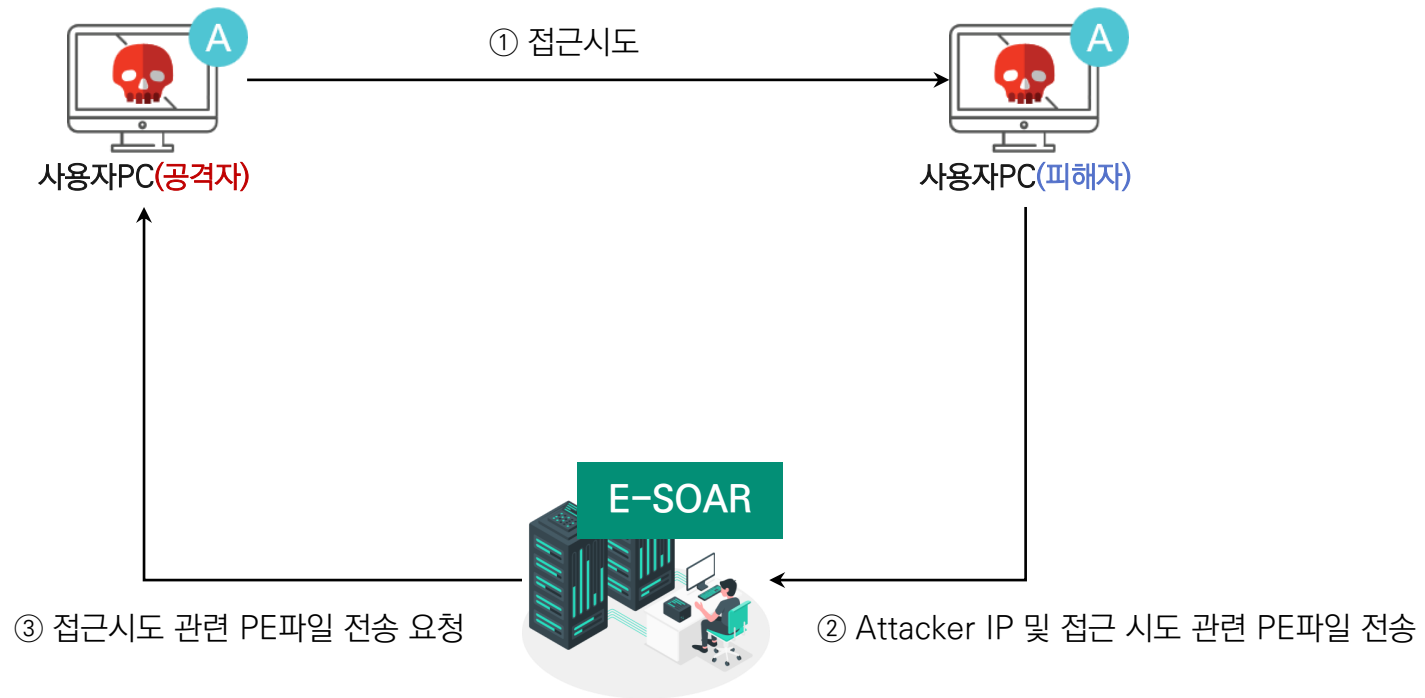
NO	탐지번호	탐지일자	사용자정보	접근정보	프로세스명	사용비율	서명	다운로드	분석결과
1	2368	2021-07-12 15:09:33			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
2	2367	2021-07-12 15:02:33			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
3	2366	2021-07-12 14:40:17			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
4	2364	2021-07-12 14:38:12			javaw.exe	0.44%	○	다운로드	0.4 / 6.6
5	2365	2021-07-12 14:34:35			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
6	2363	2021-07-12 13:37:18			javaw.exe	0.44%	○	다운로드	0.4 / 6.6
7	2362	2021-07-12 13:19:08			javaw.exe	0.44%	○	다운로드	0.4 / 6.6
8	2361	2021-07-12 11:35:46			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
9	2360	2021-07-12 11:07:35			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
10	2359	2021-07-12 11:00:06			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
11	2357	2021-07-12 10:37:49			javaw.exe	0.44%	○	다운로드	0.4 / 6.6
12	2358	2021-07-12 10:30:56			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
13	2356	2021-07-12 10:16:16			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
14	2355	2021-07-12 08:42:53			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6
15	2354	2021-07-12 07:46:45			kript.transfer.exe	0.06%	✖	다운로드	5.2 / 6.6

1

목록수 30개

프로세스통계

원격접근 탐지



원격접근 탐지 현황

사용자로그정보모니터링분석결과정책설정시스템관리

YYMM

원격접근 탐지

모니터링 > 원격접근 탐지

PDF출력엑셀출력

경신주기

정지

새로고침

2021-07-12

2021-07-12

통합검색

검색

Total 7,980

NO	탐지번호	탐지일자	구분	사용자정보	접근정보	프로세스명	사용비율	서명	다운로드	분석결과
1	3084060	2021-07-12 15:34:42	출발지 목적지	- [redacted]	- [redacted]	- parsecd.exe	- 0.19%	 ○	- ⚠	- -
2	3084061	2021-07-12 15:34:42	출발지 목적지	- [redacted]	- [redacted]	- hasplms.exe	- 0.06%	 ✖	- ⚠	- -
3	3084058	2021-07-12 15:34:33	출발지 목적지	- [redacted]	- [redacted]	- hasplms.exe	- 0.57%	 ✖	- ⬇	- 5.0 / 6.6
4	3084057	2021-07-12 15:34:29	출발지 목적지	- [redacted]	- [redacted]	- spoolsv.exe	- 20.67%	 ✖	- ⚠	- -
5	3084056	2021-07-12 15:34:28	출발지 목적지	- [redacted]	- [redacted]	- spoolsv.exe	- 20.67%	 ✖	- ⬇	- 1.0 / 6.6
6	3084055	2021-07-12 15:34:26	출발지 목적지	- [redacted]	- [redacted]	- spoolsv.exe	- 20.67%	 ✖	- ⬇	- 1.0 / 6.6
7	3084054	2021-07-12 15:34:25	출발지 목적지	- [redacted]	- [redacted]	- spoolsv.exe	- 20.67%	 ✖	- ⬇	- 1.0 / 6.6
8	3084053	2021-07-12 15:34:24	출발지 목적지	- [redacted]	- [redacted]	- spoolsv.exe	- 20.67%	 ✖	- ⬇	- 1.0 / 6.6


프로세스통계


멀웨어 분석센터 연동


- ☑ 멀웨어로 의심되는 파일의 Hash값을 아이티스테이션 분석센터와 연동하여 멀웨어 자동 판별


← → ↺ 203.250.2.14/manageDefinitionFile.do


Nutanix Web Cons...





 사용자

 로그정보

 모니터링

 분석결과

 정책설정

 시스템

정의 파일 관리

🏠 > 관리 > 정의 파일 관리

☐ McAfee

☐ BlackIP

☒ 경고파일 데이터

다운로드 받은 경고파일 건수	21173건
업데이트 건수	0건
최근 다운로드 일자	2021-07-06 22:50:01.0



멀웨어 탐지 결과

멀웨어 탐지 현황

📌 멀웨어 탐지건수: 총 26건 / 실행파일: 24건 / DLL파일:5건

No	탐지항목	파일명	분석결과	분석일자
1	Black IP	ww31.exe	he Generic trojan.pr trojan !!!	2021-07-12 13:50:05
2	Black IP	xteat12.exe	VirusToTal	2021-07-11 18:55:40
3	Black IP	54ab.exe	VirusToTal	2021-07-11 17:42:20
4	IPS	alzip1130.exe	VirusToTal	2021-07-09 20:33:06
5	Black IP	filterdll.exe	he RDN/Generic Dropper trojan !!! System	2021-07-09 15:33:06
6	Black IP	vguuu.exe	he GenericRXOZ-GX!6020914469ED trojan !!!	2021-07-09 15:32:21
7	Black IP	askinstall50.exe	he GenericRXLT-RQ!F38F444C7F07 trojan !!!	2021-07-09 15:30:47
8	Black IP	kdfinj.dll	VirusToTal	2021-07-02 21:35:14
9	Black IP	ksbizapp.dll	VirusToTal	2021-06-12 22:45:15
10	원격접근	utorrent.exe	VirusToTal	2021-06-11 20:49:14
11	Black IP	setup.exe	VirusToTal	2021-06-11 02:46:50
12	Black IP	chrome.exe	VirusToTal	2021-06-10 22:55:00
13	IPS	mopinstaller.exe	VirusToTal	2021-06-10 19:25:38
14	IPS	restoromain.exe	VirusToTal	2021-06-10 16:36:04
15	IPS	engine.dll	VirusToTal	2021-06-10 16:17:20
16	Black IP	sch.exe	VirusToTal	2021-06-02 23:51:13
17	Black IP	ml20201223.exe	he GenericRXMW-JZ!D54ADE674CB0 trojan !!!	2021-03-31 14:51:36
18	Black IP	haleng.exe	he GenericRXMC-KT!F066CF5648DE trojan !!!	2021-03-31 14:41:44
19	Black IP	helper.exe	VirusToTal	2021-03-25 20:49:12
20	IPS	rei_axcontrol.dll	VirusToTal	2021-03-25 15:34:33
21	Black IP	starpdf.exe	VirusToTal	2021-03-23 20:22:11
22	Black IP	utorrent.exe	PUA:Win32/uTorrent	2021-03-18 16:01:18
23	Black IP	utorrentie.exe	PUA:Win32/uTorrent	2021-03-18 16:00:54
24	원격접근	utorrent.exe	VirusToTal	2021-03-08 19:46:10
25	원격접근	winrmsrv.exe	he RDN/Generic PUP.z trojan !!!	2021-03-04 18:41:19
26	Black IP	winlogui.exe	he RDN/Generic.dx trojan !!!	2021-03-04 17:16:15
27	네트워크 탐지	pbwin32.Win32.Agent	Trojan.Win32.Agent	2021-08-17 18:06:14
28	Black IP	xteat12.exe	Trojan.Agent/Gen-Zusy	2021-07-11 18:55:40
29	Black IP	54ab.exe	Trojan.Ransom.Stop	2021-07-11 17:42:20

멀웨어 탐지 사용자 현황

203.250.2.14/reportVirus.do?menuID=40

Nutanix Web Cons...

사용자
 로그정보
 모니터링
 정책설정
 시스템
 관리

admin

멀웨어 현황

로그정보 > 멀웨어 현황

통합검색

검색

Total 4

NO	탐지항목	파일명	체크섬	분석결과	다운로드	보고서	사용비율	조치여부	분석일자	조치일자
1	BlackIP	utorrent.exe	0E2646AD4C5C9DC3ED2D...	PUA:Win32/uTorrent			0.12%		2021-03-18 16:01:18	-
2	BlackIP	utorrentie.exe	71677BE971BACB2BCBAB...	PUA:Win32/uTorrent			0.12%		2021-03-18 16:00:54	-
3	윌격접근	winrmsrv.exe	5B85CEB558BADED794E...	he RDN/Generic PUP.z trojan !!!			0.06%		2021-03-04 18:41:19	-
4	BlackIP	winlogui.exe	91BF82ED5C32979368E...	he RDN/Generic.dx trojan !!!			0.06%		2021-03-04 17:16:15	-

① Click

사용비율

0.12%

0.12%

② 팝업 생성

프로세스 사용자정보



NO	네트워크 차단	부서위치	사용자 정보	기기OS	IP주소	백신설치	실시간감시
1		전체		Windows 10 Pro (2004)	공인 : 사설 :	AhnLab V3 Internet Security 9.0	동작중
2		전체		Windows 10 Pro (1903)	공인 : 사설 :	Windows Defender	동작중

Hash 기준 파일 행위 추적

Utorrent.exe

- Black IP: 36건
- 원격접근: 72건

!

프로세스 정보

✕

프로세스정보

BlackIP 36건

ESM/SIEM 0건

IPS 0건

중요서버 0건

네트워크장비 0건

원격접근 72건

분류

미정의

IP경로

203.250.21.38 >> 204.11.56.48:2710

프로세스명

utorrent.exe

OS (SP)

Windows 10 64bit (2004)

NO	상태	파일명	파일 경로	체크섬	사용비율	화이트 프로세스	멀웨어 유무	서명	다운로드	분석결과
1	화이트 프로세스	imm32.dll	c:\Windows...	1E497A15FB...	77.04%	ON	OFF	✓	↓	9.2
2	화이트 프로세스	safeusb32.dll	c:\Windows\progra...	FFFE6F756...	66.09%	ON	OFF	✓	↓	5.6
3	화이트 프로세스	ntdll.dll	c:\Windows...	AF7C147F9B...	58.17%	ON	OFF	✓	↓	2.0
4	화이트 프로세스	winhttp.dll	c:\Windows...	62E4230DCA...	55.8%	ON	OFF	✓	↓	2.0

ww31.exe

- Black IP: 1871건
- IPS: 70건

!

프로세스 정보

✕

프로세스정보

BlackIP 1871건

IPS 70건

2021-07-05 ~ 2021-07-12

조회

분류

미정의

IP경로

203.250.13.46 >> 157.240.215.35:443

프로세스명

ww31.exe

OS (SP)

Windows 10 64bit (20H2)

NO	상태	파일명	파일 경로	체크섬	화이트 프로세스	멀웨어 유무	서명	다운로드	분석결과
1	화이트 프로세스	safeusb32.dll	c:\Windows\progra...	FFFE6F756...	ON	OFF	✓	↓	5.6
2	화이트 프로세스	gdi32.dll	c:\Windows...	CC84015691...	ON	OFF	✓	↓	0.8
3	화이트 프로세스	imm32.dll	c:\Windows...	1E497A15FB...	ON	OFF	✓	↓	9.2
4	화이트 프로세스	iphlpapi.dll	c:\Windows...	FE52D53B0D...	ON	OFF	✓	↓	1.6

상관분석 경고 등록

- Utorrent.exe이 비정상행위로 여러 항목(BlackIP,원격접근)에서 발생될 때 상관분석으로 등록

NO	탐지항목	파일명	체크섬	분석결과	상관분석	서명	사용비율
8	IPS	engine.dll	A62082ABCD29AC4ADC0...	VirusToTal		○	0%
9	BlackIP	utorrentie.exe	697A4488141819B...	VirusToTal		×	0%
10	BlackIP	www31.exe	CTD5A585FCE188423D31...	McAfee		×	0%

- 파일명 > 프로세스 정보 > Black IP

프로세스정보 BlackIP 40건 원격접근 211건 2021-03-01 ~ 2021-03-31 조회

Total 40건

NO	탐지번호	탐지일자	사용자정보	접근정보	프로세스명	서명	분석결과
1	3331932	2021-03-22 08:52:47			utorrent.exe	○	0
2	3331706	2021-03-22 08:50:56			utorrent.exe	○	0
3	3331153	2021-03-22 08:45:25			utorrent.exe	○	0
4	3331108	2021-03-22 08:44:47			utorrent.exe	○	0
5	3168391	2021-03-19 08:36:30			utorrent.exe	○	0
6	3131686	2021-03-18 17:08:51			utorrent.exe	○	0
7	3128891	2021-03-18 16:25:48			utorrent.exe	○	0

- 파일명 > 프로세스 정보 > 원격접근


프로세스정보 BlackIP 40건 원격접근 211건 2021-03-01 ~ 2021-03-31 조회

Total 211건

NO	탐지번호	탐지일자	사용자정보	접근정보	프로세스명	서명	분석결과
1	938725	2021-03-23 19:45:01			utorrent.exe	○	0
2	938718	2021-03-23 19:44:50			utorrent.exe	○	0
3	938080	2021-03-23 19:24:47			utorrent.exe	○	0
4	938075	2021-03-23 19:24:41			utorrent.exe	○	0
5	938069	2021-03-23 19:24:29			utorrent.exe	○	0
6	937401	2021-03-23 19:04:10			utorrent.exe	○	0
7	936896	2021-03-23 18:48:34			utorrent.exe	○	0

상관분석 경고 발생

- 예전에 멀웨어 판별 된 Sch.exe에서 탐지된 비정상행위(BlackIP, IPS:HTTPD Overflow)와 동일한 행위가 탐지된 파일은 연관성경보로 등록

NO	탐지항목	파일명	체크섬	분석결과	상관분석	서명	사용비율
8	IPS	engine.dll	A62082ABCD29AC4ADC0...	VirusToTal		○	0%
9	BlackIP	ww31.exe	697A4488141819B...	VirusToTal		×	0%
10	BlackIP	ww31.exe	CTD5A585FCE188423D31...	McAfee		×	0%

- 파일명 > 프로세스 정보 > Black IP

프로세스정보 BlackIP 1871건 IPS 70건 2021-07-05 ~ 2021-07-12 조회							
Total 1871건							
NO	탐지번호	탐지일자	사용자정보	검진정보	프로세스명	서명	분석결과
1	20230097	2021-07-12 14:53:50			ww31.exe		○
2	20221801	2021-07-12 14:34:38			ww31.exe		○
3	20221790	2021-07-12 14:34:36			ww31.exe		○
4	20221656	2021-07-12 14:34:16			ww31.exe		○
5	20219363	2021-07-12 14:28:21			ww31.exe		○
6	20219223	2021-07-12 14:27:59			ww31.exe		○
7	20219197	2021-07-12 14:27:55			ww31.exe		○

- 파일명 > 프로세스 정보 > IPS

프로세스정보 BlackIP 1871건 IPS 70건 2021-07-05 ~ 2021-07-12 조회							
Total 70건							
NO	탐지번호	탐지일자	사용자정보	검진정보	탐지명	프로세스명	
1	34923212	2021-07-12 12:37:02			(0574)MailEnable Authorization Header Buffer Overflow	ww31.exe	
2	34893244	2021-07-12 10:12:51			(0075)HTTPD Overflow	ww31.exe	
3	34885949	2021-07-12 09:37:47			(0075)HTTPD Overflow	ww31.exe	
4	34884326	2021-07-12 09:30:08			(0075)HTTPD Overflow	ww31.exe	
5	34880359	2021-07-12 09:12:26			(0574)MailEnable Authorization Header Buffer Overflow	ww31.exe	
6	34873094	2021-07-12 08:39:08			(0574)MailEnable Authorization Header Buffer Overflow	ww31.exe	
7	34872269	2021-07-12 08:34:48			(0574)MailEnable Authorization Header Buffer Overflow	ww31.exe	

프로세스 사용 비율을 통한 Utorrent 멀웨어 탐지

Black IP 프로세스 TOP

사용자

로그정보

모니터링

정책설정

시스템

관리

2021-03-18

2021-03-18

조회

프로세스 사용비율이 제일 낮은 목록

사용 비율 : 0.06%

46건

3	whale.exe	0B7CD7546B12...
4	vmnat.exe	0689E9275884...
5	wwahost.exe	1B3069159897...
6	vps.exe	86A0715ABB3D...
7	officeclicktorun.exe	1DC68C7EB3FC...
8	cfosspd.exe	0864F18C80C3...
9	powerpnt.exe	6D560AADD44D...
10	radeonsoftware.exe	E1F898BAF801...
11	windjview.exe	D1049EFEF775...
12	searchapp.exe	480441653F04...

13

utorrentie.exe

71677BE971BA...

사용 비율 : 0.18%

13건

사용 비율 : 0.24%

7건

사용 비율 : 0.3%

10건

사용 비율 : 0.36%

3건

사용 비율 : 0.42%

3건

사용 비율 : 0.47%

3건

사용 비율 : 0.53%

4건

사용 비율 : 0.59%

2건

중복탐지가 제일 낮은 프로세스 목록

중복탐지가 제일 높은 프로세스 목록

통합검색

검색

Total 270,519

사용자 정보	접근정보	프로세스명	사용비율	서명	다운로드	분석결과
전체 / skkim		backgroundtaskhost.exe	76.81%	✓	↓	6.2 / 7.4
전체 / DESKTOP-USN8NGP		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / cookcool		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / PC-C		winword.exe	14.71%	✓	↓	0 / 6.2
전체 / DESKTOP-3QT4D89		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / DESKTOP-M202HHT		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / DESKTOP-35NCS22		msedge.exe	59.02%	✓	↓	6.2 / 7.4
		searchapp.exe	53.91%	✓	↓	0.8 / 6.6
		msedge.exe	59.02%	✓	↓	6.2 / 7.4
		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / 배우산		backgroundtaskhost.exe	76.81%	✓	↓	6.2 / 7.4
전체 / DESKTOP-0N1HCIM		microsoft.photos.exe	39.8%		↓	0.4 / 2.0
전체 / 9KCHO97		chrome.exe	54.69%	✓	↓	1.2 / 2.4
전체 / DESKTOP-98R300J		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / DESKTOP-JHU4SJ8		ieexplorer.exe	51.96%	✓	↓	1.2 / 9.2
전체 / 손승환		microsoft.photos.exe	39.8%		↓	0.4 / 6.6
전체 / KEY		chrome.exe	22.89%	✓	↓	6.2 / 6.2
전체 / maum		searchapp.exe	53.91%	✓	↓	0.8 / 6.6
전체 / 김순환		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / ykmin		msedge.exe	59.02%	✓	↓	6.2 / 7.4
전체 / tycho		backgroundtaskhost.exe	76.81%	✓	↓	6.2 / 7.4
전체 / DESKTOP-B1QO7L2		backgroundtaskhost.exe	76.81%	✓	↓	6.2 / 7.4
전체 / DESKTOP-GKCM0EO		backgroundtaskhost.exe	76.81%	✓	↓	6.2 / 7.4

Agent 리소스 사용률

← → ↻ 203.250.2.14/majorDevicePolicy.do?menuID=34 Nutanix Web Cons...

STR TOPALOG 사용자 로그인보 모니터링 정책설정 시스템 관리 admin

네트워크장비 정책

정책설정 > 네트워크장비 정책

등록 목록삭제 통합검색 검색 Total 6

<input type="checkbox"/>	NO	사용여부	적용 레벨	네트워크장비명	IP	접근 허용 Port	접근 허용 IP	등록일 ▼
<input type="checkbox"/>	1	ON	2레벨	MIS_NFS	203.250.2.103			2021-03-11 16:41:52
<input type="checkbox"/>	2	ON	2레벨	MIS_tomcat3	203.250.2.108			
<input type="checkbox"/>	3	ON	2레벨	MIS_tomcat2	203.250.2.102			
<input type="checkbox"/>	4	ON	2레벨	MIS_tomcat1	203.250.2.101			
<input type="checkbox"/>	5	ON	2레벨	MIS_DB	203.250.2.104			
<input type="checkbox"/>	6	ON	2레벨	test				

Top Aegis Security

id_3959(203.250.3.....zip)

작업 관리자

파일(F) 옵션(O) 보기(V)

프로세스 성능 열 기록 시작프로그램 사용자 세부 정보 서비스

이름	상태	10% CPU	35% 메모리	0% 디스크
Spooler SubSystem App		0%	5.5MB	0MB/s
System Guard 런타임 모니터 ...		0%	3.9MB	0MB/s
TA-PRS 메인 에이전트(32비트)		0%	103.3MB	0MB/s
TA-PRS 보조 에이전트(32비트)		0%	3.2MB	0MB/s
TA-PRS 에이전트 서비스(32비트)		0.1%	1.6MB	0MB/s
TA-STR Agent(32비트)		0%	14.3MB	0MB/s
TA-STR Assistant(32비트)		0%	4.0MB	0MB/s
TA-STR 에이전트 서비스(32비트)		0.1%	1.6MB	0MB/s
User OOBE Broker		0%	1.2MB	0MB/s
Usermode Font Driver Host		0%	1.7MB	0MB/s
V3 Main UI Application		0%	1.0MB	0MB/s
Windows Defender SmartScreen		0%	6.1MB	0MB/s
Windows Security Health Service		0%	2.5MB	0MB/s
Windows 기본 잠금 화면		0%	0MB	0MB/s
Windows 셸 환경 호스트		0%	0MB	0MB/s
Windows 오디오 장치 그래픽 ...		0.3%	10.7MB	0MB/s

간단히(D) 작업 끝내기(E)

Putty 설정

분류(G)

- 세션
- 터미널
- 키보드
- 필
- 기능
- 창
- 모양
- 특성
- 변환
- 선택
- 색깔
- 접속
- 데이터
- 프락시
- 탈넷
- rlogin
- SSH
- 시리얼

Putty 세션 기본 옵션

접속 대상 정보

Host Name (or IP address) 203.250.2.104 Port 1521

접속 형식: ☐ 성파 (F) ☐ Telnet ☐ Rlogin ☒ SSH ☐ 시리얼

저장된 세션의 불러오기, 저장, 지움

저장된 세션 (E)

기본 설정

FW
RADIUS
STR
db
mis
pms

불러옴(L) 저장(V) 지움(D)

종료시에 창을 닫을 (W): ☐ 항상 ☐ 안 닫음 ☒ 접속이 끊겼을 때만



도입 효과

1. 탐지기간: 2월25일 ~ 8월17일

2. 멀웨어 탐지: 총 29건

- 멀웨어 탐지 당일 국내 Anti-Virus(V3,알약,하우리)에서 탐지 못함

- 주요 탐지 사례

- | | |
|------------------|--------------------------------------|
| - ww31.exe | Coin 마이너 |
| - Haleng.exe | Coin 마이너 |
| - MI20201223.exe | Coin 마이너 |
| - Vguuu.exe | 랜섬웨어 |
| - 54ab.exe | 랜섬웨어 |
| - winrmsrv.exe | 암호 화폐 마이닝 역할을 하는 토로이 목마 |
| - Winlogui.exe | Electroneum(일렉트로니움) ETN 이라는 Coin 마이너 |



보안이벤트와 PC연계를 통한 보안성 강화

- 도입 전 탐지하지 못한 조직 내 비정상적인 네트워크 행위를 감지하고 추적,분석하여 사용자 PC에 존재하는 멀웨어를 탐지하고 조치할 수 있는 시스템 구축