Report

사건번호	CASE_201704141331_한진섭	**분석관**	안상욱
증거번호	EVD_201704141331_한진섭		
생성시간	2017-04-14 13:31:28	**시간정보**	Local PC Time or User Modified
설 명			

가. 시스템

1. 시스템 정보

운영체제	Windows 7 Enterprise (32 bit) Service Pack 1
설치된 시간	2015-12-17 15:17:57
사용자	mcservice
컴퓨터 이름	MPC130066
작업 그룹	MAGNACHIP
설치경로	C:₩Windows
표준시간대	(UTC+09:00) 서울

2. 시스템 On/Off

최종 시스템 ON	2017-02-20 08:56:21
최종 시스템 OFF	2017-02-24 14:27:50
Total	시스템 On 69회, 시스템 Off 71회

3. 네트워크 정보

No	Adapter	IPv4	IPv6	Mac	Gateway	DNS
1	Intel(R) 82579LM Gigabit Network Connection	192.168.207.195/255.255.255.0			192.168.207.254	192.168.125.181 192.168.125.182 59.31.192.201

4. 프로그램 정보

설치 프로그램	217 개
최근 실행 프로그램	138 개

5. 공유폴더 정보

No	공유이름	경로
1	통합업무	

6. 자동 실행프로그램

No	이름	Command
1	BCSSync	"C:₩Program Files₩Microsoft Office₩Office14₩BCSSync.exe" /DelayServices
2	IME14 KOR Setup	C:₩Program Files₩Common Files₩Microsoft Shared₩IME14₩SHARED₩IMEKLMG.EXE /SetPreload /KOR /Log
3	IgfxTray	C:₩Windows₩system32₩igfxtray.exe
4	HotKeysCmds	C:₩Windows₩system32₩hkcmd.exe
5	Persistence	C:₩Windows₩system32₩igfxpers.exe
6	RTHDVCPL	C:₩Program Files₩Realtek₩Audio₩HDA₩RtHDVCpl.exe -s
7	V3 Session Process	"C:₩Program Files₩AhnLab₩V3IS80₩V3SP.exe"
8	USB3MON	"C:₩Program Files₩Intel₩Intel(R) USB 3.0 eXtensible Host Controller Driver₩Application₩iusb3mon.exe"
9	PaTray	C:₩Program Files₩AhnLab₩APC2₩Policy Agent₩PaTray.exe
10	MDS Session	"C:₩Program Files₩AhnLab₩MDS₩TwaTray.exe" /session
11	SafeWnd	C:₩Windows₩nics₩safewnd.exe
12	safeout	C:₩Windows₩nics₩safeout.exe
13	Communicator	"C:₩Program Files₩Microsoft Lync₩communicator.exe" /fromrunkey
14	MADRMAgent	C:₩MarkAny₩Document SAFER₩MADRMAgent.exe
15	NCleaner	"C:₩Program Files₩Naver₩NaverCleaner₩ncleaner.exe" /reboot
16	wizvera-veraport	"C:₩Program Files₩Wizvera₩Veraport20₩veraport.exe" wizvera-veraport://exec/x86/16105/
17	AhnLab Safe Transaction Application	"C:₩Program Files₩AhnLab₩Safe Transaction₩stsess.exe" /tray
18	Adobe Flash Player Updater	C:₩Windows₩system32₩Macromed₩Flash₩FlashPlayerUpdateService.exe
19	Adobe Flash Player Updater	C:₩Windows₩system32₩Macromed₩Flash₩FlashPlayerUpdateService.exe
20	ProgramDataUpdater	%windir%₩system32₩compattelrunner.exe -maintenance
21	Microsoft-Windows-DiskDiagnosticDataCollector	%windir%₩system32₩rundll32.exe dfdts.dll,DfdGetDefaultPolicyAndSMART
22	ActivateWindowsSearch	%SystemRoot%₩ehome₩ehPrivJob.exe /DoActivateWindowsSearch
23	ConfigureInternetTimeService	%SystemRoot%₩ehome₩ehPrivJob.exe /DoConfigureInternetTimeService
24	DispatchRecoveryTasks	%SystemRoot%₩ehome₩ehPrivJob.exe /DoRecoveryTasks $(Arg0)
25	ehDRMInit	%SystemRoot%₩ehome₩ehPrivJob.exe /DRMInit
26	InstallPlayReady	%SystemRoot%₩ehome₩ehPrivJob.exe /InstallPlayReady $(Arg0)
27	mcupdate	%SystemRoot%₩ehome₩mcupdate $(Arg0)
28	MediaCenterRecoveryTask	%SystemRoot%₩ehome₩mcupdate.exe -MediaCenterRecoveryTask
29	ObjectStoreRecoveryTask	%SystemRoot%₩ehome₩mcupdate.exe -ObjectStoreRecoveryTask
30	OCURActivate	%SystemRoot%₩ehome₩ehPrivJob.exe /OCURActivate
31	OCURDiscovery	%SystemRoot%₩ehome₩ehPrivJob.exe /OCURDiscovery $(Arg0)
32	PBDADiscovery	%SystemRoot%₩ehome₩ehPrivJob.exe /PBDADiscovery
33	PBDADiscoveryW1	%SystemRoot%₩ehome₩ehPrivJob.exe /wait:7 /PBDADiscovery
34	PBDADiscoveryW2	%SystemRoot%₩ehome₩ehPrivJob.exe /wait:90 /PBDADiscovery
35	PeriodicScanRetry	%windir%₩ehome₩MCUpdate.exe -pscn 0
36	PvrRecoveryTask	%SystemRoot%₩ehome₩mcupdate.exe -PvrRecoveryTask
37	PvrScheduleTask	%SystemRoot%₩ehome₩mcupdate.exe -PvrSchedule
38	RecordingRestart	%SystemRoot%₩ehome₩ehrec /RestartRecording
39	RegisterSearch	%SystemRoot%₩ehome₩ehPrivJob.exe /DoRegisterSearch $(Arg0)
40	ReindexSearchRoot	%SystemRoot%₩ehome₩ehPrivJob.exe /DoReindexSearchRoot
41	SqlLiteRecoveryTask	%SystemRoot%₩ehome₩mcupdate.exe -SqlLiteRecoveryTask
42	UpdateRecordPath	%SystemRoot%₩ehome₩ehPrivJob.exe /DoUpdateRecordPath $(Arg0)
43	ConfigNotification	%systemroot%₩System32₩sdclt.exe /CONFIGNOTIFICATION
44	Sidebar	%ProgramFiles%₩Windows Sidebar₩Sidebar.exe /autoRun
45	mctadmin	C:₩Windows₩System32₩mctadmin.exe
46	SMemo Start	"C:₩SMYSoft₩SMemo₩SMemo.exe" /login
47	NaverAgent	"C:₩Program Files₩Naver₩NaverAgent₩NaverAgent.exe" /autorun
48	DaTools LiveUpdate	"C:₩Program Files₩HumanTalk₩DaViewIndy₩LiveUpdate.exe"
49	OneNote 2010 화면 캡처 및 시작 기능.lnk	C:₩Program Files₩Microsoft Office₩Office14₩ONENOTEM.EXE

나. 사용자 정보

No	사용자	방문웹페이지	포털검색어	최근열어본 문서	휴지통 삭제파일	연결된 외부저장장치	실행된 명령어
1	Administrator	0	0	0	0	0	0
2	Guest	0	0	0	0	0	0
3	mcservice	14	14	0	0	1	0
4	Administrator	0	0	0	0	0	0
5	138001	1,269	1,269	372	0	2	2
6	mcservice.MAGNACHIP	19	19	0	0	0	1

다. 파일정보

문서	MS-Office : 0개, 일반 : 0개, 한글 : 0개, 도면 : 0개
압축파일	0개
삭제파일	0개
이메일	0개
키워드	0개

라. 메일 정보

메일 파일				
메일첨부파일	0 개			
NO	파일명	메일	첨부파일	
키워드	발견된 키워드 수 : 0 개			
NO	키워드	메일	첨부파일	합계

마. 외장형저장장치

No	디바이스정보	사용자계정	볼륨/볼륨명	제조사	시리얼넘버	최초연결시간	마지막 연결해제시간
1	USB_DISK_2.0	138001	USB DISK		07052461B6C12C06	2016-11-23 10:29:48	2016-11-23 10:30:02
2	USB_Flash_Drive	138001	F:₩	ADATA	2311211302040065	2016-10-28 13:21:37	2016-10-28 13:21:42
3	HM121HC			SAMSUNG	6&33937423&0	2017-01-25 08:09:15	2017-01-25 08:09:16
4	Cruzer_Blade	mcservice	Windows7 Enterprise K x86	SanDisk	4C530201450206108094	2015-12-17 15:14:56	2015-12-17 15:16:05

바. 개인정보 수집

구 분	파일	메일	첨부파일(메일)
전체	0 / 0	0 / 0	0 / 0
주민등록번호	0 / 0	0 / 0	0 / 0
이메일	0 / 0	0 / 0	0 / 0
은행계좌	0 / 0	0 / 0	0 / 0
카드번호	0 / 0	0 / 0	0 / 0
전화번호	0 / 0	0 / 0	0 / 0
여권번호	0 / 0	0 / 0	0 / 0
사업자번호	0 / 0	0 / 0	0 / 0
외국인등록번호	0 / 0	0 / 0	0 / 0
운전면허번호	0 / 0	0 / 0	0 / 0
사용자정의	0 / 0	0 / 0	0 / 0

형식: (항목 수 / 파일 수)