악성코드 상세 분석 보고서

보안 설치 프로그램으로 위장한 북한의 XCTDoor 실행 과정

(Document No : DT-20260327-001)

HAURI

www.hauri.co.kr

∘ 분석 개요

1. 개요

국내 은행 및 공공기관 웹사이트 이용 시 필수적으로 설치가 요구되는 통합 보안 프로그램으로 위장한 악성코드 유포 사례가 확인되었다. 해당 공격은 정상 소프트웨어로 위장하여 사용자의 신뢰를 확보한 뒤, 시스템 감염 및 추가 악성 행위를 수행하는 지능형 공격 기법을 사용한다.

2. 감염 방식

- 정상 보안 프로그램으로 위장한 설치 파일 유포
- 정상 소프트웨어 파일명 및 아이콘 모방
- 사용자에 의한 직접 실행 유도 (사회공학 기법 활용)

3. 주요 동작 방식

3.1. DLL 사이드로딩

정상 실행 파일을 이용하여 악성 DLL을 로드 정상 프로그램 실행 흐름 내에서 악성 코드 수행 보안 솔루션 탐지 우회

3.2. 정상 행위 위장

악성 코드 실행 이후 정상 설치 프로세스 진행 사용자에게 정상 프로그램으로 인식되도록 위장 감염 사실 은폐 및 의심 회피

4. 악성 DLL 분석

4.1 코드 은닉 기법

DLL 및 함수명 커스텀 암호화 적용 문자열 기반 동적 복호화 수행

4.2 위협 그룹 연관성

암호화 키에 특정 문자열 사용 해당 문자열을 근거로 북한 계열 위협 그룹과의 연관성 추정

5. 추가 페이로드 동작

외부 C&C 서버 통신 수행 추가 악성 페이로드 다운로드 복호화 후 메모리 또는 디스크 상에서 실행

6. 지속성 확보 기법

- 정상 시스템 경로에 파일 생성
- Microsoft Edge 관련 파일로 위장
- 자동 실행을 통한 지속성 유지

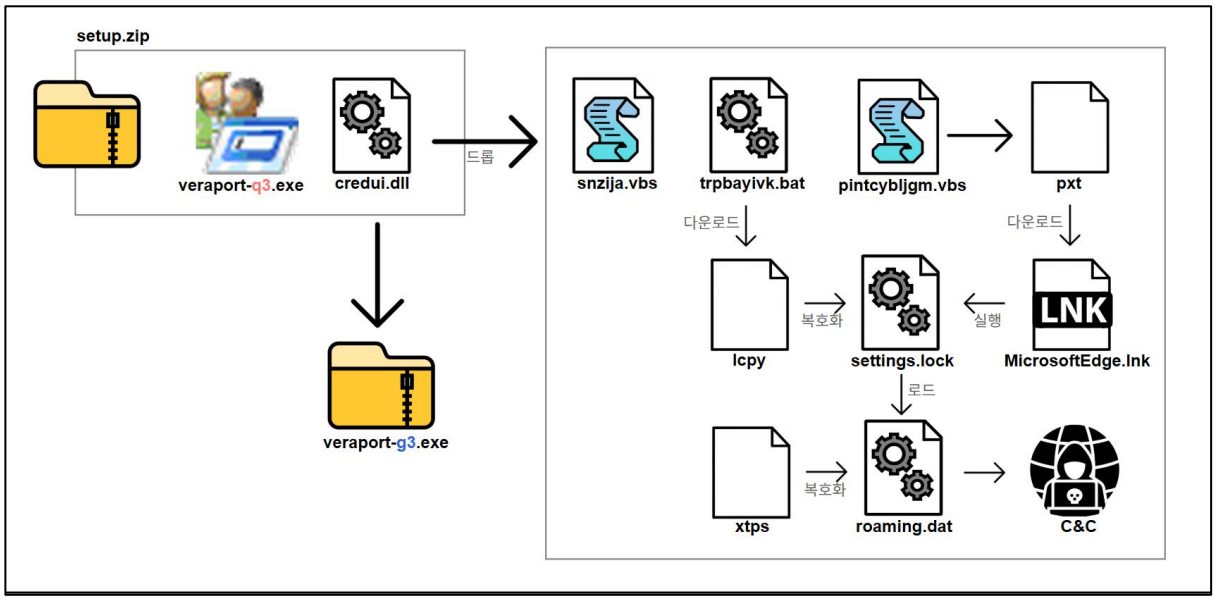
7. 최종 페이로드

최종적으로 **XCTDoor** 악성코드가 실행되며, 다음과 같은 기능을 수행한다.

- 시스템 정보 수집 및 모니터링
- 원격 명령 실행 (RCE)
- 추가 악성코드 다운로드 및 실행
- 감염 시스템 제어

8. 결론

본 공격은 정상 프로그램을 악용한 DLL 사이드로딩 기법과 사회공학 기법을 결합한 정교한 공격으로, 사용자 신뢰를 기반으로 감염을 유도하고 정상 행위를 가장하여 탐지를 회피한다.
또한 암호화된 문자열과 특정 키를 통해 APT 계열 위협 그룹과의 연관성이 의심되며, 최종적으로 백도어 기능을 수행하는 악성코드를 설치함으로써 지속적인 침해 활동이 가능하다.



[공격 도식도]

1. setup.zip

(MD5 : F05D11616979D4B3A02024F0EC075B3B, SIZE : 27,157,683)

개요 : 보안 설치 프로그램으로 위장한 악성 파일이 포함된 압축파일이다.

ViRobot	ZIP.S.IncludeMal.27157683

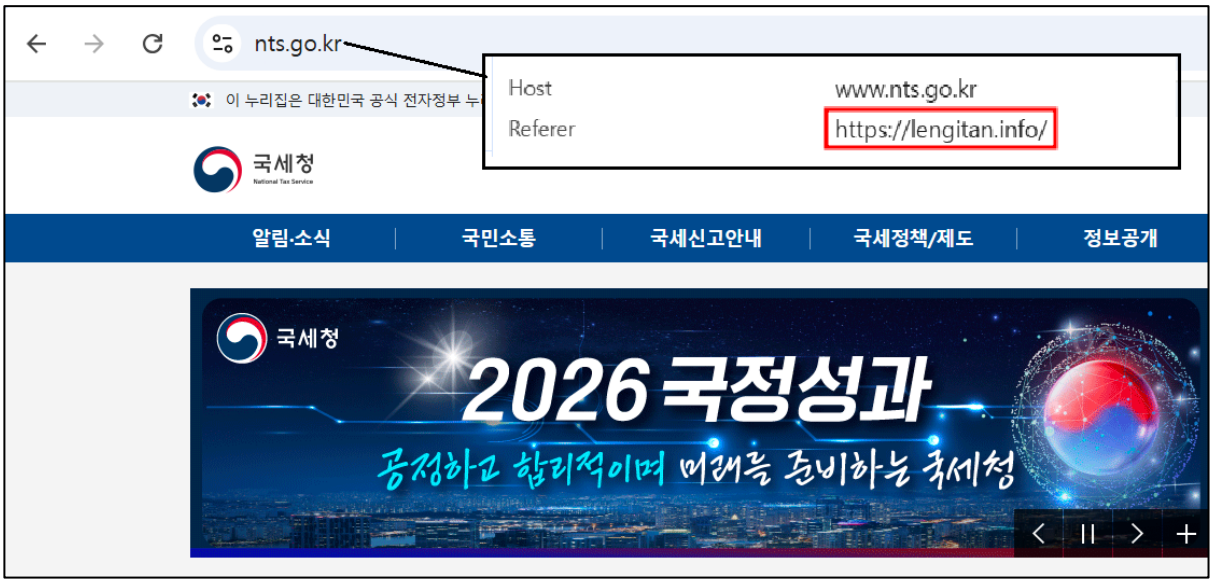
상세분석 :

(1) 악성 ZIP 파일이 유포되는 URL 을 식별하였다. 분석 당시 링크 접속 시, ZIP 파일이 다운로드 되었으나 현재는 페이지 접근이 안되어 파일 확인은 불가하였다.

- C&C: lengitan[.]info/download

[그림 1] 파일 다운로드

(2) 해당 URL 의 도메인 접속 시, 국세청 사이트로 접속되는데 해당 URL 이 정상으로 보이기 위해 리디렉션하는 것으로 보인다. 이는 국세청으로 위장하여 금융관련 업무를 보는 국내 사용자를 타겟으로 공격이 진행되고 있는 것으로 추정된다.



[그림 2] 국세청으로 리디렉션

(3) setup.zip 내부에는 veraport-q3 파일이있다. veraport 는 은행 및 공공기관 사이트 이용 시, 설치가 필요한 통합 보안 프로그램이다. 정상적으로 배포되는 파일명인 veraport-g3을 모방한 것으로 보인다. veraport-q3은 MS 의 정상 유틸리티이며 숨김 속성이 적용된 악성 파일 credui.dll 을 사이트 로딩하여 실행한다.

[그림 3] zip 파일 내부

(4) credui.dll 은 악성 루틴을 실행하며, 이후 정상 설치 과정을 수행하여 사용자 의심을 피한다.

```
int __stdcall sub_10003470(int a1, int a2, int a3)
{
  if ( a2 == 1 )
  {
    dword_1001B45C = a1;
    ((void (__cdecl *)(int))loc_10002B30)(1);   // 실행에 필요한 DLL, 함수 동적 매핑
    ((void (*)(void))loc_10002FA0)();           // 파일 생성, 실행
  }
  return 1;
}
```

[그림 4] credui.dll 악성 루틴

(5) loc_10002B30에서 실행에 필요한 DLL 을 동적 할당하는데, 이때 필요한 DLL 과 함수들은 암호화되어 있다. 암호화 알고리즘은 커스텀 XOR 기반 암호문 체이닝 방식이 사용되었다.

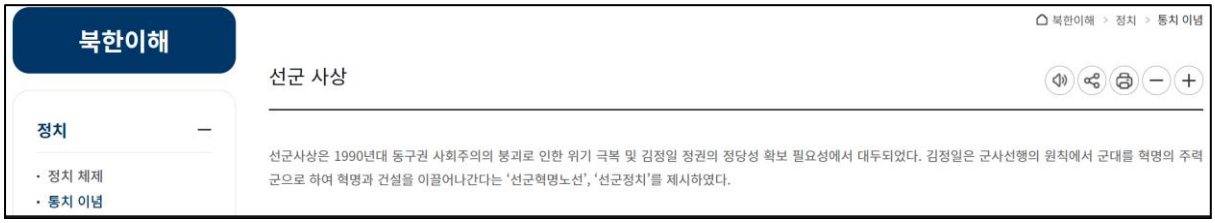
- iv: 13245768
- Key: 70C96DADB5D17CC720C170ADCCB938C1 (쥰국통일선군만세)

```
0025F738  70 C9 6D AD B5 D1 7C C7 20 C1 70 AD CC B9 38 C1  pÉm.µÑ|Ç Áp.Ì¹8Á
0025F748  00 00 00 00 E8 21 D5 A5 74 F8 25 00 EA 2B 00 10  ....è!Õ¥tø%.ê+..
```

[그림 5] 암호화키

[그림 6] 문자열 변환 결과

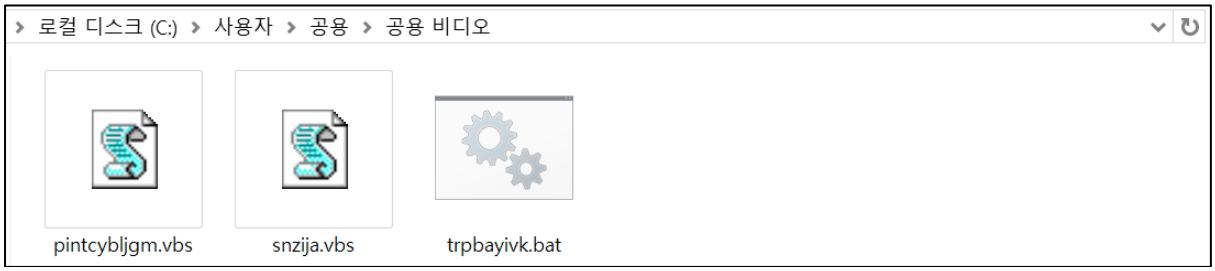
(6) 암호화에 사용된 키 문자열에는 선군이 사용되었다. 선군(先軍)은 군사를 최우선으로 하는 북한의 정치 체제를 의미한다.



[그림 7] 통일부 – 북한정보포털 자료

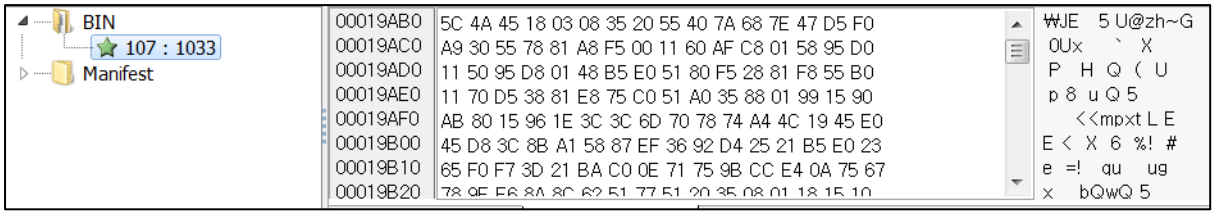
(7) 이후 실행에 필요한 스크립트들을 공용 비디오 폴더에 생성한 뒤 작업 스케줄러를 통해 실행되도록 한다.

- 파일 경로: C:₩Users₩Public₩Videos
- 생성 파일: pintcybljgm.vbs, snzija.vbs, trpbayivk



[그림 8] 파일 생성

(8) 마지막으로 리소스 영역에 암호화하여 저장되어있는 veraport 설치 파일을 실행함으로써 사용자들이 악성코드에 감염되었다는 사실을 인지하지 못하도록 한다.



[그림 9] 리소스 영역의 veraport 설치 파일

2. snzija.vbs

(MD5 : D1642D1A13DB6E2627136F4197F3A9E8, SIZE : 199)

개요 : 스크립트 파일을 통해 추가 악성코드를 다운로드하며 정상 파일로 위장하여 실행한다.

ViRobot	VBS.S.Starter.199

상세분석 :

(1) office365라는 작업을 통해 실행된 snzija.vbs 는 trpbayivk.bat 파일을 실행한다.

- 작업 이름: office365

```
TaskName  Command                                  Interval
--------  -------                                  --------
office365 c:₩₩users₩₩public₩₩videos₩₩snzija.vbs 00:02:00
```

[그림 10] office365 작업

(2) 실행된 trpbayivk.bat 파일은 C&C 에서 추가 파일을 다운로드하여 공용 비디오 폴더에 저장하며, AdobeUpdate 라는 작업을 생성하여 작업 스케줄러를 통해 pintcybljgm.vbs 파일이 실행되도록한다.

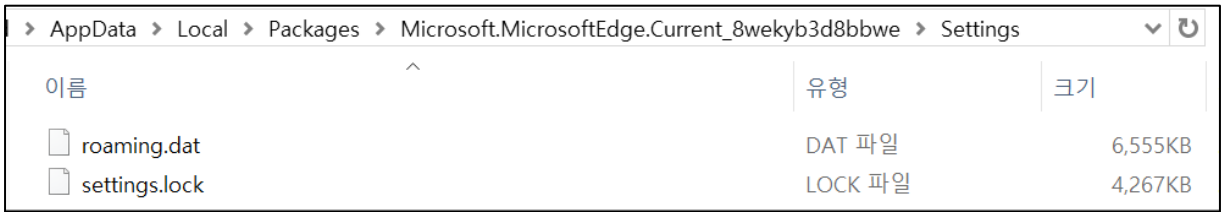
- C&C: hxxps://hesenorm[.]info/download/lcpy
- C&C: hxxps://hesenorm[.]info/download/xtps
- 파일 경로: C:₩Users₩public₩pictures
- 작업 이름: AdobeUpdate

```
TaskName    Command                                   Interval
--------    -------                                   --------
AdobeUpdate C:₩users₩public₩videos₩pintcybljgm.vbs 00:01:00
```

[그림 11] AdobeUpdate 작업

(3) pintcybljgm.vbs 는 C&C 에서 추가 스크립트를 로드하며, 앞서 다운받은 xtps, lcpy 를 복호화하여 다음 경로에 저장한 뒤, 이전에 사용한 파일들과 작업은 삭제한다.

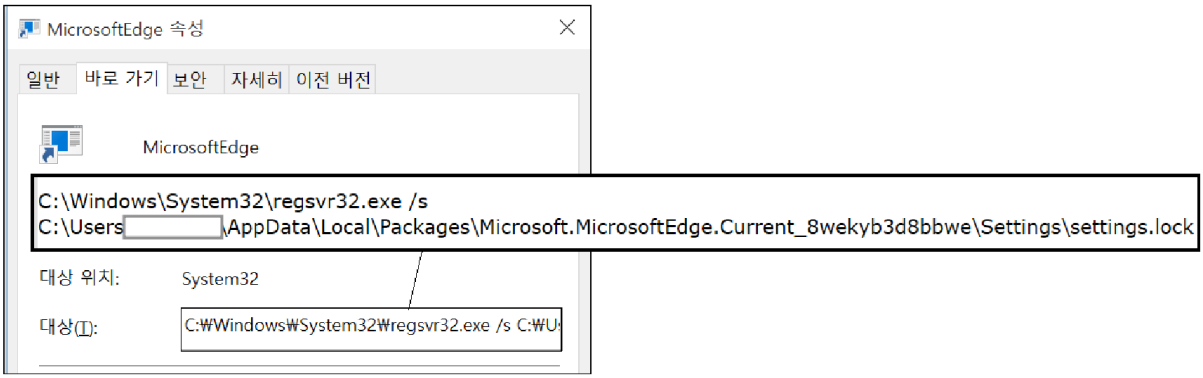
- C&C: hxxps://hesenorm[.]info/download/pxt
- 파일 경로: C:₩%LocalAppData%₩Packages₩Microsoft.MicrosoftEdge.Current_8wekyb3d8bbwe₩Settings
- 생성 파일: roaming.dat, settings.lock



[그림 12] 파일 생성

(4) settings.lock 과 roaming.dat 은 Go 언어로 작성된 DLL 파일이며 단일 실행이 불가하다. 따라서 시작 폴더에 MicrosoftEdge 라는 바로가기 파일을 생성하며, 이를 통해 실행 및 지속성을 유지한다.

- 파일 경로: C:₩%Startup%₩MicrosoftEdge.lnk



[그림 13] MicrosoftEdge.lnk

(5) settings.lock 은 xcloader.dll 파일로, XCTdoor 인 raoming.dat 을 로드하여 실행되도록 한다.

```
                    s_xcloader.dll_293c4a046                XREF[1]:     293c4a00c(*)
293c4a046 78 63 6c        ds         "xcloader.dll"
          6f 61 64
          65 72 2e ...
```

[그림 14] settings.lock 디컴파일 화면

(6) 최종 실행된 roaming.dat 에서는 monunit, cmdunit, rootunit_send_spec_info 등의 기능이 식별되었으며, 이를 통해 C&C 통신을 통해 시스템 정보 전송, 모니터링, 원격 명령 실행 등의 악성행위를 수행한다는 것을 알 수 있다.

```
.rdata:00000002F39DB9B0 aXctMainGo      db 'xct/main.go',0      ; DATA XREF: .rdata:00000002F39D8250↑o
.rdata:00000002F39DB9BC aXctMonunitV1Go db 'xct/monunit_v1.go',0
.rdata:00000002F39DB9BC                                         ; DATA XREF: .rdata:00000002F39D8234↑o
.rdata:00000002F39DB9CE aXctProcessunit db 'xct/processunit_v1.go',0
.rdata:00000002F39DB9CE                                         ; DATA XREF: .rdata:00000002F39D8258↑o
.rdata:00000002F39DB9E4 aXctRootuintGo  db 'xct/rootuint.go',0  ; DATA XREF: .rdata:00000002F39D825C↑o
.rdata:00000002F39DB9F4 aXctUnitGo      db 'xct/unit.go',0      ; DATA XREF: .rdata:00000002F39D8260↑o
.rdata:00000002F39DBA00 aXctXctGo       db 'xct/xct.go',0       ; DATA XREF: .rdata:00000002F39D823C↑o
.rdata:00000002F39DBA0B aXctXctV1Go     db 'xct/xct_v1.go',0    ; DATA XREF: .rdata:00000002F39D8270↑o
```

[그림 15] roaming.dat 디컴파일 화면

IOC

***C&C**

hxxps://lengitan[.]info/download
hxxps://hesenorm[.]info/download/xtps
hxxps://hesenorm[.]info/download/lcpy
hxxps://hesenorm[.]info/download/pxt

***MD5**

F05D11616979D4B3A02024F0EC075B3B
97B14304761A2BAA620007B2DF8D6547
B86F07F60186E65DFFCA615CC69EAFF1
C43A146F8B3287A68BCA193CAF7BE16A
00671B085EB385DEECB3FBAD1316CA42
1A77DDDAE05B6BD96820902B6AEE9CC3
3A61B8DA99F73E60A0C305FF7A5085E1
D1642D1A13DB6E2627136F4197F3A9E8
B004470D1E888ABC8F68CEDC374A9CE4
9A6758045179DBE96EF34AB3811C3D1E
1F0E8B66339C5994A0E9ED5BDF8BC375