S/W 다운로드 위장, 다양한 종류의 악성코드 유포

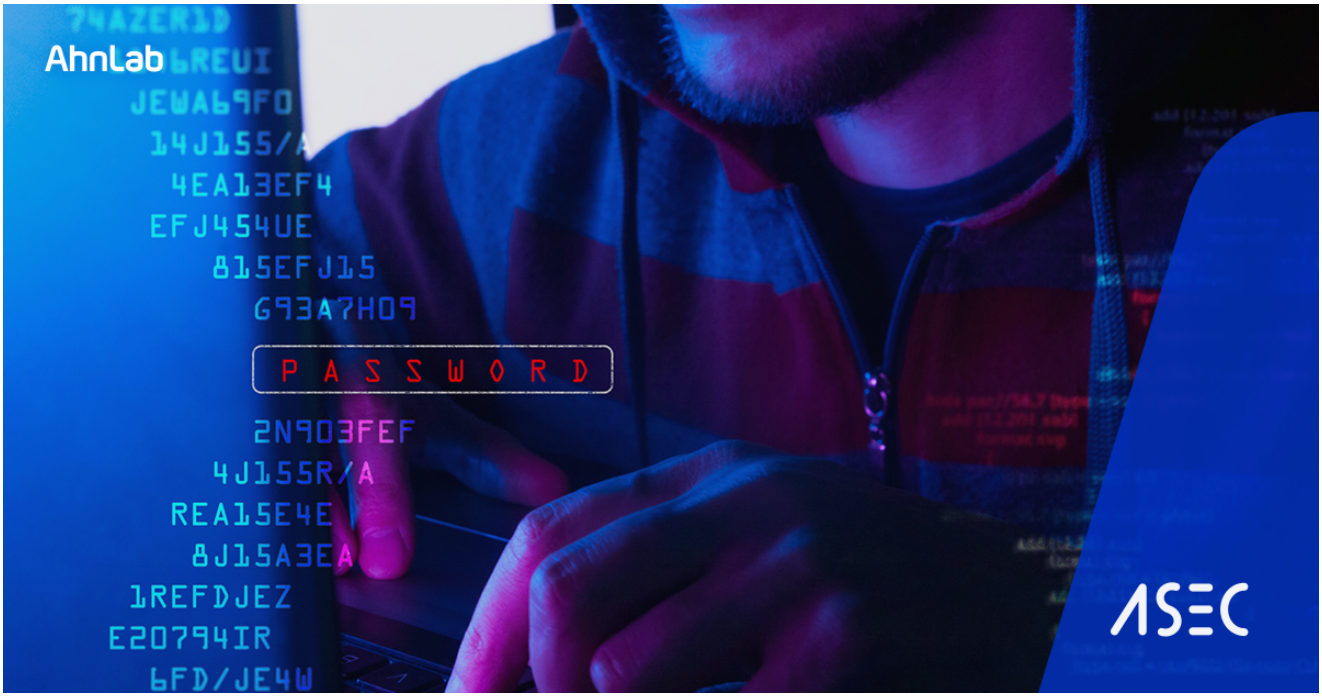
asec.ahnlab.com/ko/25837/

2021년 8월 4일

ASEC 분석팀에서는 기존 다수의 블로그 포스팅을 통해 상용 소프트웨어의 Crack, Serial 등의 키워드로 검색되는 악성 사이트로부터 유포되는 CryptBot 악성코드에 대하여 언급하며 사용자의 주의를 당부하였다.

피싱 사이트를 통해 유포되는 CryptBot 정보탈취 악성코드 – ASEC BLOG

ASEC 분석팀은 유틸리티 프로그램으로 위장하여 정보탈취 악성코드를 유포하는 피싱 사이트를 아래 블로그를 통해 소개한 바 있다. 해당 악성코드는 구글 검색 키워드로 유틸리티 프로그램 이름을 검색할 시 사용자에게 비교적 상단에 노출된다. 현재까지도 활발히 유포되고 있으며, 감염 과정은 지속해서 변화되고 있다. 해외에서 CryptBot 으로 알려진 해당 정보 탈취 악성코드의 최근 유포 파일의 감염 방식에 관해 설명한다. [그림 1], [그림 2]는 유틸리티 프로그램으로 위장하여 악성코드를 유포하는 피싱 사이트의 모습이다. 영문 사이트 …



지속적으로 변형되며 유포 중인 CryptBot 정보탈취 악성코드 – ASEC BLOG
CryptBot 악성코드는 S/W 다운로드 페이지를 위장한 악성 사이트에서 유포 중인 정보탈취 유형의 악성코드이다. 다수의 악성 사이트가 개설되어 있으며, 유명 상용 소프트웨어의 Crack, Serial 등의 키워드 검색 시 검색 결과 상위에 다수 노출되기 때문에 많은 사용자가 해당 악성코드를 다운로드하여 실행한다. 또한 해당 샘플은 SFX 방식의 패킹을 사용하기 때문에 정상과 악성의 구분이 쉽지 않은 편이며, 하루에도 몇 번씩 잦은 변형이 발생한다. 다운로드 페이지로 위장하였기 때문에 사용자는 정상 파일로 오인하여 V3 제품에서 …
이러한 악성 사이트로부터 유포되는 악성코드는 CryptBot 악성코드가 대다수이지만, 간혹 타 악성코드가 유포되곤 한다. 본 블로그에서는 동일 유형의 악성코드 유포 중 CryptBot을 제외한 타 악성코드에 대하여 언급하고자 한다.

기존의 블로그에서도 언급했듯이 해당 악성코드는 검색엔진에 특정 상용 소프트웨어의 Crack, Serial, Keygen, License 등의 불법적인 키워드를 검색할 경우 상위에 노출되는 악성 페이지로부터 유포된다.

해당 악성 페이지는 대표적으로 다음과 같으며 정상 툴을 다운로드 받을 수 있을 것처럼 꾸며 놓았지만, 실제로 다운로드되는 파일은 악성코드가 담긴 압축 파일이다. 자세한 내용은 다음 블로그에 상세히 기술되어 있다.

그림1. 악성코드 유포 사이트 예시

다른 외형으로 유포 중인 CryptBot 정보탈취 악성코드 – ASEC BLOG

CryptBot 악성코드는 유틸리티 다운로드 페이지를 위장한 악성 사이트를 통해 유포되는 정보 탈취형 악성코드다. 특정 프로그램, 크랙, 시리얼 등의 키워드를 검색 시 관련 유포지가 상단에 노출되며, 해당 페이지에 접속하여 다운로드 버튼을 누를 경우 CryptBot 악성코드 다운로드 페이지로 리디렉트 된다. 악성 사이트는 다양한 키워드로 매우 많은 수량이 개설되어 있다. 대부분의 유명 소프트웨어 키워드를 검색 시 다수의 악성 사이트가 상위 페이지에 노출되며, 관련 파일 탐지 수량 또한 상당하다. 웹 서핑 중 아래와 같은 페이지를 마주…

이러한 악성 사이트에서 유포 중인 악성코드는 크게 두가지 유형으로 나뉜다.

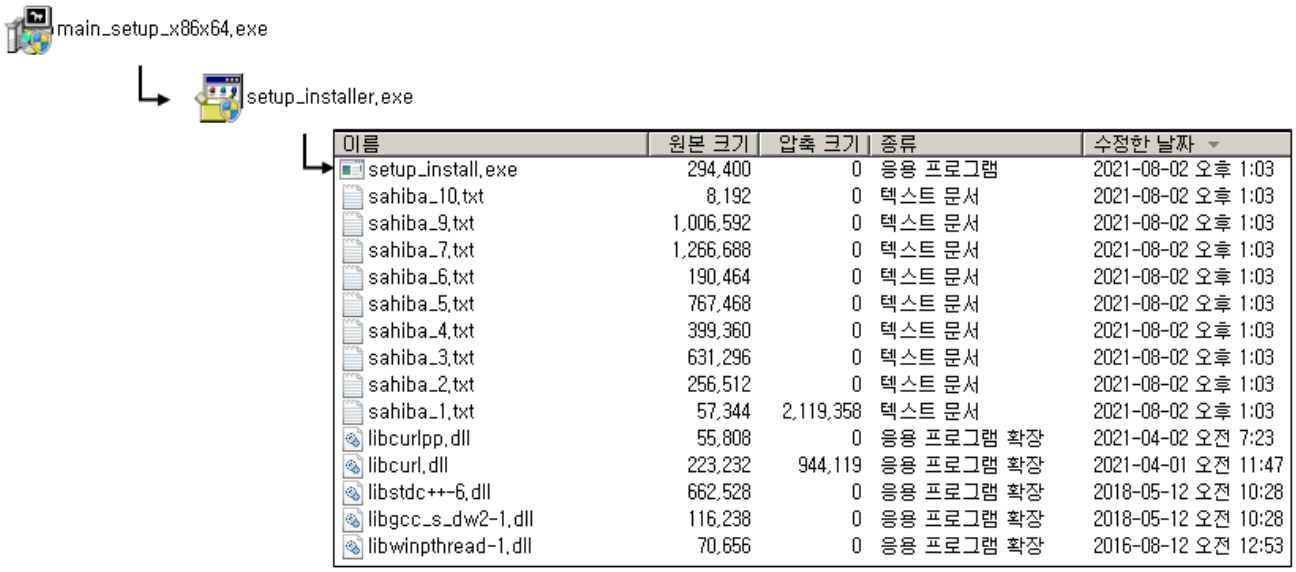
NSIS 드로퍼 유형과 Autoit Loader 유형이다.

전자는 실행 시 다수의 악성코드를 동시에 드롭하여 실행한다. 드롭 과정에서 AV 제품의 진단이 발생할 경우 실행이 불가능하여 본 블로그에서는 다루지 않았지만, 어떠한 경우에서 실행되었다면 복구 불가능할 정도로 다수의 악성코드에 감염된다. 보통 10개 정도의 악성코드를 드롭 후 실행하며, 이 중 다운로더형 악성코드도 다수 포함되어 있기 때문에 실제 감염되는 악성코드는 더 많게 된다. 해당 드로퍼로 인해 감염되는 악성코드는 대표적으로 다음과 같다.

BeamWinHTTP, SmokeLoader, RedLine, YAHOOYLO, Socelars Stealer, ClipBanker, Backstage Stealer, Androm 외 다수

해당 유형의 특징은 최종 압축 해제한 실행파일의 아이콘이 NSIS 기본 아이콘이며, 그 내부 파일은 “setup_installer.exe”이름을 가진 7zSFX 실행파일인 점이다. 실행 시 특정 디렉토리에 내부 파일들을 압축 해제 후 “setup_install.exe” 파일을 실행하는데, 동일 디렉토리에 생성된 txt 파일을 실행하는 역할을 한다.

내부에 존재하는 다수의 txt 파일은 텍스트 파일로 위장한 악성코드 파일이다. 별도의 인코딩이나 암호화를 거치지 않았기 때문에 압축 해제 즉시 V3 제품에 의해 탐지되어 차단된다.



이름	원본 크기	압축 크기	종류	수정한 날짜
setup_install.exe	294,400	0	응용 프로그램	2021-08-02 오후 1:03
sahiba_10.txt	8,192	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_9.txt	1,006,592	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_7.txt	1,266,688	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_6.txt	190,464	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_5.txt	767,468	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_4.txt	399,360	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_3.txt	631,296	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_2.txt	256,512	0	텍스트 문서	2021-08-02 오후 1:03
sahiba_1.txt	57,344	2,119,358	텍스트 문서	2021-08-02 오후 1:03
libcurlpp.dll	55,808	0	응용 프로그램 확장	2021-04-02 오전 7:23
libcurl.dll	223,232	944,119	응용 프로그램 확장	2021-04-01 오전 11:47
libstdc++-6.dll	662,528	0	응용 프로그램 확장	2018-05-12 오전 10:28
libgcc_s_dw2-1.dll	116,238	0	응용 프로그램 확장	2018-05-12 오전 10:28
libwinpthread-1.dll	70,656	0	응용 프로그램 확장	2016-08-12 오전 12:53

그림2. NSIS Dropper 악성코드 실행 구조

- Dropper/Win.MulDrop.*
- Dropper/Win.MuDrop.*

후자의 경우는 실행 시 Autoit 관련 파일을 생성 후 실행하는 유형이다. 기존 블로그에서 언급했던 CryptBot의 경우가 해당 유형에 속한다. CryptBot을 주로 유포하는 점에서 자사에서는 해당 패킹 유형을 “CryptLoader” 진단명으로 대응 중이다. 대부분의 경우에는 CryptBot 악성코드를 유포하고, CryptBot은 Clipbanker를 다운로드하여 실행하지만, 간혹 타 악성코드가 유포되곤 한다.

최근 약 한 달간 해당 유형으로 유포된 악성코드 중 CryptBot을 제외한 악성코드는 다음과 같다. 다음 샘플들은 악성 페이지로부터 직접 다운로드 되거나 CryptBot, NSIS Dropper 등 해당 공격 유형의 샘플에 의하여 추가 생성된 악성코드이다.

1. RedLine

RedLine 악성코드는 .NET 언어로 빌드된 악성코드로 각종 사용자 정보를 탈취하여 C2로 전송한 후 추가 악성코드를 다운로드 실행 및 자가삭제 행위가 가능하다. 행위적으로는 CryptBot 악성코드와 유사하지만 기능은 훨씬 다양하며 약 100KB의 비교적 적은 용량을 가진

다.

실행 시 오토잇 스크립트 내부 쉘 코드에 의해 RegAsm.exe 프로세스를 실행 후 해당 프로세스에 할로잉되어 동작한다.

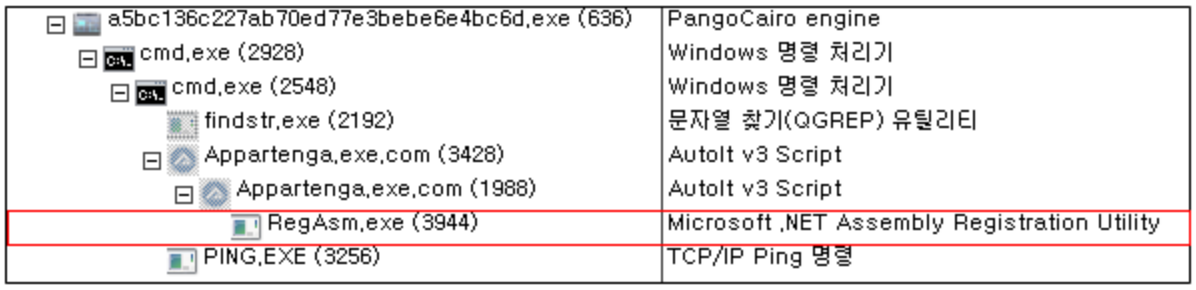


그림3. RedLine 악성코드 프로세스 트리

실제로는 RegAsm.exe에 할로잉되어 동작하지만 내부 바이너리를 추출해보면 다음과 같이 유효 인증서가 존재하며, 타 .NET 악성코드와는 다르게 난독화가 거의 되어있지 않은 형태이다.

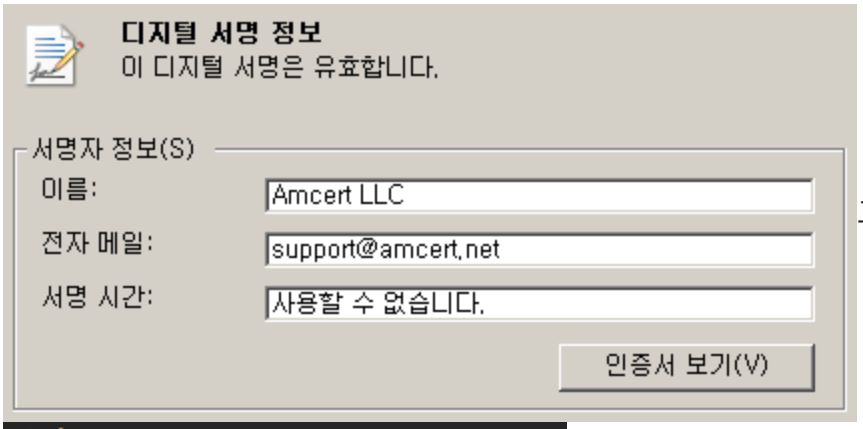


그림4. 서명 정보

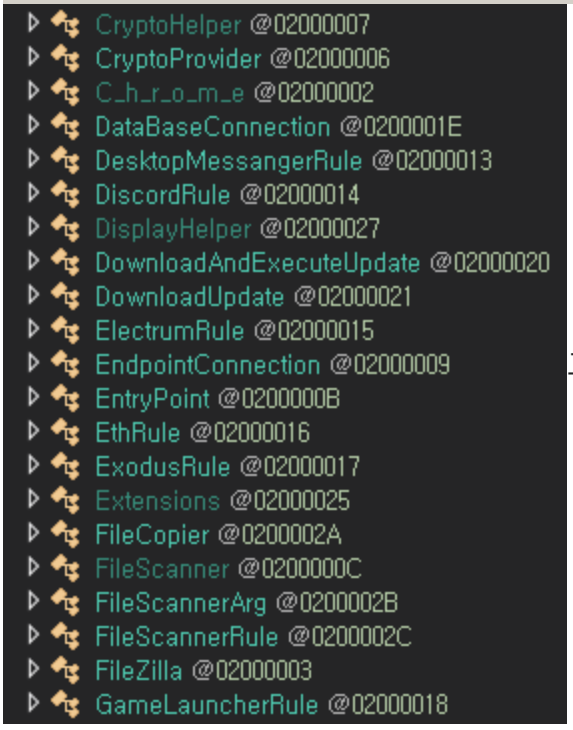
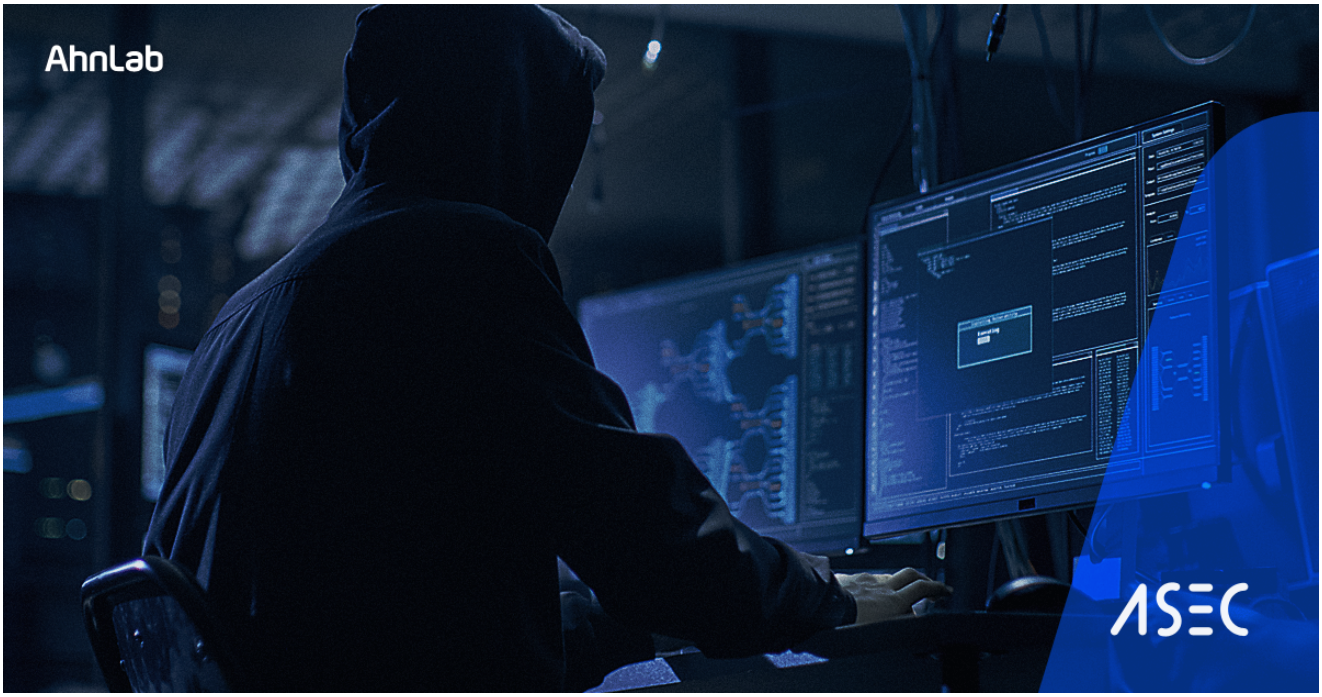


그림5. 내부 메소드 목록

각종 브라우저에 저장된 계정 및 패스워드, 암호화폐 지갑 파일, Discord 등의 메신저 토큰, FTP 클라이언트 정보, VPN 정보 등 다양한 주요 정보가 탈취 대상이 되며 과거에는 아래 블로그와 같이 Youtube를 통해 유포된 이력이 있다.



유튜브를 통해 유포 중인 RedLine 인포스틸러 – ASEC BLOG

ASEC 분석팀은 최근 RedLine 인포스틸러 악성코드가 크랙 프로그램 다운로드 링크로 위장한 유튜브 사이트를 통해 유포 중인 것을 확인하였다. RedLine은 정보 유출 악성코드로서 웹 브라우저 및 FTP 클라이언트 프로그램에 저장되어 있는 사용자 계정 정보나 스크린샷, 코인 지갑 주소 등 사용자 정보를 C&C 서버에 유출하는 기능을 갖는다. RedLine 악성코드가 최초로 확인된 것은 2020년 3월경으로 코로나 바이러스 이슈를 이용한 스팸 메일을 통해 유포된 것이 첫번째 사례이다. 이후부터 꾸준히 다양한 경로를 통해 유포되고…

C2: gimpimageeditor.com

2. Vidar

Vidar 악성코드 또한 정보 탈취 목적의 악성코드이다. 본 샘플의 경우 nslookup.exe를 실행 후 프로세스 할로잉하여 동작한다.

21be2e389bc3d34f6a20dad828aa80b2.exe (3212)	7z Setup SFX (x86)
cmd.exe (3256)	Windows 명령 처리기
cmd.exe (3288)	Windows 명령 처리기
findstr.exe (3296)	문자열 찾기(QGREP) 유틸리티
Melagrani.exe.com (3304)	AutoIt v3 Script
Melagrani.exe.com (3332)	AutoIt v3 Script
nslookup.exe (3580)	nslookup
PING.EXE (3312)	TCP/IP Ping 명령

그림6. Vidar 악성코드 프로세스 트리

내부에서 추출 가능한 원본 바이너리의 WinMain 함수에서는 다음과 같이 안티 디스어셈블 기능을 하는 가비지 코드가 포함되어 있으며, 이를 제거해야 정상적으로 디스어셈블이 가능하다. 안티 디스어셈블의 경우 대표적인 분석 방해 기법 중 하나이다.

```
.text:0040C9B3 loc_40C9B3:                             ; CODE XREF: .text:0040C9CB↓j
.text:0040C9B3                 mov     ax, 1AB8h
.text:0040C9B7                 mov     bx, 6BBh
.text:0040C9BB                 mov     cx, 0B9h
.text:0040C9BF                 mov     dx, 1BAh
.text:0040C9C3                 mov     si, 0FFBEh
.text:0040C9C7                 mov     di, 32BFh
.text:0040C9CB                 jmp     near ptr loc_40C9B3+1
```

그림7. 안티 디스어셈블 코드

Vidar 악성코드는 정보 수집 행위 전에 C2에 접속하여 행위에 필요한 다양한 라이브러리를 다운로드 받는 것이 특징이며 해당 C2 주소를 구하기 위해 공격자가 개설해 놓은 텀블러 주소로 접속을 시도한다. 해당 텀블러에 접속할 경우 다음 그림과 같이 내부 소스코드에 Vidar의 실제 C2 주소가 명시되어 있다.

```
<html>
   <head prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb# blog: http://ogp.me/ns/blog#">
      <meta param="about:116.202.183.50|">
      <meta charset="utf-8">
      <title></title>
   <style>figure{margin:0}.tmblr-iframe{position:absolute}.tmblr-iframe.hide{display:none}.tmblr
   <body>
```

그림8. 공격자 텀블러 페이지

과거 Faceit 등의 게임 플렛폼을 이용하여 C2 정보를 업데이트하는 Vidar 악성코드에 대한 정보를 ASEC블로그를 통해 포스팅한 바 있다. 이처럼 공격자는 C2를 업데이트하기 위해 정상 도메인을 활용하는 사례가 잦아지고 있다.

특정 게임 플랫폼을 악용한 Vidar 인포스틸러 – ASEC BLOG

ASEC 분석팀에서는 최근 Vidar 인포스틸러 악성코드가 Faceit이라는 게임 매칭 프로그램을 악용하여 C&C 서버 주소를 구하는 것을 확인하였다. Vidar는 스팸 메일이나, PUP 그리고

KMSAuto 인증 툴을 위장하여 설치되는 등 과거부터 꾸준히 유포되고 있는 악성코드이다. (본 블로그 하단의 이전 블로그 링크 참고) Vidar는 정보 탈취 행위를 수행하기 이전에 C&C 서버에 접속하여 명령을 전달받고, 추가적으로 여러 DLL들을 다운로드 받아 사용자의 정보들을 수집한다. 과거에는 일반적인 악성코드들과 같이 단순히 C&C…
탈취한 정보를 압축하여 C2로 전송하며 C2의 명령에 따라 다양한 추가적인 악성 행위가 가능하다.

C2: shpak125.tumblr.com / 116.202.183.50

3. Remcos

Remcos 악성코드는 RAT 유형의 악성코드로 키로깅을 포함한 다양한 사용자 정보를 수집 및 유출하며, 다양한 공격자의 명령을 수행할 수 있다. 원격 관리를 위한 도구로 제작자의 웹 페이지에서 판매되고 있지만 대부분 악성코드로 악용되는 경우가 많다.

스팸 메일로 유포 중인 Remcos RAT 악성코드 – ASEC BLOG
Remcos는 RAT(Remote Administration Tool) 악성코드로서 수년 전부터 스팸 메일을 통해 꾸준히 유포되고 있다. Remcos는 제작자가 아래와 같은 웹 사이트를 통해 원격 관리를 위한 RAT 도구로 설명하면서 판매하고 있으며 최신까지도 주기적으로 업데이트 되고 있다.
Remcos 홈페이지에서 설명하는 기능들만 본다면 원격 지원을 위한 목적으로 또는 도난 시 민감한 데이터를 삭제하거나 추적하는 목적으로도 사용 가능하다고 적혀져 있다. 물론 이러한 기능들이 지원되는 것은 사실이다. 하지만 키로깅, 스크린샷 캡쳐…
본 샘플에서는 vidar의 경우와 마찬가지로 nslookup.exe를 실행 후 할로잉하여 동작한다.

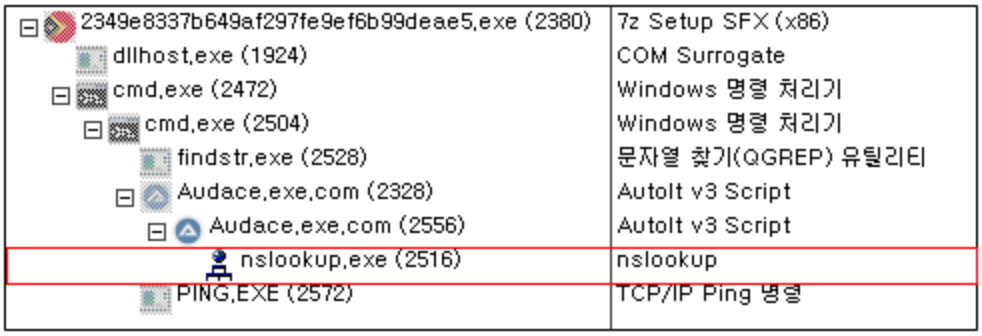


그림9. Remcos 악성

코드 프로세스 트리

실행 시 “Remcos_Mutex_Inj” 뮤텍스를 생성한다.

```
v12 = OpenMutexA(0x100000u, 0, "Remcos_Mutex_Inj");
v13 = v12;
if ( v12 )
{
  WaitForSingleObject(v12, 0xEA60u);
  CloseHandle(v13);
}
```

그림10. 뮤텍스 생성 코드

권한 상승, 키로깅, 각종 정보 탈취, 웹캠 및 마이크 녹음, 클립보드 탈취, 실시간 스크린 전송 및 원격 제어 등의 다양한 악성 행위가 가능하다.

```
sub_410B9B(
  HKEY_CURRENT_USER,
  L"Software\\Classes\\mscfile\\shell\\open\\command",
  &ValueName,
  v2,
  v3,
  v5,
  v7,
  v9,
  v11,
  2u);
sub_41805E("eventvwr.exe");
v1 = sub_401EEB(v12);
if ( ShellExecuteW(0, L"open", v1, &ValueName, &ValueName, 0) > 0x20 )
  ExitProcess(0);
```

그림11. 권한 상승 코드

본 샘플에서 사용된 Remcos의 버전은 “3.2.0 Pro” 이다. 버전과 관련된 문자열은 rdata 영역에 하드코딩 되어있으며, 해당 버전은 2021.07.30 일자로 릴리즈된 최신 버전이다.

```
strcpy(v7, " * Remcos v");
v9 = &v17;
while ( *++v9 )
  ;
strcpy(v9, "3.2.0 Pro");
v11 = &v17;
while ( *++v11 )
  ;
```

그림12. Remcos 버전 정보

최근 유포된 Remcos 샘플 중에서는 내부 파일이 추가적인 패킹이 되어있는 경우도 확인되었다. UPX와 Mpress등의 패커로 포장된 악성코드가 정상 프로세스에 할로잉된다. 공격자는 탐지 우회를 위해 여러 테스트를 거친 것으로 판단된다.

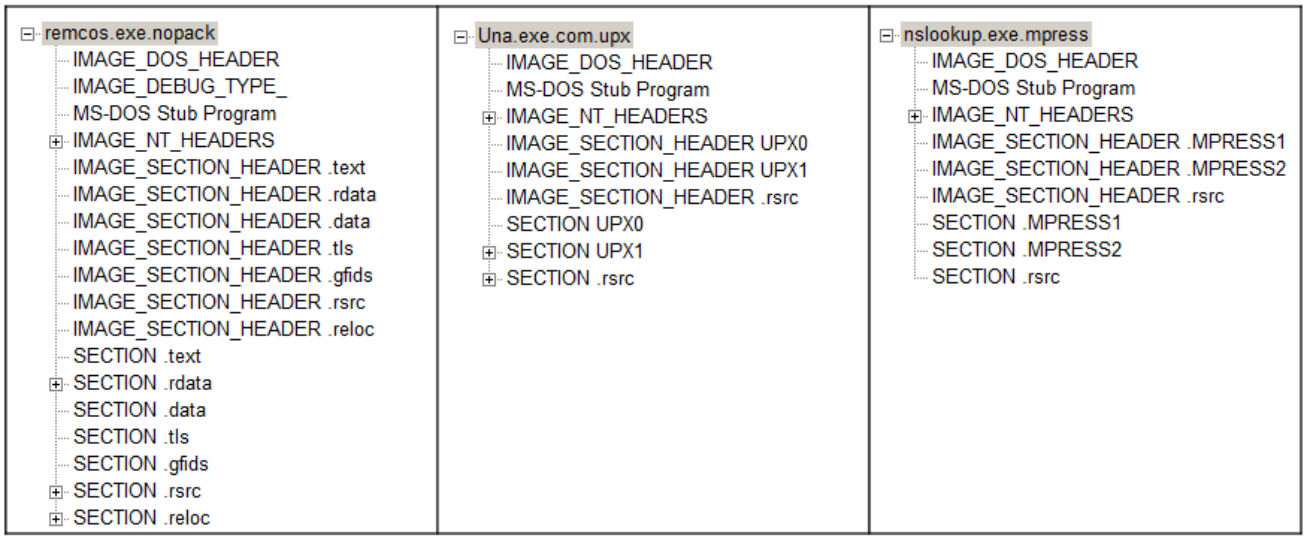


그림13. 원본 샘플, UPX 패킹 샘플, Mpress 패킹 샘플
C2: 146.0.72.170:9094

4. Raccoon Stealer

최근 유포된 Raccoon Stealer의 경우 MalPE 유형의 패커를 사용하여 유포되었다. 과거 Autoit Loader 유형이 아닌 MalPE 유형의 유포에 관련된 내용을 포스팅하였다. 이후로도 종종 MalPE 유형의 악성코드가 유포되었으며 해당 유형은 이메일, 익스플로잇킷 등을 통한 유포에서도 활발하게 사용되는 패킹 유형이다.

다른 외형으로 유포 중인 CryptBot 정보탈취 악성코드 – ASEC BLOG
CryptBot 악성코드는 유틸리티 다운로드 페이지를 위장한 악성 사이트를 통해 유포되는 정보탈취형 악성코드다. 특정 프로그램, 크랙, 시리얼 등의 키워드를 검색 시 관련 유포지가 상단에 노출되며, 해당 페이지에 접속하여 다운로드 버튼을 누를 경우 CryptBot 악성코드 다운로드

페이지로 리디렉트 된다. 악성 사이트는 다양한 키워드로 매우 많은 수량이 개설되어 있다. 대부분의 유명 소프트웨어 키워드를 검색 시 다수의 악성 사이트가 상위 페이지에 노출되며, 관련 파일 탐지 수량 또한 상당하다. 웹 서핑 중 아래와 같은 페이지를 마주…
해당 패킹 유형은 다음과 같이 한 파일 안에 여러 아이콘이 존재하며 리소스 영역에에 랜덤 문자열을 담고 있는 특징이 있다.

그림14. 샘플 내부 리소스의 아이콘
Raccoon Stealer 악성코드 또한 정보 탈취 유형의 악성코드 이며 실제 C2 주소를 얻기 위해 공격자의 텔레그램 주소로 접속 시도한다. 해당 페이지에는 다음과 같이 암호화된 문자열이 명시되어 있으며 해당 문자열을 복호화하여 C2 주소를 구한다.

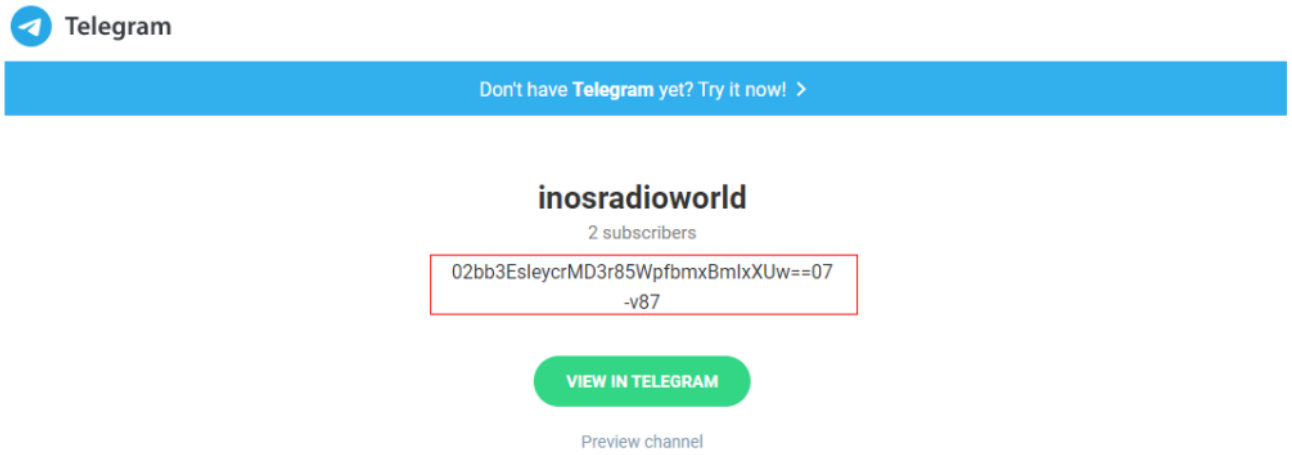


그림15. 공격자 텀블러 페이지
공격자 텀블러 페이지에 명시된 문자열의 앞뒤를 규격에 맞게 잘라 Base64 디코딩 후 RC4 알고리즘을 사용하여 복호화한다. RC4에 대한 키값은 샘플 파일의 rdata 영역에 하드코딩 되어 있다. 이러한 방식으로 공격자는 이미 유포된 샘플의 C2를 지속적으로 변경 가능하다.

```
0007CDB0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0007CDC0  20 20 20 20 00 00 00 00 37 35 61 62 34 64 66 66      ....75ab4dff
0007CDD0  37 31 32 34 62 33 62 38 62 30 63 63 37 63 30 36  7124b3b8b0cc7c06
0007CDE0  38 66 33 33 66 37 61 37 20 20 20 20 20 20 20 20  8f33f7a7
0007CDF0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

그림16. RC4 복호화 키

```
004A7FC8  68 74 74 70 3A 2F 2F 35 2E 31 38 31 2E 31 35 36  http://5.181.156
004A7FD8  2E 36 30 00 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .60(■¿·■¿·■¿·
```

그림17. 복호화 결과

C2: telete.in/inosradioworld / 5.181.156.60

위에서 열거한 악성코드 이외에도 랜섬웨어 등 정보탈취 유형이 아닌 악성코드가 유포된 이력 또한 확인된다. 이처럼 공격자는 다양한 악성코드를 유포하며 그 효과를 테스트 중인 것으로 추정된다. 앞으로도 언제든지 타 악성코드 유포가 가능한 만큼 사용자의 주의가 필요하며 신뢰할 수 없는 페이지로부터 다운로드된 파일은 실행해서는 안된다.

[IOC 정보]

a5bc136c227ab70ed77e3bebe6e4bc6d
21be2e389bc3d34f6a20dad828aa80b2
2349e8337b649af297fe9ef6b99deae5
8680a71a54f5eb063aedc7d8922e031c

gimpimageeditor.com
shpak125.tumblr.com
116.202.183.50
146.0.72.170:9094
telete.in/inosradioworld
5.181.156.60

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보