TLP : GREEN

Lazarus 그룹의 NukeSped 악성코드 분석 보고서

안랩 시큐리티대응센터(ASEC)

2021. 11. 10

AhnLab

문서 등급에 대한 안내

발간물이나 제공되는 컨텐츠는 아래와 같이 문서 등급 별 허가된 범위 내에서만 사용이 가능합니다.

문서 등급	배포 대상	주의 사항
TLP : RED	특정 고객(사)에 한정하여 제공되는 보고서	**보고서 수신자 혹은 수신 부서 만 접근이 허가된 문서** 수신자 외 복제 및 배포 불가
TLP : AMBER	제한된 고객(사)에 한정하여 제공되는 보고서	**보고서 수신 조직(회사) 내부에서는 복제 및 배포 가능** 다만, 조직 외 교육 목적 등을 위해 사용될 경우에는 안랩의 허락 필수
TLP : GREEN	해당 서비스 내 누구나 이용 가능 보고서	**해당 업종 등에서는 자유로운 사용이 가능하며 출처만 밝히면 내부 교육, 동종 업계, 보안 담당자 교육 자료로 활용 가능** 다만, 일반인 대상 발표자료에는 엄격히 제한
TLP : WHITE	자유 이용 가능 보고서	출처표시 상업적, 비상업적 이용 가능 변형 등 2 차적 저작물 작성 가능

일러두기

보고서에 통계와 지표가 포함되어 있는 경우 일부 데이터는 반올림되어
세부 항목의 합과 전체 합계가 일치하지 않을 수도 있습니다.

목차

CAUTION

'본 보고서에는 현재까지 확인한 내용을 기반으로 분석가 의견이 다수 포함되어 있습니다. 분석가들마다 의견이 다를 수 있으며 새로운 근거가 확인되면, 본 보고서 내용도 사전 고지 없이 변경될 수 있습니다.

개요

본 문서는 NukeSped 악성코드에 대한 분석 보고서이다. 2020년경부터 최근까지 Lazarus로 알려진 공격 그룹에 의해 국내 공공기관과 기업들을 대상으로 하는 다수의 공격이 확인되고 있다. 안랩 ASD 인프라의 로그들을 기반으로 과거 감염 사례들을 확인해 보면 공격자는 공공기관 및 대학교들 그리고 다수의 물류, IT, 제조업 기업들을 대상으로 공격을 수행하였다. 각 공격들의 공통점은 동일한 백도어 악성코드가 사용되었다는 점이 있으며, 이 백도어는 일반적으로 Lazarus 그룹의 공격들에서 확인되는 백도어 악성코드들 간의 유사성을 기반으로 했을때 NukeSped로 정리한다.

NukeSped는 Lazarus 그룹이 사용하는 대표적인 백도어 악성코드들로서 C&C 서버로부터 공격자의 명령을 받아 다양한 악성 행위를 수행할 수 있다. 기본적으로 커맨드 라인 명령 외에도 파일 관련 작업을 지원하며, 키로깅 및 스크린 로깅 그리고 탈취 대상 파일을 C&C 서버에 업로드하는 등 일반적인 백도어 악성코드에서 제공하는 대부분의 기능들이 지원된다. 과거 공격들에서 확인된 여러 변종들과 달리 여기에서 확인된 NukeSped는 정적인 또는 기능적인 내용 외에도 바이너리에 포함되어 있는 클래스 이름들을 통해 동일한 악성코드인 것을 확인할 수 있다. 물론 이외에도 진단을 회피하기 위한 목적으로 사용된 자체 패킹 방식이나 감염 이후 동일한 악성코드들을 추가적으로 설치한 점을 통해서도 동일한 공격자에 의한 것임을 추정할 수 있다.

본 문서에서는 NukeSped를 이용한 공격들에 대한 전체적인 흐름을 분석한다. 차례대로 확인된 유포 방식부터 시작하여 NukeSped의 기능들을 분석하고, 공격자로부터 전달받은 명령이나 추가적으로 설치한 악성코드들까지 각 단계별로 상세하게 정리한다.

1. 최초 침투 방식

현재까지 확인된 초기 침투 방식은 크게 2가지이다. 하나는 문서 파일 포맷의 악성코드를 첨부하는 형태의 타겟형 악성 메일을 이용한 방식이며, 다른 하나는 KISA의 "타겟형 워터링홀 공격전략 분석"[1] 보고서에 언급된 워터링홀 공격을 이용한 방식이다.

악성 메일을 이용한 초기 침투 방식은 과거 TI보고서 "워드 문서로 유포된 APT 공격(라자루스) 분석보고서"[2]를 통해 상세하게 다루었기 때문에 여기에서는 간략하게 언급한다. 참고로 해당 보고서에서는 특정 기업을 타겟으로 하는 악성코드들에 대해서만 다루었지만, 여기에서는 해당 공격 외에도 ASD 인프라를 통해 확인된 IOC들 즉 과거 공격에서 사용된 악성코드들을 아래의 IOC 항목에서 추가적으로 정리한다.

1.1. 메일 첨부 문서 파일을 통한 유포 사례

2021년 4월 다수의 워드 문서 파일 악성코드들이 수집되었다. 메일을 통해 유포된 것으로 추정되는 해당 악성코드들은 DOC 형식이며 내부에는 매크로 사용을 유도하는 그림이 포함되어 있다.

[1] https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=36210

[2] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=344495af-919d-49a4-9956-ec2c9ce20819

[그림 1] 매크로 활성화를 유도하는 그림 - 3

매크로 실행 시 악성 행위가 시작됨과 동시에 정상 문서 내용을 출력한다. 해당 문서의 내용은 공격 대상, 즉 특정 기업에 관련한 실제 문서로 구성되어 있다. 악성 매크로는 이미지 변환 기법을 사용하여 악성 PE 바이너리를 로드하는데, 기존에 보고되지 않은 방식으로 많은 이슈가 되었다.

```
Public Function WIA_ConvertImage(sInitialImage As String, sOutputImage As String, Optional lQuality As Long = 85) As Boolean
    On Error GoTo Error_Handler
    Dim oWIA        As Object   'WIA.ImageFile
    Dim oIP     As Object   'ImageProcess
    Dim sFormatID   As String
    Dim sExt        As String
    sFormatID = "{B96B3CAB-0728-11D3-9D7B-0000F81EF32E}"
    sExt = "BMP"
    If lQuality > 100 Then lQuality = 100
    Set oWIA = CreateObject("WIA.ImageFile")
    Set oIP = CreateObject("WIA.ImageProcess")
    oIP.Filters.Add oIP.FilterInfos("Convert").FilterID
    oIP.Filters(1).Properties("FormatID") = sFormatID
    oIP.Filters(1).Properties("Quality") = lQuality
    oWIA.LoadFile sInitialImage
    Set oWIA = oIP.Apply(oWIA)
    oWIA.SaveFile sOutputImage
    WIA_ConvertImage = True
```

[그림 2] 이미지 변환 기법을 이용한 PE 로드

위의 코드는 문서 내부 PNG 파일을 BMP 파일로 변환하는 내용이다. 해당 변환의 결과는 악성 PE 파일 또는 악성 스크립트인데 PE 파일일 경우에는 iexplore.exe 와 같은 이름으로 생성한 후 실행하며, 스크립트의 경우에는 또 다른 PE 악성코드를 디코딩하여 생성한 후 실행하는 기능을 갖는다.

결국 최종적으로 생성 및 실행되는 것은 PE 포맷의 악성코드이며, 해당 악성코드는 외부에서 추가 악성코드를 다운로드 받고 실행하는 기능을 하는 다운로더이다. 해당 악성코드들에 대해서는 아래의 "2.1. 다운로더 #1" 항목에서 다룬다.

참고로 이와 같은 스피어피싱 메일을 이용한 유포 사례는 과거 카스퍼스키의 “Andariel evolves to target South Korea with ransomware” 보고서에도 다루어진 바 있다.[3]

1.2. 워터링홀 공격을 통한 유포 사례

안랩에서는 과거 TI 보고서 "국가 기반시설 타겟 악성코드 분석 보고서"[4]를 통해 특정 공공기관을 대상으로 한 공격에 사용된 악성코드들을 분석하였다. 해당 보고서에서는 최초 침투 방식이 확인되지 않아 이후 과정부터 다루었지만, KISA 보고서 "타겟형 워터링홀 공격전략 분석"에 따르면 공격자는 타겟형 워터링홀 공격을 이용하였으며, 대상 기관이 사용 중인 소프트웨어의 취약점을 이용해 다운로더 악성코드를 설치하였다고 한다. 해당 악성코드에 대해서는 아래의 "2.2. 다운로더 #2" 항목에서 다룬다.

[3] https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

[4] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=15bbe345-5a6c-42f9-8e95-5e69bbb4e137

2. 다운로더

위의 두가지 방식을 통해 설치되는 것은 다운로더 악성코드로서 실제 NukeSped 백도어를 설치하는 기능을 담당한다. 여기에서는 위에서 다룬 각각의 다운로더 악성코드들을 다룬다. 참고로 악성코드 제작자는 파일 진단을 우회하기 위한 목적으로 각각의 파일들을 패킹하여 유포하고 있다. 여기에서 다루는 다운로더 악성코드들뿐만 아니라 뒤에서 다룰 NukeSped 백도어 악성코드들도 모두 유사한 패커가 사용된다는 공통점이 있으며 이에따라 세번째 항목에서는 공통점이라고 할 수 있는 패커를 간략하게 다룬다.

2.1. 다운로더 #1

"1.1. 메일 첨부 문서 파일을 통한 유포 사례" 항목의 문서 파일로부터 실행되는 다운로더 악성코드는 사용되는 API와 DLL 이름 등의 문자열을 암호화하여 저장하고 있다. 또한 두 가지 이상의 C&C 주소를 포함하고 있으며 요청할 때마다 다른 User-Agent를 사용한다. 샘플에 따라서는 시작 프로그램 폴더에 바로가기를 생성하는 경우도 존재한다.

이후 C&C 서버와 연결하여 아래 표와 같이 공격자로부터 전달받은 명령에 따라 다양한 악성 행위를 수행한다.

명령	기능
1111	C&C 접속 간격 설정
1234	쉘코드(다운로드) 및 실행
3333	자가 삭제
4444	특정 포트 스캔
8877	파일 생성(다운로드)
8888	파일 생성(다운로드) 및 실행
9876	자가 종료
9999	CMD 명령어 실행 및 결과 데이터 전송

[표 1] 다운로더 #1의 C&C 명령

본 악성코드의 경우 다양한 기능을 수행할 수 있지만, 결과적으로는 NukeSped 감염을 위한 중간 단계 다운로더의 역할을 위해 해당 악성코드를 사용한 것으로 판단된다. 실제 자사 ASD 인프라의 탐지 로그에 따르면 해당 악성코드가 NukeSped 악성코드를 직접 다운로드하여 실행한 로그를 확인할 수 있다.

다운로더	NukeSped
f3fcb306cb93489f999e00a7ef63536b	4c852d06c4976657ec63e7f618765585

de82e6e3972989f79256056815df4e27	4df757390adf71abdd084d3e9718c153

[표 2] 실제 다운로드 로그가 확인된 샘플셋 예시

2.2. 다운로더 #2

NukeSped는 워드 문서가 아닌 워터링 홀 공격 방식을 통해서도 유포된 바 있다. KISA의 "타겟형 워터링홀 공격전략 분석" 보고서에 따르면 특정 기관에서 사용중인 소프트웨어 취약점으로 인하여 다운로더(TigerDownloader)가 최초로 설치되었고 다운로더에 의해 실제 백도어 행위를 수행하는 NukeSped(TigerRAT)가 실행되었다고 한다.

안랩에서는 당시 최초 침투 방식은 확인할 수 없었지만, 다운로더에 의해 NukeSped가 설치되는 정황은 안랩 ASD 인프라를 통해 확인이 가능하였다. 최초로 설치된 다운로더는 C&C 서버와 통신하며 공격자 명령을 받아 파이프 통신으로 다양한 명령을 수행한다. 다운로더가 실행되면 우선 감염된 시스템의 사용자 이름, 컴퓨터 이름, MAC 및 IP 정보 등 기본적인 정보를 Base64 인코딩하여 다음과 같은 형태로 C&C 서버에 전송한다.

```
fn_GetUserName();
fn_GetComputerName(v7);
fn_GetAdaptersInfo();
fn_vsprintf(data_Info, "%s%d%s", "Tiger", 101, str_MAC);
wcslen(word_41E76E);
v1 = (char *)fn_base64(&v7);
strcat_s(data_Info, 0x410u, "|");
strcat_s(data_Info, 0x410u, v1);
j___free_base(v1);
wcslen(Destination);
v2 = (char *)fn_base64(&v7);
strcat_s(data_Info, 0x410u, "|");
strcat_s(data_Info, 0x410u, v2);
j___free_base(v2);
wcslen(word_41E976);
v3 = (char *)fn_base64(&v7);
strcat_s(data_Info, 0x410u, "|");
strcat_s(data_Info, 0x410u, v3);
j___free_base(v3);
wcslen(word_41EB7E);
v4 = (char *)fn_base64(&v7);
strcat_s(data_Info, 0x410u, "|");
strcat_s(data_Info, 0x410u, v4);
j___free_base(v4);
wcslen(word_41ED86);
v5 = (char *)fn_base64(&v7);
strcat_s(data_Info, 0x410u, "|");
strcat_s(data_Info, 0x410u, v5);
j___free_base(v5);
dword_41F6B4 = strlen(data_Info);
```

[그림 3] 탈취한 정보를 Base64 인코딩하는 과정

- Tiger101"MAC주소"| "사용자 이름" | "컴퓨터 이름" | "AAA=" | "IP 주소" | "MAC 주소"

C&C 서버에 감염 시스템 정보 전송이 끝나면 다운로더는 공격자로부터 명령을 전달받아 추가 악성 행위를 수행할 수 있다.

명령	기능
o	CMD 명령 수행
p	파일 업로드
q	파일 다운로드
r	현재 스레드 종료
s	C&C 업데이트 (config 파일 수정)

[표 3] 다운로더 #2의 C&C 명령

악성코드는 최초로 접속하는 C&C 서버 주소를 난독화하여 시스템의 %TEMP% 경로에 "lnk{22A98A71-67ED-40BB-A5F4-8CCAF6BFA6EB}.tmp" 데이터 파일로 저장하는데, C&C 주소 정보가 업데이트될 경우 기존에 저장된 내용을 지우고 새로운 C&C 정보를 난독화하여 저장한다.

C&C URL
- hxxp://34.221.66[.]33/StSess_Update.php
- hxxp://34.221.66[.]33/ASDClient.php
- hxxp://34.221.66[.]33/Semenser.php

관련해서 악성코드가 C&C 정보를 업데이트 하는 과정을 분석한 결과에 따르면 C&C의 도메인 주소는 동일하고 URI만 계속해서 바꿔 저장하는 구조이다. 다음 URL 목록은 안랩 ASD 인프라에서 확인된 call.exe, ais.exe, lsdev.exe 추가 파일이 다운로드된 URL 정보이다.

NukeSped 다운로드 URL
- hxxp://34.221.66[.]33/call.exe
- hxxp://34.221.66[.]33/AIS.exe
- hxxp://34.221.66[.]33/msdev.exe
- hxxp://34.221.66[.]33/lsdev.exe

2.3. 패커

현재까지 유포된 NukeSped 관련 파일들의 외형을 보면 모두 유사한 패커를 사용한다는 공통점이 있다. 이는 위에서 다룬 2개의 다운로더들 뿐만 아니라 NukeSped 백도어도 동일하다. 다수의 악

성코드들이 존재하지만 여기에서는 특정 샘플을 기준으로 관련 내용을 분석한다.

해당 패커는 먼저 안티 바이러스의 파일 진단을 우회하기 위해 다음 그림과 같이 사용자 정의 함수 중간에 악성 행위 동작과 관련이 없는 가비지 API(Garbage API)들을 삽입하였다.

```
GetWindowRect(0, &Rect);                        // Garbage API
dword_4261DC = dword_426310 * dword_4260D8;
dword_426F24 = dword_426F90 + dword_426EC4;
ModuleHandleA = GetModuleHandleA(0);            // Garbage API
DC = GetDC((HWND)ModuleHandleA);                // Garbage API
SetRect(&Rect, 10, 10, 100, 30);                // Garbage API
FillRect(DC, &Rect, (HBRUSH)6);                 // Garbage API
v4 = GetModuleHandleA(0);
ReleaseDC((HWND)v4, DC);                        // Garbage API
dword_42612C = dword_4261F4 * dword_4260C0;
dword_426F18 = dword_426E80 | dword_426D5C;
GetParent(0);                                   // Garbage API
```

[그림 4] 가비지 API 루틴

NukeSped 관련 악성코드들의 외형은 시그니처 진단 우회 시도뿐만 아니라 안티 샌드박스(Anti Sandbox) 기능도 존재한다. 현재 자신의 프로세스에 로드된 모듈 중 sbiedll.dll, api_log.dll, dir_watch.dll 라는 이름의 DLL 모듈이 존재하는지 확인하고 만일 존재할 경우 안티 샌드박스 환경에서 동작 중인 것으로 간주하고 즉시 종료된다. 이때 검사 대상 문자열인 DLL 모듈의 이름은 모두 하드코딩된 XOR 연산으로 암호화 상태로 저장되는 것이 특징이다.

```
dword_425BA8 = 52;
v15 = 0x4D48315A;                               // 0x5A31484D281D444557225B -> XOR Key
v16 = 0x45441D28;
v17 = 0x5B2257;
dword_426D38 = dword_426F24 + dword_426C20;
strcpy(v14, ")S!(Lq(k3N7XnlXF");
memset(FileName, 0, 0x7D0u);
v0 = 0;
dword_426F6C = dword_426CD8 + dword_426C94;
for ( i = 0; i < 11; ++i )
{
  v2 = v14[v0++];
  FileName[i] = *((_BYTE *)&v15 + i) ^ v2;
  if ( v0 == 15 )
    v0 = 0;
}
ModuleHandleA = GetModuleHandleA(FileName);   // sbiedll.dll
```

[그림 5] 패커의 안티 샌드박스 루틴

시그니처 및 샌드박스 탐지 우회 루틴이 끝나면 악성코드는 파일의 끝 더미 데이터에 암호화 상태로 저장된 실제 백도어 악성코드를 메모리 상에서 실행한다. 파일 끝 더미 데이터 구성은 다음 그림과 같다. 더미 데이터는 백도어 악성코드의 실제 크기 4바이트, 복호화 키 16바이트, 암호화 데이터를 포함하고 있으며 RC4 알고리즘으로 암호화 되어있다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00023FD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00023FE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00023FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00024000	00	D4	01	00	29	53	21	28	4C	71	28	6B	33	4E	37	58
00024010	6E	6C	58	46	00	CC	D9	A8	21	6F	4C	52	8D	76	43	F2
00024020	5C	FA	E4	A8	8A	E1	4F	17	81	B0	56	43	E2	D7	C7	77
00024030	77	47	F4	20	F9	C0	74	20	A6	54	2E	B0	2E	27	64	31

[그림 6] 설정 데이터

바이트	데이터 의미
0x1D400	복호화 데이터 크기
0x29 0x53 0x21 0x28 0x4C 0x71 0x28 0x6B 0x33 0x4E 0x37 0x58 0x6E 0x6C 0x58 0x46	RC4 복호화 키
0xCC 0xD9 0xA8 0x21 0x6F 0x4C 0x4C 0x52 0x8D 0x76 0x43 0xF2 0x5C …	RC4로 암호화된 백도어 악성코드

[표 4] 원본 악성코드 복호화를 위한 설정 데이터

```
dword_426D10 = dword_426F1C ^ dword_426C68;
v12 = v1;
v11 = 16;
memset(v9, 0, sizeof(v9));
unknown_libname_11(v9);
dword_426928 = dword_426B14 + dword_426810;
for ( i = 0; i < 256; ++i )
  v10[i] = i;
v13 = v10;
qmemcpy(v12, v10, 0x100u);
v3 = v12;
*((_WORD *)v12 + 0x80) = 0;
v4 = 0;
v5 = 0;
v6 = 0;
do
{
  v7 = v3[v5];
  LOWORD(v6) = (unsigned __int8)(*(_BYTE *)(a1 + v4) + v7 + v6);
  v3[v5] = v3[v6];
  v3[v6] = v7;
  ++v5;
  v4 = (unsigned __int16)((unsigned __int16)(v4 + 1) % (unsigned __int16)v11);
}
while ( !BYTE1(v5) );
dword_426FF4 = dword_426E00 * dword_426D2C;
return GetSysColorBrush(2);
```

[그림 7] 원본 악성코드를 디코딩하는 루틴

여기까지의 과정이 끝나면 복호화되는 원본 악성코드를 메모리 상에서 실행 가능하도록 IAT(Import Address Table)를 보정하고, 메모리 재배치 과정을 거친 뒤 실제 원본 악성코드를 실행한다.

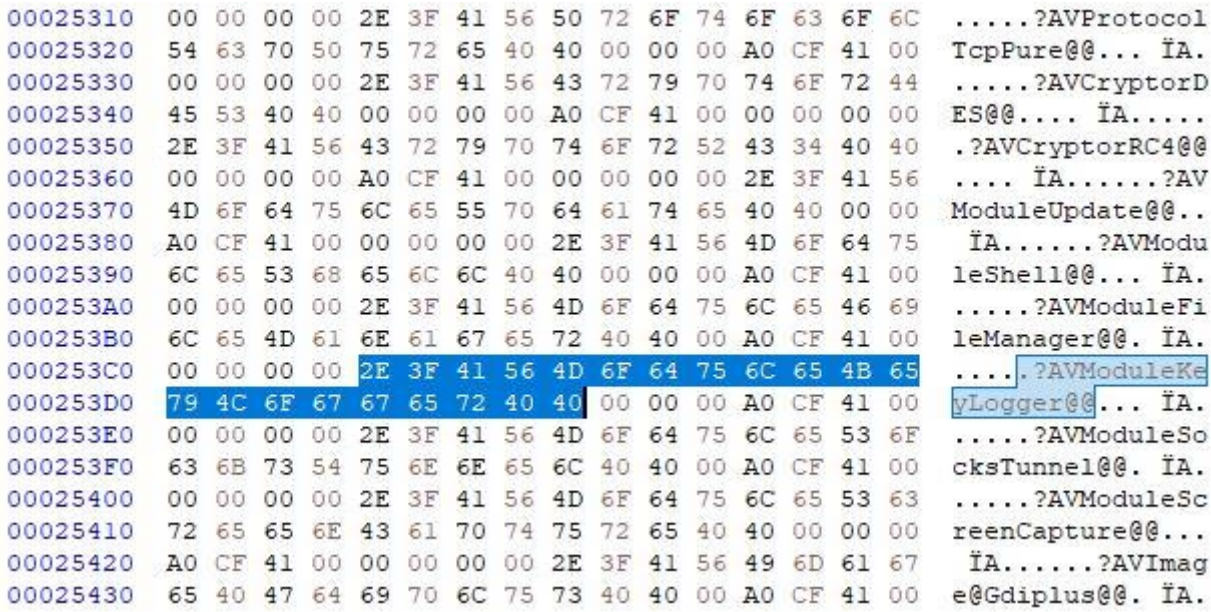
3. NukeSped 분석

3.1. 특징

NukeSped는 C&C 서버에서 공격자의 명령을 전달받아 수행할 수 있는 백도어 악성코드이며 현재까지 다양한 형태로 확인되고 있다.

여기에서 다루는 분석 대상은 NukeSped 백도어 변종들 중 하나이며 최소 2020년부터 최근까지 확인되고 있다. 해당 변종의 특징이라고 한다면 C++로 개발되어 있으며 가상 함수를 사용함에 따라 다음과 같은 클래스 이름들이 바이너리에 포함되어 있다는 점이다. 아래는 현재 분석 대상 샘플을 기준으로 하며, NukeSped 샘플들에 따라 키로깅이나 Socks 프록시 등과 같은 다른 기능들이 더 추가되어 있거나 존재하지 않는 경우도 있다. 각각의 기능들은 아래의 기능 분석 항목에서 다룬다.

```
ProtocolTcpPure
CryptorDES
CryptorRC4
ModuleUpdate
ModuleShell
ModuleFileManager
ModuleScreenCapture
```



[그림 8] 바이너리에 하드코딩되어 있는 클래스 이름들

이외에도 ProtocolTcpPure 클래스를 보면 알 수 있듯이 Raw TCP 프로토콜을 이용해 C&C 서버와 통신한다. 그리고 대부분의 NukeSped 변종들과 달리 추가적인 데이터 파일을 필요로 하지 않아 실행 파일 단독으로 악성 행위를 수행할 수 있다.

3.2. C&C 통신

초기 버전에서는 주로 1개의 C&C 서버 주소가 사용되었으며, 이후 평균 3-4개의 C&C 서버가 사용되고 있다. 하지만 대부분의 경우 3-4개를 지원한다고 하더라도 동일한 C&C 서버 주소를 사용하기 때문에 실질적으로 1개의 C&C 서버를 포함하는 샘플이 다수이다. 현재 바이너리의 경우도 3개의 C&C 서버만 설정되어 있고 모두 동일한 주소인 "23.229.111[.]197"이다.

NukeSped는 복호화한 순서대로 각각의 C&C 서버에 접속하는데, 접속 실패할 경우에는 다음 주소를 사용한다. C&C 서버는 대부분 IP 포맷이지만 도메인 포맷도 지원한다. 물론 보조용 C&C 서버로 도메인 포맷을 지원하는 경우가 대부분이며 IP 포맷의 C&C 서버를 최소한 1개 이상 포함하고 있다.

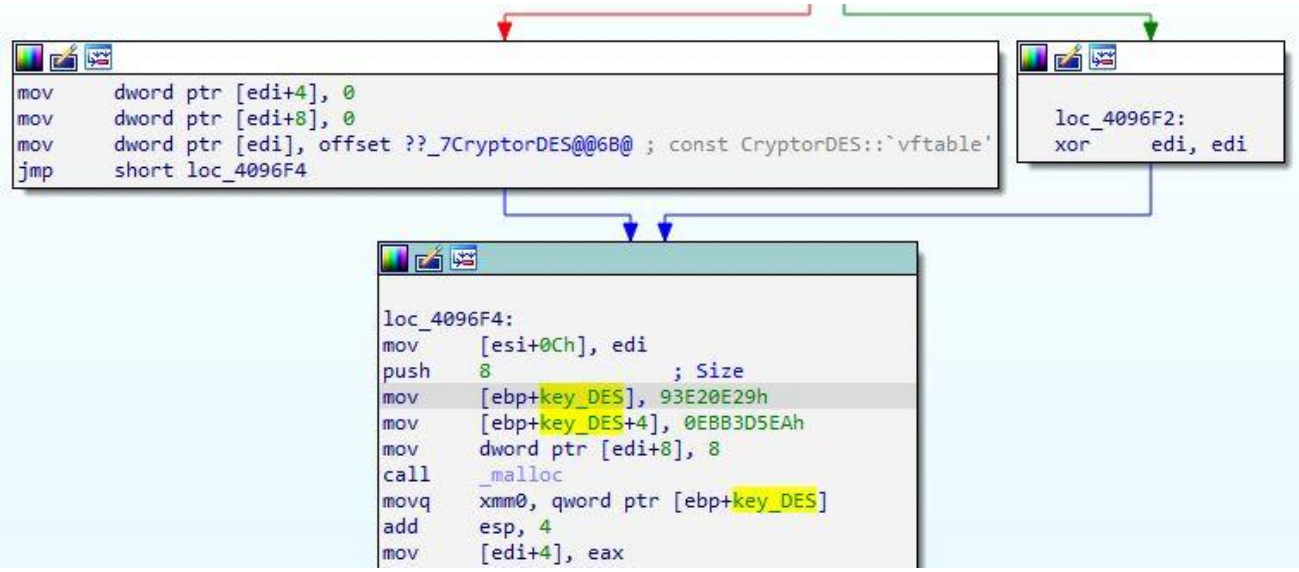
특이사항이 있다면 사설망 IP 주소를 C&C 주소로 갖는 샘플도 확인되며, 비정상적인 주소들도 존재한다. 실제 file.naverapi[.]com은 다른 NukeSped에서도 사용되기 때문에 file.naverapi는 제작자의 실수로 추정된다.

- **사설망 C&C 주소** : 10.101.30[.]127:443

- **제작자의 실수로 추정되는 C&C 주소** : app.naverapi:443 , file.naverapi:443

각각의 C&C 서버에 대한 포트 주소들은 암호화 없이 하드코딩되어 있으며, C&C 서버의 주소는 DES ECB 알고리즘을 이용해 인코딩되어 있다. 해당 샘플의 경우 복호화를 위한 키 값은 다음과 같다.

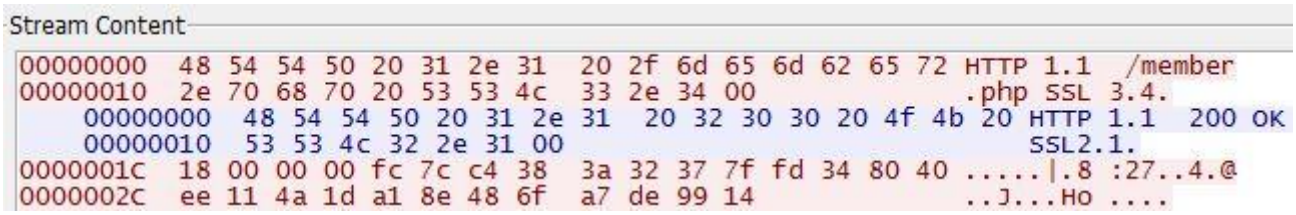
- **DES Key** : 29 0E E2 93 EA D5 B3 EB



[그림 9] 하드코딩되어 있는 DES 키

이후 API Resolving 과정을 진행하는데, 각 클래스 별로 사용할 문자열들과 API 이름을 앞의 과정과 동일한 DES 암호화 과정을 거쳐 복호화한다.

여기까지의 과정이 끝나면 C&C 서버와 통신을 시도한다. 접속이 이루어진 후에는 검증 과정을 진행하는데, C&C 서버에 "HTTP 1.1 /member.php SSL3.4" 문자열을 전송한 후 "HTTP 1.1 200 OK SSL2.1"를 전달받을 경우에만 실제 C&C 서버로 인식하고 이후 통신을 진행한다.



[그림 10] C&C 서버와의 인증 과정

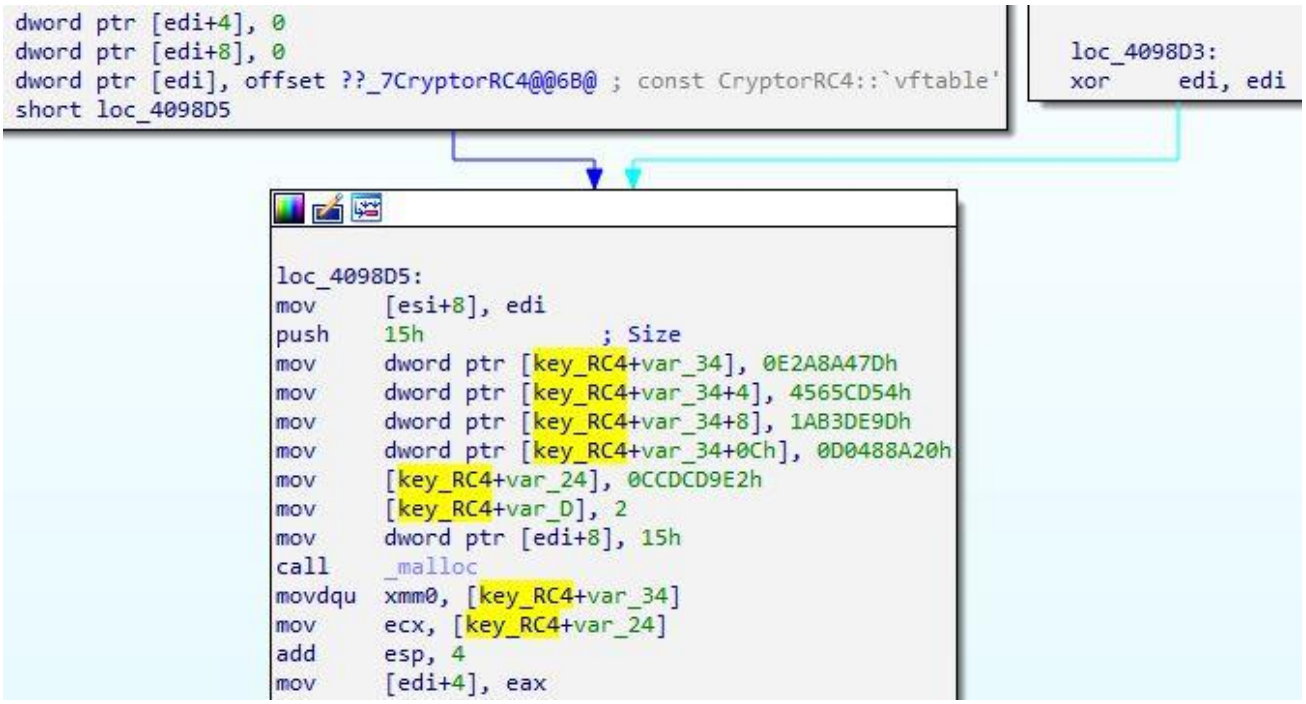
참고로 모든 샘플들에서 동일한 검증 문자열들이 사용되는 것은 아니며, 특정 샘플들의 경우 "HTTP 1.1 /index.php?member=sbi2009 SSL3.3.7" 문자열을 C&C 서버에 전송한다. C&C 서버

로부터 전달받는 문자열은 확인된 샘플들 모두 동일하게 "HTTP 1.1 200 OK SSL2.1"이다.

여기에서 다루는 변종들은 8080번 포트를 사용하는 몇 개를 제외하면 대부분 C&C 서버의 포트 번호가 443 또는 8443이다. 즉 위와 같은 과정을 거치는 이유는 C&C 서버 검증 외에도 HTTPS 통신을 위장하기 위한 목적도 포함하는 것으로 추정된다.

인증 과정이 끝나면 먼저 이전에 구했던 MAC 주소를 포함한 데이터를 RC4 알고리즘으로 인코딩한다. 여기서 다루는 NukeSped는 C&C 통신에 RC4 암호화를 이용하는데, 전달할 데이터 외에 전달받은 데이터도 RC4로 암호화하여 통신한다.

- **RC4 Key** : 7D A4 A8 E2 54 CD 65 45 9D DE B3 1A 20 8A 48 D0 E2 D9 DC CC 02



[그림 11] 하드코딩되어 있는 RC4 키

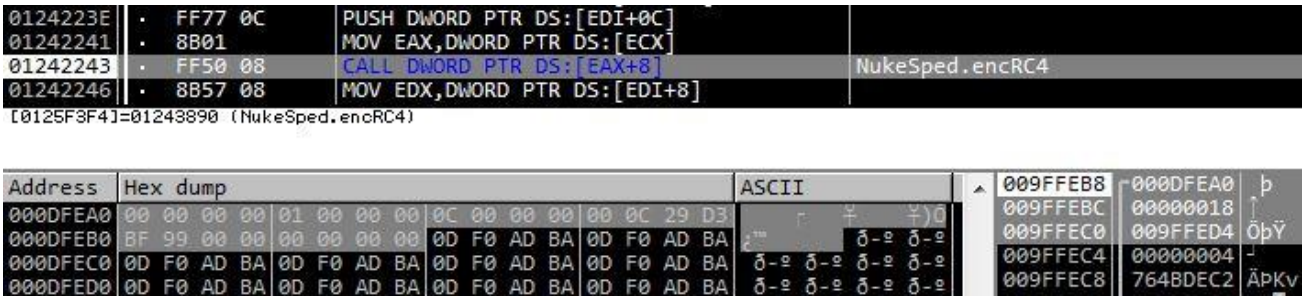
패킷의 경우 2개의 파트로 이루어져 있는데 처음 4바이트는 본문의 사이즈이며 해당 사이즈만큼 RC4로 인코딩된 데이터가 포함되어 있다.

최초 접속 시 전달 패킷
- Size : 18 00 00 00
- Encoded Data : B4 EB 78 2C 6B 58 A6 98 33 A3 0D F7 97 F9 73 4A C1 42 EA 3D 2A 33 5F 79

인코딩된 데이터는 다음과 같은 구조를 갖는다. 0x00으로 채워진 처음 4바이트는 사용되지 않으며

이후 전달할 데이터의 종류와 사이즈 그리고 데이터이다. 아래의 데이터는 위에서 언급한 MAC 주소이다.

최초 접속 시 전달 데이터
- Unused : 00 00 00 00
- Type : 01 00 00 00
- Size : 0c 00 00 00
- Data : 00 0c 29 d3 bf 99 00 00 00 00 00 00



[그림 12] RC4 암호화되기 전의 데이터

이후 주기적으로 C&C 서버와의 통신을 유지하기 위해 스레드를 생성하여 15초 간격으로 다음과 같은 데이터를 전달한다.

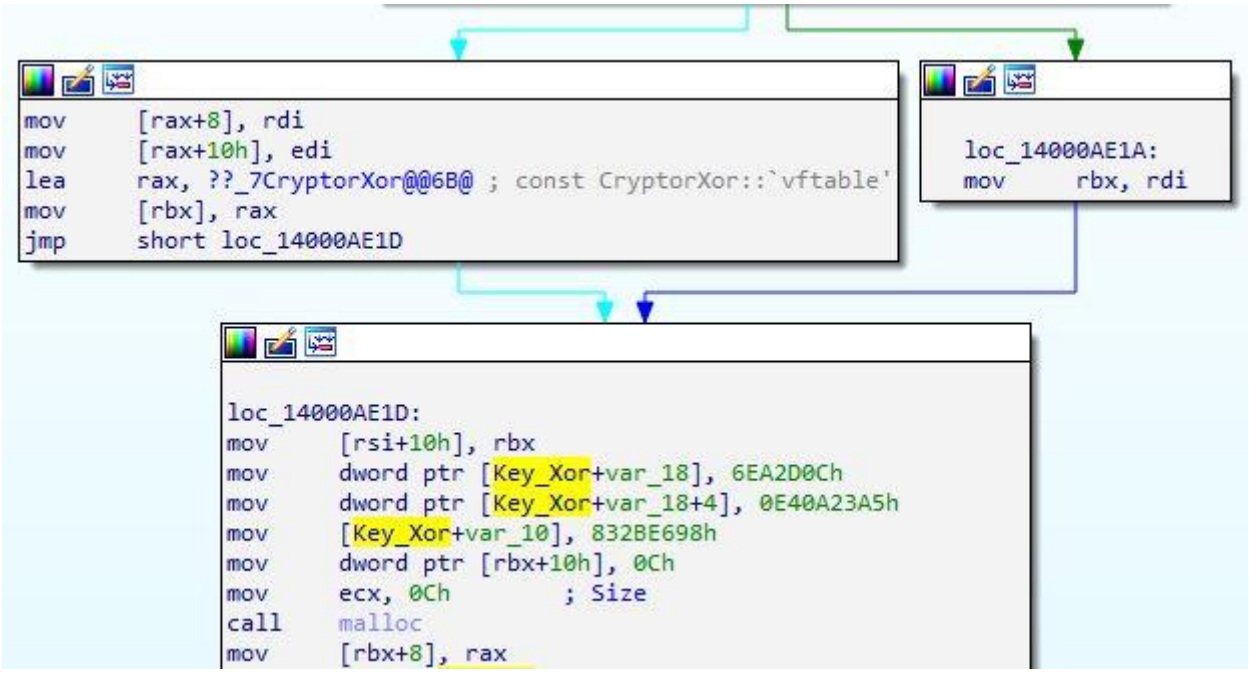
15초 간격으로 패킷 전송
- Size : 0C 00 00 00
- Encoded Data : 65 ED 7C C6 3F A3 22 48 1A D0 E6 0C

최초 접속 시에는 0x00000001 명령이 전달되었다면, 15초 간격으로 전달하는 명령은 0x00000010이며 데이터는 존재하지 않는다.

15초 간격으로 전달하는 데이터
- Unused : 00 00 00 00
- Type : 10 00 00 00
- Size : 00 00 00 00

참고로 악성코드 56283a2c2fd2b72991929e020f37cb05 (내부 PE : 2c93bcf8285c7a956e7f73afe7b56f30)의 경우 CryptorDES 클래스 대신 CryptorXor 클래스가 존재한다. CryptorXor 클래스는 이름과 같이 Xor 알고리즘을 이용해 데이터를 암호화하는 메소드를 지원한다. 대부분의 경우 API 이름을 포함한 내부 문자열, C&C 서버 목록은 DES 알고리즘으로 복호화하여 사용하지만 해당 악성코드는 RC4 알고리즘을 이용한다. 대신 C&C 서버와의 통신에 RC4 알고리즘 대신 Xor 암호화를 이용한다.

- XOR Key : 0C 2D EA 06 A5 23 0A E4 98 E6 2B 83



[그림 13] 하드코딩되어 있는 Xor 키

3.3. 기능 분석

이후 C&C 서버로부터 전달받는 패킷도 동일하게 RC4로 인코딩되어 있으며 동일한 포맷을 갖는다. NukeSped는 전달받은 명령에 따라 키로깅, 스크립 캡쳐, 파일 및 쉘 작업을 수행할 수 있는데, 해당 기능들은 다음 클래스들에 존재한다.

```
ModuleUpdate
ModuleShell
ModuleFileManager
ModuleKeyLogger
ModuleSocksTunnel
ModuleScreenCapture
ModuleInformation
ModulePortForwarder
```

참고로 현재 분석 대상 샘플에는 몇 개의 클래스가 존재하지 않지만 다수의 샘플에서 ModuleInformation 클래스가 확인되며, ModulePortForwarder 클래스의 경우에도 특정 샘플들에서 확인된다.

a. ModuleUpdate

이름은 ModuleUpdate지만 기능적으로는 자가 삭제 기능만을 수행한다. 현재 실행 중인 악성코드 및 Batch 파일을 삭제하는 명령을 담고 있는 Batch 파일을 %TEMP%₩edg88DE.bat 경로에 생성하고 실행한다.

edg88DE.bat ×

H: > output > edg88DE.bat

```
1   @echo off
2   :L1
3   del "C:\Users\test\Desktop\malware.exe"
4   if exist "C:\Users\test\Desktop\malware.exe" goto L1
5   del "C:\Users\test\AppData\Local\Temp\edb88DE.bat"
6
```

[그림 14] 생성된 Batch 파일

b. ModuleShell

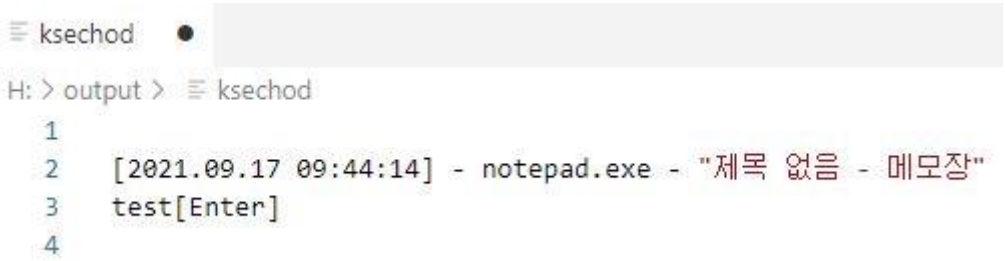
- 현재 작업 경로 구하기 : 현재 작업 경로를 구해 C&C 서버에 전달한다.
- 현재 작업 경로 설정 : 전달받은 경로로 현재 작업 경로를 설정한다.
- 스캐닝 : 전달 받은 주소에 대해 접속 가능 여부를 확인하고 결과를 C&C 서버에 전송한다.
- 명령 수행 : 전달받은 명령을 cmd.exe를 이용해 수행하고 결과를 C&C 서버에 전송한다.

c. ModuleFileManager

- 파일 시스템 정보 획득 : 현재 파일 시스템에 존재하는 각각의 드라이브에 대해 드라이버 타입, 가용 용량, 디스크 볼륨 정보를 수집해 전달한다.
- 파일 정보 획득 : 전달받은 경로의 파일에 대한 정보들을 수집하여 전달한다.
- 폴더 정보 획득 : 전달받은 경로 내의 파일들에 대한 정보들을 수집하여 전달한다.
- 폴더 조회 : 전달받은 경로 내에 존재하는 폴더 및 파일 개수 그리고 전체 용량을 전달한다.
- 파일 다운로드 : 전달받은 데이터를 지정한 경로에 쓴다.
- 파일 삭제 : 전달받은 경로의 파일을 삭제한다.
- 파일 업로드 : 전달받은 경로의 파일을 C&C 서버에 업로드한다.
- 폴더 업로드 : 전달받은 경로 내의 파일들을 C&C 서버에 업로드한다.
- 파일 실행 : 전달받은 경로의 파일을 실행한다.

d. ModuleKeyLogger

키로깅은 GetAsyncKeyState() 함수를 이용하며 키로깅된 로그 데이터는 %LOCALAPPDATA%₩ksecshod 경로에 저장된다. 아래의 그림과 같이 키로깅 문자열 외에도 날짜 및 시간, 키 입력 대상 프로세스의 이름 및 윈도우 타이틀 이름이 함께 저장된다.



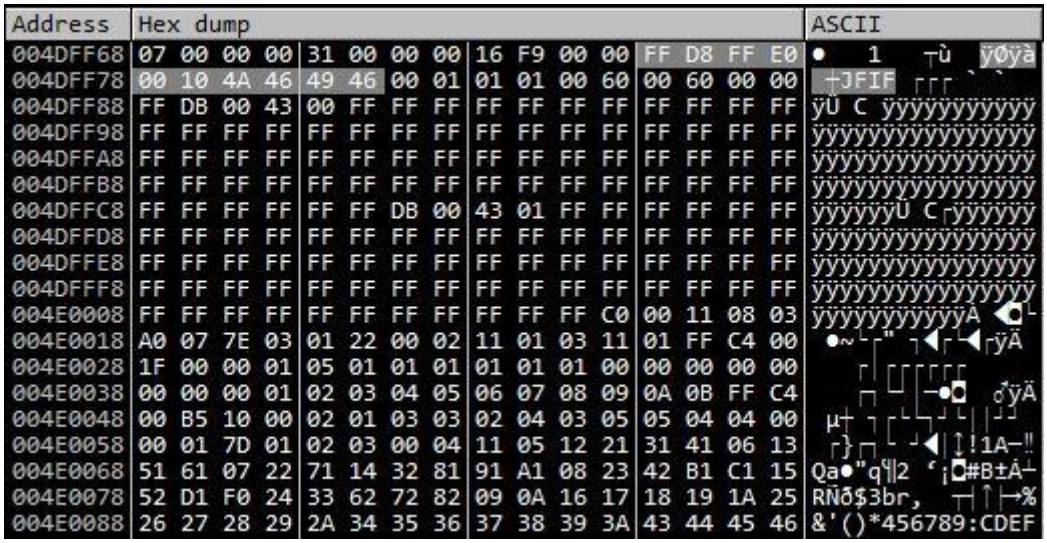
[그림 15] ksechod 파일에 저장된 키로깅 데이터

e. ModuleSocksTunnel

ModuleSocksTunnel 클래스에서는 이름과 같이 터널링 기능을 제공할 것으로 추정된다. C&C 서버로부터 특정 주소를 전달 받고 연결을 확립한 후 C&C 서버와 해당 주소 간의 프록시로서 동작한다. 즉 C&C 서버로부터 전달받은 데이터를 목적지에 전달하고, 목적지에서 전달받은 데이터를 C&C 서버에 전달해주는 역할을 한다. 이를 통해 공격자는 새로운 공격 대상에 직접 통신하는 대신 NukeSped를 통해 원격지에 접근이 가능하게 된다.

f. ModuleScreenCapture

현재 화면에 대한 스크린 캡쳐를 찍어 C&C 서버에 전송한다.



Address	Hex dump																ASCII
004DFF68	07	00	00	00	31	00	00	00	16	F9	00	00	FF	D8	FF	E0	• 1 ┬ù ÿØÿà
004DFF78	00	10	4A	46	49	46	00	01	01	01	00	60	00	60	00	00	┼JFIF ┌┌┌ ` `
004DFF88	FF	DB	00	43	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÛ C ÿÿÿÿÿÿÿÿÿÿÿÿ
004DFF98	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
004DFFA8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
004DFFB8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
004DFFC8	FF	FF	FF	FF	FF	FF	DB	00	43	01	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÛ C┌ÿÿÿÿÿÿ
004DFFD8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
004DFFE8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
004DFFF8	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
004E0008	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	C0	00	11	08	03	ÿÿÿÿÿÿÿÿÿÿÿÀ ◘└
004E0018	A0	07	7E	03	01	22	00	02	11	01	03	11	01	FF	C4	00	•~└┘" ┐◄┌◄┌ÿÄ
004E0028	1F	00	00	01	05	01	01	01	01	01	01	00	00	00	00	00	▼ ┌┌┌┌┌┌
004E0038	00	00	00	01	02	03	04	05	06	07	08	09	0A	0B	FF	C4	┌┐└ ─•◘ ♂ÿÄ
004E0048	00	B5	10	00	02	01	03	03	02	04	03	05	05	04	04	00	µ┼ ┐ └┌┬┘└┘ ┘└┘
004E0058	00	01	7D	01	02	03	00	04	11	05	12	21	31	41	06	13	┌}┌┐└ ┘◄┘↕!1A─‼
004E0068	51	61	07	22	71	14	32	81	91	A1	08	23	42	B1	C1	15	Qa•"q¶2 ‘¡◘#B±Á┴
004E0078	52	D1	F0	24	33	62	72	82	09	0A	16	17	18	19	1A	25	RÑð$3br, ┼↑├→%
004E0088	26	27	28	29	2A	34	35	36	37	38	39	3A	43	44	45	46	&'()*456789:CDEF

[그림 16] jpg 포맷으로 저장된 스크린 캡쳐

g. ModuleInformation

- 컴퓨터 이름 : 현재 감염 시스템의 컴퓨터 이름을 C&C 서버에 전송한다.
- 사용자 이름 : 현재 사용자 이름을 C&C 서버에 전송한다.
- 시스템 정보 : 윈도우 버전 정보 및 GetNativeSystemInfo() API를 이용해 수집한 정보를 C&C 서버에 전송한다.
- 어댑터 정보 : GetAdaptersInfo() API를 이용해 수집한 정보를 C&C 서버에 전송한다.

h. ModulePortForwarder

ModulePortForwarder 클래스에서는 이름과 같이 포트 포워딩 기능을 지원한다. C&C 서버로부터 전달받는 명령 중에는 먼저 리스닝할 포트 번호가 있으며 해당 포트에 대해 리스닝하며 대기한다. 이후 외부에서 해당 포트로의 연결이 확립되면, C&C 서버로부터 전달받았던 특정 호스트의 주소와 연결하여 2개의 호스트 사이에서 데이터를 전달한다. 일반적으로 포트 포워딩은 외부와 사설 네트워크에 존재하는 특정 주소와의 통신을 포워딩해주는 기능이다. 이에따라 외부에 존재하는 공격자는 포트 포워딩 기능을 지원하는 NukeSped를 통해 감염 시스템 내부 즉 사설 네트워크에 존재하는 공격 대상과 통신했을 것으로 추정된다.

4. 감염 이후

NukeSped는 백도어 악성코드임에 따라 위에서 언급한 다양한 공격자의 명령들을 수행할 수 있다. 여기에서는 공격자의 명령을 받아 NukeSped가 수행한 이력이 있는 커맨드 라인 명령과, NukeSped가 추가적으로 설치한 이력이 확인되는 또는 추정되는 악성코드들을 정리한다.

생성하는 악성코드들 중에는 정보 탈취, 포트 스캐닝, 포렌식 및 분석 방해를 목적으로 하는 악성코드들이 확인된다.

참고로 아래에서 다루지는 않지만 새로운 버전의 NukeSped로 업데이트하고, ModuleUpdate 클래스의 기능을 이용해 자가 삭제하는 이력도 함께 확인된다.

4.1. NukeSped 명령

여기에서는 공격자로부터 전달 받은 커맨드 라인 명령들 즉 ASD 인프라에서 확인되는 NukeSped가 실행한 커맨드 라인 명령들을 다룬다. 명령들은 크게 설치 과정에서 사용되는 파일 복사 및 현재 실행 프로세스를 확인하는 명령들이 있으며, 기본적인 정보 수집을 위해 사용한 ipconfig, systeminfo, net과 같은 명령들이 있다. 그리고 NukeSped에서는 지속성 유지를 위한 기능이 존재하지 않기 때문에 직접 커맨드 라인 명령을 이용해 작업 스케줄러에 등록시키는 명령들도 확인된다.

a. 설치 과정

```
> cmd.exe /c "copy svchost.exe c:₩windows₩system32₩synctask.exe"
> cmd.exe /c "dir "c:₩users₩%USERNAME%₩documents₩rsupport₩remotecall₩received files""
> cmd.exe /c "dir *.exe"
> cmd.exe /c "move c:₩programdata₩acwinrt.exe c:₩windows₩apppatch₩apppatch64₩acwinrt.exe"
> cmd.exe /c "tasklist"
> cmd.exe /c "tasklist | findstr acwinrt"
```

b. 정보 수집

```
> cmd.exe /c "ipconfig /all"
```

```
> cmd.exe /c "whoami"
> cmd.exe /c "systeminfo"
> cmd.exe /c "net user"
> cmd.exe /c "net user user"
> cmd.exe /c "netstat -naop tcp"
```

c. 작업 스케줄러 등록

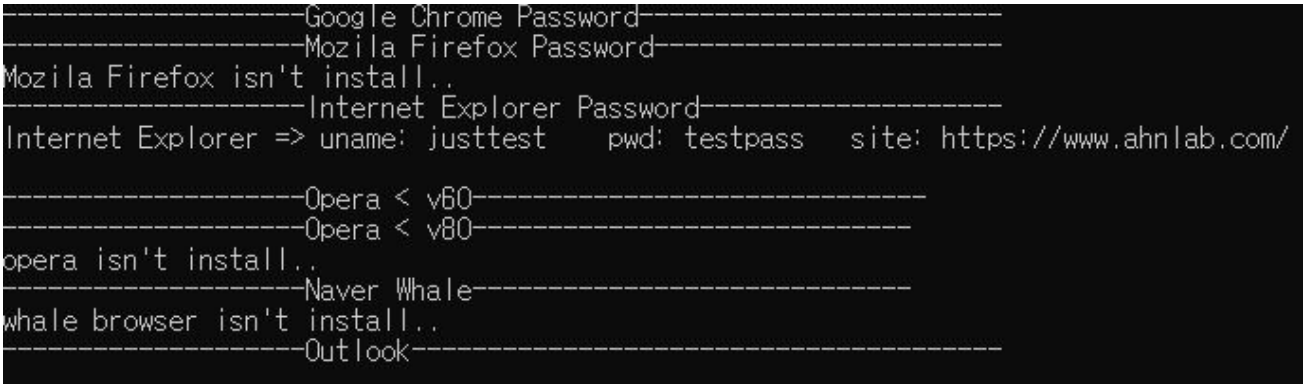
```
> schtasks /create /tn "ahnlab₩asdclient" /tr "c:₩programdata₩ahnlab₩ais₩asdcli.exe" /sc daily /st 09:35:20 /ru 231946
> schtasks /create /tn "microsoft₩windows₩performance₩winsat" /tr c:₩windows₩performance₩winsat₩winsat.exe /sc daily /st 10:25:00 /ru chamoil
> schtasks /delete /tn "microsoft₩windows₩appid₩acwinrt" /f
> schtasks /run /tn "microsoft₩windows₩appid₩acwinrt
```

4.2. 추가 악성코드 생성

4.2.1. 웹 브라우저 및 아웃룩 계정 정보 탈취

NukeSped는 백도어이다 보니 정보 탈취와 관련된 기능들이 충분히 존재하지는 않는다. 공격자는 추가적인 정보를 수집하기 위해 다른 인포스틸러 악성코드처럼 웹 브라우저들과 아웃룩 클라이언트에 저장되어 있는 사용자의 계정 정보를 탈취하는 악성코드를 사용했다.

해당 악성코드는 크롬, 파이어폭스, 인터넷 익스플로러, 오페라, 네이버 웨일 웹 브라우저 및 아웃룩 클라이언트에서 사용자의 계정 정보를 탈취한 후 커맨드 라인으로 출력해 주는 악성코드이다. 공격자는 NukeSped를 이용해 해당 악성코드의 출력 결과를 수집해 C&C 서버로 전달했을 것으로 추정된다.



[그림 17] 비밀번호 추출 결과

4.2.2. 클립보드 및 윈도우 텍스트 정보 탈취

다음으로 확인되는 악성코드는 사용자의 클립보드 및 현재 사용 중인 윈도우의 텍스트를 수집하여 특정 경로에 저장해 주는 기능을 수행한다. 주기적으로 스레드를 돌면서 사용자가 복사한 클립보드 문자열을 %TEMP% 경로의 "KJSIW89S7S-SQP9LKC.gdk" 파일에 저장하며, 실시간으로 사용자가 사용하고 있는 프로그램의 윈도우 텍스트를 %TEMP% 경로의 "MSVE-AGEB-89S4-9JW2F.mx" 파일에 저장한다.

[그림 18] MSVE-AGEB-89S4-9JW2F.mx 파일에 수집된 현재 작업 윈도우 텍스트

- 클립보드 저장 경로 : %TEMP%₩KJSIW89S7S-SQP9LKC.gdk
- 윈도우 텍스트 저장 경로 : %TEMP%₩MSVE-AGEB-89S4-9JW2F.mx

또한 위의 로그 파일들이 일정 사이즈 이상일 경우에는 ZIP 압축하여 저장하며 비밀번호 "ZIPPROTECT"이다. ZIP 압축 파일들이 저장되는 경로는 아래와 같으며 압축 파일은 랜덤한 이름을 갖는다.

- 클립보드 압축 파일 경로 : %APPDATA%₩Microsoft₩Protect₩S-5-3-231-2183467-89346543-75436053658-1031₩Development₩[Random]
- 윈도우 텍스트 압축 파일 경로 : %APPDATA%₩Microsoft₩Protect₩S-5-3-231-2183467-89346543-75436053658-1031₩[Random]

4.2.3. 파일 MAC Time 수정

이외에도 파일의 MAC Time을 수정해주는 악성코드를 사용해 NukeSped 백도어의 MAC Time을 변경한다. MAC Time은 파일의 수정 시간(Modification Time), 접근 시간(Access Time), 변경 시간(Metadata Change Time)이며, 첫번째 인자로 받은 파일의 MAC Time을 구해 두번째 인자로 받은 파일의 MAC 주소를 변경한다. 자사 ASD 인프라의 로그를 보면 MAC 시간 변경의 대상 NukeSped 백도어인 것으로 확인된다.

```
handle_File1 = CreateFileA(argv[1], 0x80u, 3u, 0, 3u, 0x80u, 0);
if ( handle_File1 == (HANDLE)-1 )
{
  printf("can not open source file.");
  return 0;
}
else
{
  handle_File2 = CreateFileA(arg2, 0x100u, 3u, 0, 3u, 0x80u, 0);
  if ( handle_File2 == (HANDLE)-1 )
  {
    CloseHandle(handle_File1);
    printf("can not open dest file.");
  }
  else
  {
    GetFileTime(handle_File1, &CreationTime, &LastAccessTime, &LastWriteTime);
    SetFileTime(handle_File2, &CreationTime, &LastAccessTime, &LastWriteTime);
```

[그림 19] MAC Time 변경

4.2.4. Launcher

해당 악성코드는 커맨드 라인 툴이며 재부팅 시 인자로 받은 악성코드를 실행시켜 주는 지속성 유지 기능을 담당한다. 이를 위해 간단하게 레지스트리 Run Key를 사용하지만, 여기에 직접적인 악성코드의 경로를 넣는 대신 아래와 같이 일반 사용자가 인지하기 힘든 값을 써넣는다.

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run / (Default) / Default

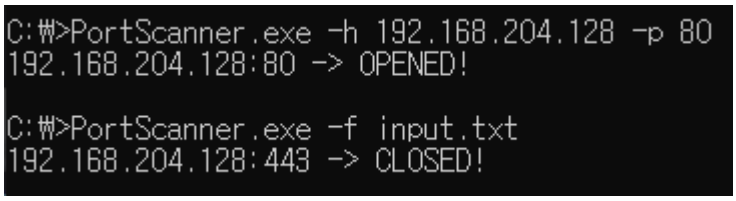
일반적으로 시스템이 재부팅되면 Run 키에 등록되어 있는 파일을 실행할 것이며, Default라는 값만 들어가 있기 때문에 별다른 동작이 불가하다. 하지만 추가적으로 아래와 같은 값들을 적음에 따라 Default.exe 즉 Default를 실행해도 등록한 악성코드가 동작할 수 있게 한다.

- HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩App Paths₩Default.exe / (Default) / c:₩windows₩system32₩msdxm.tlb
- HKCU₩SOFTWARE₩Classes₩.tlb / (Default) / System.Collections.Logic.tlb
- HKCU₩SOFTWARE₩Classes₩System.Collections.Logic.tlb₩Shell₩Open₩Command / (Default) / 실행시킬 악성코드의 경로

4.2.5. 포트 스캐너

기본적인 커맨드 라인 포트 스캐닝 툴이다. 인자 또는 파일을 통해 스캐닝할 주소를 획득한 후 결과를 출력해 준다. 커맨드 라인 모드에서는 -h, -p 옵션을 이용해 대상에 대한 스캐닝이 가능하며, 파일 모드에서는 호스트 주소와 포트 번호는 띄어쓰기로 구분하여 저장하는 형태로 사용할 수 있다.

- -h : 호스트 주소 (커맨드라인 모드)
- -p : 포트 번호 (커맨드라인 모드)
- -f : 호스트 주소 및 포트 번호가 저장된 파일 경로 (파일 모드)
- -o : 결과를 파일로 출력



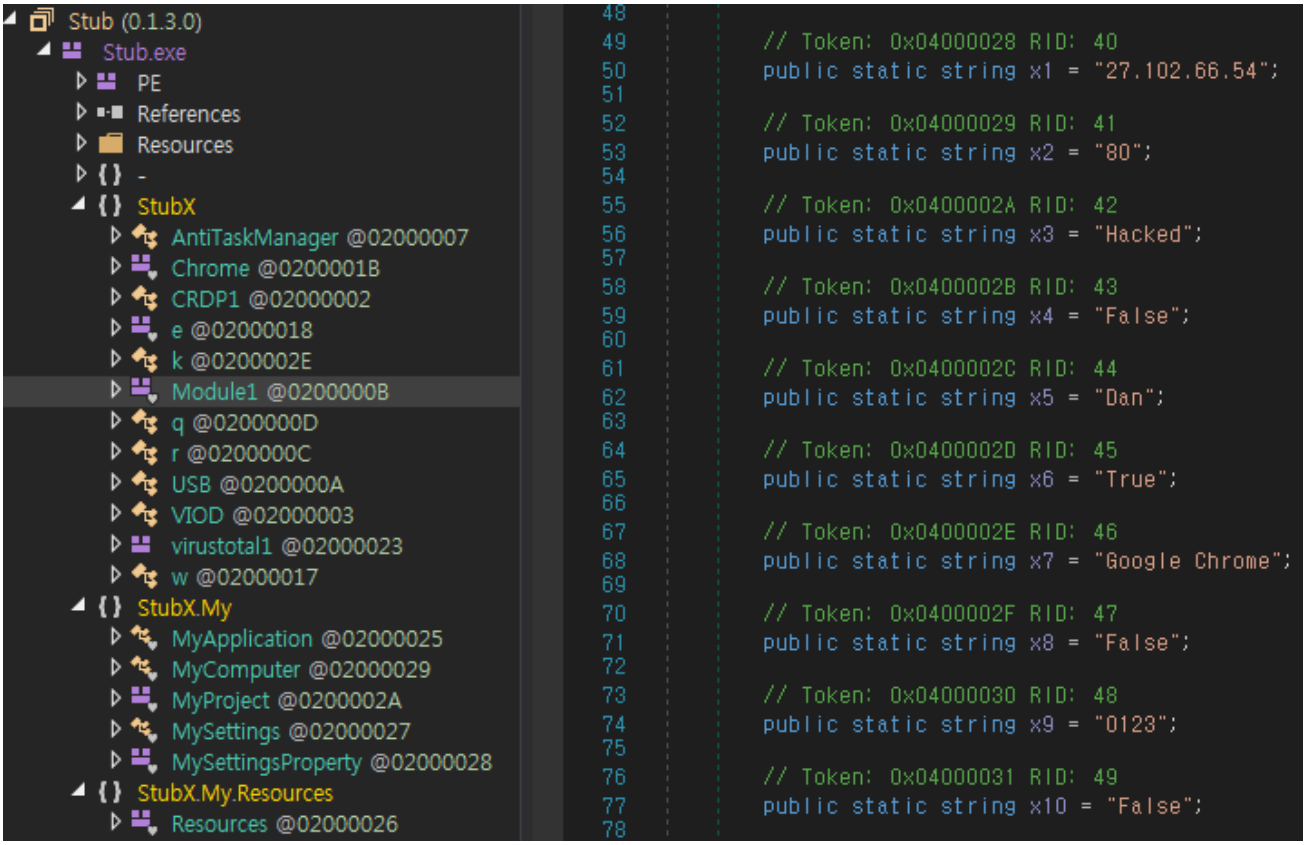
[그림 20] 포트 스캐닝

4.2.6. DarkComet RAT

직접적인 연관 관계는 확인되지 않지만 수집된 샘플들 중에서 동일한 패커를 이용해 패킹된 DarkComet RAT 악성코드도 확인된다. DarkComet은 키로깅, 스크린 캡쳐를 포함한 정보 탈취 및 공격자의 명령을 수행할 수 있는 RAT 악성코드이다.

즉 Lazarus 그룹은 NukeSped라는 백도어 악성코드 외에도 감염 시스템을 조작하기 위해 DarkComet RAT 악성코드를 사용한 이력이 있는 것으로 추정된다. 하지만 닷넷으로 개발된

DarkComet에 대해 다른 악성코드들과 동일하게 C++로 개발된 패커를 사용함에 따라 실질적으로는 동작이 불가능하다. 이에 따라 실제 감염 시스템에 설치되었다고 하더라도 공격자의 명령을 수행하지는 못했을 것으로 보인다.



[그림 21] DarkComet RAT 설정 데이터

안랩 대응 현황

안랩 제품군의 진단명과 엔진 버전 정보는 다음과 같다.

Dropper/DOC.Generic (2021.04.15.00)
Downloader/Win.AndarLoader.R345348 (2020.07.21.00)
Trojan/Win.Akdoor.R415757 (2021.04.15.00)
Trojan/Win.Akdoor.R415775 (2021.04.15.00)
Trojan/Win.Akdoor.R416722 (2021.04.20.00)
Trojan/Win.Akdoor.R418327 (2021.04.30.00)
Trojan/Win.Akdoor.C4413289 (2021.04.14.04)
Backdoor/Win32.Agent.C4166071 (2020.07.22.05)
Downloader/Win.AndarLoader.C4164499 (2020.07.21.00)
Downloader/Win.AndarLoader.R440947 (2021.09.11.00)
Trojan/Win.Akdoor.R432553 (2021.07.20.00)
Trojan/Win.Akdoor.C4546339
Backdoor/Win.NukeSped.C4633114 (2021.09.16.00)
Trojan/Win.Andardoor.C4527869 (2021.06.17.00)
Trojan/Win.Akdoor.C4510678 (2021.06.03.03)
Backdoor/Win.NukeSped.C4629675 (2021.09.11.00)
Backdoor/Win.NukeSped.C4631988 (2021.09.15.01)
Trojan/Win.Andaeldoor.C4413251 (2021.04.14.03)
Backdoor/Win.NukeSped.C4225340 (2020.11.14.00)
Trojan/Win64.Andaeldoor.C4319491 (2021.02.02.06)
Malware/Win64.Generic.C4293634 (2021.01.11.01)
Backdoor/Win.NukeSped.C4650495 (2021.09.26.03)
Backdoor/Win.NukeSped.C4199334 (2020.09.24.04)
Backdoor/Win.NukeSped.C4681538 (2021.10.09.00)
Backdoor/Win.NukeSped.C4681541 (2021.10.09.00)
Backdoor/Win.NukeSped.R345576 (2020.07.22.05)
Backdoor/Win.NukeSped.R351799 (2020.09.22.07)
Backdoor/Win32.Agent.R352629 (2020.10.05.09)
Trojan/Win.Andardoor.R427270 (2021.06.24.03)
Trojan/Win.Akdoor.R427276 (2021.06.25.00)
Trojan/Win.Andardoor.R432554 (2021.07.20.00)
Backdoor/Win.NukeSped.C4629673 (2021.09.11.00)
Backdoor/Win.NukeSped.C4536924 (2021.09.11.00)
Backdoor/Win.NukeSped.C4562087 (2021.07.22.03)
Backdoor/Win.NukeSped.R440946 (2021.09.11.00)
Backdoor/Win.NukeSped.R443312 (2021.09.29.03)
Backdoor/Win.NukeSped.R443314 (2021.09.29.03)
Trojan/Win32.MalPacked.C4198714 (2020.09.22.08)
Backdoor/Win.DARKCOMET.R264065 (2021.09.29.03)
Trojan/Win.Loader.C4543326 (2021.07.06.03)

Trojan/Win.Launcher.C4660650 (2021.09.29.03)
Trojan/Win32.Agent.C4198704 (2020.09.22.08)
Trojan/Win.Akdoor.C4413252 (2021.04.14.03)
Infostealer/Win.Pwstealer.C4510631 (2021.06.04.03)
Trojan/Win.Stealer (2021.09.29.03)
Infostealer/Win.Pwstealer.C4681931 (2021.10.09.00)
Trojan/Win.Stealer.C4660769 (2021.09.29.03)
Trojan/Win.Stealer.C4533178 (2021.09.29.03)
Trojan/Win.Stealer.C4660927 (2021.09.30.00)
Trojan/Win.Keylogger.C4533236 (2021.06.25.00)
Trojan/Win.Akdoor.C4533235 (2021.10.09.00)
Trojan/Win.Loader.C4543328 (2021.07.06.03)
Trojan/Win.Scanner.C4660875 (2021.09.30.01)

이 위협 그룹의 활동이 최근 공개되었다고 해도 일부 악성코드는 안랩 제품에서 진단되고 있었다. ASEC에서 이 그룹의 활동을 추적하며 악성코드를 대응했지만 확인되지 않아 미진단 중인 변형이 존재할 수 있다.

결론

Lazarus 그룹이라고 불리는 공격자들은 최근까지도 다수의 국내 공공기관 및 기업들을 대상으로 APT 공격을 수행하고 있다. 최초 침투 방식은 사회공학적 공격 방식 즉 이메일의 첨부 파일을 이용하는 것으로 알려져 있으며, 이외에도 워터링홀 공격과 같은 다양한 형태의 공격 방식들이 사용되고 있다고 한다.

공격자에 의해 최종적으로 설치되는 NukeSped 악성코드는 백도어로 동작하며 공격자의 명령을 받아 다양한 악성 행위를 수행할 수 있다. 대표적으로 키로깅, 계정 정보를 포함하여 감염 시스템에서 사용자의 다양한 정보를 탈취할 수 있으며, 나아가 탐지 및 분석을 우회하기 위한 목적으로 추가적인 악성코드들을 설치할 수 있다.

이에 따라 사용자들은 의심스러운 메일을 받게 된다면 첨부 파일의 실행을 지양해야 한다. 또한 사용하고 있는 소프트웨어 및 V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경써야 한다.

IoC (Indicators of Compromise)

파일 경로 및 이름

악성코드에서 사용한 파일 경로 및 이름은 다음과 같다. 일부는 정상 파일 이름과 동일할 수 있다.

다운로더 #1
%SystemDrive%₩users₩%USERNAME%₩iexplore.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩algstore.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩appstore.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩comstore.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩netsvc.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩winsrv.exe

다운로더 #2
%SystemDrive%₩users₩%USERNAME%₩iexplore.exe

NukeSped
%ALLUSERSPROFILE%₩acwinrt.exe
%ALLUSERSPROFILE%₩ahnlab₩ais₩adscli.exe
%ALLUSERSPROFILE%₩ahnlab₩ais₩asdcli.exe
%ALLUSERSPROFILE%₩ahnlab₩v3lauth₩v3update.exe
%ALLUSERSPROFILE%₩spool.exe
%ALLUSERSPROFILE%₩svchost.exe
%ALLUSERSPROFILE%₩symantec₩snac.exe
%ALLUSERSPROFILE%₩synctask.exe
%ALLUSERSPROFILE%₩v3patch.exe
%ProgramFiles%₩estsoft₩alzip₩alutil.exe
%SystemDrive%₩temp₩winstx.exe
%SystemDrive%₩users₩%USERNAME%₩certsvc.exe
%SystemDrive%₩users₩%USERNAME%₩documents₩iexplore.exe
%SystemDrive%₩users₩%USERNAME%₩documents₩iexplorer.exe
%SystemDrive%₩users₩%USERNAME%₩documents₩rsupport₩rcc50₩rsuimgr.exe
%SystemDrive%₩users₩%USERNAME%₩documents₩rsupport₩remotecall₩received files₩setup.exe
%SystemDrive%₩users₩%USERNAME%₩documents₩rsupport₩remotecall₩received files₩svchost.exe
%SystemDrive%₩users₩%USERNAME%₩downloads₩chromeupdate.exe
%SystemDrive%₩users₩%USERNAME%₩iexplore.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩commgr.exe
%SystemDrive%₩users₩%USERNAME%₩libraries₩netmon.exe
%SystemDrive%₩users₩%USERNAME%₩music₩lsdev.exe
%SystemDrive%₩users₩%USERNAME%₩notework.exe

%SystemDrive%₩users₩%USERNAME%₩pictures₩lsdev.exe
%SystemDrive%₩users₩%USERNAME%₩svchost.exe
%SystemDrive%₩users₩%USERNAME%₩taskpm.exe
%SystemRoot%₩apppatch₩apppatch64₩acwinrt.exe
%SystemRoot%₩performance₩winsat₩winsat.exe
%SystemRoot%₩system32₩synctask.exe
%SystemRoot%₩syswow64₩xspwizard.exe
%SystemRoot%₩xswizard.exe
C:₩Users₩Public₩chrome.exe

DarkComet
%SystemDrive%₩temp₩mshelp.exe

Launcher
%ALLUSERSPROFILE%₩a.exe

정보 탈취 악성코드
%SystemDrive%₩temp₩chrome2.exe
%ALLUSERSPROFILE%₩s.exe
%ALLUSERSPROFILE%₩s2.exe
%ALLUSERSPROFILE%₩so.exe
%SystemDrive%₩temp₩chromeall.exe
%SystemDrive%₩users₩%USERNAME%₩music₩call.exe

클립보드 로깅
%ALLUSERSPROFILE%₩syncproxy.exe
%SystemRoot%₩syswow64₩syncproxy.exe

파일 MAC 시간 변경
%ALLUSERSPROFILE%₩t.exe
%SystemDrive%₩temp₩%USERNAME%₩t.exe

포트 스캐너
%ALLUSERSPROFILE%₩p.exe

파일 Hashes (MD5)

관련 파일의 MD5는 다음과 같다. (단, 민감 샘플이 존재할 경우 제외된다.)

DOC
3ef3ab96409c6d06eaca0976ef96b88a
d5e974a3386fc99d2932756ca165a451
4d7f44e3ea3215a8b5104b474b0be89e
6f58ad5d76b271a0dcdf13f21b9dec87

a2284607feebd04a2cb31cb54420df3f
db0caea66ba52103c495ec16c20c4413
71759cca8c700646b4976b19b9abd6fe
8192ee65c7cc9c19e8693a6bd29803cd
4c25c8400f26aee01aef25b438cdf61a

다운로더 #1
76b1d184e1b056d39c0602c496535989
927f0a1090255bc724953e1f5a09a070
c1ab671c412af7e080abe7ff8ff3f9e4
fd84b6d5f77861a10fc888e381a4616d
c1ab671c412af7e080abe7ff8ff3f9e4
2479abd20adc9115efff7fcc79ac06f7
118cfa75e386ed45bec297f8865de671
f4d46629ca15313b94992f3798718df7
53648bf8f0121130edb42c626d7c2fc4
0812ce08a75e5fc774a114436e88cd06
1bb267c96ec2925f6ae3716d831671cf
f3fcb306cb93489f999e00a7ef63536b
0ecfa51cd4bf1a9841a07bdb5bfcd0ab
df1e7a42c92ecb01290d896dca4e5faa

다운로더 #1 (언패킹된 원본 바이너리)
b6985e5204e7227aef08c6ebbfb24b6c
b7cc5c40cbe8ea8c7cd914ca5331ad3a
00f18f1d62197ebd3c0c3838cd33c2b7
0660c645deb1554a9e92906330f6863c
4d30612a928faf7643b14bd85d8433cc
fb84a392601fc19aeb7f8ce11b3a4907
3a72889649faa2e21a68be3be3232c6d
fdc66cdabd46bc3b26aba4e59943726b

다운로더 #2
a54d444005af121e99221e17e65bffbd
54ed652086038418047c993d73d655d5
e402008449eb99a3037dc103a2c9a869
de82e6e3972989f79256056815df4e27

다운로더 #2 (언패킹된 원본 바이너리)
4d7782a8013abe14426ad5b6e03e2a38

NukeSped
6d0dea9bff819a3a34e6346fc7320409
e64e2754703c016ebfb6a3b12b91407b
36362db5ae8916124b538078e4c06000
de69c3490eaea6a20f5a3c9bf1f87a4b
3fdc03a1ab079dd019f83b0e58adf43d
3b1b8702c4d3e2e194c4cc8f09a57d06

f990445da44d0ac48e81d60269a210fd
60b5ff9a485f27b2f56168c193de5942
947b3b580c630a31410451fd74f9c440
bc5835b173b1619ad3c4960ffabc1a42
cd951654378615e956005af1c8120849
2c47c6cf9889c9bff1f0fb0229c7d864
8b378eabcec13c3c925cc7ca4d191f5f
5b387a9130e9b9782ca4c225c8e641b3
62eae43a36cbc4ed935d8df007f5650b
eef723ff0b5c0b10d391955250f781b3
d1a99087fa3793fbc4d0adb26e87efce
d63bb2c5cd4cfbe8fabf1640b569db6a
569246a3325effa11cb8ff362428ab2c
3b494133f1a673b2b04df4f4f996a25d
fc3c31bbdbeee99aba5f7a735fac7a7e
159ad2afcab80e83397388e495d215a5
96d5ee709494d4417e92f5af3676082c
fb43468cef3338f7fe0fce30e2279854
71da09313fde65f9e594098c375be7c2
918a86dd73bc2651e26377ae01b9b069
e28547cb6cdfc11f5213f9ccc1b3e232
3bf9b83e00544ac383aaef795e3ded78
0b698039ebdaf08f2cab30a01bc3e3e6
d0deb5d79ffeda20128436e4167dba67
56faddb6918a067a71d2ab2b56c7d9bf
15b1d3d8df2d204e99911dc72482913e
a9611cc4ab734bef371af07d73540478
cad1373200da75dbb068f3eb49e18ea8
e9849f65f159c19357bbbe78ebfc6e48
91038ff04bf85c19e377aef3381e47f9
cb9e18e21226a89ce2c26c695a989e0d
205585799d0d0f62422a3cfce253001b
bf4a822f04193b953689e277a9e1f4f1
5be46724c1452af366523b24acc8ea6b
19702399b3936dc2ccb5fde011fdf3ba
38917e8aa02b58b09401383115ab549e
ef3a6978c7d454f9f6316f2d267f108d
1d092fd15d957805bb140c61a728d767
67220baf2a415876bee2d43c11f6e9ad
33c2e887c3d337eeffbbd8745bfdfc8f
3fa627c43d3c6efee8693510309ad4ec
f890e61b228f634b2dcf73db8032f769
98d270cf03c4ffe1c05cf7c3d3f70dcc
c34cfe7b3e0a25978e16d917d795f6d4
5fedd4089f64ee0356120dc662ff967a
def1b5e508d13c3dd5f44df3e72e8fff
abaeecd83a585ec0c5f1153199938e83
fffad123bd6df76f94ffc9b384a067fc

4c852d06c4976657ec63e7f618765585
c827d95429b644e918d53b24719dbe6e
0d7340efbf5fbd24c83d1cf9fa334c7d
2430a6e629eb4948819d65bf481467ee
c703d4d46373c1c54107b0944192e472
4df757390adf71abdd084d3e9718c153
9421518543233d820328c62cbb2c1141
5e21cafd920575cbd19c064e2b2b0526
3274c1afc58618bf52ff047e15b680c7
0468f100865277c608531ebf49b171ed
56283a2c2fd2b72991929e020f37cb05

NukeSped (언패킹된 원본 바이너리)
c975dfa5a7d31468b014e2e440d7d02a
6e8be6cd7187548ee859ac7d520e225a
1f5ef44039113df7ab917e55b7fadce7
b0c4c6d6ae62fec10e97aab1756dc17f
4832189ecba45ef64d7596e22d8560bd
24ca459046aa4ecb01b6c5fb9ad5af68
d58df22f7838c900d979f5e737ffc480
bdf14488c4f0b44b6cc1ec985d3900aa
e22487b2a35f258e82f9166bc0b3f972
0edb25adab3af46f3d900767a3247607
7b81ea543bb57d2b6db1610d8b424e95
9ca8bbcad9d63a01f694c5bfd4d7c816
2be5bae0be955d613c71ff2eb3b46d25
265e6604fe577ba404285d32a1f4f4cf
5c41cbf8a7620e10f158f6b70963d1cb
fc48213b2906342a33cce216e53e3e4e
4ea1be624b726ef79db88e86d235ff42
1eb180e739fe5a7966b62dc1af252000
9625e5bdb1084f48d49caa8ad40b1cbe
693e3d88a67872ebc0268f1475bfcbf9
643c2ad6067051e3daf7d08b4adeaed4
85e4b3a92ee42d70fc609ae846d3fafa
f947b444d30736483d7f22debe978770
d6121d74dcef566a5e2f9aba179b8cca
92e34e16ea05360adab1e66521b989c4
525cc10803d9858fca5dc4010925ba68
a35a8c64870b9a3fe45348b4f2a93e75
c4f4ba469250568619a7de6f4ba96d14
821f27568f8de910d45305aac100e5fb
9bc9fda251021d0c911b23ce46223164
505262547f8879249794fc31eea41fc6
d6708dcfcc0fc0a7fdf227c7ea1acab0
dc8e380e78067c02341df6c0ede65630
2c93bcf8285c7a956e7f73afe7b56f30

DarkComet
7916bb075141cebf72f735ba43191f6e

DarkComet (언패킹된 원본 바이너리)
bc4889f75b874b171a931ee4c546b745

Launcher
779e53e6a0e08805617479d1f4ac4cca
5a234286dcc1aef933a951b298445ba8

Launcher (언패킹된 원본 바이너리)
f2132947d0668084620c7687342c7bb9

정보 탈취 악성코드
3aadb4653ff99633771ee2e28df08db1
fb60f04f65d169a4471129e171d6b88d
09dd50472eba443b39aec993bcf4f159
05fa64753726ec0f548b7f1894af0e13
4387a3e2b3e55911d8e93b18dd873eff
85995257ac07ae5a6b4a86758a2283d7
88b44b5df9efbf0d350d06ee8ef79a0c

정보 탈취 악성코드 (언패킹된 원본 바이너리)
37ca3b0a14a66adf57ec1a41f9a969a0
c3cecb6c82be49658ba01872e0f643b9
1bff2a65522bb08bd576c5056268e3bb

클립보드 탈취 악성코드
17817b9836b0e2463a05d42afa59e89d

MAC 시간 변경 악성코드
194486fb936dcbdc104eb670adddd9fc
02e8384a5f0354ece7b9b5b69918e6a8

MAC 시간 변경 악성코드 (언패킹된 원본 바이너리)
9df2dfee4bed45f0fea0f73a055d3d17

포트 스캐너
9a570c53b1a811aba02b2b76cc65b5eb

포트 스캐너 (언패킹된 원본 바이너리)
88f9824b5a76591d62d391e6b1ef1d31

관련 도메인, URL 및 IP 주소

사용된 다운로드 혹은 C&C 주소는 다음과 같다. (http는 hxxp로 변경했으며 민감 정보가 존재할 경우 제외된다.)

다운로더 #1
hxxp://hivekorea[.]com/jdboard/member/list.php
hxxp://www.jinjinpig.co[.]kr/Anyboard/list.php
hxxp://www.jinjinpig.co[.]kr/Anyboard/skin/board.php
hxxp://mail.namusoft[.]kr/jsp/user/eam/board.jsp
hxxp://www.conkorea[.]com/cshop/getenforce/board.php
hxxp://www.isalim.co[.]kr/exam/board.php
hxxp://snum.or[.]kr/skin_img/skin.php
hxxp://www.ddjm.co[.]kr/bbs/icon/skin/skin.php
http://mail.sisnet.co[.]kr/jsp/user/sms/sms_recv.jsp
http://mail.neocyon[.]com/jsp/user/sms/sms_recv.jsp

다운로더 #2
hxxp://34.221.66[.]33/StSess_Update.php
hxxp://34.221.66[.]33/ASDClient.php
hxxp://34.221.66[.]33/Semenser.php

NukeSped
13.233.87[.]126:443
149.56.201[.]228:443
173.44.62[.]102:8080
185.12.45[.]134:443
185.12.45[.]134:8443
185.208.158[.]204:443
185.208.158[.]205:443
185.208.158[.]208:443
193.56.28[.]251:443
198.55.119[.]112:443
23.229.111[.]197:443
23.229.111[.]197:8443
25.255.77[.]106:443
27.102.113[.]100:443
27.102.129[.]91:443
27.102.134[.]33:443
27.102.70[.]192:443
27.102.70[.]192:8080
27.255.77[.]106:443
45.58.112[.]77:443
52.202.193[.]124:443
52.79.101[.]146:443

54.68.42[.]4:443
78.157.207[.]15:443
78.157.207[.]15:8443
86.106.131[.]104:443
87.98.183[.]116:8443
file.naverapi[.]com:80
files.codencorp[.]com:443
playpingpong12[.]com:443
sorriso[.]kr:443

DarkComet
27.102.66[.]54:80

참고 문헌

[1] https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=36210
[2] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=344495af-919d-49a4-9956-ec2c9ce20819
[3] https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
[4] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=15bbe345-5a6c-42f9-8e95-5e69bbb4e137

More security, More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우) 13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 팩스 : 031-722-8901
www.ahnlab.com

AhnLab