ASEC Report

Vol. 94

2019년 1분기

ASEC REPORT

VOL.94 2019년 1분기

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.

2019년 1분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

- 동시다발적으로 국내 기업 노린 Ammyy 해킹 툴과 클롭 랜섬웨어

보안 이슈

Security Issue

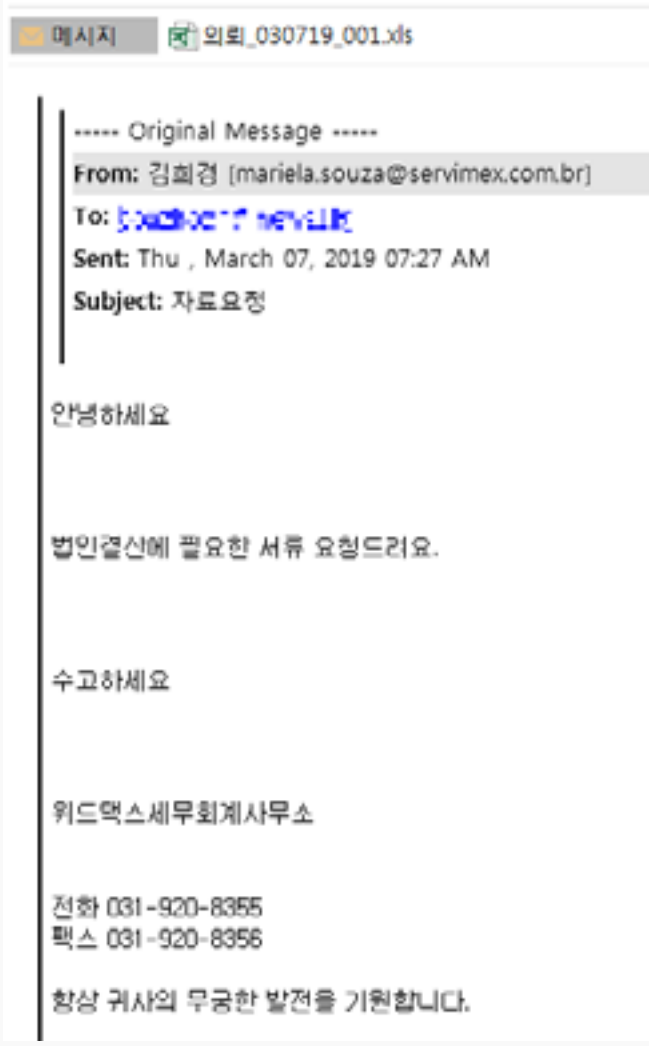
동시다발적으로 국내 기업 노린 Ammyy 해킹 툴과 클롭 랜섬웨어

최근 첨부 파일 내 악성 매크로를 이용한 공격 사례가 지속적으로 증가하고 있다. 지난 2월에는 국내 기업 사용자를 타깃으로 메일의 첨부 파일을 통해 'Flawed Ammyy RAT'라고 명명된 원격제어 해킹 툴이 유포됐다. 한편 동일한 시기에 국내 기업을 노린 '클롭(CLOP) 랜섬웨어'가 유포되고 있는 정황이 안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)에 포착됐다. 안랩은 Flawed Ammyy RAT과 클롭 랜섬웨어의 인증서를 추적하던 중 이들 두 악성코드가 동일한 서명을 공유하고 있으며, 공격 대상 또한 국내 기업 사용자인 점 등 다수의 공통점이 존재하는 것을 확인했다.

안랩 시큐리티대응센터는 국내 기업 사용자를 노린 Flawed Ammyy RAT과 클롭 랜섬웨어의 유포 방법 및 공격 기법과 함께 이들 두 악성코드의 연관성을 면밀히 분석했다.

1. 해킹 툴 Flawed Ammyy RAT 공격 개요

먼저 원격제어 기능을 가진 해킹 툴 Flawed Ammyy RAT(Remote Access Tool)의 공격 방식을 살펴보자. 공격자는 스팸 메일을 이용한 악성코드 유포하는 방식을 사용했다. [그림 1-1], [그림 1-2]과 같이 메일의 내용만 보면 다운로드나 실행을 유도하지 않는 일반적인 내용의 메일로 보인다. 또한 첨부 파일의 이름은 "의뢰_030719_001.xls" 또는 "증명서.xls"이다. 해당 메일을 수신한 사용자는 별 다른 의심없이 메일의 첨부 파일을 열어볼 소지가 있다.


메시지 의뢰_030719_001.xls

----- Original Message -----
From: 김희경 [mariela.souza@servimex.com.br]
To: [redacted]
Sent: Thu , March 07, 2019 07:27 AM
Subject: 자료요청

안녕하세요

법인결산에 필요한 서류 요청드려요.

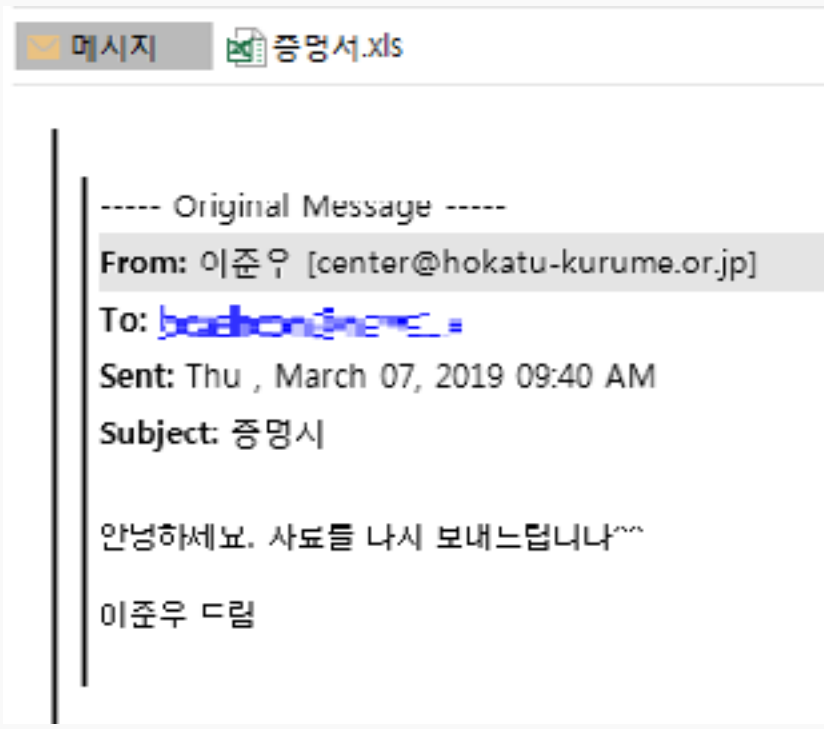
수고하세요

위드맥스세무회계사무소

전화 031-920-8355
팩스 031-920-8356

항상 귀사의 무궁한 발전을 기원합니다.

그림 1-1 | 스팸 메일 사례 (1)


메시지 증명서.xls

----- Original Message -----
From: 이준우 [center@hokatu-kurume.or.jp]
To: [redacted]
Sent: Thu , March 07, 2019 09:40 AM
Subject: 증명서

안녕하세요. 사됴들 나시 보내느덥니나^^^

이준우 드림

그림 1-2 | 스팸 메일 사례 (2)

사용자가 첨부된 악성 엑셀 문서를 다운받은 후 실행하면 [그림 1-3]과 같은 화면이 나타난다. 공격자는 사회공학적 기법을 이용하여 매크로 설정이 꺼져 있는 마이크로소프트 오피스(Microsoft Office) 프로그램에서 사용자가 화면 상단의 '콘텐츠 사용' 버튼을 클릭하도록 유도했다.

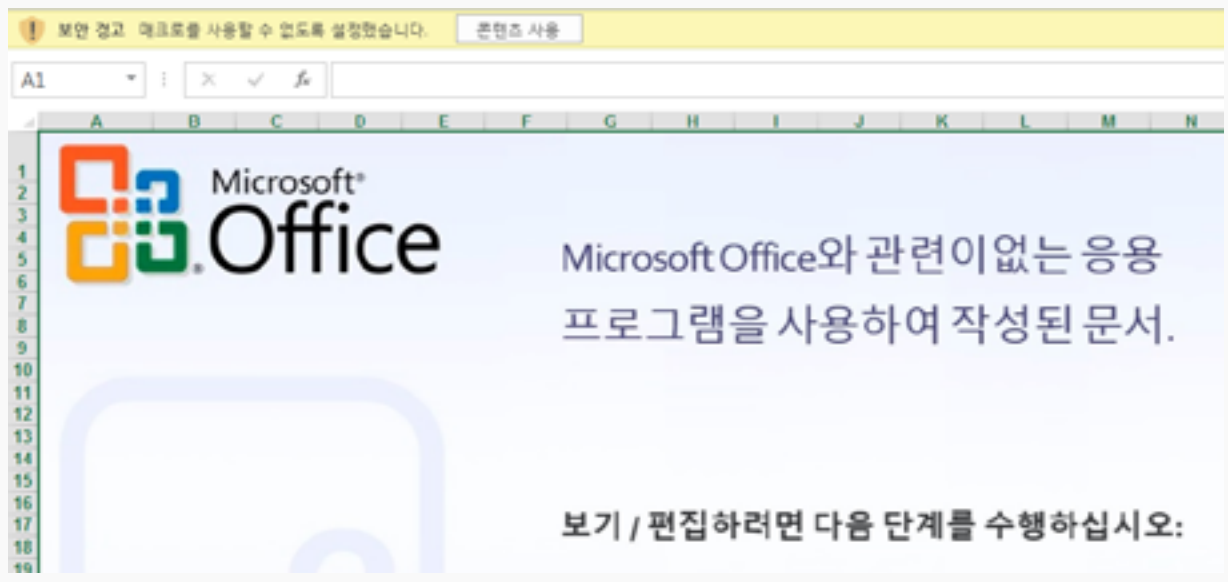


그림 1-3 | 매크로를 활성화시키기 위해 사용되는 사회공학적 기법

일반적인 사용자의 경우 매크로 활성화 버튼 클릭만으로 백도어(Backdoor)가 컴퓨터에 설치될 수 있다는 것을 알기 어렵다. 또한 해당 문서는 일반적인 악성 문서 파일과 달리 VBA(Visual Basic for Application)를 이용한 악성 매크로를 포함하지 않는 대신 XLM을 이용한 매크로가 포함되어 있다. XML은 엑셀의 이전 버전인 4.0 버전에서 사용하는 매크로다. 일반적인 악성 문서 파일에서 사용되는 VBA는 엑셀 5.0 버전에서 도입된 매크로이다.

대부분의 악성 오피스 문서 파일들은 대부분 VBA를 이용하여 제작되어 악성코드를 다운로드하거나 드랍하고 실행시킨다. 최근에는 파워셸을 이용하는 공격 방식 또한 증가하는 추세다. 반면, 이번 공격에 사용된 방식은 보안 프로그램의 탐지 회피를 위해 엑셀 프로그램의 초기 버전에서 이용하는 매크로 제작 방식을 사용했다는 점이 특징적이다.

엑셀 파일 하단의 숨겨진 워크 시트를 해제하면 [그림 1-4]와 같은 명령을 확인할 수 있는데, 이는 msiexec.exe를 이용해 악성 서버에서 msi 파일을 다운로드하고 실행하는 방식이다.

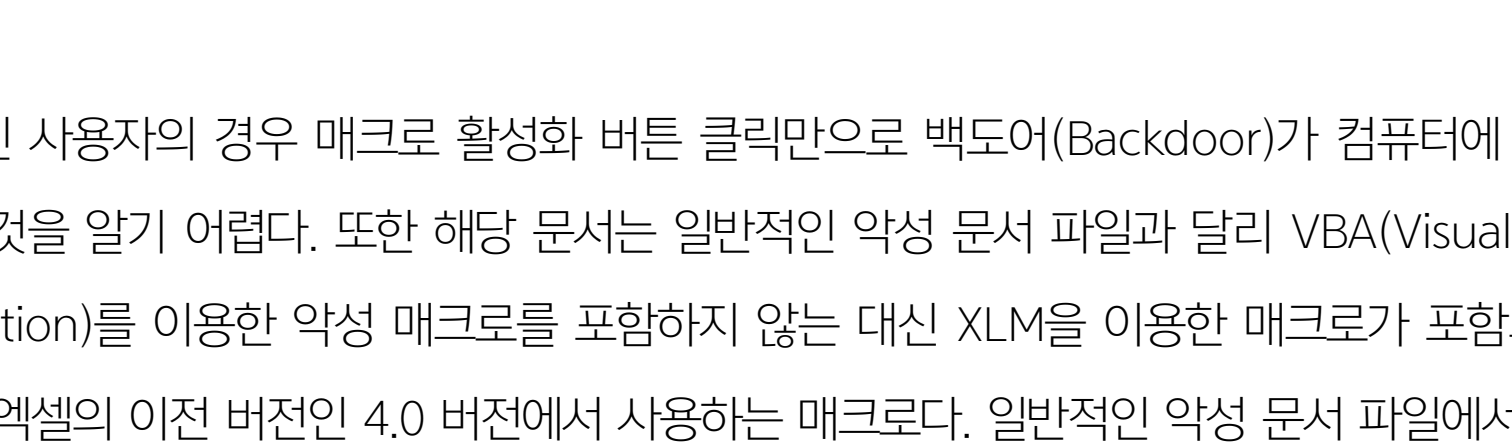


그림 1-4 | XML을 이용한 다운로드 방식

서버로부터 다운로드된 악성 msi 파일은 내부에 exe 파일을 포함하고 있는데 해당 exe 파일은 실제 악성 백도어 역할을 담당하는 또 다른 exe 파일을 다운로드하는 기능을 수행한다. 또한 파일을 실행시키기 전 [그림 1-5]와 같이 현재 실행 중인 프로세스를 검사하여 현재 백신 프로그램이 실행 중인 경우에는 해당 백신 프로그램의 프로세스를 종료한다.

```
if ( LoadLibraryExW(L"kernel32.dll", 0, 0)
  && (sub_411FF0(L"QHACTIVEDEFENSE.EXE")
   || sub_411FF0(L"QHSAFETRAY.EXE")
   || sub_411FF0(L"QHWATCHDOG.EXE")
   || sub_411FF0(L"CMDAGENT.EXE")
   || sub_411FF0(L"CIS.EXE")
   || sub_411FF0(L"V3LITE.EXE")
   || sub_411FF0(L"SPIDERAGENT.EXE")
   || sub_411FF0(L"DWENGINE.EXE")
   || sub_411FF0(L"DWARKDAEMON.EXE")
   || sub_411FF0(L"BULLGUARDTRAY.EXE")
   || sub_411FF0(L"BDAGENT.EXE")
   || sub_411FF0(L"BULLGUARD.EXE")
   || sub_411FF0(L"BDSS.EXE")
   || sub_411FF0(L"BULLGUARD.EXE")
   || sub_411FF0(L"V3MAIN.EXE")
   || sub_411FF0(L"V3SP.EXE")
   || sub_411FF0(L"EGUI.EXE")
   || sub_411FF0(L"EKRN.EXE")) )
{
  ExitProcess(0);
}
```

그림 1-5 | 백신 프로세스를 검사하는 루틴

이후 특정 url에서 인코딩된 형태의 파일이 다운로드되며, 최종적으로 디코딩 과정을 거치면 exe 형태의 악성코드가 생성된다. 한편 다운로더는 악성코드 설치 이후 자가 삭제되는데 이때 설치된 악성코드가 실제 악성 행위를 담당하는 해킹 툴인 'Flawed Ammyy RAT'이다.

[그림 1-6]은 Flawed Ammyy RAT가 다운로드되기까지의 일련의 과정을 나타낸 것이다. 공격자는 다수의 백신 프로그램에서 오피스 문서 파

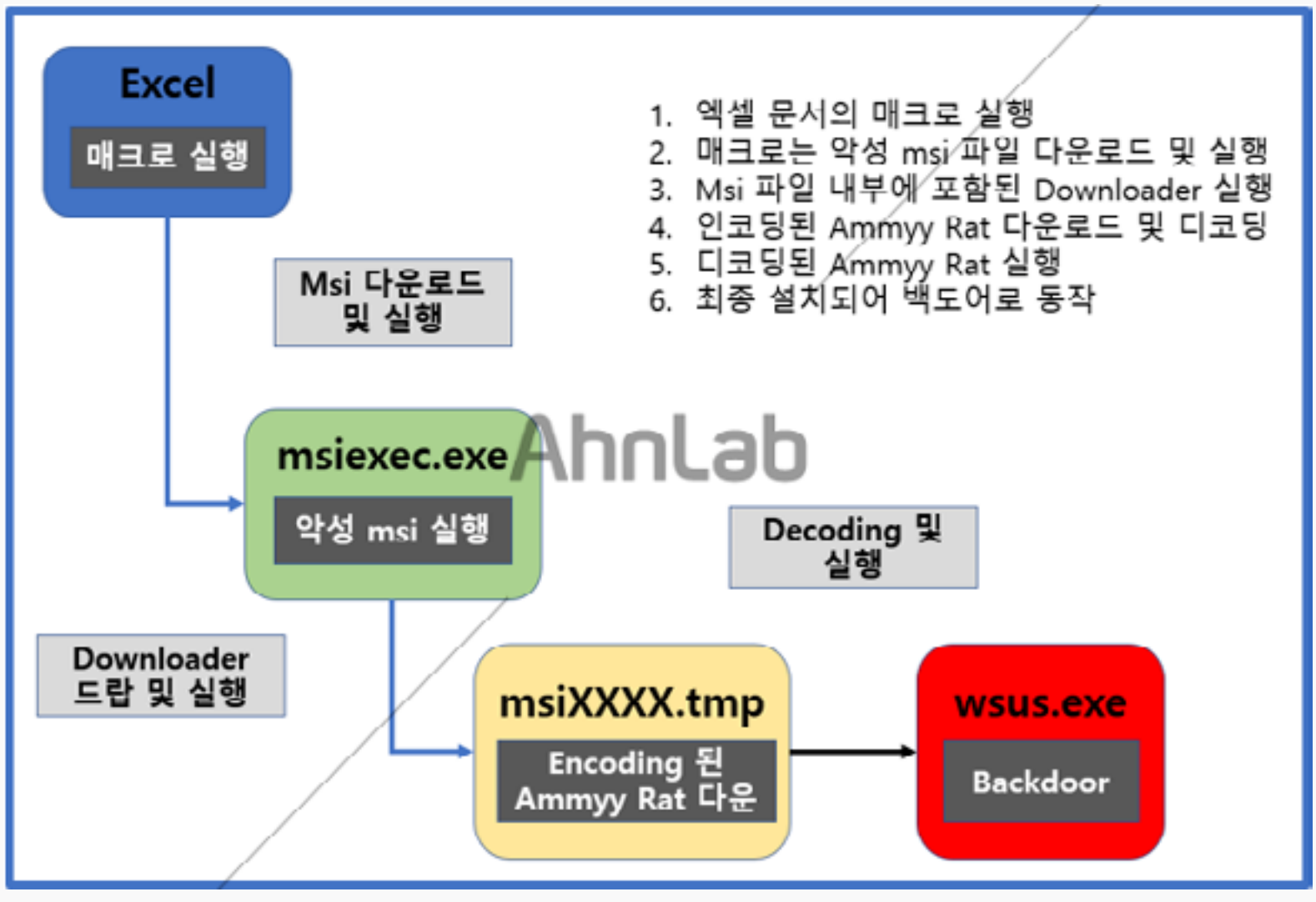


그림 1-6 | 악성코드 공격 흐름도

일의 VBA 매크로가 주요 분석 대상이라는 점을 이용하여 XLM을 사용한 공격 방식을 통해 백신 프로그램의 탐지를 효과적으로 우회했다.

공격자는 악성 exe 파일을 직접 다운로드하여 실행시키지 않고, msiexec의 기능 중 하나인 외부에 존재하는 msi 파일을 설치하는 방식을 통해 간접적으로 다운로더 프로그램을 다운로드 및 실행했다. 또한 실제 백도어 악성코드 역할을 하는 Flawed Ammyy RAT 역시 인코딩된 형태로 다운로드받아 디코딩 과정을 거친 후 설치가 진행되었다. 또한 프로세스 목록을 검사하여 백신 프로그램이 동작하고 있는 경우에는 행위를 진행하지 않고 바로 종료한다. 마지막으로 유효한 인증서를 통해 각각의 바이너리를 서명함으로써, 인증서가 존재하지 않거나 유효하지 않은 인증서로 서명된 일반적인 악성코드에 비해 쉽게 정상 프로그램으로 위장했다.

한편 Flawed Ammyy RAT은 원격 데스크탑 프로그램인 Ammyy Admin의 유출된 소스 코드를 기반으로 제작되었다. Ammyy Admin 프로그램은 파일 전송이나 화면 캡쳐와 같은 원격 컴퓨터에 대한 제어 기능을 포함하고 있어 공격자는 해당 소스 코드를 기반으로 악성 행위를 수행할 수 있도록 코드를 추가, 수정하여 RAT 악성코드를 제작한 것으로 보인다.

Flawed Ammyy의 초기 루틴을 분석한 결과 다운로더와 유사하게 현재 실행 중인 프로세스를 검사하고 백신 프로그램이 실행 중인 경우 종료하는 기능이 확인되었다. 또한 서버에서 사용자 컴퓨터에 접속할 수 있도록 OS 정보, 권한, 사용자 이름 등의 기본 정보를 전송하는 것이 확인되었다.

2. Flawed Ammyy RAT과 클롭(CLOP) 랜섬웨어의 연관성

앞서 언급한 것과 같이 Flawed Ammyy RAT은 악성코드 본체뿐만 아니라 다운로더 또한 유효한 서명을 포함한다. 유효하지 않은 서명을 포함한 여타 악성코드와는 달리, 악성코드 바이너리가 여러 유효한 인증서를 통해 서명되어 유포되는 것은 Flawed Ammyy RAT만의 특징적인 점이라고 볼 수 있다. 그런

데 최근 국내 기업을 대상으로 유포된 클롭(CLOP) 랜섬웨어에서도 이와 같은 특징이 발견되었다.

ASEC에서는 이 점을 이용해 Flawed Ammyy RAT과 클롭 랜섬웨어의 인증서를 추적하던 중 두 악성 코드가 동일한 인증서로 서명된 경우가 존재하는 사실을 확인했다. [그럼 1-7], [그림 1-8]은 동일한 인증서 'DELUX LTD'와 'MAN TURBO (UK) LIMITED'로 서명된 Flawed Ammyy RAT과 클롭 랜섬웨어의 속성 화면이다.

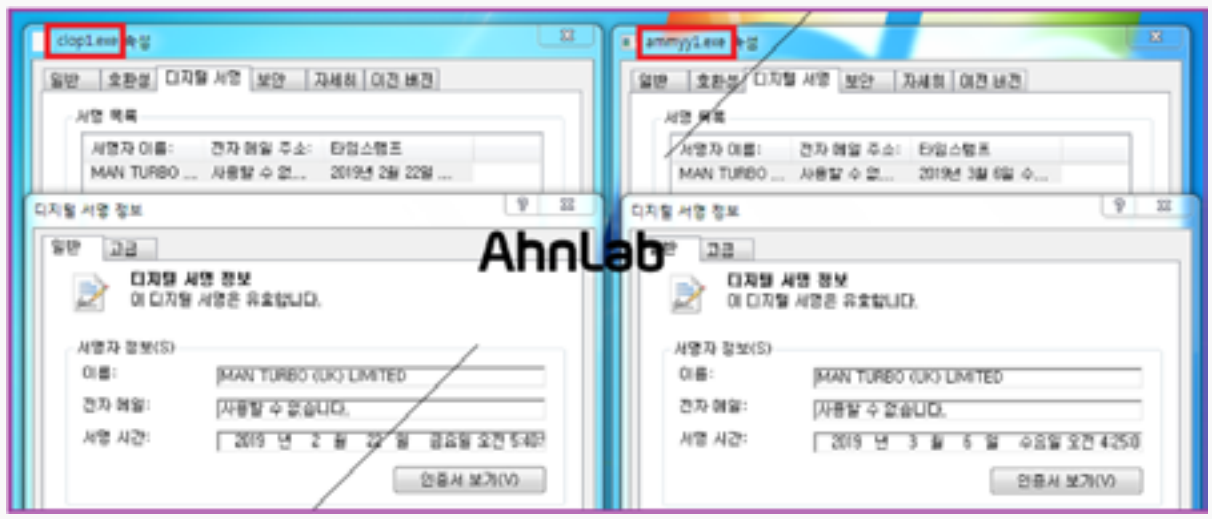


그림 1-7 | 동일 인증서 사례 (1)

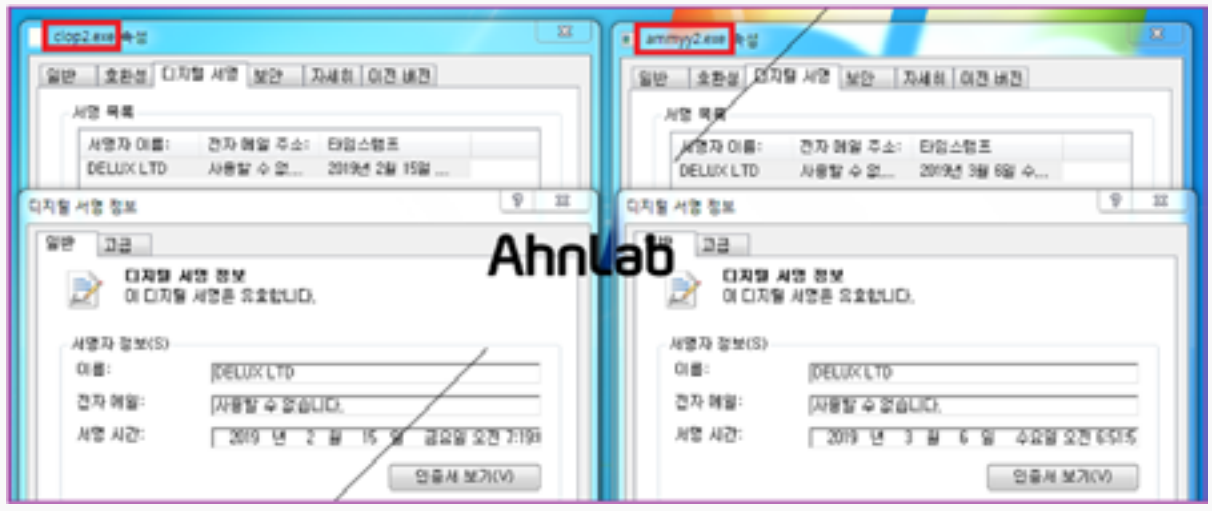


그림 1-8 | 동일 인증서 사례 (2)

Flawed Ammyy RAT과 클롭 랜섬웨어의 또 하나의 공통점은 일반 사용자가 아닌 기업 사용자를 대상으로 유포된다는 점이다. 클롭 랜섬웨어는 다수의 일반 사용자들을 대상으로 하는 대부분의 랜섬웨어들과 달리 기업을 공격 대상으로 하는데, 유포 방식 및 감염 방식은 아직 확인되지 않았다. 다만 공

격자는 중앙 관리 서버에 침투한 후 관리 서버에 연결된 시스템에 악성코드를 삽입 및 감염시킨다는 사실만 알려져 있다.

최근 Flawed Ammyy의 다운로더에 변화된 코드가 포착됐다. 백신 프로그램의 프로세스 검사 루틴 이후에 기업 사용자 환경을 탐지하는 루틴이 포함된 것이다. [그림 1-9]과 같이 'net user /domain' 명령을 수행하고, 그 결과에 WORKGROUP 문자열이 출력되는지 검사한다. 일반 개인 사용자의 경우 별다른 설정이 없기 때문에 WORKGROUP 문자열이 출력되지만 기업 사용자의 경우 각 환경에 맞게 설정된 그룹명이 출력될 수 있다. 공격자는 WORKGROUP 문자열이 출력되는 일반 개인 사용자의 경우, Flawed Ammyy RAT 악성코드를 다운로드 및 설치하는 악성 행위를 수행하지 않고 종료하도록 했다.

```
BOOL sub_411140()
{
  HANDLE v0; // eax
  void *v1; // esi
  HANDLE v2; // edi
  DWORD v3; // esi
  const CHAR *v4; // esi
  CHAR Parameters; // [esp+Ch] [ebp-314h]
  CHAR pszPath; // [esp+110h] [ebp-210h]
  CHAR FileName; // [esp+214h] [ebp-10Ch]
  DWORD NumberOfBytesRead; // [esp+318h] [ebp-8h]
  LPCSTR lpFirst; // [esp+31Ch] [ebp-4h]

  SHGetSpecialFolderPathA(0, &pszPath, 35, 0);
  wsprintfA(&FileName, "%s\\TMPUSER.DAT", &pszPath);
  wsprintfA(&Parameters, "/C net user /domain  > \"%s\"", &FileName);
  ShellExecuteA(0, 0, "cmd", &Parameters, 0, 0);
  while ( 1 )
  {
    v0 = CreateFileA(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
    v1 = v0;
    if ( v0 != (HANDLE)-1 && GetFileSize(v0, 0) > 1 )
      break;
    Sleep(0x3E8u);
    CloseHandle(v1);
  }
  CloseHandle(v1);
  v2 = CreateFileA(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  v3 = GetFileSize(v2, 0);
  lpFirst = (LPCSTR)GlobalAlloc(0x40u, v3);
  ReadFile(v2, (LPVOID)lpFirst, v3, &NumberOfBytesRead, 0);
  CloseHandle(v2);
  DeleteFileA(&FileName);
  v4 = lpFirst;
  return !StrStrA(lpFirst, "WORKGROUP") && !StrStrA(v4, "workgroup");
}
```

그림 1-9 | WORKGROUP 문자열을 검사하는 루틴

3. 클롭(CLOP) 랜섬웨어 동작 방식

클롭 랜섬웨어의 공격 방식 및 암호화 과정을 살펴보자. 클롭 랜섬웨어는 [그림 1-10]과 같이 시스템 서비스로 등록되어 실행되며, 서비스로 실행되지 않는 경우에는 정상적으로 동작하지 않는다.

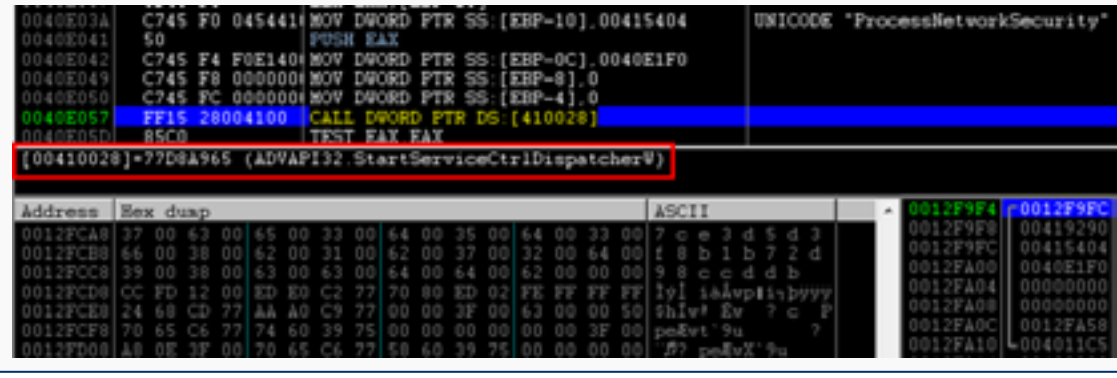


그림 1-10 | 클롭 랜섬웨어의 실행 방법

또한 클롭 랜섬웨어는 파일 암호화를 진행하기 전 일부 프로세스를 강제로 종료시킨다. 이는 암호화를 진행하는 과정에서 보다 많은 대상을 암호화 시키기 위한 것으로 추정된다. 프로세스 강제 종료 대상은 [그림 1-11]과 같다.

```
sub_40D8D0(L"zoolz.exe");
sub_40D8D0(L"mysqld-nt.exe");
sub_40D8D0(L"syntime.exe");
sub_40D8D0(L"agntsv.exe");
sub_40D8D0(L"mysqld-opt.exe");
sub_40D8D0(L"tbirdconfig.exe");
sub_40D8D0(L"dbeng50.exe");
sub_40D8D0(L"oautoupds.exe");
sub_40D8D0(L"thebat.exe");
sub_40D8D0(L"dbsnmp.exe");
sub_40D8D0(L"ocomm.exe");
sub_40D8D0(L"thebat64.exe");
sub_40D8D0(L"ensv.exe");
sub_40D8D0(L"ossd.exe");
sub_40D8D0(L"thunderbird.exe");
sub_40D8D0(L"excel.exe");
sub_40D8D0(L"onenote.exe");
sub_40D8D0(L"visio.exe");
sub_40D8D0(L"firefoxconfig.exe");
sub_40D8D0(L"orale.exe");
sub_40D8D0(L"winword.exe");
sub_40D8D0(L"infopath.exe");
sub_40D8D0(L"outlook.exe");
sub_40D8D0(L"wordpad.exe");
sub_40D8D0(L"isqlplussv.exe");
sub_40D8D0(L"powerpnt.exe");
sub_40D8D0(L"xfssvon.exe");
sub_40D8D0(L"msaess.exe");
sub_40D8D0(L"sqboreservie.exe");
sub_40D8D0(L"tmlisten.exe");
sub_40D8D0(L"msftesql.exe");
sub_40D8D0(L"sqlagent.exe");
sub_40D8D0(L"PNTMon.exe");
sub_40D8D0(L"mspub.exe");
sub_40D8D0(L"sqlbrowser.exe");
sub_40D8D0(L"NTAoSMgr.exe");
sub_40D8D0(L"mydesktopqos.exe");
sub_40D8D0(L"sqlservr.exe");
sub_40D8D0(L"Ntrtsan.exe");
sub_40D8D0(L"mydesktopservie.exe");
sub_40D8D0(L"sqlwriter.exe");
sub_40D8D0(L"mbamtray.exe");
sub_40D8D0(L"mysqld.exe");
sub_40D8D0(L"steam.exe");
```

그림 1-11 | 강제종료 프로세스 목록

```
if ( v5 != (HANDLE)-1
  && !StrStrW(&First, L"Chrome")
  && !StrStrW(&First, L"Mozilla")
  && !StrStrW(&First, L"Recycle.bin")
  && !StrStrW(&First, L"Microsoft")
  && !StrStrW(&First, L"AhnLab")
  && !StrStrW(&First, L"Windows")
  && !StrStrW(&First, L"All Users")
  && !StrStrW(&First, L"ProgramData")
  && !StrStrW(&First, L"Program Files (x86)")
  && !StrStrW(&First, L"PROGRAM FILES (X86)")
  && !StrStrW(&First, L"Program Files")
  && !StrStrW(&First, L"PROGRAM FILES") )
```

그림 1-12 | 암호화 제외 경로

클롭 랜섬웨어의 특징적인 점은 암호화 진행 시 일부 경로와 파일을 암호화 대상에서 제외하는 점이다. [그림 1-12]은 암호화 제외 경로를 나타낸 것이다. 경로에 해당 문자열을 포함하고 있으면 암호화 대상에서 제외된다.

[그림 1-13]은 암호화 제외 파일 목록이다. 제외 경로와 마찬가지로 파일명에 해당 문자열을 가지고 있으면 암호화 대상에서 제외된다.

```
if ( !(FindFileData.dwFileAttributes & 0x10)
  && lstrcmpW(FindFileData.cFileName, L"..")
  && lstrcmpW(FindFileData.cFileName, L".")
  && !StrStrW(FindFileData.cFileName, L"ClopReadMe.txt")
  && !StrStrW(FindFileData.cFileName, L"ntldr")
  && !StrStrW(FindFileData.cFileName, L"NTLDR")
  && !StrStrW(FindFileData.cFileName, L"boot.ini")
  && !StrStrW(FindFileData.cFileName, L"BOOT.INI")
  && !StrStrW(FindFileData.cFileName, L"ntuser.ini")
  && !StrStrW(FindFileData.cFileName, L"NTUSER.INI")
  && !StrStrW(FindFileData.cFileName, L"AUTOEXEC.BAT")
  && !StrStrW(FindFileData.cFileName, L"autoexec.bat")
  && !StrStrW(FindFileData.cFileName, L".Clop")
  && !StrStrW(FindFileData.cFileName, L"NTDETECT.COM")
  && !StrStrW(FindFileData.cFileName, L"ntdetect.com")
  && !StrStrW(FindFileData.cFileName, L".dll")
  && !StrStrW(FindFileData.cFileName, L".DLL")
  && !StrStrW(FindFileData.cFileName, L".exe")
  && !StrStrW(FindFileData.cFileName, L".EXE")
  && !StrStrW(FindFileData.cFileName, L".sys")
  && !StrStrW(FindFileData.cFileName, L".SYS")
  && !StrStrW(FindFileData.cFileName, L".OCX")
  && !StrStrW(FindFileData.cFileName, L".ocx")
  && !StrStrW(FindFileData.cFileName, L".LNK")
  && !StrStrW(FindFileData.cFileName, L".lnk") )
```

그림 1-13 | 암호화 제외 파일

클롭 랜섬웨어는 [그림 1-14]와 같이 공격자의 공개키가 파일 내부에 포함되어 있으며, 해당 공개키는 파일 암호화 시 사용된다

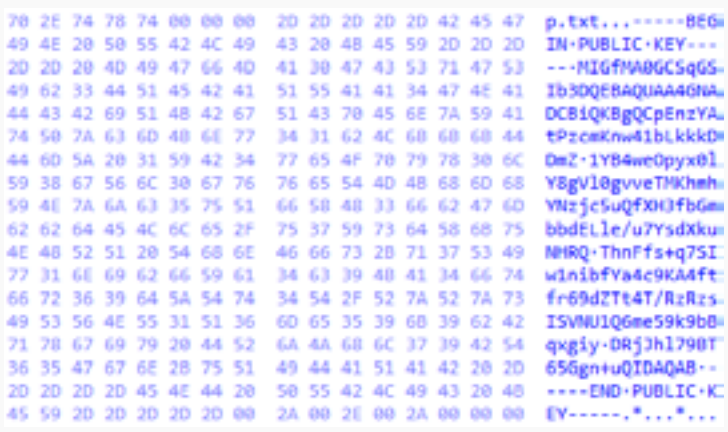


그림 1-14 | 랜섬웨어 공격자의 공개키

또한 클롭 랜섬웨어는 AES 알고리즘을 이용하여 파일 암호화를 진행한다. 사용자 PC에서 생성한 대칭키로 대상 파일을 암호화하는데, [그림 1-15]와 같이 클롭 랜섬웨어의 시그니쳐인 'Clop^_-'를 삽입하고 공격자의 공개키로 사용한 대칭키를 암호화하여 시그니쳐의 뒷부분에 사용한다.

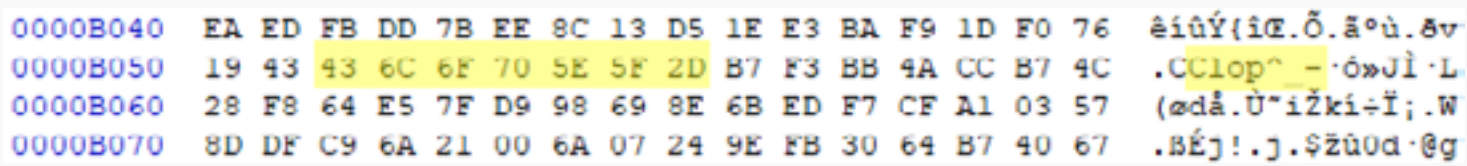


그림 1-15 | 암호화된 파일의 시그니쳐

[그림 1-16]은 암호화 전과 후의 파일 구조를 비교하여 나타낸 것이다.

그림 1-16 | 암호화 전/후 파일 비교

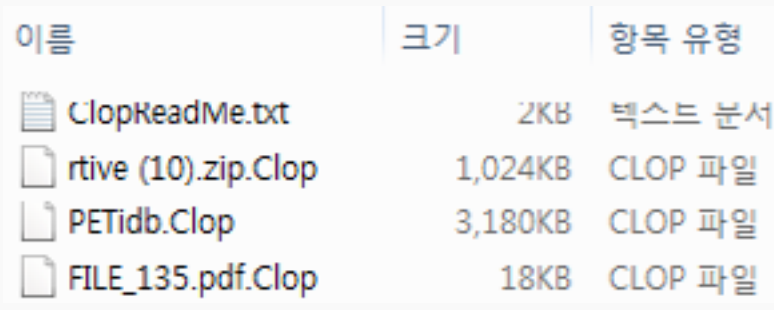


그림 1-17 | 암호화된 파일

최종적으로 암호화된 파일은 [그림 1-17]과 같이 파일명이 [원본파일명].Clop로 변경된다.

지금까지 살펴본 내용 및 두 악성코드의 연관성을 통해 현재 유포 방식 및 감염 방식이 확인되지 않은 클롭 랜섬웨어의 감염 벡터 중 하나로 Flawed Ammyy RAT이 사용되었음을 추정할 수 있다. Flawed Ammyy RAT은 원격제어를 통해 정보 유출 및 악성코드 설치를 위한 명령 수행이 가능하기 때문이다. [그림 1-18]은 Flawed Ammyy RAT와 클롭 랜섬웨어 이들 두 악성코드를 이용한 공격자

의 유포 방법을 정리한 것이다.

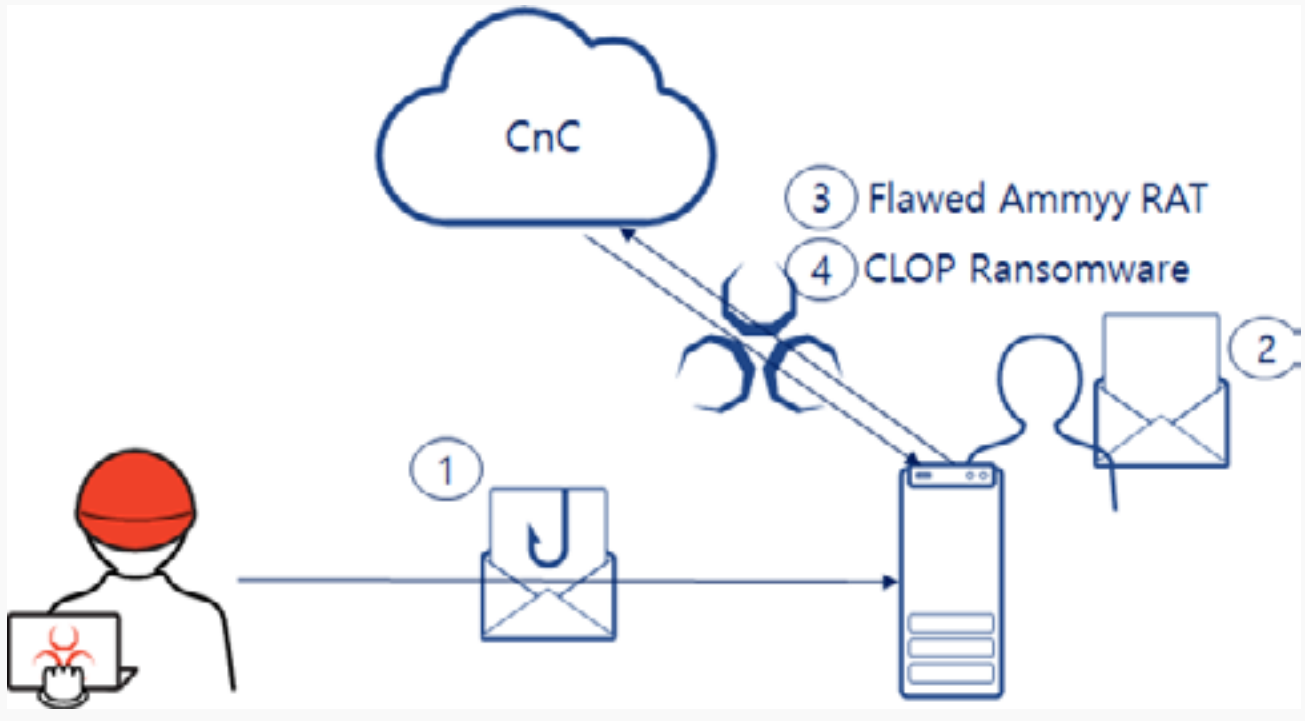


그림 1-18 | 유포 방법 추정

4. 결론

ASEC에서 분석한 결과 Flawed Ammyy RAT과 클롭 랜섬웨어는 활동 시기가 겹치는 점, 국내 사용자를 직접적인 대상으로 하는 점, 백신 프로그램을 우회하는 루틴을 포함하는 점, 그리고 여러 유효한 인증서를 통해 변형을 포함하는 다수의 악성코드들을 서명하고 유포하였다는 점 등 다수의 공통점이 존재한다. 또한 두 악성코드가 동일한 서명을 공유하고 있고, 공격 대상 또한 기업 사용자라는 점으로 미루어 동일한 공격자가 제작한 것으로 추정할 수 있다.

기업 사용자를 주요 공격 대상으로 삼는 Flawed Ammyy RAT, 클롭 랜섬웨어와 같은 악성코드 피해를 최소화하기 위해서는 항상 윈도우 보안 패치 및 V3 백신 프로그램을 최신 업데이트 상태로 유지하는 것이 중요하다. 또한 사내에서 신뢰할 수 없는 출처의 메일 등의 첨부 파일 실행 및 확인되지 않은 웹 페이지 방문은 삼가는 등 각별한 주의가 필요하다.

V3 제품군에서는 Flawed Ammyy RAT과 클롭(CLOP) 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

< V3 제품군 진단명>

- XLS/Downloader
- MSI/Downloader
- BinImage/Encoded
- Trojan/Win32.Agent
- Trojan/Win32.Downloader
- Backdoor/Win32.Agent
- Trojan/Win32.ClopRansom

악성코드 상세 분석

ANALYSIS-IN-DEPTH

- 워너크라이의 그림자,
  2019년형 SMB 취약점 공격

악성코드 상세 분석

Analysis-In-Depth

워너크라이의 그림자, 2019년형 SMB 취약점 공격

지난 2017년 5월 약 30만대 이상의 시스템을 감염시키며 전 세계를 랜섬웨어 공포로 몰아넣었던 워너크립터(WannaCryptor, 일명 워너크라이)는 윈도우 SMB 보안 취약점(MS17-010)을 이용하여 급속도로 확산됐다. 당시 국내에서도 다수의 기관 및 기업이 피해를 입은 것으로 보고된 가운데, 약 2년의 시간이 경과한 최근까지도 워너크립터가 사용한 해당 SMB 취약점(MS17-010)을 통해 국내 기업을 노린 공격이 활발하게 이뤄지고 있다. 특히 이번에 발견된 악성코드는 '코인마이너'라는 암호화폐 채굴형 악성코드로 더욱 각별한 주의가 필요하다.

이번 보고서에서는 2018년부터 2019년 1분기 현재까지 국내에서 발생한 SMB 취약점(MS17-010) 공격 사례를 상세히 살펴본다.

1. NrsMiner 악성코드 공격 사례 (2018년)

2018년 3월, 해외에 위치하고 있는 국내 기업을 대상으로 NrsMiner 악성코드가 감염된 사례가 발견되었다. 해당 악성코드는 워너크립터가 이용하는 SMB 취약점(MS17-010)을 통해 내부 네트워크를 스캐닝하고, 취약한 시스템인 경우 암호화폐의 한 종류인 모네로 코인을 채굴하는 악성코드를 설치한다. NrsMiner 악성코드는 ZIP 압축 파일 형식의 패키지 파일로 구성되어 있으며, 패키지 파일명(MsraReportDataCache32.tlb)은 변형마다 다른 것으로 확인되었다.

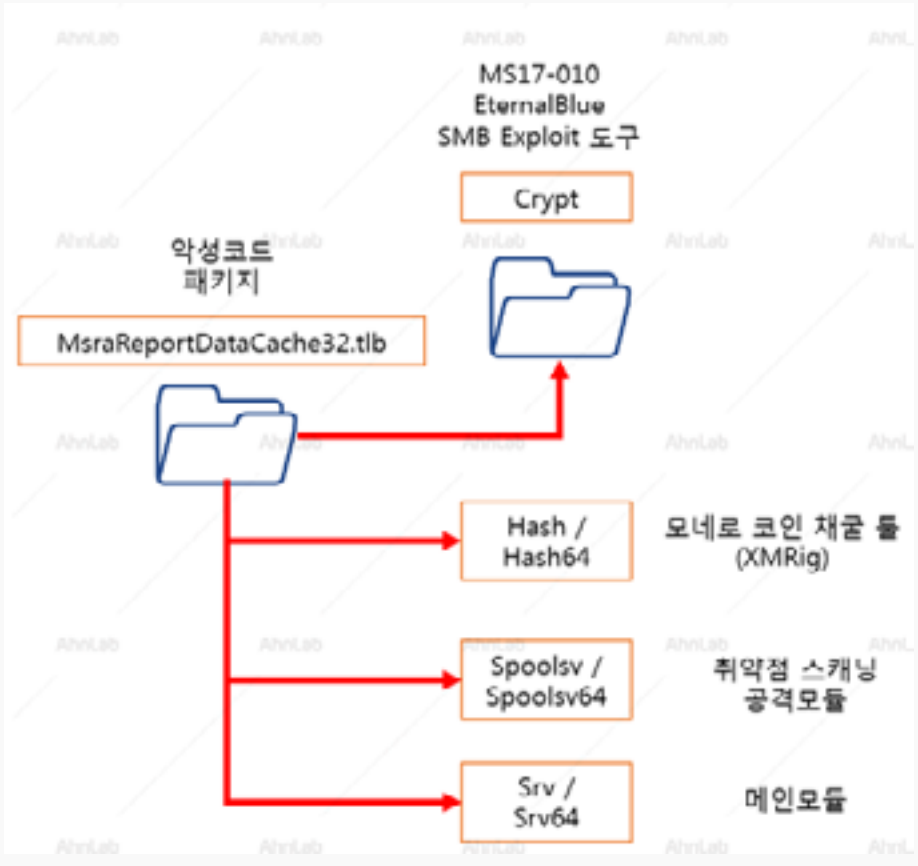


그림 2-1 | NrsMiner 패키지 구조

[그림 2-1]는 NrsMiner 패키지 파일의 구조이다. 취약점을 통한 시스템 감염 시 설치된 OS 환경에 맞게 Srv, Srv64 파일 중 하나를 'tpmagentservice.dll' 파일명으로 변경하여 서비스로 등록한다. 이는 이후에 나올 공격 모듈과 채굴 툴을 생성 및 실행하는 주체가 된다. Spoolsv, Spoolsv64는 패키지 파일을 로드하여 환경에 따라 필요한 모듈을 설치하며, 특히 시스템 내 MS17-010 취약점을 스캐닝한다. Hash, Hash64는 모네로 코인을 채굴하는 것으로 알려진 공개 툴인 XMRig이다. Crypt 폴더는 공개된 MS17-010 취약점 관련 도구와 파일들이 포함된 ZIP 형태의 압축 파일이다.

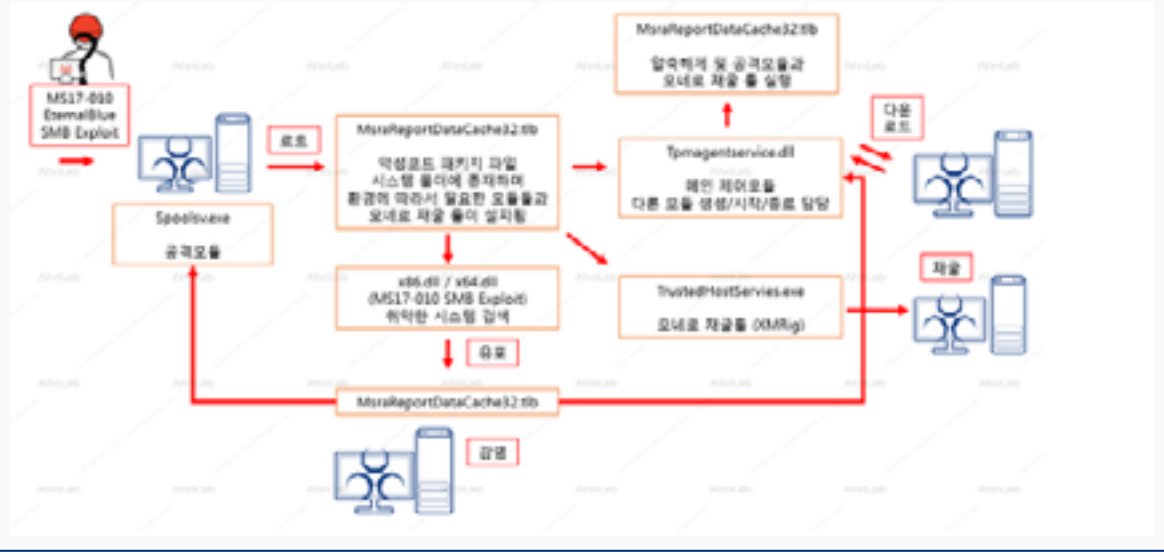


그림 2-2 | Spoolsv.exe 실행 흐름

[그림 2-2]는 공격 모듈인 Spoolsv.exe 파일의 동작 방식이다. 'spoolsv.exe'은 'MsraReportDataCache32.tlb 패키지를 압축 해제하여 내부 모듈들을 로드하는 기능을 수행한다. 해당 tlb 파일은 앞서 살펴본 [그림 2-1] NrsMiner 패키지 구조에서 설명한 것처럼 hash, hash64 파일명의 XMRig(공개 모네로 채굴 툴), spoolsv, spoolsv64 파일명의 공격 모듈, 그리고 srv, svr64 파일명의 메인 모듈, 이터널블루(Eternalblue) SMB 취약점인 MS17-010 관련 Crypt 파일명의 압축 파일로 구성되어 있다. Spoolsv.exe 파일이 실행되면 6개의 스레드(Thread)를 구동하며, 다음의 일련의 과정을 수행한다.

먼저 시스템에 [표 2-1]의 폴더를 생성한 다음, 악성코드 패키지 파일을 로드한 후 로드된 파일의 압축을 해제한다.

- %Windows%\SecureBootThemes\
- %Windows%\SecureBootThemes\Microsoft\
- %Windows%\System32\MsraReportDataCache32.tlb (*.tlb 파일 (zip) 압축 해제)
- %Windows%\SecureBootThemes\Microsoft\crypt (압축 해제 완료 후 삭제)

표 2-1 | Spoolsv.exe 파일이 생성하는 폴더

또한 SMB 취약점 전파를 위해 'MsraReportDataCache32.tlb' 파일 내부에 있는 crypt 압축 폴더 내 svchost.exe(Eternalblue-2.2.0.exe)와 spoolsv.exe(Doublepulsar-1.3.1.exe)를 실행한다. 윈도우 환경에 따라 x64.dll, x86.dll 파일을 로드하는데, 해당 파일명은 spoolsv64.exe 내 하드코딩 되어 있다.

최종적으로 'spoolsv64.exe' 프로세스의 스레드에서 취약점 스캔을 수행하며 성공 시 x64.dll, x86.dll 모듈에서 타겟 시스템으로 *.tlb 파일을 복사하고 압축 해제한다. 이 후 tpmagentservice.dll으로 파일명을 변경하고 srv 서비스를 등록한 후 'spoolsv64.exe' 파일을 재실행하는 과정을 거친다.

한편 취약점을 이용한 내부 네트워크 전파는 [그림 2-3]과 같이 진행된다.(x64 윈도우 기준)

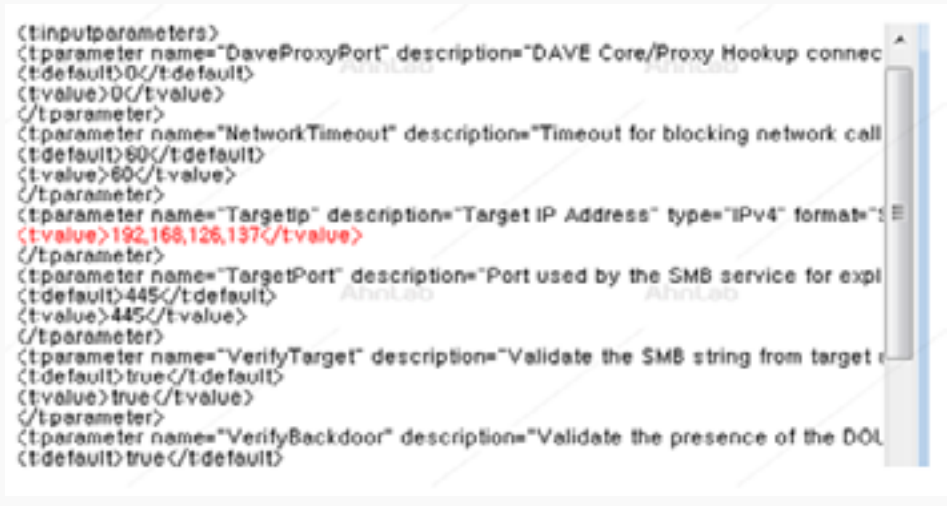


그림 2-3 | 이터널블루(Eternalblue) 공격 툴 설정 파일

이후 이터널블루(Eternalblue) 도구가 실행되는데, [표 2-2]의 stage1.txt, stage2.txt과 같이 2개의 로그 파일이 생성된다.

```
cmd.exe /c C:\WINDOWS\SecureBootThemes\Microsoft\\svchost.exe > stage1.txt // Eternalblue
cmd.exe /c C:\WINDOWS\SecureBootThemes\Microsoft\\spoolsv.exe > stage2.txt // Doublepulsar
```

표 2-2 | 생성된 로그 파일

stage1.txt 파일은 이터널블루 툴의 실행 로그 파일이며, 상세 내용은 [그림 2-4]와 같다.

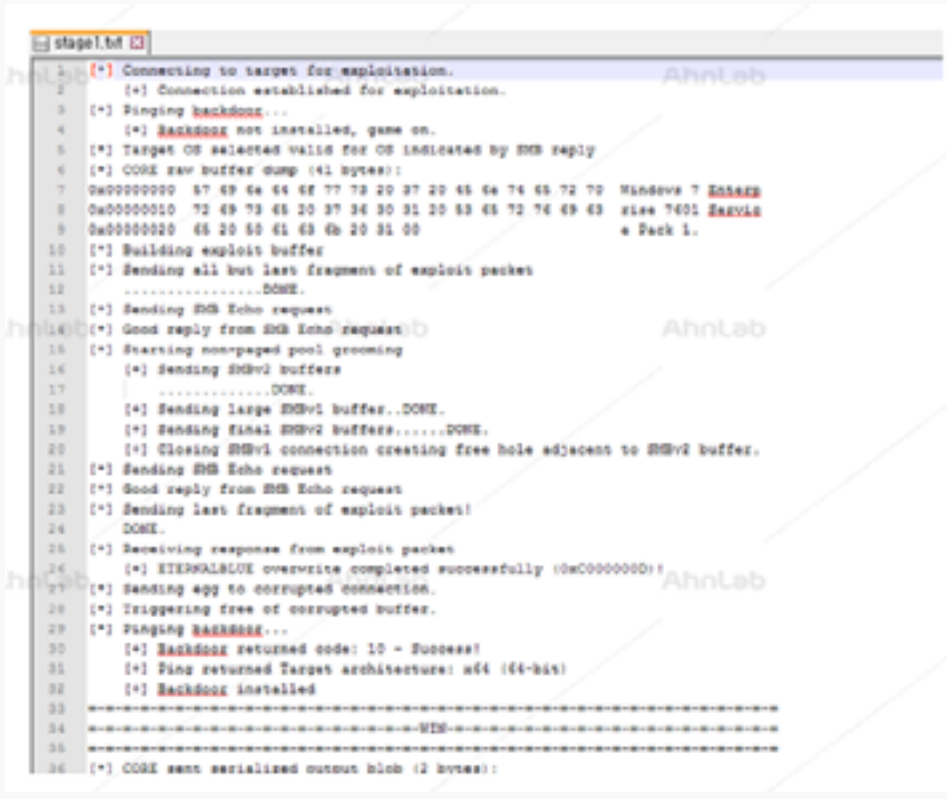


그림 2-4 | 이터널블루(Eternalblue) 툴 로그 파일

또한 취약점 패킷은 [그림 2-5]와 같이 타깃 시스템에 전송된다.

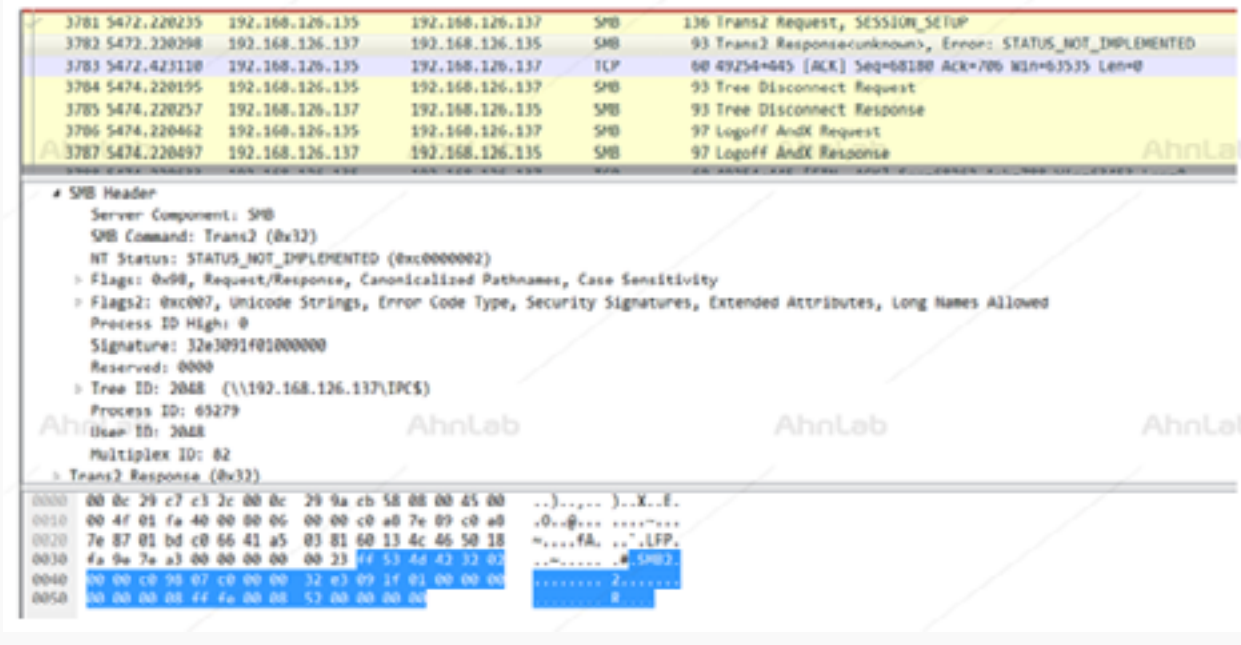


그림 2-5 | 취약점 패킷 전송

이 후 'lsass.exe' 파일에 의해 악성코드 패키지 파일인 'MsraReportDataCache32.tlb' 파일이 원격 시스템 내에 생성된다. [그림 2-6]은 취약점 공격 성공 후에 생성된 패키지 파일이다. 전송되는 패키지 파일은 102,400 바이트씩 분할하여 파일에 기록되며, 별도의 암호화 과정없이 플레인 바이너리를 직접 전송하도록 되어 있다.

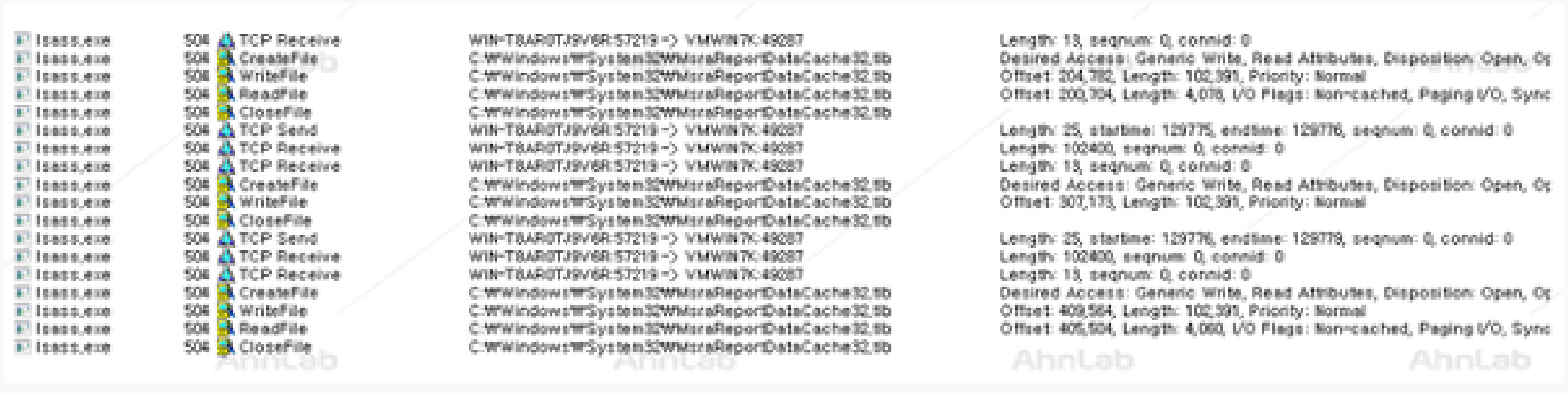


그림 2-6 | 취약점 공격 성공 후 lsass.exe 의한 *.tlb 패키지 파일 생성

패킷 전송 시 사용하는 TCP 포트는 동적으로 할당한 492xx 대역과 572xx 대역을 사용한다. 테스트 과정에서는 src:49287, dest:57219가 사용되었다.

취약점 공격이 성공하면 'MsraReportDataCache32.tlb' 파일이 전송되고, 전송된 파일이 압축 해제된다. 압축 해제 폴더는 Windows\SecureBootThemes\Microsoft로 동일하다. srv64 파일은 system32\tpagentservice.dll 파일명으로 변경된 후 시스템에 복사되고, 서비스로 등록되어 동작한다. 해당 모듈은 메인 제어 모듈로 tlb 내부의 spoolsv64.exe 파일을 실행하고 또 다른 취약한 시스템을 찾아 패키지 파일을 유포한다. 최종적으로 모네로 코인을 채굴하는 XMRig 툴(hash, hash64 파일명)이 실행되는데, 마이닝 풀(Mining Pool) 주소는 [표 2-3]과 같다.

-o p3.qsd2xjpzfky.site:45560 -u wvsymvtjeg
-o p1.mdfr6avyyle.online:45560 -u lqbpyceupn
-o p1.qsd2xjpzfky.site:45560 -u odiqldkee2
-o p5.mdfr6avyyle.online:45560 -u jodkrofar
-o p5.qsd2xjpzfky.site:45560 -u dkw1kaxlep

표 2-3 | 마이닝 풀(Mining Pool) 주소

메인 제어 모듈은 악성코드 패키지 파일인 'MsraReportDataCache32.tlb' 파일을 압축 해제한 후, 공격 모듈과 모네로 코인 채굴 프로그램인 TrustedHostServices.exe을 생성하여 실행시킨다. 메인 제어 모듈의 주요 행위 코드는 [그림 2-7]과 같다.

```
sprintf_sub_1800017A0((__int64)&Dst, (__int64)"%s\\MsraReportDataCache32.tlb", (__int64)&Buffer, v6);
memset(&FileName, 0, 0x104ui64);
sprintf_sub_1800017A0((__int64)&FileName, (__int64)"%s\\%s", (__int64)&Buffer, (__int64)"TrustedHostServices.exe");
v7 = CreateFileA(&FileName, 0x80000000, 1u, 0i64, 3u, 0, 0i64);
if ( v7 == (HANDLE)-1i64 )
{
  sub_180003570((__int64)&Dst, "hash64", (__int64)&Buffer);
  renamefile_sub_180003480((__int64)&Buffer, (__int64)&Buffer, (__int64)"hash64", (__int64)"TrustedHostServices.exe");

while ( !v11 );
v11 = byte_180088C54 == 0;
*(_QWORD *)v10 = xmmword_180071140;          // @protonmail.com
*((_QWORD *)v10 + 1) = xmmword_180071150;    // -p x -t %d --don
*((_QWORD *)v10 + 4) = 'evel-eta';           // ate-level=1
*((_QWORD *)v10 + 10) = '1-l';
if ( !v11 )
{
  v12 = &v19;
  do
    v11 = (v12++)[1] == 0;
  while ( !v11 );
  *(_QWORD *)v12 = 'hecin-- ';               // --nicehash
  *((_QWORD *)v12 + 2) = 'hsa';
}
memset(&CommandLine, 0, 0x800ui64);
sprintf_sub_1800017A0((__int64)&CommandLine, (__int64)&v20, v9, v13);
result = CreateFileA(&strMinerName, 0x80000000, 1u, 0i64, 3u, 0, 0i64);
if ( result == (HANDLE)-1i64 )
  break;
CloseHandle(result);
v4 = createProcess_sub_180003890(&strMinerName, &CommandLine);
Sleep(0x12Cu);
```

그림 2-7 | 메인 제어 모듈의 주요 행위 코드

또한 [표 2-4]와 같이 이전 버전으로 추정되는 파일들을 삭제하고, 서비스 중지 및 작업 스케줄 삭제를 수행한다.

```
dnsclientprovider_userdata.mof
NrsDataCache.tlb
SecUpdateHost.exe
ServicesHost.exe
settings7283.dat
SysprepCache.ini
vmichapagentsrv.dll
("schtasks.exe", " /Delete /TN \"\\Microsoft\\Windows\\UPnP\\Services\" /F");
("sc.exe", " stop vmichapagentsrv");
("sc.exe", " delete vmichapagentsrv");
("schtasks.exe"," /End /TN \"\\Microsoft\\Windows\\Tcpip\\TcpipReportingServices\"");
("schtasks.exe"," /Delete /TN \"\\Microsoft\\Windows\\Tcpip\\TcpipReportingServices\" /F");
```

표 2-4 | 파일 삭제와 서비스 중지 및 작업 스케줄 삭제 수행

Mongoose 기반의 자체 웹 서버 기능이 있어, 다른 감염 시스템에 'MsraReportDataCache32.tlb' 패키지 파일 전송을 담당하며 포트 26397를 사용한다. 또한 외부로 인터넷 연결이 가능한 경우 [그림 2-8]과 같이 원격 서버로부터 악성 패키지 파일을 다운로드 받는다.

그림 2-8 | 다운로드 관련 코드

*.tlb 패키지는 메인 제어 모듈이 담당하는 웹 서버를 통해 업데이트되며, 다운로드 주소는 [표 2-5]와 같다.

rer.njaavfxcgk3.club/f79e53 (port: 4431)
ccc.njaavfxcgk3.club/a4c80e (port: 4433)
ccc.njaavfxcgk3.club/5b8c1d (port: 4433)
ccc.njaavfxcgk3.club/d0a01e (port: 4433)

표 2-5 | 다운로드 주소

2. 국내 POS 공격 사례 (2018년)

지난 2018년 7월, 국내 POS 단말기 10만대가 해킹되는 사례가 발생했다. 대부분의 POS 단말기에 인터넷 연결이 되지 않아 결제 서비스가 정상적으로 이루어지지 않는 증상이 나타났다. 당시 피해 업체 중 한 곳에서는 [그림 2-8]과 같이 윈도우 보안 취약점으로 인한 서비스 장애 및 보안 패치 관련 권고 사항을 게시했다.

그림 2-8 | POS 제조사 장애 관련 권고 사항

감염 기기는 대부분 보안에 취약한 XP 운영체제 환경이었으며, 모두 SMB 취약점 관련 보안 업데이트를 적용하지 않은 상태였다. 공격자는 워너크립터 랜섬웨어가 사용한 SMB 취약점을 이용하여 POS 시스템에 '고스트랫(GhostRAT)'이라는 백도어 악성코드와 '코인마이너'를 설치했다. [그림 2-9]는 악성코드의 동작 과정을 나타낸 것이다.

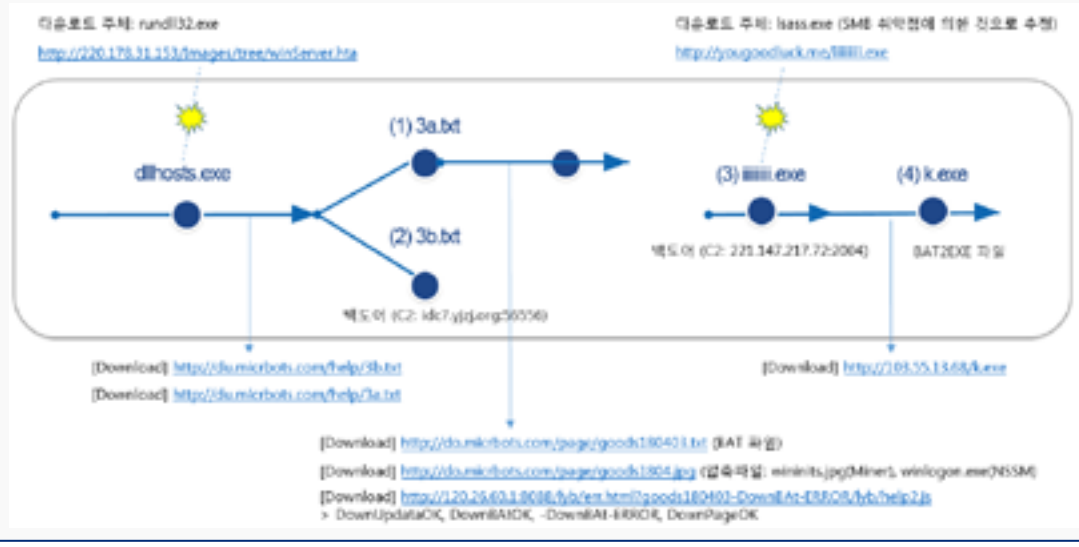


그림 2-9 | POS 악성코드 동작 과정(2018.07)

안랩 ASD(AhnLab Smart Defense) 엔진을 통해 확인한 결과 [그림 2-9]의 (3)번 파일인 iiiiiiii.exe을 생성한 대상이 윈도우 시스템 파일인 'lsass.exe'인 것으로 미루어, 해당 공격은 SMB 취약점을 이용한 공격으로 감염된 시스템에 의해 공격이 이루어진 것을 추정할 수 있다. '고스트랫(GhostRAT)' 원격제어 악성코드는 (2)번 3b.txt 파일이며, (1)번 3a.txt 파일에 의해 다운로드된 파일은 암호화폐 채굴 목적의 '코인마이너'로 확인되었다.

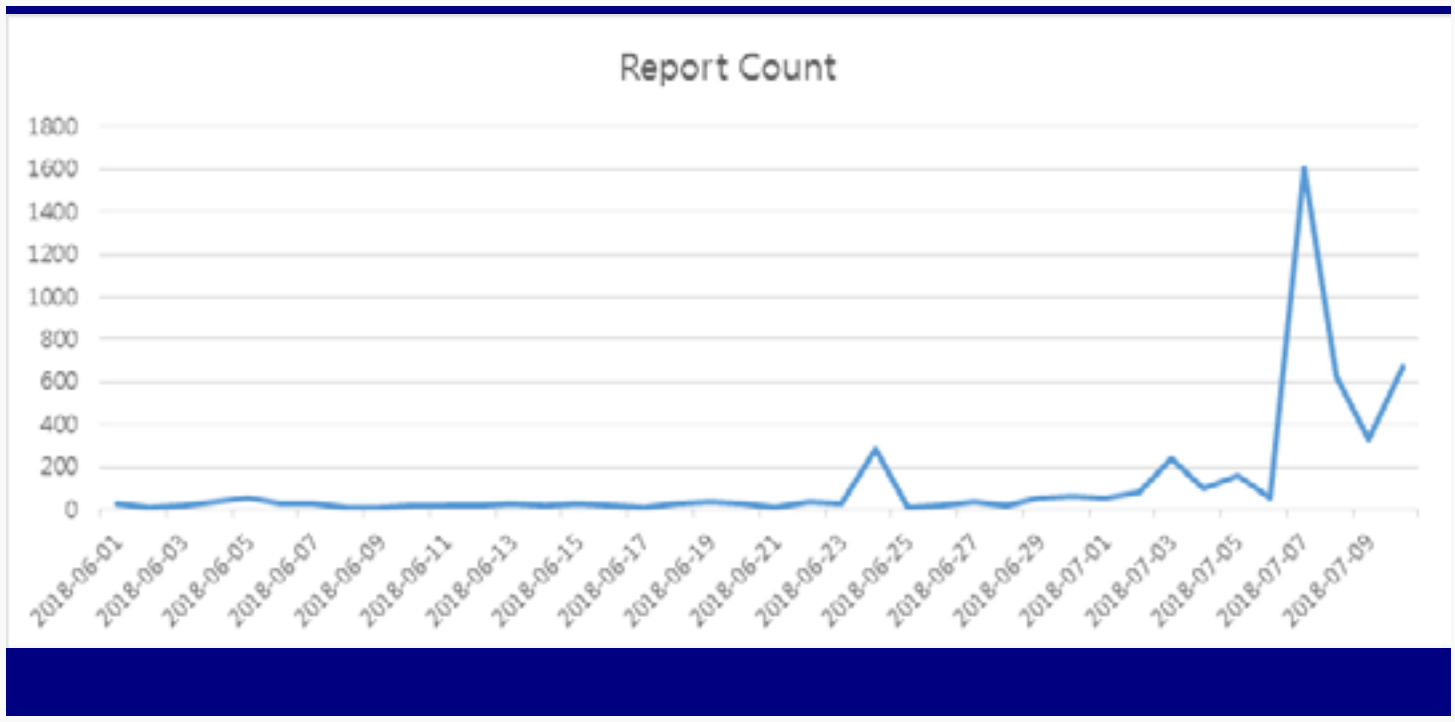


그림 2-10 | SMB 취약점 행위 탐지 리포트 (2018.06~2018.07)

V3 제품군에서는 이와 같은 SMB 취약점 공격에 대한 행위 탐지 기능을 제공하고 있으며, [그림 2-10]의 탐지 리포트를 살펴보면 국내 POS 해킹 피해가 있었던 2018년 6월 24일과 7월 7일에 공격 시도가 급증한 것을 확인할 수 있다.

3. 국내 POS 공격 사례 2 (2019년)

2019년 2월, 또다시 국내 POS 기기를 대상으로 SMB 취약점을 통한 '코인마이너' 악성코드 감염 사례가 확인되었다. ASEC은 블로그(https://asec.ahnlab.com/1196)를 통해 관련 내용을 공유한 바 있다. 전체적인 악성코드 동작 과정은 아래의 [그림 2-11]과 같다.

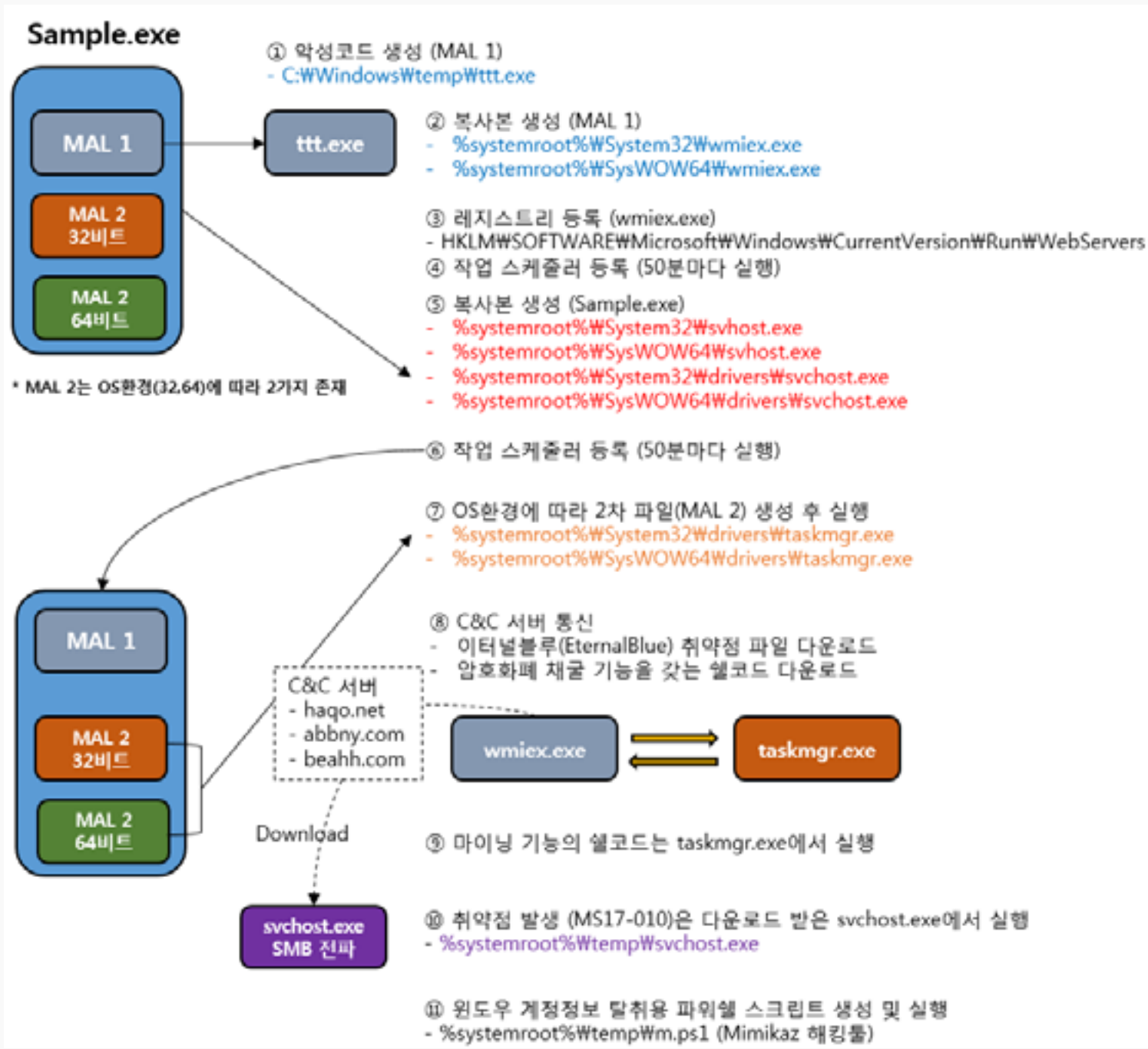


그림 2-11 | POS 악성코드 동작 과정 (2019.02)

악성코드인 Sample.exe 파일 내부에는 운영체제 환경에 따라 32비트, 64비트 2가지 형태를 포함하는 구조이며, 시스템 경로의 드라이버 폴더(%system%drivers)에 복사된 'svchost.exe' 파일이 SMB 취약점 공격을 발생시킨다. 최종적으로 다운로드되어 설치되는 파일은 '코인마이너' 악성코드와 윈도우 계정 정보 탈취용 해킹 툴인 'Mimikaz'이다. 2018년 7월의 국내 POS 공격 사례와는 달리 해당 '코인마이너' 악성코드는 실행 파일 형태가 아닌 스크립트로 동작하는 것이 특징이다. [그림 2-12]의 탐지 리포트에서 2019년 1월부터 2월까지의 SMB 취약점 관련 행위 탐지 수가 특정 기간에 급증한 것을 확인할 수 있다.

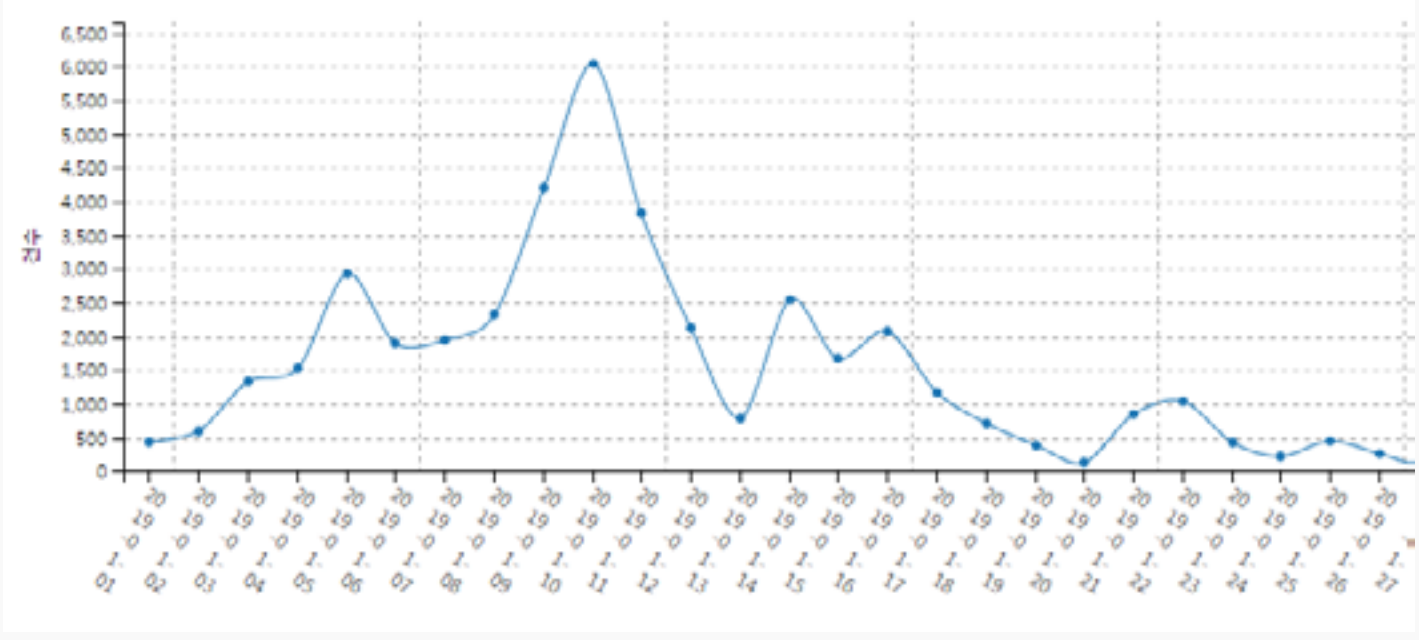


그림 2-12 | SMB 취약점 행위 탐지 리포트 (2019.01~2019.02)

4. 결론

지난 2008년에도 SMB 취약점(MS08-067)을 통해 전파 기능을 갖는 컨피커(Conficker)로 불리우는 웜(Worm)이 국내에 많은 피해를 입히고 수 년 동안 끊임없이 공격이 지속된 바 있다. 그만큼 국내 기업의 시스템은 SMB 서비스를 이용하는 환경이 많고, 그 중에는 보안 업데이트가 되지 않아 취약한 환경에 노출된 경우가 많아 각별한 주의가 필요하다. 이와 같은 피해를 예방하기 위해서는 마이크로소프트 윈도우 운영체제의 이터널블루(Eternalblue) SMB 취약점(MS17-010)과 관련된 보안 패치를 적용해야 한다.

이 보고서에서 살펴본 2018년 3월 NrsMiner 악성코드를 이용한 공격 사례 및 2018년 7월과 2019년 2월에 발생한 POS 공격 사례를 볼 때, SMB 취약점(MS17-010) 공격은 앞으로도 고도화되어 계속될 것으로 추정된다. 특히 보안에 취약한 환경의 국내 POS 기기에 대한 점검 및 보안 업데이트 등의 조치가 필수적이다.

[SMB 취약점(MS17-010) 패치]

- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

ASEC REPORT Vol.94

2019년 1분기

AhnLab

집필 안랩 시큐리티대응센터 (ASEC)

편집 안랩 콘텐츠기획팀

디자인 안랩 디자인랩

발행처 주식회사 안랩

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901