Security Lab
http://www.maxoverpro.org

바이러스 분석 과 전용 백신 제작
(Virus analysis and production to vaccine)

2006. 4. 18

By Maxoverpro[max](장상근)
maxoverpro@paran.com
http://www.maxoverpro.org

1. 서 론

2001년 Slammer 웜으로 인한 '1.25 인터넷 대란'이 일어날 만큼 현재 사이버 세상에서는 바이러스, 스파이웨어, 트로이, 웜, Bot 등. 많은 악성코드가 퍼져있어 인터넷에 연결되어 있는 것 자체가 위험에 노출되어 있는 것이나 다름없으며 악성코드는 진화하면서 보안 패치나 업데이트가 나오기 전에 취약점을 이용한 공격법이 나오는 Zero-Day가 현실이 되어 버렸다.

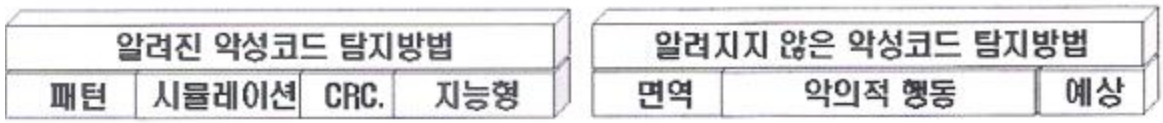
이 문서는 바이러스 패턴을 분석하는 방법에 대해 알아보겠으며 바이러스를 제작하거나 하는 방법은 기술하지 않는다. 이 문서에서 사용된 바이러스는 악성코드가 없이 주로 바이러스에서 나타나는 일반적인 현상들을 보기 위해 만든 실험용 바이러스임을 염두 해두길 바라며 실험용 바이러스를 치료하기 위해 바이러스를 분석하고 그에 따른 전용 백신을 제작하는 방법에 대해서 알아보도록 하겠다.

2. 본 론

Max는 자기의 메일로 "안녕! 오래간만이야~"라는 제목의 메일을 열었고 메일에 첨부된 loveme.exe 라는 파일을 실행시켰다. 할 일을 다하고 Max는 컴퓨터를 끄고 다음날 컴퓨터를 켜보니 컴퓨터가 30초 뒤 컴퓨터가 재부팅 되는 현상이 발생되어 바이러스에 걸렸다고 의심을 갖게 되었고 Max의 컴퓨터에는 백신이 설치되어 있긴 하지만 최신 업데이트가 안된 백신이고 바이러스도 잡히지 않았다. 그래서 Max는 바이러스를 치료하기 위해 전용 백신을 만들기로 했다.

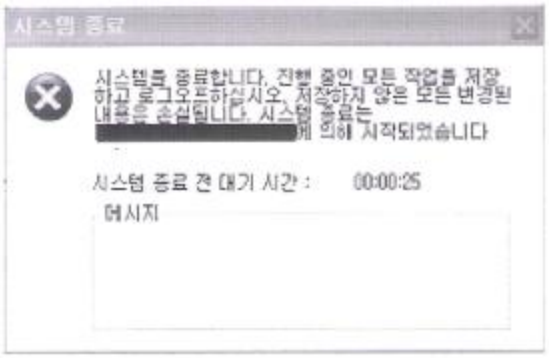
✔ 분 석

위 바이러스 분석에 앞서 바이러스등의 악성코드들을 어떻게 탐지해내야 할지에 대해 알아보도록 하겠다. 현재 악성코드를 탐지하는 방법으로 알려진 악성코드에 대한 탐지와 알려지지 않은 악성코드의 탐지 방법으로 나누어져있다.

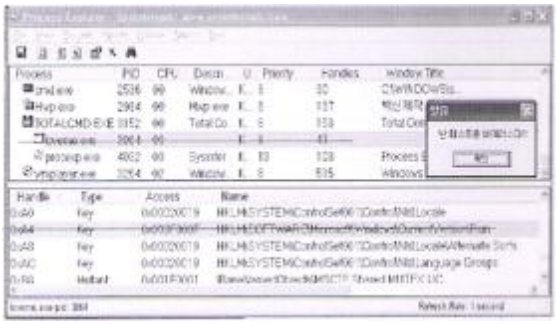


이 문서에서 다루는 바이러스는 패턴 방식으로 접근하는 것으로 패턴에는 프로세스 상태, 레지스트의 접근, 파일, 네트워크 상태에서의 나오는 일정한 패턴등을 찾아내 악성코드를 탐지해 내는 방법이다.

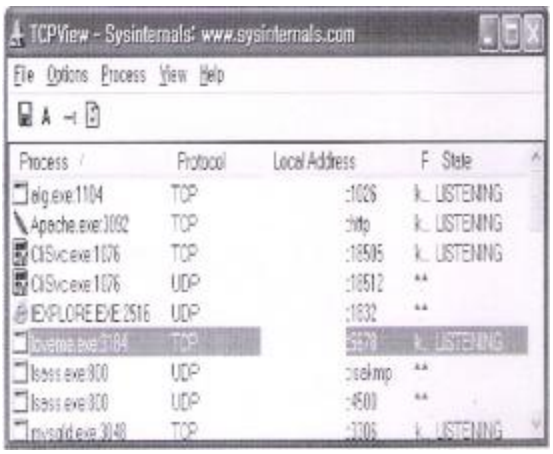
- 기초적인 분석법



첫째, loveme.exe를 실행시킨 후부터 컴퓨터를 킨 후 옆의 화면이 나오면서 계속 30초가 지나면 컴퓨터가 재부팅이 되는 현상을 확인을 하였다.



둘째, Process Explorer라는 Process 모니터링 프로그램으로 모니터링 해보면 loveme.exe가 실행되면서 어떠한 행동을 하는지 옆의 화면처럼 확인할 수 있다.



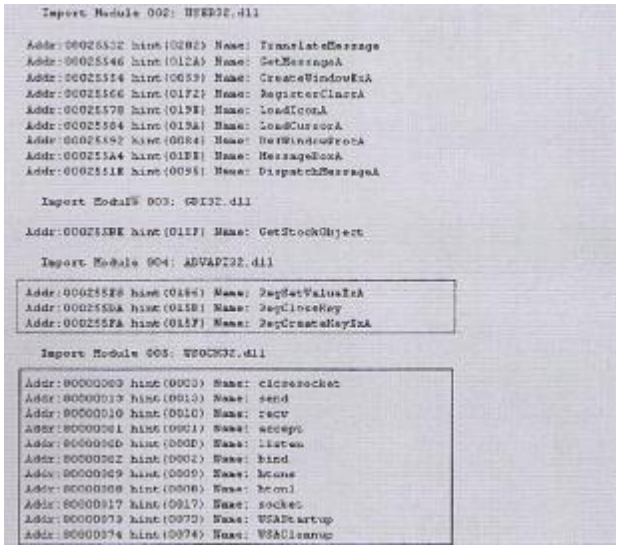
셋째, 옆의 그림은 TCPView라는 것을 통해 현재 어떤 프로세스가 어떤 포트를 열고 어떤 상태인지를 확인 할 수가 있는데 현재 loveme.exe가 샐힝 중인 상태에서 loveme.exe의 프로세스가 사용하는 포트가 5678로 LISTENING되어 있는 상태로 보아 바이러스가 5678포트로 백도어 기능을 수행하거나 네트워크를 통해 바이러스를 전파할 수 있는 가능성을 확인하였다.

- 상세 분석

디코딩한 코드가 긴 관계로 바이러스의 중요 부분만 보기로 하겠다.

디코딩한 부분에서 레지스트리를 조작, 파일 생성을 확인하였으며 아래 부분 디코딩 부분에서는 소켓을 열르어두는 행위를 확인하였다.

기타 악성코드 등에서 사용할 수 있는 아래의 API를 알아둘 필요가 있다.



- Kernel32.dll

CreateFile, CopyFile, DeleteFile, Movefile
FindFirstFile, FindNextFile,
WriteProcessMemory, ReadProcessMemory,
CreateProcess, OpenProcess, GetStartupinfo,
TerminateProcess, CreateRemoteThread

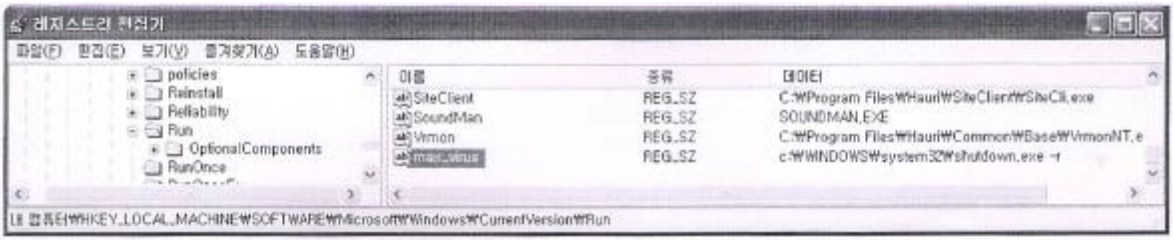
- user32.dll

SetWindowsHook, CallNextHook

- advapi32.dll

RegCreateKey, RegOpenKey, RegSetValue, RegDeleteValue, RegEnumKey,
RegEnumValue, CreateService, DeleteService, inet_adr, htons, gethostbyname

loveme.exe를 위처럼 디어셈블 해보면 프로그램의 작동구조와 무슨 짓을 하는지 알 수 있었다. 정리하자면 loveme.exe를 실행하게 되면 C:₩ 아래 max_virus.txt라는 파일이 생기며, 'Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run'이란 레지스트리에 무언가가 생긴 것을 확인 할 수 있다. 확인해 보면 계속 부팅이 되는 원인을 알 수 있었고, 그리고 소켓을 사용하여 특정 포트를 열어두는 행위를 확인할 수 있었다.



'Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run'의 위치에 max_virus라는 이름으로 'c:₩WINDOWS₩system32₩shutdown -r'라고 값이 들어가 있는 것을 확인했다.
이제 실험용 바이러스의 실체를 알았으니 쉽게는 그냥 max_virus란 이름의 레지스트리를 지우고 max_virus.txt를 삭제하고 loveme.exe를 삭제하면 되지만, 다른 누군가는 혹시나 바이러스에 고생 하고 있을 사람을 위해 전용백신을 제작하는 법을 알아보도록 하겠다.

✔ 전용 백신 제작.

바이러스 분석을 통해 실험용 바이러스 loveme는 loveme.exe를 실행하면 C:₩에 loveme.exe 파일과 max_virus.txt를 생성하며 레지스트의 ...
'Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run'의 위치에 max_virus라는 이름으로 ':₩WINDOWS₩system32₩shutdown -r'를 생성하여 컴퓨터가 재부팅 되도록 shutdown이 자동으로 실행되어 30초 뒤에 계속 부팅되는 현상이 발생하였다. 이 발생된 현상을 해결하기 위해서는 작동중인 loveme 바이러스 프로세스를 찾고 바이러스와 관련된 파일과 해당 레지스트리를 지워줌으로서 해결 할 수 있으며 전용 백신에 관한 것은 아래의 소스를 참고해 주길 바란다. 그리고 바이러스를 치료할 때에는 [안전모드]로 부팅해서 실행 시켜주기 바란다. 그 이유는 처음 실행시 레지스트리에 있는 shutdown이 윈도우에 들어가면서 작동되지 않는 이유도 잇으며 일반 모드에서는 죽여도 계속 프로세스가 살아나는 경우도 있기 때문에 [안전모드[에서 작업해 주도록 한다.

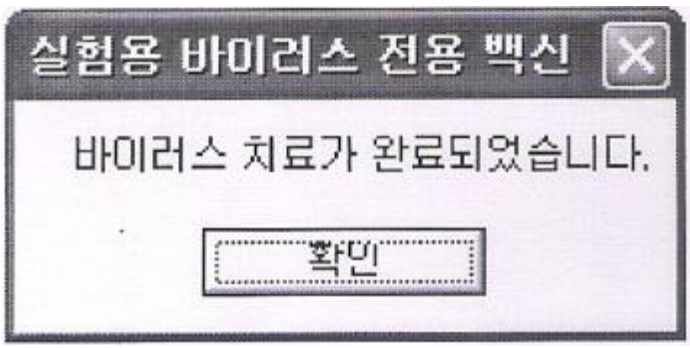
전용 백신 소스

```
#include "stdafx.h"
#include <tlhelp32.h>

BOOL KillProcess(char *pname);
int GetProcessList(char *pname);

//바이러스 관련 파일 삭제 처리 함수.
int DelFile(char *path)
{
        int count = 0;
        char buf[255];

        FILE *fp = NULL;
        sprintf(buf,"%s", path);
        fp=fopen(buf,"r");

        if( fp == NULL )
        return 0;

        fclose(fp);
```

```
            unlink(buf);
            return 1;
}

int kill_count = 0;

//프로세스 얻어 오는 함수.
int GetProcessList(char *pname)
{
    int Index = 0;
    HANDLE hProcessSnap = NULL;
    DWORD Return = FALSE;
    PROCESSENTRY32 pe32 = {0};
    HANDLE          hProcess;

    if ( (hProcessSnap=CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)) == INVALID_HANDLE_VALUE)
        return 0;

     pe32.dwSize = sizeof(PROCESSENTRY32);



if (Process32First(hProcessSnap, &pe32))
    {
        DWORD Code = 0;
        DWORD          dwPriorityClass;
   do
        {
            hProcess = OpenProcess (PROCESS_ALL_ACCESS, FALSE, pe32.th32ProcessID);

            dwPriorityClass = GetPriorityClass (hProcess);

                        if ( strcmp(pe32.szExeFile, pname) == 0 )
                                return pe32.th32ProcessID;
                        CloseHandle (hProcess);
        }
        while (Process32Next(hProcessSnap, &pe32));
    }
    CloseHandle (hProcessSnap);
            return -1;
}

//프로세스 죽이는 함수.
BOOL KillProcess(char *pname)
{
            int pid = GetProcessList(pname);

            if( pid == -1 )
                        return false;

            HANDLE hProcess = OpenProcess( PROCESS_ALL_ACCESS, FALSE, pid );

            if( hProcess == NULL )
                        return false;

            if(!TerminateProcess( hProcess, 1 ))
            {           CloseHandle( hProcess );
                        return false;
            }

            CloseHandle( hProcess );
            kill_count++;
            return true;
}

int APIENTRY WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow)
{
            int idel = 0 , delent = 0;
```

```
    int kill_count_save = 0;
    char prtstr[1024];

    //레지스트리 삭제 부분.
    HKEY dkey;
    ::RegOpenKeyGHKEY_LOCAL_MACHINE, "SoftwareWWMicrosoftWWWindowsWWCurrentVersionWWRun",&dkey);
    ::RegDeleteValue(dkey, "max_virus");

    //프로세스 종료 부분.
    KillProcess("LOVEME.EXE");
    KillProcess("loveme.exe");

    //파일 삭제 부분.
    DelFile("c:WWmax_virus.txt");
    DelFile("c:WWloveme.exe");

    sprintf(prtstr,"바이러스 치료가 완료되었습니다.Wn");
    MessageBox(NULL, prtstr, "실험용 바이러스 전용 백신", MB_OK);

    return 0;
}
```

✔ 전용 백신 실행



3. 결 론

이 문서에서는 간단한 실험용 바이러스를 통해 일반적인 바이러스 현상을 분석·확인하고 해당 바이러스를 치료할 수 있는 전용 백신 제작을 제작하는 기본적인 방법을 다뤘지만 점점 진화하는 악성코드와 심지어 사용자의 승인 없이 몰래 설치된 안티스파이웨어가 사용자의 PC에 있지도 않은 악성코드 치료를 위해 과금을 물리는 양심적이지 못한 보안 소프트웨어등 인터넷에 떠도는 검증되지 않은 소프트웨어와 파일 하나하나 여는 것에 대해 주의하길 바라는 의미에서 쓰여졌다. 차후 이 문서에 더하여 바이러스에 감염된 파일을 바이러스로부터 복구 하는 기술과 간단한 몇 가지 바이러스 패턴과 스팸 메일을 네트워크에서 걸러내는 기술에 대해서 다루도록 하겠다. 우선 이 문서를 통해 통합 백신이나 안티 스파이웨어 등을 만드는데 약간이나마 도움이 되길 바란다.