백도어 분석 보고서

By Dalgona (dalgona@wowhacker.org)

Email: zwsonic@gmail.com

http://www.wowhacker.org

1. 요약

모 회사의 웹 서버에 의심스러운 파일이 발견되어 이를 분석한 결과 백도어 프로그램인 것으로 밝혀졌다. 해당 백도어는 하드코딩된 IP주소로 접속하여 명령을 받아 수행하는 역할을 하는 것으로 파악된다. 이 백도어 파일은 아스키 문자로 이루어진 텍스트 파일이며 이것이 스크립트 해석기에 의해 디코딩되어 바이너리 파일로 변환된다. 바이너리는 실행파일의 형태로 존재하며 다시 dll 파일을 생성한다. 그리고 이 dll은 다른 응용프로그램에 붙어 실행되며 공격자의 명령을 수신하는 역할을 한다.

2. 개요

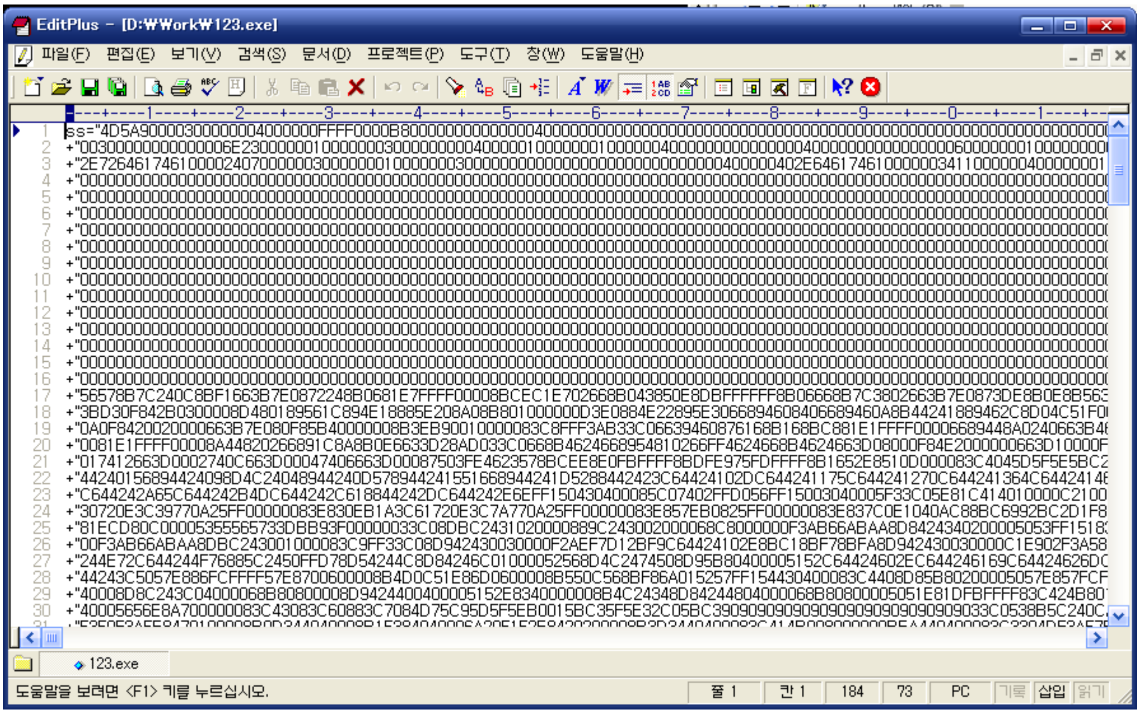
모 회사의 웹 서버에 의심스러운 파일이 발견되어 이를 분석하게 되었다. 처음 파일 이름이 123.exe로 되어 있어 실행파일일 것으로 추측하고 IDA와 OllyDbg를 이용하여 open하였으나 정상적인 바이너리로 인식하지 못하였다. 아주 독특한 형태의 코드라 생각하고 분석을 해 보려 했으나 도저히 알아먹을 수 없는 어셈블리코드들이었다.

생각을 바꾸어 에디터를 이용하여 파일을 오픈하니 전혀 의미 없는 숫자와 문자로 이루어진 데이터들이 보였고 아래에는 VBscript로 작성된 코드가 발견되었다. 해당 스크립트를 실행을 하면 백신(virus chaiser)이 악성 웜 감지를 알려왔다. 무시를 하고 계속 실행한 결과 또 다시 다른 이름의 악성 웜을 감지하였다고 알려왔으며 계속 진행을 하면서 모니터링 한 결과 특정 IP 주소로 접속을 시도하는 백도어인 것으로 파악되었다.

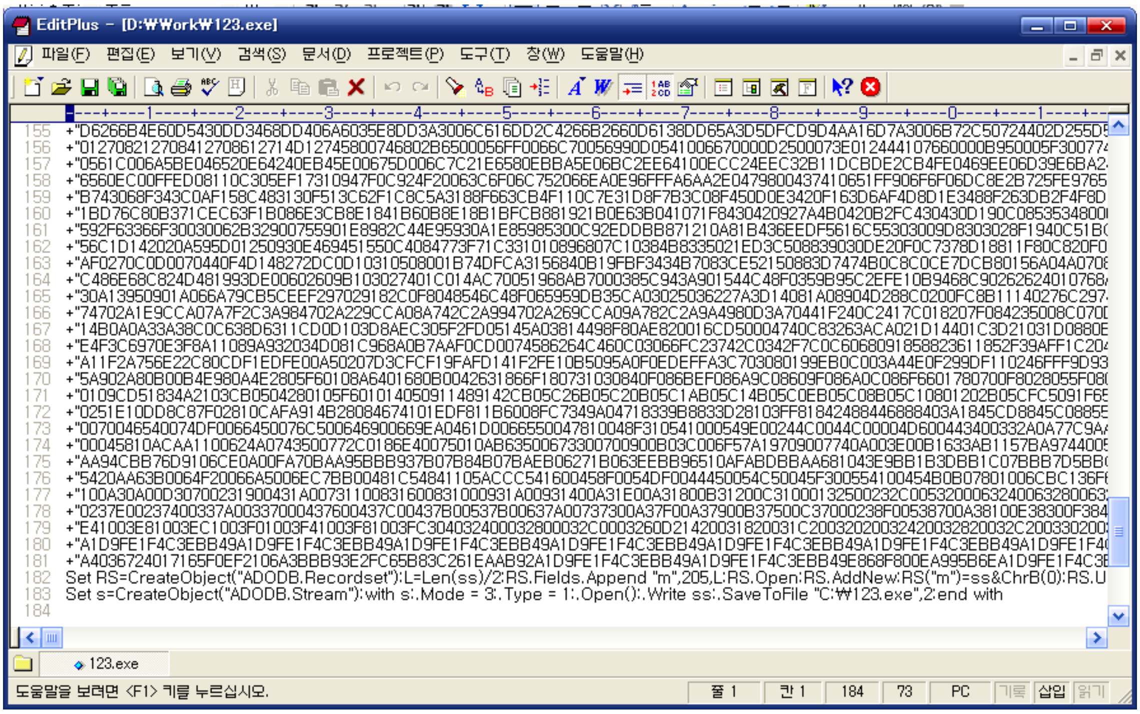
시간의 제약이 있어 바이너리를 모두 분석하지는 못하였으나 문자열 데이터를 파악한 결과 백도어가 확실시 되었다.

3. 외형

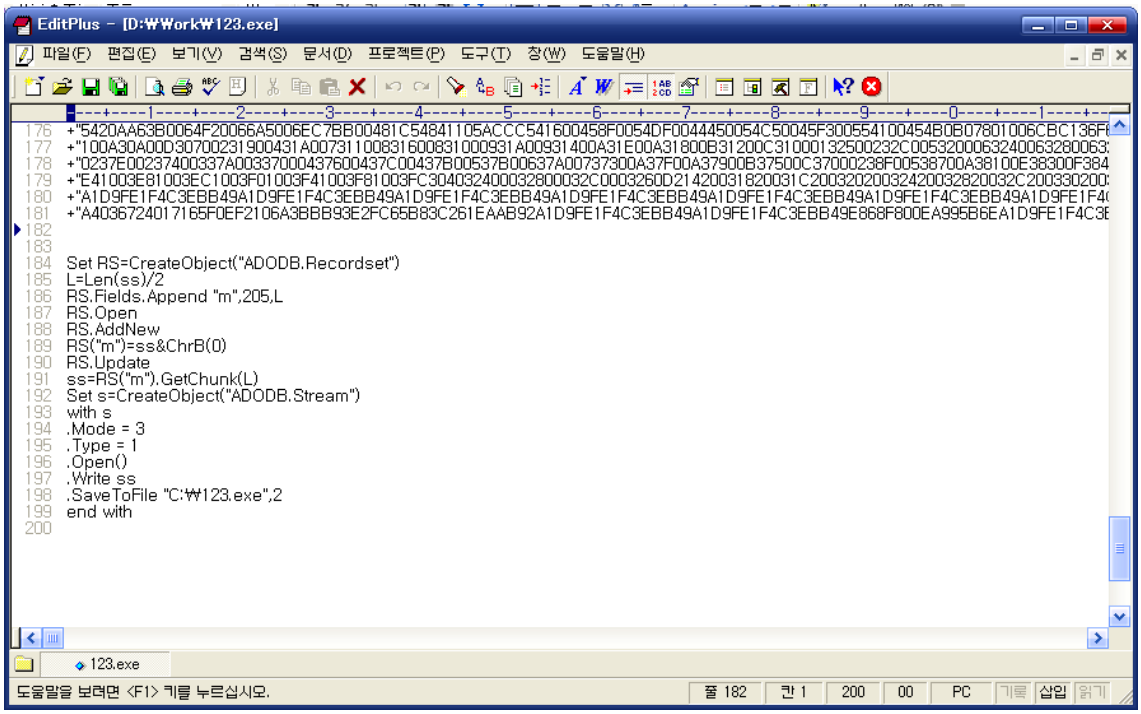
처음 발견한 파일의 이름은 123.exe였으며 93,808바이트의 크기를 가진다. 이것을 Edit Plus로 오픈한 모습은 아래와 같다.



스크롤을 좀 더 내려보면 아래와 같다.



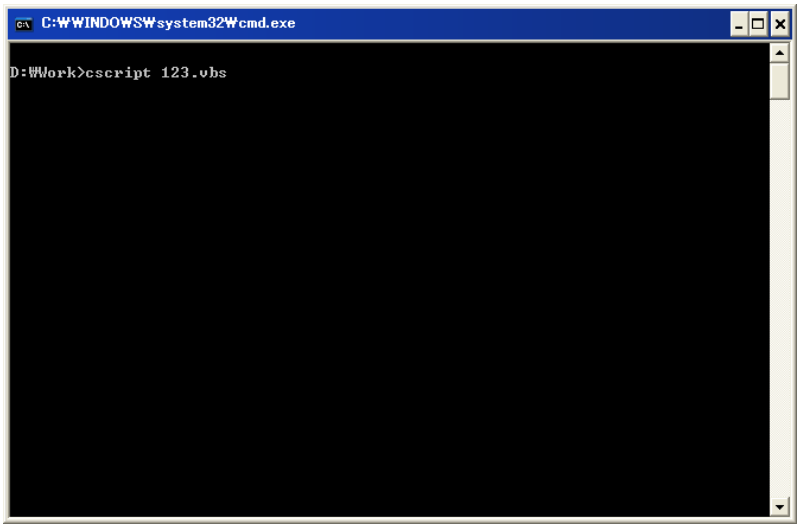
그림에서 볼 수 있는 바와 같이 앞부분의 문자열들은 “ss”라는 이름의 문자열형 변수로 선언되어 있으며 아래에서는 이를 decoding하는 vbscript 코드가 들어있다. 이 스크립트 코드를 풀어보면 아래와 같다.



"ss" 변수를 decoding한 다음 C:₩123.exe 라는 이름으로 저장하는 역할을 하는 코드이다. 이 코드를 직접 수행해 보았다.

4. 실행결과 및 분석

실행에 앞서 파일 이름을 123.exe에서 123.vbs 로 바꾸었다.



위와 같이 스크립트를 실행하면 트로이를 감지했다는 백신의 메시지를 볼 수 있다. 공격자는 파일 업로드가 되는 경로를 통하여 123.exe를 업로드 했을 것으로 추정된다. 확장명이 .exe이므로 대부분의 업로드 페이지에서 업로드가 허용됐을 것이다. 스크립트의 실행은 SQL injection 기법을 통해서 수행했을 것으로 추정된다. 아마 "Exec master..xp-cmdshell

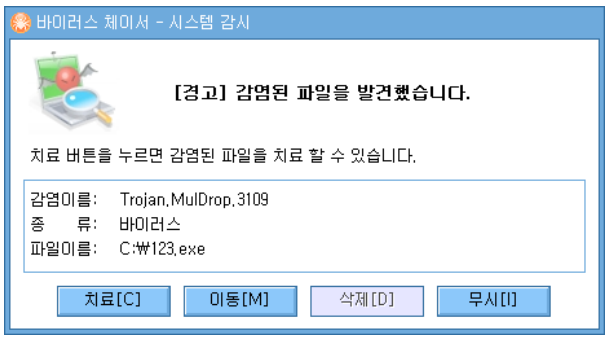
cscript 123.exe" 와 같이 스크립트를 실행시킨 후 "Exec master..xp-cmdshell c:₩123.exe" 명령을 내렸을 것으로 추측된다. 해당 서버에 직접 모의 해킹을 수행해보지 않아서 위와 같은 과정을 증명해 보진 못했다. 또한 로그파일도 볼 수 없었기에 증명할 순 없지만 위와 같은 시나리오가 추측된다.

스크립트 파일 123.exe의 스크립트 코드를 보면

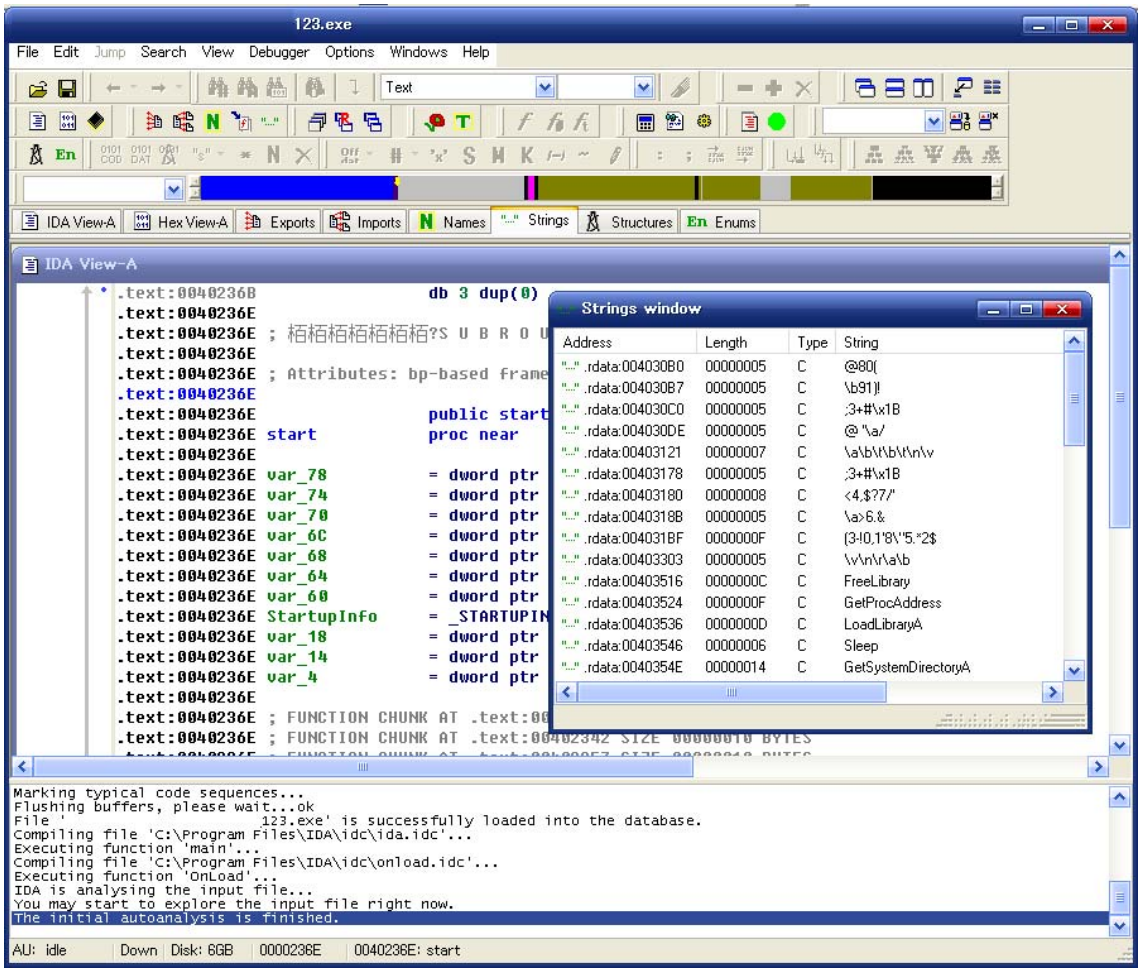
```
...
RS("m")=ss&ChrB(0)
RS.Update
ss=RS("m").GetChunk(L)
Set s=CreateObject("ADODB.Stream")
with s
...
```

가 있는데 "ss"로 정의된 변수를 & (bit AND)를 수행한 후 stream으로 c:₩123.exe를 생성하도록 하고 있다.

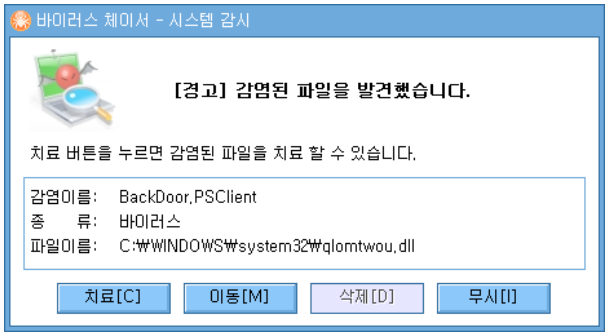
스크립트가 실행된 후 123.exe가 생성되는 순간 아래와 같은 악성코드 발견 메시지가 뜬다.



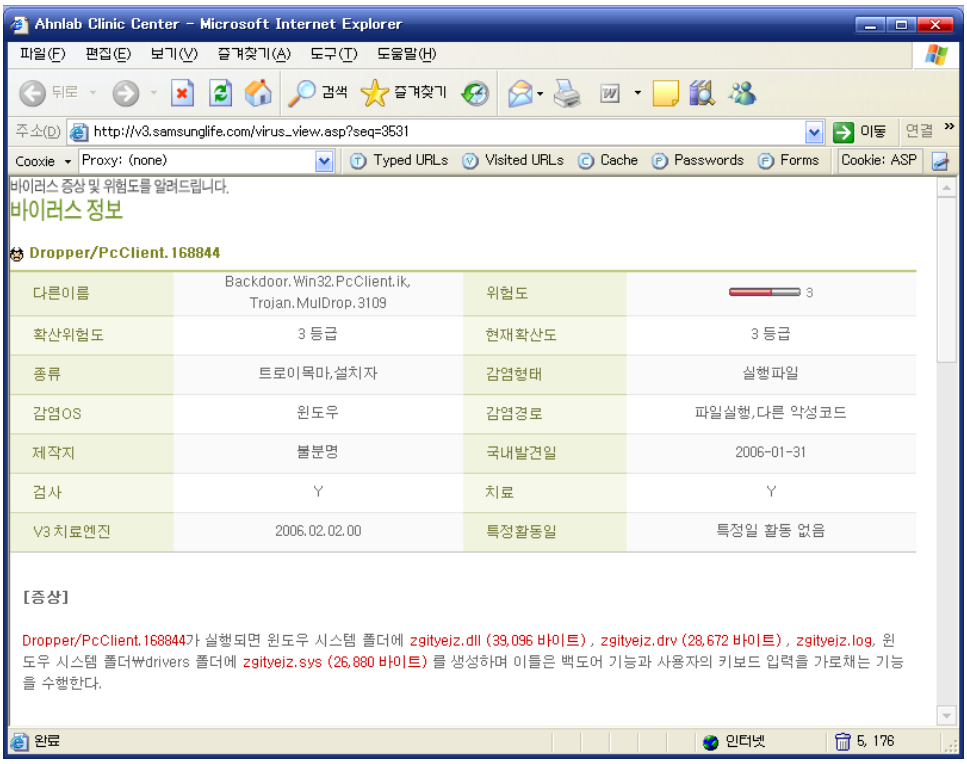
123.exe를 IDA로 문자열 데이터를 보면 아래와 같다.



123.exe를 직접 실행하기에 앞서 sysinternal.com 사의 Process Explorer, File Mon, TCP Mon을 모두 구동시킨 상태에서 실행하였다.

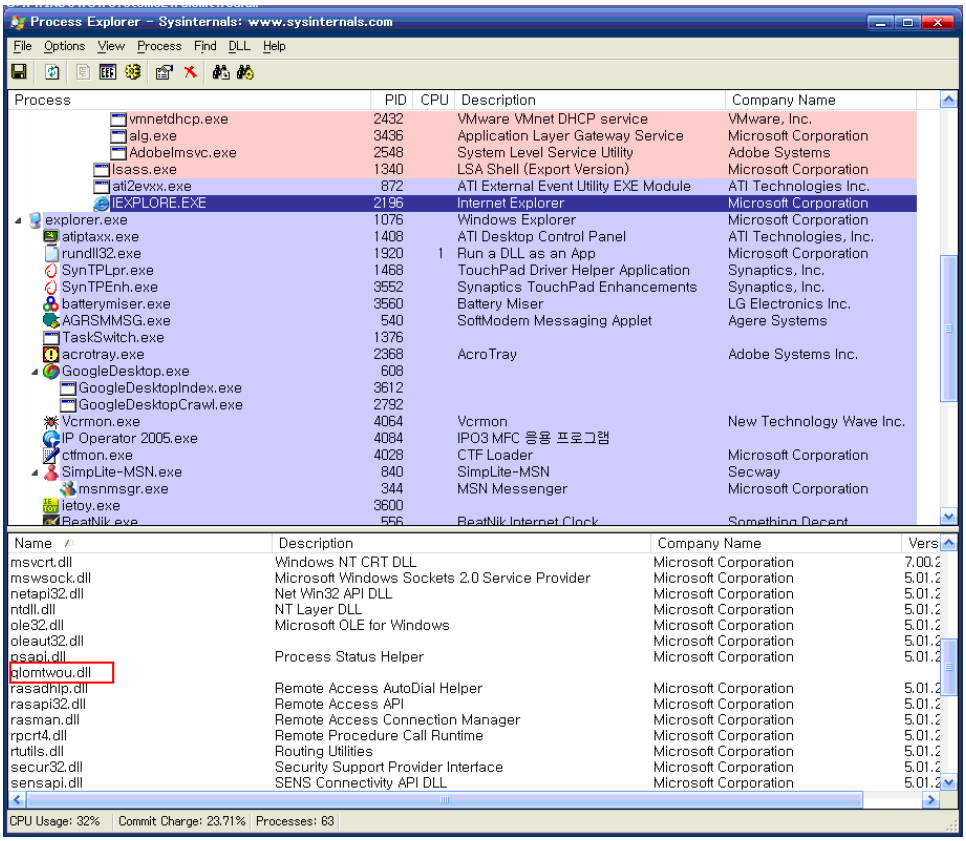


C:₩123.exe를 실행하는 순간 위와 같은 메시지가 떴다. 이번에는 백도어로 나타났으며 C:₩windows₩system32₩qlomtwou.dll 이란 파일을 가리키고 있다. 위에서 발견된 두 개의 감염이름을 바탕으로 웹 검색을 해 보면 악성코드 정보를 볼 수 있다.

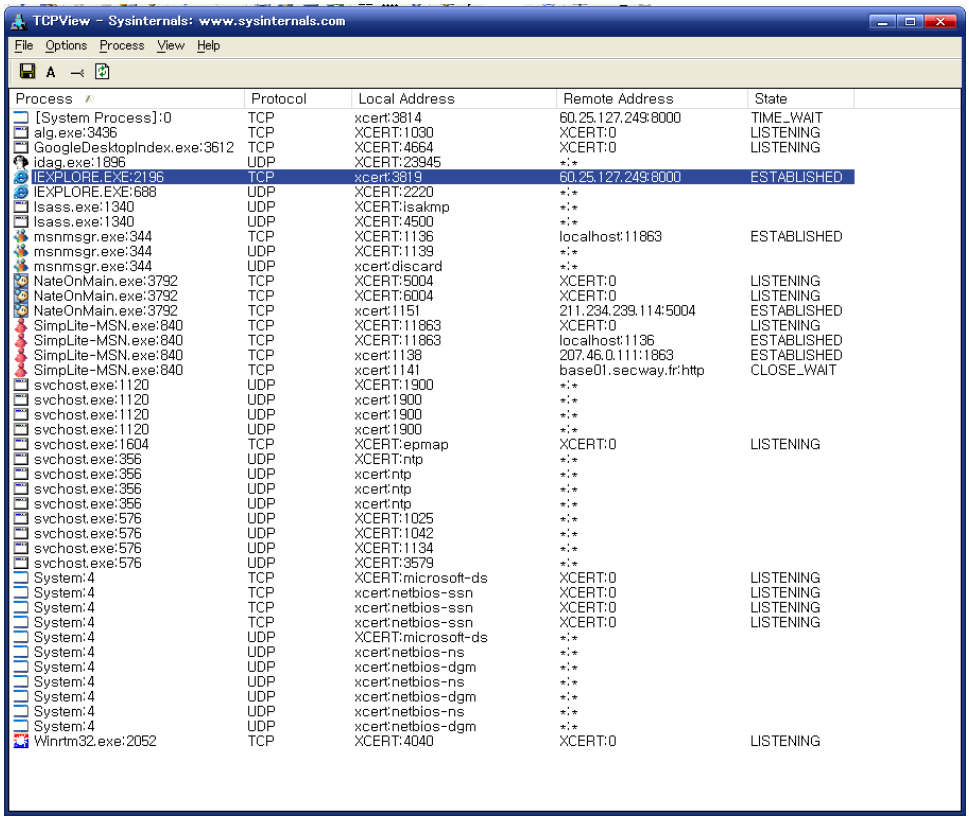


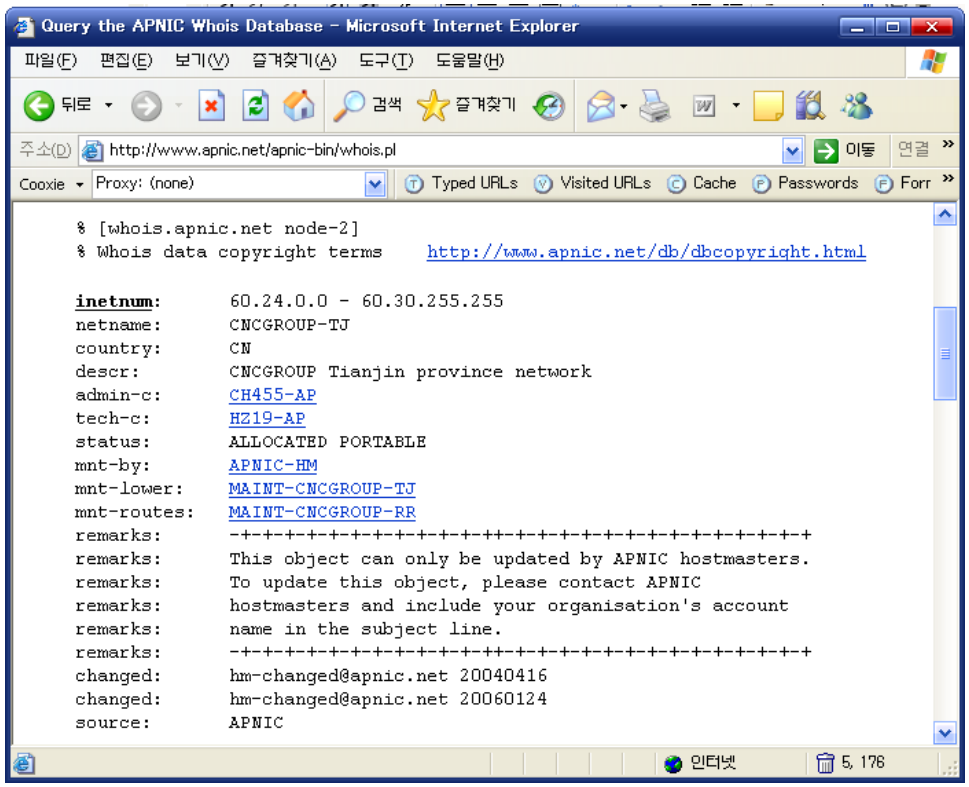
국내에서는 2006년 2월 2일에 처음 보고된 것으로 알려져 있다.

Process Explorer를 통하여 123.exe를 실행한 후의 변화를 살펴보면 악성 코드로 검사된 qlomtwou.dll 파일을 Internet Explorer가 링크하여 실행하고 있음을 확인할 수 있다.



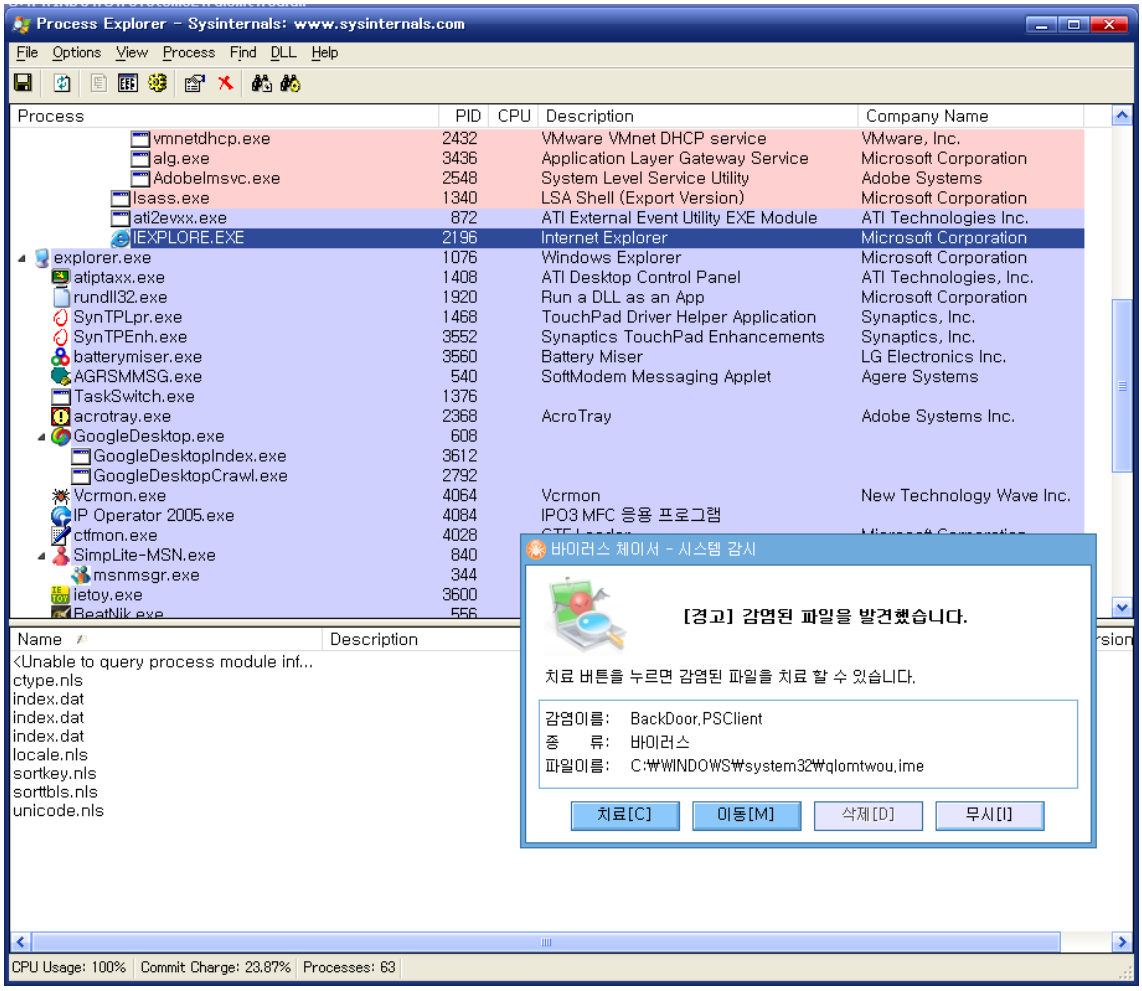
그리고 TCP Monitor로 확인한 결과 connection은 지정된 몇 개의 IP 주소 중 하나가 선택되고 그 주소의 8000번 포트로 접속을 시도한다. 몇 번의 테스트 결과 단 한 번만 연결이 성공하였다. 이 백도어는 단독으로 TCP 연결을 시도하는 것이 아니라 Internet Explorer에 기생하여 connection을 생성하므로 Windows XP SP2의 방화벽에도 감지되지 않는다. 또한 의심스러운 프로세스가 아니기 때문에 사용자는 이를 눈치채지 못할 것이다. 현재까지 분석된 IP주소는 211.196.142.220, 221.197.19.198, 60.25.127.249이고 211.196.142.220은 한국의 IP이고 나머지 IP 주소는 조회한 결과 중국에 위치한 주소였다. 여기서 IP 주소는 배포자가 필요한 주소를 임의로 변경한 것으로 추정된다.





이 백도어는 여러 개의 IP 주소를 DLL 파일 자체에 가지고 있으며 이것은 인코딩 된 값으로 저장되어 디버거로 쉽게 알아볼 수 없고 실행시 디코딩 되어 랜덤하게 선택하여 접속하

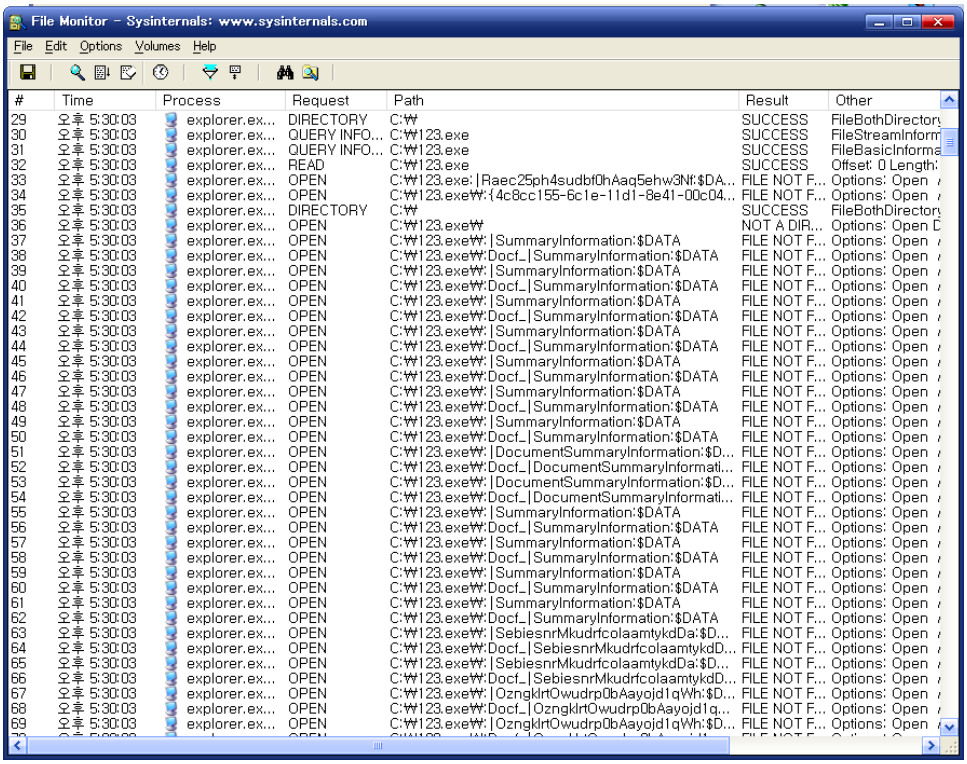
는 것으로 파악된다.

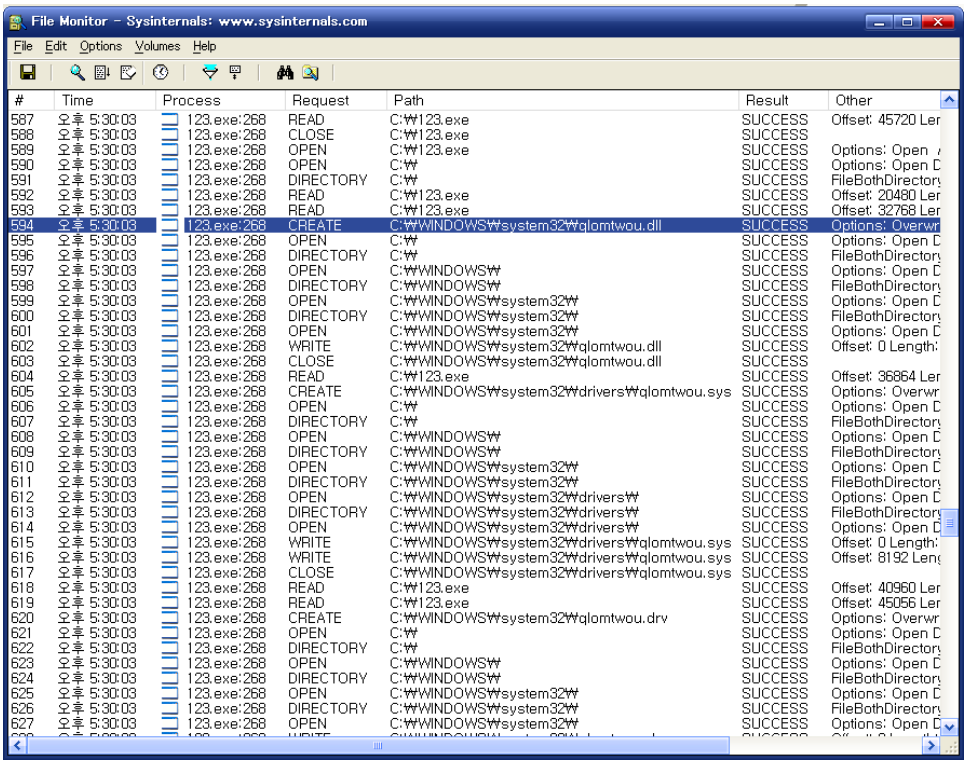


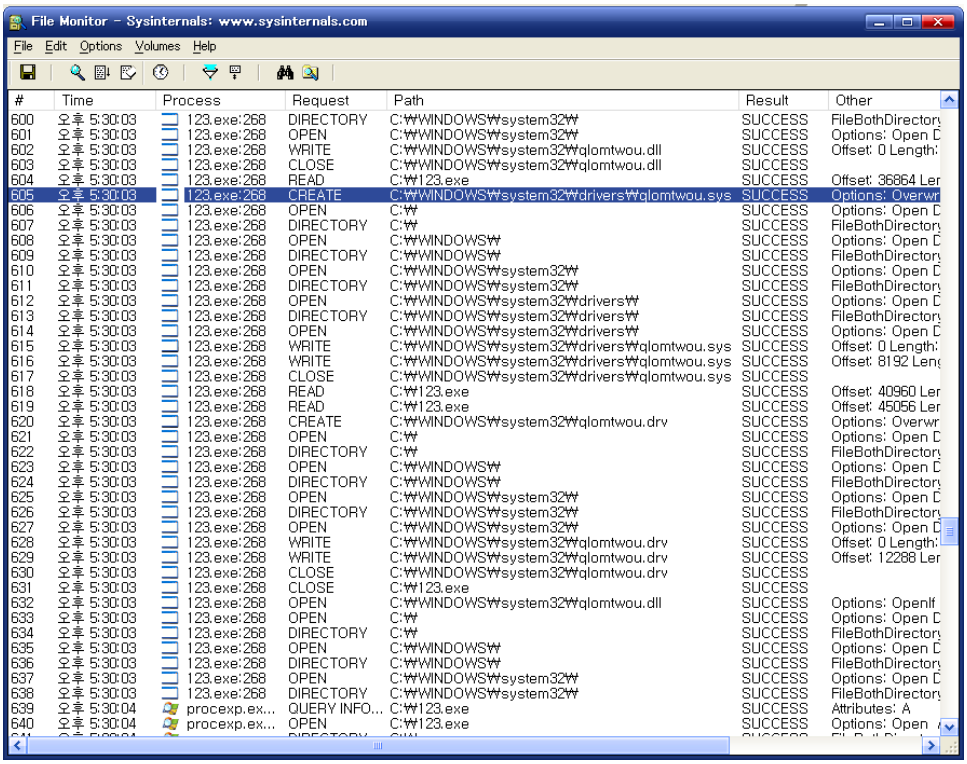
Internet Explorer 이 실행되는 동안 계속하여 여러 파일이 생성되는데 그 중 qlomtwou.ime 파일 역시 바이러스로 감지가 되었다.

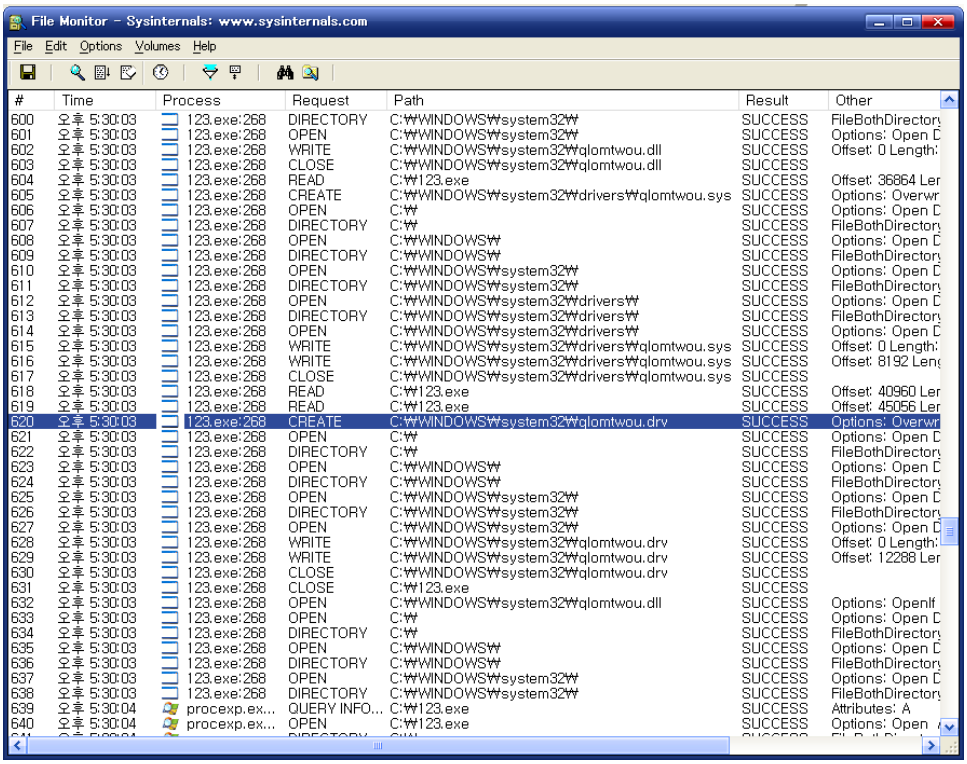
File Monitor을 통하여 감지된 File IO는 초기에 여러 파일들을 open하기 위해 시도를 하고 Windows₩system32 폴더에 qlomtwou.dll과 qlomtwou.drv를 생성한다.

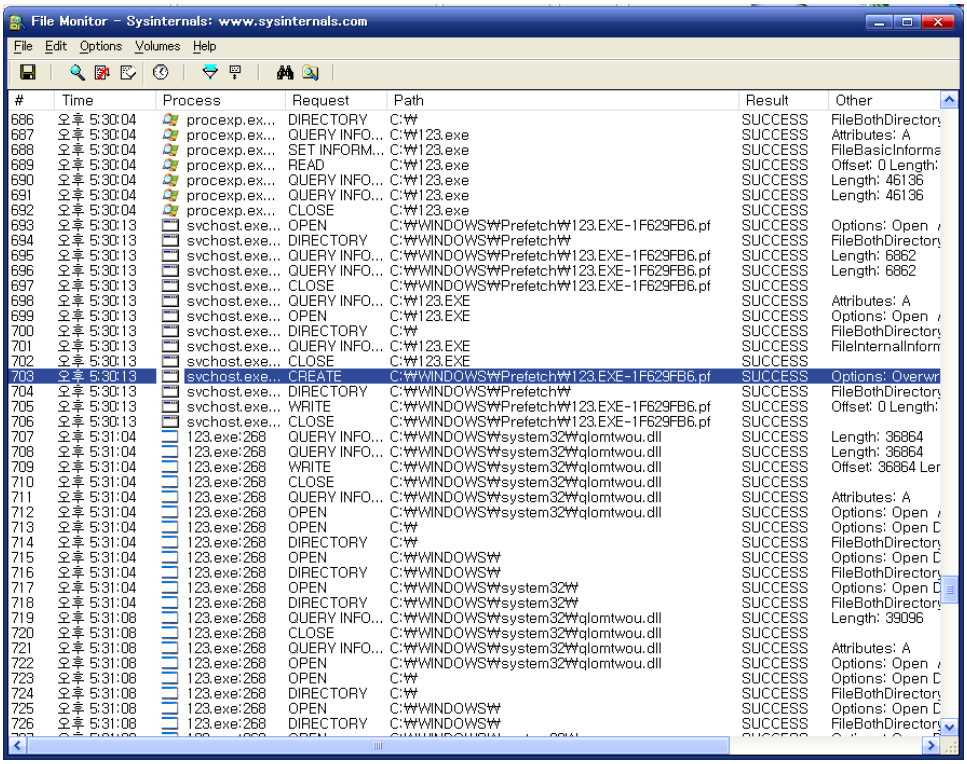
아래 그림들은 File Monitor를 통해 감지된 파일 생성 event 들을 캡쳐 한 것이다.


File Monitor - Sysinternals: www.sysinternals.com
File Edit Options Volumes Help
Time Process Request Path Result Other
29 오후 5:30:03 explorer.ex... DIRECTORY C:₩ SUCCESS FileBothDirectory
30 오후 5:30:03 explorer.ex... QUERY INFO... C:₩123.exe SUCCESS FileStreamInform
31 오후 5:30:03 explorer.ex... QUERY INFO... C:₩123.exe SUCCESS FileBasicInforma
32 오후 5:30:03 explorer.ex... READ C:₩123.exe SUCCESS Offset: 0 Length:
33 오후 5:30:03 explorer.ex... OPEN C:₩123.exe:|Raec25ph4sudbf0hAaq5ehw3Nf:$DA... FILE NOT F... Options: Open
34 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:{4c8cc155-6c1e-11d1-8e41-00c04... FILE NOT F... Options: Open
35 오후 5:30:03 explorer.ex... DIRECTORY C:₩ SUCCESS FileBothDirectory
36 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩ NOT A DIR... Options: Open D
37 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
38 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
39 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
40 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
41 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
42 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
43 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
44 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
45 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
46 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
47 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
48 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
49 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
50 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
51 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|DocumentSummaryInformation:$D... FILE NOT F... Options: Open
52 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|DocumentSummaryInformati... FILE NOT F... Options: Open
53 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|DocumentSummaryInformation:$D... FILE NOT F... Options: Open
54 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|DocumentSummaryInformati... FILE NOT F... Options: Open
55 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
56 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
57 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
58 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
59 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
60 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
61 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SummaryInformation:$DATA FILE NOT F... Options: Open
62 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SummaryInformation:$DATA FILE NOT F... Options: Open
63 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SebiesnrMkudrfcolaamtykdDa:$D... FILE NOT F... Options: Open
64 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SebiesnrMkudrfcolaamtykdD... FILE NOT F... Options: Open
65 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|SebiesnrMkudrfcolaamtykdDa:$D... FILE NOT F... Options: Open
66 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|SebiesnrMkudrfcolaamtykdD... FILE NOT F... Options: Open
67 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|OzngklrtOwudrp0bAayojd1qWh:$D... FILE NOT F... Options: Open
68 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:Docf_|OzngklrtOwudrp0bAayojd1q... FILE NOT F... Options: Open
69 오후 5:30:03 explorer.ex... OPEN C:₩123.exe₩:|OzngklrtOwudrp0bAayojd1qWh:$D... FILE NOT F... Options: Open

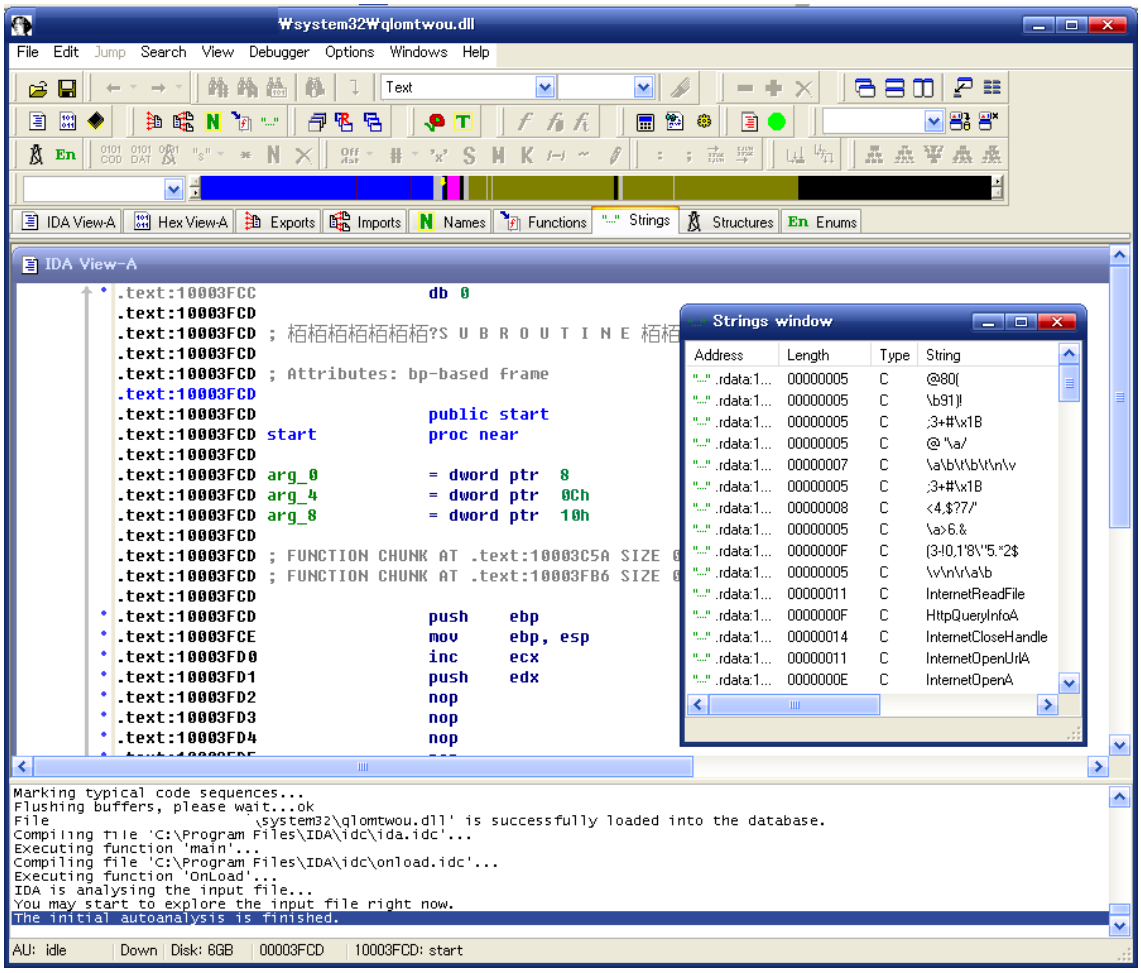

File Monitor - Sysinternals: www.sysinternals.com
File Edit Options Volumes Help
Time Process Request Path Result Other
587 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 45720 Ler
588 오후 5:30:03 123.exe:268 CLOSE C:₩123.exe SUCCESS
589 오후 5:30:03 123.exe:268 OPEN C:₩123.exe SUCCESS Options: Open
590 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
591 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
592 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 20480 Ler
593 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 32768 Ler
594 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS Options: Overwr
595 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
596 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
597 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
598 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
599 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
600 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
601 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
602 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS Offset: 0 Length:
603 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS
604 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 36864 Ler
605 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Options: Overwr
606 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
607 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
608 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
609 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
610 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
611 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
612 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩drivers₩ SUCCESS Options: Open D
613 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩drivers₩ SUCCESS FileBothDirectory
614 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩drivers₩ SUCCESS Options: Open D
615 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Offset: 0 Length:
616 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Offset: 8192 Len
617 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS
618 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 40960 Ler
619 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 45056 Ler
620 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Options: Overwr
621 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
622 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
623 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
624 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
625 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
626 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
627 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D


File Monitor - Sysinternals: www.sysinternals.com
File Edit Options Volumes Help
Time Process Request Path Result Other
600 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
601 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
602 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS Offset: 0 Length:
603 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS
604 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 36864 Ler
605 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Options: Overwr
606 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
607 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
608 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
609 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
610 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
611 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
612 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩drivers₩ SUCCESS Options: Open D
613 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩drivers₩ SUCCESS FileBothDirectory
614 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩drivers₩ SUCCESS Options: Open D
615 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Offset: 0 Length:
616 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Offset: 8192 Leng
617 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS
618 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 40960 Ler
619 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 45056 Ler
620 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Options: Overwr
621 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
622 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
623 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
624 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
625 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
626 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
627 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
628 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Offset: 0 Length:
629 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Offset: 12288 Ler
630 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS
631 오후 5:30:03 123.exe:268 CLOSE C:₩123.exe SUCCESS
632 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS Options: OpenIf
633 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
634 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
635 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
636 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
637 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
638 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
639 오후 5:30:04 procexp.ex... QUERY INFO... C:₩123.exe SUCCESS Attributes: A
640 오후 5:30:04 procexp.ex... OPEN C:₩123.exe SUCCESS Options: Open


File Monitor - Sysinternals: www.sysinternals.com
File Edit Options Volumes Help
Time Process Request Path Result Other
600 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
601 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
602 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS Offset: 0 Length:
603 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS
604 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 36864 Ler
605 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Options: Overwr
606 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
607 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
608 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
609 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
610 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
611 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
612 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩drivers₩ SUCCESS Options: Open D
613 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩drivers₩ SUCCESS FileBothDirectory
614 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩drivers₩ SUCCESS Options: Open D
615 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Offset: 0 Length:
616 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS Offset: 8192 Leng
617 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩drivers₩qlomtwou.sys SUCCESS
618 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 40960 Ler
619 오후 5:30:03 123.exe:268 READ C:₩123.exe SUCCESS Offset: 45056 Ler
620 오후 5:30:03 123.exe:268 CREATE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Options: Overwr
621 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
622 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
623 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
624 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
625 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
626 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
627 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
628 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Offset: 0 Length:
629 오후 5:30:03 123.exe:268 WRITE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS Offset: 12288 Ler
630 오후 5:30:03 123.exe:268 CLOSE C:₩WINDOWS₩system32₩qlomtwou.drv SUCCESS
631 오후 5:30:03 123.exe:268 CLOSE C:₩123.exe SUCCESS
632 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩qlomtwou.dll SUCCESS Options: OpenIf
633 오후 5:30:03 123.exe:268 OPEN C:₩ SUCCESS Options: Open D
634 오후 5:30:03 123.exe:268 DIRECTORY C:₩ SUCCESS FileBothDirectory
635 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩ SUCCESS Options: Open D
636 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩ SUCCESS FileBothDirectory
637 오후 5:30:03 123.exe:268 OPEN C:₩WINDOWS₩system32₩ SUCCESS Options: Open D
638 오후 5:30:03 123.exe:268 DIRECTORY C:₩WINDOWS₩system32₩ SUCCESS FileBothDirectory
639 오후 5:30:04 procexp.ex... QUERY INFO... C:₩123.exe SUCCESS Attributes: A
640 오후 5:30:04 procexp.ex... OPEN C:₩123.exe SUCCESS Options: Open



백도어 본체인 qlomtwou.dll 을 IDA를 이용하여 살펴보면



와 같은 문자열 데이터를 볼 수 있다. ‘Strings window’ 창의 맨 위에서부터 몇 줄이 인코딩된 IP 주소들이다. 또한 실행된 Internet Explorer에 의해 C:₩123.exe 바이너리 파일은 삭제된다. 바이러스 리포트나 시험 결과에 따르면 전파기능은 가지고 있지 않는 것으로 파악된다.

5. 결론

이번에 발견된 악성파일은 텍스트로 이루어진 스크립트 파일의 형태로 존재하여 악성 코드 분석에 지식이 부족한 서버 관리자가 발견하더라도 쉽게 알아채지 못하도록 자신을 위장하고 있는 것이 특징이다. 또한 실행파일로 존재하지 않고 dll 형태로 존재한다. 이 백도어는 단독으로 실행되지 않으며 Internet Explorer에 기생하여 실행되므로 PC 방화벽에도 감지되지 않는다. 뿐만 아니라 실제 Internet Explorer의 창이 뜨지 않고 백그라운드로 실행되며 프로세스명만 보고는 의심을 받지 않도록 위장되고 있는 것이 특징이다.