#다량의 트래픽 전송

Protocol	Zone_A	IP_A	Port_A	Zone_B	IP_B	Port_B	Idle	Bytes	Flags
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:25	275	-
UDP	outside	[redacted]	30305	inside(12)	[redacted]	30303	0:01:47	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:08	275	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:01:26	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:01:44	278	-
UDP	outside	[redacted]	30388	inside(12)	[redacted]	30303	0:00:20	566	-
UDP	outside	[redacted]	30150	inside(12)	[redacted]	30303	0:02:01	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:41	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:30	275	-
UDP	outside	[redacted]	30204	inside(12)	[redacted]	30303	0:01:36	1112	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:01:36	275	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:59	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:00	275	-
UDP	outside	[redacted]	30304	inside(12)	[redacted]	30303	0:01:09	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:29	278	-
UDP	outside	[redacted]	21002	inside(12)	[redacted]	30303	0:00:50	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:12	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:12	278	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:01:50	275	-
TCP	outside	[redacted]	30303	inside(12)	[redacted]	44088	0:00:00	1088772824	UxIO
TCP	outside	[redacted]	18110	inside(12)	[redacted]	41844	0:00:00	175841108	UxIO
TCP	outside	[redacted]	30303	inside(12)	[redacted]	38150	0:00:00	665716265	UxIO
TCP	outside	[redacted]	30303	inside(12)	[redacted]	55060	0:00:00	281492438	UxIO
UDP	outside	[redacted]	30305	inside(12)	[redacted]	30303	0:01:11	278	-
UDP	outside	[redacted]	28657	inside(12)	[redacted]	30303	0:01:22	277	-
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:40	550	-
TCP	outside	[redacted]	30303	inside(12)	[redacted]	49270	0:00:00	484001387	UxIO
UDP	outside	[redacted]	30303	inside(12)	[redacted]	30303	0:00:38	275	-

[redacted](Inside) -> 다수의 IP(Outside), (UxIO flag)

- 참고

Port: 30303/UDP

30303/UDP - Known port assignments *(2 records found)*		
Service	Details	Source
	Unassigned	IANA
threat	[threat] Sockets de Troie (A French Trojan Horse and virus)	Bekkoame

Port: 30303/TCP

30303/TCP - Known port assignments *(5 records found)*		
Service	Details	Source
	Unassigned	IANA
threat	[threat] Sockets de Troie (A French Trojan Horse and virus)	Bekkoame
socketsdestroie	[trojan] Sockets des Troie	SANS
socketsdetroie	[trojan] Sockets de Troie	SANS
trojan	[trojan] Sockets des Troie. Remote Access / ICQ trojan / Virus. Works on Windows 95 and 98, together with ICQ. Features as telnet and finger. Aliases: Sockets23, Lame, BACKDOOR.KAMIKAZE, IRC_TROJAN, TROJ_BACKDOOR, W32/Cheval.gen , Backdoor.Sockets23, Control Du Sockets, W32.HLLP.DeTroie, DeTroie.drp	Simovits

192.168.12.250(Inside)에서 다수의 IP(Outside)로(UxIO flag), 임의의 포트(30303/UDP,TCP)를 통해 트래픽을 전송했습니다.

#다량의 트래픽 전송 2

Protocol	Zone_A	IP_A	Port_A	Zone_B	IP_B	Port_B	Idle	Bytes	Flags
TCP	outside	13.125.103.48	80	inside(21)	192.168.21.151	52065	0:00:33	3108000	UxIO
TCP	outside	13.125.103.48	80	inside(21)	192.168.21.151	52532	0:00:03	1169770	UxIO

[redacted](Inside) -> [redacted](Outside), (UxIO flag)

- 참고

80	tcp	http	Hyper Text Transfer Protocol (HTTP) - port used for web traffic. See also TCP ports 81, 8080, 8081.	*SG*

[redacted](Inside)에서 13.125.103.48(Outside)로(UxIO flag), HTTP 통신(80/TCP)을 통해 트래픽을 전송하였습니다.

#Xsan 파일시스템(Apple 매킨토시 장치 간 공유) 접속

Protocol	Zone_A	IP_A	Port_A	Zone_B	IP_B	Port_B	Idle	Bytes	Flags
TCP	outside	[redacted]	548	inside(21)	[redacted]	62178	0:00:01	340145	UxIO
TCP	outside	[redacted]	548	inside(21)	[redacted]	55556	0:00:00	2699155978	UxIO
TCP	outside	[redacted]	55427	inside(21)	[redacted]	49356	0:01:29	518369	UxIO
UDP	outside	[redacted]	50806	inside(21)	[redacted]	60513	0:01:51	1867	-

[redacted](Inside) -> [redacted]:548(Outside), (UxIO flag)
[redacted](Inside) -> [redacted]:548(Outside), (UxIO flag)
[redacted](Inside) -> [redacted]:55427(Outside), (UxIO flag))
[redacted](Inside) -> [redacted]:50806(Outside)

- 참고

55427/TCP - Known port assignments *(2 records found)*		
Service	Details	Source
	Dynamic and/or Private Ports	IANA
	Xsan. Xsan Filesystem Access	Apple

[redacted](Inside)에서 [redacted]:55427(Outside)로, Xsan 파일시스템을 이용하여 원격 전송이 가능한 포트(55427/TCP)로 트래픽을 전송하였습니다.

Port(s)	Protocol	Service	Details
548	tcp	afpovertcp	AppleShare, Personal File Sharing, Apple File Service ExtremeZ-IP.exe in ExtremeZ-IP File and Print Server 5.1.2x15 and earlier allows remote attackers to cause a denial of service (daemon crash) via an invalid UAM field in a request to the Apple Filing Protocol (AFP) service on TCP port 548. References: [CVE-2008-0759], [BID-27718]

[redacted](Inside)에서 [redacted]:548(Outside)로, AppleShare 서비스의 daemon 포트(548/TCP)를 통해 다량의 트래픽(약 2574MB)을 전송하였습니다.

Port	Protocol	Service Name	Description	Source
50806	TCP		Xsan, Xsan Filesystem Access	Apple.com
50806	UDP		Back to My Mac	Apple.com

[redacted]:50806(Outside)에서 [redacted](Inside)로, Xsan 파일시스템 응답 포트(50806/UDP)를 통해 트래픽(Back to My Mac)을 전송하였습니다.

#SMB 통신

Protoco	Zone_A	IP_A	Port_A	Zone_B	IP_B	Port_B	Bytes	Flags
TCP	outside	[redacted]	443	inside(21)	[redacted]	63259	11448	UFRxIO
TCP	outside		443	inside(21)		63339	5446	UFRxIO
TCP	outside		443	inside(21)		63039	9513	UFRxIO
TCP	outside		443	inside(21)		63709	5411	UxIO
TCP	outside		443	inside(21)		63341	18601	UxIO
TCP	outside		443	inside(21)		63167	13374	UxIO
TCP	outside		443	inside(21)		60318	16977	UxIO
TCP	outside		443	inside(21)		59481	62003	UxIO
TCP	outside		443	inside(21)		53012	44888	UxIO
TCP	outside		443	inside(21)		63746	18384	UxIO
TCP	outside		443	inside(21)		44020	6704	UFxIO
TCP	outside		443	inside(21)		39538	7479	UxIO
TCP	outside		443	inside(21)		39536	3256	UxIO
TCP	outside		443	inside(21)		33074	29782	UxIO
TCP	outside		443	inside(21)		45416	6084	UxIO
TCP	outside		443	inside(21)		45414	18824	UxIO
TCP	outside		443	inside(21)		54623	7651	UFRxIO

[redacted](Inside) -> 다수의 IP:443(Outside), (UxIO flag)

[redacted](Inside) ->다수의 IP:443(Outside), (UxIO flag)

- 참고

445	tcp		Microsoft-DS Active Directory, Windows shares (official)	*Wikipedia*
445	udp		Microsoft-DS SMB file sharing (official)	*Wikipedia*

[redacted]와 [redacted](Inside)에서 다수의 IP(Outside)로(UxIO flag), SMB 포트(445/TCP)를 통해 트래픽을 전송하였습니다.