

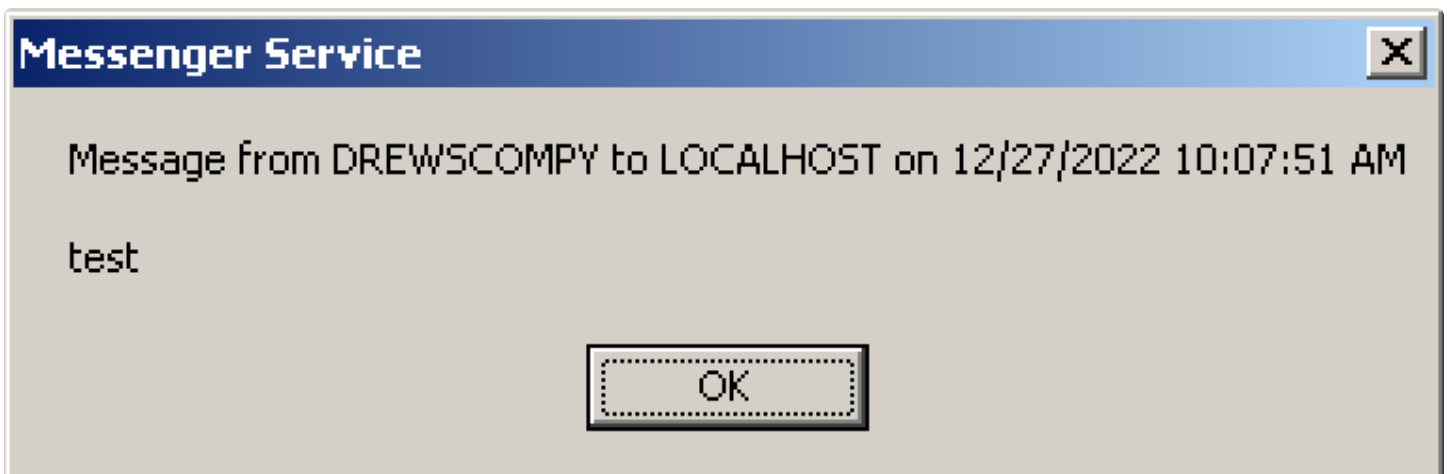
sup

December 26, 2022 · 4 min · Drew Schuster

When I was in junior high, my friends and I discovered that a Command Prompt command called `net send` was enabled on our school network. AIM and similar services were blocked, but if we wanted to send messages to each other we could open up the Command Prompt and type something like:

```
net send lab2126-24 test
```

and get an alert that looked like:



The computer names were predictable, something like lab + room number + computer number, and the computer numbers were physically written on the machines themselves. It was pretty clunky, and there was no scrollbar, but it was a fun way to goof off during class by sending each other short messages.

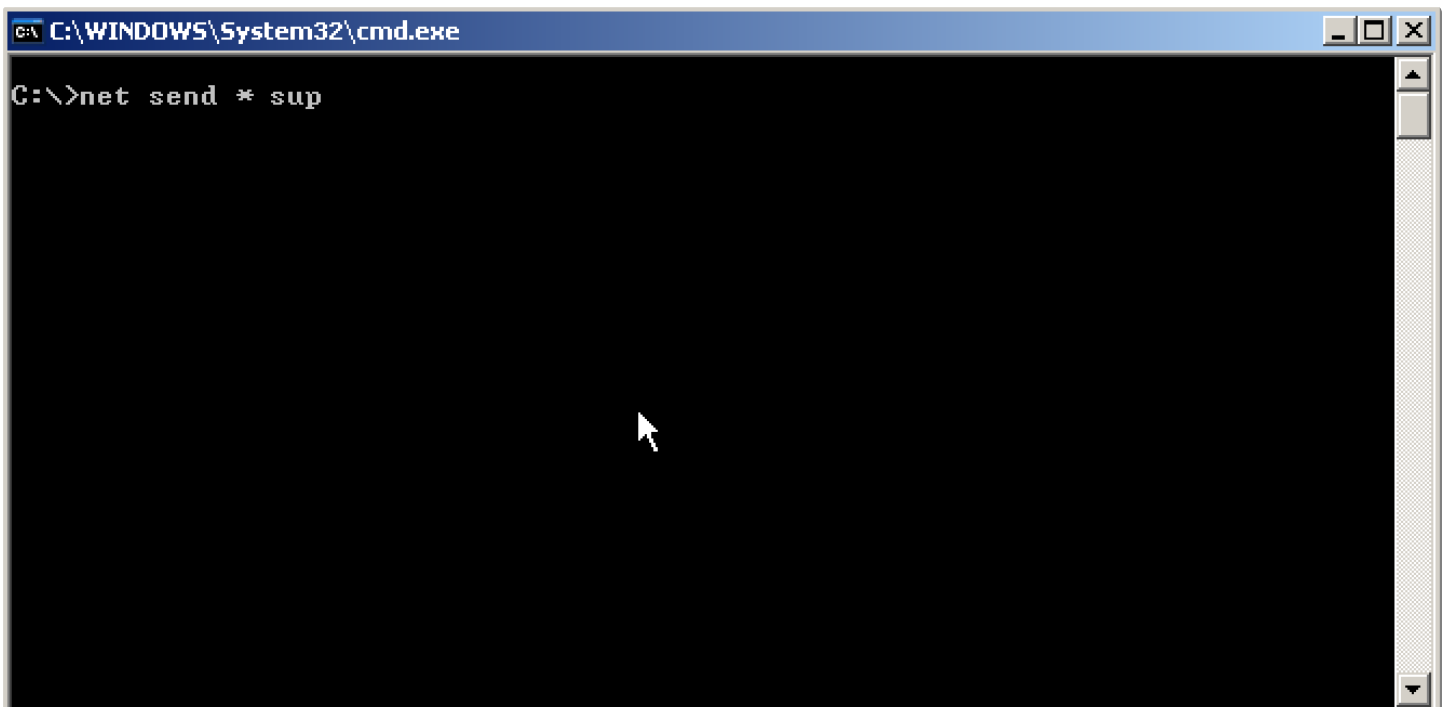
We quickly discovered a few interesting characteristics of `net send` that could be used for some silliness. For one, the alert dialog that opened up stole keyboard focus and was generally disruptive. You could spam as many `net send` commands as you wanted and the alerts would just pile up on a user's screen, with no clear way to dismiss them all. We took advantage of this by mashing up and enter as well as writing batch scripts to render our friends' computers useless. Eventually a tense truce was called, when we found out that receiving a `net send` message while playing the hidden copy of Unreal Tournament

GOTY we had installed on the school network would temporarily take the player out of the game for just long enough to be killed in a critical moment.

The most creative exploit we came up with for `net send` was on students (and teachers) who weren't yet aware of the feature. We had the ability to open an official windows alert on anyone's machine, and at a glance it wasn't obvious these messages were coming from another computer on the network. We started sending messages like "Critical Error: Please Restart Your Computer Immediately" and would watch with glee as our victim sighed deeply before restarting their computer.

The `net send` joyriding was shortlived, however. Curious about any other avenues of abuse, I looked up the documentation for `net send` at home one evening and saw that it had wildcard support! Reading the docs, it appeared that if you did `net send * MESSAGE`, the MESSAGE would be sent to every computer on the entire network. As I did not have a home network to test this on at the time, I anxiously waited until the next day at school to tell my friends.

The next day at lunch, I went to the computer lab and pulled up the documentation online for my friend Eric, and began explaining what I thought it did. As I was explaining that of course we shouldn't try such a thing because we would get in huge trouble if it worked, he ignored me and quickly typed into his machine and submitted the command that would forever live in infamy among our friends:

A screenshot of a Windows command prompt window. The title bar at the top reads "C:\WINDOWS\System32\cmd.exe". The main area of the window is black with white text. The prompt "C:\>" is followed by the command "net send * sup". A mouse cursor is visible in the center of the window.

```
C:\WINDOWS\System32\cmd.exe
C:\>net send * sup
```

After a very brief moment, Eric's computer received the sup message. I glanced at mine and saw the very same sup message. A terrifying slow pan of our heads across the entire lab confirmed our fears: sup on every screen. **We'd gone wall to wall sup!**

If you look back at the screenshot of the alert above, there's another detail you might have missed: the alert text contains the name of the computer that sent the message. We were sitting at computer XX in room YYYY while everyone else looked at a message from lab-YYYY-XX. We were seated directly in front of the smoking gun. Like any reasonable 8th graders, we responded by immediately unplugging the computer and sprinting out of the room and down the stairs.

When I got home from school, my younger sister who went to another school in the same district told me and my parents that every machine in her school had received a strange message that day that simply said "sup". I held the best poker face my 14 year old self could, which I'm sure was not very convincing.

In retrospect, it's fortunate that the `net send` alert didn't include the username, only the originating machine. I'm not sure if there are potentially audit logs that could determine which user sent which message, and now that I'm a grownup I know that this was pretty harmless and we wouldn't have gotten in very much trouble anyway.

By the time we got to school the next day, the IT person had disabled `net send` across the network. We'd flown too close to the sun, and I forever learned my lesson: **never read the docs.**

This is my first post on this website, and when trying to think of what to say first this story came back to me, because Eric said everything that needed to be said on that fateful day:

↓

↓



sup