Trouble connecting to Web sites and services because of certificate errors? Check if you're being held captive

devblogs.microsoft.com/oldnewthing/20221206-00

December 6, 2022

Raymond Chen

So you're minding your own business, and you find that Web sites and services are all failing due to certificate errors:

outlook.office365.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

	The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
✔	The security certificate date is valid.
	The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

And then if you're the sort of nerd who actually looks at the certificate, you get something like this:

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to:	US
Issued by:	US
Valid from	1/13/2011 **to** 1/8/2031

Who is "US"? Is the United States government trying to hack my connection? (And if so, why would they admit to it right in their certificate identification?)[1]

Or is "US" the guy to whom all my base are belong?[2]

While it's true that you are undergoing a man-in-the-middle attack, there's a good chance that this attack is not malicious. If you are using a public WiFi connection, say in a coffee shop or hotel, then check whether you are trapped in the captive portal.

Open a Web browser and go to a plain `http` Web site (not `https`). You'll probably see a message from the provider of the public WiFi connection asking you to agree to the terms of service or enter subscriber information.

Once you get past that, go back to the Web site or service you were originally interested in, and it should work better now.

Bonus chatter: So what's up with the "US"?

My guess is that whoever generated the certificate for the captive portal went through some "Make me a certificate" wizard and left all the fields blank. The wizard defaulted to "Country = US", and since that's the only thing that was filled in, that's the only information in the certificate.

Related reading: How does Windows decide whether your computer has limited or full Internet access?

Some follow-up notes on how Windows decides whether your computer has Internet access.

The idea behind probing the Network Connectivity Status Indicator (NCSI) endpoint is that the system wants to know whether access to "random" Web sites will succeed, and it checks this by accessing the NCSI endpoint, which is a "random" Web site. If the access to the NCSI endpoint fails, then access to other "random" Web sites will probably also fail.[3]

Yes, this can be hacked by setting up a weird WiFi network. But who cares? All that'll happen is that the user on your network gets the wrong connectivity icon (either being told that they have full connectivity when they don't, or vice versa), and they'll try to connect to some Web site, and they'll get an error, and now you have a support problem when they complain that your WiFi is broken.

Yes, this can be fooled by uncommon network configurations. But that means that connections to random Web sites are probably also going to fail, seeing as there's nothing particularly special about the NCSI endpoint. A user who opens a Web browser is probably not going to be able to browse the Internet.

An important detail is that the NCSI endpoint uses `http`, not `https`. If the endpoint had been `https`, then the captive portal's interruption would break the secure connection (which is what we experienced above), whereas on `http`, the captive portal can inject a redirect to their sign-in page.

You can configure the NCSI probes via Group Policy. You can read more on the page I linked to in the original post.

This technique for detecting basic Internet access is common across all major operating systems. Windows isn't doing anything particular sneaky here.

[1] That's one of the things I don't get about the conspiracy theorists who look for clues like this. If you assume that there's some deep, highly-organized, hyper-competent conspiracy afoot, why also assume that this highly-organized conspiracy is not just inept at keeping secrets, but is openly bragging out in public? The first rule of Fight Club is "you do not talk about Fight Club." The second rule of Fight Club is "YOU DO NOT TALK ABOUT FIGHT CLUB."

[2] Yes, I use ridiculously old memes. I'm slow to pick up on these things.

[3] In Windows 10, the name of the endpoint changed from `msftncsi` to `msftconnecttest`, presumably to make the purpose of the access more obvious in security and audit logs. Nobody will understand that NCSI stands for Network Connectivity Status Indicator. (They'll probably confuse it with the Naval Crime Investigative Service.)

Raymond Chen

Follow