

Forum:[Hack Forums](#)

Thread: [An notice to all users using skype](#)

d000000h - May 15, 2013, 5:01 am

I will quote here a recent news post about microsoft reading all your messages.

Quote:Anyone who uses Skype has consented to the company reading everything they write. The H's associates in Germany at heise Security have now discovered that the Microsoft subsidiary does in fact make use of this privilege in practice.

Shortly after sending HTTPS URLs over the instant messaging service, those URLs receive an unannounced visit from Microsoft HQ in Redmond.

A reader informed heise Security that he had observed some unusual network traffic following a Skype instant messaging conversation. The server indicated a potential replay attack.

It turned out that an IP address which traced back to Microsoft had accessed the HTTPS URLs previously transmitted over Skype.

Heise Security then reproduced the events by sending two test HTTPS URLs, one containing login information and one pointing to a private cloud-based file-sharing service.

A few hours after their Skype messages, they observed the following in the server log:

65.52.100.214 - - [30/Apr/2013:19:28:32 +0200]

"HEAD /.../login.html?user=tbtest&password=geheim HTTP/1.1"

The access is coming from systems which clearly belong to Microsoft.

Source: Utrace They too had received visits to each of the HTTPS URLs transmitted over Skype from an IP address registered to Microsoft in Redmond.

URLs pointing to encrypted web pages frequently contain unique session data or other confidential information.

HTTP URLs, by contrast, were not accessed. In visiting these pages, Microsoft made use of both the login information and the specially created URL for a private cloud-based file-sharing service.

In response to an enquiry from heise Security, Skype referred them to a passage from its data protection policy:

"Skype may use automated scanning within Instant Messages and SMS to (a) identify suspected spam and/or (b) identify URLs that have been previously flagged as spam, fraud, or phishing links."

A spokesman for the company confirmed that it scans messages to filter out spam and phishing websites. This explanation does not appear to fit the facts, however. Spam and phishing sites are not usually found on HTTPS pages.

By contrast, Skype leaves the more commonly affected HTTP URLs, containing no information on ownership, untouched. Skype also sends head requests which merely fetches administrative information relating to the server. To check a site for spam or phishing, Skype would need to examine its content.

Back in January, civil rights groups sent an open letter to Microsoft questioning the security of Skype communication since the takeover. The groups behind the letter, which included the Electronic Frontier Foundation and Reporters without Borders expressed concern that the restructuring resulting from the takeover meant that Skype would have to comply with US laws on eavesdropping and would therefore have to permit government agencies and secret services to access Skype communications.

In summary, The H and heise Security believe that, having consented to Microsoft using all data transmitted over the service pretty much however it likes, all Skype users should assume that this will actually happen and that the company is not going to reveal what exactly it gets up to with this data.

Source article:

[source](#)

if i posted this in the wrong section please move it and sorry

[edit1]

some additions by helpfull people in this topic, if you are scared about your security you should try out Jabber + Off the Record

[here is a hackforums topic](#) on how to set it up

[/edit1]

DeadLine - May 15, 2013, 5:02 am

I've seen a similar article this morning. Just another reason why people should not use Skype. Thank you for the share, people really need to know about this.

TheCl0wnhelper - May 15, 2013, 5:10 am

Good article, but what are some other alternatives?

d000000h - May 15, 2013, 5:14 am

I think mirc with ssl + FiSH encryption is still a good option, at least it was a few years back so im not completely sure right now.

It not too hard to setup and if you keep changing keys every x amount of time it would be pretty hard to decrypt the messages.

DeadLine - May 15, 2013, 5:15 am

Pidgin/Jabber in combination with

<http://www.cypherpunks.ca/otr/>

Racr - May 15, 2013, 5:18 am

(May 15, 2013 05:10 AM)TheCl0wnhelper Wrote: [\[CITE\]](#) Good article, but what are some other alternatives?

I suggest Jabber. There were some tutorials on HF but I can't seem to find them.

Edit: found one of the tutorials. <https://hackforums.net/showthread.php?tid=3479563>

d000000h - May 15, 2013, 5:20 am

(May 15, 2013 05:15 AM)DeadLine Wrote: [\[CITE\]](#) Pidgin/Jabber in combination with <http://www.cypherpunks.ca/otr/>

that seems like a good alternative indeed, according to their website the support a shitload of chat systems

Quote:Supported chat networks:

AIM
Bonjour
Gadu-Gadu
Google Talk
Groupwise
ICQ
IRC
MSN
MXit
MySpaceIM
SILC
SIMPLE
Sametime
XMPP
Yahoo!
Zephyr

nedkelly - May 17, 2013, 3:10 pm

Excellent info here, not many people would really know this!

The Commander - May 17, 2013, 3:11 pm

Thank you for the share. We should stop using skype!

barukoru - May 30, 2013, 8:20 am

?Thank you for the share.Nice post

adelti - May 30, 2013, 8:24 am

Nice post, thank you for the share. :)

outlaw_mak - May 30, 2013, 8:35 am

Cool post. But i think microsoft, firefox, google, ect are all up to the same. A simple trace log of a standalone sytem connected to the internet will have thousands of connections coming from akimah tecnology, verizone, and untraceable unspecified companys even the microsoft and verizone servers have so many ip ranges that they are impossible to block even when you disable manual downloads have no viruses or malware.

This days if your are dealing with any thing from the states or europe consider it a backdoor into your system on way or another and the O.P. has proved it. so much for freedom and civil liberty's.

wont be sending anything senstive over skype next time. think i should be looking for a alternative.

djgeneral - May 31, 2013, 12:11 am

hahaha wow. this is pretty creepy! greedy companies

+Pirate - May 31, 2013, 4:49 am

If you delete the message, is it still seen in full?

?? - May 31, 2013, 4:53 am

I never liked Skype it's the worst for IM.

Wonders - May 31, 2013, 4:55 am

Might have to call it a day for Skype myself. Jabber looks nice, will make an account soon.

ANONYMOUS - May 31, 2013, 4:57 am

Can someone sum this up for me of what it means

CBF to read it all.

Racr - May 31, 2013, 4:59 am

(May 31, 2013 04:57 AM)ANONYMOUS Wrote: [\[CITE\]](#) Can someone sum this up for me of what it means

CBF to read it all.

Basically it means: don't send private/confidential info over Skype(especially https:// links), Microsoft has access to it all.

wolfman1337 - May 31, 2013, 8:52 am

Skype, skype ... thanks for posting this mate.

Visionary - May 31, 2013, 4:41 pm

XMPP in the place to be! Jabber is good for OTR shit.

jake1218 - June 29, 2013, 7:06 pm

Very useful thread, thank you very much OP.

xxxpool - June 30, 2013, 4:01 am

i think all programs will be monitored someday

Grizz - June 30, 2013, 5:04 pm

Yeah I discovered this myself a while ago while playing around with a Geolocator and my resolver. Nice share nonetheless.

Rogerball - July 6, 2013, 12:04 pm

thank you for the information it's very helpful!

xtremegamer1882 - July 6, 2013, 11:54 pm

We as Hackers should all come together and create our own Encrypted Browsers, Vpn's, IM's and File sharing Sites that seem ordinary.

Encryption could be that every line and sentence looks like people are talking about news but are not when you are logged in...

Kristoff - July 13, 2013, 10:27 am

As a response to all this hype going on about the NSA and other companies going through your messages, I'm developing a secure messenger that doesn't require a 3rd party server. Secure enough for any sensitive information. PM me if you're interested.

Again, it does NOT require a 3rd party host or service. Super secure, asymmetric encryption, ect.

uruk2012 - July 24, 2013, 5:20 am

nice post. thank you for that information.

(ultimate message countermeasure)

tired- - *July 24, 2013, 6:04 am*

And back to MSN we go..

(/sarcasm)