

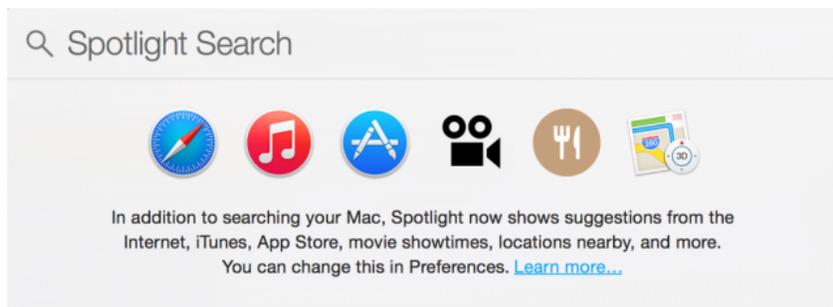
RISK ASSESSMENT / SECURITY & HACKTIVISM

Spotlight search in OS X Yosemite exposes private user details to spammers

Search feature overrides widely used setting blocking remote images.

by Dan Goodin - Jan 9, 2015 7:13am PST

69



Using the Spotlight search feature in OS X Yosemite can leak IP addresses and private details to spammers and other e-mail-based scammers, according to tests independently performed by two news outlets.

The potential privacy glitch affects people who have configured the Mac Mail App to turn off the "load remote content in messages" setting, as security experts have long advised. Spammers, stalkers, and online marketers often use remote images as a homing beacon to surreptitiously track people opening e-mail. Because the images are hosted on sites hosted by the e-mail sender, the sender can log the IP address that viewed the message, as well as the times and how often the message was viewed, and the specific e-mail addresses that received the message. Many users prefer to keep their e-mail addresses, IP addresses, and viewing habits private, a goal that's undermined by the viewing of remote images.

Like Mozilla Thunderbird, Microsoft Outlook, and many other e-mail clients, Mail allows users to block remote images for precisely this reason. But even when remote image viewing is disabled in Yosemite-based Mail app settings, the images will be opened by Spotlight, according to two recent media reports. The feature is used to search a Mac for files or e-mail containing a specified search term. When spotlight returns a preview of e-mails containing the term, it loads the images, overriding the option. Images are loaded even when the previewed message has landed in a users' junk mail folder.

The behavior was reported early Friday by German security publication Heise and later confirmed by IDG News. It's not clear if Spotlight similarly overrides image blocking in third-party apps. Apple hasn't immediately commented on the reports.

READER COMMENTS 69



Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
[@dangoodin001 on Twitter](#)

LATEST FEATURE STORY ▾



FEATURE STORY (2 PAGES)

Review: Mint 17.3 may be the best Linux desktop distro yet

If you don't want to think too hard about which OS you're using, Mint is for you.

WATCH ARS VIDEO ▾

Ars visits Nest Labs

We learn about their programmable, self-learning, sensor-driven, Wi-Fi-enabled thermostats.

STAY IN THE KNOW WITH ▾

LATEST NEWS ▾

THAT ESCALATED QUICKLY

Martin Shkreli's other pharma company is dramatically collapsing

ROUNDTRIP TICKET TO THE IRON AGE

Scientists find 1500-year-old Viking settlement beneath new airport site

MINDLESS MUNCHING

Making healthy foods the default menu dupes people into eating better

Asian-American band "The

← OLDER STORY

NEWER STORY →

YOU MAY ALSO LIKE ▾



Slants" overturns USPTO rule on "disparaging" trademarks

FOIA REINFORCEMENTS

Suspecting climate change conspiracy, Judicial Watch sues NOAA for scientists' e-mails



Progress! New CMOS chip can process both light and electricity

SITE LINKS

- [About Us](#)
- [Advertise with us](#)
- [Contact Us](#)
- [Reprints](#)

SUBSCRIPTIONS

[Subscribe to Ars](#)

MORE READING

- [RSS Feeds](#)
- [Newsletters](#)
- [Visit Ars Technica UK](#)

CONDE NAST SITES

- [Reddit](#)
- [Wired](#)
- [Vanity Fair](#)
- [Style](#)
- [Details](#)

[Visit our sister sites](#)

[Subscribe to a magazine](#)

[VIEW MOBILE SITE](#)

CONDÉ NAST

© 2015 Condé Nast. All rights reserved
Use of this Site constitutes acceptance of our [User Agreement](#) (effective 1/2/14) and [Privacy Policy](#) (effective 1/2/14), and [Ars Technica Addendum](#) (effective 5/17/2012)
[Your California Privacy Rights](#)

The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.

[Ad Choices](#)