https://arstechnica.com/security/2013/11/lg-smart-tv-snooping-extends-to-home-networks-second-blogger-says/

LG smart TV snooping extends to home networks, second blogger says

Internet-connected TVs from LG phone home with file names in shared folders.

Dan Goodin - 11/21/2013, 5:11 PM

A second blogger has published evidence that his LG-manufactured smart television is sharing sensitive user data with the Korea-based company in a post that offers support for the theory that the snooping isn't isolated behavior that affects a small number of sets.

In addition to transmitting a list of shows being watched and the names of files contained on USB drives, the Internet-connected TV also sent the names of files shared on home or office networks, the blogger reported. He made the discovery after plugging the Wireshark packet-sniffing program into his home network and noticing that an LG TV\u2014model number 42ls570, purchased in April\u2014was transmitting file names that sounded vaguely familiar even though there was no USB drive plugged in.

"It turns out it was pulling filenames from my shared folders over the network and broadcasting those instead," he wrote in a blog post published Thursday. "I moved all the media out of the folder and put a few duds in named 'GiantPorn,' turned the TV off and on and it was still broadcasting the old filenames. The TV couldn't see those files whilst browsing manually so I'd hazard a guess it\u2019s caching some of these locally."

Within about 10 minutes, voil\340. The name of the GiantPorn MPEG file was transmitted to 193.67.216.135, an IP address belonging to LG Electronics, according to Whois records.
Data packets show an LG smart TV sending the name of a video file to an IP address owned by the manufacturer.
Enlarge / Data packets show an LG smart TV sending the name of a video file to an IP address owned by the manufacturer.

Mark, a Web developer who asked Ars not to publish his last name, said he also noticed that his TV sent an authorization code to LG as soon as he turned it on and a deauthorization code each time he turned it off.

"I'm not sure how unusual this practice is, but it gives LG a pretty precise measurement of when and how long you are using the TV," he wrote.
An LG TV reporting when it has been shut down. A similar report is sent when the

TV is turned on.
Enlarge / An LG TV reporting when it has been shut down. A similar report is sent when the TV is turned on.

As was the case with the previous blogger, the HTTP POST requests containing file names that Mark observed returned a 404 error typically used to indicate that a requested file wasn't found at a specified address. That could indicate the file information the smart TVs are sending wasn't received, but that's by no means certain since it's trivial for that information to be logged even when such errors are broadcast. And even if the data isn't currently being received for whatever reason, the packet captures provide almost irrefutable proof that the data is being sent to LG servers, whether or not they're actually accepting it. With minor fuss, those servers can be tweaked to permanently log the data.

What's more, since LG TVs are sending the data unencrypted, it's trivial for anyone on the same home or office network to monitor the communications. That data is similarly available to anyone who has the ability to monitor communications sent over the larger Internet.

Representatives of LG didn't respond to a request for comment for both this story and a previous post.

On Thursday, security blogger Graham Cluley posted a statement issued by LG representatives confirming the monitoring and pledging to stop it. The statement read:

At LG, we are always aiming to improve our Smart TV experience. Recently, it has been brought to our attention that there is an issue related to viewing information allegedly being gathered without consent. Our customers\u2019 privacy is a very important part of the Smart TV experience so we began an immediate investigation into these claims. Here\u2019s what we found:

Information such as channel, TV platform, broadcast source, etc. that is collected by certain LG Smart TVs is not personal but viewing information. This information is collected as part of the Smart TV platform to deliver more relevant advertisements and to offer recommendations to viewers based on what other LG Smart TV owners are watching. We have verified that even when this function is turned off by the viewers, it continues to transmit viewing information although the data is not retained by the server. A firmware update is being prepared for immediate rollout that will correct this problem on all affected LG Smart TVs so when this feature is disabled, no data will be transmitted.

It has also been reported that the names of media files stored on external

drives such as USB flash devices are being collected by LG Smart TVs. While the file names are not stored, the transmission of such file names was part of a new feature being readied to search for data from the internet (metadata) related to the program being watched in order to deliver a better viewing experience. This feature, however, was never fully implemented and no personal data was ever collected or retained. This feature will also be removed from affected LG Smart TVs with the firmware update.

LG regrets any concerns these reports may have caused and will continue to strive to meet the expectations of all our customers and the public. We hope this update clears up any confusion.

Further Reading
How an Internet-connected Samsung TV can spill your deepest secrets
The revelations that LG TVs actively transmit viewing habits provide a good opportunity for consumers to evaluate just how many of their home devices they want to have Internet connectivity. No doubt, smart devices offer convenience by, for instance, allowing us to turn on a furnace a half-hour before we're scheduled to arrive home from work. But they can also offer a dark side, since the temptation to mine all that easily available data is apparently too strong for some companies to resist.

And even if manufacturers can be trusted to avert their eyes, there's the issue of security, as demonstrated last year when researcher Luigi Auriemma uncovered a vulnerability in many Samsung smart TVs that allowed him to remotely take control of devices that were connected to the same local network he was on. If Apple, Microsoft, and Google have trouble securing their devices, what reason is there to think the LGs and Samsungs of the world will do better?