Ungagged Google warns users about FBI accessing their accounts

06 SEP 2018 2

Google, Law & order, Malware, Security threats

Previous: MEGA secure upload s... Next: Thousands of unsecured 3D...

by Lisa Vaas

Dozens of people say they've received an email from Google informing them that the FBI has been sniffing around for information on their accounts. Now that a gag order has been lifted, the company is able to "disclose the receipt of the legal process" to any affected users, Google said.

That's not entirely surprising: the gag orders that often accompany such requests keep organizations such as Google, Microsoft, Facebook and Apple from disclosing the order for a given period of time. Any email provider worth its salt nowadays issues transparency reports, and the biggest companies have called for increased transparency in government surveillance requests.

But these nondisclosure orders can be lifted, cybercrime lawyer Marcia Hoffman told Motherboard:

> *It looks to me like the court initially ordered Google not to disclose the existence of the info demand, so Google was legally prohibited from notifying the user. Then the nondisclosure order was lifted, so Google notified the user. There's nothing unusual about that per se. It's common when law enforcement is seeking info during an ongoing investigation and doesn't want to tip off the target(s).*

Who are the targets in the FBI's inquiry – targets who can now be safely tipped off?

The emails lack specific details about whatever the FBI was investigating, though they did contain a case number that corresponded to a sealed case when Motherboard looked it up on PACER.

Some who received the letters posted screenshots in online forums. From one such:

> *Google received and responded to legal process issue by Federal Bureau of Investigation (Eastern District of Kentucky) compelling the release of information related to your Google account. A court order previously prevented*

> *Google from notifying you of the legal process. We are now permitted to disclose the receipt of the legal process to you.*

Though the letters had scanty detail, some of the recipients have a hunch regarding what it's all about.

In threads on Reddit, Twitter, and Hack Forums, conjecture is that the FBI was looking for information on people associated with LuminosityLink: an easy to use, remote access Trojan (RAT) that was selling for as little as $39.99.

> *Ever seen this?! 😏 https://t.co/1xJO1rALTh*
>
> —
>
> *☎️Luca Bongiorni☎️ (@LucaBongiorni) August 30, 2018*

...until, that is, it wasn't. Europol snuffed out LuminosityLink in February, following a UK-led dragnet in September 2017 that involved over a dozen law enforcement agencies in Europe, Australia and North America that went after hackers linked to the tool.

In July, 21-year-old Kentuckian Colton Grubbs pleaded guilty to federal charges of creating, selling and providing technical support for the RAT to his customers, some of whom used it to gain unauthorized access to thousands of computers across 78 countries worldwide.

Some of those who received the notice from the newly ungagged Google said that they consider the mystery solved: they had purchased LuminosityLink, which may well have caught the attention of the FBI.

> *@michalmonday problem solved. I bough a copy of LL time ago for research https://t.co/HTflXTLpYf*
>
> —
>
> ☎Luca Bongiorni☎ *(@LucaBongiorni) August 30, 2018*

Buying LuminosityLink doesn't necessarily brand somebody a cybercrook. It had a split personality when it came to its marketing: it was sold as a legitimate tool for Windows admins to "manage a large amount of computers concurrently". On the flip side, it was also a cheap, easy-to-use, multi-purpose pocket knife with a slew of malware tools you could flip out: a RAT that could be surreptitiously installed without a user being aware and which disabled anti-virus and anti-malware protection on targets' computers before going to work switching on webcams to spy on video feeds; accessing and viewing documents, photographs, and other files; stealing passwords; and/or installing a keylogger to automatically record victims' keystrokes.

Some bought it to do legitimate systems administration. Others say they bought it for research purposes. Their activities would only be illegal if they used the tool's more nefarious capabilities.

While it's not unusual for a gag order to be subsequently lifted, it is perhaps unusual for the FBI to try to track down every person who purchased software that may not be considered illegal, as one lawyer pointed out to Motherboard. Gabriel Ramsey, a lawyer with a specialty in cybersecurity and internet law, said that just buying a tool like LuminosityLink doesn't determine guilt:

> *If one is just buying a tool that enables this kind of capability to remotely access a computer, you might be a good guy or you might be a bad guy. I can imagine a scenario where that*