Firefox: No-exit browser scammers want you to call bogus support

November 8 2019, by Nancy Cohen

Credit: CC0 Public Domain

This week tech watchers were sending out headlines about scammers taking advantage of a Firefox bug to freeze users out of their browser. The punch-up consists of a user getting a warning message and then browser lockout. The scammers tell you to call a number posing as a bogus support line.

The attack works on both Windows and Mac versions. Upset by a flood of continuous authentication-required prompts, a user might try to leave the warning page; not possible, or may try to close it; forget about it.

The Firefox bug fools users to think their computers have been hacked. Then victim users who believe this is all happening for real are tricked to call the bogus support line. It is as if Borat is talking which should possibly give people a hint this is all a dupe.

"Please stop and do not close the PC…The registry key of your computer is locked. Why did we block your computer? The Windows registry key is illegal. The Windows desktop is using pirated software. The Window desktop sends viruses over the Internet. This Windows desktop is hacked. We block this computer for your safety."

(A reader comment in *Ars Technica*: "There is a theory that all the bad grammar and spelling mistakes in many scams are deliberate too. Because it weeds out the skeptical. Scammers don't want to waste time with savvy, smart or skeptical people.")

Well, observers agreed that victims falling for the information as genuine fell into the category of victims of tech support scams through the years.

Another reader's comment, this time on *ExtremeTech*: "...this has been common practice for scammers for over three years...This is not just a Firefox issue. It's scammers taking advantage of advertisements. They load a specific javascript code into their hosted ad that people are unlucky enough to have loaded when they visit a webpage and thus, locked browser. This happens in all browsers."

Jonathan Lamont in *MobilSyrup.com* offered advice. "The best thing to do in these circumstances is to remain calm and not react suddenly to

what's happening...Typically, these scams want to frighten users into handing over valuable information or money." Dan Goodin in *Ars Technica*: "Whatever else people may do, they should never call the phone number displayed."

Ravie Lakshmanan in TNW: Terminate the browser process via the Windows Task Manager or use the Force Quit feature in macOS. It's possibly messy, however, for "if you've turned the restore tabs option on," said Lakshmanan, "you'll be stuck in a perpetual loop, with the only option being disconnecting from the internet before opening the browser again."

Forcibly closing Firefox and restarting it may be enough, provided the browser isn't set to reopen previously closed tabs, said JC Torres in *SlashGear*.

Back in April, though, Catalin Cimpanu in *ZDNet* reported Firefox was to add protection against the login prompt spam.

"Twelve years after it was first notified of the issue, Mozilla has finally shipped a fix this week that will prevent abusive websites —usually tech support scam sites— from flooding users with non-stop 'authentication required' login popups and prevent users from leaving or closing their browsers. The fix has been shipped in Firefox v68, the current Nightly release, and will hit the browser's stable branch sometimes in early July."

Goodin had more about this: "Earlier this year, Mozilla shipped a comprehensive fix for these types of attacks some 12 years after being reported. Chrome and other browsers have also been vulnerable to this variety of attacks. Segura said he's aware of a separate Firefox browser lock bug that remains unfixed two years after it was reported. Although it was actively exploited in the past, Segura said, he hasn't seen any recent attacks targeting the flaw."

Goodin was referring to Jérôme Segura at Malwarebytes.

"Jérôme Segura, head of Threat Intelligence at Malwarebytes, this week found that tech-support scammers have found a bypass for Mozilla's fix, allowing them to use the same tactics to con victims." said Cimpanu in *ZDNet.* Segura said this time the "browlock" was using a technique that was "new to me."

What's next? Mozilla is reportedly working on a fix.

Sergiu Gatlan in BleepingComputer explained what was going on this time around. How does the bug allow crooks to lock the browser? "This is done by spamming them [targets] with a large amount of authorization confirmation prompts because there is no rate limiting to prevent it and by stealing focus from the main page."

Gatlan recalled some techniques used in past blocks and tech support scams: "In December 2018, JavaScript was used by crooks to create an inescapable loop that would claim all CPU resources thus making it impossible for users to close the tab, the web browser, and even their computer without killing Chrome's process.

"As Symantec found in November 2018, tech support scam campaigns have also been more frequently spotted using obfuscation techniques like custom obfuscation routines, Base64 encoding, or AES encryption to make them even harder to detect and block."