New security loophole allows spying on internet users visiting websites and watching videos

June 24 2024

The "SnailLoad" loophole is based on combining the latency of internet connections with the fingerprinting of online content. Credit: IAIK - TU Graz

Internet users leave many traces on websites and online services. Measures such as firewalls, VPN connections and browser privacy modes are in place to ensure a certain level of data protection. However, a newly discovered security loophole allows bypassing all of these protective measures.

Computer scientists from the Institute of Applied Information Processing and Communication Technology (IAIK) at Graz University of Technology (TU Graz) were able to track users' online activities in detail simply by monitoring fluctuations in the speed of their internet connection. No malicious code is required to exploit this vulnerability, known as "SnailLoad," and the data traffic does not need to be intercepted. All types of end devices and internet connections are affected.

The researchers have published their work in a paper titled "SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript."

Attackers track latency fluctuations in the internet connection via file transfer

Attackers only need to have had direct contact with the victim on a single occasion beforehand. On that occasion, the victim downloads a basically harmless, small file from the attacker's server without realizing it—for example, while visiting a website or watching an advertising video.

As this file does not contain any malicious code, it cannot be recognized by security software. The transfer of this file is extremely slow, providing the attacker with continuous information about the latency variation of the victim's internet connection. In further steps, this information is used to reconstruct the victim's online activity.

'SnailLoad' combines latency data with fingerprinting of online content

"When the victim accesses a website, watches an online video or speaks to someone via video, the latency of the internet connection fluctuates in

a specific pattern that depends on the particular content being used," says Stefan Gast from the IAIK. This is because all online content has a unique fingerprint: For efficient transmission, online content is divided into small data packages that are sent one after the other from the host server to the user. The pattern of the number and size of these data packages is unique for each piece of online content—like a human fingerprint.

The researchers collected the fingerprints of a limited number of YouTube videos and popular websites in advance for testing purposes. When the test subjects used these videos and websites, the researchers were able to recognize this through the corresponding latency fluctuations.

"However, the attack would also work the other way round," says Daniel Gruss from the IAIK. "Attackers first measure the pattern of latency fluctuations when a victim is online and then search for online content with the matching fingerprint."

Slow internet connections make it easier for attackers

When spying on test subjects who were watching videos, the researchers achieved a success rate of up to 98%.

"The higher the data volume of the videos and the slower the victims' internet connection, the better the success rate," says Gruss. Consequently, the success rate for spying on basic websites dropped to around 63%.

"However, if attackers feed their machine learning models with more data than we did in our test, these values will certainly increase," says Gruss.

Loophole virtually impossible to close

"Closing this security gap is difficult. The only option would be for providers to artificially slow down their customers' internet connections in a randomized pattern," says Gruss. However, this would lead to noticeable delays for time-critical applications such as video conferences, live streams or online computer games.

The team led by Gast and Gruss has set up a website describing SnailLoad in detail. They will present the scientific paper on the loophole at the conferences Black Hat U.S. 2024 and USENIX Security Symposium.

More information: Stefan Gast et al, SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript (2024)

Provided by Graz University of Technology

Citation: New security loophole allows spying on internet users visiting websites and watching videos (2024, June 24) retrieved 30 June 2024 from https://techxplore.com/news/2024-06-loophole-spying-internet-users-websites.html