

Kaspersky AV injected unique ID that allowed sites to track users, even in incognito mode



reader comments

149 with 88 posters participating

Share this story

Antivirus software is something that can help people be safer and more private on the Internet. But its protections can cut both ways. A case in point: for almost four years, AV products from Kaspersky Lab injected a unique identifier into the HTML of every website a user visited, making it possible for sites to identify people even when using incognito mode or when they switched between Chrome, Firefox, or Edge.

The identifier, as reported Thursday by c't Magazine, was part

of a blob of JavaScript Kaspersky products injected into every page a user visited. The JavaScript, presented below this paragraph, was designed to, among other things, present a green icon that corresponded to safe links returned in search results.

c't reporter Ronald Eikenberg found something unsettling about the JavaScript injected by the Kaspersky AV product installed on his test computer—the tag 9344FDA7-AFDF-4BA0-A915-4D7EEB9A6615 was unique to his machine, and it was injected into every single page he visited. It didn't matter if he used Chrome, Firefox, Edge, or Opera or whether he turned on incognito browsing. The identifier acted as a unique serial number that website operators could use to track him.

Kaspersky stopped sending the identifier in June, after Eikenberg privately reported the behavior to the AV company. The identifier was introduced in the fall (for those in the Northern Hemisphere, anyway) of 2015. That meant that for close to four years, all consumer versions of Kaspersky software for Windows—including the free version, Kaspersky Internet Security, and Kaspersky Total Security—silently branded users with a unique identifier.

Eikenberg wrote:

In other words, any website can read the user's Kaspersky ID and use it for tracking. If the same Universally Unique Identifier comes back or appears on another website of the same operator, they can see that the same computer is being used. If this assumption is correct, Kaspersky has created a dangerous tracking mechanism that makes tracking cookies look old. In that case, websites can track Kaspersky users, even if they switch to a different browser. Worse yet, the super tracking can even overcome the browser's incognito mode.

The behavior stopped in a new version Kaspersky Lab released in June, and the company issued an advisory about the threat a

month later. The security issue is tracked as CVE-2019-8286.

Before readers get worked up into too much of a lather, let's review a few things. Even without a unique tracking number, there are plenty of ways for websites to uniquely identify their visitors. IP addresses and cookies are the most obvious ways, but often the specific combination of installed fonts, extensions, and configuration settings are all that's needed to fingerprint a specific user, in some cases even when someone uses multiple browsers.

What's more, Eikenberg told Ars he tested older Kaspersky products with the Tor browser and found no evidence the identifier was injected. The upshot of all this: adding a unique identifier to a security feature seems unnecessary and less than ideal for privacy, but it's not something to make a federal case out of. Last, it wouldn't be surprising if other AV products do, or have done in the past, similar things.

In a statement, Kaspersky officials wrote:

Kaspersky has changed the process of checking webpages for malicious activity by removing the usage of unique identifiers for the GET requests. This change was made after Ronald Eikenberg reported to us that using unique identifiers for the GET requests can potentially lead to the disclosure of a user's personal information.

After our internal research, we have concluded that such scenarios of user's privacy compromise are theoretically possible but are unlikely to be carried out in practice, due to their complexity and low profitability for cybercriminals. Nevertheless, we are constantly working on improving our technologies and products, resulting in a change in this process.

We'd like to thank Ronald Eikenberg for reporting this to us.

Kaspersky Lab officials also confirmed that the company's AV products don't interact with TOR traffic.

The larger point of all this is that, as noted earlier, AV protection—whether from Kaspersky or anyone else—can be double-edged. Yes, it may save someone who clicks recklessly on links or attachments, but it can also increase attack surface or add behaviors that many security experts argue are unsafe. (Completely unmentioned in the c't article is the installation of a self-signed digital certificate that many AV products use to inspect HTTPS-protected traffic. That sits wrong with many people who say no application should tamper with TLS traffic.)

Deciding whether to use AV will depend on the user and the type of machine. For a dissident or government contractor actively targeted by state-sponsored hackers—especially when the target is using a Mac or Linux machine—AV probably offers more risk than benefit, since the unique identifier Kaspersky Lab was adding is within the scope of things that might be exploited.

A less experienced user surfing porn sites on a Windows machine, on the other hand, would arguably be better off using AV, since as Kaspersky's statement notes, the identifier isn't something profit-seeking hackers are likely to target. One thing is for certain, whatever decision you make, there will be someone on Twitter to tell you you're wrong and that your choice is reckless.

<https://arstechnica.com/?p=1552529>