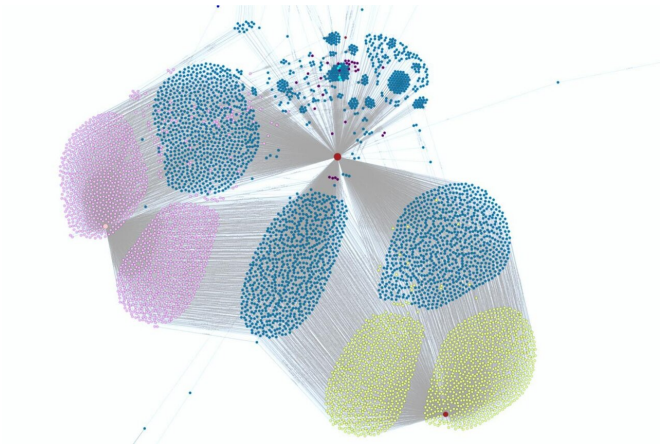
Team uncovers the danger caused by subdomains

28 June 2021



Example of a website structure with many subdomains. Credit: TU Wien

The internet is full of dangers: Sensitive data can be leaked, malicious websites can allow hackers to access private computers. The Security & Privacy Research Unit at TU Wien in collaboration with Ca' Foscari University has now uncovered a new important security vulnerability that has been overlooked so far. Large websites often have many subdomains—for example, "sub.example.com" could be a subdomain of the website "example.com." With certain tricks, it is possible to take control of such subdomains. And if that happens, new security holes open up that also put people at risk who simply want to use the actual website (in this example, example.com).

The research team studied these vulnerabilities and also analyzed how widespread the problem is: 50,000 of the world's most important websites were examined, and 1,520 vulnerable subdomains were discovered. The team was invited to the 30th USENIX Security Symposium, one of the most prestigious scientific conferences in the field of cybersecurity. The results have now been published online.

Dangling records

"At first glance, the problem doesn't seem that bad," says Marco Squarcina from the Institute of Logic and Computation at TU Vienna. "After all, you might think that you can only gain access to a subdomain if you're explicitly allowed by the administrator of the website, but that's a mistake."

This is because often a subdomain points to another website that is physically stored on completely different servers. Maybe you own the website example.com and want to add a blog. You don't want to build it from scratch, but instead use an existing blogging service of another website. Therefore, a subdomain, such as blog.example.com, is connected to another site. "If you use the example.com page and click on the blog there, you won't notice anything suspicious," says Marco Squarcina. "The address bar of the browser shows the correct subdomain blog.example.com, but the data now comes from a completely different server."

But what happens if one day this link is no longer valid? Perhaps the blog is not needed anymore or it is relaunched elsewhere. Then the link from blog.example.com points to an external page that is no longer there. In this case, one speaks of "dangling records"—loose ends in the website's network that are ideal points of attack.

"If such dangling records are not promptly removed, attackers can set up their own page there, which will then show up at sub.example.com," says Mauro Tempesta (also TU Wien).

This is a problem because websites apply different security rules to different areas of the internet. Their own subdomains are typically considered "safe," even if they are in fact controlled from outside. For example, cookies placed on users by the main website can be overwritten and potentially accessed from any subdomains: In the worst case,

an intruder can then impersonate another user and carry out illicit actions on their behalf.

Alarmingly common problem

The team composed by Marco Squarcina, Mauro Tempesta, Lorenzo Veronese, Matteo Maffei (TU Wien), and Stefano Calzavara (Ca' Foscari) investigated how common this problem is. "We examined 50,000 of the most visited sites in the world, discovering 26 million subdomains," says Marco Squarcina. "On 887 of these sites we found vulnerabilities, on a total of 1,520 vulnerable subdomains." Among the vulnerable sites were some of the most famous websites of all, such as cnn.com or harvard.edu. University sites are more likely to be affected because they usually have a particularly large number of subdomains.

"We contacted all the people responsible for the vulnerable sites. Nevertheless, 6 months later, the problem was still only fixed on 15 % of these subdomains," says Marco Squarcina. "In principle, it would not be difficult to fix these vulnerabilities. We hope that with our work we can create more awareness about this security threat."

More information: More information is available at canitakeyoursubdomain.name/ass … bdomain_usenix21.pdf

Provided by Vienna University of Technology

APA citation: Team uncovers the danger caused by subdomains (2021, June 28) retrieved 26 January 2022 from https://techxplore.com/news/2021-06-team-uncovers-danger-subdomains.html