How cybercriminals disguise URLs

By Roman Dedenok

Published: 2023-12-12 · Archived: 2026-04-05 22:53:21 UTC

Corporate information security specialists usually know quite a few confident employees who say that they don't click on dangerous links and are therefore not susceptible to cyberthreats. Sometimes those employees use this argument when asking to have corporate security measures turned off, which somehow interfere with work. But attackers often disguise malicious and phishing links, trying to confuse both mail filters and human observers. What they want is to make victims (even if they are examining URLs as we repeatedly advise) click on an address that actually takes them to a different one. Here are the most common methods used by cybercriminals to hide malicious or phishing URLs.

An @ symbol in the address

The simplest way to hide the real domain in the address is to use the @ symbol in the URL. This is a completely legitimate symbol that can be used to integrate a login and a password into the website address — HTTP allows to pass credentials to the web server via the URL simply by using login:password@domain.com format. If the data before the @ symbol is incorrect and not suitable for authentication, the browser simply discards it, redirecting the user to the address located after the @ symbol. So cybercriminals use this: they come up with a convincing page name, use the name of a legitimate site in it, and place the real address after the @ symbol. For example, look at our blog's address disguised in this way:

It looks like a page with many words in the name hosted somewhere on the Google domain, but the browser will take you to http://kaspersky.com/blog/.

Numbers instead of the IP address

In the previous method, attackers often try to confuse the user with a long page name in order to distract them from the real address — because it still remains in the URL. But there's a way to hide it completely — by converting the IP-address of a site into an integer. As you may know, IP addresses are not very conveniently stored in databases. Therefore, at some point, a mechanism was invented to convert IP addresses into integers (which are much more convenient to store) and vice versa. And these days, when modern browsers see a number in an URL they automatically convert it into an IP address. In combination with the same @ symbol, it effectively hides the real domain. This is how a link to our corporate website can look like:

In using this trick, cybercriminals try to focus attention on the domain before the @ symbol, and make everything else look like some kind of parameter — various marketing tools often insert all sorts of alphanumeric tags into web links.

URL shortener services

Another fairly simple way to hide the real URL is to use one of the legitimate link shortening services. You can include absolutely anything inside a short link — and it's impossible to check what hides there without clicking.

Google Accelerated Mobile Pages

Several years ago, Google and some partners created the Google AMP framework — a service that was intended to help webpages load faster on mobile devices. In 2017, Google claimed that AMPed pages load in less than a second and use 10 times less data than the same pages without AMP. Now attackers have learned how to use this mechanism for phishing. An email contains a link starting with "google.com/amp/s/", but if the user clicks it, they'll be redirected to a site that doesn't belong to Google. Even some anti-phishing filters often fall for this trick: due to Google's reputation, they consider such a link to be sufficiently reliable.

Email service providers

Another way to hide your page behind someone else's URL is to use an ESP; that is, a service for creating legitimate newsletters and other mailouts. We've already written in detail about this method in one of our previous posts. In short, criminals employ one of these services, create a mailing campaign, input a phishing URL, and as a result get a ready-made clean address, which has the reputation of an ESP company. ESP companies of course try to fight such misuse of their service, but it doesn't always work out.

Redirect via Baidu

The Chinese search engine Baidu has quite an interesting approach to showing search results. Unlike Google, it doesn't give you links to the sites, but instead makes links to itself with a redirect to the site searched for. That is, in order to disguise a malicious URL as Baidu, all cybercriminals need do is search for the page (and that is quite simple if you enter the exact address), copy the link and paste it in the phishing email.

And by and large, we don't know just how many other services there are that can redirect URLs or even cache pages on their side (be it for their own needs or in the name of convenience of content delivery).

Practical takeaways

No matter how confident your employees are, we doubt that they really can understand whether a link is dangerous or not. We therefore recommend backing them up with protective solutions. Moreover, we recommend to use such solutions both at the corporate mail server level, and at the level of internet-enabled working devices.
