RESOURCES • BLOG

THREAT DETECTION

“semaG dna nuF” with Right-

Override Unicode Characters

JOE MOLES

Originally published September 13, 2017. Last modified April 30, 2024.

Our Security Operations team loves to share insights on TTPs when we see them in the wild. Today we're focusing on an oldie but a goodie: right-to-left override attacks.

First, a Refresher on Right-to-Left (RLO) Overrides.

Unicode contains several characters designed to allow right to left (RTL) characters to be inserted inside text that is normally left to right. One of these is the "RIGHT-TO-LEFT OVERRIDE" character, U+202E.

For example, we can write a normal (left to right) sentence that suddenly switches to right to left:

That's cool. As soon as your terminal, browser, or operating system sees that Right-to-Left Override character, it renders every character afterward as right to left. The characters are still stored in the order they were typed — it is only the presentation

How Attackers Use Right-to-Left Overrides

Crafty attackers have been using Unicode characters to trick users into opening malicious files for years. These attacks most often try to trick the user into opening a file that they wouldn't otherwise. The trick is to make the file look like a PDF or Office document when in reality it is a piece of malware.

Let's say we have a piece of malware we want Bobby to open, and it is named with the "scr" extension, a Windows Portable Executable ("PE") associated with Windows screensaver files.

As the attacker, we can name our file: `"charity_fundraiser_bb\u202Excod.scr"`

Because of the Right-to-Left character, Bobby's email client and operating system are going to display that as:

DOCX file.

Using EDR Data to Detect Potential Threats

To detect these potential attacks, look for any filenames that include the Right-to-Left characters. In many tools it isn't possible to directly search for specific Unicode characters using the escape sequence (ie, \u202E) so you may need to copy that character, which will look invisible, and paste it into the tool's search panel. You can tell your paste was successful if you type characters following your text and they appear right to left.

[table id=3 /]

To further extend this, also look for the Left-to-Right character (U+202D) that might be used to further obfuscate the true filename.

The accuracy of this detector will be partially based on how global of a workforce you are monitoring. If your users commonly use right-to-left languages, you will see these matches more often. In that case, you can add further detection criteria to limit matches by additional context such as filename extension, file type (it is an executable/binary PE, ELF, etc), etc.

> At Red Canary, we've seen roughly 300 hits of this detector over the past 90 days across hundreds of thousands of endpoints. This is a reasonably accurate detector without a high workload impact or false positive rate to your team.

Responding to Potential Threats

Triaging and investigating these hits can be challenging because your EDR platform's

It takes a careful eye to identify the whitespace indicative of the Right-to-Left character in many browsers. The below screenshot shows an example of Carbon Black Response in Chrome.

After triaging many of these filenames, our Security Operations team is working on ways to flag these special characters in the Red Canary platform so they stand out clearly for our analysts. For the devout DFIR analyst, a Chrome plugin that flags these characters on the page would be a useful feature.

Happy Hunting!

RELATED ARTICLES

THREAT DETECTION

Artificial authentication: Understanding and observing Azure OpenAI abuse

THREAT DETECTION

Apple picking: Bobbing for Atomic Stealer & other macOS malware

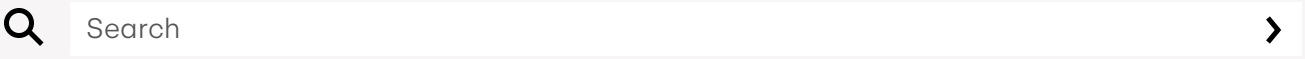
THREAT DETECTION

Keep track of AWS user activity with SourceIdentity attribute

THREAT DETECTION

Trending cyberthreats and techniques from the first half of 2024

Subscribe to our blog



GET A DEMO ›

Contact Us

Trust Center and Security

 info@redcanary.com

+1 855-977-0686 Privacy Policy Trust Center and Security Cookie Settings

GET A DEMO ›