There’s an app for that: web skimmers found on PaaS Heroku

By Jérôme Segura

Published: 2019-12-03 · Archived: 2026-04-06 01:50:46 UTC

Criminals love to abuse legitimate services—especially platform-as-a-service (Paas) cloud providers—as they are a popular and reliable hosting commodity used to support both business and consumer ventures.

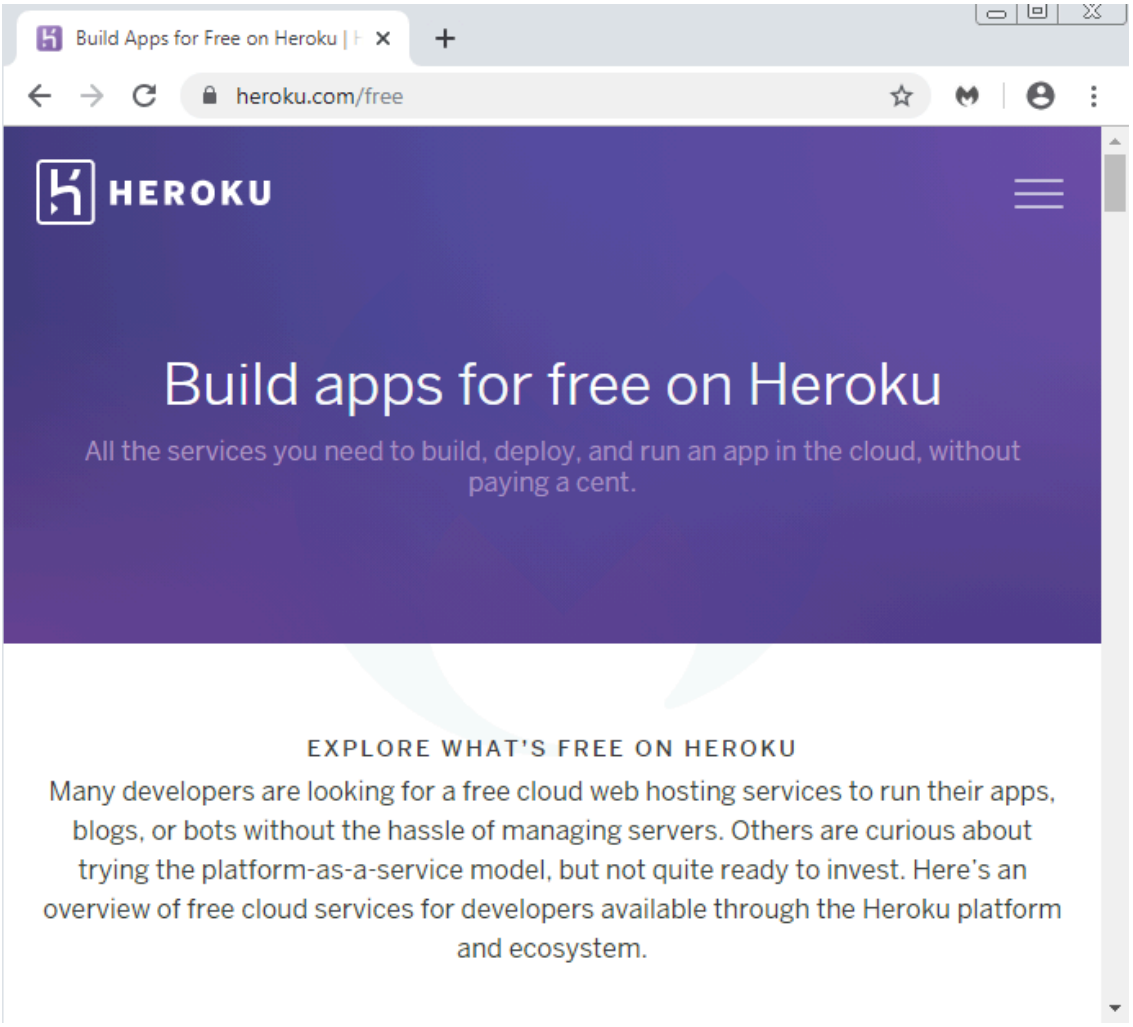
Case in point, in April 2019 we documented a web skimmer served on code repository GitHub. Later on in June, we observed a vast campaign where skimming code was injected into Amazon S3 buckets.

This time, we take a look at a rash of skimmers found on Heroku, a container-based, cloud PaaS owned by Salesforce. Threat actors are leveraging the service not only to host their skimmer infrastructure, but also to collect stolen credit card data.

All instances of abuse found have already been reported to Heroku and taken down. We would like to thank the Salesforce Abuse Operations team for their swift response to our notification.

Abusing cloud apps for skimming

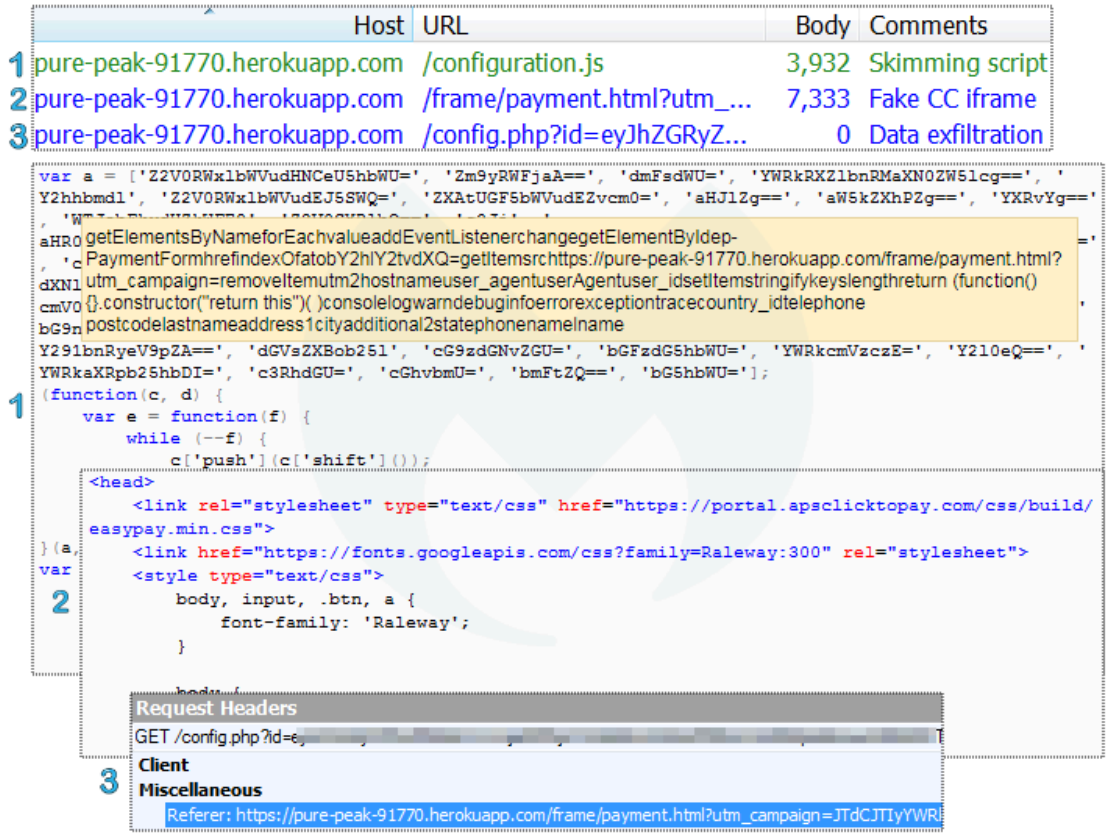
Developers can leverage Heroku to build apps in a variety of languages and deploy them seamlessly at scale.



Heroku has a freemium model, and new users can experiment with the plaform's free web hosting services with certain limitations. The crooked part of the Magecart cabal were registering free accounts with Heroku to host their skimming business.

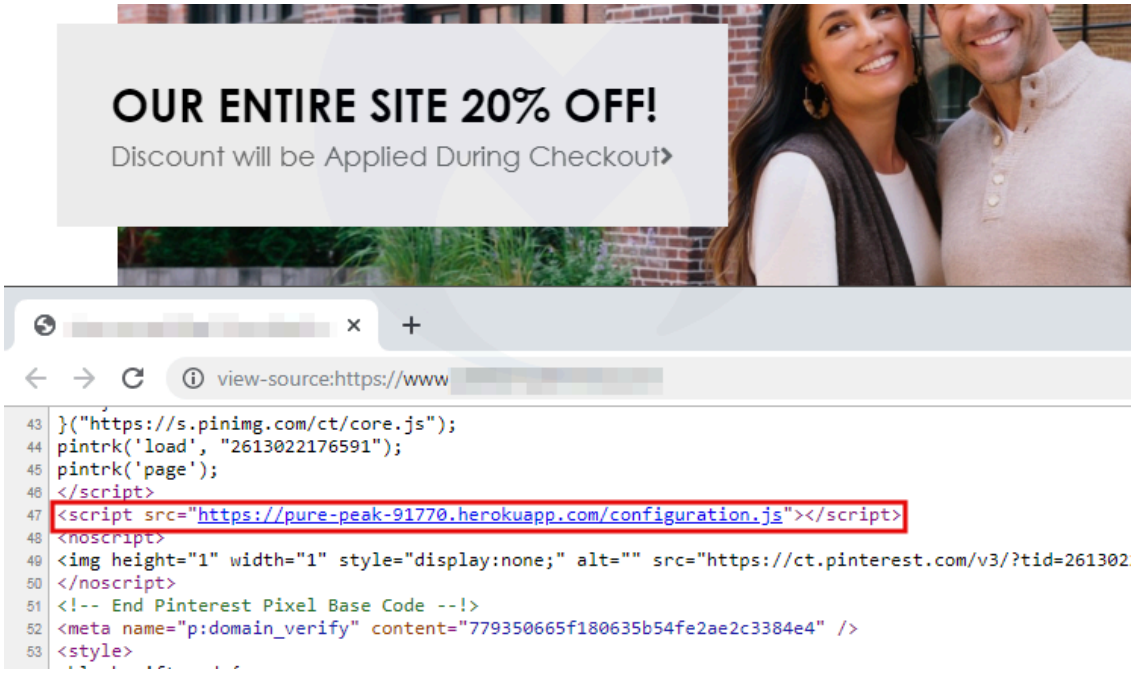
Their web skimming app consists of three components:

- The core skimmer that will be injected into compromised merchant sites, responsible for detecting the checkout URL and loading the next component.
- A rogue iframe that will overlay the standard payment form meant to harvest the victim's credit card data.
- The exfiltration mechanism for the stolen data that is sent back in encoded format.

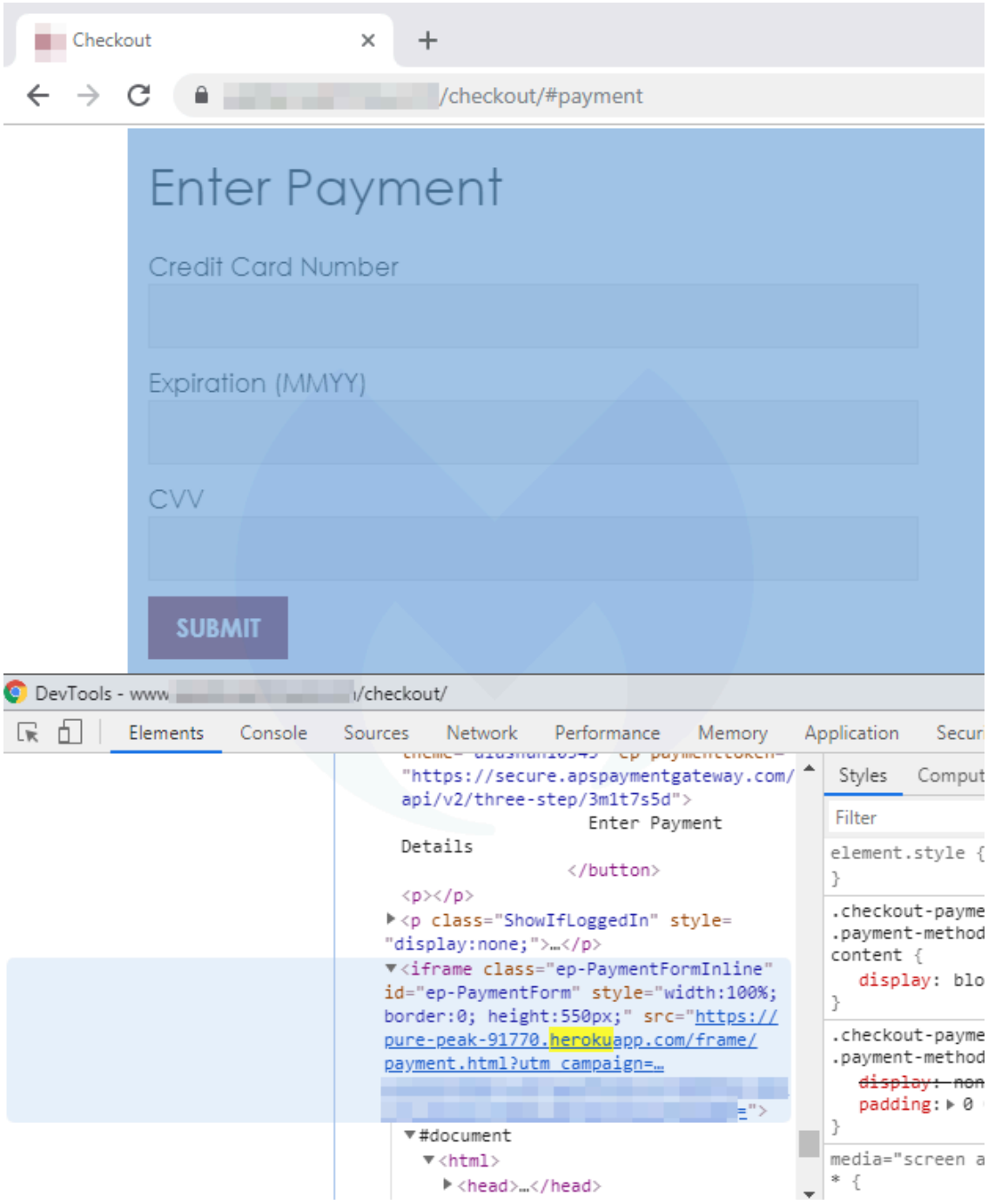


iframe trick

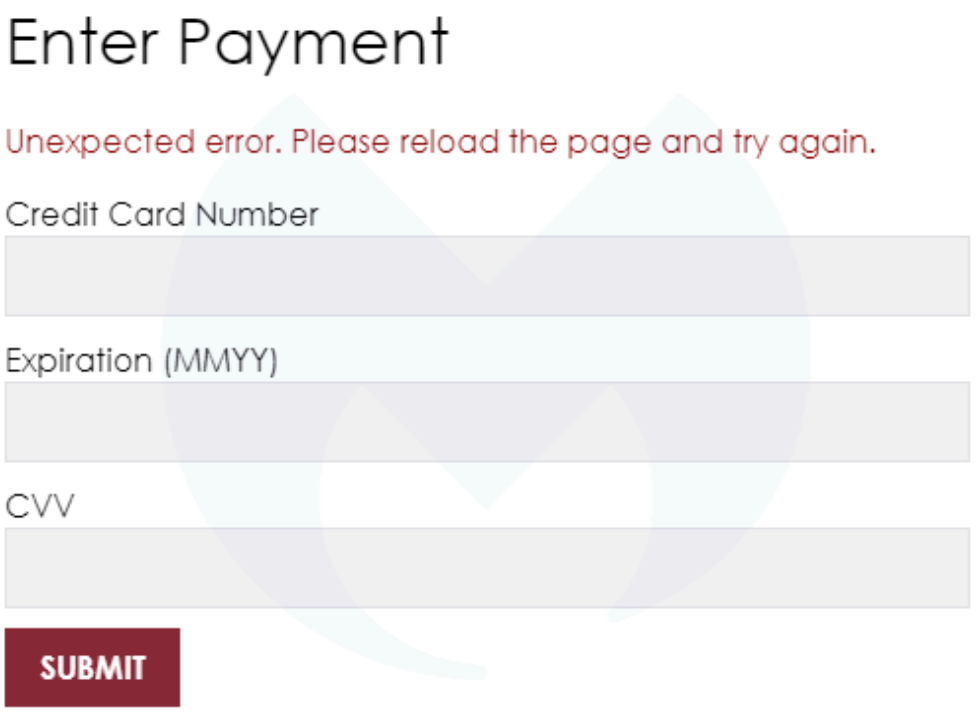
Compromised shopping sites are injected with a single line of code that loads the remote piece of JavaScript. Its goal is to monitor the current page and load a second element (a malicious credit card iframe) when the current browser URL contains the Base64 encoded string *Y2hlY2tvdXQ=* (checkout).



The iframe is drawn above the standard payment form and looks identical to it, as the cybercriminals use the same cascading style sheet (CSS) from *portal.apsclicktopay.com/css/build/easypay.min.css*.



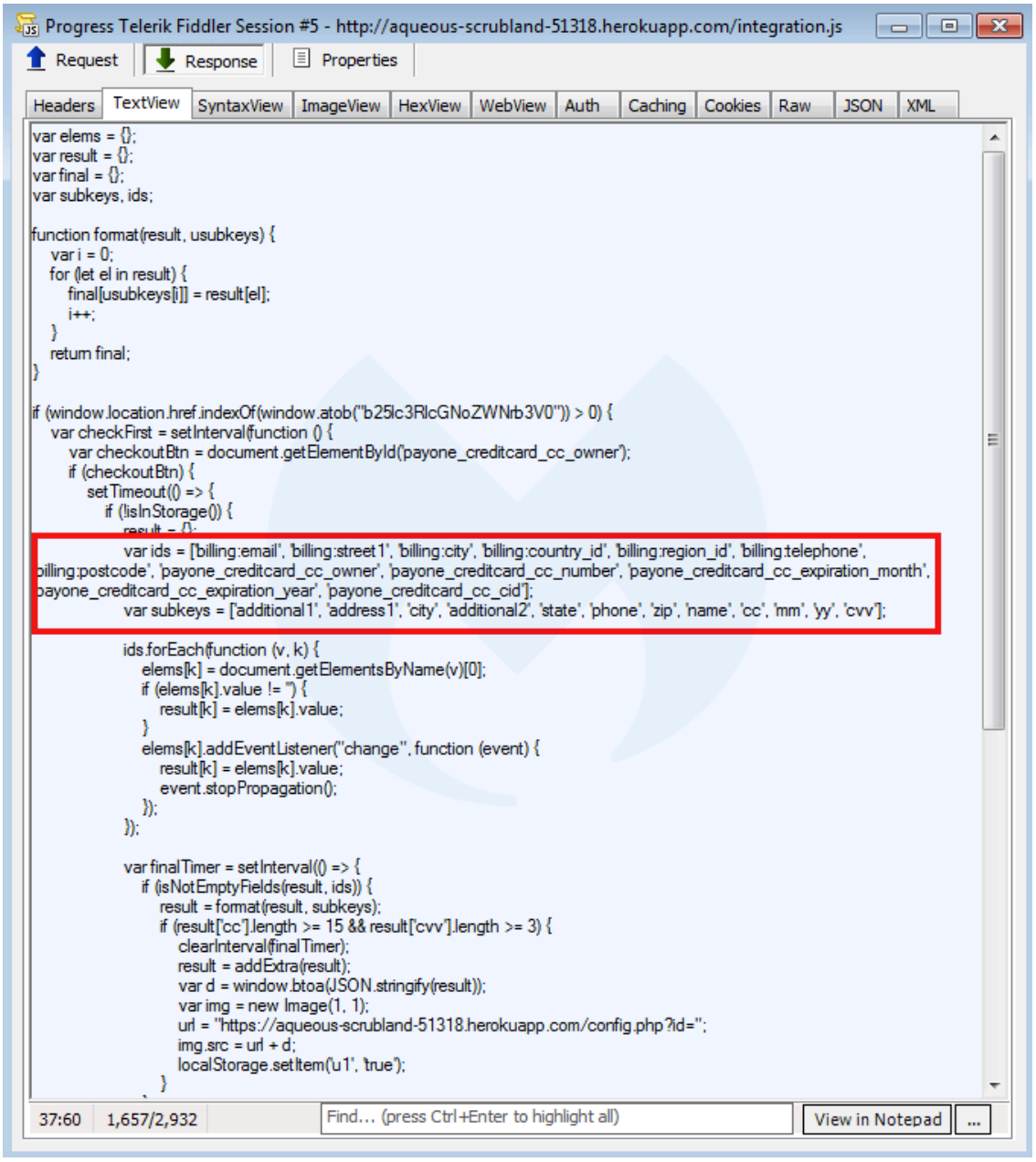
Finally, the stolen data is exfiltrated, after which victims will receive an error message instructing them to reload the page. This may be because the form needs to be repopulated properly, without the iframe this time.



Several Heroku-hosted skimmers found

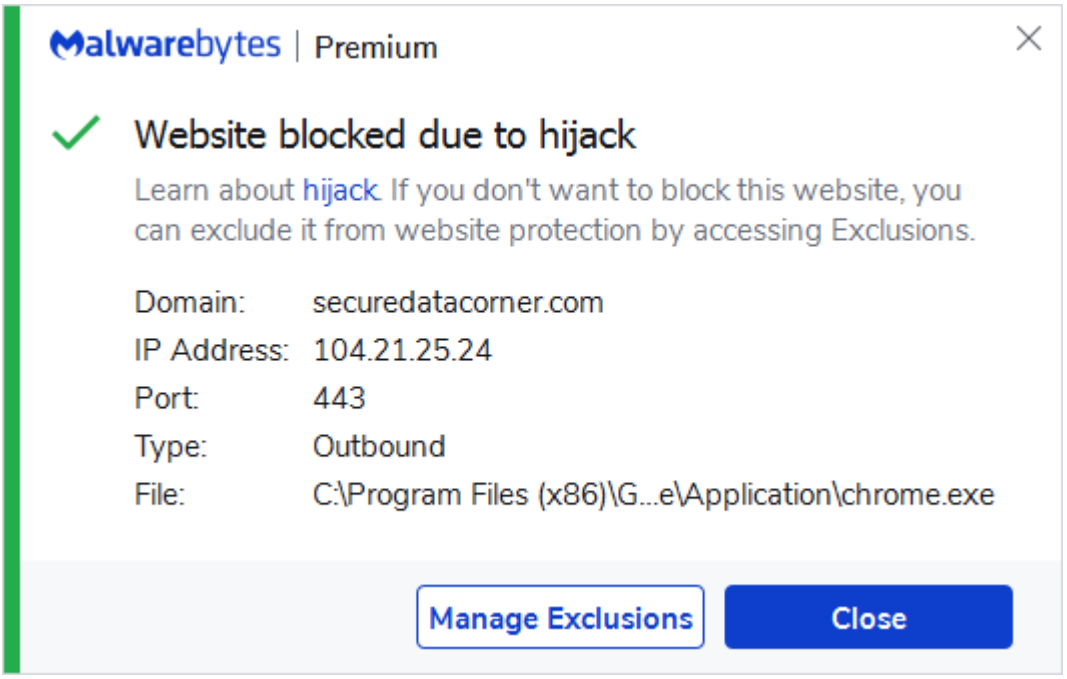
This is not the only instance of a credit card skimmer found on Heroku. We identified several others using the same naming convention for their script, all seemingly becoming active within the past week.

In one case, the threat actors may have forgotten to use obfuscation. The code shows vanilla skimming, looking for specific fields to collect and exfiltrate using the *window.btoa(JSON.stringify(result))* method.



We will likely continue to observe web skimmers abusing more cloud services as they are a cheap (even free) commodity they can discard when finished using it.

From a detection standpoint, skimmers hosted on cloud providers may cause some issues with false positives. For example, one cannot blacklist a domain used by thousands of other legitimate users. However, in this case we can easily do full qualified domain (FQDN) detections and block just that malicious user.



Indicators of Compromise (IOCs)

Skimmer hostnames on Heroku

ancient-savannah-86049[.]herokuapp.com
pure-peak-91770[.]herokuapp[.]com
aqueous-scrubland-51318[.]herokuapp[.]com
stark-gorge-44782.herokuapp[.]com

Source: https://www.malwarebytes.com/blog/news/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku