Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus

Lookout ⋮⋮ 12/11/2024

- EagleMsgSpy is a lawful intercept surveillance tool developed by a Chinese software development company with use by public security bureaus in mainland China.
- Early samples indicate the surveillance tool has been operational since at least 2017, with development continued into late 2024.
- The surveillanceware consists of two parts: an installer APK, and a surveillance client that runs headlessly on the device when installed.
- EagleMsgSpy collects extensive data from the user: third-party chat messages, screen recording and screenshot capture, audio recordings, call logs, device contacts, SMS messages, location data, network activity.
- Infrastructure overlap and artifacts from open command and control directories allow us to attribute the surveillanceware to Wuhan Chinasoft Token Information Technology Co., Ltd. (武汉中软通证信息技术有限公司) with high confidence.

Researchers at the Lookout Threat Lab have discovered a surveillance family, dubbed EagleMsgSpy, used by law enforcement in China to collect extensive information from mobile devices. Lookout has acquired several variants of the Android-targeted tool; internal documents obtained from open directories on attacker infrastructure also allude to the existence of an iOS component that has not yet been uncovered.

EagleMsgSpy

The surveillance family has been operational since at least 2017, and appears to require physical access to the device to initiate surveillance operations. An installer component, which would presumably be operated by law-enforcement officers who gained access to the unlocked device, is responsible for delivering a headless surveillance module that remains on the device and collects extensive sensitive data. We believe that this is the only distribution mechanism and neither the installer nor the payload have been observed on Google Play or other app stores.

At launch, the installer presents the user with multiple options for installing, initiating and granting additional permissions to the surveillance module.

This installer app also suggests that this surveillance tool is likely used by multiple customers of the software vendor, since it requires the user to input a “channel”, which, according to documentation Lookout researchers were able to access, corresponds to an “account”.

Lookout researchers have observed an evolution in the sophistication of the use of obfuscation and storage of encrypted keys over time. This indicates that this surveillanceware is an actively maintained product whose creators make continuous efforts to protect it from discovery and analysis.

The surveillance payload collects an extensive amount of data about the victim device:

- Notification Listener and Accessibility Services monitor device use and intercept incoming messages
- Collects all messages from QQ, Telegram, Viber, WhatsApp and WeChat
- Initiates screen recording of the device through the Media Projection service
- Captures screenshots
- Captures audio recordings of the device while in use
- Collects call logs
- Collects device contacts
- Collects SMS messages
- Compiles a list of installed applications on the device
- Retrieves GPS coordinates
- Details wifi and network connections
- Compiles a list of files in external storage
- Collects bookmarks from the device browser

After data is collected, it is stored in a staging area in a hidden directory of the file system of the device for eventual exfiltration. The data files are then compressed and password protected before being sent to the command-and-control (C2) server.

EagleMsgSpy C2 servers host an administrative panel requiring user authentication, with landing pages that read “维稳研判系统” (“Stability Maintenance Judgment System”). This administrative panel is implemented using the AngularJS framework, with appropriately configured routing and authentication preventing unauthorized access to the extensive admin API. However, Lookout researchers were able to access large parts of the panel’s source code.

The source code revealed multiple functions that distinguish between device platforms (Android vs. iOS). This implies the existence of an iOS version of this surveillance tool though Lookout researchers have not been able to locate it to date.

```
function getListIOS() {
    var _param = {
        collect_target_id: _collect_target_id,
        type: routeType
    };
    vm.isLoading = true;
    IM.getAccountInfo(_param).then(
        function (result) {
            vm.isLoading = false;
            if (result.data.retcode === 1) {
                if (result.data.data.last_sync_time) vm.lastSyncTime = result.data.data.
                last_sync_time;
                $rootScope.$broadcast('setLastSyncTime', vm.lastSyncTime);
                if (result.data.data.account.length > 0) {
                    vm.list = result.data.data.account;  // 得到登录的3个QQ账号
                    if (vm.list.length > 0) {
                        handelList();
                        // vm.currentAccount.nickname = vm.list[0].nickname;
                        // vm.currentAccount.accountId = vm.list[0].account;

                        // $state.go('home.device.im.' + vm.routeType + '.account', {
                        //     id: vm.navId,
                        //     accountId: vm.currentAccount.accountId
                        // });
                    }
                }
            }
        },
        function () {
            vm.isLoading = false;
        }
    )
}
```

A function, getListIOS(), from /assets/js/controller/device/im.js is called separately for devices identified with the iOS platform.

Lookout researchers were also able to uncover two documents that direct the user to two help files: one titled “EAGLE 系统用户说明书” (Eagle System User Manual) for using the “Eagle” admin panel, and one for installing and configuring the “MM” EagleMsgSpy surveillance client.

概述

本产品（手机临侦） 是一款集大成的手机司法监听产品， 在嫌疑人毫不知情的情况下通过网络控制实时获得嫌疑人手机信息， 监控犯罪份子的一切手机活动，并归纳整理。 其中主要包括以下几个功能点：

a) 获取嫌疑人基本信息。 其中包括联系人， 短信还有通话记录， 随时掌控嫌疑人的一切手机动态， 让办案人员清楚的了解嫌疑人的活动。

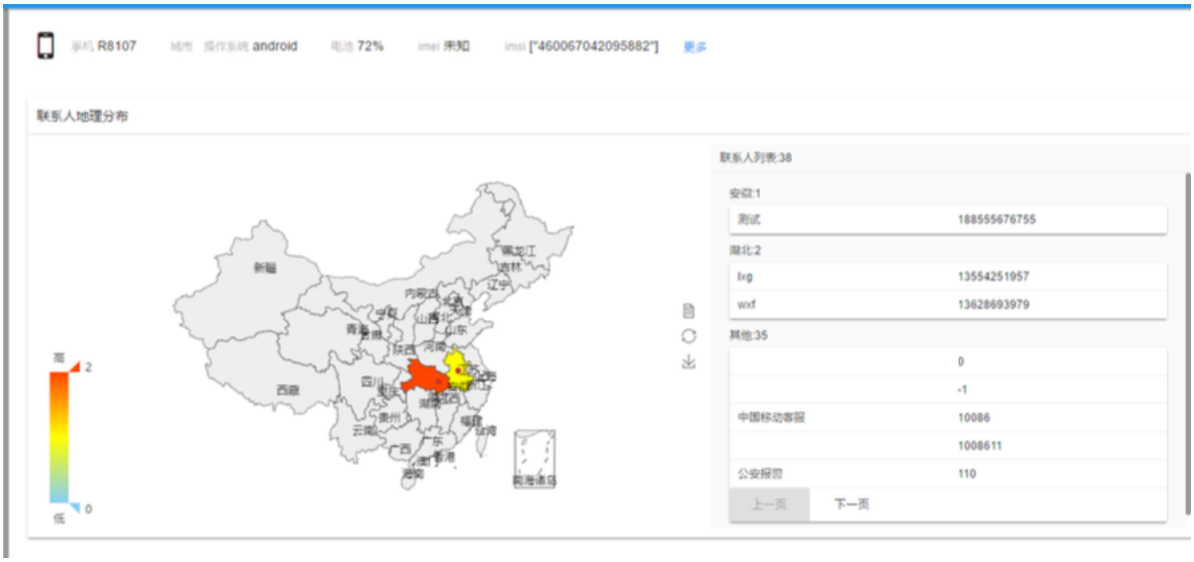
b) 获取 GPS 信息， 屏幕截图及多媒体信息。

c) 随时随地拍照， 录音， 动态了解嫌疑人的活动。

An introduction page summarizes the EagleMsgSpy client's capabilities and use cases.

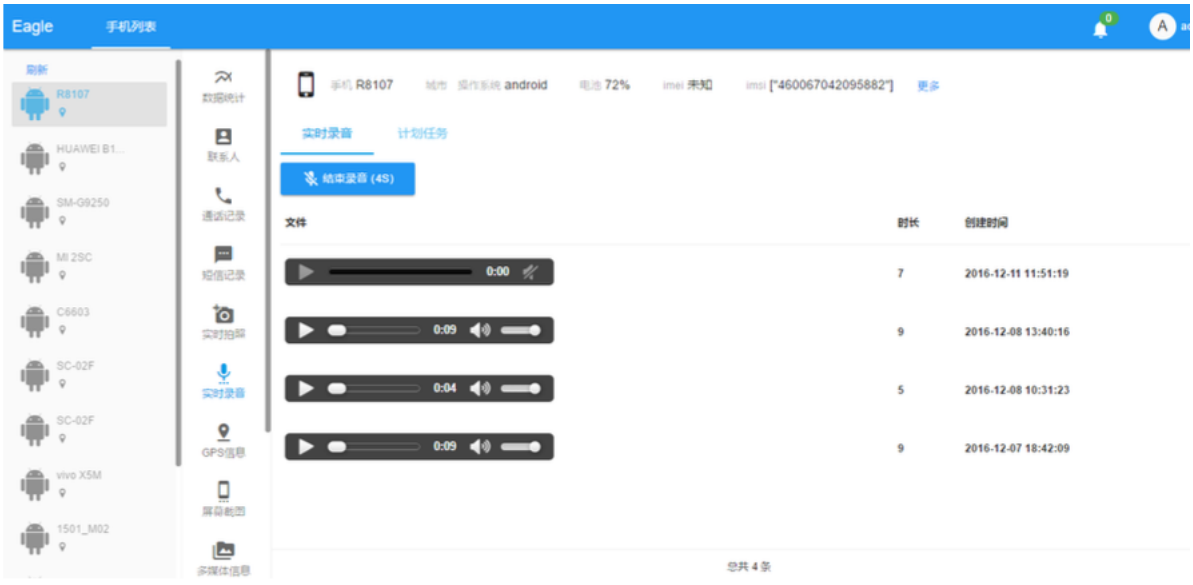
The introduction to the "EAGLE 系统用户说明书" manual calls the EagleMsgSpy surveillanceware "手机临侦" ("Mobile Phone Temporary Investigation") and describes it as a "comprehensive mobile phone judicial monitoring product" that can obtain "real-time mobile phone information of suspects through network control without the suspect's knowledge, monitor all mobile phone activities of criminals and summarize them".

The document further describes various methods for acquiring the surveillance client and installing it to the device: through a QR code or through a physical device that is able to install the client when connected to USB.



The Eagle system manual describes this view as the "Contact Geographical Distribution" graph, and explains in the documentation tha "shows the geographical distribution of contacts in the phone's address book, text messages, and call records."

The Eagle System User Manual also documents many of the views available to administrators through the Eagle web panel. These include distribution graphs and heatmaps for geographical data tied to a target device's contacts, a "Top 10" list of most frequently contacted individuals, as well as numerous views dedicated to reviewing data collected from a compromised device. The administrator is also able to trigger real-time photo collection from a device, real-time screenshot collection, block incoming and outgoing calls and SMS messages to specific phone numbers, and initiate real-time audio recording from the device.



The admin panel allows users to trigger real-time audio recordings on the device, as demonstrated in this screenshot from the manual.

Attributing EagleMsgSpy

The IP address of one of the C2 servers encountered during the investigation had previously been pointed to by several subdomains associated with a private Chinese technology company, Wuhan Chinasoft Token Information Technology Co., Ltd. (武汉中软通证信息技术有限公司). The root domain, tzsafe[.]com, was encountered in promotional materials found during an OSINT investigation into this Wuhan-based technology company. The string tzsafe also appears in all known versions of the MM surveillance module as part of a password used for encryption.

A screenshot of the GPS analysis panel shows 2 sets of GPS coordinates for locations near the 武汉中软通证信息技术有限公司 office.

In the aforementioned EagleMsgSpy admin user manual, a screenshot displaying locations of target devices (presumably test devices) shows two sets of coordinates, located ~1.5 km from the registered official business address of Wuhan Chinasoft Token Information Technology Co., Ltd.

Business registration documents for the company list an opening date of July 14th, 2016 and a staff size of less than 50 personnel. Its listed “English company name” is Wuhan Zhongruan Tongzheng Information Technology Co., Ltd with a registered address at the Wuhan East Lake New Technology Development Zone (武汉市东湖新技术开发区). In the promotional documents obtained by Lookout, the company refers to themselves as “Wuhan ZRTZ Information Technology Co, Ltd.” with the ZRTZ presumably referring to the acronym for the Pinyin “zhōngruǎn tōng zhèng” (中软通证).

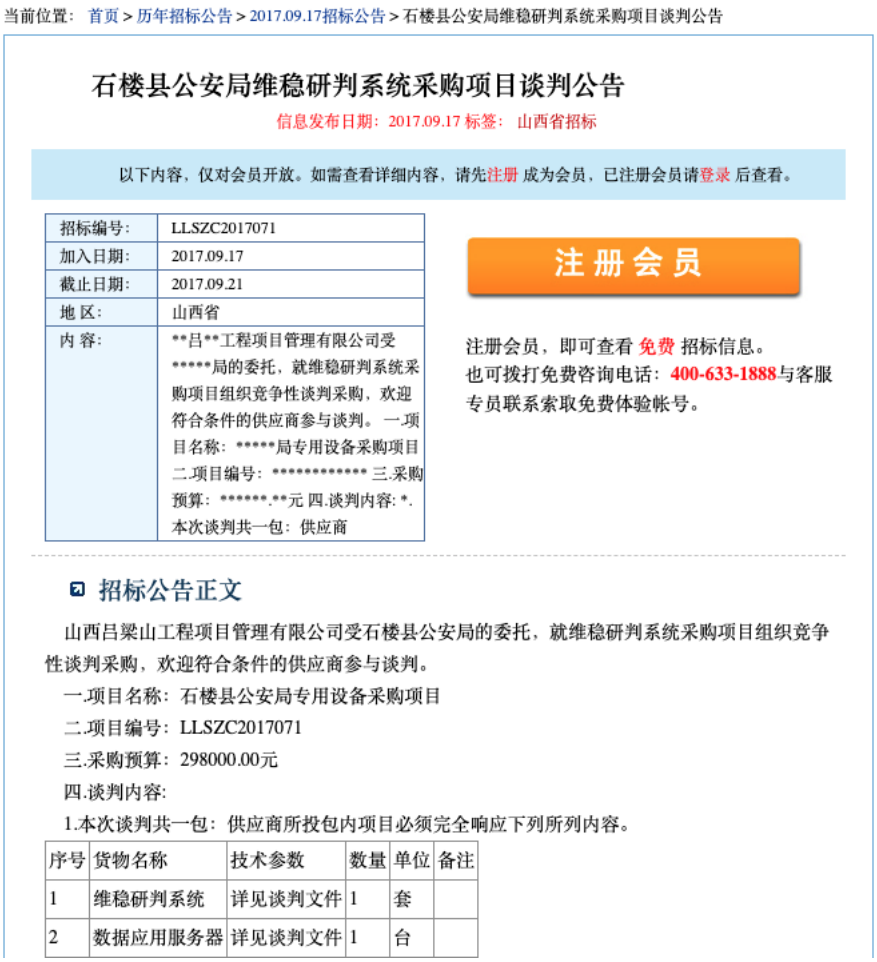
Based on this infrastructure overlap, open-source intelligence and references within the source code to part of the company’s commercial domain, Lookout researchers assess with high confidence that EagleMsgSpy was developed (and continues to be maintained) by Wuhan Chinasoft Token Information Technology Co., Ltd.

Connections to Public Security Bureaus

Infrastructure overlap between EagleMsgSpy C2s and domains used by public security bureaus (公安局) in mainland China indicate that the surveillance tool was likely used by several throughout the region. Public security bureaus are government offices that essentially act as local police stations, responsible for social order and local policing.

Public security bureaus in mainland China identified with ties to EagleMsgSpy infrastructure.

An early EagleMsgSpy variant from 2017 specifies a hardcoded C2 address that was the resolving IP for two Chinese government websites during the time in which this EagleMsgSpy variant was packaged. The domains, zfga.gov[.]cn and ytga.gov[.]cn are used for the public-facing websites of the Yantai Public Security Bureau and its associated branches. The domain zfga.gov[.]cn refers to the Zhifu Branch of Yantai Public Security Bureau (烟台市公安局芝罘分局) while ytga.gov[.]cn refers to the main Yantai Public Security Bureau (烟台市公安局). Earlier domains resolving to this IP, gyga.gov[.]cn and ykga.gov[.]cn were used by the Gui Yang Public Security Bureau (贵阳市公安局) and Yantai Development Zone Public Security Bureau (烟台开发区公安局) websites. Furthermore, an SSL certificate used by three C2s hardcoded in EagleMsgSpy variants was also used by an IP address that was the former resolving IP for the Dengfeng Public Security Bureau (登封市公安局) website.



当前位置： 首页 > 历年招标公告 > 2017.09.17招标公告 > 石楼县公安局维稳研判系统采购项目谈判公告

石楼县公安局维稳研判系统采购项目谈判公告

信息发布日期：2017.09.17 标签： 山西省招标

以下内容，仅对会员开放。如需查看详细内容，请先注册 成为会员，已注册会员请登录 后查看。

招标编号：	LLSZC2017071
加入日期：	2017.09.17
截止日期：	2017.09.21
地 区：	山西省
内 容：	**吕**工程项目管理有限公司受*****局的委托，就维稳研判系统采购项目组织竞争性谈判采购，欢迎符合条件的供应商参与谈判。 一.项目名称：*****局专用设备采购项目 二.项目编号：********** 三.采购预算：******.**元 四.谈判内容: *. 本次谈判共一包：供应商

注 册 会 员

注册会员，即可查看 免费 招标信息。
也可拨打免费咨询电话：400-633-1888与客服专员联系索取免费体验帐号。

招标公告正文

山西吕梁山工程项目管理有限公司受石楼县公安局的委托，就维稳研判系统采购项目组织竞争性谈判采购，欢迎符合条件的供应商参与谈判。

一.项目名称：石楼县公安局专用设备采购项目

二.项目编号：LLSZC2017071

三.采购预算：298000.00元

四.谈判内容:

1.本次谈判共一包：供应商所投包内项目必须完全响应下列所列内容。

序号	货物名称	技术参数	数量	单位	备注
1	维稳研判系统	详见谈判文件	1	套	
2	数据应用服务器	详见谈判文件	1	台	

A document announcing the Shilou County Public Security Bureau's request for the development of a Stability Maintenance Judgement System.

CFPs for government contracts in China are often available publicly and Lookout researchers were able to locate multiple bidding contracts for similar systems with identical generic names to the panels used at EagleMsgSpy C2 servers from other security bureaus were encountered. This suggests that EagleMsgSpy is just one of many contracted mobile surveillance tools used by law enforcement throughout mainland China.

Connections to other Chinese Surveillanceware Apps

Infrastructure sharing SSL certificates with EagleMsgSpy C2 servers was also used by known Chinese surveillance tools in earlier campaigns. The IP address 202.107.80[.]34 was used by 15 PluginPhantom samples from early 2017 to late 2020. PluginPhantom has been used in campaigns by Chinese APTs.

A sample of CarbonSteal - a surveillance tool discovered by Lookout and attributed to Chinese APTs - was observed communicating with another IP tied to the EagleMsgSpy SSL certificate, 119.36.193[.]210. This sample, created in July 2016, masquerades as a system application called "AutoUpdate".

In a 2020 threat advisory, Lookout researchers detailed CarbonSteal activity in campaigns targeting minorities in China, including Uyghurs and Tibetans. Significant overlap in signing certificates, infrastructure and code was observed between CarbonSteal and other known Chinese surveillance, including Silkbean, HenBox, DarthPusher, DoubleAgent and PluginPhantom.

Conclusion

EagleMsgSpy is a lawful intercept surveillance tool developed by Wuhan Chinasoft Token Information Technology Co., Ltd. (武汉中软通证信息技术有限公司) used by public security bureaus in mainland China. The malware is placed on victim devices and configured through access to the unlocked victim device. Once installed, the headless payload runs in the background, hiding its activities from the user of the device and collects extensive data from the user. Public CFPs for similar systems indicate that this surveillance tool or analogous systems are in use by many public security bureaus in China.

Indicators of Compromise

SHA1

dab40467824ff3960476d924ada91997ddfce0b0

fef7ad2b74db3e42909c04816c66c61c61b7a8c4

ddc729ecf21dd74e51e1a2f5c8b1d2d06ed4a559

f092dfab5b1fbff38361077f87805403318badfa

d4e943ba47f762194bcf3c07be25a9f6ea5a36b0

cea796beb252d1ab7db01d8a0103f7cca5d0955d

5208039ef9efb317cc2ed7085ca98386ec31b0b4

5d935d5ab7b7c6b301a4c79807c33e0bee23e3ff

5e282b0395093c478c36eda9b4ee50c92d8cf6eb

ec580142c0dff25b43f8525f9078dd3d6a99361c

87d925a95d584e4c46545579b01713f6d74eee00

880c46bf7e65e3f9a081f42582af1f072e22cf1a

0b1d3d87a453f63129e73b2a32d95ef3eea94b4e

8ee651a90c36a98b2ab240efb64c597c21fb6f1e

f0f3e8f01a17c7d5be440dfa7ef7e5ac1f068fe5

9557eebe4ee2dc602750365e722002d9f686b7fb

29bbb04c0180e78bd6bad49719ce92ae17081a3b

01003f047caa05873ee420e29ee54d6cc8203ca6

64aca40e982836b72f156fb66b6383a0634d12cc

e6b270be7a6c3cca16ae7268f3a93c74c14b0510

caa93aa37353cab26a30e291c41fe579d3304e1a

d6d706b23caefb2822914e294452ada77710eff3

4dfcc0b99f81b66c56059a72d4e149bc5d728b87

81c572580d09231fbdc3cf4fedb2aa07be3b7769

59987ceadbd899314ffcf77958faf3b35aa064cd

89642d092adaea7ad1e5ae77dea97bbdef5839d1

6d043b4d7bc513cc6d3e308a84ed8b63e3bab4f6

IP

61.136.71[.]171

149.28.21[.]203

47.112.137[.]199

59.48.241[.]214

61.163.69[.]238

59.48.241[.]22

220.168.203[.]197

218.200.20[.]254

202.107.80[.]34

124.163.212[.]149

119.36.193[.]210

101.201.213[.]210

111.21.6[.]126

Domain

xkong.tzsafe[.]com

www.tzsafe[.]com

qzapp.tzsafe[.]com

kong.tzsafe[.]com

i.tzsafe[.]com

git.tzsafe[.]com

es.ngrok.tzsafe[.]com

efence.demo.tzsafe[.]com

eagle.zrtsafe[.]com

eagle.tzsafe.tk

eagle.tzsafe[.]com

eagle.demo.tzsafe[.]com

bug.tzsafe[.]com