The Asacub Trojan: from spyware to banking malware

By Roman Unuchek

Published: 2016-01-20 · Archived: 2026-04-05 21:27:50 UTC

We were recently analyzing a family of mobile banking Trojans called Trojan-Banker.AndroidOS.Asacub, and discovered that one of its C&C servers (used, in particular, by the earliest modification we know of, as well as by some of the more recent ones) at chugumshimusona[.]com is also used by CoreBot, a Windows spyware Trojan. This prompted us to do a more detailed analysis of the mobile banking Trojan.

The earliest versions of Asacub that we know of emerged in the first half of June 2015, with functionality that was closer to that of spyware Trojans than to banking malware. The early Asacub stole all incoming SMS messages regardless of who sent them, and uploaded them to a malicious server. The Trojan was capable of receiving and processing the following commands from the C&C:

- get_history: upload browser history to a malicious server;
- get_contacts: upload list of contacts to a malicious server;
- get_listapp: upload a list of installed applications to a malicious server;
- block_phone: turn off the phone's screen;
- send_sms: send an SMS with a specified text to a specified number.

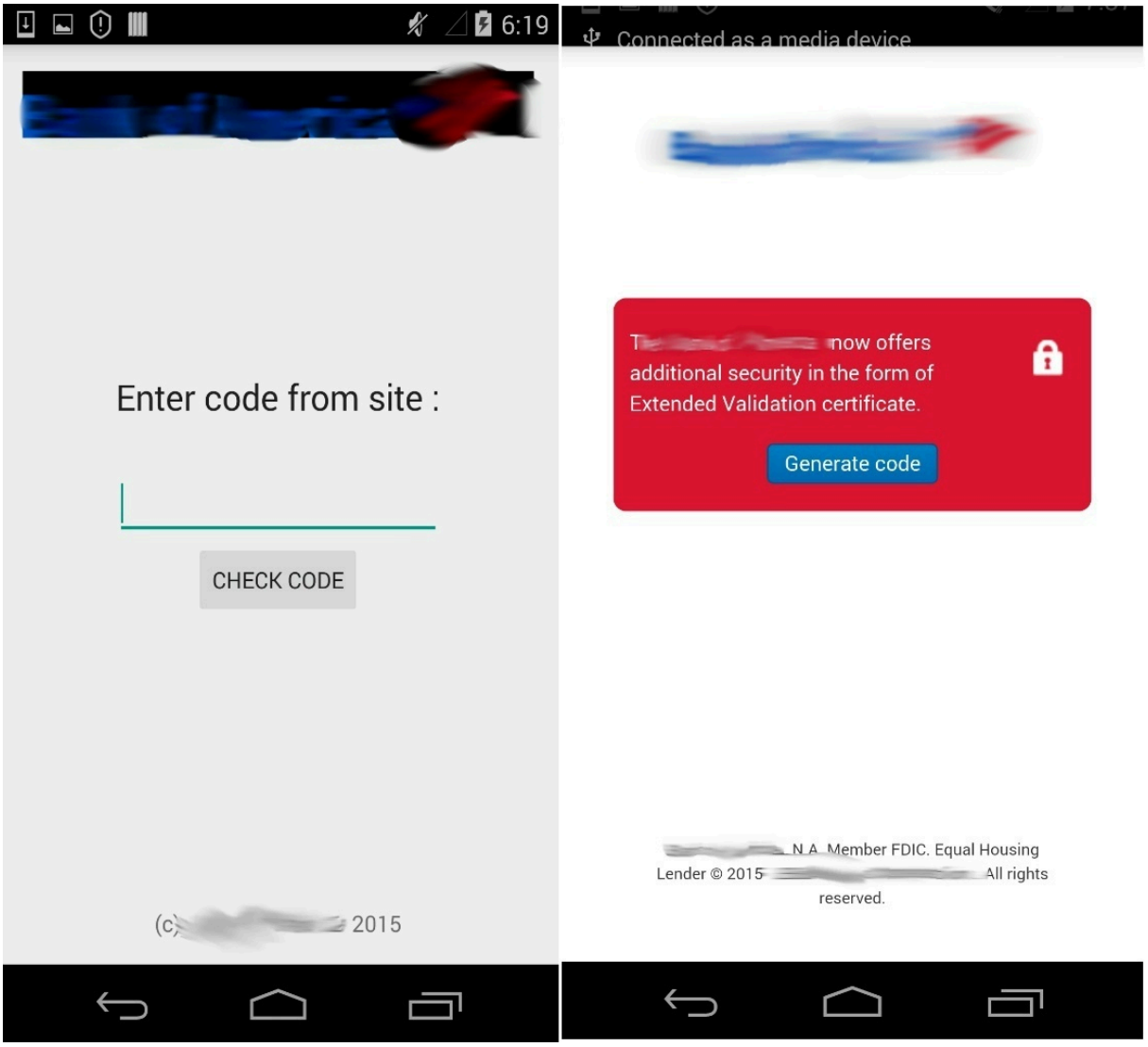
New versions of Asacub emerged in the second half of July 2015. The malicious files that we are aware of used the logos of European banks in their interface, unlike the early versions of the Trojan, which used the logo of a major US bank.

There was also a dramatic rise in the number of commands that Asacub could execute:

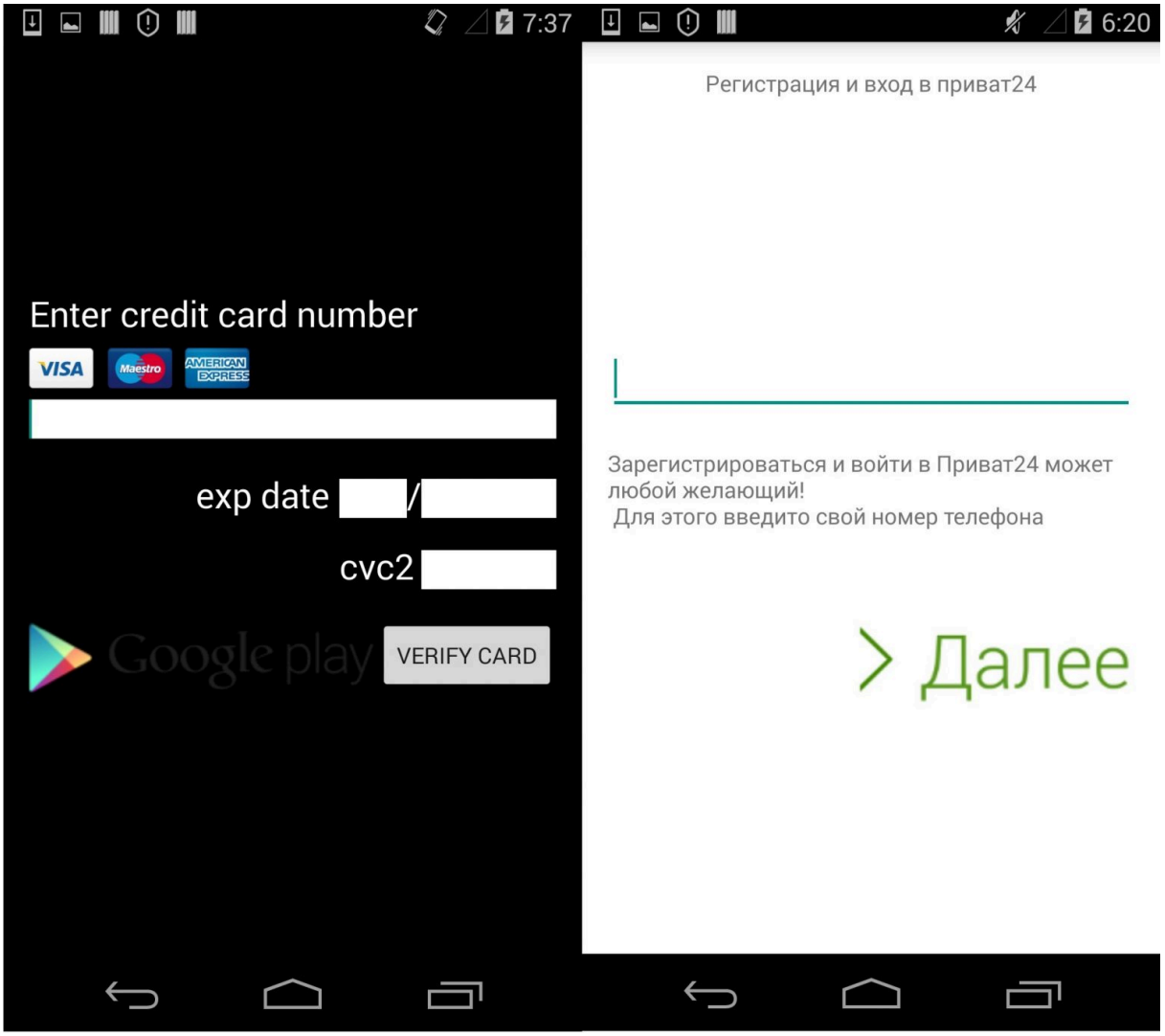
- get_sms: upload all SMSs to a malicious server;
- del_sms: delete a specified SMS;
- set_time: set a new time interval for contacting the C&C;
- get_time: upload the time interval for contacting the C&C to the C&C server;
- mute_vol: mute the phone;
- start_alarm: enable phone mode in which the device processor continues to run when the screen goes blank;
- stop_alarm: disable phone mode in which the device processor continues to run when the screen goes blank;
- block_phone: turn off the phone's screen;
- rev_shell: remote command line that allows a cybercriminal to execute commands in the device's command line;
- intercept_start: enable interception of all incoming SMSs;
- intercept_stop: disable interception of all incoming SMSs.

One command that was very unusual for this type of malware was rev_shell, or Reverse shell, a remote command line. After receiving this command, the Trojan connects a remote server to the console of the infected device, making it easy for cybercriminals to execute commands on the device, and see the output (results) of those commands. This functionality is typical of backdoors and very rarely found in banking malware – the latter aims to steal money from the victim's bank account, not control the device.

The most recent versions of Asacub – detected in September 2015 or later – have functionality that is more focused on stealing banking information than earlier versions. While earlier versions only used a bank logo in an icon, in the more recent versions we found several phishing screens with bank logos.



One of the screenshots was in Russian and was called 'ActivityVTB24' in the Trojan's code. The name resembles that of a large Russian bank, but the text in the screen referred to the Ukrainian bank Privat24.



Phishing screens were present in all the modifications of Asacub created since September that are known to us, but only the window with bank card entry fields was used. This could mean that the cybercriminals only plan to attack the users of banks whose logos and/or names they use, or that a version of Asacub already exists that does so.

After launching, the ‘autumnal version’ of the Trojan begins stealing all incoming SMSs. It can also execute the following commands:

- get_history: upload browser history to a malicious server;
- get_contacts: upload list of contacts to a malicious server;
- get_cc: display a phishing window used to steal bank card data;
- get_listapp: upload a list of installed applications to a malicious server;
- change_redir: enable call forwarding to a specified number;
- block_phone: turn off the phone’s screen;
- send_ussd: run a specified USSD request;
- update: download a file from a specified link and install it;
- send_sms: send an SMS with a specified text to a specified number.

Although we have not registered any Asacub attacks on users in the US, the fact that the logo of a major US bank is used should serve as a warning sign. It appears the Trojan is developing rapidly, and new dangerous features, which could be activated at any time, are being added to it.

As for the relationship between Asacub and the Corebot Trojan, we were unable to trace any link between them, except that they share the same C&C server. Asacub could be Corebot's mobile version; however, it is more likely that the same malicious actor purchased both Trojans and has been using them simultaneously.

Asacub today

Very late in 2015, we discovered a fresh Asacub modification capable of carrying out new commands:

- GPS_track_current – get the device's coordinates and send them to the attacker;
- camera_shot – take a snapshot with the device's camera;
- network_protocol – in those modifications we know of, receiving this command doesn't produce any results, but there could be plans to use it in the future to change the protocol used by the malware to interact with the C&C server.

This modification does not include any phishing screens, but banks are still mentioned in the code. Specifically, the Trojan keeps attempting to close the window of a certain Ukrainian bank's official app.

```
public void run()
{
  ActivityManager localActivityManager = (ActivityManager)this.a.getApplicationContext().getSystemService("activity");
  List localList = localActivityManager.getRunningAppProcesses();
  for (int i = 0; i < localList.size(); i++) {
    if (((ActivityManager.RunningAppProcessInfo)localList.get(i)).processName.equals("ua.privatbank.ap24"))
    {
      localActivityManager.killBackgroundProcesses("ua.privatbank.ap24");
      Process.killProcess(((ActivityManager.RunningAppProcessInfo)localList.get(i)).pid);
      Log.w("inject", "browser is running");
    }
  }
}
```

Code used to close a banking application

In addition, our analysis of the Trojan's communication with its C&C server has shown that it frequently gets commands to work with the mobile banking service of a major Russian bank.

During the New Year holidays, the new modification was actively distributed in Russia via SMS spam. In just one week, from December 28, 2015 to January 4, 2016, we recorded attempts to infect over 6,500 unique users. As a result, the Trojan made the Top 5 most active malicious programs. After that, the activity of the new Asacub modification declined slightly. We continue to follow developments related to this malware.
