Banload Malware Analysis Using Yara Rule

Banload (also known as TrojanDownloader:Win32/Banload) is a family of malware-distribution trojans. If installed, trojans from this family inject systems with other computer infections, most of which are categorized as banking trojans that collect user-system information (anti-virus suites typically detect these injected infections as "Win32/Banker"). The presence of Banload (and its payload) on your system can lead to serious privacy issues and significant financial loss.

The main purpose of Banload is to download a banking Trojan that steals personal details relating to victims' bank accounts. For example, logins, passwords, and other confidential information. Once the payload has stolen these details, it sends the information to the cyber criminal responsible for distribution/development of this trojan. Having Banload installed might thus cause problems with privacy and financial loss. This Trojan also changes internet settings by modifying the system registry to bypass the network proxy setting. If you have reason to believe that your system is infected with this Trojan, it should be uninstalled/removed immediately. In the screenshot above, Banload runs in Task Manager as the "**AMGZ**" process, however, it might also use other names. The "**TextInputDocsx.exe**" file on the Desktop is the attachment used to proliferate Banload.

|  |  |
| --- | --- |
| **Name** | Banload virus |
| **Threat Type** | Trojan, Password-stealing virus, Banking malware, Spyware. |
| **Detection Names (TextInputDocsx.exe)** | Avast (Win32:Trojan-gen), BitDefender (Trojan.GenericKD.41231057), ESET-NOD32 (a variant of Win32/TrojanDownloader.Delf.CRQ), Kaspersky (HEUR:Trojan-Banker.Win32.Banbra.gen), Full List ([VirusTotal](https://www.virustotal.com/" \l "/file/53c614141a6b646dc043d11271ca5dd97cd36f507c245bc1530aadba1504dcbe/detection" \t "_self)) |
| **Malicious Process Name(s)** | AMGZ (the process name can vary depending on the Banload variant). |
| **Payload** | Various banking trojans. |
| **Symptoms** | Trojans are designed to stealthily infiltrate the victim's computer and remain silent. Thus, no particular symptoms are clearly visible on an infected machine. |
| **Distribution methods** | Infected email attachments, malicious online advertisements, social engineering, software 'cracks'. |
| **Damage** | Stolen banking information, passwords, identity theft, victim's computer added to a botnet. |

**Yara Rule Details:**

* The malware samples for banload have few common urls being used as below, which I have used to detect the same in the Yara rule.
  + - http://th.symcb.com/th.crl0
    - http://th.symcd.com0&
* Builds the following file: 74c72d885e167c1ce277d33f8d8798f72c9c1c4 which seems to be unique to the sample.
* One of Banload sample file contains ykernel32.dll which is not the actual KERNEL32.dll.
* The malware uses a delete File Delete function in order to delete files from the victim machine. The below string is thus used to identify it:
  + - "F:\\Sistema\\Drivers-Denis\\FileDelete\\FileDelete\\x64\\Debug\\B.pdb"