**The signatures (static and Dynamic) used in this study for 9 families are listed:**

**Banload**

***Static Signature***

HKEY\_LOCAL \_MACHINE\SOFTWARE\Microsoft\Internet\Explorer\Main\FeatureControl\FEATURE\_VALIDATE\_URLHOSTNAME

***Dynamic Signature***

"api": URLDownloadToFileW

"arguments": {

"filepath": c:\\windows\\[Random name].[Any extension]

**Bifrose**

***Static Signature***

HKEY\_LOCAL\_ MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"system""%System%\system.exe"

***Dynamic Signature***

"mutant\_name": "Bif[Any number of Decimal characters]"

**Buzus**

***Static Signature***

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

***Dynamic Signature***

"filepath\_r": "C:\DOCUME~1\root\LOCALS~1\Temp\ [Random 8 characters].tmp"

"filepath": "C:\Documents and Settings\root\Local Settings\Temp\[Random 8 characters].tmp"

**Farfli**

***Static Signature***

"buffer": "[InternetShortcut]\r\nURL=http://www.6781.com/?001\r\n"

***Dynamic Signature***

http://install[Any single number from 1 to 4].ring520.org/kk

**Small**

***Static Signature***

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Windows Overlay Components

***Dynamic Signature***

http:/[Any domain].com/[{[Any characters]/[Any name].[exe or jpg]} or {[Any name].[exe or jpg]}]

**Swizzor**

***Static Signature***

HKEY\_CURRENT\_USER\Software\AXIS32RULE\Trans Gram

***Dynamic Signature***

[Any number of characters]s.[Any number of characters]s-local.com

**Vundo**

***Static Signature***

SysUpdProtectSynchronizeMutex

***Dynamic Signature***

"url": http://[Any domain]:80

**Zbot**

***Static Signature***

C:\WINDOWS\system32\wsnpoem\audio.dll

***Dynamic Signature***

"api": RegSetValue,

"arguments": "regkey": [Any path]\userinit\[Any path]

**Zlob**

***Static Signature***

http://auto.search.msn.com/response.asp?MT=

***Dynamic Signature***

HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\ Services\Tcpip\Parameters NameServer = "[Three digits from 0-255].[Three digits from 0-255].[162.160 or 166.191]