**Description:**

Banload is a banking malware created by Brazilian cybercrime groups.

1) It uses a digital signature in order to look like a genuine software and there by tries to evade the security solutions.

The driver is digitally signed with a certificate with the name “M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA” and uses a Thawte Code Signing Certificate.

Hence the below strings are present in the malware which can be used to identify the malware:

$b = "https://www.thawte.com/" nocase

$c = "M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA110" nocase

$d = "M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA0" nocase

2)The malware has a url embedded in it and is trying to redirect to it while executed. Below string is used to identify the malware using the presence of the url

$a = "http://th.symcb.com" nocase

3) The malware is trying to delete any AV solutions present on the victim machine. And in order to do that it has the paths of various antivirus softwares are present in the code.

These path files can be used to identify the malware. The condition is such that it identify if there is paths of different AVs on a single file.

$e = "C:\\Program Files\\AVAST Software\\Avast\\AvastUI.exe"

$f = "C:\\Program Files\\AVAST Software\\Avast\\AvLaunch.exe"

$g = "C:\\Program Files\\AVAST Software\\Avast\\AvEmUpdate.exe"

$h = "C:\\Program Files\\AVG\\Antivirus\\AvEmUpdate.exe"

$i = "C:\\Program Files\\AVG\\Antivirus\\AVGUI.exe"

4) The malware uses a delete filedelete function in order to delete files from the victim machine. The below string can be used to identify it:

$j = "F:\\Sistema\\Drivers-Denis\\FileDelete\\FileDelete\\x64\\Debug\\B.pdb" wide ascii

**Yara Rule:**

rule Sample

{

meta:

description = "Rule to identify Banload malware"

author = "Jerald"

strings:

$a = "http://th.symcb.com" nocase

$b = "https://www.thawte.com/" nocase

$c = "M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA110" nocase

$d = "M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA0" nocase

$e = "C:\\Program Files\\AVAST Software\\Avast\\AvastUI.exe" wide ascii

$f = "C:\\Program Files\\AVAST Software\\Avast\\AvLaunch.exe" wide ascii

$g = "C:\\Program Files\\AVAST Software\\Avast\\AvEmUpdate.exe" wide ascii

$h = "C:\\Program Files\\AVG\\Antivirus\\AvEmUpdate.exe" wide ascii

$i = "C:\\Program Files\\AVG\\Antivirus\\AVGUI.exe" wide ascii

$j = "F:\\Sistema\\Drivers-Denis\\FileDelete\\FileDelete\\x64\\Debug\\B.pdb" wide ascii

condition:

$a and

($b and $c and $d) or

// digital certificate intended to evade security solutions

($e or $f or $g) and ($h or $i) or

// the malware tries to delete AV solutions

$j

}