

Threat Category: Remote Access Trojan (RAT) ? Malware

Threat Name: Indetectables RAT

Threat Description: Indetectables RAT is a Brazilian remote administration tool known for its stealth and evasion capabilities. It was identified based on research by Paul Rascagneres and Ronan Mouchoux, highlighting unique string artifacts left in the malware binaries.

Indicators of Compromise (IoCs):

File must contain at least one of the following strings:

\$s1 = "Coded By M3" (fullword, wide)

\$s2 = "Stub Undetector M3" (fullword, wide)

\$s3 = "www.webmenegatti.com.br" (wide)

\$s4 = "M3n3gatt1" (fullword, wide)

\$s5 = "TheMisterFUD" (fullword, wide)

\$s6 = "KillZoneKillZoneKill" (fullword, ascii)

\$s7 = "[\_\_M3\_F\_U\_D\_M3\_\_]\$" (fullword, ascii)

\$s8 = "M3\_F\_U\_D\_M3" (ascii)

\$s9 = "M3n3gatt1hack3r" (fullword, wide)

\$s10 = "M3n3gatt1hack3r" (fullword, ascii)

Detection Mechanism:

The file must have a Windows executable signature (MZ header, uint16(0) == 0x5a4d).

The file size must be less than 5000KB.

Detection is triggered if at least one of the strings is found.

Reference: Research article: When a Brazilian String Smells Bad

Author: Florian Roth (Nextron Systems)

Rule Metadata:

description: "Detects Indetectables RAT based on strings found in research by Paul Rascagneres & Ronan Mouchoux"

license: "Detection Rule License 1.1"

date: "2015-10-01"

reference: "http://www.sekoia.fr/blog/when-a-brazilian-string-smells-bad/"

id: "f8322822-617c-50cf-8b64-60da3a202ca5"

hash1: "081905074c19d5e32fd41a24b4c512d8fd9d2c3a8b7382009e3ab920728c7105"

hash2: "66306c2a55a3c17b350afaba76db7e91bfc835c0e90a42aa4cf59e4179b80229"

hash3: "1fa810018f6dd169e46a62a4f77ae076f93a853bfc33c7cf96266772535f6801"

super\_rule: 1