Metamorfo (aka Casbaneiro)

github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/metamorfo.md

jeFF0Falltrades

jeFF0Falltrades/
IoCs

A collection of Indicators of Compromise (IoCs), most aligning with samples derived from the signatures in the YARA-Signatures repo

1 Contributor

0 Issues

27 Stars

2 Forks

Reporting

YARA

```
rule metamorfo_msi {
  meta:
    author = "jeFF0Falltrades"
    ref = "https://blog.trendmicro.com/trendlabs-security-
intelligence/analysis-abuse-of-custom-actions-in-windows-installer-msi-
to-run-malicious-javascript-vbscript-and-powershell-scripts/"
    description = "This is a simple, albeit effective rule to detect most
Metamorfo initial MSI payloads"

  strings:
    $str_1 = "replace(\"pussy\", idpp)" wide ascii nocase
    $str_2 = "GAIPV+idpp+\"\\\\\"+idpp" wide ascii nocase
    $str_3 = "StrReverse(\"TEG\")" wide ascii nocase
    $str_4 = "taller 12.2.1" wide ascii nocase
    $str_5 = "$bExisteArquivoLog" wide ascii nocase
    $str_6 = "function unzip(zipfile, unzipdir)" wide ascii nocase
    $str_7 = "DonaLoad(ArquivoDown" wide ascii nocase
    $str_8 = "putt_start" wide ascii nocase
    $str_9 = "FilesInZip= zipzipp" wide ascii nocase
    $str_10 = "@ u s e r p r o f i l e @\"+ppasta" wide ascii nocase
    $str_11 = "getFolder(unzipdir).Path" wide ascii nocase

  condition:
    2 of them
}
```

Sample Hashes

```
22c51c43fe8344d36005613209fecb9219b06abfdb12e3019876eca0d1495e23
d663f2c1a5075b43cc2706d58ae98dbb4b1ab168d5c99b43d5cb0b80e18937cf
0113d8a67b61dd6163b003c806d997f1f26da9df316744571aa1295c7ffb9995
1bb9382349266630cfc2f36d2af3c8b06ba4b153867161bf44143f952d33680b
3f9a7292c3b4837477ef5d8181fae11e827753a575f0ee852546fe64c79389ab
42c82a811f4eb41e1a6c613c9b017b7e8abf062c3694cb77e671464954facf3b
67255c29a1b2fcc1f9067f08fcf575a2d654e4f8d235a5a583ff2605b7728455
77ca06b5bd03556261e7f2359eaaad2c220771618456d9128b1750eef3fa2b8e
8aa574ba92ef3177d786c519d9f2acc86aa7d16afd44819cb23eddd28720776c
d9114962efbc4f34b093bd04e5d41000ebd416fcc8a6d68faeb7455d64d78081
```

Sample C2

```
http[:]//80[.]211[.]252[.]12/sfsfsdgfbd456416[.]zip
http[:]//buleva[.]webcindario[.]com/01/
https[:]//s3-eu-west-1[.]amazonaws[.]com/disenyrt3/image2[.]png
https[:]//s3-eu-west-1[.]amazonaws[.]com/sharknadorki/image2[.]png
https[:]//s3-eu-west-1[.]amazonaws[.]com/jasonrwk5wg/image2[.]png
https[:]//s3[.]eu-west-2[.]amazonaws[.]com/stocksoftbr/ModPumMs2003[.]zip
https[:]//s3[.]eu-west-
3[.]amazonaws[.]com/abrilgeralll/ModPmAbrilzada[.]zip
https[:]//s3[.]eu-west-2[.]amazonaws[.]com/stocksoftbr/Mod1803xrd[.]zip
```