FRat

github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/frat.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

Note: I have not seen much coverage of this malware family.

The name 'FRat' was derived from research by @James_inthe_box, seen in the linked Tweet thread below.

If you have more information on this threat, please contact me on Twitter

A RAT employing Node.js, Sails, and Socket.IO to collect information on a target.

Reporting

Snort/Suricata

> https://twitter.com/James_inthe_box/status/1270804510957428736 (H/T @James_inthe_box)

YARA

```
rule frat_loader {
  meta:
    author = "jeFF0Falltrades"
    ref =
"https://twitter.com/jeFF0Falltrades/status/1270709679375646720"

  strings:
    $str_report_0 = "$ReportDone = Get-BDE" wide ascii
    $str_report_1 = "$Report = Get-BDE" wide ascii
    $str_img_0= "$ImgURL = Get-BDE" wide ascii
    $str_img_1 = "Write-Host 'No Image'" wide ascii
    $str_img_2 = "$goinf + \"getimageerror\"" wide ascii
    $str_link = "$eLink = Get-BDE" wide ascii
    $str_tmp_0 = "$Shortcut.WorkingDirectory = $TemplatesFolder" wide
ascii
    $str_tmp_1 = "TemplatesFolder = [Environment]::GetFolderPath" wide
ascii
    $str_tmp_2 = "$vbout = $($TemplatesFolder)" wide ascii
    $str_shurtcut = "Get-Shurtcut" wide ascii
    $str_info_0 = "info=LoadFirstError" wide ascii
    $str_info_1 = "info=LoadSecondError" wide ascii
    $str_info_2 = "getimagedone?msg" wide ascii
    $str_info_3 = "donemanuel?id" wide ascii
    $str_info_4 = "getDone?msg" wide ascii
    $str_info_5 = "getManualDone?msg" wide ascii

  condition:
    3 of them
}

rule frat_executable {
  meta:
    author = "jeFF0Falltrades"
    ref =
"https://twitter.com/jeFF0Falltrades/status/1270709679375646720"

  strings:
    $str_path_0 = "FRat\\\\Short-Port" wide ascii
    $str_path_1 = "FRatv8\\\\Door\\\\Stub" wide ascii
    $str_path_2 = "snapshot\\\\Stub\\\\V1.js" wide ascii
    $str_sails = "sails.io" wide ascii
    $str_crypto = "CRYPTOGAMS by <appro@openssl.org>" wide ascii
    $str_socketio = "socket.io-client" wide ascii

  condition:
    3 of them
}
```

Sample Hashes

FRat Loader Scripts

```
dc948f4aacc765b1fbdd58372bb847750fcf08544841ef4a44454da8e3b46bae
1fa16740010c3608870f4b14ccc33cd58417648d0e26a417b0e125bc4671e70a
e1a982ab68b5fd14c6723eab266d371184d395ad8e22a9d3cd93ba1c9c228458
```

FRat Executables

```
b330cd9151ebb66615ef6c16ab60b41dd312356505ee10a02f85bccfedda3948
0aa12e18ff73617f4c12a82dc35980ec1edbb9e0fdadfaa8dcf964c70ccfbe7e
dd011c1e7417131018d25543880d96c0c1ff44a6c4454b9020a183b69da80b9f
a9552d16e9c6c1a2ceb9d8ae52725cbcdac331908c37f253299d399e12c63018
804f30400752e1bfaf21b2f37fffb99c34876372b95181aca98dbb04efe19368
0f25d3cf1a783e4e0d70fba2fa0b87e2ed74bff26a4da6890dac36ba99a72726
1345900b66f803046730cd9c3a4465777a28e004f8de6b19f9e8ce948397f57a
```

Sample C2

```
go[.]ehades[.]best
go[.]ehades[.]best:8443/socket.io/?
__sails_io_sdk_version=1.2.1&__sails_io_sdk_platform=node&__sails_io_sdk_

e[.]hemera[.]best
v[.]hemera[.]best
paravan[.]duckdns[.]org
download[.]xn--screensht-nsd[.]net
travma.duckdns[.]org
```