Government of India
National Critical Information Infrastructure
Protection Centre
(A Unit of NTRO)

Date: 28 Nov 2019

Cyber Security Advisory: Weekly Mirai Activity Report

This data is to be considered as **TLP:GREEN**

This report is generated by our trusted partner from statically analyzed Mirai samples identified over seven days.

* Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.
* Network IOCs are identified from newly identified samples but may themselves not necessarily be net new.
* Because of the nature of the static analysis there is MODERATE confidence in the accuracy of the network IOCs.

IoC's

Sample IOCs (SHA256):

```
8e79db6745ac4c3130a61da78c3c1e8d0dad59cee9e0cd309380478b42c62a17
e8368d2ff72e817e5a90d6ba52c1e4f1c79883140f0882f64d0170c800cd4376
8974b3af36eb1fb11989ca1a1e7fcde489c64b70f9f9f8b532c51c2eec14841e
fc9313c2105e879eeddc314eb742860797453d933c7e8e9c29280f0efd8922ee
80e42c251ebb75fbc3b9259ddc3c93ab71f2e5a9c12c5804b15bc4808ab976ca
48cb524e22a07401715a014d7a1b1df130ede9ab9660516531edc952f7dd268d
0cc36e494f75122b031cbbbed636e84273d0b57255b37837dc2526605f4c1efc
6ae7f56ef8cdd4272a2f2512d1bd03ec6c71b3da2bef39acfd3752ed11ee53e0
eacdbdd2b6bdcc7fba6119cd989d55fbb7ea11d4980f285c90c4a8675e958636
999b3740df0975104e868f5fd2c32636c2d7e64511ec678079a531a7be2bd466
48e641953bb1f03fb03523b41f7f86cb0723d63b4a3c7ac596b65ac56d9d5f3b
28bfcb319555058db7fbabaea449e9031ac2a79151d313211dd2dbc74a7a6387
764d2fb187c6daaba4750869857cc89538f47fcb3ad35c416fedb230992e1911
944ba15d204793dfcd67fc7065dd829f0e0c6c239d7f42cf1f3f983bd7b96301
da3a08c353d348e2d2ebacef465ad87d0cee44e06d553c4c795d6c0a654a0417
357d7f32597d980f328eccaa8e542d768b82c388fd95093ddbfae521e948432d
8a07aeea35721918ebc5b820ee919dc1ed29a4323c1351be0adf342748fcc8c8
94a9172ac6de1252eb9b3d709ac804bc71eabe02430e93c5e86a7c9af520293b
69d10d0fdf354d66bf2f2d3f9ffad3eacec2a7a5026db93165969a97b71e8cd0
d3de9848aeb41f62264cd193312926738fc0ea7a0ac0f5bbfc2cfd488c1df25b
2e3f5679674e401b7774d07a852a29b45044bd04fc6ec2149c2d97ee0303de18
8d6dadfa8de21e286c4dbef4f437f340f22d4c6fec1240a4e5ae30bca5a91a4f
0e7228db76a6727989a2fdc00278ab8bcf8784d2c06c669881a6c8cb9451067e
d12aded9a07fbc13b3ac53ec29b878ea1c371441b1fa3703232c2ade15dc767e
492104230b352ac46f9fb162a2e786a9568c51d8e0446f40b49b6b023d3dbadd
b3cf5e09853e21157c302ba69868d4bb6b3c0e9922d0e99b6691d2e8ae2df404
fd27fec374cccaeb6966470c085ba7163fb2eeedba84b0c5b14e699cdf66db35
2d85395ca3256cc6ce3bd6848bf9e18a95f7bd88752638b7bc71a2d748a870a0
334561521b48efaa35174b00236cc02455dae0d6bfb6ceac626d342ec851637d
12143df094bf7dfe3436b9846f9c11da6071ff7692d57dab3c92e2cc047cb0a1
736169d6a5644980652e40439dc16a5b368b712b1e5435eae1560540a8b75f56
55485e0654445cf9dc148a993fb6d3db4fb090f424064ffd654f24723dadc8df
2d8564bf4995dc9f3b2a0967ebc0290129afdb1c4b20570bc1aa11a0895b0074
bd7981f10db227d6cc85f86125a0704aa1ed5f141e7e2b043da767ea5104d92c
81caa4f63cf2e940b7abdddcf87e904694ddebfceb72b572d98b926d3c17bef9
cc3f9d4d29fced5e324f0930397429de14255cf6088db43f8baca17e6890ffad
3b17de5d0af24988f410ad75a83a5b00c8251d96aae6d4dcf3c18e9e39362bcf
ec93fafde671640753882c9ba1552c4bb76d03d11458a48f4479048562ad808d
fec19e296ddd00834ce1f70627b8c586b9175d1d9a7f5bb0a65672624da9dc21
ec42c40c0352a4b31994e6d3f5459b2a1b58682de88fd75f44ede5f2ba3a0a64
3ef588064d9962026322a1ef33e0d627c5f3650cc5265a3e267ded1016c7e03a
3ca14e48b9d61896f3296a3d74ede6838ea2279b54b11e65dd964218ebb49b7d
08d6c9afae79763446a1aa8d2a30d72ea50491f103da258911c55d86a0318ede
2ebe9ff281750599ac9c4e8f31d78e48edad0ec5e12aaebcdb8bb819f63f7590
9367d43f2fa357ee68599e1d861563822260ac28012d6319b823074cfe59d099
3dba8971d720ba1afe99655a35501660722352cfd6ced37dce3d3927d6b569f8
1365f6bf082d48633a9a29082b9d2f6c5e0f429b022a0c909d2dd3033464b064
b912d0d464a0e51e1b08ab42d07d106454036a78200e269a6e7a514891d3a28a
4801d177ae92b03cd17c0b79763ab1aaf6afa5f210dfd199c9fda2e6217da4f5
```

```
fa8d14c301fd72f74a371686704ce0feed2ec2aea7dea5829491f9b84ef9919b
c86a4f2e6fbcccc9df8269819070e81764c001f2bb95f69a09b8b1b23b04ec02
3069d93572d6e37c696a01eede423fe134d101865005861ee5d86ce064c5374d
ae1a25b87952d3c6ab8079b3f43afe08acd02c0c1e47c8ac29045dda5e3b59ce
30d31e32322fa3ec42949bf08762619e972ed151700dc90fdb9df3709b338bfa
093ef2f13e366d05e4beec82f9fcdcd6b624b09c22e9463e80c29be726bac0e6
e7cab34a34b36de1d456a186372f2b01e683f546d0a91c0beb6267a055bb0a11
8f12122c88e54d8e6f964535734831645bbbede4042d573cb9eef95901966a64
704ffaec3be8c8ebaa96af05bbd85bd80c4c279f4c994cfb3a458b540e9c451c
8c50f80bd254aa67a91ce7066ceb0af46fe461446dcefc40011977c343da1519
319a74e87d69f9ab9a035ee433dfc176de766b32ba0d6dd923bfa4dd9fc4ecd7
0139b5b94ffcc4cb007fe0df802d2b852a3afa258f57c79c6a78dcf23663dd04
d52f241fa9a47af92d7740959e9344b97d01991db511c6fe62cc3c8c7eff0676
3ecd15ffe26f1c6d0b6ec2bb3bf4be05a5fe8987a693b09699c560d255dc3737
5a437e095a5ed869d85c937fcac5e4309472c338e877f1dbcaff1222e6d73d0f
121d72d9f91b60e3e346da204fef7f472b465d38ffcc2c1054ab5f0a45c2e82f
e0ad9afd4d53d76362f8db952d8f947b0a97a9004071c47c9b0778a0881e998c
acbfbab4be5c78664c2f947f4d316b6b12c853b7f0ca3f6e4da81d0e2b1b0517
3c2dec446897e35bca28f867fd74fb35330e4f8c04ed37cfaa5ec613cf43c101
990e0c2d850b3cca09304b0b5144256a9fec28f3fcbbcd915ad991402474195c
0598cad7d6af84a0f4a803439c868269e00eed1b097f9430168d8e21761cdb63
8958bbdceca378f49a433ebe2a904b22ccc225cd58973881f60ef09ce878d8dc
47608163e5376960306d45fa0addebba03187e623149b12ebd2d77a361649aac
9ae714f07c32e8d049085fdaee8f3e4b7e7d10d7a0ae3553d2435289faae67c6
5c2ead62514b2921057d353fd49388a371f317908886b2ce795fafd4c2ffcd27
7f5787dc95903248c2747c03ac6a3cd19f9cfc570a33eee621bc0cf43ee97580
55919c1e3a3a14c40231cb6207da12b43f7453a7af1bb99cd7ce2dcba5567ff2
d6f266f5797c13c63bcc91567fb2484dbf6cc36ffdd67f8b8c6ea305c53bb32b
dfe0c1017c17c6d0e07baf2b7cbfc9090acc45df104f772d29ea4f4a0c7cdaa0
3022c38d9069f89d3321182bd36c3612711545cb2c971ced1ed8401240d1cee1
b297852011a96ebde702697dae1f5be58f120a28d945295d34f41a753ac305a0
22497a5311be9b52cc6fcd9b0985c964fd42b19562b31b0fb313d21187f6ed2c
0a8df1e4b9c2bcd56eca81e6788d7aba60a0758ea72e77ba692fb7f2e01109d4
7f02bb1c899afd44178a4fb6963778387389a4eb1f3ba528b10a12b7a9513229
7ff6d1ab542334ffcba358178fd901c84e4dd3dbfcad1a9b449a0676105b08ec
5c8dea96246dbbc252183414bbe5417d89ba432fd53ffb6ac59780e915c7d607
2de428d26cc64ac4d37672586a06f100412d9534c01daaeb10f6f1d36c3f4427
cb0ef32d9fa5de715112db4074af652b082cf08caa91eafd2b97e071123ded1d
f4f5554c28222fee3c905c3a942b73f97bb5f3e822e18d87d2da42c728648e57
ac6ca88bf5b537c7698ea3f0577a973a383f190ce26777bf0260e2b696ce6559
47ab4a2df408865a71758dc0bd705adaa5bd3859c847fd787f4cd1c7f6094b96
f9119a6a91f70765613b94650b2e48739f71c621b93ae4b8ba9b29f8a74aa9c2
9d59ae0e5c9dc8b6c5a9fdb60125a1f0131a302dc733c2de2d4fc83bcac64698
9755c6f9645ff2169839cf2b9ce530052c9fb5582607767b119d8563a0c3e2bf
8fd4e679e2d5eac28cf8a5f52fb8c234d49e2f35bef893c9c825a07bc4718751
844cbe2108daa051a320fa6bc2daf540f6bcd648ceaa2c9a58b6e692850c58ab
b4c071995ed102dcf840450f62b91aeef32afe36fac009ddb745c56d48807791
07fa656b395011f2f1d7eafe933303afa2cb5740073cf6650359c73ce8289c57
374ed4d02f11468f74e144744469cbaa59975650a702d3205af6f8b3a9891c4d
5e265cefb299da1f90d16ae363cf29496c578a38e7dc462e12aa4b4b36b8b7da
cde8f75bb522c7cc3ef93722758ecf076458524af85ac689712496db177b7746
bd198a202bbb128905074ae765592f4bb91b18e78e89b6e03d7474036cb6cbde
9dd4de8913a82a72d8537f49cdd381cc1b85504063d62fbdef60f89c08dc0ceb
3fd5f621ea2ab7d0907a15da6c4daef26c5b78cf1ea2c924f3c131a37cd97acb
7642722cbaef43d58dd83ef1c2a7a1cc1fd1ae63102486b3a73f74bc433c330f
6f5ac633cb63af10102fdfc7fa6b49f303115ec616b21a18639df55814e5e231
2232931731ef4ba4da7b1d764119c6143e553b5a36102afcdbece56b074d00aa
47ffd5a3224c4b6ca23e4cbc946d4fefabe0f96a21f5ced83f70676285069fd5
3d163a122b5ea59294d2d2e80b6a173def238fc3db023de8bf1b64955b731c12
3674080fbb84dcaad076d30fb0f3b9a8e642cc0221328954e79d06df8fc1a91f
119eb7e1fd5f571da044e5f16b34e19155dd4b27855ea0131c535eb597be6962
706894f8c3101a92babbb2b4fac50a1597de50577dd67a18c9d5df75f83a2508
5b75be7b07d837066d2277841847f9e85498d9d45602d5eb2e016d267be0514b
fdc17880620ddca2ad6cf48b73a25bab977648c1d632c662bc802a50bf32514d
5f4cdae45ab1c8615652792dad955a68280de21916ff2d84d063669893d29824
7aa31e28d1c7fb8941d535acf2259a62b9ec2643577a5403f2ab98e3f91f6eb0
6d82e682c494d0d336be97624240d2bd30a7cdda683d36acecc51bed533f2b9c
384a1f3841624dd727405ca7e4511a27482863a5e062fe16c9e81f23b4116195
57a0009fcdbc5870fcb68f771144111f4a6375f032f6eeaf04f27d44b70cbbd6
d1e85def9a961e2b787e94ff2d5fbf2c90f0d2732e8a3b1fcfbf63bcf7c20128
c1b87f8fa463164ca7efbfb5c0b2c59e88005d0f946b5dcfdaa02de930863db1
```

6f545f9fb21855a1f9f0b564a4751ec01a49c79cbb21f82f57db63ac59b531aa
f2f39bebb0417c1757b19a20864784a6af3a4ce2f73102541f3a20bace903363
ac9afd494c9bf7c612f0df9508f1dde26ed6a792a5927e119eb22b71323c6fe7
942608176a92b7150dfb2116816ca345f9965f3b8fdb70c1e85855137d81f433
878bc2cc983b139cbf92455d4b60fccf6a20fb5a642ce1c2db9724816b78cd3c
9b98f72d52db1cc9630ced00b2629254f4f364aff1428d9b2cf7a854405b12ae
5b4329a2c621f687035a9c707051b1350179c5ca5c2faaefbf81649019e4d384

Network IOCs:

138[.]68[.]45[.]190
157[.]245[.]182[.]3
159[.]203[.]89[.]50
165[.]22[.]121[.]199
192[.]119[.]81[.]34
159[.]89[.]238[.]116
142[.]93[.]134[.]89
45[.]55[.]44[.]210
134[.]209[.]85[.]199
205[.]185[.]118[.]143
185[.]144[.]157[.]252
165[.]22[.]101[.]15
145[.]239[.]38[.]111
149[.]56[.]142[.]196
193[.]56[.]28[.]103
2[.]56[.]152[.]241
data[.]rel[.]ro
172[.]105[.]67[.]236
185[.]130[.]56[.]95
134[.]209[.]192[.]96
192[.]119[.]110[.]60
185[.]227[.]108[.]37
46[.]101[.]140[.]202
159[.]203[.]56[.]48
23[.]254[.]230[.]120
144[.]217[.]12[.]61
198[.]98[.]50[.]97
165[.]22[.]62[.]79
108[.]170[.]53[.]100
192[.]119[.]110[.]130
172[.]105[.]91[.]79
159[.]89[.]161[.]163
209[.]141[.]39[.]101
157[.]230[.]191[.]220
157[.]230[.]104[.]88
136[.]244[.]109[.]127
149[.]28[.]238[.]68
45[.]95[.]147[.]89
159[.]89[.]131[.]203
134[.]209[.]89[.]79
68[.]183[.]236[.]65
191[.]96[.]25[.]217
185[.]112[.]249[.]39
blaskjar[.]xyz
79[.]143[.]25[.]235
134[.]209[.]219[.]109
173[.]232[.]146[.]145
34[.]77[.]200[.]86
MIPS[.]stubs
167[.]172[.]253[.]57
167[.]172[.]253[.]234

Reference: CISCO Talos Intelligence

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

This document is distributed as TLP:GREEN. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430