

Forum:[Hack Forums](#)

Thread: [Methods for infecting bots?](#)

richmitchman - December 10, 2021, 7:32 pm

Haven't been in the scene for a while, but I remember back around 2017 people would be using LRAB/zmap, and python scanners to find vulns and load them in a qBot or IRC net. More advanced methods were router exploits and telnets.

I've tried using an old python scanner and some IP ranges to test ssh passwords like admin:1234 and root:root but have not picked up on a single vulnerable machine (probably because of all the bot killers). Do computers with default ssh passwords still exist? What are the new methods of scanning?

NotKover - December 10, 2021, 8:06 pm

(Dec 10, 2021 08:32 PM)richmitchman Wrote: [\[CITE\]](#) Haven't been in the scene for a while, but I remember back around 2017 people would be using LRAB/zmap, and python scanners to find vulns and load them in a qBot or IRC net. More advanced methods were router exploits and telnets.

I've tried using an old python scanner and some IP ranges to test ssh passwords like admin:1234 and root:root but have not picked up on a single vulnerable machine (probably because of all the bot killers). Do computers with default ssh passwords still exist? What are the new methods of scanning?

A lot of things have happened since then but people gained a iq and had it when they infected to just change the creds and since mirai people stopped using basic creds like that and yes i suppose there are probably devices with basic creds but a lot of people do have killers and or lockers keeping the devices

richmitchman - December 11, 2021, 1:00 am

(Dec 10, 2021 09:06 PM)NotKover Wrote: [\[CITE\]](#) A lot of things have happened since then but people gained a iq and had it when they infected to just change the creds and since mirai people stopped using basic creds like that and yes i suppose there are probably devices with basic creds but a lot of people do have killers and or lockers keeping the devices

Do you know of conventional methods used to infect bots?

NotKover - December 11, 2021, 4:35 pm

(Dec 11, 2021 02:00 AM)richmitchman Wrote: [\[CITE\]](#) Do you know of conventional methods used to infect bots?

You can find CVEs for rce(remote command execution just incase you dont know the meaning) for IoT devices and you can write a loader for it if you know how etc

richmitchman - December 11, 2021, 8:45 pm

(Dec 11, 2021 05:35 PM)NotKover Wrote: [\[CITE\]](#) You can find CVEs for rce(remote command execution just incase you dont know the meaning) for IoT devices and you can write a loader for it if you know how etc

Wow, looks like nets are not for the lazy anymore. Will definitely look into this though. Thx

Young Sosa - December 12, 2021, 3:11 am

(Dec 11, 2021 09:45 PM)richmitchman Wrote: [\[CITE\]](#) Wow, looks like nets are not for the lazy anymore. Will definitely look into this though. Thx

never been a job for lazy people boy

NotKover - December 12, 2021, 12:02 pm

(Dec 12, 2021 04:11 AM)Young Sosa Wrote: [\[CITE\]](#) never been a job for lazy people boy
anna, vamp, and zeta say otherwise but you can't blame them since a large chunk of devices used
the utmost basic creds back then

Young Sosa - December 13, 2021, 2:30 am

(Dec 12, 2021 01:02 PM)NotKover Wrote: [\[CITE\]](#) anna, vamp, and zeta say otherwise but you can't
blame them since a large chunk of devices used the utmost basic creds back then
Maybe they never had to work with HTTP botnets ...

wyvn - December 13, 2021, 2:49 am

I recently came up with a spreading method thats fairly unique, and i believe could be pretty
effective.

hmu if u wanna work on testing it with me

richmitchman - December 13, 2021, 12:19 pm

(Dec 13, 2021 03:49 AM)0xj4y Wrote: [\[CITE\]](#) I recently came up with a spreading method thats fairly
unique, and i believe could be pretty effective.

hmu if u wanna work on testing it with me

Couldn't PM you because you reached some sort of limit. My discord is Noodles#7731. Shoot me a
friend request and we can chat.

(Dec 12, 2021 04:11 AM)Young Sosa Wrote: [\[CITE\]](#) never been a job for lazy people boy
It once was. qBots and IRCs were so easy to set up and all you had to do was scan on your favorite
ip ranges with basic creds and u can get a net near 1k bots.

wyvn - December 13, 2021, 4:28 pm

(Dec 13, 2021 01:19 PM)richmitchman Wrote: [\[CITE\]](#) Couldn't PM you because you reached some
sort of limit. My discord is Noodles#7731. Shoot me a friend request and we can chat.

It once was. qBots and IRCs were so easy to set up and all you had to do was scan on your favorite
ip ranges with basic creds and u can get a net near 1k bots.

added, though you should connect your discord to the forums if ur gonna post it on here, its a
requirement

gemini220 - December 13, 2021, 6:05 pm

RCE exploits are quite common, i prefer using nmap for the version scan which the versions, then
check for public exploits. If there are no exploits, i get the fuzzers out. Then once you have a nice
collection of similar devices say dlink routers, you can then generate a payload such as kaitan or
mirai (i have private version) or even recompile nc into say mips. Then you can use that as proxy,
portscanner, or remove shell, i prefer meterpreter or kaitan personally its less hassle. You can then
create a script to take that common exploit group and infect them all at once with your payload. TBH
i know people used to do this, but i dont know why people STOPPED. Another way is through XSS
and spamming which pretty much gets the same results.