FortiGuard Labs Research

Affected Platforms: Linux Impacted Users: Any organization Impact: Remote attackers gain control of the vulnerable systems Severity Level: Critical

Between February and March 2022, our FortiGuard Labs team observed that the Beastmode (aka B3astmode) Mirai-based DDoS campaign has aggressively updated its arsenal of exploits. Five new exploits were added within a month, with three targeting various models of TOTOLINK routers.

This inclusion of TOTOLINK exploits is especially noteworthy as they were added just a week after the exploit codes were published on GitHub. We previously reported on the MANGA campaign, which similarly adopted exploit code within weeks of their release.

By rapidly adopting newly released exploit code, threat actors can potentially infect vulnerable devices and expand their botnets before patches are applied to fix these vulnerabilities.

TOTOLINK has already released updated firmware for affected models and users are strongly encouraged to update their devices.

This post details how this threat leverages these vulnerabilities to control affected devices, and ways to protect users from these attacks.

Exploiting New Vulnerabilities

The Beastmode campaign derives its name from filenames and URLs used for its binary samples (Figure 1), as well as a unique HTTP User-Agent header "b3astmode" (Figure 2) within the exploit requests. Binary samples are based on the publicly available source code of the Mirai botnet.

Figure 1. Honeypot log excerpt displaying usage of “beastmode” and “b3astmode” in filenames and URLs

Like most DDOS botnets, aside from brute-forcing credentials, Beastmode employs a variety of exploits to infect more devices, as listed below.

CVE-2022-26210 targets TOTOLINK A800R, A810R, A830R, A950RG, A3000RU, and A3100R (Figure 2).

Figure 2. CVE-2022-26210 exploit request

CVE-2022-26186 targets TOTOLINK N600R and A7100RU (Figure 3).

Figure 3. CVE-2022-26186 exploit request

CVE-2022-25075/25076/25077/25078/25079/25080/25081/25082/25083/25084 are a family of similar vulnerabilities targeting TOTOLINK A810R, A830R, A860R, A950RG, A3100R, A3600R, T6, and T10 routers. (Figure 4).

Interestingly, the samples caught on 20 Feb 2022 contained a typo in the URL, where “downloadFile.cgi” was used instead of “downloadFlile.cgi” used by the devices. This had been fixed in samples captured three days later, suggesting active development and operation of this campaign.

Figure 4. CVE-2022-25075 exploit with the correct request

Apart from TOTOLINK products, this campaign also targets discontinued D-Link products (DIR-810L, DIR-820L/LW, DIR-826L, DIR-830L and DIR-836L) via CVE-2021-45382 (Figure 5). Note that updated firmware is not available as these products have reached their end of life/support cycles.

Figure 5. CVE-2021-45382 exploit request

It is interesting to note that this campaign also attempts to exploit CVE-2021-4045 (Figure 6), a vulnerability for the TP-Link Tapo C200 IP camera, which we have not observed in other Mirai-based campaigns. While the current implementation of the exploit is incorrect, device owners should still update their camera firmware to fix this vulnerability.

Figure 6. CVE-2021-4045 exploit request

A couple of older vulnerabilities were also found in the samples analyzed by FortiGuard Labs researchers, namely CVE-2017-17215 (Figure 7) targeting Huawei HG532 routers, and CVE-2016-5674 (Figure 8) targeting NUUO NVRmini2, NVRsolo, Crystal Devices, and NETGEAR ReadyNAS Surveillance products.

Figure 7. CVE-2017-17215 exploit request

Figure 8. CVE-2016-5674 exploit request

While affecting a variety of products, these vulnerabilities are all similar in that they allow threat actors to inject commands to be executed after successful exploitation. This usually involves using the wget command to download shell scripts to infect the device with Beastmode.

In addition, exploits lead to slightly different shell scripts. Snippets of the scripts downloaded from the successful exploitation of CVE-2021-45382, CVE-2022-26186, and CVE-2022-25075, respectively are shown below (Figure 9).

Figure 9. Executing Beastmode with different filenames and parameters

As shown in the above figure, each script downloads the same file to different filenames but is executed with different parameters.

For instance, successful exploitation of CVE-2021-45382, a vulnerability involving a function named "DDNS" within D-Link router firmware, leads to the download and execution (Figure 5) of the shell script "ddns.sh". Then, as shown in Figure 9, the script then downloads the Beastmode binary, which is saved as "ddns" and executed with the "ddns.exploit" parameter. The parameter (highlighted in blue) allows the infected device to register itself as part of the "ddns.exploit" sub-group within the botnet. It could then be used by the botnet operators to assess the viability of specific exploits by measuring the number of bots or simply for ease of management.

Once devices are infected by Beastmode, the botnet can be used by its operators to perform a variety of DDoS attacks commonly found in other Mirai-based botnets, including:

- attack_app_http
- attack_tcp_ack
- attack_tcp_syn
- attack_udp_plain
- attack_udp_vse
- attack_udp_ovhhex
- attack_udp_stdhex
- attack_udp_CLAMP

Conclusion

Even though the original Mirai author was arrested in fall 2018, this article highlights how threat actors, such as those behind the Beastmode campaign, continue to rapidly incorporate newly published exploit code to infect unpatched devices using the Mirai malware.

By continuously monitoring the evolving threat landscape, FortiGuard Labs researchers identify new vulnerabilities exploited by Mirai variants and malware targeting IoT devices to bring greater awareness to such threats and better secure our customers' networks.

Fortinet Protections

Fortinet customers are protected by the following:

- The following generic FortiGuard IPS signatures detect exploitation attempts from Beastmode and other Mirai-based botnets:
  - Mirai.Botnet
  - HTTP.Unix.Shell.IFS.Remote.Code.Execution
- FortiGuard Labs also provides IPS signatures against the following vulnerabilities.
  - CVE-2017-17215 - Huawei.HG532.Remote.Code.Execution
  - CVE-2016-5674 - NUUO.Surveillance.Application.UNAUTH.Remote.Code.Execution
- The FortiGuard Web Filtering Service blocks downloaded URLs and identified C2s.
- The FortiGuard AntiVirus service detects and blocks this threat as Linux/Mirai and ELF/Mirai

FortiGuard IP Reputation & Anti-Botnet Security Service proactively blocks these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

IOCs

Download URLs

http://195.133.18[.]119/beastmode/b3astmode.86_64

http://195.133.18[.]119/beastmode/b3astmode.arm4

http://195.133.18[.]119/beastmode/b3astmode.arm5

http://195.133.18[.]119/beastmode/b3astmode.arm6

http://195.133.18[.]119/beastmode/b3astmode.arm7

http://195.133.18[.]119/beastmode/b3astmode.m68k

http://195.133.18[.]119/beastmode/b3astmode.mips

http://195.133.18[.]119/beastmode/b3astmode.mpsl

http://195.133.18[.]119/beastmode/b3astmode.ppc

http://195.133.18[.]119/beastmode/b3astmode.sh4

http://195.133.18[.]119/beastmode/b3astmode.x86

C2 IPs

195.133.18[.]119

136.144.41[.]69

Samples (SHA256)

04a50c409a30cdd53036c490534ee7859b828f2b9a9dd779c6b0112b88b74708

0ca74024f5b389fcfa5ee545c8a7842316c78fc53d4a9e94c34d556459a58877

0d442f4327ddd254dbb2a9a243d9317313e44d4f6a6078ea1139ddd945c3f272

14726d501dd489e8228af9580b4369819efb3101f6128df1a1ab0fcc8d96e797

18cefe4333f5f1165c1275c956c8ae717d53818b2c5b2372144fb87d6687f0d8

36a85f2704f77d7e11976541f3d77774109461e1baae984beb83064c2e34239a

3d0a119b68044b841128e451d80ee41d8be9cc61f9ff9a01c3db7d3271e15655

5adfd18422a37a40e6c7626b27d425a4c5a6ca45ecbc8becd690b8533d9d6c7c

635569c7612278d730cb87879843de03d1ea0df4e1c70262ab50659780eace3b

676b2aa6839606d49bbd2f29487e4c218e7d14dd1a9b870edcabdd11fcab9cf7

9c88fa218af7fb72188a0262b3a29008fedcf3d434b90e8fa578ac8f250f5025

a21aa45045c0d4b0d785891b8be57496d62bc2396d01c24a34b40f3e2227ef07

a5cbe89bf1f3121eb2012e3c5bb5c237c613b8b615384be0f1cc92817a2f1efe

a6a7e46bd0e9ec67a1adec64af8fddee18ce019f731ee9cbf8341b35b2519dd9

b573f4d58b1fe6309b90611dd1d1030d7a3d1eb8ddb18de6dc58eefa876820fd

be3248d97653e8f97cb8f69af260f03b19965489478211a5565b786e9f5d3c02

ca8980cb3bd286e41950d78555fd070eaf2d3bebf2751cb0d12a3eff0a41f829

cd48523a6dced4054cce051d4dd8c06268cee375e56afbf59d724faa91c3e766

d799ae8a017e76d22f1f35f271ebae9168b7712dce0ce86753edabd6e5f4f0d6

ded30dbc39e310ebbc17a9667a14e7f0f2e08999bfc5ebd4eae5c1840b82860a

e7db388460d4e1f8d740018e6012af0ad785d3876a35c924db1f4982d7902db3

e85c3d3ed49d44b1ec3af89d730e129d68a32212e911e6431f405e201597f6ed

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.