Severity

Medium

Analysis Summary

Enemybot is a new and emerging botnet that has been targeting router vulnerabilities to infect devices. The botnet resembles and borrows source codes from Mirai Botnet and Gafgyt_tQor. Enemybot also connects to CnC servers hosted on the Tor network, which makes its takedown more complicated. The malware first infects multiple environments to infect further devices. Enemybot also targets desktop/server architectures such as x64, including Darwin (macOS), and BSD.

Enemybot targets the following architectures:

- arm
- arm5
- arm64
- arm7
- bsd
- darwin
- i586
- i686
- m68k
- mips
- mpsl
- ppc
- ppc-440fp
- sh4
- spc
- x64
- x86

Impact

- Server Outage
- Data Loss
- Website Downtime
- DDoS

Indicators of Compromise

MD5

- 504e645c12057db465d775e3c874a3ae
- 4cc80fa5bd2f712a4639aa5cb42e441c
- 3126475d4ffc5b24ce516675d11aa58d
- 77b54b3bb68607eb862942826dc66883
- 6099c242dce7e173df17cc93eeb08227
- 03cbc46499e34a01cd9fc483a445bd1c
- e67d19e849ee997460422bb067daf8de
- 6f115796421bcf5937b6b834b2b6a1bc
- 890a76e5e460b53e1361f2e313ce6b0b

SHA-256

- 5260b9a859d936c5b8e0dd81c0238de136d1159e41f0b148f86e2555cf4a4e38
- bf2f2eb08489552d46b8f50fb07073433f4af94e1215865c48d45f795f96342f
- adb51a8d112590a6fdd02ac8d812b837bbe0fcdd762dba6bbba0bd0b538f9aef
- 373b43345a7e4a6b1d5a6d568a8f6a38906760ea761eacd51a11c164393e4bad
- b56655c3c9eed7cd4bce98eeebdcead8daa75a33498ad4f287c753ecc9554aca
- cebd50b3a72a314c935b426c0e6b30ec08e0e0cb53e474efffb66f0907309243
- 73e929575afc04758a23c027ebe4f60ab5c4ba0ab7fa8756b27ed71548302009
- 33d282c6bccf608d4fbf3a211879759019741c1b822c6cea56c6f479be598367
- 80f264d7b45a52bd000165f3f3b0fdc0e405f3f128a60a9ec6f085bfba114971
- 9acf649b74f4aae43a2db90b8d39a7cd39bf6b82c995da7a1ffa6f23c3549b14

SHA-1

- a7b7931f76bc86bf625e3afaf61bbfdcbc322023
- a902ca63aabd82fb52a7f40fa9657629f0163fb3
- 08c314b9cfdbe2d1d3c94a1a95b6c2625f1ae340
- 8999c3c84bdc6e75f0c1f7d24180afa0f7c81b6a
- 67e3b9974a094772e6f4902d02a9fe123a8c99dc
- 66e65e506c025051883fb3075dce7e6d928d98aa
- 66800f443681848b1c4d22c8339c78d7d96e8fef
- e70c4238a17bbbe6d92242f760ee9e19d46bfb92
- 9cb53c8b4c52369931a37b28143b93c990e17375

URL

- http[:]//198[.]12[.]116[.]254/folder/dnsamp[.]txt
- http[:]//198[.]12[.]116[.]254/folder/enemybotarm
- http[:]//198[.]12[.]116[.]254/folder/enemybotarm5
- http[:]//198[.]12[.]116[.]254/folder/enemybotarm64
- http[:]//198[.]12[.]116[.]254/folder/enemybotarm7
- http[:]//198[.]12[.]116[.]254/folder/enemybotbsd
- http[:]//198[.]12[.]116[.]254/folder/enemybotdarwin
- http[:]//198[.]12[.]116[.]254/folder/enemyboti586
- http[:]//198[.]12[.]116[.]254/folder/enemyboti686
- http[:]//198[.]12[.]116[.]254/folder/enemybotm68k
- http[:]//198[.]12[.]116[.]254/folder/enemybotmips
- http[:]//198[.]12[.]116[.]254/folder/enemybotmpsl
- http[:]//198[.]12[.]116[.]254/folder/enemybotppc
- http[:]//198[.]12[.]116[.]254/folder/enemybotppc-440fp
- http[:]//198[.]12[.]116[.]254/folder/enemybotsh4
- http[:]//198[.]12[.]116[.]254/folder/enemybotspc
- http[:]//198[.]12[.]116[.]254/folder/enemybotx64
- http[:]//198[.]12[.]116[.]254/folder/enemybotx86
- http[:]//198[.]12[.]116[.]254/folder/enemybotx64
- http[:]//198[.]12[.]116[.]254/update[.]sh

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.