Severity

High

Analysis Summary

A new Mirai variant is making the rounds called mirai_pteamirai. The botnet exploits a vulnerability in KGUARD DVR to spread within an environment. The vulnerability exists in the 2016 firmware version and is fixed in any version after the 2017 release. This botnet is active and used to cause DDoS conditions.

Impact

- Server Outage
- Data Loss
- Website Downtime

Indicators of Compromise

MD5

- 24c3d3efceebba5a7a1cb2b46256c88a
- fd8dc4cebede5d84460bb2fc01212812
- cf6f314eddd6da908a8008c2db3584fd
- c64778b0311703f81641c42a0fedb899
- 5539af6b6a7c3c26e920a767eef6e48e
- f9f60e94dd2e99fa7ce089c5accd8a0e
- fc372ca42528c00502395cf26b12a10e
- 4b4cc9484757048e602324e42c78b2a3
- a3447143f670fda0841d6fb05ca3f0a5
- 942239c620ce80223f63af100293d811
- f7cd2915ddfeb916b63e229cc40a13f5
- 214093991deaa35eb76326d3ef1c7aa1
- 8b52192b1a4e865d1ec09df05b3e14fd

SHA-256

- 051c2c86d136052e51dbe09fe7b62e860462b438afd25d2472b9f6625b24b488
- 9fe4adb801e9914577072dc13e3127a25122e16930c4dcf7216a233952a23ea5
- 81edfa9ea6cb9902b03f92161a09aaf93a73a5bb1ca67ca841fb2e9ab8c0b3a3
- 686cdfbe5d32ba22e1cbfd5c1d156b120b8eff2b106f8d3c9723cab66829d64d
- e6706ab5e5433ac512e3b1908d663cae9a758c187ea8320716effc176749da56
- 79d0826aece8c61b6a7935a07a84ad8fd517311c11020e04a363d0d5463cc8be
- ff4acb86909ec87667ee082718bfabb593d809ed8d3dcd966931867e0d070a7c
- 41c9894a844a1fe861dc48e4262ceb518128156ff194cb504a537e140fc29268
- bba1585dfefe5dce88d436500500a77e8781df34b3424dd1f37090f441993c9f
- 4f7f52c652528d607b418a9541e08309168d18845a66a6a6f61b8c96ef6db456
- c59ba2dfc6a5c3be0e3c285b950438982251ad5e00b408efb2087ecb8b736818
- ea413ff622f561ec59167df919fdd76ef326be1095236ae0ea6a6f96a61a44db
- c6b7fa40a007fd459373371a2a9b593cf8c30eb7cefaabeb96b9b4902df3713d

SHA-1

- 92bab3e82ab273c25d98fccfd904b88bdf35e725

- 316f5d8302345cb2f4ae4d152363b0b7973c1ae2
- 0bd7968c2df1b3e0af902732dad399d03ccda193
- dad54d3adbb68c4cecb12e019e0cdd84943776cb
- 4022a1f0623202cb63ef3ca7ddef9b3ee6732816
- a9abf92a5d25d885c8f558aa1e5e946723785b75
- 4b190eb3df8736a1bb28c3c316d6c0a67abc1868
- 7953b559b31eaf5da8464f89b7d246baa0a74fde
- 65dcdea7e6038971d7fd49b3f2afef3970838532
- 440a3d3d0d58ea95a8fd3a092719de65a032b058
- 2c431e3f80c1e0fb2d5af5627deb901025968ee3
- d9e3b8f030ade7d3ce133663031ec4ec70e9d450
- 82c44ffebe8eb8d35ee8ae0fe23c52ee23fdf687

Remediation

- Upgrade your operating system.
- Don’t open files and links from unknown sources.
- Install and run anti-virus scans.