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

- e327edd9399c3fcfb76a9cf366752576
- f62837836336da7663fe7d0ce6b24e5e
- 971ee762d8a7de8e90a7c3bcb1f9a690
- d79a6982eef00cf50cb890075f5893e2
- 47f1a0e81def1e439fe9be508bc98368
- 51f3b8992b2c2868d3742ba281be49f1
- f0dd77cc751a44f86bc870ea52e8e900
- 4e9c80c76d17e3e08a55a73367427c6e
- 511fb99c799c58050d4ed70d3ce078ae
- fe167d713f32f879c04bfa7eff12b556
- b4d165a48fa5906a193b865e3beabc79
- 0121822912650335336c9ab8bba4510d
- c91ca46372e619131a9ad156f828fb62
- bc4e4cdd3978f2f0b69a45be1a2eb5ec
- 05448212f673f8b32e4f1de0a94a6c0c
- 6082087e475eecba35de98db8a7d3b2b

SHA-256

- 74d4cc65ee427ec617e820c0078d8f0b0ba090d69af5ecce652b257fb0820c15
- 259c550340c203c7437a108f36fa816250ee8dbe3d7c715357f7338d150511b1
- 984a7090003bb8515a2ecb03ffc6ee2da324f9e998a9291f0140c07756585e73
- 797dc6c810613db268f6d3c27c52bccbf11e353cc0445048a58c54a586d8aa96
- 281fb9f525197687b55d302676d12e7f1fb228c51d1523881211b505dd513ef4
- 0d28f687603acd7501f07d8382767519d014dca4019ac3f7a7d9e636fed63d38
- af2a0ecff71a5f23a587f10294c6c3bd5289c9e0d1a3ac0464c5a9bd91d84934
- 53a3294bc39b7eb68ee35358f531757851d4289857dcdfa7a154892a24c93b2c
- 36e4c8d60917804c3e4168b93bba35439d2e1b8eac125755e767560088de8cf1
- 1bcdf322f4adfd73d44095e7cac2077f9c3806e0ec6078c42ca220af235a7809
- 188341c46a52f0c1b42307d5b618f35d4c7626a436f5d4741643540fe562ffa4
- 103212e1da84c42ddb0a65b32ed6dbfc67b4995b7eb20ef1ed2d740fb44fe2a7
- adff7876deb3db74ed336b2386edae6a662c9f1703f99c03f0845d118abbbcb7
- 5ec4bc9aae411d9f37c7eab7157e6c3d6335d2692e33b056eb62dac678659ecf

- 046ae27f38d4c57f4ff99a648dacd8783af7d61b842380815f9b8335a37163dd
- 4d94c65efc439ebea3dd35ddc4243a8d2a3e4cfc41f6c9de64a97e35604f6669

SHA-1

- 31aa1037fd8828635a94351c21cd69e4c66eacb6
- 18b7fc55aa7136a7186ffcd5e174bf62a53333fc
- 430502c4ebc33f2faaff05ee97a859cfb835bfe3
- b8b3c0531869b29c6ec5c72b98957a25caeff54f
- 1f5f5170bc486e10d29ed10c3e49c7e851a17d51
- 26d576d2697d9ea64f31366d8be0a2a68e5ee0bb
- 90ae61e6c4ad16db3da1b85988987d727f898d20
- a4b9306df6bc1d4bd770728c1787f7d069fe6c74
- 27c790f1078817147c55f67b4bf671b0cb83ad5a
- a781c958dcadb9b3c748c8a91946701beb4e7407
- 59d183d5a254010d3680f5e5fbcee5833b0548be
- ed2dd6b4d04a42a80c06654a06a2a6109e61b42c
- fd271ba4ca17cf462ceff6198b122ea18f61d061
- e6c7d6543c206d6241aeaf69f8ba8763274e56c2
- 09daf42e200fcd9b71523e4f9926b11645aa6716
- 6c01acb6444a44bad2a48f09ca28dbe52940faf5

Remediation

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