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

- 7659d3fd8d81cfb97063e306c69f17e0
- 3f24f844fba73b88e31aafee5be5abc8
- e7f872e8ede927df4979acd31ed9d3f0
- 003dfe6f969d943a47f5ee4ecbfb180f
- 3f626303026800b4947d4baa8d18f5ab
- c797e54a254be058aa55251f2de01d23
- 63ce183770ac05da5844022a6c03008b

SHA-256

- 3c1a8f363ac2e6bb04159d461eaf51bbcffacd9570d0b0cfdb56e51f548526f9
- 0f02b01ce395d6f584d6ead6253636109d731468b551138a5c6bb16f31c66676
- 8a1bee0ace3c93e1f58a2ee3927e59b2a96321cc922a6eac768d87347990b62b
- 029517cb3575b4a47f1ba4101f35d8e9a2514c2f480afecea9df4c3436d5bce4
- d680a3f1beb976e1ca13166d314ad2bd47d40876dee05120953f427d4d0501d0
- adccb2303c8b248209744ef043cfd8082a73a7b73fd7f68848d6af605d789dac
- 1350c788fd15931f25843ccc6b6c9c91ce3e2c5c4d64b948841da0fe0cdaa305

SHA-1

- a881f27a060c4c397052d11cc87f9e86b2f9b89b
- 6e09f1bfc6b9c41b769224face67b29ad65d93aa
- 22aaab23e97c69a92a45876ac79535a84d16f844
- 22c713762968b3d19a98ad3c4a47b393283aea6a
- a3c77cc0fe116a37b7eb464f0b832fa7f777f3a2
- a258639e0e1e4c636dfe7c78a8e7cecf87178458
- 17745e279c002bb99f3824e02a6b3a05d71251dd

Remediation

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