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

- 9381a7df8ff1b8e688dd371e53e261fb
- f7b3724458a1b5124c208a963ec5fbfa
- a9cfbdbbf22f91366b77827c7f2d679d
- f72cd2bc6ba0c9ae45ca3b3ee355ba16
- 5ad94fd583fdc0eee9c86f8f68c4c7dc
- 63fb938f90494efe645b9421be38b7b0
- 0c616a850710fd085321d2fd900a3a37
- 0e5254a3467c7acd8e0f5a969c5ecf80

SHA-256

- 43ff650dc00cf1b52d283df18fa95fed9375aa29fe65fa5abef40ce2191f14b8
- 950299f1a1f2a6ef9a6f31f78b6fb796dfb6a84b3f81d6c9b1f7aa82783f8e27
- 930473d7ae73220df6f007bd61fc943249d338e197900089d46c2121b61cb735
- d6b4a1a92ba68f9054911c62aa9670138522f408fa318dfad28cb78bf1da4a9a
- 1d6307e30b5a0f8ed44efc55894ff194584241eb692ac7bac1b1e458a49b0f2d
- a52123ac41844b4a189faba35e895ee92e2c99fd86c21e44136bad51ec9bbbfd
- 576a89f24ac7629a76d9277a54161ec76c06967f92b216de694e9ad823c29e2a
- 5b13555c5b2681219323b20da2297fe2f85b31920a6567cd429176d29d5b61b5

SHA-1

- d6103010f62caf381caf70918b2801542bdf1853
- d5dd4f5d653500a871e6cc2139d0ebe18d1e2135
- 2c4a8b0296548cec24b56afa99617054f1aa015a
- 8132e16bb8f03031b28a1f2766a16e8336f76188
- 8d33e0249c3561ea2a03061609f1db1d1353b829
- fa2c81777a9f921a6b058267ac2ab8824cc83307
- 6fd9b52acdfebe858e805037b7d82d1c61501e9e
- 3de11a6be682f785a27555d4e29b17ed50c179f0

Remediation

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