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

- 84acee860651e4f5ab842edc359d3db0
- 1718b6be79c44d7070414677447123d8
- 9252a3510f8179a9dc535c5b68c86b88
- 53a1b31433d7933a50f4d75d32306cb6
- b5ae2f82cd3633056cd5c82d86fb3c65
- 55de9038f8dd6d08aa772cda2bd54aeb
- 055e5b5094c5f0fc246843c2119f0153
- 0a602160060ffac2c9d7c1f4d55a7d3c
- f974ec99e93e9644fee4b3847dfc2cf0
- 63f9dd451f673f5a8d72ed0d332578b3
- d4e95f72002923eb8d87371b5f6958c4

SHA-256

- f8be6d645a78c1591be42a6a9f44e2d06d4fa45814f1c99390bd8e07fedbef76
- f8b0489b58ce8a8dfa43f96eb31d9b65ac13c8a81c606044b8ae4b6bce4539bb
- 76ef2c0ba9be33ecb46c7a15f9a98c77043ad1ee0b052e38f633ac806092b836
- 23354c49f80f700bc33ec13bf5850fec544abc0770357d4bebad61c8a9e045f0
- d632e889ef214838a0177bd1649ff59adce73e2972034944ab052e2a439e5861
- 42393a476841cb9d33308458914c833824ed1934cc6298e1d7c634ce41ec163d
- e0047ab40441af90ec304e1f0132c3aa1369ca2a0871a8fe76d116e32d050fa6
- cf2856a7b559c51797730452e9cd8e7152b52407e51a114ed354b331400a0425
- d3fc4ecd564da9f669f4474cee6dbede40fba31f0de0a76a8edf237fb18e5a9a
- 0ac6c3947eb976ff52d39c6bb052f136533a8a6f34c8ccfdc836d449406188c9
- a943200b69baf622191a5d898a1b7cafbac713e2c1107cb025fbfcb3ba924d93

SHA-1

- f21cdde8dd1974d94dea715c954e677d24d766ea
- 7ec463cd24c42ed31e5acd03dc65328981e1394b
- 756579a8fc7fb2d1ffba103eb1c127708975ab58
- e9ffac9b56e9fb2f60bd2f31a9739addfe3742e0
- 61433002f1737942dfd7a21e71d5405d5fb7b53e

- f65b10a85485d608d17f2d371eef0644a5e03ffb
- 4b5ffe9a44ff9348e736fc5dd8df1554fc5fea01
- 6c5048ccadd98bfc2bc31238312c81d970f6d860
- 7163ce4bfde11fd39f7e7b4ad6f98d4de0ee77f2
- 33ffcc9d04ab07703c3af02e4889f0d28cf8cfe2
- 96ce7ec300185341aa127006798a01380d513626

Remediation

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