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

- 57c5d195579ddd19d76388c972550c06
- 92ff1b5328e88d3483480f3c478e06ac
- d14bd7064868b58cb72461cfc200f7b6
- 24ed66ec70b34b9907e780093cdbacd5
- 52be0ebdd6fb3157a8ceeb6a0f7c0bc9
- f2b50352b6acb3ae03269d7ed7f72a5b
- 506f1d8619eb23597c686852ee693831
- 7aca73894c3ed1aa8c1a70c4d44c7e89
- 5f0f5ef9e076d775f6b6f1d4aaad6a4b
- d59fa088cc4a453e5985a6e580daab90

SHA-256

- 6c86edb815741688488f2da741b332587912372334a4f053579397b0d40458a2
- bf3dc5a33e0c1f983f666a9bd524a99030eb5c943f645d9d3725b30d05087e77
- 57469ff3eabef501cf41f6aab685f5d1c7e2ff8520b8414a58e34ffe0b346287
- b863bb04b9770ac70b815ce492d9cfc7afff671fced667acecbf80c354b83caa
- 4be86ce1adf8561a0ad43680f93f9363f27e7a698ae2b5de51b0be30be6588e0
- bd0d99d5958c013bd33398486ee8620c75e8020d009e85d75c22aa99d9584e9c
- a20d6b84bd747b41116c176b4394be4627347d307aec7bbc68fa2f810d1aa6ee
- d4f8ffe4443bd8afb05024ceef99c30ac4e5ab2c54e6e75c64808d9d1ec888b0
- b19397cf9ae08b8ab6b104dc8182318565f81f90f6b73bd51109aabd6859f64c
- b25e93366519f767691dc74ad83124ff5580d047ded829f4ae890ae71288190f

SHA-1

- c87b025c011fc226e3ea6ea4b7ad32401a976f88
- 142d3677c46dfbfa79fac218c47d767b9641250a
- e319b916f726f3dd37ede584d62d6cc7406db9c9
- 2bc4bdfb993869952907c49edefa97cd25eac16c
- b60bbe4c2710fc1948be3ae28e42cab5e704fd78
- 84e1a6aa37adc0a4668768d704487278f8ec4507
- 0787084015610809be82dde171c7595a045968ac

- cf9a84794cda2a5ca65946fbe0eb7c646dd74691
- 1f3364ea3f74ec8a01ec74c9bdc784ae22db00bd
- a49be9a022580238ecb8ede73e56a01c57986710

Remediation

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