## 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

- 4427918fc0d6fbdc65c0c4e120d74d9c
- 5b04f248b140c4b6b8108c67994f9b40
- 1fac1ff9dcf110718f0acc94e64c2872
- 58b1f25c7e239a810efa3e47e23eb7fd
- bc7b5860c0d8d05f7301951dc785aea3
- cccba430c0273cf92cb3bccc5f9d85d5
- 39836b3fd85ea38063ad43688000b82e
- 95cb523dd81dfde6a1351f6ed478599e
- c66bf1471472e2be693cd2ecbe7a7a21
- b36b818086012a4d655ef2860f5f7cfa
- 2b9c587bc73ed5c099bd6bfe04611443
- 6ba72f6988b09cb8bf2eeb8284b74133
- 8197a50e4233ca2a2d282ad486299799
- ad1991b615d9bf04dc6260c9653cf5e8
- 3476ada9e20f015c82db2c2bc319490b
- 855eb4e41244293e69e88b93b6ffca3b

### SHA-256

- 3d16ef9262005ad57df6fcf5ae69b88bc4899ad56d26f652a4eec28af94538e3
- 3869e9513162159412bc626bb076a9e263726fc04b0ec5781bed490cca536e8d
- 56abfe3f69a30a0a3bb55213f6cc074704bd9de47ce5afeb5e5d1dc0900346ae
- 5e466a9ae582b87991946217cb566ce87f4b81215f78f07880ec37f1da83ac95
- 479e29641beded9463f9cb125fcc35fe6d572e4503937f061be95661bc6ea394
- 314d102eb54c745478af7061cadd13eb85dd98d33ce9639e42da5103f7623f9d
- 15d29ecafd715e65fb413f84a25f4ff3f8e01f81d473283be2880fe8151baa7c
- ba13a185a59bf30ba4f2819d261862a8ac386f8c4a92d648c5892120ecb69e6e
- 4f18e25803b72fac2a58f621d5d8024b9a717b728432d9f4edccd43c78d0d27d
- 909fea0549945d6a0d6bf95ed647fb6959a28c730742b0ffcf84cd621068e1c6
- 16e726706204e3b471ba75438e1ad4b6fdf8f53e15cba631fddea25b965bb47b
- 36d07b9f5fddcd57aa7f4441a2f6d7f8d18f8626999eaf5571c5878ad6a66dc1

- 652a26095aea955a8d492c3da6e18cc007bc675284f46681686962092f6ebc0c

- d4a85def79f2ed38cee0dee47822123eda8967178dce2b9777ecfb64d9158427
- a5e7914940f9ed0b3eb2368dfbca87a5749aa62174a69362a73cd2d18487c9b0
- 327195c89ff0279167fd0ebad71f10a28b4c74aca507120acb897a199882e859

SHA-1

- 4b3c6e067c1bda640ea0a36b2745f6673e219f02
- 675ba3c8355b4aa67812ecb7fb4c9babd9359942
- f22bfdcd12e553896c63f9cc86a9589f5490dab4
- 7aae823b8088100fa97b8d7dd24172948006f033
- f287ec4497e42c4dfa102cb2507634b1ca6c552b
- 7c9648fb6ed37a897dad8ef775b544a1d796b4d7
- 9f70afdfc8bc4f84efbafc24c51f94bc9c1d5b18
- 586780f3467c52eb8da918f9c5d60bacddb66309
- 28ecc9b0cdc5321bb8c9945227ad170229956cfa
- a97a583dc1228d60ba4f5dce4bc274fd9c321082
- fd4d255ff566a6de371c0072318c83ff7cac9606
- 02f4e3f238a2125eb5da4133b67a598a25f8fe09
- 2223d876253342966ce0c5793c01b12c503c2a49
- 3128b3aa24880a075076c8163fcb3aaf375e9f52
- 8521816fa69ee25bc70a4dad296754dcd984da9c
- be89eb3e5479c5060897ec0714a57a24bc51a253

## Remediation

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