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

- e55082237c555b2f3f1cc55eca27a8fe
- b8c64cdc287d8f3ea03e3f126f17267a
- 698efc7ffa5504ed7c904df71a28bd59
- 6d108b7609a967122b15b5f1dbde7848
- f22f312a820147ec7b86002dba37cbaa
- d8a5f6781a0f59c077b20eae101c1079
- 3b3e313747f5c30f755b0d1e56dd1967
- cae6d542f460343f208270f8ad7f8352
- cac63f9e7b1a665400b29bfd5728be88
- 2750070acaf4d1dd0e54f223e7d7b567
- f5a01bff7c228490555e8f5f1f7479e8
- b228ab5e76a86ec32c8bebe4734fe361
- 283852fc33e1e0c9b351befe5fe81450
- 7f7e7d563e29bcc248c1adb22ab6a37d
- 5075d3c1d14e3e6204b5f8ee625e32d4
- 2d78a3655b1aa0a7589ba127c30fd1f4

SHA-256

- 2f88be9d428b67b3479565cededda58dbc3883b36fd1221e1c8ea6b20162c009
- 243e7a0d5f6b804fb4aaddf23a0ee7bd6bdde8e7efc8f9778da025776649c60f
- bf2ab7698435155636ecd6008170ff933a367fe019961a84aec08efe1b2a6492
- bef9fb3b4c5d3a8895b91461ebb4afec5fbcf276399c086b97c0eda3d92da261
- eeb7c8dd754b01aea19d763f2a0fb6af43b867bce5d78961091458348e6596c4
- 37a716ace8a79981b1ff36de7eb260fba5aa921a5ed12d07b8ee129a1ab56494
- 040766c48a6856134603b191795f731b9520f074d67f987254a7db55a7e71a7a
- 202c482d83984b7331a309cb6b98e0e323629a946909a4982aac5fde5874d014
- b085cdbd00df7bcc174ce236778020dbf81311e6fd4286e64b52284e8de70fd1
- 6b2cb32f2b46f7aa21ae60af35757d8ae4e40f2bc3daf10a6b8fea3694dad4d1
- ca32543acaf69fa9f238a9944f51cd7801265f84c4bd22f0e3764f7a424f37aa
- f158dfe238e93f8d614ca1c502f16234012542094089e292c203914ab765717a
- 230a3ffa2bf3d8e6ea420076824d3e363dfb59c810587a7a0116bcf60394d545
- cbde8dcd201a9d35f3c80f1a12c31f2ea38b0c9fe92d0f60d05414d6e3e9d0b0

- f925227ec0d671ae94a90b7911f62b9447d158b092360fc2fc56404e795cc079
- 781a0b953517dba9b70a7b4aa681afeccaa3605eaa49bc0076fe69d571d898eb

SHA-1

- 49c411e5143febac5da2e43689fc116bd2c88665
- b48fb137d3ab8f3da93d126e9dc1bd7109e72086
- b1bdbc5713eec0838e26e5cd0a276bffd1819236
- a124a1232325e62892d7bef15bb7290bbf129c09
- e7237f5b5112b2680738660e57d8a1490655d9f3
- 64e0236bf78ac0401313ff50aea151b116f4aca0
- 6431b5542c8528c2a8373bd192451a2b93fdfe45
- 3e3b755b0e7503168857bd3580625e924e503ea6
- 8401c1b015f52069fd32b5a2cfe17096461b798a
- 99b674b6b02606aa202e27ee6f6b2e0ba0b13423
- b51e4fa30a3a8c7f728dba6e05f3263d112c1501
- 2ba5ae7f6adde444e0ea781549ac3a5758e61430
- 1ed3a32c83c04f3e336c225bbf92ecba06e6a2f2
- ce4217929e10d6bcb1736fe6fa001f9ad4dbe699
- d8481a792d184d77d408b249b293f97294e8379b
- d13db577c6ac6717bb1514f2aaa6d1b8e68323d5

Remediation

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