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

- 5676c7e75bc51935899c7a21d23a4393
- 179167e000aa3de75439a50c92134de8
- 7c063a02696ecb0d8aee487938425811
- 2fa159163c2dfd831da9d714879590d2
- d4d19805fddde4fa9d85fbc66e31364c
- d2f3324586d284b951982909cd201221
- 597830f6e251ad5ad58c47337d800c2a
- d3e82cf8ff40b6f7152ea94ab42c46d9
- 4d94c3c4eba7bf30fc824d9a829908ab
- 2806c54c2c6c0fd6669d1428f7a73b81
- 32157adda4cd15284b60d6885f8aa25e
- a943cde47e7bf2169ce748cf65d4f81f
- e22472bed68182de84a44953841f0237
- fb58f2b3c4818ee146de289ccb716c52
- 63a9402a6fa90a5e0f09ed89ac1a2069
- 9511316ef89f1b12254cac467f6bab2f
- 27454d780db6d8e512d96583d0b21a21
- a772ae63664a8fef2cad963e790cf5b5
- c9d6b874526ab495032b8f5fb1639d27

SHA-256

- 024963ebdf37624bc3c38604389eaf520deaf94b646dc92c47da6dd7b469ca06
- c990a0ec16258375c44fe2ffd3756313300b49f9ce56736d6bd4b847692e3933
- c92746bd03b6fc5a84c50ff7e8b5a2980b11d0078d6018ef8f193461cdf03855
- 7cc9988ca85ba065ffa5bac94df768b39cc0f73355769543a774c5338e03db6d
- d4f9b424a1639bc3c46726e4f72c259bf6b9ca33af7377490b1bb292867603e7
- 1dfd53b8143951436dfc0cac52d70416034f768c0bb992e1f637e478fe1813b1
- 141ab6882632101808a6338e0a5cfd7b031cc2b3f6e152b700afd2653298bb5e
- f89f346a6ed3ad7270750659ade1b6616ed703dc7f8d9b2296ebad64a68582c7
- eb9f74709a69189e81fa94f437cf906205c7a653ca1975331a7458a832a8ef9b
- 2b6bab37bdd7d8af99c18c1568ddcecf13122926d66017825584de67a606835e
- 912d4115122c2018f180e4e88dfa876cf6576e9dc6fca0b30094ba8d23bfacbb

- baf1e69cb5de8531764a249ada742782ba4309ed1c376b7246b6ad9a7517b236
- 5f7c6d091482605a1c5c06180a90858c35d44bb7d0c791334cd3944ef3315c89
- 77370507aab14252e4c97ffc429439fd34918c830b8f0bb55545390b278c3b04
- abdb0a44b6ea61e6e2cfd1c78f1993a3cd3191728da4201096968577c535a422
- 321f6b7e38a0e452300c5437699de64e9e63d54d1a2aa3ddfc024735cffe78ae
- 2aca29a4434dc41c65abce7c6b990f248a199bc2b4d2a7779fbc37d9e6cee09c
- 81dc502962bbd31b059daa3c5c647849a726aa1ec767ddcdc22907fb8f021719
- dec276adf51bb75362123d379e6a686f8bc6189c7bff986ce651a5254ea131b3

SHA-1

- e62790a7d8f1d495411f9f3c490aaa02c9e08028
- 479b282f353b1b580c17149562001447d859a95f
- c42f8f2b8288f126cdcf5f6c53adce025f292c68
- df25a885063baa87de025894c66c0aef1fe1429c
- 8125ab5fdcf01bded21399b1fcae4d73f200eda6
- 29bc3f3496dcdcc0294f2494fa80842116e46cac
- 9749813bb0d365d1cedaa7f6452c9158a64642b0
- bf6ebcc70f3b3ef267f7236fef42561432d2608d
- 8068bb895caee8ce5c0be0de6added207517eb9b
- 960ff2ccb41174c531672affdfc50d7f361ca257
- 11c9d27f01520911ca186719c169de6fce45e37f
- 04e04466f1a36cc0ee137f4d76a97f9dbc25f694
- 50ba2b5132c98d36b2686cf4d96b08287ff93b2d
- 52a16652546c5c2a48594bea656a5969295ba1db
- 18c078fca9042e571ae32a21fb3f292f10f579dd
- 13eb4f6a08159e6ba94bb52c57448262a2ea0c92
- ebe4425d791757248d31780d32763600d9878fc0
- 3ec9d8e6c2e32f3b5b3eb04dfd2d12f19a72b798
- cb3d0e45ee2fe755eee20ae826c1c24b89bace80

Remediation

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