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

- 5f5c306b241a84194ff3483ec7b7d2fa
- 4a26f8031152f1f2b7976fed301a5616
- cc8a0a4708372c9ff9ecbe0c4a3e4059
- aab5e011ce5b082feae7588438277823
- eaa7181a11ad939f9d9db326e9acb956
- 55b44eb59533588bccc18eaeea1d79ac
- 33492a5e4e83a8cfaa01f73c9ceabbc2
- 42faeb7536cca092c33a739a33221974
- 12e18ae34211ae498a9ccad7fec8efe8
- 3275112f3e46895f1e881f2671ebbe4a
- b9cfad73e21a24302e1355c3fa45eb18
- a8da801a71b09b23b40a082eb8389cca
- 0dd5811f84ac3d71ae96d6072421c4c6
- 383953e8404db5f3e735c77f54603ecb
- fac093453426b1012c3c8c614a290278
- f2e7e10c0ae765fa8b4fc8523108b4c7
- caa4c04d20ca4d9b7b1b37c0379e91c9
- 1c1c54a0ab544ab21ca9f3b894acc863
- 51df255c821f7fe32ddd3c32344529eb

SHA-256

- 2905d677ad42d8690e9dbad8daa5cc51fa77b9a43d7065121e626c52de283243
- 920b5dc483b4d0773bbc753f190dba5384f5683f85a719d70da16013cc6ab2f1
- 8640212124000fd6a88e4147c49e09e681aaead8c9b6756215f7ff2271d4b6cc
- 442d977d920b36858618edc62c516e637189590f13eb99f92a030fade2645933
- 259c1941f9804bdbe44fc0637df1f20f0f41721c96d2c80f622c57660ac5be8c
- 86c99581adc0c5a9f7e4ded23a1a7c6cd0d2e953e703c1dd025535a886eae11f
- 02b90a22d4a80865da76fc94a675b5d83bc79f30876fee9daad55dd9f65dd688
- 7a8923caab04505e4720c0fd8a601be2b5b9b6a37f7a478a4cdf2ca6728b0e0e
- 129463a3e73dfac4372b8781921e61bf1ba0458474e92e0785236b6cba3ac1b3
- 90d4c26d248ca4fc0866363664e9e16b416eaa7e78253063e4e395ecb2595392
- 4546fcf377a64f9d1795d88f093d8d9526be1c95a0ccc0437b87fe2dd6e5df49

- 822476f603a7c8b26a426fae3d4463509eebaa714a116ab02260a4af8de8a27d
- 173be3dac9ad053ddf92111136b982711d70580ce115945b8be156de634056c7
- b3323a5bba07180281870cd79e77f69a2d8b448d81af5c84ad145b73c33d3b34
- fdec1f038fdba45ba380ebeb970c30203afffd4862dc7e51080c542ea6e0dcee
- 2497439848f5a3ca782f66342b8becf7d6f60ef436683e648b7df4c87fc3dc13
- b6be4529f5ad301a331aaf7b37b455e48c8d14204ede8d34f41159d7cf19240b
- 7c12120046176ef45af97206ac081c3f8aaa2bdffcd72e8907651baa9c25a5ce
- e389702b7194c5c62d0cf23617cd54694f97dd25ca6fccd1daa19f0eee08746a

SHA-1

- 1b7a702d3b326c8a1b9dee4b766ad1fce2bdd8d4
- 67db17bd88317ef6930df697281dead93c8a932b
- f74d90b2e5362ed78e05d79bb5ca644699bb778d
- d5f7450d1976fa4cb7584c4977e616773a3de87c
- a510d9637a648e3550793d48612dd8c4c708668e
- 196e51c753f5b25743120ad1b242ed84386626ab
- e471f9c4372d20417b576e3989a60f504c74b683
- a783df1322b2fe79f6e80eab391f813bc70c49c5
- e531b7acbbc3cbc879ae3103da066cecc65071e2
- aaba73db817696982563225ebd65212d2e40c5b1
- e81f985649ce25dd7bbcb994fe17f62f7cc111d7
- d26f5a290808b7e102c9f2fb5723b201bf753f8a
- 7a8395100cad6193c2fe54a4dae83626d8b3160d
- 3b0d8a2764b6dc093187b5e8870481e93601145d
- ead3c8840fbd42e7f35ca66f479b4cad29799bce
- 6ae26b7ba46172850627c58909a456429d831c41
- 4fe0dc2848b01c2c947879f5abfcdc4d186a41a4
- 684ff6d68c255ee76fe5ce50caccd05c49d0045a
- 9488bc0b05cdadcf7b962594f9246c4b797f4db6

Remediation

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