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

- 8f0b0e981372950c04e5cd81700c26a8
- ac49194afce3bdaa39ed3402892f2fc6
- 343377f50db578ae35143dd9c9b66de2
- 9f51b8128a7ba3fd6d2a5d2ac529f099
- 9a793d3abc0c31540f09ec6e4e005927
- d2a865785105193835e11616f0f351b9
- 2fcdd9bd169475f870a82d43d1e56a70
- da298d785c1a0d5d7d408de79b1c2110
- 7ec576b970e48d2bc1a701ce35e1e8a4
- 608c1c9236e99c2b08fc220fc896a7a1
- 6cfed2d2ac3175d800b38a9309db7e38
- faa23241e8b1401e7da983bf9773c702

SHA-256

- 10544eeabc46be66a14dd2dabf01c007ba9e8fec8f60da6cbad58eec9f988e6ds
- a4e5f08ac2f84f03ed7abd1aeafd4a2d7cc1d8656b13d54cb7c236c40c4cc0f3
- e894f6648858c59d59a73da5e329fe66708ce2f7920e105a574ec1b7940a6f3b
- d1f2016637efe5df86887c2be9b3a1e1d8f4d24f93ba03d9bd5205e8cd312345
- 3e3b992d11ec46fa3b662b06ca69cb89db2ed72f10a4993b17193e189fc8ab00
- c57650d7dc7de252ed81b82f4bcf0e0b669fef6b22ade25623bbba7464357e06
- 5688783ff8f939f0a3f740c3f5e0a389bd578451163f2259a1bcde5e7476230b
- f2f5a28e7db8cc6130da2c08a5441adde1d4ef7d835b3948d7a39f270fa4eb58
- cf56d816e8070dff56b03d29a9143adfddf3b6f344233f609bc17b1a9e9d722e
- a3b53c66dddb3f266d1d1a415229ec034f5809cf69a86588b07169e8665dabed
- 6e80657b7c0f79fdba542a1b65365ba411fbe310f7c09b8a8b62603b571fbafc
- 415d7c34e6ef8c7f28dae18e842bef187a4342e15ec8ee0d10692ef38eaaa9f

SHA-1

- 6636717593b60df8105f864db4501ac0ad353278
- 3b5688fa573cf9835bfb18d8f501a569a958ed66
- f785a48783cce329b5d128d47ea65fc9088fa753

- 14b11445258ffba6e600e7e9a186da3392ec5d31
- a040c8bf2447779b71a98197eaaa4d899129ef4a
- 5622f7fdbfbe3df1515ddeab93d7bdd3c667a4eb
- 13e1d53e465c38da82706d21640ea4533d6b8147
- cf7ff15e3fa352e443358f8e391f99a20df815ff
- 78cfb48d4ffef1f04f5c1ccce43790e5afd218bb
- 656b456a54ab21df21886c324416c53bf50a53d4
- 2e4f89451e59956159cf7ba166602007dcccb3e5
- 14c04aafb7a5945414279fc54547c268d4a72760

Remediation

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