|  |  |
| --- | --- |
| **日期** | 2022.07.19 |
| **事件名稱** | Mirai Malware |

|  |  |
| --- | --- |
| hash | comment |
| 0a38acadeb41536f65ed89f84cc1620fb79c9b916e0d83f2db543e12fbfd0d8c.bin |  |
| 3d604ebe8e0f3e65734cd41bb1469cea3727062cffc8705c634558afa1997a7a.bin |  |
| 3d9487191dd4e712cbfb8f4dcf916a707f60c3fb23807d4c02fb941e216f951d.bin |  |
| 58d2db0bc8d93a30101eb87ef28c7dbf1af61ae2ebc355f6a236ab594a236f4b.bin |  |
| ac13002f74249e0eab2dacb596a60323130664b8c19d938af726508fdc7500a2.bin |  |
| bc5f1b69b6edfd58a56b104568cb73fe74ccefea6651b1a1bcf7613331b56597.bin |  |
| e666e0c720387db27e23c65d6a252f79587ca1b9d1c38e96d6db13b05d5b73fa.bin |  |

|  |
| --- |
| **說明** |
| “Mirai (from the Japanese word for "future", 未来) is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.[1] The Mirai botnet was first found in August 2016[2] by MalwareMustDie,[3] a white hat malware research group, and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016[4] on computer security journalist Brian Krebs' web site, an attack on French web host OVH,[5] and the October 2016 Dyn cyberattack.[6][7] According to a chat log between Anna-senpai and Robert Coelho, Mirai was named after the 2011 TV anime series Mirai Nikki.[8]” - wikipedia |
| **原始碼** |
| N/A |