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

|  |  |
| --- | --- |
| hash | comment |
| 7a79658a16949142e7c17c9612713679 [48/1910] |  |
| a1f3ac69bc5030ecf1b351246986621a |  |
| 07c070b717a23453a2b71c7582d6a928 |  |
| e1ec02725fcf3bce48e3131b1a6f2684 |  |
| df7bba1c415ec78a6d9e29d6c92f8a86 |  |
| 39b38284c6ca30d09481fcb5dc7197aa |  |
| b808c078b9786115200002b910a5a05c |  |
| 75a00aad5b506496a2644488064c39b4 |  |
| 7eba17d4ea5615e239c00e47d182e08a |  |
| 24dca1b2097ad6c2e5d8b03d3022f010 |  |
| 4ab3b8eb803e6c4690abe2209b700335 |  |
| 7354323ff72a6132359c5aa76bf9904a |  |
| 0aefb67c01a24d05351b093455203fa2 |  |
| 0bc90c333f08237475a08c7158aba345 |  |
| d130caa1294885cc39ee0bc38037a0ee |  |
| eadf8abf7738144e929a25e9eb7d8076 |  |
| 98d38858bcdcb327df21c3aee1ff40bc |  |
| 96f125505ca736ff5d85ed33fa1c9b15 |  |
| 127ee9c007774e8f1101fb40ea05b42e |  |
| e8c7e887a3e46bfe41fc34a396184f79 |  |
| 16eb5d018d45024462dd63de470a8575 |  |

|  |
| --- |
| **說明** |
| “XOR DDoS is a Linux Trojan malware with rootkit capabilities that was used to launch large-scale DDoS attacks. Its name stems from the heavy usage of XOR encryption in both malware and network communication to the C&Cs. It is built for multiple Linux architectures like ARM, x86 and x64.” - XORDDOS Malware Information, Trend Micro. |
| **原始碼** |
| N/A |