Chai Linyuan

en

Mirai_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability

Overview On 2021-06-22 we detected a sample of a mirai variant that we named mirai_ptea propagating through a new vulnerability targeting KGUARD DVR. Coincidently, a day later, on June 23, we received an inquiry from the security community asking if we had seen a new DDoS botnet, cross-referencing some

· Jul 1, 2021 · 11 min read

nday

Mirai_ptea Botnet利用KGUARD DVR未公开漏洞报告

2021-06-22我们检测到一个我们命名为mirai_ptea的mirai变种样本通过未知漏洞传播。经过分析，该漏洞为KGUARD DVR未公开的漏洞。从我们的分析看该漏洞存在于2016年的固件版本中。我们能找到的2017年之后的固件厂家均已经修复该漏洞

· Jul 1, 2021 · 12 min read

Backdoor

窃密者Facefish分析报告

背景介绍 2021年2月，我们捕获了一个通过CWP的Nday漏洞传播的未知ELF样本，简单分析后发现这是一个新botnet家族的样本。它针对Linux x64系统，配置灵活，并且使用了一个基于Diffie–Hellman和Blowfish的私有加密协议。但因为通过合作机构（在中国区有较好网络通信观察视野）验证后发现对应的C2通信命中为0，所以未再深入分析。 2021年4月26号，Juniper发布了关于此样本的分析报告，我们注意到报告中忽略了一些重要的技术细节，所以决定将漏掉的细节分享出来。 该家族的入口ELF样本 MD5=38fb322cc6d09a6ab85784ede56bc5a7是一个Dropper，它会释放出一个Rootkit。因为Juniper并未为样本定义家族名，鉴于Dropper在不同的时间点释放的Rootkit有不同的MD5值，犹如川剧中的变脸，并且该家族使用了Blowfish加密算法，我们将它命名为Facefish。 Facefish概览 Facefish由Dropper和Rootkit 2部分组成，主要功能由Rootkit模块决定。Rootki

· May 28, 2021 · 17 min read

en

Analysis report of the Facefish rootkit

Background In Feb 2021, we came across an ELF sample using some CWP's Ndays exploits, we did some analysis, but after checking with a partner who has some nice visibility in network traffic in some China areas, we discovered there is literarily 0 hit for the C2 traffic. So

· May 27, 2021 · 13 min read