





木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

CentOS)

◆概要信息

	00033b5b33b59ad88aa4f196c08eb7a6d2e6ab181ec729e8ed577d55f8b1f3ee
	BinExecute/Linux.ELF
大小	164 KB
MD5	60A775F4A99420644181D1DDBD2D6D1D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Mirai.s
判定依据	

https://antiy.pta.center/_lk/details.html?hash=60A775F4A99420644181D1DDBD2D6D1D

◆运行环境

CentOS release 6.8 (Final)	Firefox LibOfÿce

◆文件扫描

	MD5		yara
null	60a775f4a99420644181d1ddbd2d6d1d	N/A	N/A

◆UDP 信息

IP		IP	
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.166	68
192.168.122.166	39164	192.168.122.1	53
192.168.122.1	53	192.168.122.166	39164
192.168.122.166	56620	192.168.122.1	53
192.168.122.1	53	192.168.122.166	56620
192.168.122.166	38094	192.168.122.1	53
192.168.122.1	53	192.168.122.166	38094
192.168.122.166	50078	192.168.122.1	53
192.168.122.1	53	192.168.122.166	50078
192.168.122.166	40654	192.168.122.1	53
192.168.122.1	53	192.168.122.166	40654
192.168.122.166	52039	192.168.122.1	53
.....	.....	.....	.....



实现安全架构的自动化

类 型	内 容				
	0day				
英文标题	Freedom Mobile	1.5			
	Zack Whittaker				
	_ l ᴹ g ᴺ l r uq ǯ.	Freedom Mobile ȳ ₐl	Elasticsearch	500	15,000