木马程序

1A6F9190E7C53CD4E9CA4532547131AF

病毒类型 木马程序

恶意判定 / 病毒名称 Trojan[Downloader]/MSOfÿce.Agent.b

判定依据

https://antiy.pta.center/_lk/details.html?hash=1A6F9190E7C53CD4E9CA4532547131AF

◆运行环境

Win7 x86 6.1.7600 Build 7600	IE9 Google Chrome Firefox Ofÿce 2007 Flash WPS FoxitReader Adobe Reader

◆常见行为

◆UDP 信息

IP		IP	
192.168.122.165	57211	192.168.122.1	53
192.168.122.165	60542	192.168.122.1	53
192.168.122.165	52183	192.168.122.1	53
192.168.122.165	57660	192.168.122.1	53
192.168.122.1	53	192.168.122.165	57211
192.168.122.1	53	192.168.122.165	60542
192.168.122.1	53	192.168.122.165	52183
192.168.122.1	53	192.168.122.165	57660
192.168.122.165	56787	192.168.122.1	53
192.168.122.1	53	192.168.122.165	56787
0.0.0.0	68	255.255.255.255	67
192.168.122.165	49275	224.0.0.252	5355
.....	.....	.....	.....

“ ”





Windows (CVE-2019-0708)