安天周报

2019 09 02 (198) 4 antiylab

“ ”

2019

3-4



8 23 1

CERT

50



10

木马程序

β γ

BD YARA Win7 x86

BD

(WinXP)

◆ 概要信息

	267a9dcf77c33a1af362e2080aaacc01a7ca075658beb002ab41e0712ffe066e
	BinExecute/Microsoft.EXE[:X86]
	183 KB
KB3	0E0B7B238A06A2A37A4DE06A5AB5E615
	木马程序
-	Trojan/Win32.Generic
	BD

https://1.119.163.6/vue/details?hash=0E0B7B238A06A2A37A4DE06A5AB5E615

◆ 运行环境

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Office 2003 Flash WPS FoxitReader Adobe Reader

◆险危行为

PE	

◆常见行为

DLL	
, ,	
PE	

◆ UDP 信息

IP		IP	
192.168.122.111	1032	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1032
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
.....	.....	.....	.....

TA

TA

Tr

Fl

ht