样本基本信息

文件名	cd0f52f5d56aa933e4c21294162336 52a391b5c6f37 2c079ed2c6eaca1b96b85
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	176 KB
MD5	9FAEF92CBFCAE8C809636A906221E775
病毒类型	[redacted]
恶意判定 / 病毒名称	Trojan/Win32.CMY3U
判定依据	)

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Office 2003 Flash WPS FoxitReader Adobe Reader

行为描述	危险等级

行为描述	危险等级
DNS	

ς ∋ Ă ⊿ ⊿ Ă Ë

“ Ă ڜ Ë

Ό ” ˆ Ж ă Ό

Љ ڗ ă “ ” “ ”

Ό Ό Ό

Ë Ό ⊿ Ό ę Ă ⊿

Є Ό ┐ Ă ờ I

Ç Ό Ę Ă ⊿ щ ϡ

ã Ό “ 40 “ ” Ę ⊿

ă “ ” Ë

■ ┐ щ 60

“ ⊿ ϰ Љ ⊦ ⊿ “ ”

ڜ

ϰ Ę Ό

11

CNE ă˚ ▲

ă Ц Ă

Ό

ę Ό ‘ ⊿ ښ

Ë ц

Ό Ë щ Ë Ë “ “ ” “ “ ϔ Љ

Ę Ό Љ ⊿ Ţ “ ”

Ό “ ⊿ ⊿ ă¸ ę Ë ⊿

Ό ă ⊿ ┤ “ Љ

⊿

Ë ڜ

Ă Ë Ѐ

Ę

Ă Ë Ѐ

NSA “ ” Ę

Ă ⊿

30 Ж ϔ

Ă Ѝ e e Ό

Ḍ щ

Ă Ό ă

Ă Ό Ę Ḍ Ό ⊿ Ă

Ë “ ” Ό

Ό e