BD YARA WinXP

Win7 x86

Win7sp1 x86 BD

	Xjs.dll
	BinExecute/Microsoft.DLL[:X86]
	33 KB
MD5	7D602363A760AC03092DF5A2FFD774D6
	[redacted]
/	Trojan/Win32.Generic

Image Version	

https://1.119.163.6/vue/details?hash=7D602363A760AC03092DF5A2FFD774D6

File Size	33 kB
File Type	Win32 DLL
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2021:06:24 14:26:59+08:00
PE Type	PE32
Linker Version	10.0
Code Size	18432
Initialized Data Size	14336
Uninitialized Data Size	0
Entry Point	0x13a9
OS Version	5.1

周观察

2021 09 13 (295)

CNCERT APT

CNCERT

13 78

8 APT 5 2021

APT

APT APT

APT

APT

“ ”

APT

CNCERT

200

App

App

https://mp.weixin.qq.com/s/GdE36gNXVKFnfaZfRV80rA

App

IT

Ľ Ľ 2020

300

Ľ Ľ Ɛ

1.

Ľ Ľ

Colonial Pipeline

IT

Colonial Pipeline ך ג

ך

Verizon

ג

80%

75% “ ”

2.

3. DRaaS

“ Ƀ

” ך

Ɛ

“ ” (DRaaS)