CERT

6688123

6688123 2020 9

RSA AES z z z z z .23/+640/7./6 - ./.+60671501 0.0/ .4 .5 & 06/ ' 2

BD YARA

Win7 x86

BD

Win7sp1 x86 WinXP

	6bb.exe
	BinExecute/Microsoft.EXE[:X86]
	128 KB
MD5	B0E68A3352D31A9DD403A5ACAE6387A0
	[redacted]
/	VCS/Instruction.JunkCode

https://1.119.163.6/vue/details?hash=B0E68A3352D31A9DD403A5ACAE6387A0

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Ofÿce2003 Flash WPS FoxitReader AdobeReader

App

App

https://mp.weixin.qq.com/s/EZNxqIFjoJU18pMoHac7Bg

CVE-2018-13379 BMR Boot NetBackup BMR SQLTELEMETRY SQLWriter Mimikatz Cobalt Strike mspub.exe mydesktopqos.exe Cring mydesktopservice.exe

Backup backup

https://mp.weixin.qq.com/s/3UUbbZewFwoNHRNqwV3YOQ

Cring Crypt3r Vjiszy1lo Ghost Phantom 2020

AES256+RSA8192 kill.bat

2