‰ώь نڜ ԟQl_icɢ Δ

CERT VMware

Snake Microsoft System Center Operations Manager

Snake 2020 1 Sqlservr

Go Microsoft SQL Server

Snake

IEP VPN

Snake

Snake Snake “ AES+RSA ”

“ Fix-

Your-Files.txt ”

Snake

VMware Tools

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

BD YARA

Win7 x86

BD

WinXP)

	e5262.exe
	BinExecute/Microsoft.EXE[:X86]
大小	3.55 MB
MD5	3D1CC4EF33BAD0E39C757FCE317EF82A
病毒类型	[redacted]
恶意判定 / 病毒名称	Trojan/Win32.Antavmu
判定依据	BD

n Ŵ Ö ﺹ

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

DLL	

z z z z z .23/+640/7./6 - ./.+60671501

DNS

“ ”

“ ” 5G

Q “

”

A “

”

Q “

”

A “

”

Q “

”

A “ ‘ ’ ‘

’

”

“ ” “

”

2•«e›eB×4mñ#ÜAå4G,Þ6 8ÜSú93•l²y3ÌÐ.ŽÞ?• …˜É2ÒàrÎCÙ Tã••GÓ¨Ä@ # € _Ð VÞ ! P P Z

? Ñ }L L Ë

$ Æ 9í Í u Ò q1×G L ,ºH ?ü ¸ Þ Þ

¼5‡5 ¿ žN¼ c-. Ê?ú H,º } >

英文标题	Supercomputers hacked across Europe to mine cryptocurrency
	Catalin Cimpanu for Zero Day
	https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/