CERT 200 1500
Velar Velar “ AES+RSA ”
Velar 2020 3
VPN
Velar

“ .Velar ”
“ readme.txt ”

USER_ID

木马程序

	106017ca2da2422722ecff4ce1fa74454f7964c0e4b5b45eacff97ec0b34903c
	BinExecute/Microsoft.EXE[:X86]
	506 KB
KB3	4482844622C6CC5027927A856E8BAD57
	[redacted]
-	Trojan/Win32.Wacatac

PID		
2156	target.exe	"c:\222294fcd0e64302a58a25ae545f771e\share\target.exe"
2244	vssadmin.exe	vssadmin delete shadows /all /quiet

Win7 x86 6.1.7600 Build 7600	IE9 Google Chrome Firefox Ofÿce 2007 Flash WPS FoxitReader Adobe Reader

DLL	

CERT

WannaRen
“ WannaCry ”
“ .WannaRen ”
CERT
WannaRen

KMS PowerShell
PowerShell

PowerShell DLL
DLL
“ WINWORD.exe ”

_] > : ¯ Ã Ẁ £ Windo
“ you ” “ WINWORD. C:\User\Public ẄA ЛĮ ɣ ɣ ɣ
exe ” “ wwlib.dll ” DLL
DLL
+

0.05BTC 2500

PowerShell WannaRen

0.00009490
IEP
WannaRen

ATT&CK

ATT&CK
WannaRen

2020 4 13 (226)
antiynews@antiy.cn

Berkine Maze
Maze ransomware group hacks oil giant; leaks data online
Deeba Ahmed
2020 4 1 Berkine