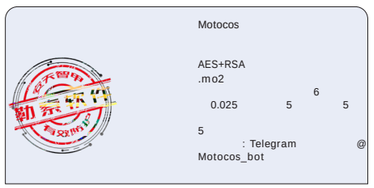
Motocos



CERT
Motocos
2021 5

IEP
Motocos
Motocos Delphi

10

“

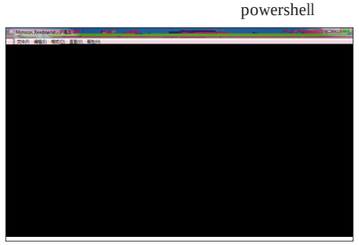
+.mo2 ”

“ Ransomware_ Motocos “ AES+RSA ” Readme.txt ” “ Motocos_Readme.txt ” “ Readme.txt ”

RSA Telegram

0.025
vssadmin.exe wmic.exe
bcdedit.exe wbadmin.exe

powershell



VPN

▲ Motocos

木马程序

BD YARA WinXP
Win7 x86
Win7sp1 x86 BD

	88af65ad6b23ee2f9745ddacff604748
	BinExecute/Microsoft.EXE[:X86]
	2.23 MB
MD5	88AF65AD6B23EE2F9745DDACFF604748
	[redacted]
/	Trojan/Win32.Agentb

https://1.119.163.6/vue/details?hash=88AF65AD6B23EE2F9745DDACFF604748

.....	.....

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

“ ”

2010 7 15 EastNets
APT 2010 9 27 “ ”
NSA “ ” Stuxnet “ ”
Stuxnet 2019 6 1
A²PT “ ” SWIFT
2020 EastNets
3 4 IT
“ ”
“ ” Stuxnet
“ TCTF ” V2

2013-2017

2013
/ 2020 1
A²PT 2015
NSA
“ ”

2015 3 A²PT
“ ”
——
EQUATION
“ ” EquationLaser
EquationDrug DoubleFantasy
2010 7 TripleFantasy Fanny GrayFish
, —— “
nls_933w.dll ”
A²PT

2018-

https://mp.weixin.qq.com/s/RGIfplSiDK8_AQekn-nImA

2010-2012 APT

2010 7

2019 1
“ ”