DoppelPaymer

CERT

DoppelPaymer .readme2unlock.txt

DoppelPaymer TOR

2019 6 RDP data

DoppelPaymer

RSA+AES

DoppelPaymer arp a VPN

INDRIK SPIDER BitPaymer ARP

DoppelPaymer

INDRIK SPIDER

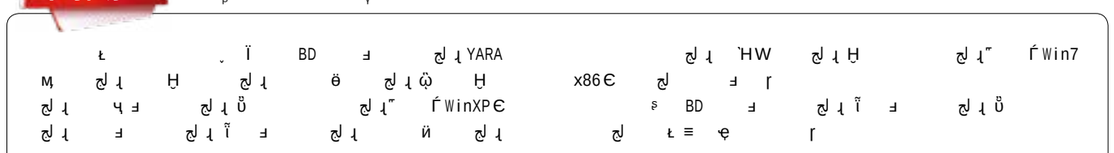
%Users%

gratemin p1q135no.

exe

.locked

木马程序



◆概要信息

	f658ddcf8e87de957a81bb92d44ce02913b427e8bccbe663669ee2613d355555
	BinExecute/Microsoft.EXE[:X86]
	3.24 MB
KB3	8C54BBE3F191A8627BFEEB4CB02634A9
	木马程序
-	Trojan[Ransom]/Win32.Encoder

◆操作系统

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

◆常见务曞

DLL	

.....	.....

◆完整报告地址

安天周报察
2019 11 25 (209) antiylab

2019 11 10 6

181

3800

711.3

23%

类 型	内 容
	Windows Cyborg
英文标题	Fake Windows Update Spam Leads to Cyborg Ransomware and Its Builder
	Diana Lopera
	Trustwave Windows Update Cyborg ".jpg" .NET Github bitcoingenerator.exe btcgenerator Cyborg Cyborg .777 500
	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/fake-windows-update-spam-leads-to-cyborg-ransomware-and-its-builder/