CERT 11
.NET URL
InnfiRAT InnfiRAT Cookie
2017

CMD
InnfiRAT Cookie
CERT

Process
Hacker Process Explorer Process
Monitor
InnfiRAT

◆概要信息

	755894e632485b30d1522058a63b830f4c4c245207141cad4a8b456acee487f5
	BinExecute/Microsoft EXE[:X86]
	1.03 MB
KB3	F992DD6DBE1E065DFF73A20E3D7B1EEF
	木马程序
-	Trojan/Win32.Razy
	BD

https://1.119.163.6/vue/details?hash=F992DD6DBE1E065DFF73A20E3D7B1EEF

◆运行环境

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

◆危险行为

WMI CPU	
WMI CPU	

◆常见行为

内 容
TFlower
wer Ransomware - The Latest Attack Targeting Businesses
rence Abrams
TFlower PowerShell Empire PSExec
s://www.bleepingcomputer.com/news/security/tÃower-ransomware-the-latest-attack-targeting-businesses/