CERT installer.bat
GroksterMiner installer.bat
GroksterMiner Lucio 001.tmp
Dalla Discografia Completa svchost.exe
svchost.exe

P2P PE
SFX
7-Zip WinRAR
13 .tmp P2P
1 .vbs 1 .bat DOS program
1 setup 7
run.vbs HASH
CERT
run.vbs

β γ

BD YARA Win7
x86
(WinXP) BD

◆ 概要信息

	f9b2e61200addf760d7bd157c73201e97257b12d 5177837a1bffb98f4064e76a
	BinExecute/Microsoft.EXE[:X86]
	6.25 MB
KB3	D6D388E0883F8CFEA196BA1C8FB32043
	木马程序
-	Trojan/BAT.BitMin

https://1.119.163.6/vue/details?hash=D6D388E0883F8CFEA196BA1C8FB32043

◆ 运行环境

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

◆常见行为

	•i0 pX • ƒAB-3,ßS¨ä 'žÓâRCœã ø05D1 ˜4 •i0 pX •)X†CA,"9,õ:ŽÍ0 ƒ TBfxd4 É É “ ÷ € pxcAC #˜"µ#• R@ðCR© /¼ã ø05D#WxcAAÉ É “ ÷ € a 4 *•1l*'2ûÎ0 ƒ TB`Wp3AAÉ “ ÷ € Fib‡ˆy Î0 ƒ TB b‡ˆy Î0U

概述
2019 4 CERT

Mykings } □ ã

视频成为恶意软件攻击的传播载体

内 容
Beapy
m-C ombo Lets You Game While Using NSA Exploits to Move Laterally
AR d BUDACA
Bitd Beapy Beapy/PCASTLE PUA Beapy Python Powershell CPU tern SA C&C
s://l /08/worm-cryptominer-combo-lets-you-game-while-using-nsa-exploits-to-move-laterally/