LockerGoga

CERT

LockerGoga

CPU

LockerGoga
master/slave
LockerGoga %TEMP%
-m
Master -m

M M ò Ъ ð ~ η IPC

LockerGoga

木马程序 β γ .locked Internet

LockerGoga cipher.exe VPN

VPN

CERT

◆概要信息

	7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
	BinExecute/Microsoft.EXE[:X86]
	1.19 MB
KB3	7E3F8B6B7AC0565BFCBF0A1E3E6FCFBC
	木马程序
-	Trojan[Ransom]/Win32.Crypren

https://1.119.163.6/_lk/details.html?hash=7E3F8B6B7AC0565BFCBF0A1E3E6FCFBC

◆运行环境

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

◆危险行为

◆常见行为

, ,	









APT 2018

类 型	事件一	事件二
		ActiveX
	VirusTotal XTunnel APT28 2016 DNC VirusToal ZoneAlar VirusTotal 71 41	ActiveX ActiveX Microsoft Microsoft Edge ActiveX ActiveX ActiveX Internet Explorer ActiveX 2019 ActiveX 10 ActiveX 40

WhatsApp telegram

2019-05-19 Trojan/Android.interapp.a[prv,spy]

2019-05-21 Trojan/Android.FakeJioPrime.a[exp,rog]

Trojan/Android.ichipspy.a[prv,spy]

G-Ware/Android.FakeWG.b[prv,rog]

RiskWare/Android.xiaokuangyl.a[exp]

Tool/Android.merchant.a[prv]

64

DNF

G-Ware/Android.CoinMiner.e[exp,rog]

NSIS NullsoftInstallScriptable Install System Windows NSIS

Trojan/Android.kicoSpy.a[prv,spy]

Windows PHP IRC Linux

0day RiskWare[WebToolbar]/NSIS.Agent

GrayWare[AdWare]/Win32.Boran