DanaBot

CERT

DanaBot crypt.exe

Windows

DanaBot AES128

.non crypt.exe

HowToBackFiles.txt

word 14 CERT

DanaBot

VBS %TEMP% Blitzkrieg

DanaBot Yaroslav

Harakhavik Aliaksandr Chailytko VPN

DanaBot Blitzkrieg

Delphi DanaBot

crypt.exe crypt.exe RDP VNC TOR

%TEMP% b.bat WUSA

b.bat Windows UAC C&C

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

◆ 概要信息

	8a21e1224a8f1d7dd9d4e42c78c829fb82808631577477e8f699f15feb7c8988
	BinExecute/MicrosoftEXE[:X86]
大小	144 KB
MD5	E48067D2AD6ADCBF2E4CF7E705D4BD82
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.CryFile
判定依据	

https://1.119.163.6/vue/details?hash=E48067D2AD6ADCBF2E4CF7E705D4BD82

◆ 运行环境

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

◆ 危险行为

USP	
all	

◆ 常见行为

.....	.....

Powload CreatePopupMenu AppendMenu

WH_

CALLWNDPROC EVENT_SYSTEM_

MENUPOPUPSTART

Emotet 5 TrackPopupMenu

Powload EVENT_SYSTEM_

MENUPOPUPSTART

Powload

VBA

PowerShell WH_CALLWNDPROC

Powload

XML

Forms

VBA

https://blog.trendmicro.com/trendlabs-security-intelligence/powload-loads-up-on-evasion-techniques/

2019 6 ESET

Windows

07 15 (1
antiynews@antiy.cn