CERT Ursnif Pushdo
Ursnif Ursnif
Ursnif Dreambot Gozi
ISFB API
Ursnif
Pushdo
Pushdo

“ iexplorer.
exe ”

COM C&C
DHL
Excel Excel
CERT

“ ”
2019 8 8
9
300
com/us/threat-insight/post/psixbot-continues-evolve-updated-dns-infrastructure

“ ”

Wandera

β γ

BD YARA Win7
x86
(WinXP) BD

◆ 概要信息

	aac9d2d21f634157eb8d3867a2c72042a83cabc3f0142b12763312f5a0b0a83a
	BinExecute/Microsoft.EXE[:X86]
	296 KB
KB3	59CEADA6218D87ED00FEE4D025AE58C7
	木马程序
-	Trojan[Spy]/Win32.Ursnif

https://1.119.163.6/vue/details?hash=59CEADA6218D87ED00FEE4D025AE58C7

◆ 运行环境

Win7 x86 6.1.7600 Build 7600	IE9 Google Chrome Firefox Office 2007 Flash WPS FoxitReader Adobe Reader

◆危险行为

i ㄐ D

类 型	
英文标题	Be
	La
	ht