应急服务背景

CERT

2019 5

HASH

深度分析支持和支持归零复盘

HASH

WannaMine

BD YARA Win7

x86

WinXP BD

◆概要信息

	ec61768e0a7da9650f8662ae0918fc48dc2bed6b4a97f277ceb5fdd4b1ef65f4.exe
	BinExecute/Microsoft.EXE[:X86]
	6.38 MB
KB3	80402E15A81E4F513980857455EB5A9C
	木马程序
-	Trojan/Win32.Miner

◆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

DLL	

CMD	

◆常见行为

DLL	
PE	
.....	.....

◆完整报告地址

现场信息采集观测和研判

ID

制定加固策略、分发安全补丁、查杀终端威胁

EternalBlue “ ”

445 MS17-010

WannaMine

MS17-010

“ ”

STIG

HASH

CERT

类型	内容
	Drupalgeddon2
英文标题	New Campaign Targets Drupalgeddon2 Flaw to Install Malware
	Ionut Arghire
	Akamai Drupalgeddon2 Drupal CVE-2018-7600 Drupal 6 7 8 2018 3 Akamai Larry W. Cashdollar .gif
	https://www.securityweek.com/new-campaign-targets-drupalgeddon2-faw-install-malware