Magecart KPOT

2019 8 CERT
KPOT
C2
Magecart
Magecart
Chrome Firefox Internet Explorer
Magecart 2016 cookies shype telegram
KPOT discord battle.net Steam
cookies FTP Jabber
RIG windows
Fallout
KPOT C2 CERT

C2 KPOT

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：

BD YARA Win7 x86
BD
WinXP

◆ 概要信息

	9f5e85a120c4c5d393d5a4f5196ab48771c347e870236bf760968c8233976333.exe
	BinExecute/Microsoft.PE[:X86]
大小	441 KB
MD5	E55ADC77DA695DF375AB985469B5E5E4
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Chapak
判定依据	

◆ 操作系统

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

◆ 常见行为

◆ UDP 信息

IP		IP	
192.168.122.111	1034	192.168.122.1	53
192.168.122.111	1033	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1034
192.168.122.1	53	192.168.122.111	1033
192.168.122.111	137	192.168.122.255	137
192.168.122.111	138	192.168.122.255	138
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
192.168.122.61	138	192.168.122.111	138
192.168.122.111	137	192.168.122.61	137

◆完整报告地址

北佛罗 达州妇 科数据泄 影响约 52 万患者信息

OB-GYN 528,188

OB-GYN

2019 5 6
7 27

2019 4 29

全球性科技公司 Pitney Bowes 遭到恶意软件的攻击

Pitney Bowes

Pitney Bowes 500
90%
, 100
Pitney Bowes