2019

2019 9 16

22

70

DLL DLL Astaroth

Userinit

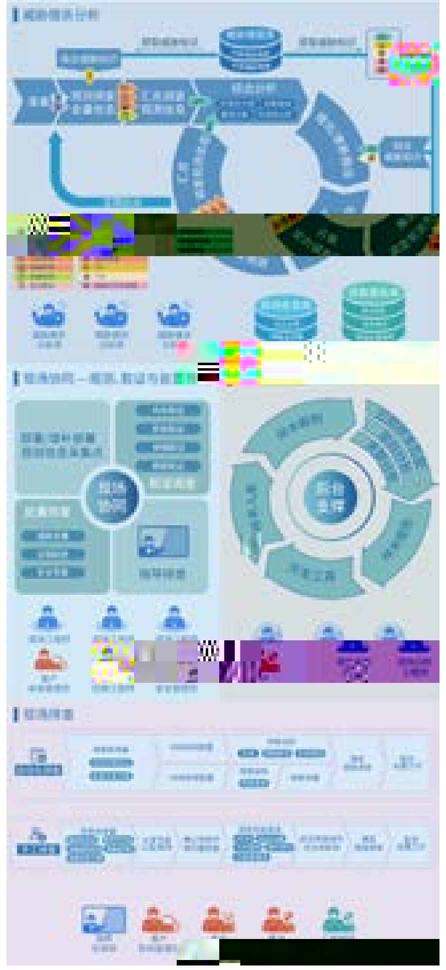
Astaroth

IE

Astaroth

IE IE

CERT



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

	e44548f0c7d26a6d11f3ab29753e36f525559dc2e443bff96346f1be17cd644a
	BinExecute/Microsoft.DLL[:X86]
大小	1.43 MB
MD5	A882D96751F0D49B04751BE7EE319B5D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Occamy
判定依据	

https://1.119.163.6/vue/details?hash=A882D96751F0D49B04751BE7EE319B5D

◆ 运行环境

WinXP 5.1.2600 Service Pack 3 Build 2600	= ʏ Ɛ6 ǯ ȝ ȝ m ȝ 7

IP		IP	
192.168.122.111	137	192.168.122.255	137
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.1	67	192.168.122.111	68

◆进程监控

PID		
1376 }	rundll32.exe Ǹ0	"C:\WINDOWS\system32\rundll32.exe" c:\5d0bfbc7b85646e4a1cad1aa7a13acec\share\target.dll,TMethodImplementationIntercept
1880	rundll32.exe	"C:\WINDOWS\system32\rundll32.exe" c:\5d0bfbc7b85646e4a1cad1aa7a13acec\share\target.dll,DllMain

类 型	内 容
	Red Lion
英文标题	Several Vulnerabilities Found in Red Lion HMI Software
	Eduard Kovacs
	Red Lion HMI Red Lion Crimson 3.0 3112.00 3.1 CVE-2019-10996 CVE-2019-10978 CVE-2019-10984 CVE-2019-10990 CD3
	https://www.securityweek.com/several-vulnerabilities-found-red-lion-hmi-software

---

供应链安全：选择供应商的五种 IT 策略

Ran ∫ ʘ Barr/文 @安天技术公益翻译组 / 译/