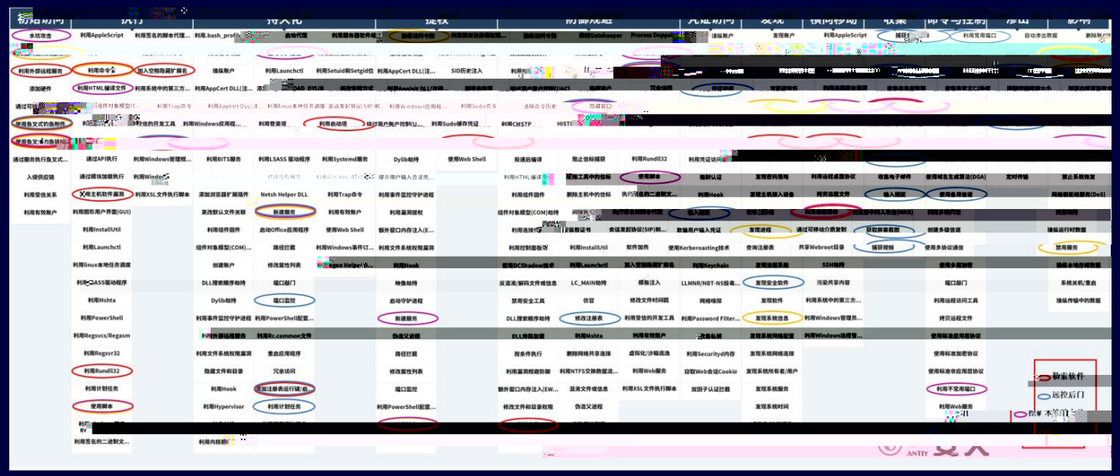
	Zeropadypt.exe
	BinExecute /Microsoft.EXE[.X86]
大小	987 KB
	117C3707F4D8DB004A0E7EF86350612B
病毒类型	[redacted]
恶意判定 / 病毒名称	Trojan[Ransom] / Win32.Crypren
判定依据	

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可精准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：

PID		
1340	target.exe	"c:\3d7317caa5e54b4e87b159cf2258d06c\share\target.exe"
1424	cmd.exe	C:\WINDOWS\system32\cmd.exe /c net stop SQLWriter
1304	net.exe	net stop SQLWriter
1624	net1.exe	net1 stop SQLWriter
1728	cmd.exe	C:\WINDOWS\system32\cmd.exe /c net stop SQLBrowser
1752	net.exe	net stop SQLBrowser
.....	.....	.....



ATT&CK

