Tencent HABO
Analysis System

SHA256:	97bbc5d487334b3ea4598455f1621ec23b32fd71684e70977b689d5a8009aafe
File type:	EXE
Copyright:	
Version:	
Shell or compiler:	PACKER:UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [Overlay]
Sub-file information:	Detail

Key behaviour

Behaviour: Modify registry of startup

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Winsock32

Process

Behaviour: Create process

Detail info: [0x000009f4]ImagePath = C:\WINDOWS\system32\wscript.exe, CmdLine = wscript C:\CasperMail.vbs

Behaviour: Create local thread

Detail info: TargetProcess: wscript.exe, InheritedFromPID = 2536, ProcessID = 2548, ThreadID = 2556, StartAddress = 01002FD4, Pa
TargetProcess: wscript.exe, InheritedFromPID = 2536, ProcessID = 2548, ThreadID = 2560, StartAddress = 765E964D, Pa

File

Behaviour: Create file

Detail info: C:\CasperMail.vbs
C:\WINDOWS\CasperEMail.txt

Behaviour: 修改脚本文件

Detail info: C:\CasperMail.vbs ---> Offset = 0

Behaviour: Modify file

Detail info: C:\WINDOWS\CasperEMail.txt ---> Offset = 0
C:\WINDOWS\CasperEMail.txt ---> Offset = 1

Behaviour: Copy file

Detail info: C:\Documents and Settings\Administrator\Local SettC:\WINDOWS\MsWinsock32.exe ---> C:\WINDOWS\MsWinsock32.ex

Behaviour: Find file

Detail info: FileName = C:\WINDOWS
FileName = C:\WINDOWS\system32
FileName = C:\WINDOWS\system32\wscript.exe

Registry

Behaviour: Modify registry

Detail info: \REGISTRY\USER\S-*\Software\CasperWorm\Author
\REGISTRY\USER\S-*\Software\CasperWorm\Version

Behaviour: Modify registry of startup

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Winsock32

Other

Behaviour: Call Sleep function

Detail info: [1]: MilliSeconds = 3000.

Behaviour: Create event

Detail info: EventName = Global\crypt32LogoffEvent

Behaviour: Create mutex

Detail info: CTF.LBES.MutexDefaultS-*
CTF.Compart.MutexDefaultS-*
CTF.Asm.MutexDefaultS-*
CTF.Layouts.MutexDefaultS-*
CTF.TMD.MutexDefaultS-*
CTF.TimListCache.FMPDefaultS-*MUTEX.DefaultS-*

Behaviour: Open mutex

Detail info: ShimCacheMutex

Behaviour: Open event

Detail info: HookSwitchHookEnabledEvent
Global\crypt32LogoffEvent
MSFT.VSA.COM.DISABLE.2548
MSFT.VSA.IEC.STATUS.6c736db0