TDL4 v2

Camal Viper Serious

Name	Value
Size	146944
MD5	4a052246c5551e83d2d55f80e72f03eb
SHA1	bc29f1e8460915596e1dcafd0c92d6309457d149
SHA256	b75fd580c29736abd11327eef949e449f6d466a05fb6fd343d3957684c8036e5
Process	Exited

Name	Type	Size	Value
LM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations	REG_MULTI_SZ	140	"\??\C:\DOCUME~1\User\LOCALS~1\Temp\3.tmp"

Name	Size	Last Write Time	Creation Time	Last Access Time	Attr
C:\Documents and Settings\User\Local Settings\Temp\3.tmp	146944	2011.05.04 10:37:26.218	2011.05.04 10:36:42.187	2011.05.04 10:36:42.187	0x20
C:\WINDOWS\Temp\5.tmp	146944	2011.05.04 10:37:26.218	2011.05.04 10:37:28.718	2011.05.04 10:37:28.718	0x20

Name	Size	Last Write Time	Creation Time	Last Access Time	Attr
C:\TEST\sample.exe	146944	2011.05.04 10:37:26.218	2011.05.04 10:36:42.187	2011.05.04 10:36:42.187	0x20

C:\WINDOWS\system32\drivers\etc\hosts	734	2011.05.0412:00:00.000	2011.05.0412:00:00.000	2011.05.0409:14:46.187	0x20

PId	Process Name	Base	Size	Flags	Image Name
0x530	spoolsv.exe	0x76bf0000	0xb000	0x800c4004	C:\WINDOWS\system32\PSAPI.DLL
0x530	spoolsv.exe	0x771b0000	0xa6000	0x80084004	C:\WINDOWS\system32\WININET.dll

• Windows Api Calls

PId	Image Name	Address	Function (Parameters) | Return Value
0x4ac	C:\TEST\sample.exe	0x92ba7c	MoveFileExW(lpExistingFileName: "C:\TEST\sample.exe", lpNewFileName: "C:\DOCUME~1\User\LOCALS~1\Temp\3.tmp", dwFlags: 0x9)|0x1

Auto Analysis Verdict
Suspicious++

Suspicious Actions Detected
Copies self to other locations
Deletes self

PId	Image Name	Address	Mutex Name
0x4ac	C:\TEST\sample.exe	0x7c859add	DBWinMutex

• Events Created or Opened

PId	Image Name	Address	Event Name
0x4ac	C:\TEST\sample.exe	0x77a89422	Global\crypt32LogoffEvent

Binary System Activities

+ Registry				
Timestamp	Action Type	Operation	Source	Destination
2011.05.04 18:15:58.796	registry	SetValueKey	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData
2011.05.04 18:15:59.406	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Control\Print\Providers\OCEIQ.dll\Name
2011.05.04 18:15:59.421	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Control\Print\Providers\Order
2011.05.04 18:15:59.859	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData
2011.05.04 18:15:59.890	registry	SetValueKey	C:\WINDOWS\system32\	HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingF

			spoolsv.exe	ileRenameOperations
2011.05.04 18:15:59.937	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Control\Print\Providers\Order
2011.05.04 18:16:0.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Control\Print\Providers\OCEIQ.dll\Name
2011.05.04 18:16:0.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Control\Print\Providers\Order
2011.05.04 18:16:0.312	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData
2011.05.04 18:16:0.437	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData
2011.05.04 18:16:0.453	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Control\Print\Providers\Order

2011.05.04 18:16:0.734	registry	SetValueKey	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe	HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations
2011.05.04 18:16:2.890	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
2011.05.04 18:16:2.984	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Directory
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Paths
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1\CachePath
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\syst	HKLM\SOFTWARE\Microsoft\Windows\Current

			em32\spoolsv.exe	Version\Internet Settings\Cache\Paths\path2\CachePath
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\path3\CachePath
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\path4\CachePath
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\path1\CacheLimit
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\path2\CacheLimit
2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Cache\Paths\path3\CacheLimit

2011.05.04 18:16:3.0	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4\CacheLimit
2011.05.04 18:16:3.15	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies
2011.05.04 18:16:3.15	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History
2011.05.04 18:16:4.390	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
2011.05.04 18:16:4.390	registry	DeleteValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
2011.05.04 18:16:4.390	registry	DeleteValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
2011.05.04 18:16:4.390	regis	DeleteValueK	C:\WINDOW	HKU\.DEFAULT\Software\Microso

	try	ey	S\system32\spoolsv.exe	ft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
2011.05.04 18:16:4.390	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable
2011.05.04 18:16:4.390	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
2011.05.04 18:16:4.750	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
2011.05.04 18:16:4.750	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
2011.05.04 18:16:4.750	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
2011.05.04 18:16:4.796	re	SetVal	C:\WI	HKU\.DEFAULT\

	gis try	ueKey	NDOW S\syst em32\ spools v.exe	Software\Microso ft\Windows\Curre ntVersion\Internet Settings\ZoneMap\ ProxyBypass
2011.05.04 18:16:4.796	re gis try	SetVal ueKey	C:\WI NDOW S\syst em32\ spools v.exe	HKU\.DEFAULT\ Software\Microso ft\Windows\Curre ntVersion\Internet Settings\ZoneMap\I ntranetName
2011.05.04 18:16:4.796	re gis try	SetVal ueKey	C:\WI NDOW S\syst em32\ spools v.exe	HKU\.DEFAULT\ Software\Microso ft\Windows\Curre ntVersion\Internet Settings\ZoneMap\ UNCAsIntranet
2011.05.04 18:16:5.984	re gis try	SetVal ueKey	C:\WI NDOW S\syst em32\ spools v.exe	HKLM\SOFTWARE \Microsoft\Security Center\UacDisable Notify
2011.05.04 18:16:5.984	re gis try	SetVal ueKey	C:\WI NDOW S\syst em32\ spools v.exe	HKLM\SOFTWARE \Microsoft\Windows \CurrentVersion\pol icies\system\Enable LUA
2011.05.04 18:16:6.609	re gis try	SetVal ueKey	C:\WI NDOW S\syst em32\ spools v.exe	HKLM\SYSTEM\ ControlSet001\S ervices\Tcpip\Pa rameters\Interfa ces\{48DA4ED7-5BD1-4CA7-A4E6-A87B96F0BE35} \DhcpNameServer
2011.05.04 18:16:6.625	re gis	SetVal ueKey	C:\WI NDOW	HKLM\SYSTEM\ ControlSet001\S

	try		S\system32\spoolsv.exe	ervices\Tcpip\Parameters\Interfaces\{48DA4ED7-5BD1-4CA7-A4E6-A87B96F0BE35}\NameServer
2011.05.04 18:16:6.625	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\DhcpNameServer
2011.05.04 18:16:6.687	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\NameServer
2011.05.04 18:16:6.703	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{F9163EB7-D332-46DC-B71D-FB973E7381EA}\DhcpNameServer
2011.05.04 18:16:6.734	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{F9163EB7-D332-46DC-B71D-FB973E7381EA}\NameServer
2011.05.04 18:16:6.734	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\DhcpNameServer

2011.05.04 18:16:6.734	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\NameServer
2011.05.04 18:16:7.937	registry	SetValueKey	C:\WINDOWS\system32\spoolsv.exe	HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\WINDOWS\system32\spoolsv.exe

+ File				
Timestamp	Action Type	Operation	Source	Destination
2011.05.04 18:15:57.93	file	Write	C:\Documents and Settings\admin\Desktop\CaptureClient\CaptureClient.exe	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe
2011.05.04 18:15:57.156	file	Write	C:\Documents and Settings\admin\Desktop\CaptureClient\CaptureClient.exe	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe
2011.05.04 18:15:58.921	file	Write	C:\Documents and Settings\admin\Desktop\Ca	C:\Documents and Settings\admin\Application

			ptureClient\binary.exe	Data\6fd3a758.exe
2011.05.04 18:15:58.921	file	Write	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe	C:\Documents and Settings\admin\Application Data\6fd3a758.exe
2011.05.04 18:15:59.203	file	Write	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe	C:\WINDOWS\system32\spool\prtprocs\w32x86\OCEIQ.dll
2011.05.04 18:15:59.203	file	Write	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe	C:\WINDOWS\system32\spool\prtprocs\w32x86\OCEIQ.dll
2011.05.04 18:15:59.218	file	Write	System	C:\Documents and Settings\admin\Application Data\6fd3a758.exe
2011.05.04 18:16:0.562	file	Write	System	C:\Documents and Settings\admin\Application Data\6fd3a758.exe
2011.05.04 18:16:1.140	file	Write	C:\WINDOWS\system32\spoolsv.exe	C:\WINDOWS\Tasks\6fd3a758.job
2011.05.04 18:16:1.562	file	Write	System	C:\WINDOWS\Tasks\6fd3a758.job

2011.05.04 18:16:1.625	file	Write	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\Tasks\6fd3a758.job
2011.05.04 18:16:2.250	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.250	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.250	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.265	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.328	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.343	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.343	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.343	file	Write	C:\WINDOWS\system32\lsass.exe	C:\WINDOWS\system32\config\SECURITY
2011.05.04 18:16:2.578	file	Writ	System	C:\WINDOWS

		e		\Tasks\6fd3a758.job
2011.05.04 18:16:5.968	file	Write	C:\WINDOWS\system32\spoolsv.exe	C:\WINDOWS\system32\ernel32.dll

+ Process				
Timestamp	Action Type	Operation	Source	Destination
2011.05.04 18:15:57.468	process	created	C:\Documents and Settings\admin\Desktop\CaptureClient\CaptureClient.exe	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe
2011.05.04 18:16:0.828	process	terminated	C:\Documents and Settings\admin\Desktop\CaptureClient\CaptureClient.exe	C:\Documents and Settings\admin\Desktop\CaptureClient\binary.exe

Network

+ Connections							
+ Incoming TCP							
Start Time	End Time	Source IP	Source Port	Destination IP	Destination Port	Count	Bytes

Sat Feb 12 18:16:07 2011	Sat Feb 12 18:16:07 2011	208.69.34.136	80	192.168.9.100	1047	4	1659
Sat Feb 12 18:16:09 2011	Sat Feb 12 18:16:09 2011	65.55.12.249	80	192.168.9.100	1049	4	1460
Sat Feb 12 18:16:06 2011	Sat Feb 12 18:16:07 2011	67.215.65.132	80	192.168.9.100	1046	4	190
Sat Feb 12 18:16:08 2011	Sat Feb 12 18:16:08 2011	207.46.197.32	80	192.168.9.100	1048	3	484

+ Outgoing TCP							
Start Time	End	Source IP	Sour	Destinatio	Destina	Count	Bytes

	Time		ce Port	n IP	tion Port		
Sat Feb 12 18:16:08 2011	Sat Feb 12 18:16:09 2011	192.168.9.100	1049	65.55.12.249	80	5	116
Sat Feb 12 18:16:08 2011	Sat Feb 12 18:16:08 2011	192.168.9.100	1048	207.46.197.32	80	5	57
Sat Feb 12 18:16:06 2011	Sat Feb 12 18:16:07 2011	192.168.9.100	1046	67.215.65.132	80	5	182
Sat Feb 12 18:16:07 2011	Sat Feb 12 18:16:07 2011	192.168.9.100	1047	208.69.34.136	80	6	94

+ Incoming UDP							
Start Time	End Time	Source IP	Source Port	Destination IP	Destination Port	Count	Bytes
Sat Feb 12 18:16:06 2011	Sat Feb 12 18:16:08 2011	208.67.222.222	53	192.168.9.100	1025	4	286

+ Outgoing UDP							
Start Time	End Time	Source IP	Source Port	Destination IP	Destination Port	Count	Bytes
Sat Feb 12 18:16:06 2011	Sat Feb 12 18:16:08 2011	192.168.9.100	1025	208.67.222.222	53	4	134

+ DNS Queries			
Time Stamp	Queried	For	Answer
Sat Feb 12 18:16:06 2011	208.67.222.222	esbigholtem.com	67.215.65.132
Sat Feb 12 18:16:07 2011	208.67.222.222	guide.opendns.com	208.69.34.136
Sat Feb 12 18:16:08 2011	208.67.222.222	microsoft.com	207.46.197.32, 207.46.232.182
Sat Feb 12 18:16:08 2011	208.67.222.222	www.microsoft.com	toggle.www.ms.akadns.net, g.www.ms.akadns.net, lb1.www.ms.akadns.net, 65.55.12.249

+ HTTP		
+ Incoming		
File	Action	Host
192.168.9.100.1049-65.55.12.249.80	GET / HTTP/1.0	www.microsoft.com
192.168.9.100.1047-208.69.34.136.80	GET /?url=esbigholtem%2Ecom%2Fkx%2Ephp HTTP/1.0	guide.opendns.com
192.168.9.100.1048-207.46.197.32.80	GET / HTTP/1.0	microsoft.com
+ Outgoing		

File	Action	Host