LAMPIRAN

Tabel jumlah file yang diakses oleh *Ransomware*

Nama File	Lokasi File	Action		
		Open	Edit	Create
PetyaFix.exe	HKEY_CLASSES_ROOT\Applications\PetyaFix_2_0_766_127.exe	✓	X	X
OpenWithProgids	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Shell\RegisteredApplications\UrlAssociations\Directory\OpenWithProgids	✓	✓	✓
CurVer	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\CurVer	✓	X	X
ShellEx	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\{00021500-0000-0000-C000-000000000046}	✓	X	X
HideFolderVerbs	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs	✓	✓	X
UseDropHandler	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler	✓	✓	X
WantsFORPARSING	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING	✓	✓	X
WantsParseDisplayName	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName	✓	✓	X
QueryForOverlay	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay	✓	✓	X
MapNetDriveVerbs	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs	✓	✓	X

HideOnDesktopPerUser	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser	✓	✓	X
WantsAliasedNotifications	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications	✓	✓	X
NoFileFolderJunction	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction	✓	✓	X
DriveMask	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask	✓	✓	X
PropertySystem	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\PropertySystem	✓	X	X
àÄÿÿÿ	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Pacific Standard Time\Dynamic DST\2007	✓	✓	X
ReNotifyCount	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\ReNotifyCount	✓	✓	X
DisableProcessIsolation	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\DisableProcessIsolation	✓	✓	X
HideInWebView	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder\HideInWebView	✓	✓	X
.acrobatsecuritysettings	HKEY_CLASSES_ROOT\SystemFileAssociations\.acrobatsecuritysettings	✓	✓	X
WMP11.AssocFile.ADTS	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.ADT\OpenWithProgids\WMP11.AssocFile.ADTS	✓	X	✓
xmlfile	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xml\OpenWithProgids\xmlfile	✓	X	✓

.zfsendtotarget	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xml\OpenWithProgids\xmlfile	✓	X	✓
EnableShareDenyNone	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\EnableShareDenyNone	✓	✓	X

NotPetya

Nama File	**Lokasi File**	**Action**		
		Open	**Edit**	**Create**
.NETFramework	HKEY_CURRENT_USER\Software\Microsoft\.NETFramework	✓	X	X
InstallRoot	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\	✓	✓	✓
Policy	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\	✓	X	X
Policy	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\.NETFramework\Policy\	✓	✓	X
V2.0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\V2.0	✓	X	X
Mscoreei.dll	HKEY_LOCAL_MACHINE\Microsoft.NET\Framework\v2.0.50727	✓	X	✓
Upgrades	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\upgrades	✓	X	X
Upgrades	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\upgrades	✓	✓	X
AppPatch	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\AppPatch	✓	X	X

AppPatch	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\AppPatch	✓	✓	X
CLRLoadLogDir	HKEY_CURRENT_USER\Software\Microsoft\.NETFramework\CLRLoadLogDir	✓	✓	X
OnlyUseLatestCLR	HKEY_CURRENT_USER\Software\Microsoft\.NETFramework\OnlyUseLatestCLR	✓	✓	X
DisableMetaFiles	HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\GRE_Initialize\DisableMetafiles	✓	✓	X

Bad rabbit

Nama File	**Lokasi File**	**Action**		
		Open	**Edit**	**Create**
DisableUNCCheck	HKEY_LOCAL_MACHINE\Software\Microsoft\CommandProcessor	✓	✓	X
EnableExtensions	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CommandProcessor	✓	✓	X
Crypt32	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\	✓	X	X
DebugHeapFlags	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\cryp32	✓	✓	X
UseHostnameAsAlias	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\1dap	✓	✓	X
Fvevolrdyboost	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\LowerFilters	✓	✓	X

Csccfvevolrdyboost	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\LowerFilters	✓	✓	✓
dumpfve.sys	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CrashControl\DumpFilters	✓	✓	X
WinShock_Registry_Version	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\	✓	✓	X
fwpuclnt.dll	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout	✓	✓	X
Next_Catalog_Entry_ID	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\	✓	✓	X
wship6.dll	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem	✓	✓	X
mswsock.dll	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem	✓	✓	X
NLAapi.dll	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath	✓	✓	X
netprofm,netman	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SQMServiceList\SQMServiceList	✓	✓	X
WinSock 2.0 Provider ID	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winsock\Setup Migration\Providers\Psched\	✓	✓	X
wshtcpip.dll	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Winsock\HelperDllName	✓	✓	X
CryptDllDecodeObjectEx	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 1\	✓	X	✓

Web Client Network	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WebClient\NetworkProvider\Name	✓	✓	X
inetcomm.dll	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 1\CryptDllDecodeObjectEx\1.2.840.113549.1.9.16.1.1	✓	X	✓
credssp.dll	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SecurityProviders	✓	✓	X
RegistrationEnabled	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}\	✓	✓	X
WpadExpirationDays	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\	✓	✓	X
cuckoo-PC	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname	✓	✓	X

Wannacry

Nama File	**Lokasi File**	**Action**		
		Open	**Edit**	**Create**
ReNotifyCount	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\ReNotifyCount	✓	✓	X
DocObject	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\DocObject	✓	✓	X
FavoritesRemovedChanges	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartPage\FavoritesRemovedChanges	✓	✓	X
SuppressionPolicy	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\DelegateFolders\{35786D3C-B075-49b9-88DD-029876E11C01}\SuppressionPolicy \	✓	✓	X

ReaderProgramFiles	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\68AB67CA7DA73301B744CAF070E41400\ReaderProgramFiles	✓	✓	X
Acrobat Reader	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1C19FC540809F1F419A3977E0915E33F\68AB67CA7DA73301B744CAF070E41400	✓	✓	X
concrt140.dll	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8F139CF91DE936230A1FA8ED33D0E0EC\68AB67CA7DA73301B744CAF070E41400	✓	✓	X
msvcp140.dll	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C069AA2AC3DFD6A3DBF641390311FA3B\68AB67CA7DA73301B744CAF070E41400	✓	✓	X
MSPUB.EXE	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\92B7D0DC7E985C94E81ED558E8FF5239\00004119110000000000000000F01FEC	✓	✓	X
Microsoft	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\198B04717E873AC47B62DA0307073629\00004119110000000000000000F01FEC	✓	✓	X
b.wnry	C:\Users\cuckoo\AppData\Local\Temp\	✓	X	✓
WanaCrypt0r	HKEY_LOCAL_MACHINE\Software\	✓	X	✓
Disable	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\	✓	✓	X
UseHostnameAsAlias	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ldap\UseHostnameAsAlias	✓	✓	X
CUCKOO-PC	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName	✓	✓	X
SystemSetupInProgress	HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress	✓	✓	X