Process Create:
UtcTime: 2017-05-17 01:48:56.595
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
CommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467
ParentProcessGuid: {687cbaee-aafd-591b-0000-001040ea0600}
ParentProcessId: 3736
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE

File creation time changed:
UtcTime: 2017-05-17 01:48:56.642
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\b.wnry
CreationUtcTime: 2017-05-11 10:13:20.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.626

File creation time changed:
UtcTime: 2017-05-17 01:48:56.642
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\c.wnry
CreationUtcTime: 2017-05-11 10:11:58.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.642

File creation time changed:
UtcTime: 2017-05-17 01:48:56.642
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\msg\m_bulgarian.wnry
CreationUtcTime: 2010-11-19 18:16:58.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.642

and every under MSG folder different language pack

File creation time changed:
UtcTime: 2017-05-17 01:48:56.736
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}

ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\r.wnry
CreationUtcTime: 2017-05-11 05:59:14.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.736

File creation time changed:
UtcTime: 2017-05-17 01:48:57.219
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\s.wnry
CreationUtcTime: 2017-05-09 06:58:44.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.736

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\t.wnry
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.219

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\taskdl.exe
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\taskse.exe
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

File creation time changed:
UtcTime: 2017-05-17 01:48:57.282
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\u.wnry
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

Process Create:
UtcTime: 2017-05-17 01:48:57.282
ProcessGuid: {687cbaee-ac09-591b-0000-0010ad610e00}
ProcessId: 2864
Image: C:\Windows\System32\attrib.exe
CommandLine: attrib +h .
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=C10B6995861DA38E538A1FFD5ACC0BB3FC147A6C
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

Process Create:
UtcTime: 2017-05-17 01:48:57.344
ProcessGuid: {687cbaee-ac09-591b-0000-001075630e00}
ProcessId: 2876
Image: C:\Windows\System32\icacls.exe
CommandLine: icacls . /grant Everyone:F /T /C /Q
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=6141115EE9E600C9FF7C61FCDC555F0F7629F3D5
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

Process terminated:
UtcTime: 2017-05-17 01:48:57.485
ProcessGuid: {687cbaee-ac09-591b-0000-0010ad610e00}
ProcessId: 2864
Image: C:\Windows\System32\attrib.exe

Process Create:
UtcTime: 2017-05-17 01:48:58.935
ProcessGuid: {687cbaee-ac0a-591b-0000-00101e860e00}
ProcessId: 3060
Image: C:\Users\user_name\Desktop\taskdl.exe
CommandLine: taskdl.exe
CurrentDirectory: C:\Users\user_name\Desktop\

User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=47A9AD4125B6BD7C55E4E7DA251E23F089407B8F
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

Process terminated:
UtcTime: 2017-05-17 01:48:58.967
ProcessGuid: {687cbaee-ac0a-591b-0000-00101e860e00}
ProcessId: 3060
Image: C:\Users\user_name\Desktop\taskdl.exe

Process Create:
UtcTime: 2017-05-17 01:48:58.935
ProcessGuid: {687cbaee-ac0a-591b-0000-00101e860e00}
ProcessId: 3060
Image: C:\Users\user_name\Desktop\taskdl.exe
CommandLine: taskdl.exe
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=47A9AD4125B6BD7C55E4E7DA251E23F089407B8F
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

File creation time changed:
UtcTime: 2017-05-17 01:48:59.216
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\321191494985739.bat.WNCRYT
CreationUtcTime: 2017-05-17 01:48:59.154
PreviousCreationUtcTime: 2017-05-17 01:48:59.216

Process Create:
UtcTime: 2017-05-17 01:48:59.154
ProcessGuid: {687cbaee-ac0b-591b-0000-001041880e00}
ProcessId: 3360
Image: C:\Windows\System32\cmd.exe
CommandLine: cmd /c 321191494985739.bat

CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

File creation time changed:
UtcTime: 2017-05-17 01:48:59.450
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt.WNCRYT
CreationUtcTime: 2015-08-11 09:54:54.000
PreviousCreationUtcTime: 2017-05-17 01:48:59.450

File creation time changed:
UtcTime: 2017-05-17 01:48:59.450
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\ProgramData\VMware\VMware Tools\manifest.txt.WNCRYT
CreationUtcTime: 2017-05-16 06:24:35.436
PreviousCreationUtcTime: 2017-05-17 01:48:59.450

Process terminated:
UtcTime: 2017-05-17 01:48:59.372
ProcessGuid: {687cbaee-ac0b-591b-0000-001041880e00}
ProcessId: 3360
Image: C:\Windows\System32\cmd.exe

File creation time changed:
UtcTime: 2017-05-17 01:48:59.419
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\ProgramData\Microsoft\Windows NT\MSScan\WelcomeScan.jpg.WNCRYT
CreationUtcTime: 2009-06-10 21:41:50.875
PreviousCreationUtcTime: 2017-05-17 01:48:59.403

File creation time changed:
UtcTime: 2017-05-17 01:48:56.736
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}

ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\r.wnry
CreationUtcTime: 2017-05-11 05:59:14.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.736

Process Create:
UtcTime: 2017-05-17 01:48:57.282
ProcessGuid: {687cbaee-ac09-591b-0000-0010ad610e00}
ProcessId: 2864
Image: C:\Windows\System32\attrib.exe
CommandLine: attrib +h .
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=C10B6995861DA38E538A1FFD5ACC0BB3FC147A6C
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

File creation time changed:
UtcTime: 2017-05-17 01:48:57.282
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\u.wnry
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

Process Create:
UtcTime: 2017-05-17 01:48:57.344
ProcessGuid: {687cbaee-ac09-591b-0000-001075630e00}
ProcessId: 2876
Image: C:\Windows\System32\icacls.exe
CommandLine: icacls . /grant Everyone:F /T /C /Q
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=6141115EE9E600C9FF7C61FCDC555F0F7629F3D5
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\t.wnry
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.219

File creation time changed:
UtcTime: 2017-05-17 01:48:57.219
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\s.wnry
CreationUtcTime: 2017-05-09 06:58:44.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.736

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\taskse.exe
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\taskdl.exe
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

File creation time changed:
UtcTime: 2017-05-17 01:48:57.219
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\s.wnry
CreationUtcTime: 2017-05-09 06:58:44.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.736

File creation time changed:
UtcTime: 2017-05-17 01:48:57.235
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180

Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\t.wnry
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.219

Process Create:
UtcTime: 2017-05-17 01:48:57.344
ProcessGuid: {687cbaee-ac09-591b-0000-001075630e00}
ProcessId: 2876
Image: C:\Windows\System32\icacls.exe
CommandLine: icacls . /grant Everyone:F /T /C /Q
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=6141115EE9E600C9FF7C61FCDC555F0F7629F3D5
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

File creation time changed:
UtcTime: 2017-05-17 01:48:57.282
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\u.wnry
CreationUtcTime: 2017-05-11 16:22:56.000
PreviousCreationUtcTime: 2017-05-17 01:48:57.235

Process Create:
UtcTime: 2017-05-17 01:48:57.282
ProcessGuid: {687cbaee-ac09-591b-0000-0010ad610e00}
ProcessId: 2864
Image: C:\Windows\System32\attrib.exe
CommandLine: attrib +h .
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=C10B6995861DA38E538A1FFD5ACC0BB3FC147A6C
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"

File creation time changed:
UtcTime: 2017-05-17 01:48:56.736
ProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ProcessId: 1180
Image: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
TargetFilename: C:\Users\user_name\Desktop\r.wnry
CreationUtcTime: 2017-05-11 05:59:14.000
PreviousCreationUtcTime: 2017-05-17 01:48:56.736

Process Create:
UtcTime: 2017-05-17 01:48:59.154
ProcessGuid: {687cbaee-ac0b-591b-0000-001041880e00}
ProcessId: 3360
Image: C:\Windows\System32\cmd.exe
CommandLine: cmd /c 321191494985739.bat
CurrentDirectory: C:\Users\user_name\Desktop\
User: user_name-PC\user_name
LogonGuid: {687cbaee-aafc-591b-0000-0020e1ca0600}
LogonId: 0x6cae1
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5
ParentProcessGuid: {687cbaee-ac08-591b-0000-0010fe4c0e00}
ParentProcessId: 1180
ParentImage: C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE
ParentCommandLine: "C:\Users\user_name\Desktop\wanncry sample.EXE_.EXE"