# Sample: 89782b6cdaaab7848d544255d5fe7002

P3pper Reports - **http://www.peppermalware.com**.

P3pper Twitter - **https://twitter.com/P3pperP0tts**.

This report has been generated automatically by a set of malware analysis tools.



Classification: **#TROJAN #OCCAMY** (based on p3pperp0tts rules)

Analysis date: 2019-03-22 05:12:18 (p3pperp0tts platform's analysis date)

Exe timestamp: 2019-03-18 21:58:40 (timestamp of the original sample)

Unpacked mods max timestamp: 2019-03-18 21:58:40 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2019-03-21 01:17:33 (date of last time that the sample was analyzed at vt)

## Index

## Sample

- md5: 89782b6cdaaab7848d544255d5fe7002

## AV detections

- Microsoft: Trojan:Win32/Occamy.C
- Kaspersky: HEUR:Trojan.MSIL.Steamilik.gen
- Symantec:
- Malwarebytes: Trojan.Downloader

## Source

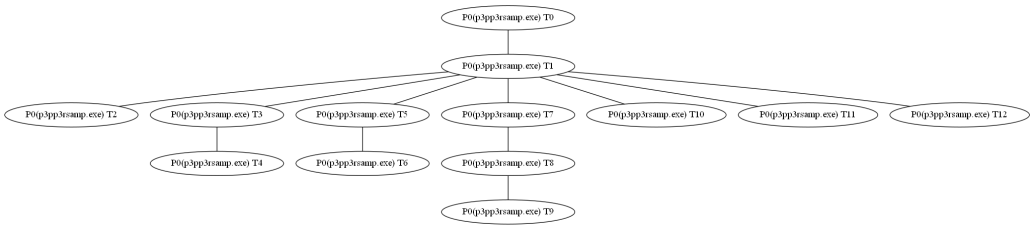
- hxxp://a4.doshimotai.ru/pxpx.exe

## Virustotal

- https://virustotal.com/es/file/ffee8c0daad6b88b91ae8f12c4564a9a7986fc55497cacf09732737893e0c186/analysis

## Threads tree

The following tree represents sample's threads. T<index> is an alias for sample's threads (numeration is done in the order of threads creation). P<index> is an alias for processes owning sample's threads.



## Most interesting behavior

The following list it's a collection of the most interesting events captured. This list is ordered by the score assigned to the event. In the section "Threads behavioural information" it's possible to find all the actions performed by each sample's thread ordered chronologically.

- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32 Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
- RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
- RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\My Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
- RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\AuthRoot Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Root\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Root\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Root\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\SmartCardRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\SmartCardRoot\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\SmartCardRoot\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKCU\\Software\\Classes\\Local Settings\\MuiCache\\32\\52C64B7E\\LanguageList Type: REG_MULTI_SZ, Length: 20, Data: en-US, en)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13\\Blob Type: REG_BINARY, Length: 1.058, Data: 0F 00 00 00 01 00 00 00 14 00 00 00 5B CA A1 C2)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13\\Blob Type: REG_BINARY, Length: 1.086, Data: 04 00 00 00 01 00 00 00 10 00 00 00 41 03 52 DC)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13\\Blob Type: REG_BINARY, Length: 1.114, Data: 19 00 00 00 01 00 00 00 10 00 00 00 6C F2 52 FE)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
• Thread Create ( Thread ID: T1)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: T2)
• Thread Create ( Thread ID: T3)
• Thread Create ( Thread ID: T5)
• RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 )
• Thread Create ( Thread ID: T7)
• Thread Create ( Thread ID: T10)
• Thread Create ( Thread ID: T11)

- Thread Create ( Thread ID: T12)
- Thread Create ( Thread ID: T4)
- Thread Create ( Thread ID: T6)
- Thread Create ( Thread ID: T8)
- Thread Create ( Thread ID: T9)

## Most interesting strings

The following list it's a collection of the most interesting strings found in the sample's modules (unpacked modules too) code or data.

- zz5lBmwx9D3NLGq/xMMPxpTGQ8fkUUSnPOASueqbeWVGZ+n+MJKwkpAMYKsbjHRFYnujxg/txKoblGygMK22JPnHSS9/jKvZz4aPuldclA==
- 0D5rpAWW/dbJ/p/kZGCCuXJPB8f+aSa2pPIQJnBMIOFJJLQNUtulcn/dHMJvjAwg0Gt+/BvrL8GjzB9/w95P9iWrNv/nHBh9zPpnfKz+4Q==
- !This program cannot be run in DOS mode.
- ToBase64String
- X2OK3wWBoz1EVMppHGRg7pW6HZHn1p9wVj8XJkp+4RtcYOsNTCx97n8Fmp0bFKJxrNTgkD+yXPXR7TUVzNcJv+6554ass9WnnEpyQ/IaqrG2Aw==
- WrapNonExceptionThrows
- m_DictionarySizeCheck
- SetLiteralProperties
- RuntimeHelpers
- get_CurrentDomain
- OriginalFilename
- ReverseDecode
- ReleaseStream
- StringFileInfo
- m_IsRep0LongDecoders
- m_PosSlotDecoder
- GetParameters
- GetEntryAssembly
- add_AssemblyResolve
- m_LenDecoder
- m_RepLenDecoder
- NumBitLevels
- SetDecoderProperties
- VS_VERSION_INFO
- m_PosAlignDecoder
- m_PosDecoders
- GCHandleType
- zz5lBmwx9D3NLGq/xMMPxpTG/El03eSgXuumPxU37p8VqrD+MJKwVGB7B+xsRaI15TKbifxCbdyk4FChjuwTWVshg3yZPbmat4YXBIQ=
- m_RangeDecoder
- BitTreeDecoder
- m_IsRepG0Decoders
- m_LiteralDecoder
- ResolveSignature
- get_FullName
- ParameterInfo
- 6z75VNea9KHNLDcVGmuVuR0pEvQMoLKRKv0zqzZ14frwqiL+MFQgna8sHC0ONYXuLWssWgPsvKBwc6KcXysJvwnENYGzApGa/3yE
- AssemblyName
- m_IsRepG2Decoders
- DecodeNormal
- GetManifestResourceStream
- m_PosStateMask
- GetExecutingAssembly
- m_IsRepG1Decoders
- LegalCopyright
- get_ManifestModule
- ResolveEventArgs
- m_IsMatchDecoders
- zz5lBmwx9D3NLGq/xMMPxpTGipHNW08zdOsEP7wgdvfaSUH3TuM5kpDeEL7QbCDTvbQsiXZduXaHcxRKJ+wkYFDxNmQPhRdXC6S1qac2y4LP5MQ=
- System.Runtime.CompilerServices
- ResolveEventHandler
- MemoryStream

- SetPosBitsProperties
- m_IsRepDecoders
- LiteralDecoder
- GetCurrentProcess
- InternalName
- m_NumPosStates
- Symantec Application
- System.Runtime.InteropServices
- CheckRemoteDebuggerPresent

## Hosts

- 185.181.9.115:2012
- a130-208-19-137.deploy.akamaitechnologies.com:http
- a130-208-19-138.deploy.akamaitechnologies.com:http
- apps.digsigtrust.com:http
- ec2-54-243-147-226.compute-1.amazonaws.com:http
- srv109-h-st.jino.ru:https
- 185.181.9.115:2012
- 192.168.149.226:49159
- 192.168.149.226:49160
- 192.168.149.226:49162
- 192.168.149.226:49166
- 192.35.177.64:80
- 54.243.147.226:80
- 81.177.141.23:443 (domekan.ru)

## Dns queries

- isatap.localdomain ---> no answers
- 254.149.168.192.in-addr.arpa ---> no answers
- domekan.ru ---> 81.177.141.23
- 23.141.177.81.in-addr.arpa ---> no answers

## Network traffic

This section contains the readable content of the captured network traffic classified by established connections.

- **tcp 81.177.141.23 (domekan.ru) :443 ---> 192.168.149.226:49159**

  Let\'s Encrypt1#0![...]www.domekan.ru0L[...]"http://cps.root-x1.letsencrypt.org0<[...]190128163103Z[...]DST Root CA X30[...]&http;://isrg.trustid.ocsp.identrust.com0;[...]160317164046Z[...]190428163103Z0[...]+http://crl.identrust.com/DSTROOTCAX3CRL.crl0[...]"http://ocsp.int-x3.letsencrypt.org0/[...]/http://apps.identrust.com/roots/dstrootcax3.p7c0[...]http://cps.letsencrypt.org0[...]#http://cert.int-x3.letsencrypt.org/0%[...]210317164046Z0J1[...]Digital Signature Trust Co.1[...]Let\'s Encrypt Authority X30

- **tcp 192.168.149.226:49160 ---> 192.35.177.64:80**

  GET /roots/dstrootcax3.p7c HTTP/1.1[...]Connection: Keep-Alive[...]User-Agent: Microsoft-CryptoAPI/6.1[...]Host: apps.identrust.com

- **tcp 192.35.177.64:80 ---> 192.168.149.226:49160**

  210930140115Z0?1$0"[...]DST Root CA X30[...]Date: Thu, 21 Mar 2019 12:53:50 GMT[...]Content-Type: application/x-pkcs7-mime[...]000930211219Z[...]Cache-control: max-age=86400[...]HTTP/1.1 200 OK[...]Content-Length: 893[...]Accept-Ranges: bytes[...]X-Frame-Options: SAMEORIGIN[...]HTTP/1.1 200 OK[...]Last-Modified: Fri, 19 Oct 2012 20:08:11 GMT[...]X-XSS-Protection: 1; mode=block[...]Server: Apache[...]Digital Signature Trust Co.1

- **tcp 192.168.149.226:49162 ---> 185.181.9.115:2012**

  Origin: ws://185.181.9.115:2012[...]Sec-WebSocket-Key: ZWQyZjQ5MzgtY2U2NC00NQ==[...]5 Ep6^$vP>"`0}[...]>?W;8Dp6^$vP>":[...]?7;8Dp6^$vP>":[...]5 Ep6^$vP>"L([...]Connection: Upgrade[...]Upgrade: websocket[...]GET /websocket HTTP/1.1[...]w_bDp6^$vP>"[...]Pc0Gt\t`_$vP>"[...]Sec-WebSocket-Version: 13[...]Q;$p07T8iM$p>[...]Host: 185.181.9.115:2012[...]nj7=4>z0>$}yv`"0>!p0>\'p88$p0E

- **tcp 185.181.9.115:2012 ---> 192.168.149.226:49162**

  Upgrade: websocket[...]Sec-WebSocket-Accept: Tt44rh/w81Z7ulnl1qKo1ZcDMC8=[...]HTTP/1.1 101 Switching Protocols[...]HTTP/1.1 101 Switching Protocols[...]Connection: Upgrade

- **tcp 192.168.149.226:49166 ---> 54.243.147.226:80**

  Host: api.ipify.org[...]Connection: Keep-Alive[...]GET / HTTP/1.1

- **tcp 54.243.147.226:80 ---> 192.168.149.226:49166**

  Vary: Origin[...]Content-Type: text/plain[...]Content-Length: 14[...]Date: Fri, 22 Mar 2019 03:56:40 GMT[...]82.221.114.154[...]Via: 1.1 vegur[...]82.221.114.154HTTP/1.1 200 OK[...]HTTP/1.1 200 OK[...]Server: Cowboy[...]Connection: Keep-Alive

## Full strings list

The following list it's a collection of all the strings found in the sample's modules (unpacked modules too) code or data.

- zz5lBmwx9D3NLGq/xMMPxpTGQ8fkUUSnPOASueqbeWVGZ+n+MJKwkpAMYKsbjHRFYnujxg/txKoblGygMK22JPnHSS9/jKvZz4aPuldclA==
- 0D5rpAWW/dbJ/p/kZGCCuXJPB8f+aSa2pPIQJnBMIOFJJLQNUtulcn/dHMJvjAwg0Gt+/BvrL8GjzB9/w95P9iWrNv/nHBh9zPpnfKz+4Q==
- !This program cannot be run in DOS mode.
- ToBase64String
- X2OK3wWBoz1EVMppHGRg7pW6HZHn1p9wVj8XJkp+4RtcYOsNTCx97n8Fmp0bFKJxrNTgkD+yXPXR7TUVzNcJv+6554ass9WnnEpyQ/IaqrG2Aw==
- WrapNonExceptionThrows
- m_DictionarySizeCheck
- SetLiteralProperties
- RuntimeHelpers
- get_CurrentDomain
- OriginalFilename
- ReverseDecode
- ReleaseStream
- StringFileInfo
- m_IsRep0LongDecoders
- m_PosSlotDecoder
- GetParameters
- GetEntryAssembly
- add_AssemblyResolve
- m_LenDecoder
- m_RepLenDecoder
- NumBitLevels
- SetDecoderProperties
- VS_VERSION_INFO
- m_PosAlignDecoder
- m_PosDecoders
- GCHandleType
- zz5lBmwx9D3NLGq/xMMPxpTG/El03eSgXuumPxU37p8VqrD+MJKwVGB7B+xsRaI15TKbifxCbdyk4FChjuwTWVshg3yZPbmat4YXBIQ=
- m_RangeDecoder
- BitTreeDecoder
- m_IsRepG0Decoders
- m_LiteralDecoder
- ResolveSignature
- get_FullName
- ParameterInfo
- 6z75VNea9KHNLDcVGmuVuR0pEvQMoLKRKv0zqzZ14frwqiL+MFQgna8sHC0ONYXuLWssWgPsvKBwc6KcXysJvwnENYGzApGa/3yE
- AssemblyName
- m_IsRepG2Decoders
- DecodeNormal
- GetManifestResourceStream
- m_PosStateMask
- GetExecutingAssembly
- m_IsRepG1Decoders
- LegalCopyright
- get_ManifestModule
- ResolveEventArgs
- m_IsMatchDecoders
- zz5lBmwx9D3NLGq/xMMPxpTGipHNW08zdOsEP7wgdvfaSUH3TuM5kpDeEL7QbCDTvbQsiXZduXaHcxRKJ+wkYFDxNmQPhRdXC6S1qac2y4LP5MQ=
- System.Runtime.CompilerServices
- ResolveEventHandler
- MemoryStream

- SetPosBitsProperties
- m_IsRepDecoders
- LiteralDecoder
- GetCurrentProcess
- InternalName
- m_NumPosStates
- Symantec Application
- System.Runtime.InteropServices
- CheckRemoteDebuggerPresent
- m_NumPrevBits
- X5uNoysciD0qzRacYHIPWoN94b6FDfpwVtDa8LwgU6f8vO2CReO+2690Rrn0bCBQvT40zYmzIcXciVvRYlV674xc
- m_DictionarySize
- AssemblyCompanyAttribute
- ConfuserEx v1.0.0-33-ga1d8d38
- AssemblyDescriptionAttribute
- UpdateShortRep
- ResolveMethod
- AssemblyProductAttribute
- ToUpperInvariant
- RuntimeCompatibilityAttribute
- FileDescription
- RuntimeFieldHandle
- SetDictionarySize
- InitializeArray
- AssemblyTitleAttribute
- BBI99B56<339**1((,$$(
- DecodeDirectBits
- zz5lBmwx9D3NLGoPGGt2uYTR4WTNnJH8oErHWlehn1rRAz6wLtCe0MQggS30FF2yLYPyOT+0ao0EtCAQMzKEi9Mv5+uMmRdX6rH6N4Rc
- System.Reflection
- kernel32.dll
- GetLenToPosState
- P+^I,N0PZ=e$E
- DecodeWithMatchByte
- System.Diagnostics
- STAThreadAttribute
- m_NumPosBits
- r''s((r))o//o55o55n77l??mCCnCCmGGlOOmQQmQQmWWn^^n
- ConfusedByAttribute
- CompilationRelaxationsAttribute
- XmOTpAWa6zeOdGqSccVqXCAOy+KLxWVWmT9GJnB+MPrwxCDLVTT0y9ZN/94rRXSyCbRUoPDtmtzztVvRz7T18TW2DzlQV9S80tlydgYtOhefD2w=
- LXJx\\=/a4;/b
- QQdQQcQQbQQaQQ`QQ_
- e9OQGUYxxwtPzTxGwcQbuS7ky76fxVqRPOASueqbeWVGZ7D+MdCe0KqwZCDNRSwUvS6bEWpd8UQmZ4z84NDXJozVcYGzfySF4dn6r6fhLxcy09HmDcPGcDBXEfE=

## Threads behaviour

In this section it's possible to find information about sample's threads, such as the actions performed by each sample's thread ordered chronologically.

- **Thread T0 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T1 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create ( Thread ID: T1)
- **Thread T1 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T2 (in process P0, p3pp3rsamp.exe)
    - Thread T3 (in process P0, p3pp3rsamp.exe)
    - Thread T5 (in process P0, p3pp3rsamp.exe)
    - Thread T7 (in process P0, p3pp3rsamp.exe)
    - Thread T10 (in process P0, p3pp3rsamp.exe)
    - Thread T11 (in process P0, p3pp3rsamp.exe)
    - Thread T12 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: T2)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32 Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
    - RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASAPI32\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
    - RegCreateKey (HKLM\\Software\\Microsoft\\Tracing Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\Software\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS Desired Access: Read, Set Value, Disposition: REG_CREATED_NEW_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableFileTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\EnableConsoleTracing Type: REG_DWORD, Length: 4, Data: 0)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\ConsoleTracingMask Type: REG_DWORD, Length: 4, Data: 4294901760)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\MaxFileSize Type: REG_DWORD, Length: 4, Data: 1048576)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Tracing\\p3pp3rsamp_RASMANCS\\FileDirectory Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\\tracing)
• Thread Create ( Thread ID: T3)
• Thread Create ( Thread ID: T5)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\My Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\CA Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\CA\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\CA\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\CA\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\Disallowed Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Disallowed\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Disallowed\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Disallowed\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\Root\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\AuthRoot Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Root\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Root\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\Root\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\Root Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\SmartCardRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\SmartCardRoot\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\SmartCardRoot\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\SmartCardRoot\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\TrustedPeople Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\TrustedPeople\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\TrustedPeople\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\TrustedPeople\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKCU\\Software\\Policies\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Policies\\Microsoft\\SystemCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)

• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Policies\\Microsoft\\SystemCertificates\\trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\Software\\Microsoft\\EnterpriseCertificates\\trust Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Trust\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Trust\\CRLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Trust\\CTLs Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKCU\\Software\\Classes\\Local Settings\\MuiCache\\32\\52C64B7E\\LanguageList Type: REG_MULTI_SZ, Length: 20, Data: en-US, en)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 )
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13\\Blob Type: REG_BINARY, Length: 1.058, Data: 0F 00 00 00 01 00 00 00 14 00 00 00 5B CA A1 C2)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 )
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13\\Blob Type: REG_BINARY, Length: 1.086, Data: 04 00 00 00 01 00 00 00 10 00 00 00 41 03 52 DC)
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegDeleteValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 )
• RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13 Desired Access: Read/Write, Delete, Disposition: REG_OPENED_EXISTING_KEY)
• RegSetValue (HKLM\\SOFTWARE\\Microsoft\\SystemCertificates\\AuthRoot\\Certificates\\DAC9024F54D8F6DF94935FB1732638CA6AD77C13\\Blob Type: REG_BINARY, Length: 1.114, Data: 19 00 00 00 01 00 00 00 10 00 00 00 6C F2 52 FE)
• Thread Create ( Thread ID: T7)
• Thread Create ( Thread ID: T10)
• Thread Create ( Thread ID: T11)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: T12)
• Thread Create ( Thread ID: TUNKALIAS)
• Thread Create ( Thread ID: TUNKALIAS)

- **Thread T2 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
- **Thread T3 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T4 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create ( Thread ID: T4)
- **Thread T4 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
- **Thread T5 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T6 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create ( Thread ID: T6)
    - Thread Create ( Thread ID: TUNKALIAS)
- **Thread T6 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)

- **Thread T7 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T8 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: T8)
- **Thread T8 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - Thread T9 (in process P0, p3pp3rsamp.exe)
  - **Thread' events**
    - Thread Create ( Thread ID: T9)
- **Thread T9 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
- **Thread T10 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
    - Thread Create ( Thread ID: TUNKALIAS)
- **Thread T11 (in process P0, p3pp3rsamp.exe) description**

- **Thread's childs**
  - No childs found
- **Thread' events**
  - Thread Create ( Thread ID: TUNKALIAS)
  - Thread Create ( Thread ID: TUNKALIAS)

- **Thread T12 (in process P0, p3pp3rsamp.exe) description**
  - **Thread's childs**
    - No childs found
  - **Thread' events**
    - Thread Create ( Thread ID: TUNKALIAS)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG_OPENED_EXISTING_KEY)
    - RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY)
    - Thread Create ( Thread ID: TUNKALIAS)

## Network by processes

The analysis environment tries to capture and collect network actions performed by sample's threads.

### Process P0 (p3pp3rsamp.exe)'s network events

- TCP Connect (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (114))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (5))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (1321))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (1326))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (359))
- TCP Send (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (134))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (5))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (54))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (37))
- TCP Connect (P3PP3R-PC.localdomain:dynport-> apps.digsigtrust.com:http (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> apps.digsigtrust.com:http (139))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> apps.digsigtrust.com:http (1186))
- TCP Send (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (117))
- TCP Disconnect (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (0))
- TCP Connect (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (146))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (5))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (140))
- TCP Send (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (176))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (5))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (304))
- TCP Connect (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (199))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (129))
- TCP Send (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (264))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (260))
- TCP Disconnect (P3PP3R-PC.localdomain:dynport-> srv109-h-st.jino.ru:https (0))
- TCP Reconnect (P3PP3R-PC.localdomain:dynport-> a130-208-19-138.deploy.akamaitechnologies.com:http (0))
- TCP Reconnect (P3PP3R-PC.localdomain:dynport-> a130-208-19-138.deploy.akamaitechnologies.com:http (0))
- TCP Reconnect (P3PP3R-PC.localdomain:dynport-> a130-208-19-137.deploy.akamaitechnologies.com:http (0))
- TCP Reconnect (P3PP3R-PC.localdomain:dynport-> a130-208-19-137.deploy.akamaitechnologies.com:http (0))
- TCP Connect (P3PP3R-PC.localdomain:dynport-> ec2-54-243-147-226.compute-1.amazonaws.com:http (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> ec2-54-243-147-226.compute-1.amazonaws.com:http (63))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> ec2-54-243-147-226.compute-1.amazonaws.com:http (186))
- TCP Send (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (81098))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (0))
- TCP Disconnect (P3PP3R-PC.localdomain:dynport-> 185.181.9.115:2012 (0))
- TCP Disconnect (P3PP3R-PC.localdomain:dynport-> ec2-54-243-147-226.compute-1.amazonaws.com:http (0))

## Unpacked or injected modules

In this section it's possible to find information about sample's modules, such as the rich signatures and strings

- **Module 1 (probably unpacked / injected by the sample)**
  - **Module 1 rich signatures**
    - No rich signatures found
  - **Module 1 strings**
    - **Module 1 most interesting strings**
      - zz5lBmwx9D3NLGq/xMMPxpTGQ8fkUUSnPOASueqbeWVGZ+n+MJKwkpAMYKsbjHRFYnujxg/txKoblGygMK22JPnHSS9/jKvZz4aPuldclA==
      - 0D5rpAWW/dbJ/p/kZGCCuXJPB8f+aSa2pPIQJnBMIOFJJLQNUtulcn/dHMJvjAwg0Gt+/BvrL8GjzB9/w95P9iWrNv/nHBh9zPpnfKz+4Q==
      - !This program cannot be run in DOS mode.
      - ToBase64String
      - X2OK3wWBoz1EVMppHGRg7pW6HZHn1p9wVj8XJkp+4RtcYOsNTCx97n8Fmp0bFKJxrNTgkD+yXPXR7TUVzNcJv+6554ass9WnnEpyQ/IaqrG2Aw==
      - WrapNonExceptionThrows
      - m_DictionarySizeCheck
      - SetLiteralProperties
      - RuntimeHelpers
      - get_CurrentDomain
      - OriginalFilename
      - ReverseDecode
      - ReleaseStream
      - StringFileInfo
      - m_IsRep0LongDecoders
      - m_PosSlotDecoder
      - GetParameters
      - GetEntryAssembly
      - add_AssemblyResolve
      - m_LenDecoder
      - m_RepLenDecoder
      - NumBitLevels
      - SetDecoderProperties
      - VS_VERSION_INFO
      - m_PosAlignDecoder
      - m_PosDecoders
      - GCHandleType
      - zz5lBmwx9D3NLGq/xMMPxpTG/El03eSgXuumPxU37p8VqrD+MJKwVGB7B+xsRaI15TKbifxCbdyk4FChjuwTWVshg3yZPbmat4YXBIQ=
      - m_RangeDecoder
      - BitTreeDecoder
      - m_IsRepG0Decoders
      - m_LiteralDecoder
      - ResolveSignature
      - get_FullName
      - ParameterInfo
      - 6z75VNea9KHNLDcVGmuVuR0pEvQMoLKRKv0zqzZ14frwqiL+MFQgna8sHC0ONYXuLWssWgPsvKBwc6KcXysJvwnENYGzApGa/3yE
      - AssemblyName
      - m_IsRepG2Decoders
      - DecodeNormal
      - GetManifestResourceStream
      - m_PosStateMask

- GetExecutingAssembly
- m_IsRepG1Decoders
- LegalCopyright
- get_ManifestModule
- ResolveEventArgs
- m_IsMatchDecoders
- zz5lBmwx9D3NLGq/xMMPxpTGipHNW08zdOsEP7wgdvfaSUH3TuM5kpDeEL7QbCDTvbQsiXZduXaHcxRKJ+wkYFDxNmQPhRdXC6S1qac2y4LP5MQ=
- System.Runtime.CompilerServices
- ResolveEventHandler
- MemoryStream
- SetPosBitsProperties
- m_IsRepDecoders
- LiteralDecoder
- GetCurrentProcess
- InternalName
- m_NumPosStates
- Symantec Application
- System.Runtime.InteropServices
- CheckRemoteDebuggerPresent

- **Module 1 other strings**

- m_NumPrevBits
- X5uNoysciD0qzRacYHIPWoN94b6FDfpwVtDa8LwgU6f8vO2CReO+2690Rrn0bCBQvT40zYmzIcXciVvRYlV674xc
- m_DictionarySize
- AssemblyCompanyAttribute
- ConfuserEx v1.0.0-33-ga1d8d38
- AssemblyDescriptionAttribute
- UpdateShortRep
- ResolveMethod
- AssemblyProductAttribute
- ToUpperInvariant
- RuntimeCompatibilityAttribute
- FileDescription
- RuntimeFieldHandle
- SetDictionarySize
- InitializeArray
- AssemblyTitleAttribute
- BBI99B56<339**1((,$$(
- DecodeDirectBits
- zz5lBmwx9D3NLGoPGGt2uYTR4WTNnJH8oErHWlehn1rRAz6wLtCe0MQggS30FF2yLYPyOT+0ao0EtCAQMzKEi9Mv5+uMmRdX6rH6N4Rc
- System.Reflection
- kernel32.dll
- GetLenToPosState
- P+^I,N0PZ=e$E
- DecodeWithMatchByte
- System.Diagnostics
- STAThreadAttribute
- m_NumPosBits
- r''s((r))o//o55o55n77l??mCCnCCmGGlOOmQQmQQmWWn^^n
- ConfusedByAttribute
- CompilationRelaxationsAttribute
- XmOTpAWa6zeOdGqSccVqXCAOy+KLxWVWmT9GJnB+MPrwxCDLVTT0y9ZN/94rRXSyCbRUoPDtmtzztVvRz7T18TW2DzlQV9S80tlydgYtOhefD2w=
- LXJx\\=/a4;/b
- QQdQQcQQbQQaQQ`QQ_

- e9OQGUYxxwtPzTxGwcQbuS7ky76fxVqRPOASueqbeWVGZ7D+MdCe0KqwZCDNRSwUvS6bEWpd8UQmZ4z84NDXJozVcYGzfySF4dn6r6fhLxcy09HmDcPGcDBXEfE=

## Module 2 (probably unpacked / injected by the sample)

### Module 2 rich signatures

- No rich signatures found

### Module 2 strings

#### Module 2 most interesting strings

- zz5lBmwx9D3NLGq/xMMPxpTGQ8fkUUSnPOASueqbeWVGZ+n+MJKwkpAMYKsbjHRFYnujxg/txKoblGygMK22JPnHSS9/jKvZz4aPuldclA==
- 0D5rpAWW/dbJ/p/kZGCCuXJPB8f+aSa2pPIQJnBMIOFJJLQNUtulcn/dHMJvjAwg0Gt+/BvrL8GjzB9/w95P9iWrNv/nHBh9zPpnfKz+4Q==
- !This program cannot be run in DOS mode.
- ToBase64String
- X2OK3wWBoz1EVMppHGRg7pW6HZHn1p9wVj8XJkp+4RtcYOsNTCx97n8Fmp0bFKJxrNTgkD+yXPXR7TUVzNcJv+6554ass9WnnEpyQ/IaqrG2Aw==
- WrapNonExceptionThrows
- m_DictionarySizeCheck
- SetLiteralProperties
- RuntimeHelpers
- get_CurrentDomain
- OriginalFilename
- ReverseDecode
- ReleaseStream
- StringFileInfo
- m_IsRep0LongDecoders
- m_PosSlotDecoder
- GetParameters
- GetEntryAssembly
- add_AssemblyResolve
- m_LenDecoder
- m_RepLenDecoder
- NumBitLevels
- SetDecoderProperties
- VS_VERSION_INFO
- m_PosAlignDecoder
- m_PosDecoders
- GCHandleType
- zz5lBmwx9D3NLGq/xMMPxpTG/El03eSgXuumPxU37p8VqrD+MJKwVGB7B+xsRaI15TKbifxCbdyk4FChjuwTWVshg3yZPbmat4YXBIQ=
- m_RangeDecoder
- BitTreeDecoder
- m_IsRepG0Decoders
- m_LiteralDecoder
- ResolveSignature
- get_FullName
- ParameterInfo
- 6z75VNea9KHNLDcVGmuVuR0pEvQMoLKRKv0zqzZ14frwqiL+MFQgna8sHC0ONYXuLWssWgPsvKBwc6KcXysJvwnENYGzApGa/3yE
- AssemblyName
- m_IsRepG2Decoders
- DecodeNormal
- GetManifestResourceStream
- m_PosStateMask
- GetExecutingAssembly

- m_IsRepG1Decoders
- LegalCopyright
- get_ManifestModule
- ResolveEventArgs
- m_IsMatchDecoders
- zz5lBmwx9D3NLGq/xMMPxpTGipHNW08zdOsEP7wgdvfaSUH3TuM5kpDeEL7QbCDTvbQsiXZduXaHcxRKJ+wkYFDxNmQPhRdXC6S1qac2y4LP5MQ=
- System.Runtime.CompilerServices
- ResolveEventHandler
- MemoryStream
- SetPosBitsProperties
- m_IsRepDecoders
- LiteralDecoder
- GetCurrentProcess
- InternalName
- m_NumPosStates
- Symantec Application
- System.Runtime.InteropServices
- CheckRemoteDebuggerPresent

- **Module 2 other strings**

- m_NumPrevBits
- X5uNoysciD0qzRacYHIPWoN94b6FDfpwVtDa8LwgU6f8vO2CReO+2690Rrn0bCBQvT40zYmzIcXciVvRYlV674xc
- m_DictionarySize
- AssemblyCompanyAttribute
- ConfuserEx v1.0.0-33-ga1d8d38
- AssemblyDescriptionAttribute
- UpdateShortRep
- ResolveMethod
- AssemblyProductAttribute
- ToUpperInvariant
- RuntimeCompatibilityAttribute
- FileDescription
- RuntimeFieldHandle
- SetDictionarySize
- InitializeArray
- AssemblyTitleAttribute
- BBI99B56<339**1((,$$(
- DecodeDirectBits
- zz5lBmwx9D3NLGoPGGt2uYTR4WTNnJH8oErHWlehn1rRAz6wLtCe0MQggS30FF2yLYPyOT+0ao0EtCAQMzKEi9Mv5+uMmRdX6rH6N4Rc
- System.Reflection
- kernel32.dll
- GetLenToPosState
- P+^I,N0PZ=e$E
- DecodeWithMatchByte
- System.Diagnostics
- STAThreadAttribute
- m_NumPosBits
- r''s((r))o//o55o55n77l??mCCnCCmGGlOOmQQmQQmWWn^^n
- ConfusedByAttribute
- CompilationRelaxationsAttribute
- XmOTpAWa6zeOdGqSccVqXCAOy+KLxWVWmT9GJnB+MPrwxCDLVTT0y9ZN/94rRXSyCbRUoPDtmtzztVvRz7T18TW2DzlQV9S80tlydgYtOhefD2w=
- LXJx\\=/a4;/b
- QQdQQcQQbQQaQQ`QQ_
- e9OQGUYxxwtPzTxGwcQbuS7ky76fxVqRPOASueqbeWVGZ7D+MdCe0KqwZCDNRSwUvS6bEWpd8UQmZ4z84NDXJozVcYGzfySF4dn6r6fhLxcy09HmDcPGcDBXEfE=

## Extra Information Recovered

In this section there is additional information recovered by platform plugins

## Configs Recovered

In this section there are malware configs recovered by platform plugins