

This is Google's cache of <http://www.threatexpert.com/report.aspx?md5=ce0296e2d77ec3bb112e270fc260f274>. It is a snapshot of the page as it appeared on Jan 8, 2014 02:13:06 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

[Text-only version](#)



ThreatExpert

Visit ThreatExpert web site | Close Report

Submission Summary:

Submission details:

- ▶ Submission received: 18 December 2013, 16:08:11
- ▶ Processing time: 5 min 50 sec
- ▶ Submitted sample:
 - ↳ File MD5: 0xCE0296E2D77EC3BB112E270FC260F274
 - ↳ File SHA-1: 0x8A6AF8587ADF0E743871AD6B9889428B5F75B86B
 - ↳ Filesize: 270,336 bytes

Summary of the findings:

What's been found	Severity Level
Downloads/requests other files from Internet.	<div style="width: 10px; height: 10px; background-color: yellow; border: 1px solid gray;"></div>

Technical Details:



Memory Modifications

There was a new process created in the system:

Process Name	Process Filename	Main Module Size
[filename of the sample #1]	[file and pathname of the sample #1]	278,528 bytes

There was a new service created in the system:

Service Name	Display Name	Status	Service Filename
POSWDS	POSWDS	"Running"	[file and pathname of the sample #1]



Registry Modifications

- The following Registry Keys were created:
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS\0000
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS\0000\Control
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\POSWDS
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\POSWDS\Security
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\POSWDS\Enum
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\Control
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\Security
 - ▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\Enum
- The newly created Registry Values are:
 - ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS\0000\Control]
 - └─ *NewlyCreated* = 0x00000000
 - └─ ActiveService = "POSWDS"
 - ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS\0000]
 - └─ Service = "POSWDS"
 - └─ Legacy = 0x00000001
 - └─ ConfigFlags = 0x00000000
 - └─ Class = "LegacyDriver"
 - └─ ClassGUID = "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
 - └─ DeviceDesc = "POSWDS"
 - ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS]
 - └─ NextInstance = 0x00000001

- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\POSWDS\Enum]
 - └─ 0 = "Root\LEGACY_POSWDS\0000"
 - └─ Count = 0x00000001
 - └─ NextInstance = 0x00000001
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\POSWDS\Security]
 - └─ Security = 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00 00 00 00 00 05 12 00 00 00 00 18 00 FF 01 0F 0
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\POSWDS]
 - └─ Type = 0x00000110
 - └─ Start = 0x00000002
 - └─ ErrorControl = 0x00000000
 - └─ ImagePath = "[file and pathname of the sample #1]"
 - └─ DisplayName = "POSWDS"
 - └─ ObjectName = "LocalSystem"
 - └─ FailureActions = FF FF FF FF 01 00 00 00 01 00 00 00 03 00 00 00 74 00 6D 00 01 00 00 00 A0 86 01 00 01 00 00 00 A0 86 01 00 01 00 00 00 A0 86 01 00
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000\Control]
 - └─ *NewlyCreated* = 0x00000000
 - └─ ActiveService = "POSWDS"
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS\0000]
 - └─ Service = "POSWDS"
 - └─ Legacy = 0x00000001
 - └─ ConfigFlags = 0x00000000
 - └─ Class = "LegacyDriver"
 - └─ ClassGUID = "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
 - └─ DeviceDesc = "POSWDS"
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_POSWDS]
 - └─ NextInstance = 0x00000001
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\Enum]
 - └─ 0 = "Root\LEGACY_POSWDS\0000"
 - └─ Count = 0x00000001
 - └─ NextInstance = 0x00000001
- ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS\Security]

- Security = 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00 00 00 00 00 05 12 00 00 00 00 18 00 FF 01 0F 0
 - ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\POSWDS]
 - ┌ Type = 0x00000110
 - ┌ Start = 0x00000002
 - ┌ ErrorControl = 0x00000000
 - ┌ ImagePath = "[file and pathname of the sample #1]"
 - ┌ DisplayName = "POSWDS"
 - ┌ ObjectName = "LocalSystem"
 - ┌ FailureActions = FF FF FF FF 01 00 00 00 01 00 00 00 03 00 00 00 74 00 6D 00 01 00 00 00 A0 86 01 00 01 00 00 00 A0 86 01 00 01 00 00 00 A0 86 01 00
 - ▶ [HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
 - ┌ ProxyEnable = 0x00000000
- The following Registry Values were modified:
 - ▶ [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ServiceCurrent]
 - ┌ (Default) =
 - ▶ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceCurrent]
 - ┌ (Default) =



Other details

- The following Internet Connection was established:

Server Name	Server Port	Connect as User	Connection Password
10.116.240.31	80	10.116.240.31	10.116.240.31

- The following Network Connection was requested:

Remote Name	Resource Type	Local Resource to Map	Connect as User	Connection Password
\\10.116.240.31\c\$\WINDOWS\twain_32	RESOURCETYPE_DISK	S:	ttcopscli3acs\Best1_user	BackupU\$r

All content ("Information") contained in this report is the copyrighted work of Threat Expert Ltd and its associated companies ("ThreatExpert") and may not be copied without the express permission of ThreatExpert.

The Information is provided on an "as is" basis. ThreatExpert disclaims all warranties, whether express or implied, to the maximum extent permitted by law, including the implied warranties that the Information is merchantable, of satisfactory quality, accurate, fit for a particular purpose or need, or non-infringing, unless such implied warranties are legally incapable of exclusion. Further, ThreatExpert does not warrant or make any representations regarding the use or the results of the use of the Information in terms of their correctness, accuracy, reliability, or otherwise.

Copyright © 2014 ThreatExpert. All rights reserved.