Outpost24

Vulnerability Management made easy

O24AUTH

Version: 1.1
2019-01-23

Table of Contents

About This Document

The main purpose of this document is to provide the users an overview of O24AUTH.

For support information, visit https://outpost24.com/support

Copyright

Trademark

1 Introduction

O24AUTH is a short-lived service initiated by the scanner on the target machine while performing an authenticated scan against a windows host.

2 Purpose

It is created to make sure that the target does not kill the process or report it internally.

3 Behavior

This service listens on a named pipe/socket to execute commands on the target sent by the scanner and reports the results. It is removed automatically after the scan is done.

***Caution**: Do not remove O24AUTH while a scan is running.*

3.1 List of Commands

Cmdlets	Function
`Test-Path`	To check if file exists
`New-PSDrive`	Create temporary power-shell drives for HKEY_CLASSES_ROOT, HKEY_USERS and HKEY_CURRENT_CONFIG
`Get-Acl`	To fetch acl list for a registry key
`Select-Object, Select-String`	To format output
`[System.Diagnostics.FileVersionInfo]::GetVersionInfo(<file>)`	To get file version
`System.IO.File.ReadAllText`	To fetch content of the file
`Get-Item`	File system lookup
`Get-ItemProperty`	To fetch registry entries and their values
`Get-ChildItem <path>`	To get underlying files/folders in the path

Cmdlets	Function
`[System.IO.Path]::GetTempPath()`	To get the Temp directory path
`New-Item -ItemType Directory -Path <path>`	To create a temporary directory (this is removed later)
`Remove-Item`	To remove the temporary directory created

`SpecialFolder's:`
 	
`[Environment+SpecialFolder]::GetNames([Environment+SpecialFolder])`
 	
`[Environment]::GetFolderPath(<folder>)`
	To list all the available SpecialFolder's
	
	To get the full path of the folder

`Get-WmiObject`	To query WMI with specific queries in a namespace
`Get-HotFix`	To get patch information
`New-Object -ComObject "Microsoft.Update.Session"`	This session is used to fetch all windows updated history
`docker images`	To list the available docker images
`WMIC logicaldisk`	To list the logical drives
`mklink`	To create link to a local directory for further operation
`go version`	To fetch golang version
`NetUserEnum`	To fetch user accounts from the server
`java -fullversion`	To get eh version information
`dism.exec`	https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/dism-image-management-command-line-options-s14
`Get-AppxPackage`	To fetch list of app packages that are installed
`lsaQueryInformationPolicy`	https://docs.microsoft.com/en-us/windows/desktop/api/ntsecapi/nf-ntsecapi-lsaqueryinformationpolicy
`LsaOpenPolicy`	Opens a handle to the Policy object on a local or remote system
`LsaAddAccountRights`	Assigns one or more privileges to an account
`LsaRemoveAccountRights`	Removes one or more privileges from an account

Cmdlets	Function
LsaEnumerateAccountsWithUserRight	Returns the accounts in the database of a Local Security Authority (LSA) Policy object that hold a specified privilege
LsaLookupSids	Looks up the names that correspond to an array of security identifiers (SIDs). If LsaLookupSids cannot find a name that corresponds to a SID, the function returns the SID in character form
LsaLookupNames2	Retrieves the security identifiers (SIDs) for specified account names. LsaLookupNames2 can look up the SID for any account in any domain in a Windows forest
LsaNtStatusToWinError	The LsaNtStatusToWinError function converts an NTSTATUS code returned by an LSA function to a Windows error code
LsaClose	The LsaClose function closes a handle to a Policy or TrustedDomain object
LsaFreeMemory	The LsaFreeMemory function frees memory allocated for an output buffer by an LSA function call
LsaQueryInformationPolicy	Retrieves information about a Policy object

4 Installation

***Note**: Temp files are not created intentionally during the installation.*

The installation procedure is as described below:

1. Outpost24 scanner connects to the target machine through the SMB port.
2. Authenticates the user credentials.
3. The O24AUTH is created via the service manage on the svcctl named pipe. The command line of the service is an encoded PowerShell script.
   ***Note**: Encoded script is used for better data transmission.*