PufferSearchAndDestroy

V1.0.0.0

05/26/2021

Andrew Ogden

[andrew.ogden@puffer.com](mailto:andrew.ogden@puffer.com)

Some code modified from an original script provided by Matt Silcox at Catapult Systems.

Contents

[Change Log 3](#_Toc72936657)

[Start-PufferMailBlock 4](#_Toc72936658)

[Synopsis 4](#_Toc72936659)

[Syntax 4](#_Toc72936660)

[Description 4](#_Toc72936661)

[Examples 4](#_Toc72936662)

[Parameters 4](#_Toc72936663)

[Start-PufferMailPurge 7](#_Toc72936664)

[Synopsis 7](#_Toc72936665)

[Syntax 7](#_Toc72936666)

[Description 7](#_Toc72936667)

[Examples 7](#_Toc72936668)

[Parameters 7](#_Toc72936669)

[Start-PufferMailSearch 8](#_Toc72936670)

[Synopsis 8](#_Toc72936671)

[Syntax 8](#_Toc72936672)

[Description 8](#_Toc72936673)

[Examples 9](#_Toc72936674)

[Parameters 9](#_Toc72936675)

[Start-PufferMailSearchPreview 12](#_Toc72936676)

[Synopsis 12](#_Toc72936677)

[Syntax 12](#_Toc72936678)

[Description 12](#_Toc72936679)

[Examples 13](#_Toc72936680)

[Parameters 13](#_Toc72936681)

[Start-PufferSearchAndDestroy 13](#_Toc72936682)

[Synopsis 13](#_Toc72936683)

[Syntax 13](#_Toc72936684)

[Description 14](#_Toc72936685)

[Examples 14](#_Toc72936686)

[Parameters 14](#_Toc72936687)

## Change Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Comments** | **Version** | **Modified By** |
| 05/26/21 | Initial document | 1.0.0.0 | Andrew Ogden |
|  |  |  |  |
|  |  |  |  |

## Start-PufferMailBlock

### Synopsis

Update Puffer mail rules to block delivery of matching emails in the future.

### Syntax

Start-PufferMailBlock -Body <String> [<CommonParameters>]

Start-PufferMailBlock -Sender <String> [<CommonParameters>]

Start-PufferMailBlock -Subject <String> [<CommonParameters>]

Start-PufferMailBlock -Header <String> [<CommonParameters>]

Start-PufferMailBlock -Domain <String> [<CommonParameters>]

### Description

Update Puffer mail rules to block delivery of matching emails in the future.

### Examples

#### Example 1

Start-PufferMailBlock -Sender ‘info@spammer.com’

Add a rule to the default anti-spam rule blocking delivery of future emails from [info@spammer.com](mailto:info@spammer.com).

#### Example 2

Start-PufferMailBlock -Domain ‘spammer.com’

Add a rule to the default anti-spam rule blocking delivery of future emails from any address at the spammer.com domain.

### Parameters

#### Body

Block emails whose body matches this text.

Type: String

Parameter Sets: Body

Aliases:

Required: True

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### Domain

Block emails that are apparently from this domain.

Type: String

Parameter Sets: Domain

Aliases:

Required: True

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### Header

Block emails whose header matches this header string.

Type: String

Parameter Sets: Header

Aliases:

Required: True

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### Sender

Block email whose sender matches this address.

Type: String

Parameter Sets: Sender

Aliases:

Required: True

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### Subject

Block emails whose subject matches this text.

Type: String

Parameter Sets: Subject

Aliases:

Required: True

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

## Start-PufferMailPurge

### Synopsis

Begin a HardDelete type purge action on the results of a search.

### Syntax

Start-PufferMailPurge [-SearchName] <String> [-Confirm] [-Return] [<CommonParameters>]

### Description

Begin a HardDelete type purge action on the results of a search.

### Examples

#### Example 1

Start-PufferMailPurge -SearchName ‘Search1’

Start a mail purge on the search named ‘Search1.’

### Parameters

#### SearchName

The name of an existing mail search case.

Type: String

Parameter Sets: (All)

Aliases:

Required: True

Position: 1

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### Confirm

Whether or not to request user confirmation prior to beginning the purge.

Type: Switch

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: $False

Accept pipeline input: False

Accept wildcard characters: False

## Start-PufferMailSearch

### Synopsis

Create and start a new mail search.

### Syntax

Start-PufferMailSearch [-CaseName] <String> [-From] <String> [-Description <String>] [-Location <String>] [-StartDate <String>] [-EndDate <String>] [-Subject <String>] [-To <String>] [-Return] [<CommonParameters>]

### Description

Create and start a new mail search. It can take several minutes to start and complete a search.

### Examples

#### Example 1

Start-PufferMailSearch -CaseName ‘Search1’ -From ‘info@spammer.com’

Start a search for [info@spammer.com](mailto:info@spammer.com) with case name ‘Search1 in all mailboxes with no date range.

#### Example 2

Start-PufferMailSearch -CaseName ‘Search1’ -From ‘info@spammer.com’ -Location ‘user@puffer.com’

Start a search for [info@spammer.com](mailto:info@spammer.com) with case name ‘Search1’ with no date range in only the mailbox belonging to user@puffer.com.

### Parameters

#### -CaseName

The search display name.

Type: String

Parameter Sets: (All)

Aliases:

Required: True

Position: 1

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -From

The sender email address for which to search.

Type: String

Parameter Sets: (All)

Aliases:

Required: True

Position: 2

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -Location

The mailbox in which to search. Can be either ‘All’ or a specific mailbox name.

Default: ‘All’

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: ‘All’

Accept pipeline input: False

Accept wildcard characters: False

#### -StartDate

The earliest date from which to search.

Type: DateTime

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -EndDate

The latest date up to which to search for emails.

Type: DateTime

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -Subject

All or part of the subject line of the email.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -To

Any recipient.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

## Start-PufferMailSearchPreview

### Synopsis

Start a preview action following the end of a search. Requires a valid search case name.

### Syntax

Start-PufferMailSearchPreview [-SearchName] <String> [-Return] [<CommonParameters>]

### Description

Start a preview action following the end of a search. Requires a valid search case name.

### Examples

#### Example 1

Start-PufferMailSearchPreview -SearchName ‘Search1’

Start a preview for the search named ‘Search1.’

### Parameters

#### -SearchName

The name of an existing search case.

Type: String

Parameter Sets: (All)

Aliases:

Required: True

Position: 1

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

## Start-PufferSearchAndDestroy

### Synopsis

Begin a search, purge, and optionally, block action.

### Syntax

Start-PufferSearchAndDestroy [-From] <String> [-To <String>] [-Subject <String>] [-Body <String>] [-Header <String>] [-StartDate <DateTime>] [-EndDate <DateTime>] [-BlockSender] [-BlockDomain] [-BlockSubject] [-BlockBody] [-BlockHeader] [<CommonParameters>]

Start-PufferSearchAndDestroy [-Domain] <String> [-To <String>] [-Subject <String>] [-Body <String>] [-Header <String>] [-StartDate <DateTime>] [-EndDate <DateTime>] [-BlockDomain] [-BlockSubject] [-BlockBody] [-BlockHeader] [<CommonParameters>]

### Description

Begin a search, purge, and block action. This meta-cmdlet wraps up the functionality of all the other module cmdlets into a single command to sequence them all.

### Examples

#### Example 1

Start-PufferSearchAndDestroy -From ‘info@spammer.com’

Search for and purge any email sent by [info@spammer.com](mailto:info@spammer.com) in the last 24 hours.

#### Example 2

Start-PufferSearchAndDestroy -From ‘info@spammer.com’ -BlockSender

Search for and purge any email sent by [info@spammer.com](mailto:info@spammer.com) in the last 24 hours and block that sender.

#### Example 3

Start-PufferSearchAndDestroy --Domain ‘spammer.com’ -BlockDomain

Search for and purge any email sent from spammer.com in the last 24 hours and block all future emails from that domain.

#### Example 4

Start-PufferSearchAndDestroy -From ‘info@spammer.com’ -BlockSender -BlockDomain

Search for and purge any email sent from [info@spammer.com](mailto:info@spammer.com) in the last 24 hours, block that sender, and block the domain.

### Parameters

#### -BlockBody

Add and entry to the Body ETR to block future emails with the matching text in the body.

Type: Switch

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: $False

Accept pipeline input: False

Accept wildcard characters: False

#### -BlockDomain

Add an entry to the default anti-spam rule to block the sender domain.

Type: Switch

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: $False

Accept pipeline input: False

Accept wildcard characters: False

#### -BlockHeader

Add an entry to the Header ETR to block future emails with matching headers.

Type: Switch

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: $False

Accept pipeline input: False

Accept wildcard characters: False

#### -BlockSender

Add an entry to the default anti-spam rule to block the sender.

Type: Switch

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: $False

Accept pipeline input: False

Accept wildcard characters: False

#### -BlockSubject

Add an entry to the Subject ETR to block future emails with the matching text in the subject line.

Type: Switch

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: $False

Accept pipeline input: False

Accept wildcard characters: False

#### -Body

All or part of the body of the email.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -Domain

The domain of the spammer or malicious sender.

Type: String

Parameter Sets: Domain

Aliases:

Required: True

Position: 1

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -EndDate

The latest date up to which to search for emails.

Default: The current day.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: (Get-Date)

Accept pipeline input: False

Accept wildcard characters: False

#### -From

The email address of the spammer or malicious sender.

Type: String

Parameter Sets: From

Aliases:

Required: True

Position: 1

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -Header

All or part of the header.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -StartDate

The earliest date from which to search for emails.

Default: The previous day.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: (Get-Date).AddDays(-1)

Accept pipeline input: False

Accept wildcard characters: False

#### -Subject

All or part of the subject line of the email.

Type: String

Parameter Sets: (All)

Aliases:

Required: False

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

#### -To

Any recipient.

Type: String

Parameter Sets: Domain

Aliases:

Required: True

Position: 1

Default value: None

Accept pipeline input: False

Accept wildcard characters: False