



Lingelihle Nyuswa  
STUDENT NUMBER:20231329

# CSP632

FA2

## Data Collection

The screenshot displays a Microsoft Excel spreadsheet titled "Q1-LINGELIHLE CSP631" with a data table containing columns for TimeGenerated, User, Action, Target, and IPAddress. The 'Save As' dialog box is open, showing the file name "Q1-LINGELIHLE CSP631" and a list of file formats for saving, including CSV, Excel Workbook, and PDF.

**Excel Data Table:**

TimeGenerated	User	Action	Target	IPAddress
4:11 am	Anonymous	Quarantine	data exfiltration	1234.4568.8950
2:35 am	Unknown	Quarantine	data exfiltration	0000.0000.0000.000
12:20 am	The dopest	stop process	unauthorized access	8884.96.0785.965
11:02 pm	captain anonymous	stop process	unauthorized access	8653.962.4456.1241

**Save As Dialog Box:**

- File name: Q1-LINGELIHLE CSP631
- Recent locations: Personal, OneDrive - Personal, Other locations, This PC, Add a Place, Browse
- File formats: CSV (Comma delimited) (\*.csv), Excel Workbook (\*.xlsx), Excel Macro-Enabled Workbook (\*.xlsm), Excel Binary Workbook (\*.xlsb), Excel 97-2003 Workbook (\*.xls), CSV UTF-8 (Comma delimited) (\*.csv), XML Data (\*.xml), Single File Web Page (\*.mht, \*.mhtml), Web Page (\*.htm, \*.html), Excel Template (\*.xltx), Excel Macro-Enabled Template (\*.xltm), Excel 97-2003 Template (\*.xlt), Text (Tab delimited) (\*.txt), Unicode Text (\*.txt), XML Spreadsheet 2003 (\*.xsm), Microsoft Excel 5.0/95 Workbook (\*.xls), CSV (Comma delimited) (\*.csv), Formatted Text (Space delimited) (\*.prn), Text (Macintosh) (\*.txt), Text (MS-DOS) (\*.txt), CSV (Macintosh) (\*.csv), CSV (MS-DOS) (\*.csv), DIF (Data Interchange Format) (\*.dif), SYLK (Symbolic Link) (\*.slk), Excel Add-in (\*.xlam), Excel 97-2003 Add-in (\*.xla), PDF (\*.pdf), XPS Document (\*.xps)

```
TimeGenerated;User;Action;Target;IPAddress.  
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950  
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000  
12:20 am;The dopest ;stop process;unauthorized access;0804.06.0785.965  
11:02 pm;captain anonymous ;stop process;unauthorized access;8053.962.4456.1241
```

**\*\*notes\*\***

- Was not sure the type of information we had to put in the columns, but managed to get the work done

## PowerShell Query

```
Get-Content '.\Downloads\Q1-LINGELIHLE CSP631.csv'

$data = Import-Csv '.\Downloads\Q1-LINGELIHLE CSP631.csv'

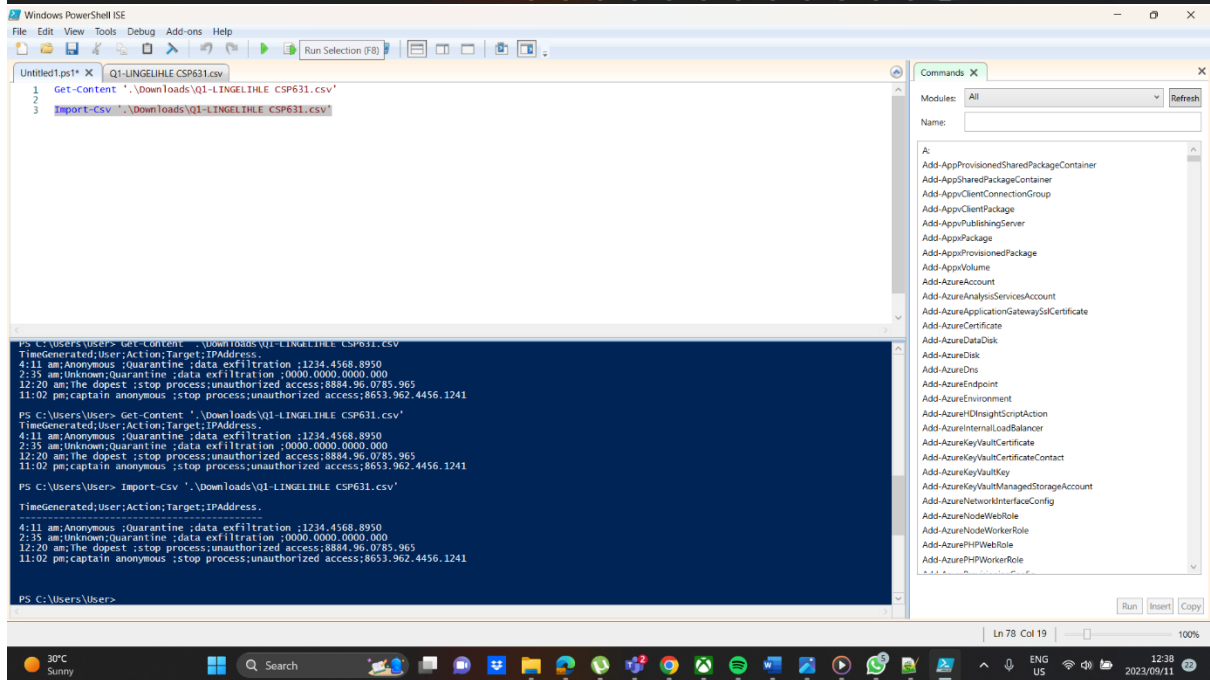
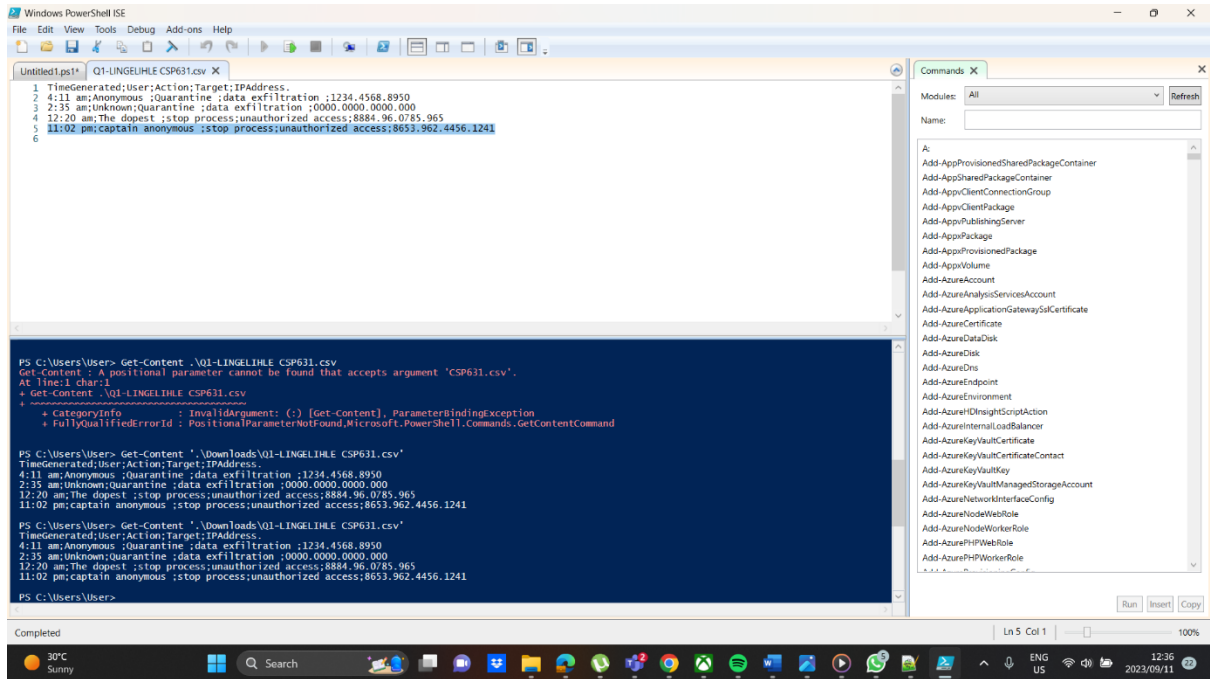
$data2 = Get-Content '.\Downloads\Q1-LINGELIHLE CSP631.csv' | ConvertFrom-Csv

$data[-1..1]

#filter world
#fetch records

$data | where-Object{
    $_.IPAddress -like '1234.4568.8950'
}

$data | where-Object{
    $_.IPAddress -like '1234.4568.8950' -and $_.Action -like 'Quarantine' -and
    $_.Target -like 'data exfiltration'
}
```



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X Q1-LINGELIHL CSP631.csv
1 Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'

4:11 am;Anonymous;Quarantine;data exfiltration;1234.4568.8950
2:35 am;Unknown;Quarantine;data exfiltration;0000.0000.0000.000
12:20 am;The dopest;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User> $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'

$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous;Quarantine;data exfiltration;1234.4568.8950
2:35 am;Unknown;Quarantine;data exfiltration;0000.0000.0000.000
12:20 am;The dopest;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User>
```

Commands X

Modules: All Refresh

Name:

A:

- Add-AppProvisionedSharedPackageContainer
- Add-AppSharedPackageContainer
- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppPackage
- Add-AppProvisionedPackage
- Add-AppVolume
- Add-AzureAccount
- Add-AzureAnalysisServicesAccount
- Add-AzureApplicationGatewaySaCertificate
- Add-AzureCertificate
- Add-AzureDataDisk
- Add-AzureDisk
- Add-AzureDns
- Add-AzureEndpoint
- Add-AzureEnvironment
- Add-AzureHdInsightScriptAction
- Add-AzureInternalLoadBalancer
- Add-AzureKeyVaultCertificate
- Add-AzureKeyVaultCertificateContact
- Add-AzureKeyVaultKey
- Add-AzureKeyVaultManagedStorageAccount
- Add-AzureNetworkInterfaceConfig
- Add-AzureNodeWebRole
- Add-AzureNodeWorkerRole
- Add-AzurePHPWebRole
- Add-AzurePHPWorkerRole

Run Insert Copy

Ln 136 Col 19 100%

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X Q1-LINGELIHL CSP631.csv
1 Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'

4:11 am;Anonymous;Quarantine;data exfiltration;1234.4568.8950
2:35 am;Unknown;Quarantine;data exfiltration;0000.0000.0000.000
12:20 am;The dopest;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User> $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'

$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous;Quarantine;data exfiltration;1234.4568.8950
2:35 am;Unknown;Quarantine;data exfiltration;0000.0000.0000.000
12:20 am;The dopest;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User> $data.GetType()

IsPublic IsSerial Name BaseType
-----
True True object[] System.Array

PS C:\Users\User>
```

Commands X

Modules: All Refresh

Name:

A:

- Add-AppProvisionedSharedPackageContainer
- Add-AppSharedPackageContainer
- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppPackage
- Add-AppProvisionedPackage
- Add-AppVolume
- Add-AzureAccount
- Add-AzureAnalysisServicesAccount
- Add-AzureApplicationGatewaySaCertificate
- Add-AzureCertificate
- Add-AzureDataDisk
- Add-AzureDisk
- Add-AzureDns
- Add-AzureEndpoint
- Add-AzureEnvironment
- Add-AzureHdInsightScriptAction
- Add-AzureInternalLoadBalancer
- Add-AzureKeyVaultCertificate
- Add-AzureKeyVaultCertificateContact
- Add-AzureKeyVaultKey
- Add-AzureKeyVaultManagedStorageAccount
- Add-AzureNetworkInterfaceConfig
- Add-AzureNodeWebRole
- Add-AzureNodeWorkerRole
- Add-AzurePHPWebRole
- Add-AzurePHPWorkerRole

Run Insert Copy

Ln 136 Col 34 100%

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X Q1-LINGELHLE CSP631.csv
1 Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELHLE CSP631.csv'

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv'
$data = Import-Csv '.\Downloads\Q1-LINGELHLE CSP631.csv'
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User> $data.GetType()

IsPublic IsSerial Name                                     BaseType
-----
True     True     Object[]                                     System.Array

PS C:\Users\User> $data[0].GetType()

IsPublic IsSerial Name                                     BaseType
-----
True     False    PSCustomObject                                     System.Object

PS C:\Users\User>
```

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X Q1-LINGELHLE CSP631.csv
1 Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELHLE CSP631.csv'
4
5 Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv' | ConvertFrom-Csv

4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241

TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv' | ConvertFrom-Csv
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241

PS C:\Users\User>
```

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1 X Q1-LINGELIHL CSP631.csv

```
1 Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
4
5 $data = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
```

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

```
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
```

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'

```
$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
$data = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
```

PS C:\Users\User> \$data = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

PS C:\Users\User>

Commands X

Modules: All Refresh

Name:

A:

- Add-AppProvisionedSharedPackageContainer
- Add-AppSharedPackageContainer
- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppPackage
- Add-AppProvisionedPackage
- Add-AppVolume
- Add-AzureAccount
- Add-AzureAnalysisServicesAccount
- Add-AzureApplicationGatewaySaCertificate
- Add-AzureCertificate
- Add-AzureDataDisk
- Add-AzureDisk
- Add-AzureDns
- Add-AzureEndpoint
- Add-AzureEnvironment
- Add-AzureHdInsightScriptAction
- Add-AzureInternalLoadBalancer
- Add-AzureKeyVaultCertificate
- Add-AzureKeyVaultCertificateContact
- Add-AzureKeyVaultKey
- Add-AzureKeyVaultManagedStorageAccount
- Add-AzureNetworkInterfaceConfig
- Add-AzureNodeWebRole
- Add-AzureNodeWorkerRole
- Add-AzurePHPWebRole
- Add-AzurePHPWorkerRole

Run Insert Copy

Ln 196 Col 19 100%

31°C High UV

Search

ENG US 12:58 2023/09/11

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1 X Q1-LINGELIHL CSP631.csv

```
1 Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
4
5 $data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
```

TimeGenerated;User;Action;Target;IPAddress

```
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
```

PS C:\Users\User> \$data = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

PS C:\Users\User>

\$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'

```
$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
```

PS C:\Users\User>

\$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

PS C:\Users\User>

Commands X

Modules: All Refresh

Name:

A:

- Add-AppProvisionedSharedPackageContainer
- Add-AppSharedPackageContainer
- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppPackage
- Add-AppProvisionedPackage
- Add-AppVolume
- Add-AzureAccount
- Add-AzureAnalysisServicesAccount
- Add-AzureApplicationGatewaySaCertificate
- Add-AzureCertificate
- Add-AzureDataDisk
- Add-AzureDisk
- Add-AzureDns
- Add-AzureEndpoint
- Add-AzureEnvironment
- Add-AzureHdInsightScriptAction
- Add-AzureInternalLoadBalancer
- Add-AzureKeyVaultCertificate
- Add-AzureKeyVaultCertificateContact
- Add-AzureKeyVaultKey
- Add-AzureKeyVaultManagedStorageAccount
- Add-AzureNetworkInterfaceConfig
- Add-AzureNodeWebRole
- Add-AzureNodeWorkerRole
- Add-AzurePHPWebRole
- Add-AzurePHPWorkerRole

Run Insert Copy

Ln 213 Col 19 100%

31°C High UV

Search

ENG US 12:58 2023/09/11



Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1 X Q1-LINGELIHL CSP631.csv

```
2 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
3
4
5 $data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
```

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'

```
$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
```

PS C:\Users\User> \$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

PS C:\Users\User> \$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv

PS C:\Users\User> \$data2.GetType()

IsPublic	IsSerial	Name	BaseType
True	True	object[]	System.Array

PS C:\Users\User>

Ln 224 Col 19 100%

EUR/ZAR -0.68%

Search

ENG US 13:01 2023/09/11

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1 X Q1-LINGELIHL CSP631.csv

```
2 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
3
4
5 $data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
6
7
8 $data[0..3]
```

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'

```
$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
```

```
$data[0..3]
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
TimeGenerated;User;Action;Target;IPAddress
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
```

PS C:\Users\User>

Ln 303 Col 19 100%

ZAR/AUD -1.03%

Search

ENG US 13:03 2023/09/11

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X Q1-LINGELHLE CSP631.csv
1 $data = Import-Csv '.\Downloads\Q1-LINGELHLE CSP631.csv'
2
3 $data2 = Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv' | ConvertFrom-Csv
4
5
6
7
8 $data[-1..1]]

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv'
$data = Import-Csv '.\Downloads\Q1-LINGELHLE CSP631.csv'
$data2 = Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv' | ConvertFrom-Csv

$data[-1..1]
TimeGenerated;User;Action;Target;IPAddress.
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241

TimeGenerated;User;Action;Target;IPAddress.
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000

PS C:\Users\User>
```

Completed Ln 8 Col 13 100%

31°C Sunny

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*(Recovered) X Q1-LINGELHLE CSP631.csv
1 Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELHLE CSP631.csv'
4
5 $data2 = Get-Content '.\Downloads\Q1-LINGELHLE CSP631.csv' | ConvertFrom-Csv
6
7
8 $data[-1..1]]
9
10 #filter world
11 #fetch records
12
13 $data | Where-Object{
14     $_.IPAddress -like '1234.4568.8950'
15 }
16
17
18 $data | Where-Object{
19     $_.IPAddress -like '1234.4568.8950' -and $_.Action -like 'Quarantine' -and $_.Target -like 'data exfiltration'
20 }
21 }

$data[-1..1]
#filter world
#fetch records

$data | Where-Object{
    $_.IPAddress -like '1234.4568.8950'
}

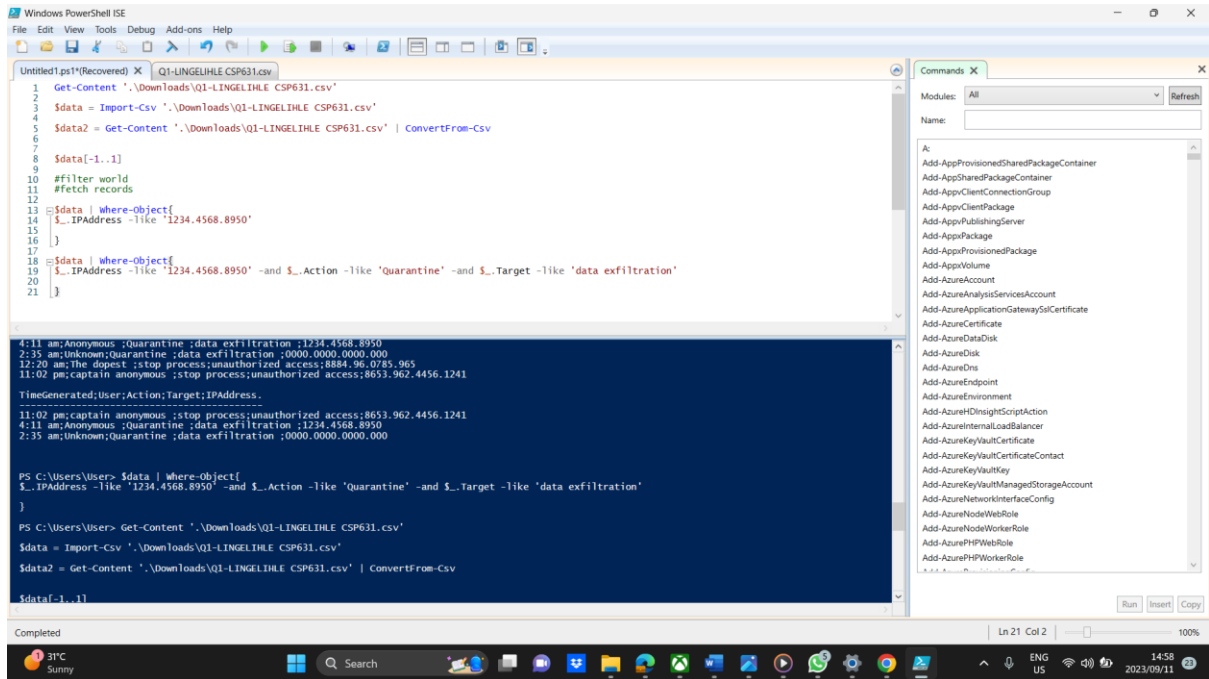
$data | Where-Object{
    $_.IPAddress -like '1234.4568.8950' -and $_.Action -like 'Quarantine' -and $_.Target -like 'data exfiltration'
}

TimeGenerated;User;Action;Target;IPAddress.
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241

TimeGenerated;User;Action;Target;IPAddress.
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
```

Completed Ln 21 Col 2 100%

31°C Sunny



```
1 Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'
2
3 $data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
4
5 $data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
6
7
8 $data[-1..1]
9
10 #filter world
11 #fetch records
12
13 $data | Where-Object{
14     $_.IPAddress -like '1234.4568.8950'
15 }
16
17 $data | Where-Object{
18     $_.IPAddress -like '1234.4568.8950' -and $_.Action -like 'Quarantine' -and $_.Target -like 'data exfiltration'
19 }
20
21 }
```

```
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;unknown;Quarantine ;data exfiltration ;0000.0000.0000.000
12:20 am;The dopest ;stop process;unauthorized access;8884.96.0785.965
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
TimeGenerated;User;Action;Target;IPAddress.
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;unknown;Quarantine ;data exfiltration ;0000.0000.0000.000

PS C:\Users\User> $data | Where-Object{
    $_.IPAddress -like '1234.4568.8950' -and $_.Action -like 'Quarantine' -and $_.Target -like 'data exfiltration'
}

PS C:\Users\User> Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv'
$data = Import-Csv '.\Downloads\Q1-LINGELIHL CSP631.csv'
$data2 = Get-Content '.\Downloads\Q1-LINGELIHL CSP631.csv' | ConvertFrom-Csv
$data[-1..1]
```

**\*\*notes\*\***

-was not sure on exporting data , just focused on the importing and getting the data, hope that's cool.

## Suspicious Activity

```
TimeGenerated;User;Action;Target;IPAddress.
-----
11:02 pm;captain anonymous ;stop process;unauthorized access;8653.962.4456.1241
4:11 am;Anonymous ;Quarantine ;data exfiltration ;1234.4568.8950
2:35 am;Unknown;Quarantine ;data exfiltration ;0000.0000.0000.0000
```

Suspicious behaviour from 11:02 pm to 4:11 am, there is a sign of unauthorized access from Different IP addresses.

On 11:02 pm an unauthorized access from 8653.962.4456.1241 , was detected.

On 2:35 am a data exfiltration was detected from 0000.0000.0000.0000

On 4:11 am data exfiltration was detected from 1234.4568.8950

Attempts to quarantine files and stop process were implemented but none were effective

### **\*\*notes\*\***

- Sir I hope you see where I was confused on the information required in the columns was supposed to be from Question 1.
- But the effort was there as seen above

## **Reporting**

Its an external threat , the attackers exploited vulnerability through a web application , then exploitation and installation then command and control, then user account got compromised revealing the vulnerability of sensitive patient information. The attacker then has access to the sensitive data allowing them exfiltration of the data.

The compromised patient records include medical histories and personal details

Using Microsoft Defender Endpoints it detects malicious payloads , share the telemetry and remediates endpoints, disabling user access from device while infected.

Shares intelligence to Microsoft Threat Intelligence

From there blocks attachments from future attacks and communicates with Microsoft Defender for O365. Enabling search on companywide web applications and database servers and removes viruses or any threats from any affected attachments or areas.

0Detect and manage incidents, in order to prevent any future threats

Asses the impact of new threats and review your resilience to the new threats

## **References**

- class slides
- [www.google.com](http://www.google.com)
- [youtube.com](http://youtube.com)