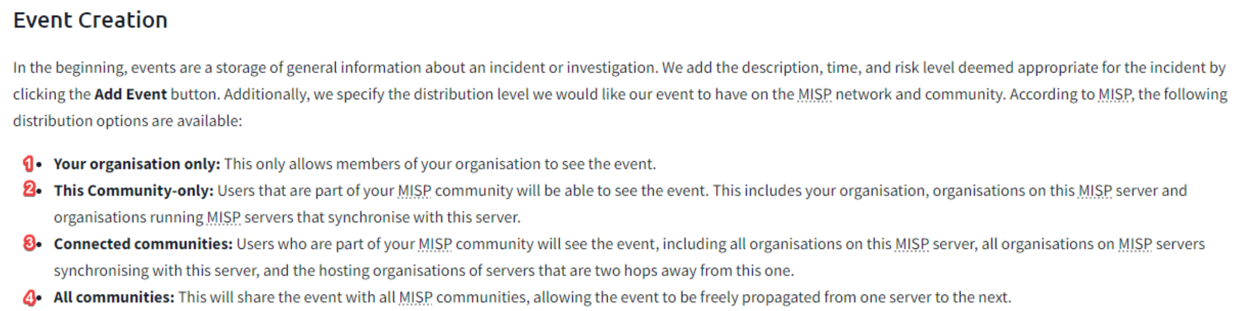
TASK 3: Using the System

Q: How many distribution options does MISP provide to share threat information?

In the task text:



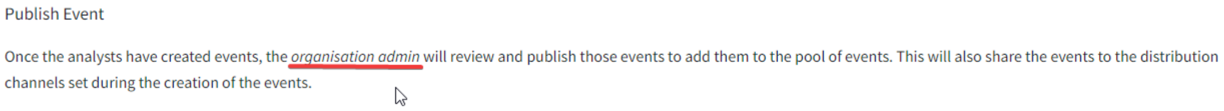
Event Creation

In the beginning, events are a storage of general information about an incident or investigation. We add the description, time, and risk level deemed appropriate for the incident by clicking the **Add Event** button. Additionally, we specify the distribution level we would like our event to have on the MISP network and community. According to MISP, the following distribution options are available:

1. **Your organisation only:** This only allows members of your organisation to see the event.
2. **This Community-only:** Users that are part of your MISP community will be able to see the event. This includes your organisation, organisations on this MISP server and organisations running MISP servers that synchronise with this server.
3. **Connected communities:** Users who are part of your MISP community will see the event, including all organisations on this MISP server, all organisations on MISP servers synchronising with this server, and the hosting organisations of servers that are two hops away from this one.
4. **All communities:** This will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next.

A: 4

Q: Which user has the role to publish events?



Publish Event

Once the analysts have created events, the organisation admin will review and publish those events to add them to the pool of events. This will also share the events to the distribution channels set during the creation of the events.

A: organisation admin

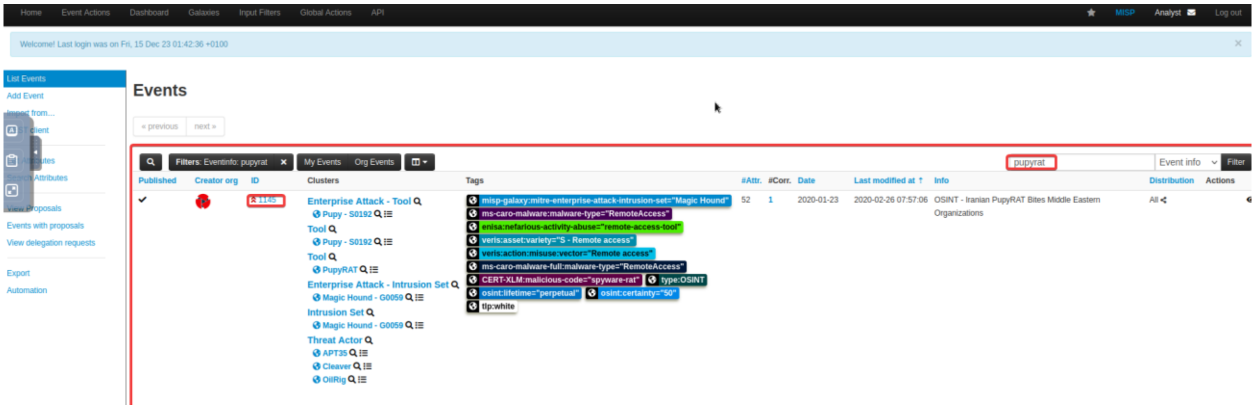
TASK 5: Scenario Event

CIRCL (Computer Incident Respons Center Luxembourg) published an event associated with PupyRAT infection. Your organisation is on alert for remote access trojans and malware in the wild, and you have been tasked to investigate this event and correlate the details with your SIEM. Use what you have learned from the room to identify the event and complete this task.

First you'll need to start the attackbox and the machine to surf to, then you can lookup the ip givin from the machine in the attackbox and start hunting the answers!

Q: What event ID has been assigned to the PupyRAT event?

Looking up pupyrat in the filter of the events tab, we can see the event id on the left side.



Welcome! Last login was on Fri, 15 Dec 23 01:42:36 +0100

Events

Filters: Eventinfo: pupyrat

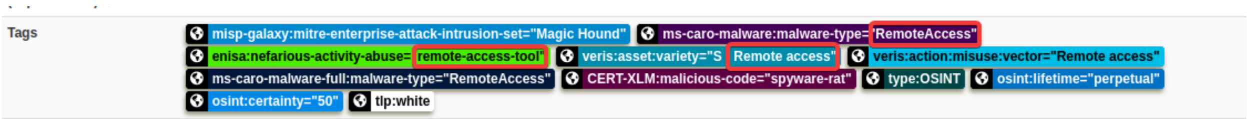
pupyrat

Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at	Info	Distribution	Actions
✓		1145	Enterprise Attack - Tool Pupy - S0192 Tool Pupy - S0192 Tool PupyRAT Enterprise Attack - Intrusion Set Magic Hound - G0059 Intrusion Set Magic Hound - G0059 Threat Actor APT35 Cleaver OilRig	misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound" ms-caro-malware:malware-type="RemoteAccess" enisa:nefarious-activity-abuse="remote-access-tool" veris:asset:variety="S - Remote access" veris:action:misuse:vector="Remote access" ms-caro-malware-full:malware-type="RemoteAccess" CERT-XLM:malicious-code="spyware-rat" type:OSINT osint:lifetime="perpetual" osint:certainty="50" tlp:white	52	1	2020-01-23	2020-02-26 07:57:06	OSINT - Iranian PupyRAT Bites Middle Eastern Organizations	All	

A: 1145

Q: The event is associated with the adversary gaining ______ into organisations.

Click on the event ID and under **Tags** we'll get our answer:



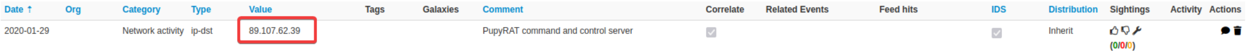
Tags

misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound" ms-caro-malware:malware-type="RemoteAccess" enisa:nefarious-activity-abuse="remote-access-tool" veris:asset:variety="S Remote access" veris:action:misuse:vector="Remote access" ms-caro-malware-full:malware-type="RemoteAccess" CERT-XLM:malicious-code="spyware-rat" type:OSINT osint:lifetime="perpetual" osint:certainty="50" tlp:white

A: remote access

Q: What IP address has been mapped as the PupyRAT C2 Server

For this I just did a Ctrl+F for "c2" which got no relevant hits, then searched "command" and that got me the answer:

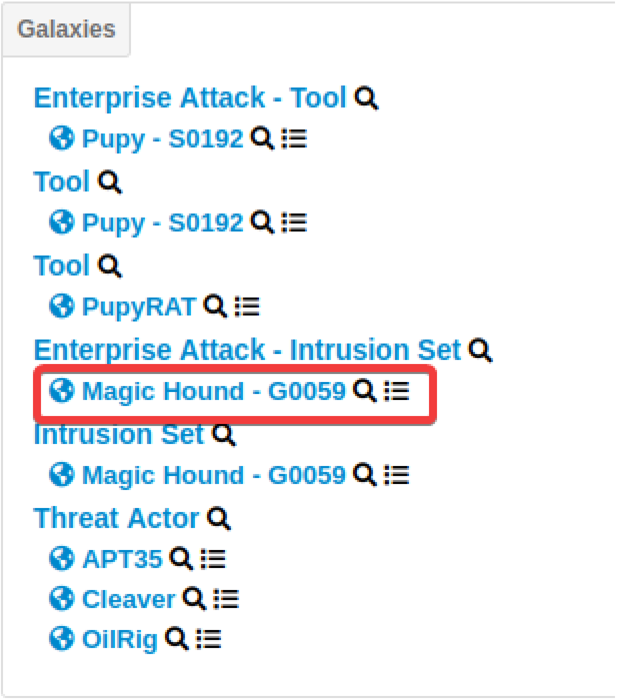


Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2020-01-29		Network activity	ip-dst	89.107.62.39			PupyRAT command and control server	☑			☑	Inherit	(0/0/0)		

A: 89.107.62.39

Q: From the Intrusion Set Galaxy, what attack group is known to use this form of attack?

just scroll down to galaxies and it's right there:



Galaxies

Enterprise Attack - Tool
- Pupy - S0192

Tool
- Pupy - S0192

Tool
- PupyRAT

Enterprise Attack - Intrusion Set
- Magic Hound - G0059

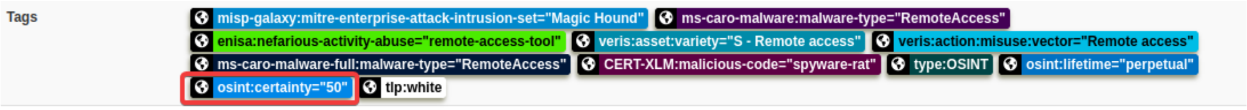
Intrusion Set
- Magic Hound - G0059

Threat Actor
- APT35
- Cleaver
- OilRig

A: magic hound

Q: There is a taxonomy tag set with a Certainty level of 50. Which one is it?

Looking to tags, we can see the osint tag.



Tags

misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound" ms-caro-malware:malware-type="RemoteAccess"
enisa:nefarious-activity-abuse="remote-access-tool" veris:asset:variety="S - Remote access" veris:action:misuse:vector="Remote access"
ms-caro-malware-full:malware-type="RemoteAccess" CERT-XLM:malicious-code="spyware-rat" type:OSINT osint:lifetime="perpetual"
osint:certainty="50" tlp:white

A: osint