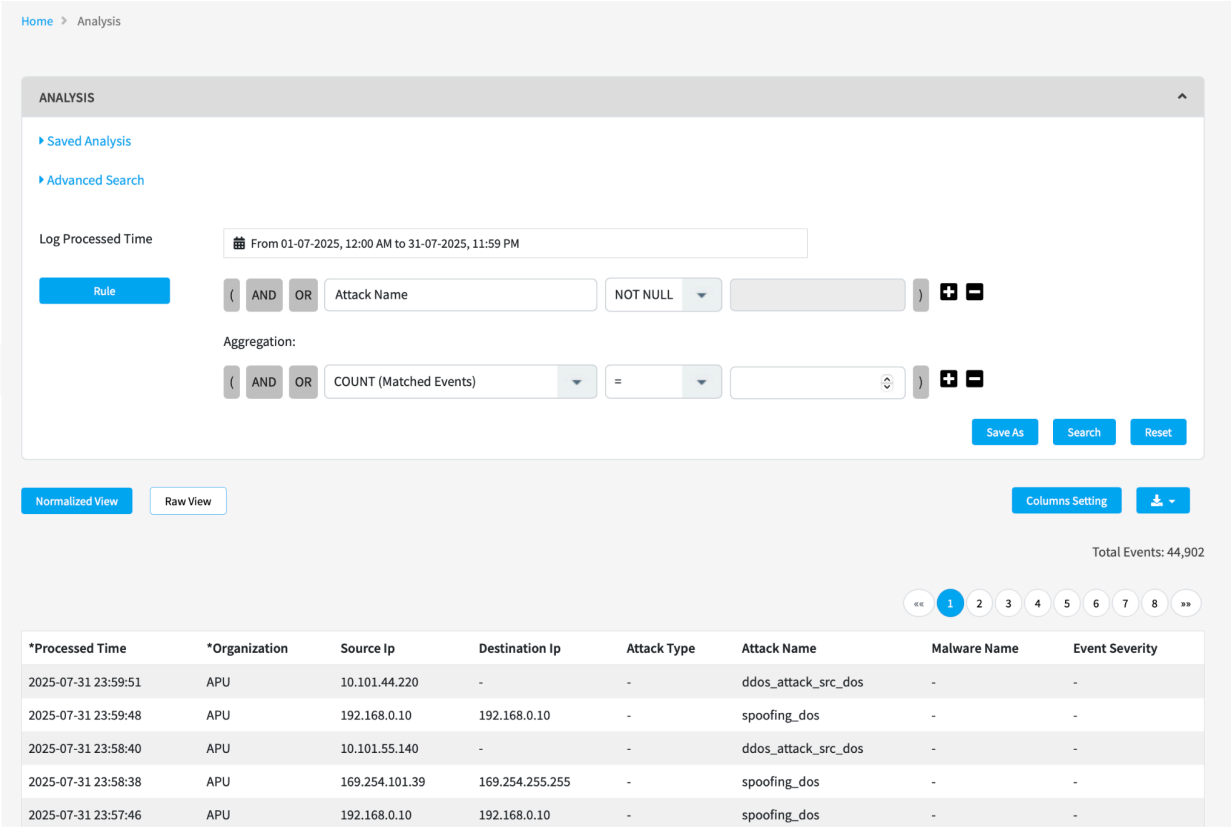
Julian bin Johan Bechler (TP091045)

Security Operations Centre

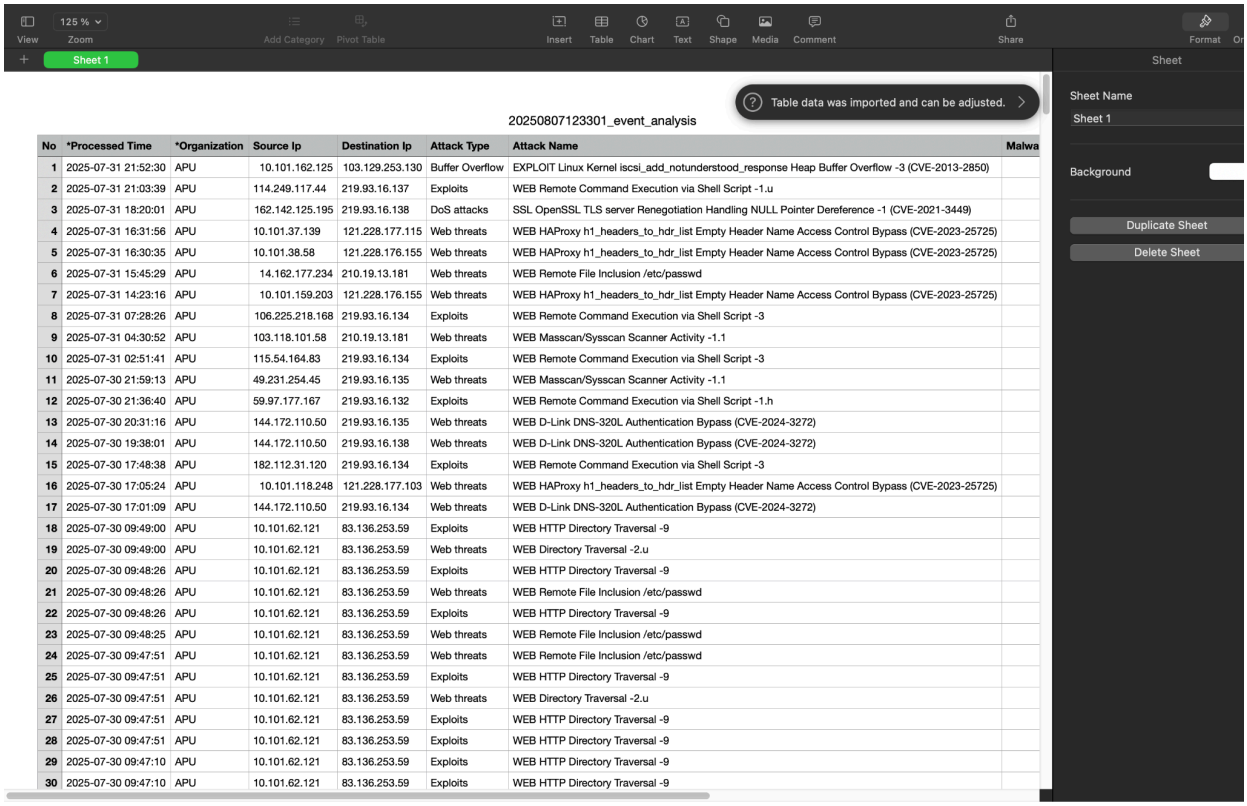
MSSGuard Class Assignment

1)



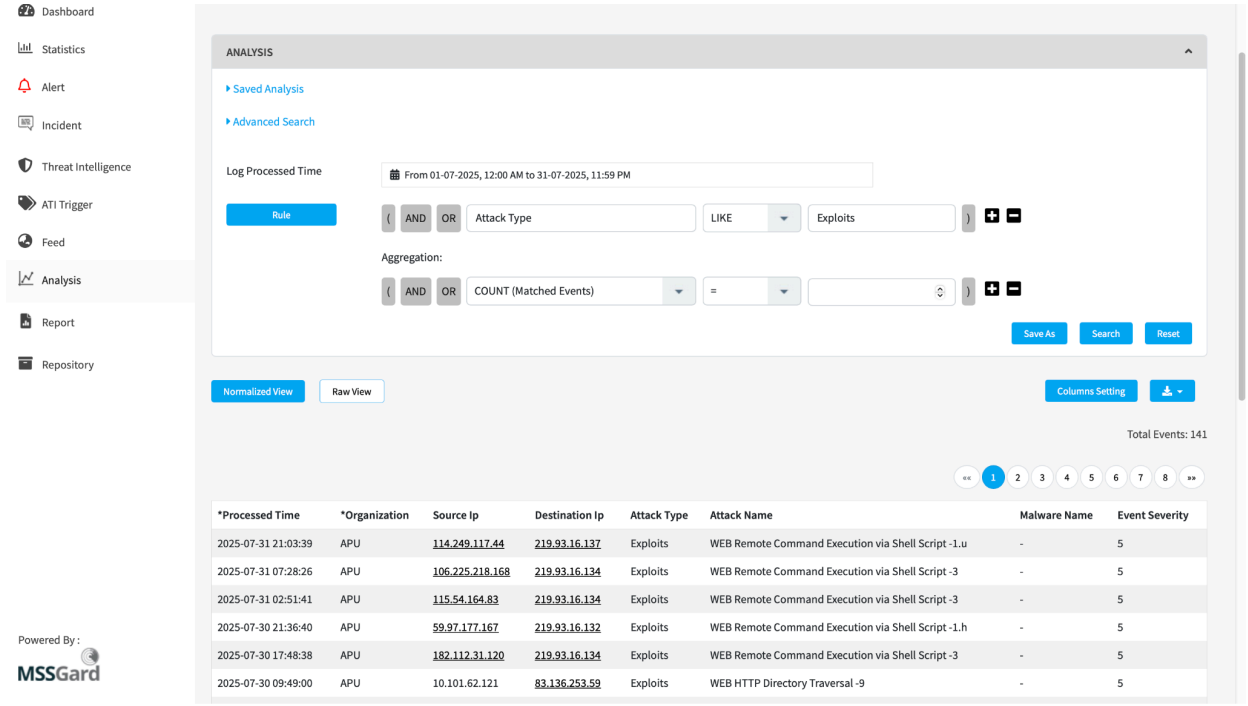
I) Total Events: 44,902

II)



No	*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Malwa
1	2025-07-31 21:52:30	APU	10.101.162.125	103.129.253.130	Buffer Overflow	EXPLOIT Linux Kernel iscsi_add_notunderstood_response Heap Buffer Overflow -3 (CVE-2013-2850)	
2	2025-07-31 21:03:39	APU	114.249.117.44	219.93.16.137	Exploits	WEB Remote Command Execution via Shell Script -1.u	
3	2025-07-31 18:20:01	APU	162.142.125.195	219.93.16.138	DoS attacks	SSL OpenSSL TLS server Renegotiation Handling NULL Pointer Dereference -1 (CVE-2021-3449)	
4	2025-07-31 16:31:56	APU	10.101.37.139	121.228.177.115	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	
5	2025-07-31 16:30:35	APU	10.101.38.58	121.228.176.155	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	
6	2025-07-31 15:45:29	APU	14.162.177.234	210.19.13.181	Web threats	WEB Remote File Inclusion /etc/passwd	
7	2025-07-31 14:23:16	APU	10.101.159.203	121.228.176.155	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	
8	2025-07-31 07:28:26	APU	106.225.218.168	219.93.16.134	Exploits	WEB Remote Command Execution via Shell Script -3	
9	2025-07-31 04:30:52	APU	103.118.101.58	210.19.13.181	Web threats	WEB Masscan/Sysscan Scanner Activity -1.1	
10	2025-07-31 02:51:41	APU	115.54.164.83	219.93.16.134	Exploits	WEB Remote Command Execution via Shell Script -3	
11	2025-07-30 21:59:13	APU	49.231.254.45	219.93.16.135	Web threats	WEB Masscan/Sysscan Scanner Activity -1.1	
12	2025-07-30 21:36:40	APU	59.97.177.167	219.93.16.132	Exploits	WEB Remote Command Execution via Shell Script -1.h	
13	2025-07-30 20:31:16	APU	144.172.110.50	219.93.16.135	Web threats	WEB D-Link DNS-320L Authentication Bypass (CVE-2024-3272)	
14	2025-07-30 19:38:01	APU	144.172.110.50	219.93.16.138	Web threats	WEB D-Link DNS-320L Authentication Bypass (CVE-2024-3272)	
15	2025-07-30 17:48:38	APU	182.112.31.120	219.93.16.134	Exploits	WEB Remote Command Execution via Shell Script -3	
16	2025-07-30 17:05:24	APU	10.101.118.248	121.228.177.103	Web threats	WEB HAProxy h1_headers_to_hdr_list Empty Header Name Access Control Bypass (CVE-2023-25725)	
17	2025-07-30 17:01:09	APU	144.172.110.50	219.93.16.134	Web threats	WEB D-Link DNS-320L Authentication Bypass (CVE-2024-3272)	
18	2025-07-30 09:49:00	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
19	2025-07-30 09:49:00	APU	10.101.62.121	83.136.253.59	Web threats	WEB Directory Traversal -2.u	
20	2025-07-30 09:48:26	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
21	2025-07-30 09:48:26	APU	10.101.62.121	83.136.253.59	Web threats	WEB Remote File Inclusion /etc/passwd	
22	2025-07-30 09:48:26	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
23	2025-07-30 09:48:25	APU	10.101.62.121	83.136.253.59	Web threats	WEB Remote File Inclusion /etc/passwd	
24	2025-07-30 09:47:51	APU	10.101.62.121	83.136.253.59	Web threats	WEB Remote File Inclusion /etc/passwd	
25	2025-07-30 09:47:51	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
26	2025-07-30 09:47:51	APU	10.101.62.121	83.136.253.59	Web threats	WEB Directory Traversal -2.u	
27	2025-07-30 09:47:51	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
28	2025-07-30 09:47:51	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
29	2025-07-30 09:47:10	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	
30	2025-07-30 09:47:10	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	

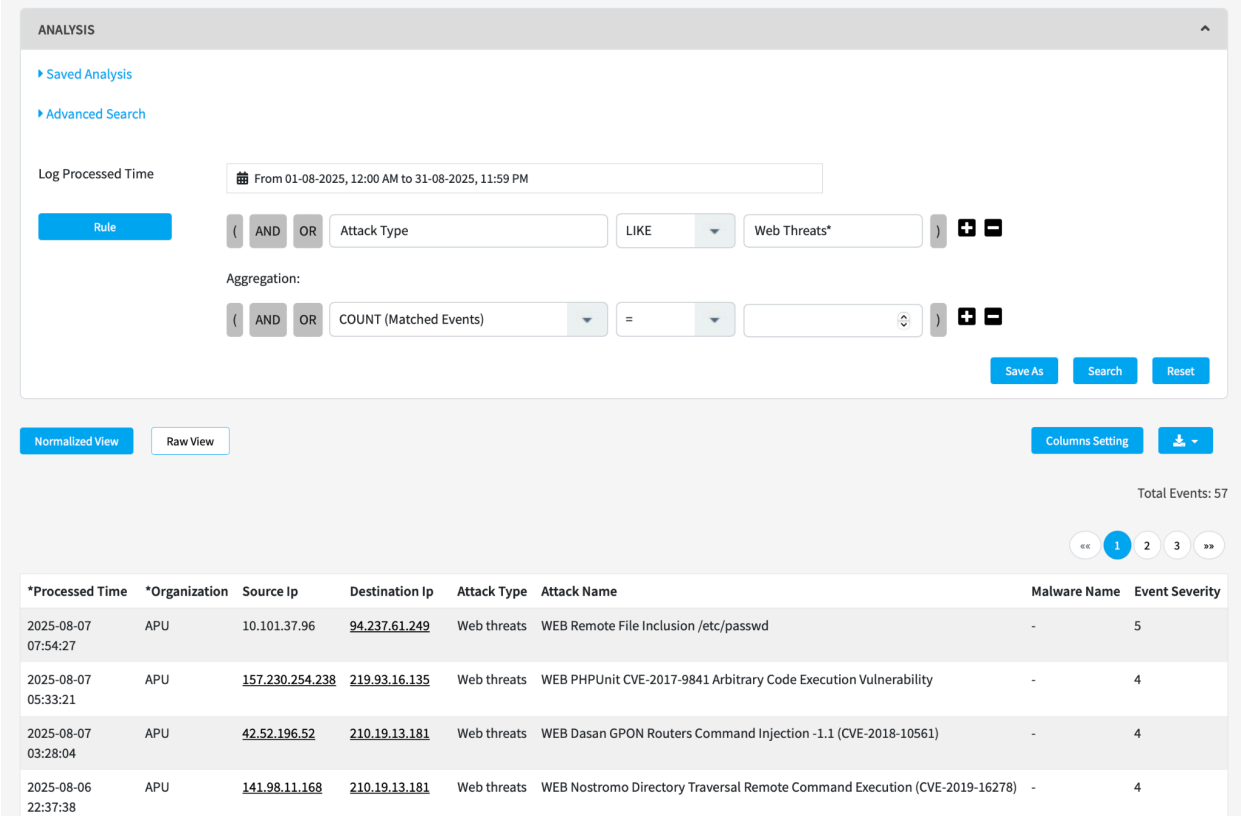
2)



*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Malware Name	Event Severity
2025-07-31 21:03:39	APU	114.249.117.44	219.93.16.137	Exploits	WEB Remote Command Execution via Shell Script -1.u	-	5
2025-07-31 07:28:26	APU	106.225.218.168	219.93.16.134	Exploits	WEB Remote Command Execution via Shell Script -3	-	5
2025-07-31 02:51:41	APU	115.54.164.83	219.93.16.134	Exploits	WEB Remote Command Execution via Shell Script -3	-	5
2025-07-30 21:36:40	APU	59.97.177.167	219.93.16.132	Exploits	WEB Remote Command Execution via Shell Script -1.h	-	5
2025-07-30 17:48:38	APU	182.112.31.120	219.93.16.134	Exploits	WEB Remote Command Execution via Shell Script -3	-	5
2025-07-30 09:49:00	APU	10.101.62.121	83.136.253.59	Exploits	WEB HTTP Directory Traversal -9	-	5

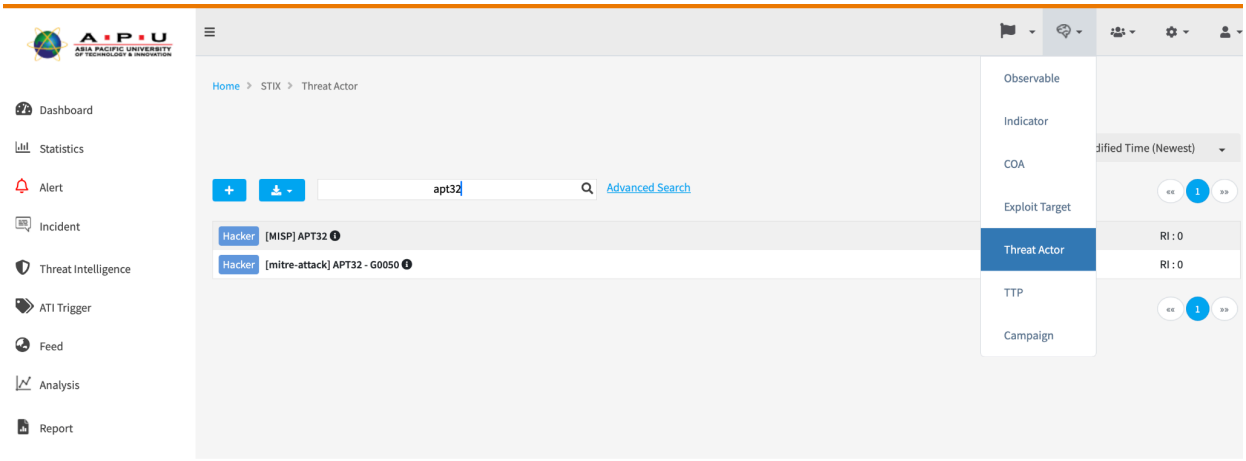
Total Exploits: 141

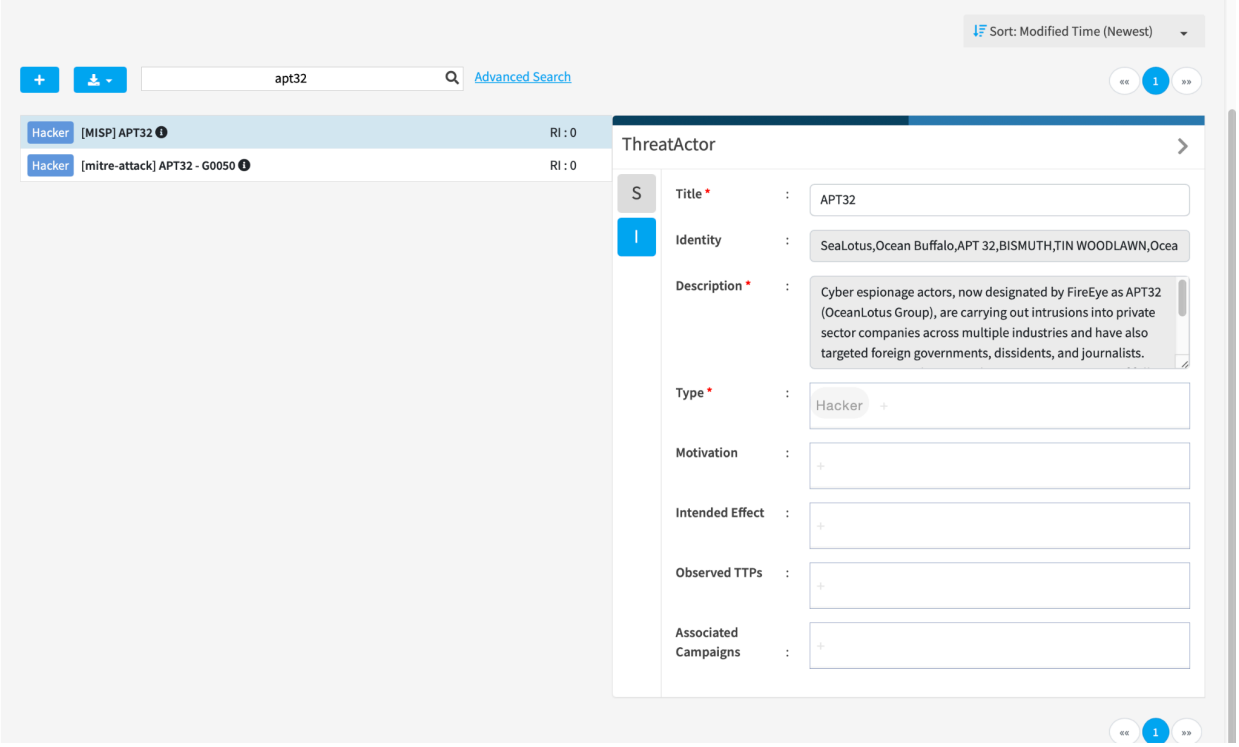
3)

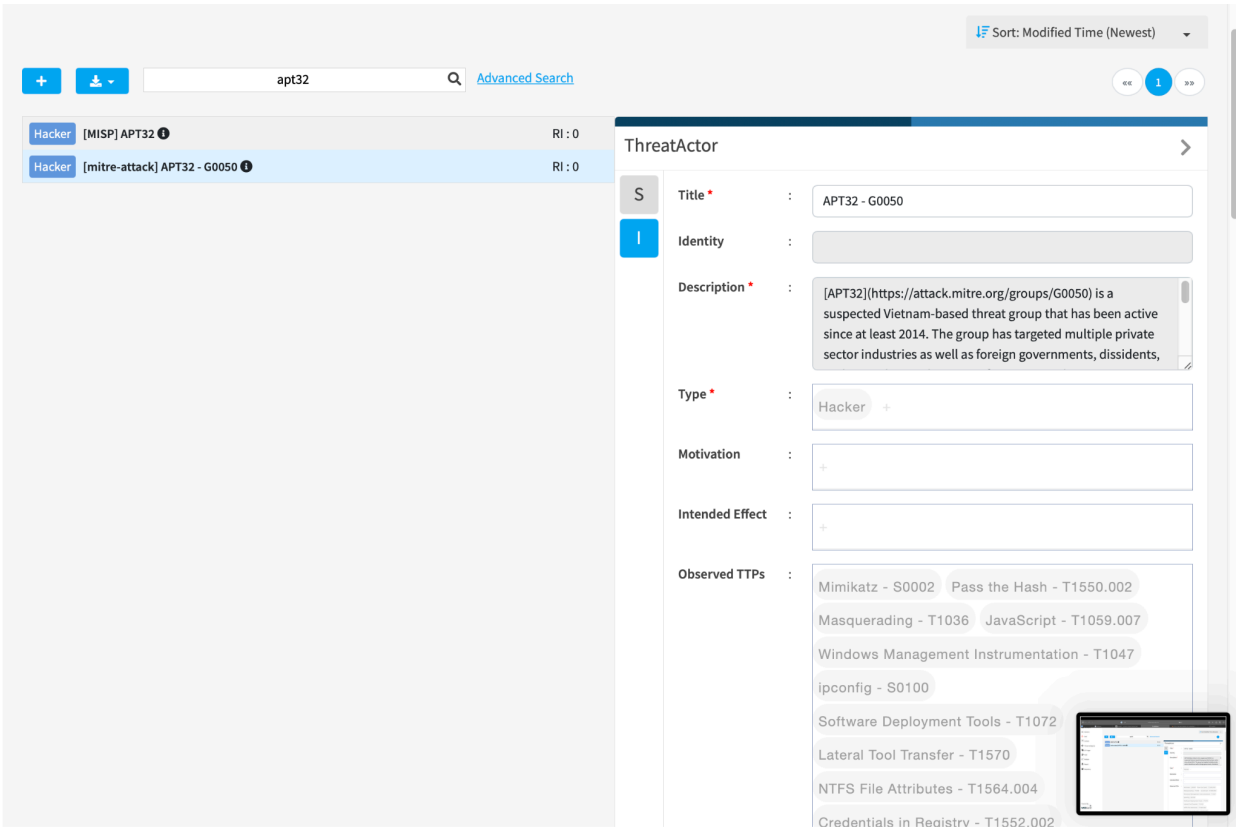


Total Web Threats: 57

4)

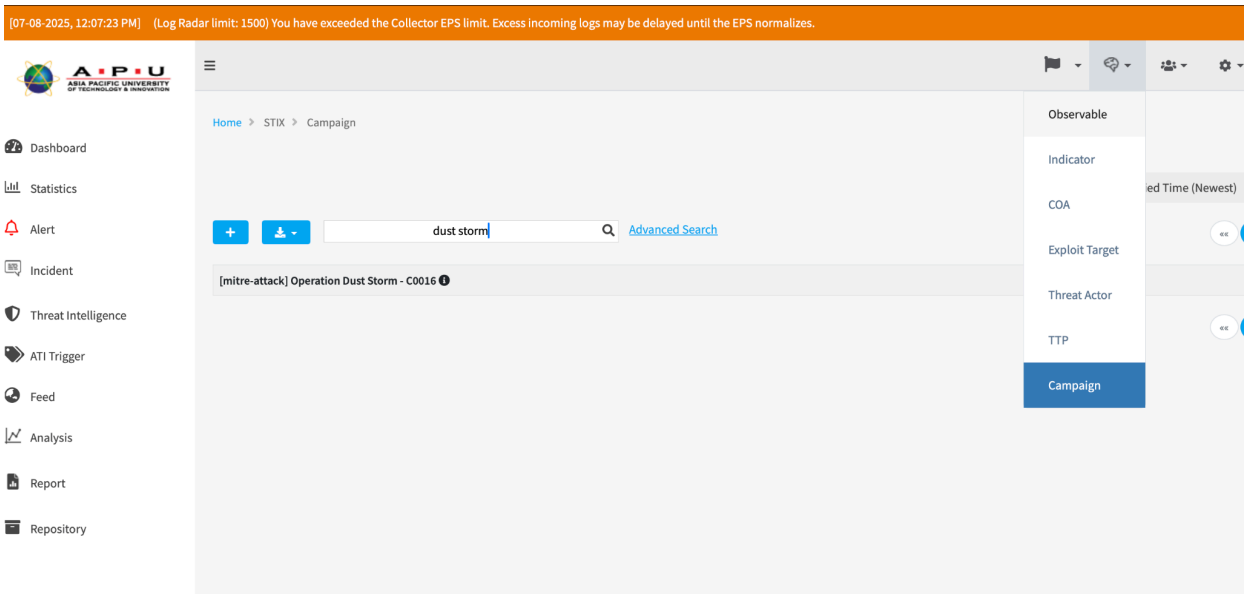


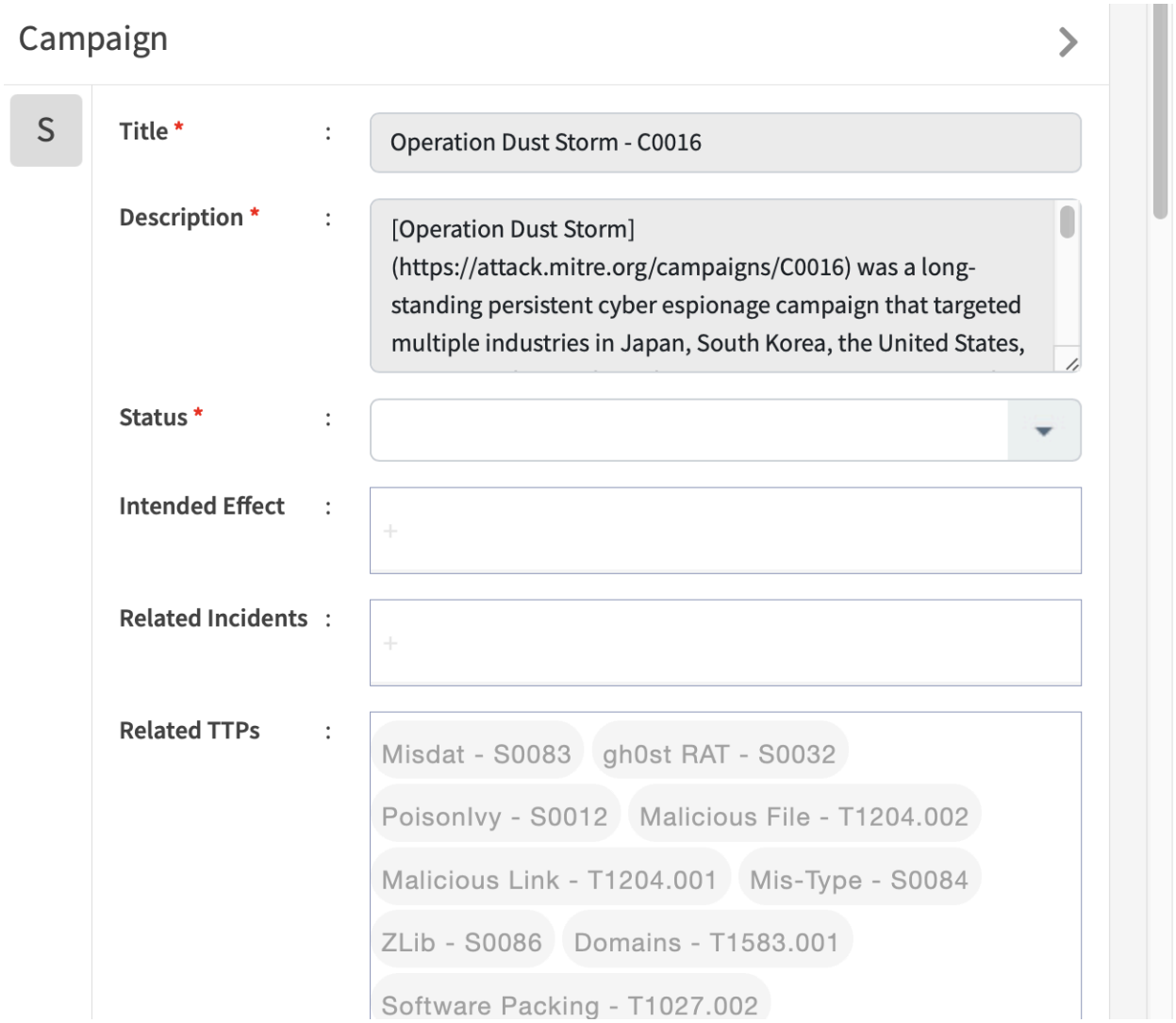

Sort: Modified Time (Newest)
apt32
Advanced Search
1
Hacker [MISP] APT32 RI : 0
Hacker [mitre-attack] APT32 - G0050 RI : 0
ThreatActor
S
I
Title *
APT32
Identity
SeaLotus,Ocean Buffalo,APT 32,BISMUTH,TIN WOODLAWN,Ocea
Description *
Cyber espionage actors, now designated by FireEye as APT32 (OceanLotus Group), are carrying out intrusions into private sector companies across multiple industries and have also targeted foreign governments, dissidents, and journalists.
Type *
Hacker
Motivation
Intended Effect
Observed TTPs
Associated Campaigns


Sort: Modified Time (Newest)
apt32
Advanced Search
1
Hacker [MISP] APT32 RI : 0
Hacker [mitre-attack] APT32 - G0050 RI : 0
ThreatActor
S
I
Title *
APT32 - G0050
Identity
Description *
[APT32](https://attack.mitre.org/groups/G0050) is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents,
Type *
Hacker
Motivation
Intended Effect
Observed TTPs
Mimikatz - S0002
Pass the Hash - T1550.002
Masquerading - T1036
JavaScript - T1059.007
Windows Management Instrumentation - T1047
ipconfig - S0100
Software Deployment Tools - T1072
Lateral Tool Transfer - T1570
NTFS File Attributes - T1564.004
Credentials in Registry - T1552.002

APT32, also known as OceanLotus, is a Vietnamese state-sponsored threat group that primarily targets foreign companies, journalists, and government organizations in Southeast Asia. Inside MSSGARD, threat intel about APT32 can be located under the Threat Intelligence or Adversary Profiles section. The group is known for spear phishing and the use of custom malware.

5)





Operation Dust Storm was a long-term cyber espionage campaign that primarily targeted organizations across Japan, South Korea, the United States, Europe, and Southeast Asia. Originally focusing on government and defense sectors, the adversary shifted its targeting around 2015 to focus on Japanese critical infrastructure sectors, including:

- Electricity generation
- Oil and natural gas
- Finance

- Transportation
- Construction

The actors behind this campaign used a combination of custom malware, spear phishing, and notably Android backdoors, all of which were confirmed to be deployed against victims in Japan and South Korea. These attacks demonstrated a high degree of persistence and stealth, consistent with advanced persistent threat (APT) tradecraft.