

Julian bin Johan Bechler (TP091045)

Security Operations Centre

MSSGuard Class Assignment

1)

[Home](#) > [Analysis](#)

ANALYSIS

▶ Saved Analysis

▶ Advanced Search

Log Processed Time

📅 From 01-07-2025, 12:00 AM to 31-07-2025, 11:59 PM

Rule

(AND OR Attack Name NOT NULL) + -

Aggregation:

(AND OR COUNT (Matched Events) =) + -

Save As

Search

Reset

Normalized View

Raw View

Columns Setting

⬇ +

Total Events: 44,902

◀ 1 2 3 4 5 6 7 8 ▶

*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Malware Name	Event Severity
2025-07-31 23:59:51	APU	10.101.44.220	-	-	ddos_attack_src_dos	-	-
2025-07-31 23:59:48	APU	192.168.0.10	192.168.0.10	-	spoofing_dos	-	-
2025-07-31 23:58:40	APU	10.101.55.140	-	-	ddos_attack_src_dos	-	-
2025-07-31 23:58:38	APU	169.254.101.39	169.254.255.255	-	spoofing_dos	-	-
2025-07-31 23:57:46	APU	192.168.0.10	192.168.0.10	-	spoofing_dos	-	-

I) Total Events: 44,902

II)

125 %

ViewZoom

Add CategoryPivot Table

InsertTableChartTextShapeMediaComment

Share

Format

Sheet 1

20250807123301_event_analysis

Table data was imported and can be adjusted.

No	*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Mahwa
1	2025-07-31 21:52:30	APU	10.101.162.125	103.129.253.130	Buffer Overflow	EXPLOIT Linux Kernel lcsli_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/Sysscanner 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/Sysscanner 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	

Sheet Sheet Name Sheet 1 Background Duplicate Sheet Delete Sheet

2)

- Dashboard
- Statistics
- Alert
- Incident
- Threat Intelligence
- ATI Trigger
- Feed
- Analysis
- Report
- Repository

Powered By :
MSSGard

ANALYSIS

Saved Analysis

Advanced Search

Log Processed Time

From 01-07-2025, 12:00 AM to 31-07-2025, 11:59 PM

Rule

(AND OR

Attack Type

LIKE

Exploits

)

Aggregation:

(AND OR

COUNT (Matched Events)

=

)

Save As

Search

Reset

Normalized View

Raw View

Columns Setting

Total Events: 141

<< 1 2 3 4 5 6 7 8 >>

*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)

ANALYSIS

Saved Analysis

Advanced Search

Log Processed Time

From 01-08-2025, 12:00 AM to 31-08-2025, 11:59 PM

Rule

(AND OR Attack Type LIKE Web Threats*) + -

Aggregation:

(AND OR COUNT (Matched Events) =) + -

Save As

Search

Reset

Normalized View

Raw View

Columns Setting

Total Events: 57

<< 1 2 3 >>

*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Malware Name	Event Severity
2025-08-07 07:54:27	APU	10.101.37.96	94.237.61.249	Web threats	WEB Remote File Inclusion /etc/passwd	-	5
2025-08-07 05:33:21	APU	157.230.254.238	219.93.16.135	Web threats	WEB PHPUnit CVE-2017-9841 Arbitrary Code Execution Vulnerability	-	4
2025-08-07 03:28:04	APU	42.52.196.52	210.19.13.181	Web threats	WEB Dasan GPON Routers Command Injection -1.1 (CVE-2018-10561)	-	4
2025-08-06 22:37:38	APU	141.98.11.168	210.19.13.181	Web threats	WEB Nostromo Directory Traversal Remote Command Execution (CVE-2019-16278)	-	4

Total Web Threats: 57

4)

APU

ASIA PACIFIC UNIVERSITY

OF TECHNOLOGY & INNOVATION

Dashboard

Statistics

Alert

Incident

Threat Intelligence

ATI Trigger

Feed

Analysis

Report

Home > STIX > Threat Actor

+ +

apt32

Advanced Search

Hacker [MISP] APT32

Hacker [mitre-attack] APT32 - G0050

Observable

Indicator

COA

Exploit Target

Threat Actor

TTP

Campaign

Modified Time (Newest)

<< 1 >>

RI : 0

RI : 0

<< 1 >>

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)

[07-08-2025, 12:07:23 PM] (Log Radar limit: 1500) You have exceeded the Collector EPS limit. Excess incoming logs may be delayed until the EPS normalizes.

APU

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Dashboard

Statistics

Alert

Incident

Threat Intelligence

ATI Trigger

Feed

Analysis

Report

Repository

Home > STIX > Campaign

+

-

dust storm

Q

Advanced Search

[mitre-attack] Operation Dust Storm - C0016

Observable

Indicator

COA

Exploit Target

Threat Actor

TTP

Campaign

ed Time (Newest)

ee

ee

Campaign



S

Title * : Operation Dust Storm - C0016

Description * : [Operation Dust Storm]
(<https://attack.mitre.org/campaigns/C0016>) was a long-standing persistent cyber espionage campaign that targeted multiple industries in Japan, South Korea, the United States,

Status * :

Intended Effect :

Related Incidents :

Related TTPs :

Misdat - S0083 gh0st RAT - S0032
PoisonIvy - S0012 Malicious File - T1204.002
Malicious Link - T1204.001 Mis-Type - S0084
ZLib - S0086 Domains - T1583.001
Software Packing - T1027.002

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.