

# Attacks against media in the Philippines continue

 [qurium.org/alerts/philippines/attacks-against-media-in-the-philippines-continue/](https://qurium.org/alerts/philippines/attacks-against-media-in-the-philippines-continue/)

**June 22, 2021** (Updated: June 29, 2021)

**Note:** This forensic report is a LIVE DOCUMENT, new findings are added to the report constantly. We are still processing and analyzing the attack data recorded.

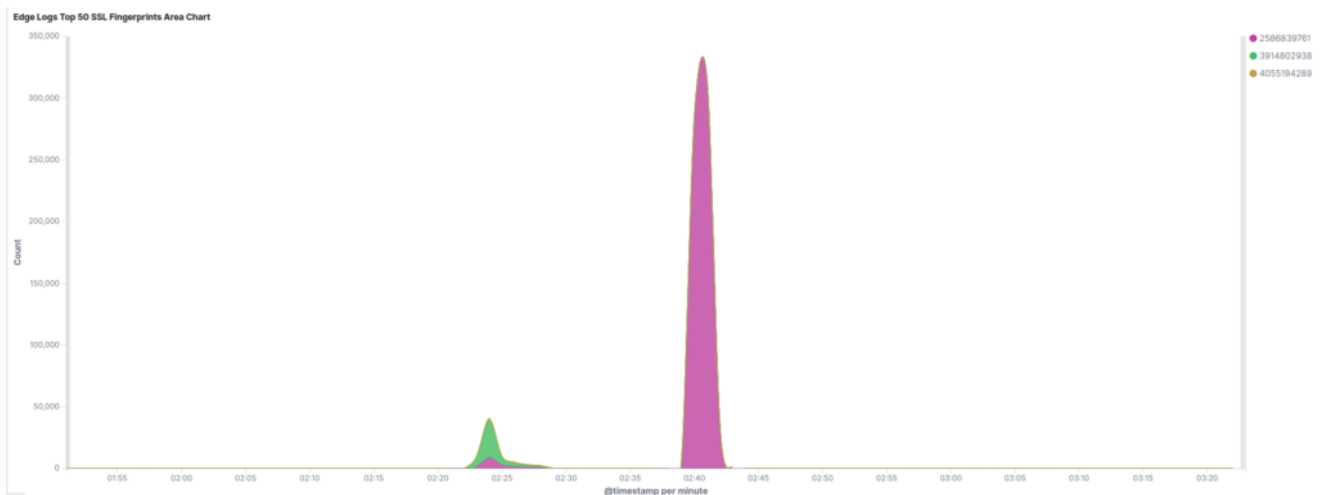
During the past month, Qurium has received brief but frequent denial attacks against the Philippine alternative media outlets [Bulatlat](#) and [Altermidya](#), as well as the human rights group [Karapatan](#).

This forensic report summarizes our findings and has been updated since the release of the first version to include the new findings.

## Summary of attacks

This section includes a brief summary of some of the attacks recorded during May – June 2021.

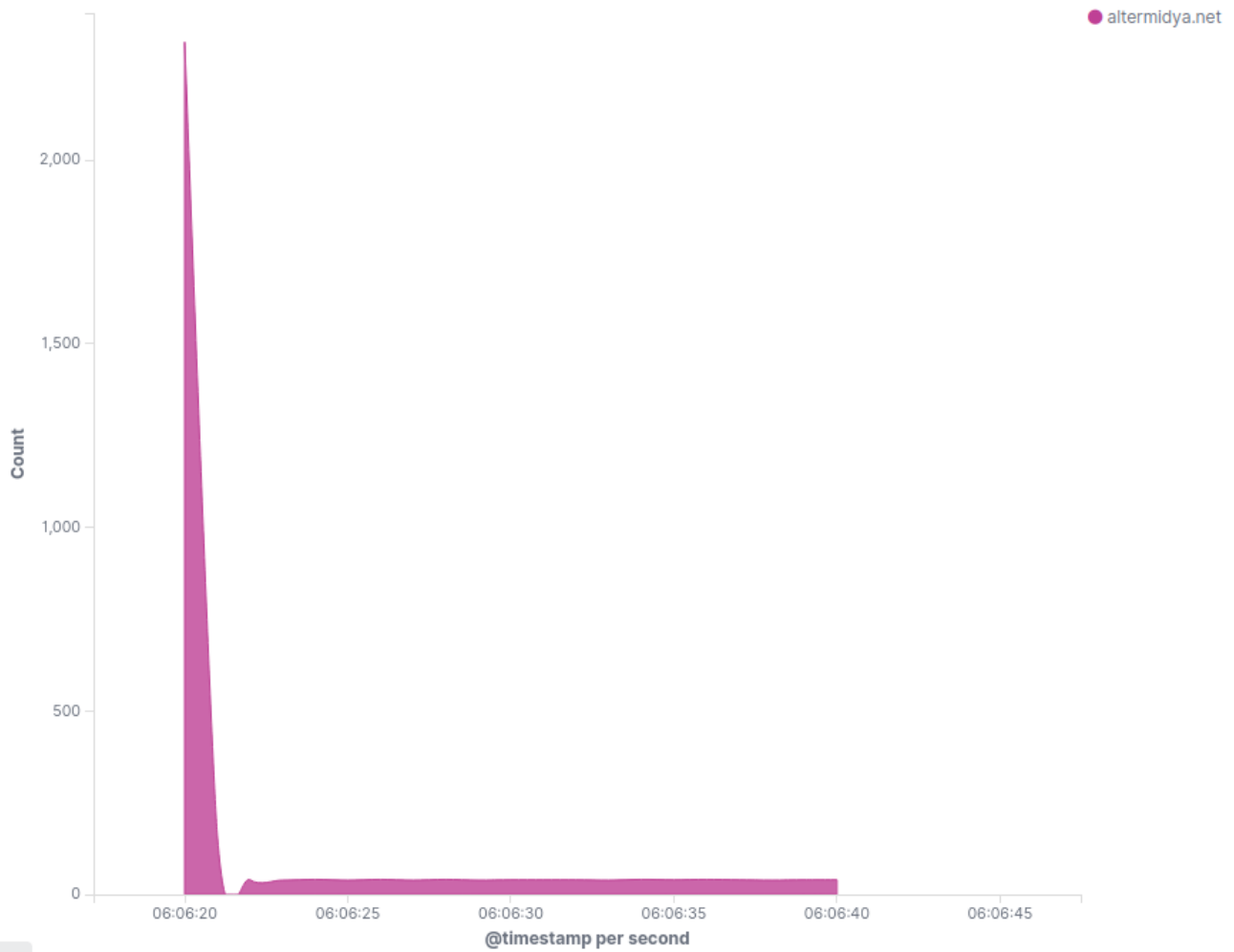
- 2021/05/17 02:24 HTTP POST flood against Bulatlat
- 2021/05/17 02:40 HTTP GET flood against Karapatan



These two attacks had specific signatures including the “SSL negotiation fingerprint”, the type of payload and that the service “[check-host](#)” was used by the attacker to verify if the attacks were successful.

2021/05/18 06:06 Using a server from [virmach.com](#) 23.95.9{.}155, the attacker floods [Altermidya](#) with requests using Apache Benchmark tool (ApacheBench/2.3)

### Edge Logs Top 20 Http Hosts



2021/05/18 07:33 A machine from the **Department of Science and Technology (PH)** with IP address 202.90.137{.}42 launches a vulnerability scan against Bulatlat. The sequence of the scan reassembles the use of the tool “Sn1per” from Xerosecurity.





Q Hosts v

202.90.137.42

### Basic Information

**Network** [DOST-PH-AP Department of Science and Technology \(PH\)](#)

**Routing** [202.90.128.0/19](#) via [AS9821](#)

**Protocols** [8094/HTTP](#)

## 8094/HTTP TCP

Telia

### Details

Q DETAILS

<https://202.90.137.42:8094>

**Request** GET /

**Protocol** HTTP/1.1

**Status Code** 400

**Status Reason** BadRequest

Sophos

### TLS

#### Handshake

**Version Selected** TLSv1\_2

**Cipher Selected** TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

#### Leaf Certificate

[866b4f40ec9b9af0f2c0ae9508550da128f80a3d07f21e2bbbb473518400a1b3](#)

emailAddress=support@ip-solutionsinc.net, C=PH, ST=NA, L=NA, O=IPSolutions Inc, OU=OU, CN=SophosApplianceCertificate\_C4307BK7HWCPJEB, emailAddress=support@ip-solutionsinc.net, emailaddress=support@ip-solutionsinc.net, C=PH, ST=NA, L=NA, O=IPSolutions Inc, OU=OU, CN=Sophos\_CA\_C4307BK7HWCPJEB, emailAddress=support@ip-solutionsinc.net

#### Issuer Chain

[b5c19a920fe4bc2415b64310a331feff8d54fba5a3bdef5266832c819a353393](#)

Certificate C4307BK7HWCPJEB signed by hardware supplier “IP Solutions Inc”  
A close look into the IP reveals that a **Sophos firewall** is behind the IP address. The appliance has a Certificate in the name of IP-Solutions Inc. The company (Lorna V. Zacate) signing the digital certificates of the appliances is a supplier of hardware and services to the Governmental Institutions in the Philippines.

### MISSION

To provide products and services that work base on the customers' unique requirements and to deliver what we promised on time.

### VISION

Is to build a long-term relationship with our customers by understanding what they need and to grow as their company expands, providing solutions necessary for business continuity.

Solutions and Services IP Solutions pride itself in partnering with products and services that best serve your needs. Network and Security – UTM, Next Gen Firewall, Endpoint Security, Encryption, Network Monitoring, Mobile Security, Network Access Control

### Contact Us

☎:(02) 6438944 / (02) 5144575  
☎:09189853177  
✉:sales@ip-solutionsinc.net

### Address

📍Unit 502 Solare Bldg,  
Capri Oasis Dr. Sixto Antonio Avenue,  
Maybunga, Pasig City  
Philippines

While searching for Sophos Firewall machines in the same network, we found another unit in the next IP 202.90.137{.}43, also with digital certificate in the name of IP Solutions Inc. This box also has a service in port 3400 with the details:

acepcionecejr{ @}army.mil.ph Taguig Red Server

The **RED Server** seems to refer to Sophos XG Technology RED, Remote Ethernet Device (*RED*) is a small network appliance that allows to build tunnels and internal networks.

2021-06-17

[Summary](#)[WHOIS](#)

### Basic Information

**Network** [DOST-PH-AP Department of Science and Technology \(PH\)](#)**Routing** [202.90.128.0/19](#) via [AS9821](#)**Protocols** [3400/UNKNOWN](#) , [8094/HTTP](#)

## 3400/UNKNOWN

TCP

NTT Communications

2021-06-17

### Details

Not Available

[DETAILS](#)

### TLS

#### Handshake

**Version Selected** [TLSv1\\_2](#)**Cipher Selected** [TLS\\_ECDHE\\_RSA\\_WITH\\_RC4\\_128\\_SHA](#)

#### Leaf Certificate

[a814c7baeb22ab26116f776fe916d3088d54734d3b4bfec0536b7628bf91da4a](#)

emailAddress=acepcionecjr@army.mil.ph, C=PH, L=Taguig, O=ARMY, CN=red\_server,

emailAddress=acepcionecjr@army.mil.ph

emailAddress=acepcionecjr@army.mil.ph, CN=ARMY Remote Ethernet Device CA, C=PH, L=Taguig, O=ARMY,

emailAddress=acepcionecjr@army.mil.ph

#### Issuer Chain

[9d4670da72d664b6fd6061e3db03a5e60e59c2ccc977b16e023c97e9e8a697e2](#)

Protocol RED. Port 3400 and TLS

We also found that the Marine Corps of the Philippines have their Scrollout F1 anti-spam mailservers inside of DOST, confirming the idea that military operates inside the IP space assigned to the Department of Science of Technology.

## Basic information

**OS** Microsoft Windows Server 2008 R2**Network** [DOST-PH-AP Department of Science and Technology \(PH\)](#)**Routing** [202.90.128.0/19](#) via [AS9821](#)**Protocols** [25/SMTP](#), [443/HTTP](#)

## 25/SMTP

TCP

Hurricane Electric

2021-06-25

## Details

Q DETAILS

**Banner** 220-scrolloutf1.marinecorps.mil.ph ESMTP - 220-scrolloutf1.mar  
220 scrolloutf1.marinecorps.mil.ph ESMTP - 220-scrolloutf1.mar**EHLO** 250-scrolloutf1.marinecorps.mil.ph  
250-PIPELINING  
250-SIZE 105092710  
250-ETRN  
250-STARTTLS  
250-ENHANCEDSTATUSCODES  
250 8BITMIME**Start TLS** 220 2.0.0 Ready to start TLS


Presence of other military infrastructure in the subnet

The certificate of the “RED” Sophos server provided the following information:

```
IP: 202.90.137.43  
emailAddress = acepcioneclr{@}army.mil.ph  
Country = PH  
Location = Taguig  
Organization = ARMY
```

Using RiskIQ we searched for the history of certificates of 202.90.137{.}43 and 202.90.137{.}42 and we found that the certificate of the attacker IP “.42” has been seen in another providers.

```
AS17639 ComClark Network & Technology Corp.|121.58.209.215|  
AS9821 Department of Science and Technology|202.90.137.42|  
AS6648 Bayan Telecommunications, Inc.|125.212.41.130|  
AS17639 ComClark Network & Technology Corp.|121.58.248.18|
```


9042f66cdd830c59f5cc7b92895d05f93f358cc
121.58.209.215
www.threepointing.synology.me
Enterprise

Certificate Search

DATA

Filters 0

- SHA 1 (1/3)
  - 9042f66cdd830c59f5cc7b92895d05f93f358cc 1
- HITS! 5626 (1/1)
  - 2019-01-18 1
- LAST SEEN (1/1)
  - 2021-02-17 1
- UNIQUE IP (4/4)
  - 121.58.209.215 1
  - 121.58.248.18 1
  - 125.212.41.130 1
  - 121.58.248.10 1


SSL Certificate Search

1 of 1 | Sort: Last Seen Descending | 25 / Page

SHA-1	First Seen	Last Seen	Infrastructure
9042f66cdd830c59f5cc7b92895d05f93f358cc	2019-01-17	2021-03-16	121.58.209.215 202.90.137.42 125.212.41.130 121.58.248.10

Serial Number: 120/486090402/5/7950  
 Issued: 2019-01-08  
 Expires: 2036-12-30  
 Common Name: Sophos\_CA\_CA3078K7HWCPJES (subject)  
 Sophos\_CA\_CA3078K7HWCPJES (issuer)  
 Alternative Names:  
 Organization Name: IPSolutions Inc. (subject)  
 IPSolutions Inc. (issuer)

But the most interesting finding was when we did a search for certificates containing the email: `acepcionechr{@}army.mil.ph` in Censys.


Certificates
"acepcionechr@army.mil.ph"

---

**Quick Filters**  
For all fields, see [Data Definitions](#)



Tag:

- 2 Unexpired
- 2 Never Trusted

Issuer:

- 1 ARMY
- 1 OG2-PA

**Certificates**  
Page: 1/1 Results: 2 Time: 464ms

- 
 emailAddress=acepcionechr@army.mil.ph, C=PH, L=Taguig, O=OG2-PA, CN=red\_server, emailAddress=acepcionechr@army.mil.ph  
 OG2-PA Remote Ethernet Device CA  
 2021-05-29 – 2038-01-01
- 
 C=PH, L=Taguig, O=ARMY, CN=red\_server, emailAddress=acepcionechr@army.mil.ph  
 ARMY Remote Ethernet Device CA  
 2018-06-14 – 2038-01-01

Another certificate showed up! This one contained the (O)rganization name= **OG2-PA**

## What is OG2-PA?

In the context of the military jargon, OG2 stands for Office of the Assistant *Chief of Staff* for *Intelligence* and PA stands for Philippine Army.



**OFFICE OF THE ASSISTANT  
CHIEF OF STAFF FOR INTELLIGENCE  
OG2, PHILIPPINE ARMY**



## Wikipedia Edits

Another interesting finding is that the attacker's IP address is present in the Edits of the Wikipedia page for "Chief of Army (Philippines)" and many other pages related to the Army.

### Chief of the Army (Philippines): Revision history

[View logs for this page](#) ([view filter log](#))

#### Filter revisions

External tools: [Find addition/removal](#) (Alternate) • [Find edits by user](#) (Alternate) • [Page statistics](#) • [Pageviews](#) • [Page history](#)

For any version listed below, click on its date to view it. For more help, see [Help:Page history](#) and [Help:Edit summary](#). **m** = minor edit, **→** = section edit, **←** = automatic edit summary

(newest | oldest) View (newer 50 | older 50) (20 | 50 | 100 | 250 | 500)

#### Compare selected revisions

- [\(cur | prev\)](#)  02:12, 10 June 2021 202.90.137.42 (talk) . . (42,751 bytes) (+17) . . [\(undo\)](#)

### Armed Forces of the Philippines Command and General Staff College: Revision history

[View logs for this page](#) ([view filter log](#))

#### Filter revisions

External tools: [Find addition/removal](#) (Alternate) • [Find edits by user](#) (Alternate) • [Page statistics](#) • [Pageviews](#) • [Fix dead links](#)

For any version listed below, click on its date to view it. For more help, see [Help:Page history](#) and [Help:Edit summary](#). (cur) = difference from current version, (prev) = difference from preceding version, **m** = minor edit, **→** = section edit, **←** = automatic edit summary

#### Compare selected revisions

- [\(cur | prev\)](#)  22:10, 7 May 2021 WereSpielChequers (talk | contribs) . . (5,880 bytes) (+3) . . [\(c/e\)](#) [\(undo\)](#)
- [\(cur | prev\)](#)  08:16, 8 January 2021 202.90.137.42 (talk) . . (5,877 bytes) (+28) . . [\(undo\)](#)
- [\(cur | prev\)](#)  02:12, 31 December 2019 112.206.32.31 (talk) . . (5,849 bytes) (-4) . . [\(→See also\)](#) [\(undo\)](#)
- [\(cur | prev\)](#)  03:45, 21 February 2019 202.90.137.43 (talk) . . (5,853 bytes) (+8) . . [\(undo\)](#)
- [\(cur | prev\)](#)  03:43, 21 February 2019 202.90.137.43 (talk) . . (5,845 bytes) (-1) . . [\(→Mission\)](#) [\(undo\)](#)
- [\(cur | prev\)](#)  05:52, 21 September 2018 202.90.137.43 (talk) . . (5,846 bytes) (+1) . . [\(→Lineage of Commanding Officers\)](#) [\(undo\)](#)
- [\(cur | prev\)](#)  05:51, 21 September 2018 202.90.137.43 (talk) . . (5,845 bytes) (+2) . . [\(undo\)](#)

We could also reconfirm that other IP addresses using the same digital certificate had also make similar edits.

# User contributions for 125.212.41.130

For 125.212.41.130 ([talk](#) | [block log](#) | [logs](#) | [filter log](#))

## ▼ Search for contributions

([newest](#) | [oldest](#)) View ([newer 50](#) | [older 50](#)) ([20](#) | [50](#) | [100](#) | [250](#) | [500](#))

- [06:21, 10 January 2019](#) ([diff](#) | [hist](#)) . . [\(+4\)](#) . . [Roman Catholic Diocese of Kidapawan](#) ([→History](#))
- [06:07, 10 January 2019](#) ([diff](#) | [hist](#)) . . [\(0\)](#) . . [Roman Catholic Archdiocese of Cotabato](#) ([→Ordinaries](#))
- [23:33, 15 October 2018](#) ([diff](#) | [hist](#)) . . [\(+8\)](#) . . [National Defense College of the Philippines](#)
- [23:28, 15 October 2018](#) ([diff](#) | [hist](#)) . . [\(-13\)](#) . . [Philippine Military Academy](#)

## Linking .42 and .43 addresses

During our research we could confirm that (1) both address run similar hardware, Sophos XG and RED tunneling, (2) both boxes have digital certificates of the hardware supplier “IP Solutions Inc” and (3) that their very first certificates were issued 2015-07-31 (Source: RiskIQ)

### 202.90.137.42 – aka Sn1per

#### CHANGE HISTORY

##### Current Record

c3258272595a3908bb607944d993ab19ebe28b19

##### 2020-04-27

9042f66cdd830c59f5ccf7b92895d05f93f358ce

##### 2019-08-16

dc07ec8554fb43f043784d745b16934eea5e9e5e

##### 2019-07-17

52df63d34c652066e4e873abcba55ad605481b62

##### 2019-07-08

8aa2d32fcb0be0d1819100c1371a5807df11cf20

#### CERTIFICATE

##### 2019-07-11

SHA-1	8aa2d32fcb0be0d1819100c1371a5807df11cf20
Serial Number	91385591299
Issued	2015-07-31
Expires	2036-12-31
Common Name	SophosApplianceCertificate_C4307BK7HWCPJEB (subject) Sophos_CA_C4307BK7HWCPJEB (issuer)

#### Alternative Names

Organization Name	IPSolutions Inc (subject) IPSolutions Inc (issuer)
-------------------	---

### 202.90.137.43 – aka acepcionejr

#### CHANGE HISTORY

##### Current Record

1912032199b43cff13e10ac7e2f5c3bc6c19e2e9

##### 2019-09-25

96ee1744e2107e7574e85d28269e379d30c794d0

#### CERTIFICATE

##### 2019-09-25

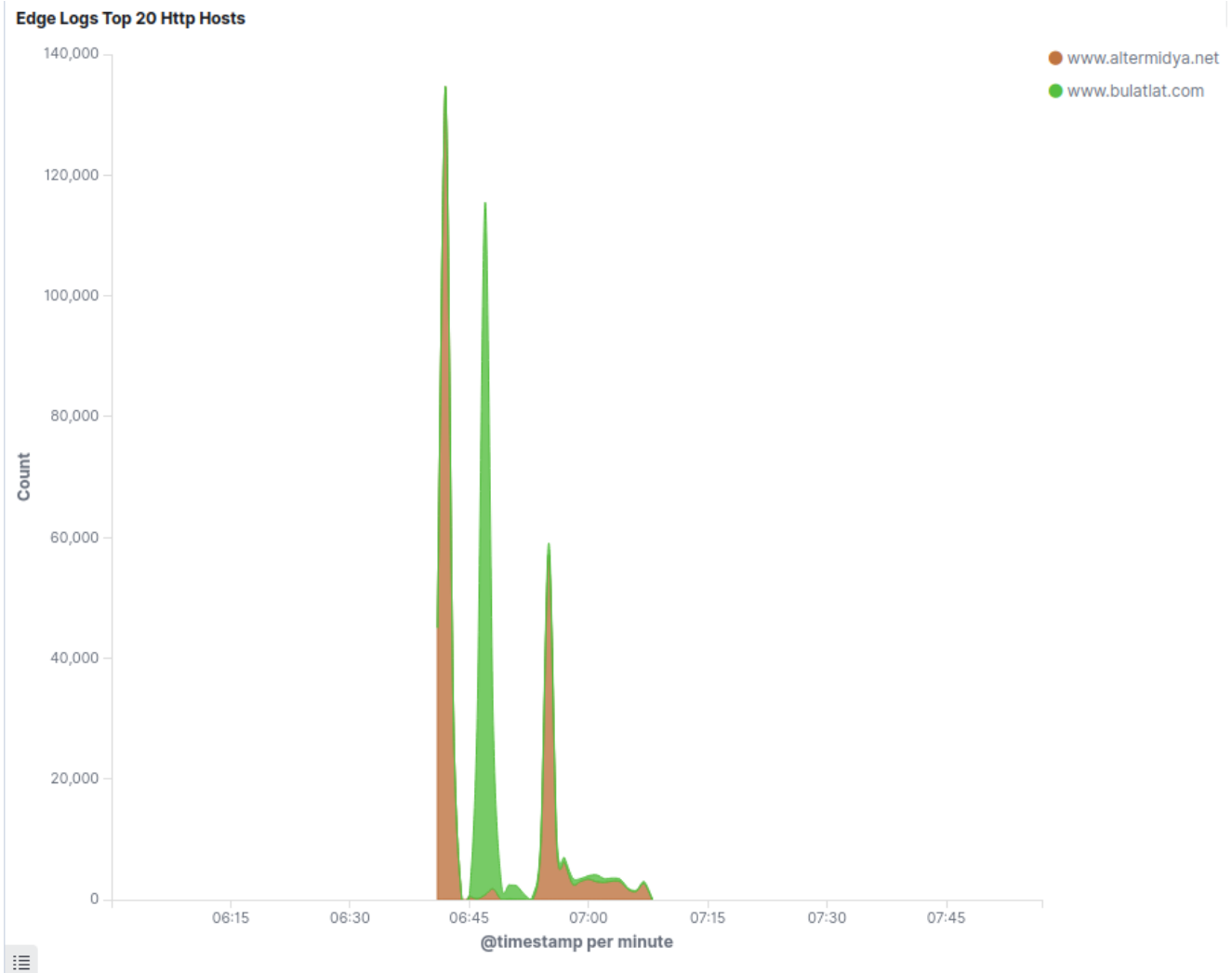
SHA-1	96ee1744e2107e7574e85d28269e379d30c794d0
Serial Number	90749376532
Issued	2015-07-31
Expires	2036-12-31
Common Name	SophosApplianceCertificate_S4307B02E1677FD (subject) Sophos_CA_S4307B02E1677FD (issuer)

#### Alternative Names

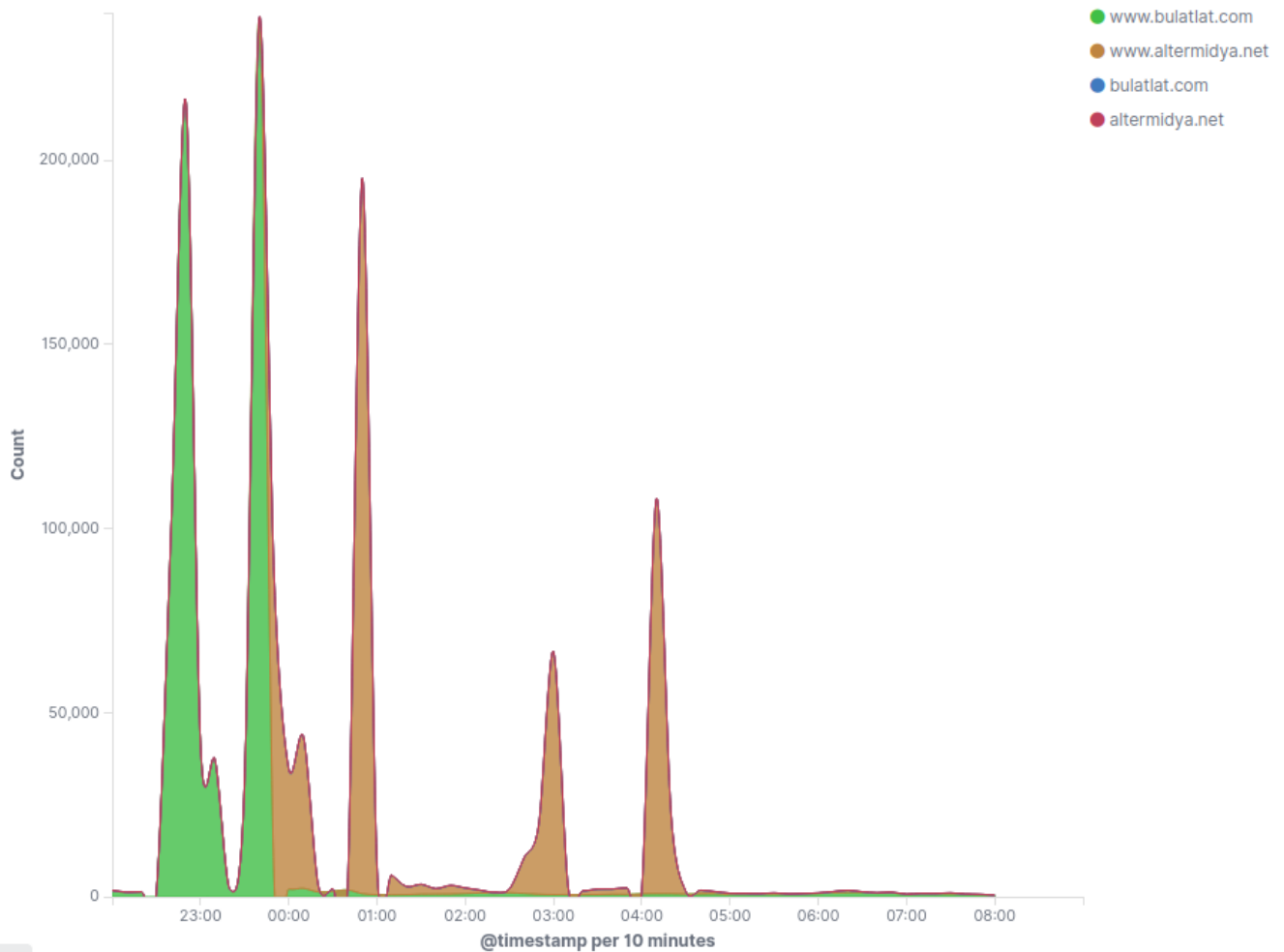
Organization Name	IPSolutions Inc (subject) IPSolutions Inc (issuer)
-------------------	---

## Attacks continue

- 2021/05/20 13:05 Karapatan receives a small flood with user-agent AdobeUxTechC4-Async/3.0.12 (win32). The machine 188.63.78{.}119 crawls heavily media from the Philippines.
- 2021/06/16 06:42 Large flood on Altermidya and Bulatlat from multiple IP addresses. Floods include requests of the type /?u144642756919q213158629662aB2146578135208224622277442H and user agent: null



2021/06/22 22:50 – 2021/06/23 – 03:00 Attacks against Bulatlat and Altermidya for several hours. During the DDOS attacks a pen testing against the sites was conducted.



The attacker launched a “Denial of Service” against bulatlat.com, flooding the site with requests of the type GET /?q=123456789. At the very same time the attacker run “Nikto” to pen test the site. The flood run 1000+ faster that the pen testing script. We have sample down 1/1000 the “Denial of Service” logs to visualize the attack.



```
role: ABUSE ASTIPH
address: Advanced Science and Technology Institute
address: ASTI Bldg., Technopark, C.P. Garcia Ave.,
address: U.P. Campus, Diliman, Quezon City
country: ZZ
phone: +0000000000
e-mail: ops@pregi.net
admin-c: DFV1-AP
tech-c: DFV1-AP
nic-hdl: AA2050-AP
remarks: Generated from irt object IRT-ASTI-PH
abuse-mailbox: ops@pregi.net
mnt-by: APNIC-ABUSE
last-modified: 2020-10-20T00:56:09Z
source: APNIC

person: Denis F. Villorente
nic-hdl: DFV1-AP
e-mail: denis@asti.dost.gov.ph
address: Advanced Science and Technology Institute
address: ASTI Bldg., Technopark, C.P. Garcia Ave.,
address: U.P. Campus, Diliman, Quezon City
phone: +63-2-426-9755
fax-no: +63-2-426-9756
country: PH
mnt-by: MAINT-PH-DOST
last-modified: 2008-09-04T07:29:17Z
source: APNIC
```

Abuse contact details for the network

[29 June 2021] The public official response that we have read in the media:

- Rowena Cristina Guevara (DOST-ASTI) told the [PNA](#) that addresses were received from the Regional Registry (APNIC) and DOST provides IP space to other Governmental Agencies.
- That Qurium traced the attack to the IP address does not mean the DOST involvement.
- DOST-ASTI has not made public which Governmental Agency is behind the IP address.
- The army spokesman Col. Ramon Zagala [stated](#) that the Philippine Army “respects freedom of expression and per policy, will never infringe that freedom”.
- In a Zoom interview for [ABS-CBN](#), DOST confirmed that the IP space belongs to an “Agency” which name can not be revealed not to burden DICT investigation.

Our open questions still remain:

1. Which Organization or Institution operates behind the address 202.90.137{.}42?
2. Why such organization and their Abuse Handling details are not properly reflected in the APNIC Whois Database or any other public resource to speed up “Network Abuse” resolution?
3. Who is acepcioneclr @ army.mil.ph?

## Media coverage

---

- [2 Jul 2021] The Register [Digital rights org claims cyberattacks against Filipino media outlets come from government and army](#)
- [30 Jun 2021] ABS-CBN [DOST, Army asked to clarify alleged links to cyberattacks](#)
- [29 Jun 2021] Inquirer.net [Probe cyberattacks](#)
- [24 Jun 2021] CNN [Palace: ‘Unfair’ to link govt. agencies to cyberattacks on alternative news sites pending probe](#)
- [23 Jun 2021] Rappler [Military, DOST links found in DDoS attacks on media – report](#)