The Registry of ccTLD .lv

Network Solutions Department,
Institute of Mathematics and Computer Science,
University of Latvia

Raina bulv. 29
Riga LV1459, LATVIA

August 2, 2010

An Open Letter
To: Everyone who works to make the Internet a Better Place

Dear Sir/Madam,

We are writing this letter on behalf of the incident response team CERT NIC.LV run by the Registry of the country code Top Level Domain .lv (NIC.LV) – the Network Solutions Department of the Institute of Mathematics and Computer Science, University of Latvia.

This letter was motivated by our recent conflict with the Spamhaus project, the international non-profit organisation that has the mission to track the Internet's spam operations and to provide dependable real-time anti-spam protection (hereinafter referred to as Spamhaus).

CERT NIC.LV strongly believes that:

1) **No-one can be declared a criminal other than according to the law,** i.e. after a fair trial at court with the right to appeal;
2) **No Internet user should be punished for the actions of another Internet user.** As nations around the globe recognise that access to the Internet is basic human right it is unacceptable to block access of those who have not committed any illegal or improper acts;
3) In fighting undesirable and potentially criminal activities on the Internet **we must avoid using questionable means to stop wrongdoers**;
4) **All countries, companies or individuals should be treated equally** and not be discriminated against for reasons of size, level of income, position or any other characteristics.

We believe that deviation from these basic principles will not make the Internet a safer or more secure place.

In fulfilling their mission **Spamhaus appears to disregard these principles; disregard commonly accepted CERT community best practice and disregard basic legal principles.** The consequence of their actions is to put the basic rights of thousands of law-abiding Internet users at risk.

In the light of our conflict with Spamhaus (as documented in the report attached to this letter) we invite members of the community and other interested stakeholders to **strongly reject the unfair and unreasonable behaviour of Spamhaus**. We think it is time to appoint an **independent adjudicator** to mediate on issues of disagreement between Spamhaus (or any other entity exercising its power in an unjust way) and the user community. Whilst we do not support spam or any other illegal activity in any form it remains our mission to **protect the rights of law-abiding users**. We hope that the community will not stand aside.

NIC.LV thanks everyone who helped in solving the situation when our IP addresses were wrongly blocked by Spamhaus. NIC.LV is willing and ready to participate in any activities which would lead to a fair handling of incidents and, as a result, to the safer and more secure Internet.

Sincerely,

Katrina Sataki
Manager of NIC.LV

Baiba Kaškina
Manager of CERT NIC.LV

Tel. +371 7085858 • Fax: +371 67225072 • E-mail: dns@nic.lv • Web: www.nic.lv
CERT E-mail: cert@nic.lv • CERT Web: cert.nic.lv

CERT NIC.LV vs Spamhaus

Report

Parties involved:

Institute of Mathematics and Computer Science, University of Latvia:

- NIC.LV – Network Solutions Department of the Institute, the Registry of ccTLD .lv
    - CERT NIC.LV – Computer Emergency Response Team run by NIC.LV
- SigmaNet – Academic Network Laboratory of the Institute, National Research and Education Network.

LATNET Serviss – private company

Microlines – private company

The "guilty" customer – a customer of Microlines

Spamhaus - an international nonprofit organization

IP addresses affected:

92.240.64.0/19 (AS5538, Institute of Mathematics and Computer Science)
159.148.79.0/24 (AS2588, LATNET Serviss)
79.135.128.0/19 (AS2588, LATNET Serviss, allocated to Microlines)

IP addresses Spamhaus complained about:

Initially **79.135.128.0/19** (AS2588, LATNET Serviss, allocated to Microlines)
After update: **79.135.128.xy** and **79.135.128.xz**

Executive Summary

The incident: on **04.06.2010** Spamhaus added to its blacklist a part of **AS5538 - 92.240.66.32/27.** Soon after, on **13.07.2010** it blacklisted the entire **92.240.66.0/24** network. This document maintains that this was a premature, unfair and unacceptable action.

SigmaNet, a department at the Institute of Mathematics and Computer Science (IMCS), hosts and maintains an e-mail cluster that is within the IP address space of the blacklisted network 92.240.66.0/24. This mail cluster is used by other departments of the IMCS, including NIC.LV – the Registry of the Top Level Domain .lv and CERT NIC.LV – incident response team hosted by NIC.LV. The mail cluster is also used by many academic users of Latvia, state and municipal institutions, non-profit organisations, companies, and individuals.

The reason for blacklisting was the fact that regional Internet service provider Microlines – the user of the IP address space **79.135.128.0/19** – did not deny Internet access to its customer allegedly hosting C&C controllers running a large botnet DDoS attack.

Spamhaus identified that the upstream provider of Microlines was LATNET Serviss (**AS2588**) using *traceroute* information. Spamhaus found an abuse report e-mail of LATNET Serviss – **abuse@latnet.lv** in the RIPE database. However, instead of sending an incident report with evidentiary information and asking to resolve the incident, Spamhaus decided to blacklist IP addresses of Microline's upstream provider, i.e. LATNET Serviss. Spamhaus identified that the IP address (92.240.66.33) of the MX record of the domain name *latnet.lv* was used for abuse reports. With no additional checks Spamhaus blacklisted 92.240.66.32/27 from **AS5538** – the Autonomous System belonging to the Institute of Mathematics and Computer Science, which is also the holder of the domain name *latnet.lv*.

E-mail address *abuse@latnet.lv* is the contact of LATNET Serviss for abuse reports, while incident reports received at *abuse@latnet.lv* are handled by CERT NIC.LV according to the agreement between IMCS and LATNET Serviss[1].

Detailed information and e-mail exchange between the parties is given in Chapter 2.1 on page 7 and Chapter 2.2 on page 13 of this document.

Once the IP addresses of IMCS were delisted, Spamhaus blacklisted IP addresses of the upstream provider of Microlines – LATNET Serviss – without giving CERT NIC.LV time to investigate and solve the incident (see Chapter 2.3 on page 16).

[1] According to agreement CERT NIC.LV provides incident response services to LATNET Serviss. Abuse and incident report sent to abuse@latnet.lv are received and processed by the CERT NIC.LV team in accordance with the CERT NIC.LV Description, Version 2.1, document OID: 1.3.6.1.4.1.28446.2.1.2.1 and RFC 2350.

The people from Spamhaus have been impolite, arrogant and even rude (see examples on pages 19 and 20) during the incident response process. They accused Latvian ISPs in their e-mails despite the very serious technical mistakes in their own decisions and judgement. Their attitude and actions showed that not all internet users are treated equally by them. Instead, they differentiate users by the size of the representative nations (see page 19). We at CERT NIC.LV regard this as an unacceptable behaviour.

LATNET Serviss rightfully asked CERT NIC.LV where they could seek for protection and appeal against the unlawful actions by Spamhaus. CERT NIC.LV had to admit that at the moment there is no organisation where an ISP or a user could ask for a quick and just opinion when their rights to access the Internet or part of Internet services are denied. In fact, organisations such as Spamhaus can act without any supervision according to rules defined by themselves and for themselves.

We do not support spam or any other illegal activity in any form. Our CERT team has been proud to be a member of FIRST and Trusted Introducer. We have always believed in principles commonly accepted by the CERT community worldwide. Therefore we do not and cannot accept the approach taken by Spamhaus. We invite members of the community and other interested stakeholders to **strongly reject the unfair and unreasonable behaviour of Spamhaus**. We also invite anyone who cares for the future of the Internet to start discussions about the appointment of an **independent adjudicator** to mediate on issues of disagreement between any entity exercising its power in an unjust way and the user community.

Table of Contents

1. Background Information

CERT NIC.LV is run by the Registry of the country code Top Level Domain .lv (NIC.LV) – the Network Solutions Department of the Institute of Mathematics and Computer Science, University of Latvia (IMCS).

IMCS was established in 1959 as Computing Centre of research character. The staff of IMCS consists of 220 researchers, assistants, engineers, and software developers.

IMCS is also one of the largest Internet service providers in Latvia. Academic Network Laboratory – another department of the IMCS – began its operation under the name LATNET in 1993, offering e-mail and dial-up services to the academic community of Latvia, as well as to state institutions, companies, individuals. The laboratory was renamed to SigmaNet in 2007 and continues providing e-mail, hosting and data centre services to thousands of its customers. Other departments of the IMCS, including NIC.LV and its CERT team, also use mail clusters maintained by SigmaNet.

Domain name latnet.lv was registered by IMCS as one of the first domain names under .lv in 1993. IMCS still is the holder of the domain name latnet.lv. The domain name latnet.lv is still used by many customers of IMCS in their e-mail addresses.

LATNET Serviss SIA (LATNET Serviss Ltd.) was registered in 1994 with the main objective to develop radio link backbone network throughout the country. The company closely collaborated with the Academic Network Laboratory LATNET (currently SigmaNet). Many customers of LATNET Serviss, including those who do not have their own domain names and prefer e-mail address @latnet.lv, have used and still use e-mail services provided by SigmaNet. Hostnames under latnet.lv are still assigned to many devices of LATNET Serviss.

The daughter company of LATNET Serviss – **LATNET Datu Centrs** – was created to provide e-mail, hosting and data centre services to the customers of LATNET Serviss and other organisations and individuals in Latvia.

LATNET Serviss also serves as an upstream provider to many regional subproviders. One of its subproviders is **Microlines** which offers internet services to the customers in its area.

IMCS has concluded an agreement with LATNET Serviss on the provisioning of incident response services by CERT NIC.LV. E-mails sent to abuse@latnet.lv are received and processed by the CERT NIC.LV team in accordance with the CERT NIC.LV Description, Version 2.1, Document OID: 1.3.6.1.4.1.28446.2.1.2.1 and RFC 2350.

The relationship between the organisations mentioned above is shown in **Figure 1 – Organisations involved and their relations**, page 6.

The **Spamhaus Project** is an international nonprofit organization whose mission is to track the Internet's spam operations, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spammers worldwide, and to lobby governments for effective anti-spam legislation. Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated team of 28 investigators and forensics specialists located in 8 countries[2].

[2] http://www.spamhaus.org/organization/index.lasso

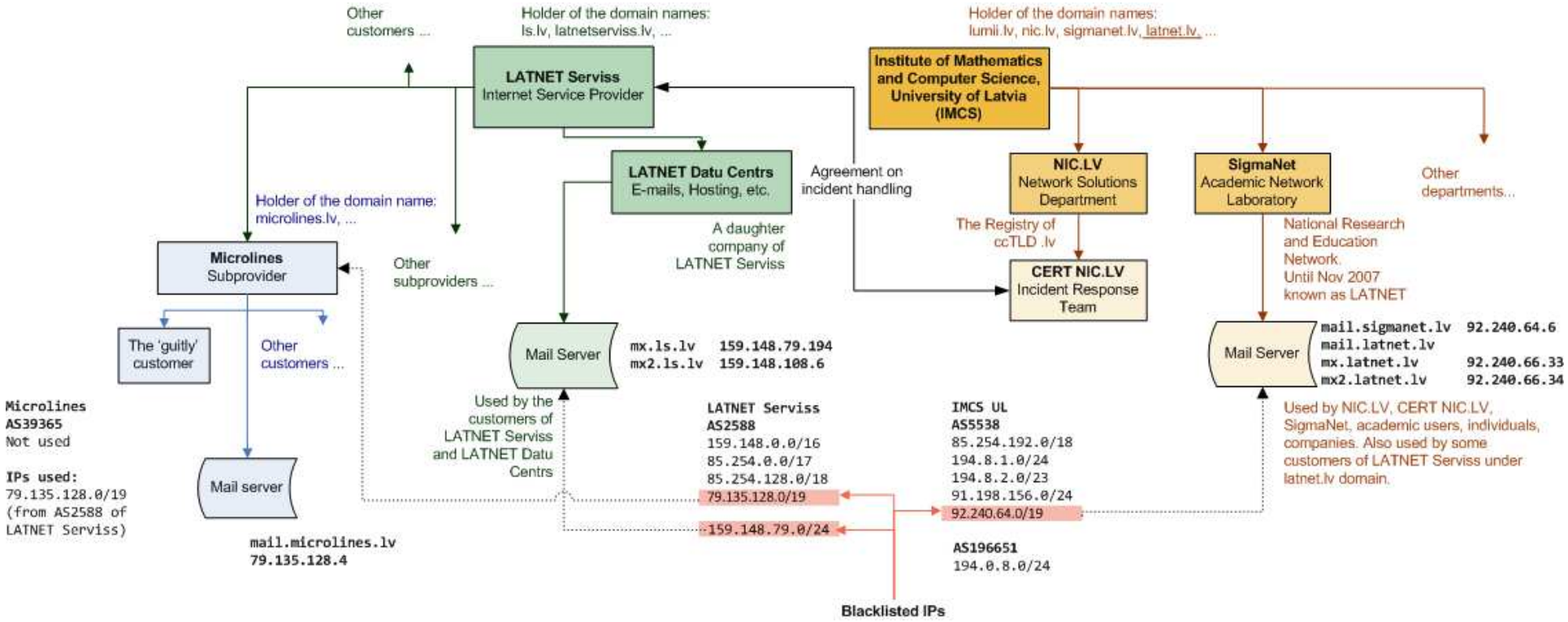


Figure 1 – Organisations involved and their relations

Abuse mailboxes:

IMCS – abuse@latnet.lv, abuse@nic.lv, cert@nic.lv

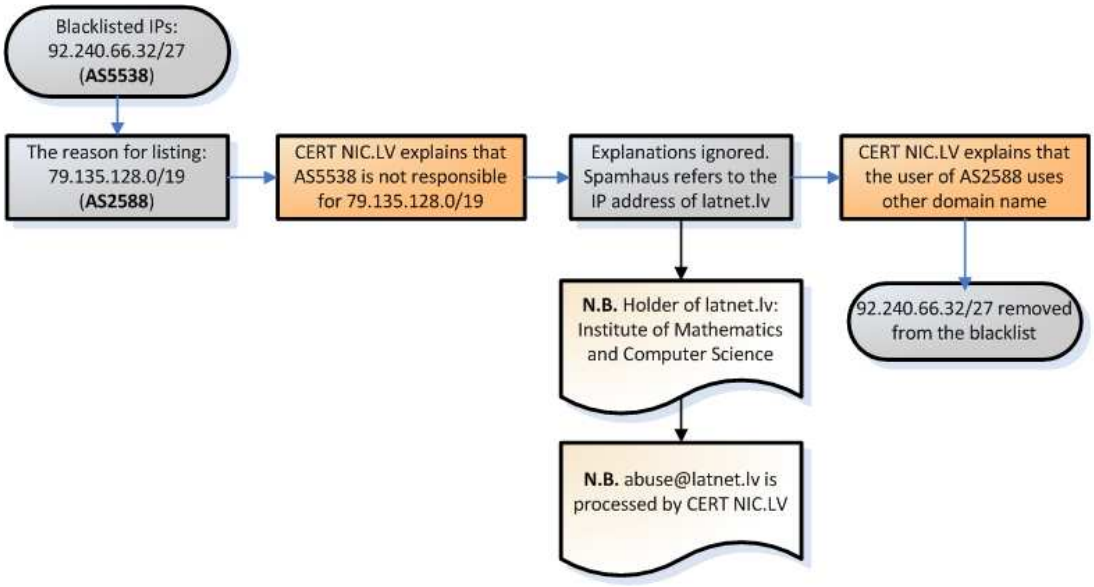
LATNET Serviss and **LATNET Datu Centrs** – abuse@latnet.lv, processed by CERT NIC.LV

Microlines – info@microlines.lv

2. Incident Analysis

2.1. Blacklisted IPs – 92.240.66.32/27

2.1.1. Graphical Overview



2.1.2. Description

On 04.06.2010 Spamhaus added to its blacklist a part of AS5538 - 92.240.66.32/27. 92.240.66.32/27 are IP addresses of the e-mail cluster hosted and maintained by SigmaNet, one of the departments of the Institute of Mathematics and Computer Science (IMCS). This mail cluster is used by other departments of the IMCS, including NIC.LV – the Registry of the Top Level Domain .lv, and CERT NIC.LV – incident response team hosted by NIC.LV. The mail cluster is also used by many academic users of Latvia, state and municipal institutions, non-profit organisations, companies, and individuals. These users have not violated Internet usage policies and were not liable for any actions taken by any other Internet user.

Spamhaus to CERT NIC.LV: Fri, 04 Jun 2010 11:44:14 +0300

SBL91402 - The Spamhaus Project - SBL International Anti-Spam System

---

Hello latnet.lv Abuse Desk,

This is an automated message from the Spamhaus Block List (SBL) database to advise you that the IP below has been added to sbl.spamhaus.org:

IP/cidr: 92.240.66.32/27
Problem: Spammer hosting (escalation) : microlines.lv

SBL Ref: SBL91402

The reason for listing the IP address(es) is explained at the url:

http://www.spamhaus.org/sbl/sbl.lasso?query=3DSBL91402

Microlines is one of the regional Internet service providers. Upstream provider of Microlines is LATNET Serviss.

CERT NIC.LV team contacted Spamhaus and explained the situation[3]:

CERT NIC.LV to Spamhaus: Fri, 04 Jun 2010 12:54:51 +0300

Hello!

IP address 92.240.66.32 is blocked using wrong escalation procedure!

IP address block 79.135.128.0/19 Microlines has no network peering trough 92.240.64.0/19, AS5538.

http://www.robtex.com/route/79.135.128.0-19.html

Its totally wrong way to block AS5538 as responsible to 79.135.128.0/19 problems!

Please remove 92.240.66.32 from blacklist!

The link given in this e-mail perfectly shows that IP addresses of Microlines have nothing to do with the AS5538. As can be seen from the picture below, IP addresses 79.135.128.0/19 are announced via AS2588, the AS of LATNET Serviss:

[3] The language in the e-mails is not edited and kept as in originals

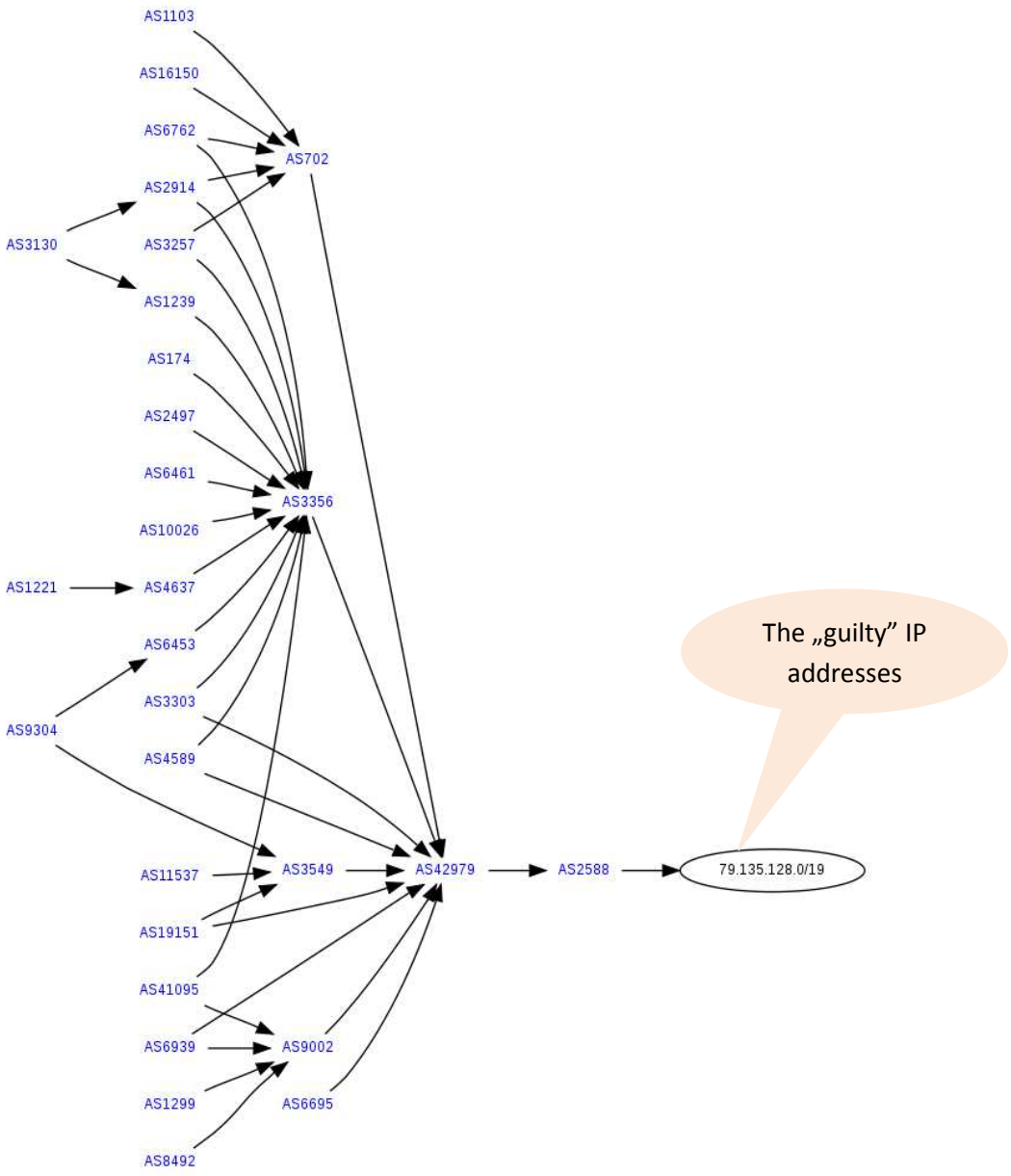


Figure 2 – Routing of 79.135.128.0/19 [4]

Meanwhile, the blacklisted IPs 92.240.66.32/27 were from AS5538. CERT NIC.LV wrongfully assumed that Spamhaus would investigate properly and see the whole picture:

[4] http://www.robtex.com/route/79.135.128.0-19.html

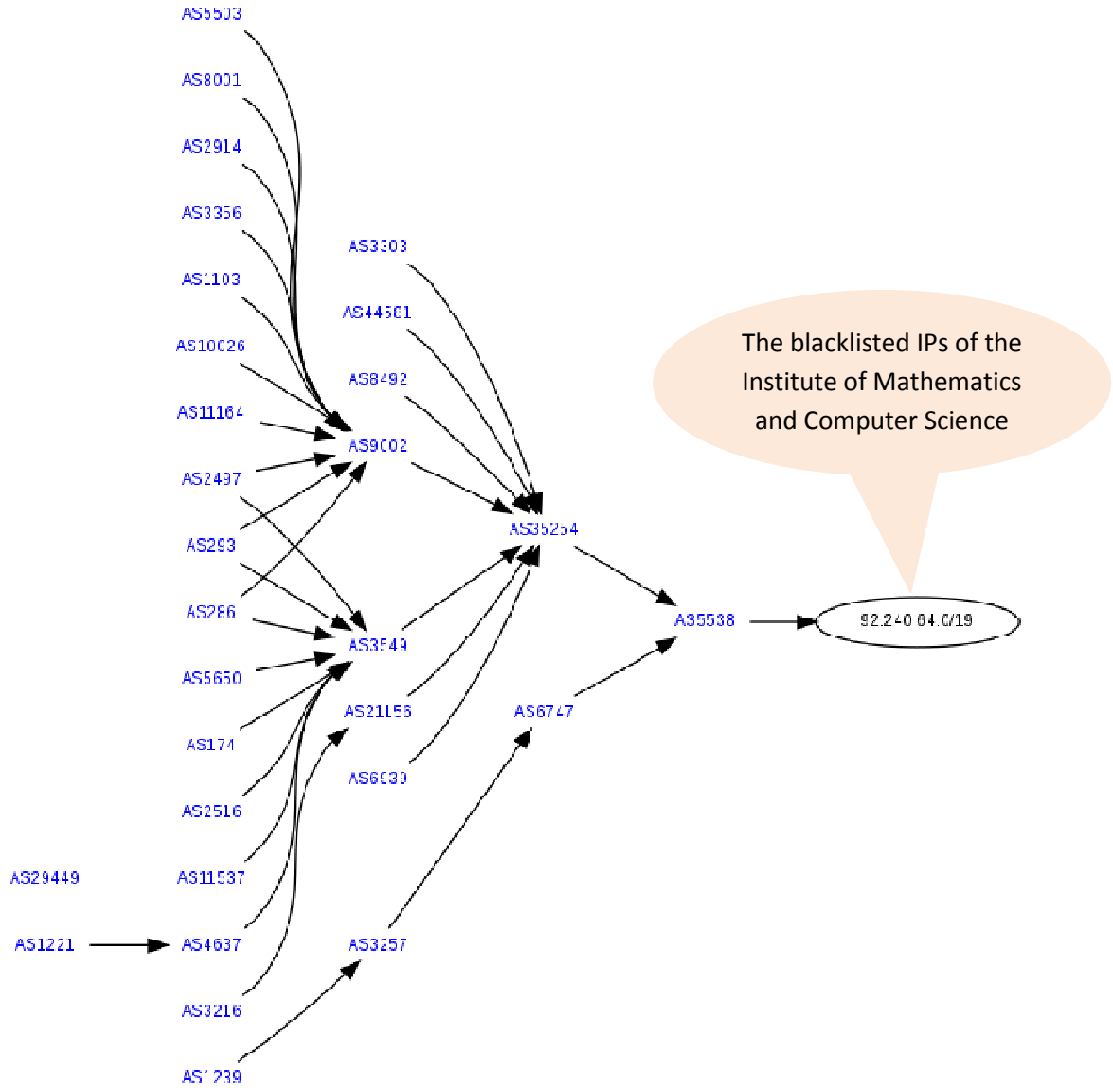


Figure 3 – The routing of the blacklisted IPs of the IMCS[5]

The following e-mail response to CERT NIC.LV's e-mail explaining the difference between the two AS, was received from Spamhaus:

Spamhaus to CERT NIC.LV: Fri, 04 Jun 2010 13:20:22 + 0300:

Hello!

Please explain traceroute:

tv6st-l3.v65.latnetserviss.lv (159.148.43.66) [AS 2588] 36 msec 36 msec 36 msec
titan-gw.v35.latnetserviss.lv (159.148.22.2) [AS 2588] 32 msec 32 msec 36 msec
tornado-gw.v846.latnetserviss.lv (159.148.16.214) [AS 2588] 32 msec 32 msec

[5] http://www.robtex.com/route/92.240.64.0-19.html

36 msec
microlines.to.latnetserviss.lv (159.148.16.210) [AS 2588] 40 msec 36 msec 40 msec
gw-2.microlines.lv (79.135.128.35) [AS 2588] 36 msec 36 msec 40 msec
155.152.135.79.microlines.lv (79.135.152.155) [AS 2588] 36 msec 36 msec 36 msec

aut-num: AS2588
as-name: LatnetServiss-AS
descr: LATNET ISP
member-of: AS-LATVIA

mx.latnet.lv A 92.240.66.33
mx2.latnet.lv A 92.240.66.34
mx3.latnet.lv A 92.240.66.34

92.240.66.32/27

Escalation listing seems correct.

As can be seen from this e-mail, the Spamhaus correctly retrieved *traceroute* information. However, Spamhaus wrongly assumed that LATNET Serviss is the holder of the domain name latnet.lv and blacklisted IP addresses without checking. Even after the explanation that AS5538 does not provide any transit services for the network 79.135.128.0/19, the staff of Spamhaus did not bother to double check their actions.

Unfortunately at that time CERT NIC.LV did not realize that Spamhaus did not have a clue from which AS were the IP addresses they had blacklisted. It just seemed too unprofessional to be true.

> As already mentioned above, abuse@latnet.lv is the abuse report e-mail for LATNET Serviss. IMCS is the holder of the domain name and processes incoming incident reports according to the agreement between the organisations. There are no rules forbidding using abuse report e-mails of other organisations. Anyone could use any e-mail address for the abuse reports, e.g. the one @gmail.com. However, this is not the reason to blacklist IPs of Google Inc.! And we are certain that Spamhaus would have never blocked those IP addresses.

CERT NIC.LV sent the following message to Spamhaus:

CERT NIC.LV to Spamhaus: Fri, 04 Jun 2010 14:30:19 +0300

What do you need to explain here?

You could traceroute the google.com and send it to us to explain it as well.

Where in your traceroute can you see AS5538?

Latnet Serviss is ISP an they have AS2588

; <<>> DiG 9.6.1-P2 <<>> mx latnetserviss.lv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20174
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;latnetserviss.lv. IN MX

;; ANSWER SECTION:
latnetserviss.lv. 1800 IN MX 10 mx.ls.lv.
latnetserviss.lv. 1800 IN MX 20 mx2.ls.lv.

Please remove the net 92.240.66.32/27 immediately.

Not trying to be rude here but please investigate more careful.

After this e-mail 92.240.66.32/27 was removed from the Spamhaus database without any further requests or responses.

CERT NIC.LV contacted LATNET Serviss as well as the Microlines and the "guilty" customer of Microlines to coordinate the incident handling. All parties responded. For more details see **Incident reports from Spamhaus**, page 21.

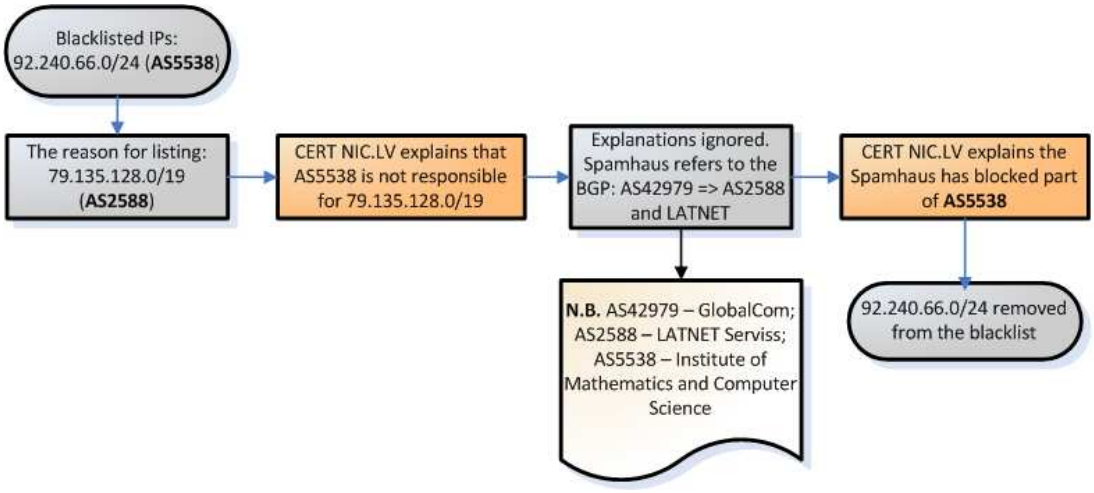
2.1.3. Summary

Spamhaus did not know from which AS were the IP addresses they blacklisted and did not care to investigate more properly even after explanatory e-mails sent by CERT NIC.LV. The main argument of Spamhaus was that they blacklisted the IP addresses of the domain name latnet.lv because this was the e-mail indicated as an abuse contact. Who is the holder of the domain name was not checked.

Spamhaus de-listed the IP addresses but did not send any incident reports to CERT NIC.LV team or any other explanations why the IP addresses had been blacklisted. Neither did Spamhaus acknowledge at any moment that the IP addresses had been wrongly blacklisted, nor they sent any apologies for the inconveniences or even damages caused to the end-users and service provider.

2.2. Blacklisted IPs – 92.240.66.0/24

2.2.1. Graphical Overview



2.2.2. Description

Nevertheless, the whole 92.240.66.0/24 network was blacklisted on 13.07.2010!

At first CERT NIC.LV sent the same message as previously, trying to call for some common sense:

CERT NIC.LV to Spamhaus: Tue, 13 Jul 2010 08:59:19 +0300

Hello!

IP address block 92.240.66.0/24 is blocked using wrong escalation procedure!

IP address block 79.135.128.0/19 Microlines has no network peering trough 92.240.64.0/19, AS5538.

http://www.robtex.com/route/79.135.128.0-19.html

Its totally wrong way to block AS5538 as responsible to 79.135.128.0/19 problems!

Please remove network 92.240.66.0/24 from blacklist!

The reply from Spamhaus again showed no understanding of the difference between the network peering and IP address of the domain name. Spamhaus still did not have a clue about the AS of the blacklisted IPs:

Spamhaus to CERT NIC.LV: Tue,13 Jul 2010 11:54:04 +0300

We see traceroutes and BGP table entries. Eg:

microlines.to.latnetserviss.lv (159.148.16.210) [AS 2588] 40 msec 36 msec 40

msec
gw-2.microlines.lv (79.135.128.35) [AS 2588] 36 msec 36 msec 40 msec

BGP: AS42979 => AS2588

As long as Microlines.lv is connected in any way to Latnet, they are responsible for their actions.

Now Microlines is allowing its cybercriminal customers host several DDoS C&C servers on their network. This must end. Now.

This response shows the following:

1. Spamhaus still cannot tell from which AS comes the IP range 92.240.66.0/24 and do not bother checking more carefully what they blacklist.
2. At no point did Spamhaus provide any evidence of C&C servers hosted by the customer of Microlines. However, Spamhaus called someone a criminal without a proper court procedure.
3. Spamhaus shows its inability to work with gathered information, which is sad because if such project as Spamhaus, which aims to improve the Internet, acts so unprofessionally it only results in making things worse.

IMCS again insisted that it had nothing to do with Microlines and it is completely wrong to block IP addresses allocated to the IMCS.

CERT NIC.LV to Spamhaus: Tue,13 Jul 2010 08:59:19 +0300

Do you understand difference between latnetseviss.lv and latnet.lv??

It's totally different domains and organisations!

What do you need to explain here?

You could traceroute the google.com and send it to us to explain it as well.

Where in your traceroute can you see AS5538?

Latnet Serviss is ISP an they have AS2588

; <<>> DiG 9.6.1-P2 <<>> mx latnetserviss.lv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20174
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;latnetserviss.lv. IN MX

;; ANSWER SECTION:
latnetserviss.lv. 1800 IN MX 10 mx.ls.lv.
latnetserviss.lv. 1800 IN MX 20 mx2.ls.lv.

Please remove the net 92.240.66.0/24 immediately.

Spamhaus replied the following:

Spamhaus to CERT NIC.LV: Tue, 13 Jul 2010 12:28 +0300

We are talking about AS42979.

Why does RIPE tell the world that AS42979 is run by Latnet and that Latnet handles abuse issues for it?

[..] *Parts of technical info from RIPE database omitted*

Information: http://www.ls.lv
Questions -- mailto:iproute@latnet.lv
Abuse reports --mailto:abuse@latnet.lv

But for AS2588, RIPE also states that Latnet also is in charge of it:

[..]*Parts of technical info from RIPE database omitted*

aut-num: AS2588
as-name: LatnetServiss-AS
descr: LATNET ISP
member-of: AS-LATVIA
[..]
Information: http://www.ls.lv
Questions -- mailto:iproute@latnet.lv
Abuse reports --mailto:abuse@latnet.lv

Surprisingly Spamhaus did not try to look at the AS5538 routing path! And instead of checking technical information still only looked at the names used by the parties. We think it is an unacceptable and wrong approach.

CERT NIC.LV to Spamhaus: Tue,13 Jul 2010 13:20:35 +0300

Your blacklist currently blocked part of AS5538!

inetnum: 92.240.66.0 - 92.240.66.15

netname: LUMII_INFR
remarks: INFRA-AW
mnt-irt: IRT-CERT-NIC-LV
descr: Raina Blvd. 29.,Riga
country: LV
admin-c: LSaS2-RIPE
tech-c: LSaS2-RIPE
org: ORG-IOMA1-RIPE
status: ASSIGNED PA
mnt-by: lumii-mnt
source: RIPE # Filtered

% Information related to '92.240.64.0/19AS5538'

route: 92.240.64.0/19
descr: SigmaNet komerctikls
origin: AS5538
mnt-by: lumii-mnt
source: RIPE # Filtered

==========

Where do you see that AS5538 announced any route for AS42979??

Only 6 hours later at ca. 19:45 +0300 AS5538 was delisted from the database of Spamhaus. Yet again, with no further explanations or response.

2.2.3. Summary:

Spamhaus repeatedly wrongly blacklisted the IP addresses of the domain name latnet.lv holder and did not check records of the e-mail exchange from the previous incident a bit more than a month before.

NIC.LV, CERT NIC.LV, thousands of Internet users – academic users, state and municipal institutions, non-profit organisations, companies, and individuals – had not violated Internet usage policies but still were not able to use the Internet services fully during the incident. Those thousands of affected users were not responsible for whatever other Internet users did. It is wrong to punish them for things done by someone else.

2.3. Blacklisted IPs – 159.148.79.0/24

2.3.1. Description

The following message from Spamhaus was received by CERT NIC.LV:

Spamhaus to CERT NIC.LV: Tue,13 Jul 2010 19:46:50 +0300

Perhaps you know someone who will null-route these two C&C controllers

running a large botnet DDoS attack:

79.135.152.xy
79.135.152.xz[6]

Then perhaps will work on removing this from the networks there:

route: 79.135.128.0/19
descr: Microlines
origin: AS2588
mnt-by: LATNET-MNT
source: RIPE # Filtered

This was the first time Spamhaus mentioned IP addresses 79.135.152.xy and 79.135.152.xz to CERT NIC.LV (or sent to abuse@latnet.lv). Unfortunately CERT NIC.LV did not have a chance to request additional information from Spamhaus and investigate the incident, because the next day, i.e. on 14 June, Spamhaus blacklisted the IP addresses 159.148.79.0/24 of LATNET Serviss, one of the largest Internet service providers in Latvia.

Spamhaus requested LATNET Serviss to block 79.135.128.0/19, i.e. the entire network of its subprovider Microlines. LATNET Serviss refused to block the entire IP address space because that would mean that many law abiding customers of Microlines would not be able to use the Internet. As nations around the globe recognise that access to the Internet is a basic human right it is unacceptable to block access of those who have not committed any illegal or improper acts. CERT NIC.LV fully supports this decision of LATNET Serviss.

LATNET Serviss agreed to block only the two mentioned IP addreses to get their mail servers delisted, even though no proper evidence that there are C&C controllers hosted was received from Spamhaus.

CERT NIC.LV, as a provider of incident response to LATNET Serviss, also sent an e-mail to Spamhaus asking for explanations:

CERT NIC.LV to Spamhaus

Do Spamhaus.org send any warning before blacklisting upstream provider servers?

Or it's common practice, blacklisting upstream provider without any complain?

[6] IP addresses are anonymised

Spamhaus to CERT NIC.LV

> We suggest you belive us, not the people at Latnet who, again, do not seem to have a clue. We've been at this anti-spam effort for longer than Latnet and Cert.lv have existed, okay? We know what we do.

Very unlikely. Not only because of the arrogant tone of the message, but also because Spamhaus had no idea of what they were blacklisting in the previous occasions.

CERT NIC.LV to Spamhaus

> Just called Microlines.lv - after quick check their support answered that IP 79.135.152.xy, 79.135.152.xz isn't used by any of customers.

Spamhaus to CERT NIC.LV

> Funny, as we checked recently and these were still the C&C servers for a DDoS botnet. Now how can that be?

Now, this time Spamhaus might be right. CERT NIC.LV asked LATNET Serviss to check on the traffic to/from these IP addresses and it showed significant activity. However, we cannot tell what kind of traffic and activity it was. No evidence of illegal activity from these IP addresses was aquired by CERT NIC.LV or LATNET Serviss.

CERT NIC.LV to Spamhaus

> Please remove LatnetServiss servers from blacklist, as we now LS currently negotiating with Microlines about their customers and working on this problem.

Spamhaus to CERT NIC.LV

> We are happy to hear this, but that's not the way our policies work. If LatnetServiss cannot stop routing cybercrime and abuse, more and more of what they route will be in the SBL. We will start with the IP space here, then move to the ASNs.

Spamhaus threatens to blacklist more and more IP addresses of the company which acts according to law, i.e. does not deny Internet access to those who have not done anything wrong and investigates the incident upon information received.

LATNET Serviss tried to explain that they serve thousands of customers and it is wrong to blacklist them for something that is done by other Internet user.

LATNET Serviss to Spamhaus

We are one of the biggest internet provider in Latvia

Spamhaus to LATNET Serviss

ok. and Latvia is one of the smallest nations in the world.

This sentence graphically illustrates the attitude of Spamhaus. It seems unbelievable that someone like Spamhaus treats incidents depending on the size of the Internet user community. Nevertheless this appears to be true.

More and more nations around the globe recognise the access to the Internet a human right. And human rights are not exercised based on some characteristics of an individual or a country that he calls home. They are universal! It is clear to such a small nation like us. LATNET Serviss refused to block Internet connectivity of those users who have not done anything wrong. Why do Spamhaus believe they are above the principles recognised by most nations?

Spamhaus to LATNET Serviss

They may tell you things, but we do not belive them. We belive they are making profit by hosting these Russian and/or Ukrainian cybercriminals. Or, if not this, they are just very, very dumb and there really is no difference to our users. Our users do not wish to have emails, or even packets, from places that host this type of crime.

People who cannot tell from which AS come IP addresses they blacklist should avoid calling other people “very, very dumb”. And, again, the attitude of representatives of Spamhaus seems unbelievable.

> LATNET Serviss rightfully asked CERT NIC.LV where could they seek for protection and appeal unlawful decision and actions of Spamhaus.
>
> CERT NIC.LV had to admit that there is no way by which an ISP or a user whose rights to access the Internet are denied by someone who considers him-/herself above the law could appeal.

2.3.2. Summary

As more and more nations around the globe recognise the access to the Internet a human right, we believe it is unacceptable to block or request to block the access to the Internet to those who have not committed any illegal or improper acts.

It is unacceptable to treat Internet users by the size or any other characteristics of the community the users are from.

CERT NIC.LV believes it is time to appoint an independent adjudicator to mediate on issues of disagreement between any entity exercising its power in an unjust way and the Internet user community.

3. Incident reports from Spamhaus

As mentioned above, after Spamhaus blacklisted IP addresses 159.148.79.0/24 of LATNET Serviss, CERT NIC.LV asked for the reason to handle incidents this way. The upstream provider first should be informed that there are any problems with IP addresses 79.135.152.xy and 79.135.152.xz.

CERT NIC.LV to Spamhaus

> Do Spamhaus.org send any warning before blacklisting upstream provider servers?
>
> Or it's common practice, blacklisting upstream provider without any complain?

Spamhaus stated that they had sent 5 abuse reports to abuse@latnet.lv and two notification e-mails regarding this particular incident involving 79.135.152.xy and 79.135.152.xz. Nevertheless, according to Spamhaus, the incident had not been investigated and no replies were received by Spamhaus.

Spamhaus to CERT NIC.LV: Wed,14 July 2010 18:09 +0300

> We have sent 5. In total since 2004, we have sent 11. None have bounced.

Spamhaus to CERT NIC.LV: Wed,14 July 2010 18:21 +0300

> MIstake, we have sent 7. abuse@latnet.lv was also notified on these two listings:
>
> 79.135.128.0/19
> Live microlines.lv SR04
> 2010-05-19 07:26:09
> SBL88903 Malware& botnet gang hosting
>
> 79.135.152.0/24
> Live microlines.lv SR15
> 2010-05-19 07:35:57
> SBL88104 SagadeLtd dedicated malware/spam block

Actually, Spamhaus counts all occasions regarding Microlines. However, they should concentrate only on reports regarding 79.135.152.xy and 79.135.152.xz, because according to the e-mail received from Spamhaus these two IP addresses were the reason for

blacklisting IP addresses of IMCS and LATNET Serviss. All other reports (if ever submitted) are irrelevant to this particular case.

> Notifications that any IP address has been blacklisted cannot be regarded as an incident report; mainly because it is *post factum* information. Immediate blacklisting of particular IP addresses used for spamming is commonly accepted practice to stop spam. In this case a *post factum* notification is understandable. But **what is the reason for blacklisting mail servers if any other potentially illegal activity is discovered**? *Post factum* notification in this case cannot be justified! In order to get their mail servers delisted organisations may take decisions and act without careful analysis of evidence provided by the party requesting the blocking of IP addresses.

CERT NIC.LV confirms that no replies were ever sent to Spamhaus, because no incident reports had ever been received from them by CERT NIC.LV via cert@nic.lv, abuse@latnet.lv or any other e-mail. CERT NIC.LV has received 5 incident reports concerning the IP range 79.135.128.0/19 used by Microlines but none of them had been submitted by Spamhaus. All the reports were investigated and solved with full cooperation from Microlines. Results were reported back to the initial submitters of the reports.

However, since the beginning of its operation in 2006[7] CERT NIC.LV has received three automated notifications from Spamhaus and a copy of an e-mail from Spamhaus to Microlines.

> ***Automated message from Spamhaus to info@microlines; abuse@microlines; abuse@latnet.lv: Wed,14 April 2010 01:26:07 +0300***

IP/cidr: 79.135.128.0/19
Problem: Malware & botnet gang hosting
SBL Ref: SBL88903

Microlines responded to this notification. CERT NIC.LV has no information if any incident reports were ever sent to Microlines prior to blocking. CERT NIC.LV has not received them.

This notification contained no new information, it only complains about the customer of Microlines in question. Activities of this customer were well known from the reports of AusCERT (23 March 2010 and 06 April 2010). Abuse contact of the said customer replied to messages sent by CERT NIC.LV (received on 23 March, 26 March and 07 April) and malware was removed within a couple of days. Microlines was informed about the fact that they were blacklisted.

CERT NIC.LV received a copy of the e-mail exchange between Spamhaus and Microlines regarding the IP addresses in question (as a copy sent to abuse@latnet.lv). As can be seen from the communication between the two parties, Spamhaus blacklisted IP addresses

[7] Initially known as LATNET CERT. LATNET CERT changed its name to CERT NIC.LV and was moved under NIC.LV in January 2008

79.135.128.0/19 (SBL88903) but Microlines asked to blacklist only the guilty IP addresses, not all other users who had not done anything wrong. At the end of e-mail exchange Spamhaus noted:

Spamhaus to Microlines, Cc to abuse@latnet.lv: Thu,15 Apr 2010 11:35:16 +0300

> If Microlines refuses to keep a clean network because it will cost your company money, we will just have to work with Latnet and ask them to help stop this problem coming from your company. We know that Latnet does not support Russian/Ukrainian cybercriminals.

In this e-mail Spamhaus warns Microlines that in case they do not do as requested, Spamhaus will contact LATNET (obviously LATNET Serviss, the upstream provider of Microlines at abuse@latnet.lv). No reports were received by CERT NIC.LV via abuse@latnet.lv. No reports were received by LATNET Serviss via any other e-mail. Blacklisting of IP addresses of LATNET Serviss and further notification about the fact of blacklisting cannot be considered an incident report.

Automated message from Spamhaus to abuse@latnet.lv: Tue,11 May 2010 14:48:00 +0300

> IP/cidr: 79.135.152.xyz/32
> Problem: Zeus botnet C&C
> SBL Ref: SBL90312

IP address checked. No ping response, ports closed (possibly in the firewall). No detailed reports were found at : https://zeustracker.abuse.ch/monitor.php?search=79.135.152.152.

Before this notification, on 6 April 2010 CERT NIC.LV received an incident report from AusCERT about the IP address used by the customer of Microlines accused by Spamhaus. The incident was investigated and the user informed. The user responded that the server had been hacked and used to host malware. The server was cleaned. Results of investigation were reported back to AusCERT. Later the pages were checked and no malware found. No further reports about the IP address were received.

No reply to the automated notification message from Spamhaus was sent.

Automated message from Spamhaus to abuse@latnet.lv: Wed,19 May 2010 10:16:00 +0300

> IP/cidr: 79.135.152.xyz/32
> Problem: fake antivirus/malware
> SBL Ref: SBL90696

The IP address given in the mail was checked. No exploits at the moment of check were found. The website offered its visitors to buy the software AntispywareSoft. Free download was not possible, hence, it was not possible to check if the software contains malware. Microlines was warned about possibly illegal activities on 22 March 2010 (reported by AusCERT), i.e. before the notification from Spamhaus was received. CERT NIC.LV reported back to AusCERT.

No reply to the automated notification message from Spamhaus was sent.

So, no incident reports with any additional details regarding IP addresses 79.135.152.xy and 79.135.152.xz were received from Spamhaus. *Post factum* notifications from Spamhaus did not contain references to these two particular IP addresses therefore they are not related to the blacklisting case described in this report.

3.1.1. Summary:

No proper incident reports were received by CERT NIC.LV regarding IP addresses 79.135.152.xy and 79.135.152.xz. Spamhaus declares that they have sent 5 incident reports and two notifications. Although it is not possible to identify who is telling the truth in this case, CERT NIC.LV affirms that it works in accordance to the industry standards and processes all properly formulated and submitted incident reports. CERT NIC.LV has never had any problems with any other entity fighting against illegal or improper activities on the Internet.

However, CERT NIC.LV confirms that it did not reply to the automated notification messages received from Spamhaus, even though IP addresses mentioned in the notifications were checked and CERT NIC.LV ensured that the affected party was informed about the fact of blacklisting. Notifications that any IP address has been blacklisted cannot be regarded as an incident report. Immediate blacklisting of particular IP addresses used for spamming is commonly accepted practice to stop spam. In this case a *post factum* notification is understandable. But **what is the reason for blacklisting mail servers if any other potentially illegal or activity is discovered**? *Post factum* notification in this case cannot be justified! In order to get their mail servers delisted organisations may take decisions and act without careful analysis of the evidence provided by the party requesting the blocking of IP addresses.

In all occasions when Microlines or its client in question were involved in incidents investigated by CERT NIC.LV, they cooperated and solved all the issues.

4. Summary and conclusions

The report contains information about three cases when IP addresses were blacklisted by Spamhaus. Even though CERT NIC.LV – a fighter against illegal and improper activities on the Internet– support anti-spam initiatives, we cannot agree with the way incidents are handled by Spamhaus.

Spamhaus **did not know** from which AS are the IP addresses they blacklisted and **did not care** to investigate more properly even after explanatory e-mails sent by CERT NIC.LV. The main argument of Spamhaus was that they blacklisted the IP addresses of the domain name latnet.lv because this was the e-mail indicated as an abuse contact. There are no rules forbidding using abuse report e-mails of other organisations. Anyone could use any e-mail address for the abuse reports, e.g. the one @gmail.com. However, this is not the reason to blacklist IPs of Google Inc.! And we are certain that Spamhaus would have never considered blocking those IP addresses. Unfortunately e-mails from Spamhaus showed that in their course of incident handling they **do not treat all Internet users equally**. Smaller countries may have a tough luck for fair treatment or careful investigation of incidents. It is unacceptable to treat Internet users by the size or any other characteristics of the community the users are from.

Thousands of Internet users – academic, state and municipal institutions, non-profit organisations, companies, and individuals – had not violated Internet usage policies but still were not able to use the Internet fully. Those thousands of affected users were not responsible for whatever other Internet users did. It is wrong to punish them for things done by someone else.

CERT NIC.LV believes it is time to appoint an **independent adjudicator** to mediate on issues of disagreement between any entity exercising its power in an unjust way and the Internet user community.