TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Laboratory Report No: 3

Malware – ITX8042

Student:
Predrag Tasevski

Lecture:
Toomas Lepik

05/10/11

Tallinn, Estonia

Table of Contents

PURPOSE

The main goal of laboratory report is to identify the responsibilities for the IP addresses below and how we can make connection to them. IP addresses are randomly chosen by the lecture.

IP addresses:

1. 69.163.171.238
2. 31.44.184.101
3. 188.72.228.69

External IP that is used for purpose of this test is following: 193.40.244.0/255[1]. The ISP that provides this network is EENet[2]. Organization that is behind is Tallinn Technical University, Estonia. City location is Tallinn and the region is Harjumaa. The phone number of my ISP is: +372 7302110. The e-mail we should report abuse are: first persons that is in charge: Viktor Borisevitch (e-mail: viktor@cc.ttu.ee and phone number: +372-2-536246) and Andres Lepp (e-mail: lovi@cc.ttu.ee and phone number: +372 6 203455). In addition, if we wont to submit an abuse we should use both persons of network administration and then we can submit and security incident on the following ISP e-mail: turvas@eeenet.ee [RIPE NCC].

All in all, Method 1 and Appendix 1 describes the website, tools and application that are used to conduct this laboratory report. In addition, Method 2 and Appendix 2 will introduce website tools and databases where we can check if following IP's have been reported before as abuse and security risk. Both methods are represented with answer and consequences confront in the result section.

Finally the conclusion made of all collected data will be concise in conclusion section of this report.

METHODS

First method describes and demonstrates web tools that have been used to collect the

1 I will not show my own IP address
2 EENet - http://www.eenet.ee/EENet/

needed information from the stated IP's addresses. Second method is pointing out website tools and databases that can be applied if the IP has been reported previously as a abuse, spam or security threat.

METHOD 1

Firstly, we need to collect as much as we can details about the IP address. In Appendix 1 is showing the wholly information of the IP's, contact details, organization name, address, location, state, country, technicians contact, abuse phone number, abuse e-mail, etc.

Depending on the location of IP we should make sure that not only we know the ISP or abuse contact details, but we should know national CERT[3] agency that is in charge too. Therefore, to collect the information we have used different web sites, agencies: [RIPE NCC][LACNIC][AfriNIC][APNIC][ARIN]. The above reference are agencies collected from IANA[4]. Authority responsible for global coordination of the Internet Protocol addressing systems [IANA].

Moreover, to have more details about the route of the IP's we are using command prompt in Windows 7 with the following command, where the results are presented in Appendix 2 section:

```
tracert [0.0.0.0]
```

To illustrate, the details information are presented in Result 1 section.

METHOD 2

After we have collected the wholly information about the concrete IP proposals, we should check if in addition those IP's previously have been reported as abused, spam or security threat. To complete the following method we need to check concrete database system that is offering following service. First that crossed on web is [MalwareURL] which is dedicated to fighting malware, trojans and a multitude of other web-related threats. In addition, we can check if the IP addresses are listed in anti-spam databases. With other words blacklist check [MyIPAddress].

3 CERT – Computer Emergency Response Team
4 IANA – Internet Assigned Numbers Authority - http://www.iana.org/

RESULTS

Results from Method 1 are presented in Result 1, further Method 2 is presented in Result 2.

RESULT 1

For each IP are presented only the most important data details that we need to collect for our goal. In addition, full description and details are presented in Appendix 1. The tables bellow are illustrating the most important information that we should look-for. In addition, the highlighted lines are indicating the abuse e-mail box that should be send mail too.

69.163.171.238
OrgName: New Dream Network, LLC Address: 417 Associated Rd. Address: PMB #257 City: Brea StateProv: CA PostalCode: 92821 Country: US #technician in charge OrgTechName: Nagel, Mark OrgTechPhone: +1-714-706-4182 OrgTechEmail: mna47-arin@dreamhost.com #abuse in charge OrgAbuseName: DreamHost Abuse Team OrgAbusePhone: +1-714-706-4182 OrgAbuseEmail: abuse@dreamhost.com

Table 1

31.44.184.101
person: Chris Burns address: Building 4 address: City West Office Park address: Gelderd Road address: Leeds LS12 6LX address: England phone: +44-208-901-2332 #abuse e-mail: abuse-mailbox: abuse@laveconetworks.co.uk

Table 2

88.72.228.69
role: Mannesmann Arcor Network Operation Center address: Arcor AG & Co. KG

```
address:        Department TBS
address:        Otto-Volger-Str. 19
address:        D-65843 Sulzbach/Ts.
address:        Germany
phone:          +49 6196 523 0864

#abuse e-mail
abuse-mailbox:  abuse@arcor-ip.de
```

Table 3

However, now that we know the abuse e-mail, phone number and contact person details, still is this information enough for us. If we look in details all of the IP's are from different countries. Therefore we need to find what is the national CERT agency contact details. First table is based in USA, therefore we need to use their reporting system, which is locate in the following link: http://www.us-cert.gov/ . Second table is UK, the national CERT agency link: www.ukcert.org.uk. Third table is based in Germany, the CERT agency link: http://www.cert-verbund.de/.

From the routing trace we can conclude that the first IP and the third respond and it did not miss route trace, where in the second IP, 31.44.184.101 there is miss route trace. That is why we will run this IP address to Method 2. Despite the fact, still we will run the rest of IP's in the Method 2, to be trusted that are not in the abuse list.

RESULT 2

Next step is to attempt to search the IP address to check if they have been previously report as a abuse, trojan, malware, security threat, etc.

To check and verify the security status we are using the service available [MalwareURL]. Where results for 69.163.171.238 and 88.72.228.69 are with status that have not been previously reported as abuse. On the other hand, 31.44.184.101 IP address is detected as an security threat before. More details are presented in Appendix 3. Where is demonstrating that the */404.php?type=stats&affid=531&subid=03&iruns* has been reported as malicious URL and it is in a blacklist of Google, MyWOT, etc.

Not only that it is listed in the malware database list, but also if we double check on service [MyIPAddress] that the 31.44.184.101 IP address is listed in few blacklist which is assess by DNSBL[5].

5 DNSBL – Domain Name System Blacklist

CONCLUSION

In conclusion, I would like to reiterate that the concrete IP's that we analysis in this report are demonstrating the process and methods that should be done in future to detect, report abuse, malware, threat, trojan, security risk, etc. Where we should gather the detail information, and to whom to turn the abuse. To be precise that are not in blacklist, spam list, etc.

In spite of following IP's: 69.163.171.238 and 88.72.228.69, from performing methods and delivering results are safe and secure, still think can be exploited in easy manners. The opposite, IP address 31.44.184.101 it has been already report infected as malicious code from few blacklist providers. When checking the DNS, host name is linking to UK company that deals with IP Transit. For further information please check the following link: http://www.laveconetworks.co.uk/.

In general, hope that laboratory report and the analyse will help to anyone else to guide them for future use.

APPENDIXES

Appendix 1 is list of details collected from service. Appendix 2 is trace route details. Where Appendix 3 is the result collected from the black list database.

APPENDIX 1

69.163.171.238

```
NetRange:       69.163.128.0 - 69.163.255.255
CIDR:           69.163.128.0/17
OriginAS:       AS26347
NetName:        DREAMHOST-BLK9
NetHandle:      NET-69-163-128-0-1
Parent:         NET-69-0-0-0-0
NetType:        Direct Allocation
Comment:        ** For abuse issues, please contact abuse@dreamhost.com **
RegDate:        2009-03-27
Updated:        2009-10-02
Ref:            http://whois.arin.net/rest/net/NET-69-163-128-0-1

OrgName:        New Dream Network, LLC
OrgId:          NDN
Address:        417 Associated Rd.
Address:        PMB #257
City:           Brea
```

```
StateProv:      CA
PostalCode:     92821
Country:        US
RegDate:        2001-04-17
Updated:        2009-03-25
Ref:            http://whois.arin.net/rest/org/NDN

OrgNOCHandle: ZD69-ARIN
OrgNOCName:   Network Operations
OrgNOCPhone:  +1-714-706-4182
OrgNOCEmail:  netops@dreamhost.com
OrgNOCRef:    http://whois.arin.net/rest/poc/ZD69-ARIN

OrgTechHandle: MNA53-ARIN
OrgTechName:   Nagel, Mark
OrgTechPhone:  +1-714-706-4182
OrgTechEmail:  mna47-arin@dreamhost.com
OrgTechRef:    http://whois.arin.net/rest/poc/MNA53-ARIN

OrgAbuseHandle: DAT5-ARIN
OrgAbuseName:   DreamHost Abuse Team
OrgAbusePhone:  +1-714-706-4182
OrgAbuseEmail:  abuse@dreamhost.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/DAT5-ARIN

RNOCHandle: ZD69-ARIN
RNOCName:   Network Operations
RNOCPhone:  +1-714-706-4182
RNOCEmail:  netops@dreamhost.com
RNOCRef:    http://whois.arin.net/rest/poc/ZD69-ARIN

RTechHandle: ZD69-ARIN
RTechName:   Network Operations
RTechPhone:  +1-714-706-4182
RTechEmail:  netops@dreamhost.com
RTechRef:    http://whois.arin.net/rest/poc/ZD69-ARIN

RAbuseHandle: DAT5-ARIN
RAbuseName:   DreamHost Abuse Team
RAbusePhone:  +1-714-706-4182
RAbuseEmail:  abuse@dreamhost.com
RAbuseRef:    http://whois.arin.net/rest/poc/DAT5-ARIN
```

31.44.184.101

```
inetnum:         31.44.184.0 - 31.44.184.255
netname:         Laveco
descr:           Laveco LTD.
country:         EU
admin-c:         CB9991-RIPE
tech-c:          CB9991-RIPE
status:          ASSIGNED PA
mnt-by:          Laveco
source:          RIPE # Filtered

person:          Chris Burns
address:         Building 4
address:         City West Office Park
address:         Gelderd Road
address:         Leeds LS12 6LX
```

```
address:         England
phone:           +44-208-901-2332
abuse-mailbox:   abuse@laveconetworks.co.uk
nic-hdl:         CB9991-RIPE
mnt-by:          Laveco
source:          RIPE # Filtered

% Information related to '31.44.184.0/24AS15884'

route:           31.44.184.0/24
descr:           Laveco LTD.
origin:          AS15884
mnt-by:          Laveco
source:          RIPE # Filtered
```

88.72.228.69

```
inetnum:         88.72.129.0 - 88.74.116.255
netname:         ARCOR-DSL-NET15
descr:           ARCOR AG
descr:           Alfred-Herrhausen-Allee 1
descr:           D-65760 Eschborn
country:         DE
admin-c:         ANOC1-RIPE
tech-c:          ANOC1-RIPE
mnt-by:          ARCOR-MNT
mnt-lower:       ARCOR-MNT
mnt-routes:      ARCOR-MNT
status:          ASSIGNED PA
source:          RIPE # Filtered

role:            Mannesmann Arcor Network Operation Center
address:         Arcor AG & Co. KG
address:         Department TBS
address:         Otto-Volger-Str. 19
address:         D-65843 Sulzbach/Ts.
address:         Germany
phone:           +49 6196 523 0864
remarks:         trouble:      Security issues mailto:abuse@arcor-ip.de
remarks:         trouble:      Information http://www.arcor.net
remarks:         trouble:      Peering contact mailto:peering@adm.arcor.net
remarks:         trouble:      Operational issues mailto:noc@adm.arcor.net
remarks:         trouble:      Address assignment mailto:ip-registry@arcor.net
admin-c:         SM9000-RIPE
admin-c:         JS19072-RIPE
admin-c:         DH6636-RIPE
admin-c:         AR9338-RIPE
admin-c:         TK11590-RIPE
admin-c:         RH12597-RIPE
admin-c:         MW877-RIPE
admin-c:         FB3293-RIPE
admin-c:         KJ993-RIPE
admin-c:         TG2269-RIPE
tech-c:          NH15-RIPE
nic-hdl:         ANOC1-RIPE
mnt-by:          ARCOR-MNT
source:          RIPE # Filtered
abuse-mailbox:   abuse@arcor-ip.de

% Information related to '88.72.0.0/14AS3209'
```

```
route:          88.72.0.0/14
descr:          ARCOR-IP
origin:         AS3209
mnt-by:         ARCOR-MNT
source:         RIPE # Filtered

% Information related to '88.64.0.0/12AS3209'

route:          88.64.0.0/12
descr:          ARCOR-IP
origin:         AS3209
mnt-by:         ARCOR-MNT
source:         RIPE # Filtered
```

APPENDIX 2

69.163.171.238

```
Tracing route to apache2-twiddle.browns.dreamhost.com [69.163.171.238]
over a maximum of 30 hops:

  1   154 ms    84 ms   181 ms  10.173.38.254
  2    <1 ms    <1 ms     1 ms  gw.campus [192.168.0.254]
  3    <1 ms     1 ms     1 ms  ttu-gw.eenet.ee [193.40.244.198]
  4    <1 ms     1 ms     1 ms  eenet-bckp.rt2.tal.ee.geant.net [62.40.124.49]
  5    14 ms    13 ms    16 ms  so-2-3-0.rt1.cop.dk.geant.net [62.40.112.121]
  6    13 ms    13 ms    13 ms  kbn-b2-link.telia.net [213.248.97.145]
  7    15 ms    16 ms    14 ms  kbn-bb1-link.telia.net [80.91.246.46]
  8    20 ms    20 ms    19 ms  hbg-bb1-link.telia.net [80.91.254.0]
  9    29 ms    29 ms    29 ms  ffm-bb1-link.telia.net [80.91.245.40]
 10    29 ms    29 ms    29 ms  ffm-b12-link.telia.net [213.155.130.146]
 11    36 ms    36 ms    37 ms  te0-3-0-7.ccr21.fra03.atlas.cogentco.com [130.11
7.14.169]
 12   125 ms   125 ms   124 ms  te0-2-0-6.ccr21.dca01.atlas.cogentco.com [154.54
.31.237]
 13   151 ms   151 ms   151 ms  te0-1-0-7.ccr21.atl01.atlas.cogentco.com [154.54
.24.154]
 14   151 ms   151 ms   151 ms  te0-2-0-1.ccr21.iah01.atlas.cogentco.com [154.54
.29.6]
 15   187 ms   187 ms   187 ms  te0-3-0-6.ccr21.lax01.atlas.cogentco.com [154.54
.0.237]
 16   189 ms   190 ms   189 ms  te7-1.mpd03.lax01.atlas.cogentco.com [154.54.28.
142]
 17   181 ms   182 ms   180 ms  38.122.20.218
 18   191 ms   194 ms   183 ms  ip-66-33-201-114.dreamhost.com [66.33.201.114]
 19   187 ms   188 ms   190 ms  apache2-twiddle.browns.dreamhost.com [69.163.171
.238]
```

31.44.184.101

```
Tracing route to 31.44.184.101 over a maximum of 30 hops

  1    88 ms    81 ms    74 ms  10.173.38.254
  2    <1 ms    <1 ms    <1 ms  gw.campus [192.168.0.254]
  3    <1 ms     1 ms     1 ms  ttu-gw.eenet.ee [193.40.244.198]
  4    <1 ms    <1 ms     1 ms  eenet-bckp.rt2.tal.ee.geant.net [62.40.124.49]
  5    13 ms    13 ms    13 ms  so-2-3-0.rt1.cop.dk.geant.net [62.40.112.121]
  6    14 ms    14 ms    14 ms  kbn-b2-link.telia.net [213.248.97.145]
  7    43 ms    14 ms    13 ms  kbn-bb1-link.telia.net [213.155.130.96]
```

```
  8    79 ms    20 ms    21 ms  hbg-bb1-link.telia.net [213.155.130.100]
  9    25 ms    25 ms    26 ms  adm-bb1-link.telia.net [213.155.133.38]
 10    26 ms    27 ms    27 ms  adm-b5-link.telia.net [80.91.253.188]
 11    31 ms     *        *     ecatel-ic-139206-adm-b5.c.telia.net [213.248.101
.90]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
```

88.72.228.69

```
Tracing route to dslb-088-072-228-069.pools.arcor-ip.net [88.72.228.69]
over a maximum of 30 hops:

  1   113 ms    74 ms    79 ms  10.173.38.254
  2    <1 ms    <1 ms    <1 ms  gw.campus [192.168.0.254]
  3     1 ms     1 ms     1 ms  ttu-gw.eenet.ee [193.40.244.198]
  4    <1 ms    <1 ms     1 ms  eenet-bckp.rt2.tal.ee.geant.net [62.40.124.49]
  5    21 ms    37 ms    14 ms  so-2-3-0.rt1.cop.dk.geant.net [62.40.112.121]
  6    13 ms    14 ms    13 ms  kbn-b2-link.telia.net [213.248.97.145]
  7    14 ms    14 ms    13 ms  kbn-bb1-link.telia.net [80.91.249.48]
  8    20 ms    20 ms    21 ms  hbg-bb1-link.telia.net [213.155.133.22]
  9   178 ms    23 ms    27 ms  hbg-b1-link.telia.net [80.91.251.78]
 10    25 ms    23 ms    22 ms  vodafone-ic-136086-hbg-b1.c.telia.net [213.248.7
5.218]
 11    34 ms    32 ms    32 ms  145.254.5.142
 12   118 ms   131 ms   132 ms  dslb-088-072-228-069.pools.arcor-ip.net [88.72.2
28.69]
```

APPENDIX 3

31.44.184.101

Domain matching **31.44.184.101** were found in our database.

17 other active domains were found on 3 IP(s) for AS15884 (SENSITIVE)

Show the report for AS15884 (SENSITIVE)

Malicious URLs on **31.44.184.101**

/404.php?type=stats&affid=531&subid=03&iruns

Additional information**Redirections**:

VirusTotal:

Anubis:

Wepawet:

ThreatExpert:

Other info:

Blacklist**Google**Google Diagnostic Page**My WOT**WOT Score Card**hpHosts**hpHosts listing**MalwareDomainList**MDL listingWhois and network detailsAdditional IP(s):Reverse:31.44.184.101
Name servers:

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the &quot;-B&quot; flag.

% Information related to '31.44.184.0 - 31.44.184.255'

inetnum:        31.44.184.0 - 31.44.184.255
netname:        Laveco
descr:          Laveco LTD.
country:        EU
admin-c:        CB9991-RIPE
tech-c:         CB9991-RIPE
status:         ASSIGNED PA
mnt-by:         Laveco
source:         RIPE # Filtered

person:         Chris Burns
address:        Building 4
address:        City West Office Park
address:        Gelderd Road
address:        Leeds LS12 6LX
address:        England
phone:          +44-208-901-2332
abuse-mailbox:  abuse@laveconetworks.co.uk
nic-hdl:        CB9991-RIPE
mnt-by:         Laveco
source:         RIPE # Filtered

% Information related to '31.44.184.0/24AS15884'

route:          31.44.184.0/24
descr:          Laveco LTD.
origin:         AS15884
mnt-by:         Laveco
source:         RIPE # Filtered
```

Bibliography

RIPE NCC: RIPE NCC, Data & Tools, 2011, https://www.ripe.net/data-tools

LACNIC: Internet Address Registry for Latin America and the Caribbean, REGISTRATION SERVICES , , http://lacnic.net/cgi-bin/lacnic/whois?lg=EN

AfriNIC: AfriNIC LTD, Query the AfriNIC Whois Database, 2011, http://www.afrinic.net/cgi-bin/whois

APNIC: APNIC, APNIC - Query the APNIC Whois Database, 2011, http://wq.apnic.net/apnic-bin/whois.pl

ARIN: ARIN, WHOIS-RWS, 2011, http://whois.arin.net

IANA: IANA, Number Resources, 2011, http://www.iana.org/numbers/

MalwareURL: The MalwareURL Team, The MalwareURL Team, 2011, http://www.malwareurl.com

MyIPAddress: What Is My IP Address, Blacklist Check, 2011, http://whatismyipaddress.com/blacklist-check